FEBRERO 2026

RIBCi

RED IBEROAMERICANA DE BLOCKCHAIN
Y CIBERSEGURIDAD

3er SIMPOSIO IBEROAMERICANO DE BLOCKCHAIN Y CIBERSEGURIDAD

Blockchain en el Comercio Internacional

NACIONES UNIDAS
UNITED NATIONS
CEPAL

Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad

PROGRAMA IBEROAMERICANO
CYTED
CIENCIA Y TECNOLOGÍA PARA EL DESARROLLO

UNIVERSIDAD DE CHILE
Instituto de Estudios Internacionales

El 3er Simposio Iberoamericano de Blockchain y Ciberseguridad se llevó a cabo los días 20 y 21 de noviembre de 2025 en la ciudad de Santiago de Chile, en la sede de la Comisión Económica para América Latina y el Caribe (CEPAL) y en el Instituto de Estudios Internacionales de la Universidad de Chile.

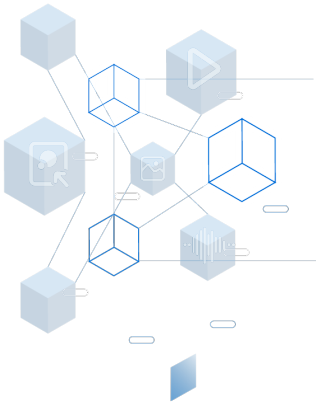
El encuentro fue coorganizado por la CEPAL, la Red Iberoamericana de Blockchain y Ciberseguridad (RIBCi) y el Instituto de Estudios Internacionales de la Universidad de Chile, con el apoyo del Programa Iberoamericano de Ciencia y Tecnología para el Desarrollo (CYTED), consolidándose como un espacio de referencia para el intercambio académico, técnico y estratégico en torno a los desafíos y oportunidades que presentan estas tecnologías emergentes en la región iberoamericana.

Instituciones acompañantes

El Simposio contó con el acompañamiento de las siguientes instituciones:

ÍNDICE

RIBCi
3er SIMPOSIO IBEROAMERICANO DE BLOCKCHAIN Y CIBERSEGURIDAD
Blockchain en el Comercio Internacional



EVALUACIÓN DE EFICACIA Y EFICIENCIA DEL USO DE PATRONES DE EVENTOS EN EL MODELADO DE CONTRATOS INTELIGENTES

Oscar Carlos Medina, Julio Martín Bono, Brenda Elizabeth Meloni, Ana María Strub, Marcelo Martín Marciszack, Diego Morardo

Universidad Tecnológica Nacional - Facultad Regional Córdoba. Argentina.

{omedina, jbono, bmeloni, astrub, mmarciszack}@frc.utn.edu.ar, diegomorardo@gmail.com

PALABRAS CLAVES

Experimento, Blockchain, Contratos inteligentes, Modelado, Patrones de eventos

RESUMEN

Este trabajo presenta los resultados de un experimento controlado diseñado para evaluar la eficacia y eficiencia en la comprensión de modelos conceptuales de contratos inteligentes mediante el uso de patrones de eventos. El estudio se realizó con 69 estudiantes universitarios avanzados de Ingeniería en Sistemas de Información. Se utilizaron tres tratamientos: patrón de eventos, descripción narrativa y ambos combinados. Los resultados muestran que el uso exclusivo de patrones de eventos mejora la eficiencia en la comprensión, mientras que no se hallaron diferencias significativas en la efectividad. Se discuten implicancias metodológicas y se proponen líneas futuras de investigación empírica en Ingeniería de Software.

OBJETIVOS

El objetivo principal es evaluar empíricamente la eficacia y la eficiencia del uso de patrones de eventos en la comprensión de modelos conceptuales de contratos inteligentes. Para ello, se diseñó y ejecutó un experimento controlado con estudiantes avanzados de Ingeniería en Sistemas de Información, considerados representativos de ingenieros de software en formación. Todo el material utilizado en el experimento se encuentra disponible en el sitio web del Centro de Investigación.

METODOLOGÍAS / HERRAMIENTAS

El diseño seleccionado fue inter-sujetos equilibrado, asignando un único tratamiento por sujeto. Este diseño busca evitar el efecto de aprendizaje o transferencia entre condiciones, garantizando independencia de las observaciones. Se utilizó asignación aleatoria balanceada y se evitaron amenazas a la validez mediante control de variables individuales, ceguera simple y supervisión estricta durante la ejecución. El estudio se realizó con 69 estudiantes de Ingeniería en Sistemas de Información, organizados en tres grupos que trabajaron con diferente representación: patrón de eventos, descripción narrativa y ambos combinados.

