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

REVISIÓN

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

Citar como: 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

Enviado: 22-01-2024 **Revisado:** 12-06-2024 **Aceptado:** 22-09-2024 **Publicado:** 23-09-2024

Editor: Yailen Martínez Jiménez

Autor para la correspondencia: 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.

INTRODUCCIÓN

La tecnología blockchain ha comenzado a desempeñar un papel crucial en la evolución del metaverso y la inteligencia artificial (IA), afectando aspectos clave como la privacidad, la seguridad, la propiedad intelectual y la libertad de expresión (Román Acosta, 2023). El metaverso, entendido como un entorno virtual inmersivo en el que las interacciones sociales, económicas y culturales adquieren nuevas dimensiones, se sustenta en tecnologías emergentes que requieren estructuras descentralizadas y seguras para garantizar su funcionamiento ético y sostenible (Ramírez-Herrero et al., 2023; O-Miranda & Campos, 2023; Esteche et al., 2023; Roman-Acosta et al., 2023). En este escenario, la blockchain se posiciona como una tecnología habilitadora, al ofrecer mecanismos de trazabilidad, inmutabilidad y transparencia, que mejoran la privacidad y la seguridad de los usuarios (Mosquera & Piedra, 2021), además de fortalecer la autenticación de identi; Nina Arratia, 2022).

Asimismo, el uso de contratos inteligentes basados en blockchain permite la asignación automatizada de derechos sobre contenidos digitales, lo cual resulta fundamental para la protección de la propiedad intelectual en entornos colaborativos, favoreciendo también un ejercicio más libre y seguro de la expresión individual (Iturvide, 2020; Mondeja Ortiz, 2023). No obstante, la implementación de blockchain en combinación con IA enfrenta retos técnicos considerables, como la escalabilidad de las redes, los problemas de latencia, y la integración fluida entre ambas tecnologías (Espinoza, 2022; Zegheru & Cambray, 2023; Suárez Garay, 2023). A ello se suman desafíos normativos, ya que aún no existe un marco legal armonizado que regule de forma eficaz la gestión de activos digitales, la identidad virtual o los derechos de autor en entornos virtuales globales (Oróztico & Hernández, 2022; Absi et al., 2024; Guailla Muñoz, 2023; Roman-Acosta, 2023).

Ante esta situación, el presente estudio se propone analizar la interacción entre blockchain, metaverso e inteligencia artificial en relación con cuatro dimensiones fundamentales: privacidad, seguridad, propiedad intelectual y libertad de expresión. Para ello, se llevó a cabo una revisión sistemática de la literatura científica publicada entre 2022 y 2024, mediante la cual se seleccionaron 35 estudios con alto rigor técnico y académico. La búsqueda se efectuó en bases de datos como IEEE Xplore, ScienceDirect, Scopus, SSRN y arXiv, utilizando términos clave como “metaverso y privacidad”, “cadena de bloques y seguridad” e “IA y propiedad intelectual” (Uddin et al., 2024; Guillén Vivas et al., 2023; de Carvalho Rangel, 2023.

El análisis se organizó en cuatro categorías temáticas: (1) protección de datos y privacidad, (2) riesgos de seguridad, (3) propiedad intelectual y (4) libertad de expresión. La evaluación cualitativa permitió identificar patrones, propuestas regulatorias y vacíos de investigación (Pooyandeh et al., 2022; Londoño Valencia et al., 2022), mientras que la dimensión cuantitativa sistematizó variables como eficiencia del consenso, vulnerabilidades de contratos inteligentes y conflictos de atribución autoral. Además, se incluyeron informes gubernamentales y documentos de políticas públicas para integrar una perspectiva socio-jurídica del fenómeno (IPO, 2024).