RESULTADOS

Los resultados mostraron que los estudiantes que utilizaron únicamente patrones de eventos obtuvieron mejores resultados descriptivos en ambas variables dependientes. Sin embargo, solo en la eficiencia se detectaron diferencias estadísticamente significativas entre grupos, concluyendo que los patrones permiten comprender correctamente los modelos en menor tiempo. En cuanto a la efectividad, si bien los patrones también alcanzaron los mejores valores medios, no se observaron diferencias significativas con los otros tratamientos.

Desde el punto de vista práctico, los resultados sugieren que el uso de patrones de eventos podría facilitar la tarea de modelado conceptual de contratos inteligentes, al permitir una representación más clara, estructurada y reutilizable. Esto puede resultar particularmente útil en entornos donde se requiere una rápida interpretación y validación de modelos, como sucede en la ingeniería de requisitos o el modelado ágil de sistemas basados en Blockchain.

No obstante, estos resultados deben interpretarse con cautela, ya que el experimento se llevó a cabo en un entorno académico con sujetos no expertos y con un único objeto experimental. Las amenazas a la validez fueron abordadas desde distintas dimensiones (interna, externa, de constructo y de conclusión), pero aun así, se reconoce la necesidad de réplicas y estudios complementarios en diferentes contextos y con muestras profesionales.

Entre las principales líneas de trabajo futuro, se destacan:

- Ampliar el estudio con nuevos experimentos en otros casos de uso, por ejemplo finanzas descentralizadas, “tokenización” de activos, salud, etc.
- Evaluar la comprensión con tareas de mayor complejidad, que incluyan diseño y verificación de contratos inteligentes.
- Incorporar herramientas automatizadas de generación de patrones y visualización interactiva.
- Investigar el impacto del uso de patrones en otras dimensiones de calidad de software como la mantenibilidad, trazabilidad o seguridad del modelo.

Los resultados obtenidos permiten avanzar en la validación de una propuesta me-

todológica basada en patrones de eventos, contribuyendo al desarrollo de enfoques sistemáticos para el modelado de contratos inteligentes en ingeniería de software.

BIBLIOGRAFÍA

[1] Maidin, S., Yahya, N., Fauzi, M., & Bakar, N., "Current and Future Trends for Sustainable Software Development: Software Security in Agile and Hybrid Agile through Bibliometric Analysis", Journal of Applied Data Sciences, 6(1), 311-324, 2024.

[2] Marciszack, M.M., Moreno, J.C., Sánchez, C.E., Medina, O.C., Delgado, A.F., Castro, C.S., "Patrones en la construcción del Modelo Conceptual para sistemas de información", 2018.

[3] Medina, O.C., Romero, R.A., Romero, M.S., Marciszack, M.A., Wismer, A.F., Morardo, D., Bossio, M.F., "Modelado de contratos inteligentes dirigido por casos de uso", RIA U.T.N., 2023, accedido desde https://ria.utn.edu.ar/items/40301b00-d974-4fc7-944d-f33811e2a86c.

[4] Medina, O.C., Marciszack, M.A., Romero, R.A., Meloni, B.E, Strub, A.M., Romero, M.S., Morardo, D., Nájera Gibert, J.I., "Una aproximación al uso de patrones de eventos para el modelado de contratos inteligentes", Revista Realidad Empresarial N° 19, Especial 2024, 7-18, Ed. Universidad UCA, El Salvador, 2024.

[5] CIDS Centro de Investigación, Desarrollo y Transferencia de Sistemas de Información, accedido desde http://www.cids.frc.utn.edu.ar.

[6] Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A., "Experimentation in Software Engineering" (2nd ed.). Springer, 2021.

[7] Genero Bocco, M., Cruz-Lemus, J. A., & Piattini Velthuis, M. G., "Métodos de investigación en ingeniería del software". Madrid, España: Editorial Ra-Ma, 2014.

[8] Khan, M.Z., Kumar, A., Kumar Sahu, A., "Blockchain applications in supply chain management: a systematic review of reviews", Global Knowledge, Memory and Communication, 74 (3-4): 1191–1208, 2025.