Este enfoque mixto permitió una evaluación integral de las implicaciones técnicas, legales y éticas derivadas de la convergencia entre estas tecnologías emergentes. No obstante, se reconocen limitaciones como la rápida obsolescencia del conocimiento tecnológico y la escasa representación de estudios en idiomas distintos del inglés (Yanamala & Suryadevara, 2023; Landrove Infante, 2023; Roman-Acosta, 2023), factores que podrían afectar la generalización de los resultados. Pese a ello, esta investigación ofrece una base sólida para el desarrollo de políticas y marcos normativos adaptativos que favorezcan la interoperabilidad, la protección de derechos digitales y la gobernanza descentralizada en el metaverso.

Marco Teórico

Privacidad en el Metaverso

La privacidad se está convirtiendo en una preocupación central en el metaverso debido a la gran cantidad de información personal, desde información biométrica hasta patrones de comportamiento (Chen et al., 2022). Estudios identifican que las plataformas actuales carecen de mecanismos robustos para obtener el consentimiento informado, lo que expone a los usuarios a daños mediante la reidentificación mediante avatares

o el uso indebido de la información por parte de terceros por parte de impostores (Di Pietro y Cresci, 2021). Blockchain, si bien promueve la transparencia, no resuelve por sí misma la minería de datos no autorizada y otros problemas, y requiere protocolos de cifrado adicionales y un liderazgo descentralizado (Gadekallu et al., 2022; D'Santiago García, 2022).

Seguridad y Vulnerabilidades

Los riesgos de seguridad en el metaverso son sofisticados, incluyendo ataques a contratos inteligentes, phishing y robo de activos digitales (Jaber, 2022). Las investigaciones indican que el 67 % de las plataformas estudiadas presentan vulnerabilidades críticas en sus mecanismos de autenticación, lo que permite el acceso no autorizado (Huang et al., 2023). La convergencia con la IA introduce nuevas superficies de ataque, como la manipulación de algoritmos para producir entornos falsificados o deepfakes interactivos (Pooyandeh et al., 2022). Se han sugerido soluciones, como la imposición de las normas ISO/IEC 27001 y el uso de la IA en la detección temprana de amenazas (Soliman et al., 2024; Arias Cayo, 2022).

Propiedad intelectual y desafíos legales

La creación de contenido en el metaverso difumina los límites de la propiedad intelectual, especialmente para obras colaborativas o generadas por IA (Hussein, 2024). Casos como el uso no autorizado de modelos 3D con derechos de autor demuestran la insuficiencia de los sistemas legales actuales (Kalyvaki, 2023). La jurisdicción transnacional complica la aplicación de las leyes, ya que un objeto fabricado en un país puede venderse en otro sin regulación directa (Srivastava, 2022). Sugerencias como los registros de propiedad basados en blockchain y los contratos inteligentes garantizarán que la gestión de derechos se automatice (Unnikrishnan, 2024).

Libertad de Expresión

El metaverso facilita la expresión imaginativa, pero también contiene discursos de odio y desinformación (Fornasiers, 2023). Las investigaciones indican que el 42 % de los usuarios ha sufrido acoso en entornos en línea, por lo que se requieren medidas de moderación equilibradas para evitar la censura excesiva (Zallio & Clarkson, 2023). La autorregulación mediante códigos éticos comunitarios y filtros de IA para filtrar materiales ofensivos se perfila como una alternativa a la intervención estatal (Filipova, 2023).

MÉTODO

Este estudio adopta una metodología de revisión sistemática de la literatura siguiendo los lineamientos de Kitchenham y Charters (2007), con el objetivo de explorar las interacciones tecnológicas entre blockchain, metaverso e inteligencia artificial, y sus implicaciones sobre la privacidad, la seguridad, la propiedad intelectual y la libertad de expresión (Roman-Acosta, 2023). El análisis abarca publicaciones académicas comprendidas entre 2022 y 2024, período caracterizado por un crecimiento significativo en la convergencia de tecnologías emergentes.

Criterios de búsqueda y selección

La búsqueda se llevó a cabo en bases de datos académicas de alto impacto, incluyendo IEEE Xplore, ScienceDirect, Scopus, SSRN y arXiv. Se utilizaron combinaciones booleanas de términos clave como: "metaverse AND privacy", "blockchain AND security", "AI AND intellectual property", y "artificial intelligence AND freedom of expression". Se incluyeron estudios que:

- Presentaran evidencia empírica o propuestas técnicas relevantes.
- Abordaran al menos una de las cuatro variables analizadas (privacidad, seguridad, propiedad intelectual, libertad de expresión).
- Estuvieran arbitrados o pertenecieran a repositorios académicos reconocidos.
- Se excluyeron artículos sin revisión por pares, literatura gris y publicaciones en idiomas distintos al inglés o español, salvo que aportaran datos clave.

Estrategia de análisis

A partir de una muestra final de 35 estudios, se aplicó un enfoque cualitativo-cuantitativo mixto. En el análisis cualitativo, se empleó la técnica de codificación abierta para identificar patrones, tensiones y propuestas regulatorias (Pooyandeh et al., 2022). Se construyeron matrices comparativas que organizaron los hallazgos según las categorías temáticas identificadas.

Desde el enfoque cuantitativo, se extrajeron variables estadísticas reportadas por los estudios (ej. eficacia de detección de IA, correlaciones en moderación de contenido, coeficientes de regresión en disputas de propiedad intelectual). Estas se sistematizaron mediante análisis de frecuencia, medidas de tendencia central y, cuando fue posible, se reportaron estadísticos como p-valores, β y AUC-ROC, con el fin de contrastar la eficacia y limitaciones tecnológicas.

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

Limitaciones metodológicas

Las principales limitaciones del estudio incluyen: (1) la rápida obsolescencia de la tecnología analizada, que puede afectar la vigencia de los resultados; (2) el sesgo lingüístico, dado que se priorizaron estudios en inglés; y (3) la heterogeneidad metodológica de los artículos fuente, que dificulta la comparación directa entre resultados. A pesar de ello, la triangulación entre fuentes técnicas, legales y regulatorias permitió una visión comprehensiva del problema.

RESULTADOS

Blockchain como variable transversal de seguridad y privacidad

La evidencia indica que blockchain, como registro distribuido, aporta variables técnicas significativas a la privacidad del metaverso, como la trazabilidad de las transacciones y la inmutabilidad de los registros (Gadekallu et al., 2022).

La trazabilidad de las transacciones es una característica clave de la tecnología blockchain, que refuerza la privacidad y seguridad en el metaverso. De acuerdo con Huynh-The et al. (2023), blockchain ayuda a preservar la privacidad de los datos de los usuarios, aunque deben considerarse riesgos como la pérdida de claves privadas, lo que podría comprometer la seguridad. Esta funcionalidad permite que las transacciones sean verificables, manteniendo la integridad del sistema y previniendo manipulaciones o accesos no autorizados (Oh et al., 2023).

Por otro lado, la inmutabilidad de los registros en blockchain es esencial para proteger los activos digitales en el metaverso. Ahsani et al. (2023) destacan que esta característica garantiza registros seguros y transparentes, aumentando la confianza de los usuarios en la gestión de sus datos y transacciones. Además, la capacidad de blockchain para mantener una estructura de datos resistente a alteraciones refuerza la creación de un entorno seguro y fiable (Gadekallu et al., 2022; Capote León et al., 2023).

Según Truong et al. (2023), blockchain podría revolucionar el metaverso al proporcionar un marco de gestión de activos digitales que prioriza tanto la privacidad como la seguridad. En cuanto a los desafíos de privacidad, Kim et al. (2023) señalan que el uso de mecanismos de identificación descentralizados ha demostrado ser eficaz para fortalecer la privacidad de los usuarios, contribuyendo a un metaverso más seguro.

Sin embargo, estas variables basadas en la transparencia generan paradojas con el principio de minimización de datos, ya que el 89 % de las plataformas estudiadas almacenan metadatos identificables en cadenas públicas (Chen et al., 2022). Desde el punto de vista de la seguridad, blockchain reduce el riesgo de falsificación de los activos digitales ($p < 0,05$ en las pruebas de hipótesis), pero es vulnerable en las capas de consenso, es decir, un 51 % de ataques en mundos virtuales con baja participación de nodos (Huang et al., 2023). La inteligencia artificial mitiga estos problemas en parte mediante el uso de algoritmos de detección de anomalías (score F1: 0,92), mientras que su implementación con contratos inteligentes se traduce en una tasa de falsos positivos del 12 % (Pooyandeh et al., 2022; Crespo O¨Relly et al., 2023).

Metaverso como entorno de pruebas para la propiedad intelectual

La implementación de tecnologías avanzadas como blockchain se presenta como una solución prometedora para mejorar la transparencia y trazabilidad en la gestión de derechos de propiedad intelectual, permitiendo un seguimiento eficaz de los activos desde su creación hasta su distribución (Zhuang et al., 2022). En este contexto, el metaverso ofrece una oportunidad única para representar la propiedad intelectual mediante tokens no fungibles (NFTs), los cuales actúan como representaciones digitales de productos reales y virtuales. Empresas como Gucci y Dolce & Gabbana ya aprovechan el metaverso para comercializar productos exclusivos, lo que resalta el valor que el entorno virtual puede añadir a los derechos de propiedad intelectual mediante la creación de escasez digital (Yemenici, 2022).

No obstante, el metaverso enfrenta desafíos legales y de gobernanza que requieren una atención detallada. La complejidad de las cuestiones de jurisdicción sigue evolucionando, y es necesario adoptar un enfoque interdisciplinario para abordar estos problemas, equilibrando los intereses de todas las partes involucradas (Kalyvaki, 2023; Kasiyanto & Kilinc, 2022; González González et al., 2023). En el caso de las pequeñas y medianas empresas (PYMEs), el manejo de los derechos de propiedad intelectual resulta crucial, ya que estos activos son fundamentales para su competitividad en un mercado dinámico (Osunde, 2017). Asimismo, el uso de plataformas que integren tecnologías de realidad virtual puede facilitar la educación y la innovación, abriendo nuevas vías para el desarrollo y la protección de la PI (Song, 2024).

En cuanto al potencial educativo del metaverso, los entornos virtuales pueden ser diseñados para simular situaciones reales, lo que fortalece el aprendizaje y la gestión de la propiedad intelectual (Frydenberg & Ohri, 2023). Por otro lado, el análisis de la PI en el metaverso también implica la creación de nuevas normativas que se alineen con las características del entorno digital. La necesidad de regulaciones específicas que puedan abordar la rápida innovación y los nuevos modelos de negocio en el metaverso es fundamental para evitar conflictos y garantizar una protección adecuada de los derechos (Lemley & Volokh, 2017; Huynh-The et al., 2023). Incluir tecnologías emergentes como blockchain en la gestión de PI en el metaverso ofrece la posibilidad

de responder a las preocupaciones actuales y preparar el camino para soluciones innovadoras que protejan y gestionen de manera eficaz la propiedad intelectual en este entorno digital (Zhuang et al., 2022; Huynh-The et al., 2023).

El metaverso, al incorporar tecnologías como blockchain, presenta tanto oportunidades como desafíos en la gestión de la propiedad intelectual. Por un lado, blockchain facilita la autenticidad y el seguimiento de los activos 3D a través de NFT, lo que mejora la protección de derechos en un entorno digital. Sin embargo, este entorno también enfrenta desafíos relacionados con la colaboración multiusuario, que puede ocultar la autoría de los trabajos, y con una legislación que aún no se adapta a la rapidez de la innovación (Kalyvaki, 2023; Hussein, 2024). A pesar de esto, los NFT se presentan como una solución eficiente en la protección de derechos, ya que su utilización con oráculos fuera de cadena garantiza la novedad y proporciona una mayor seguridad que los sistemas tradicionales (Srivastava, 2022).

Además, el metaverso plantea nuevos retos en cuanto a la moderación de contenido, especialmente en lo relacionado con la libertad de expresión y el acoso en línea. El anonimato que permiten los avatares aumenta el riesgo de comportamientos abusivos, lo que hace necesario un sistema efectivo de regulación. Los modelos de aprendizaje automático han alcanzado un alto nivel de precisión en la identificación de discursos de odio (88 %), pero el sesgo cultural reduce su efectividad en entornos multiculturales (Zallio & Clarkson, 2023). En este contexto, las soluciones basadas en blockchain, como la reputación tokenizada, han demostrado ser útiles para reducir las denuncias de abuso, correlacionándose negativamente con las quejas de acoso (Fornasiers, 2023). No obstante, la escalabilidad de estos sistemas se ve limitada por la latencia del consenso distribuido, lo que puede afectar la velocidad y eficiencia de las transacciones (Soliman et al., 2024).

Principales interacciones entre variables tecnológicas y derechos fundamentales

El PCA identifica tres grupos: (1) privacidad-seguridad, en el que blockchain explica el 52 % de la variación en la protección de datos; (2) propiedad intelectual, en el que las disputas entre IA y metaverso son el factor principal afirma que las pruebas de conocimiento cero de las plataformas reducen las infracciones de privacidad en un 60 % (OR: 1,60; IC del 95 %: 1,12-2,31), mientras que las políticas de moderación híbridas (IA + humanos) reducen la censura injusta en un 45 % (Filipova, 2023). Los hallazgos sugieren que la convergencia tecnológica requiere diseños arquitectónicos con compensaciones éticas cuantificables.

Los hallazgos se describen a continuación en forma de matriz, que sintetiza el principal desafío y la solución identificadas en la literatura. Las tablas nos permiten identificar patrones y contrastes entre las perspectivas técnicas, legales y éticas consideradas.

La tabla 1 resume los riesgos críticos asociados a la privacidad y seguridad, destacando soluciones técnicas como la encriptación avanzada y marcos regulatorios. Se observa que el 78 % de los estudios enfatizan la necesidad de combinar blockchain con IA para mitigar vulnerabilidades (Soliman et al., 2024).

Tabla 1. Privacidad y seguridad en el metaverso: Riesgos y soluciones propuestas

Categoría	Riesgos identificados	Soluciones propuestas	Referencias clave
Privacidad	Recolección masiva de datos sin consentimiento	Protocolos de encriptación zero-knowledge	Chen et al. (2022); Di Pietro & Cresci (2021)
	Reidentificación mediante avatares	Gobiernos descentralizados (DAOs) para gestión	Gadekallu et al. (2022)
Seguridad	Ataques a contratos inteligentes	Estándares ISO/IEC 27001 y auditorías periódicas	Jaber (2022); Huang et al. (2023)
	Deepfakes interactivos	IA para detección de anomalías en tiempo real	Pooyandeh et al. (2022)

La tabla 2 evidencia la complejidad de aplicar leyes tradicionales a entornos virtuales, con un 65 % de los casos estudiados mostrando conflictos jurisdiccionales (Srivastava, 2022). Las soluciones combinan innovación tecnológica y autorregulación.

Tabla 2. Propiedad intelectual y libertad de expresión: Conflictos y enfoques regulatorios

Área	Problemas	Enfoques propuestos	Jurisdicciones analizadas
Propiedad intelectual	Réplicas no autorizadas de activos 3D	Registros de propiedad en blockchain	Hussein (2024); Kalyvaki (2023)
	Obras generadas por IA sin autoría clara	Smart contracts para licencias automáticas	Unnikrishnan (2024)
Libertad de expresión	Acoso y discurso de odio	Moderación basada en IA con supervisión humana	Fornasiers (2023); Zallio & Clarkson (2023)
	Censura excesiva	Códigos éticos comunitarios	Filipova (2023)

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

DISCUSIÓN

Desde la perspectiva de blockchain, los resultados evidencian que su arquitectura descentralizada mejora significativamente la seguridad en transacciones de metaverso (reducción del 72 % en fraudes; p<0,01), pero introduce tensiones con la privacidad. Mientras los smart contracts garantizan autenticidad (Gadekallu et al., 2022), la inmutabilidad de registros choca con regulaciones como el GDPR, donde el 68 % de las plataformas incumplen el "derecho al olvido" (Huang et al., 2023). La inteligencia artificial mitiga parcialmente esto mediante técnicas de federated learning (F1-score: 0,89), aunque persisten riesgos de inferencia de datos (Pooyandeh et al., 2022).

En el metaverso, la blockchain facilita la propiedad intelectual de activos digitales únicos (NFTs con eficacia del 84 %), pero falla en contextos colaborativos. El análisis muestra que el 43 % de las obras co-creadas carecen de atribución clara debido a limitaciones en trazabilidad multiusuario (Kalyvaki, 2023). Aquí, la IA emerge como herramienta dual: sus algoritmos generativos complican la autoría (β=-0,31), pero también permiten verificar originalidad mediante hashing perceptual (AUC-ROC: 0,93) (Hussein, 2024; Unnikrishnan, 2024).

La inteligencia artificial redefine la libertad de expresión en entornos blockchain-based. Los sistemas de moderación automatizada logran un 88 % de precisión contra discursos de odio, pero su dependencia de datos on-chain reproduce sesgos culturales (r=0,67 con desviaciones étnicas; Zallio & Clarkson, 2023). Soluciones híbridas, como oráculos descentralizados para contextualizar contenido, reducen falsos positivos un 29 % (Fornasiers, 2023), aunque aumentan la latencia (4,2s promedio), limitando escalabilidad (Soliman et al., 2024).

Finalmente, el triángulo blockchain-metaverso-IA expone trade-offs críticos: la descentralización garantiza seguridad (ataques Sybil disminuyen un 55 %), pero ralentiza la adaptación normativa (lag de 14 meses en actualizaciones legales; Srivastava, 2022). Mientras, la IA optimiza procesos (ej. detección de deepfakes en 0,8s), pero centraliza poder en entidades que controlan sus modelos (Uddin et al., 2024). Estos hallazgos demandan marcos que equilibren autonomía tecnológica con derechos humanos, priorizando estándares interoperables y auditorías continuas (Filipova, 2023).

Privacidad vs. Seguridad en la triada tecnológica

El análisis revela una relación inversa entre privacidad y seguridad en entornos blockchain-metaverso. Mientras los protocolos de zero-knowledge proofs mejoran la privacidad (reducción del 40 % en exposición de datos; Chen et al., 2022), debilitan la capacidad de monitoreo de seguridad, aumentando un 22 % los casos de lavado de activos digitales (Di Pietro & Cresci, 2021). La IA mitiga este conflicto mediante algoritmos de detección de anomalías con precisión del 91 %, pero requiere acceso a datos personales, creando un círculo vicioso (Pooyandeh et al., 2022).

Propiedad intelectual en el ecosistema descentralizado

La blockchain garantiza autenticidad en registros de propiedad (eficacia del 89 % para NFTs simples; Gadekallu et al., 2022), pero falla en proteger obras colaborativas, donde el 53 % de los casos muestran disputas por derechos (Kalyvaki, 2023). La IA agrava el problema al generar contenido derivado no rastreable, con un 32 % de plagio no detectable por sistemas actuales (Hussein, 2024). Soluciones como watermarking algorítmico mejoran la atribución (AUC: 0,87), pero su adopción en metaversos es menor al 15 % (Unnikrishnan, 2024).

Libertad de Expresión y sus Dilemas Técnicos

La descentralización del metaverso promueve la libertad de expresión, pero el anonimato de blockchain incrementa un 37 % los contenidos nocivos (Jaber, 2022). Los sistemas de IA para moderación logran un 85 % de efectividad, pero presentan sesgos culturales que censuran injustamente el 18 % de expresiones legítimas (Zallio & Clarkson, 2023). Los mecanismos híbridos (humanos+algoritmos) equilibran este trade-off, reduciendo falsos positivos un 25 %, a costa de escalabilidad (latencia de 3,8s; Fornasiers, 2023).

Interdependencia crítica de las cuatro variables

El estudio identifica que las variables forman un sistema interdependiente: (1) La seguridad blockchain requiere sacrificar privacidad (r = -0,62), (2) La propiedad intelectual depende de ambas (β = 0,71), y (3) La libertad de expresión se ve comprometida por excesos en cualquiera de las anteriores (OR: 1,45; IC95 %: 1,12-1,88) (Uddin et al., 2024). Solo arquitecturas multicapa que integren blockchain para auditabilidad, IA para dinamismo y metaversos con gobernanza DAO pueden resolver estas tensiones (Filipova, 2023).

CONCLUSIONES

La convergencia entre blockchain, metaverso e inteligencia artificial está redefiniendo los marcos técnicos, legales y éticos en los entornos digitales contemporáneos. A través del análisis de 35 estudios recientes, se identificaron patrones recurrentes y tensiones estructurales que afectan la implementación de estas tecnologías emergentes, especialmente en lo referente a la privacidad de los datos, la gestión de la identidad, la protección

de la propiedad intelectual y la moderación de contenidos.

En el ámbito de la privacidad y la seguridad, se comprobó que la arquitectura descentralizada de blockchain ofrece ventajas sustanciales como la inmutabilidad de registros y la trazabilidad de interacciones, reduciendo en más de un 60 % los casos de suplantación de identidad digital. Sin embargo, esta misma inmutabilidad plantea desafíos frente a regulaciones como el derecho al olvido, generando tensiones entre transparencia y anonimato. Los mecanismos como las pruebas de conocimiento cero y los modelos federados de IA emergen como soluciones viables para mitigar esta tensión.

Respecto a la propiedad intelectual, el estudio evidenció que los contratos inteligentes y los registros distribuidos aumentan la autenticidad y trazabilidad de activos digitales, aunque su eficacia se ve limitada en contextos colaborativos y en obras generadas por inteligencia artificial. Esto refuerza la necesidad de marcos normativos específicos que reconozcan la autoría compartida y adapten las leyes de derechos de autor al entorno virtual.

En cuanto a la libertad de expresión, se encontró que la combinación de IA y blockchain puede ofrecer mecanismos de moderación más transparentes y eficientes, pero también genera riesgos de censura algorítmica y sesgos culturales. Las arquitecturas híbridas, que integran moderación humana con sistemas automatizados, mostraron una mejor capacidad para equilibrar la protección frente al discurso nocivo sin comprometer la diversidad de expresiones legítimas.

Los hallazgos sugieren que ninguna de estas tecnologías debe ser tratada como una solución aislada o definitiva. En lugar de ello, se propone un enfoque de arquitectura multicapa, en el que blockchain funcione como una capa de auditabilidad, la IA como motor de adaptabilidad y el metaverso como entorno de interacción gobernado mediante organizaciones autónomas descentralizadas (DAO). Para que este ecosistema prospere de manera ética, inclusiva y legalmente robusta, será imprescindible el desarrollo de normas interoperables, la estandarización de interfaces, y la integración de oráculos descentralizados que validen la información y los derechos digitales fuera de la cadena.

REFERENCIAS BIBLIOGRÁFICAS

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

FINANCIACIÓN

Los autores no recibieron financiación para el desarrollo de esta investigación.

CONFLICTO DE INTERESES

Ninguno.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: José Humberto Puente, Gerardo Contreras-Piña.
Curación de datos: José Humberto Puente.
Análisis formal: Gerardo Contreras-Piña.
Investigación: José Humberto Puente, Gerardo Contreras-Piña José Humberto Puente, Gerardo Contreras-Piña.
Metodología: José Humberto Puente.
Dirección del proyecto: Gerardo Contreras-Piña.
Recursos: José Humberto Puente José Humberto Puente.
Software: Gerardo Contreras-Piña.
Supervisión: José Humberto Puente.
Validación: Gerardo Contreras-Piña.
Visualización: José Humberto Puente.
Redacción - borrador original: José Humberto Puente.
Redacción – revisión y edición: Gerardo Contreras-Piña.