[9] Jedlitschka, A., Méndez Fernández, D., & Wagner, S., "Empirical software engineering: From experiment design to research reporting". In Perspectives on Data Science for Software Engineering, Springer, 2021.

[10] Torres, J. R., Rodríguez, D., & Piattini, M., "Improving requirements comprehension using conceptual models: An experimental study". Information and Software Technology, 141, 106728, 2022.

COMPUTACIÓN CUÁNTICA Y BLOCKCHAIN PERSPECTIVAS DE INVESTIGACIÓN PARA EL COMERCIO INTERNACIONAL

Fabián Castillo Peña, Rocío Sandoval Jácome y Liliana Gutiérrez Rancruel

Universidad Libre. Colombia.

{fabian.castillo, rocio.sandovalj, liliana-gutierrezr}@unilibre.edu.co

PALABRAS CLAVES

Computación Cuántica; Blockchain; Criptografía Post-Cuántica; Interoperabilidad; Trazabilidad; Logística Global; Contratos Inteligentes; Gobernanza Tecnológica

RESUMEN

La convergencia entre la Computación Cuántica y la tecnología Blockchain está configurando un nuevo paradigma para el Comercio Internacional, impulsado por avances en seguridad, optimización logística y automatización avanzada. El desarrollo de estándares de Criptografía Post-Cuántica (PQC), liderados por el NIST y la Comisión Europea, se posiciona como una respuesta urgente ante las capacidades emergentes de los computadores cuánticos y su potencial de comprometer los cimientos criptográficos del comercio global. Paralelamente, la simulación cuántica aplicada a redes logísticas globales abre oportunidades sin precedentes para la optimización de rutas, inventarios multimodales y trazabilidad avanzada, especialmente mediante algoritmos como QAOA (Quantum Approximate Optimization Algorithm - Algoritmo Cuántico Aproximado de Optimización).

El ecosistema Blockchain evoluciona hacia nuevas arquitecturas interoperables y cuánticamente seguras, integrando DLT (Distributed Ledger Technologies - Tecnologías de Registro Distribuido) con redes cuánticas basadas en QKD (Quantum Key Distribution - Distribución Cuántica de Claves). Dicho avance permite fortalecer procesos aduaneros, certificaciones de origen y auditorías digitales. Además, los contratos inteligentes comienzan a incorporar mecanismos criptográficos resistentes a ataques cuánticos, dando paso a los primeros modelos de contratos cuánticos.

La gobernanza tecnológica y las políticas públicas enfrentan el reto de anticiparse a los riesgos y desigualdades emergentes, en un contexto donde la brecha cuántica podría profundizar disparidades regionales. América Latina presenta avances relevantes, aunque fragmentados, según análisis del BID, lo cual destaca la necesidad de cooperación regional y adopción acelerada de estándares. Este estudio, sustentado en una revisión analítica de literatura especializada, evalúa el estado del arte, tendencias globales y retos estratégicos para la adopción de tecnologías cuánticas y Blockchain en el Comercio Internacional.

OBJETIVOS

Objetivo General: Analizar la convergencia entre la Computación Cuántica y la tecnología Blockchain, evaluando su impacto, oportunidades y desafíos en el Comercio Internacional, con énfasis en criptografía post-cuántica, logística global, contratos cuánticos, interoperabilidad, certificaciones y gobernanza tecnológica.

METODOLOGÍAS / HERRAMIENTAS

El estudio se desarrolla mediante una revisión documental analítica basada en literatura científica, técnica y normativa relevante. La metodología incluye:

- Análisis de estándares y migración criptográfica: A partir de los lineamientos del NIST (2024) y de la estrategia europea para la transición a la Criptografía Post-Cuántica (PQC), se examinan los modelos de migración y su aplicabilidad a sectores críticos del comercio internacional.

- Revisión de marcos regulatorios e interoperabilidad: Se analizan documentos oficiales de la Comisión Europea sobre EBSI (European Blockchain Services Infrastructure) para comprender principios, arquitectura y estándares de interoperabilidad aplicables a redes transfronterizas basadas en DLT (Distributed Ledger Technologies - Tecnologías de Registro Distribuido).

- Evaluación del uso de Blockchain en comercio internacional en América Latina: Se incorpora la evidencia del BID (2020) sobre adopción y limitaciones regionales de DLT (Distributed Ledger Technologies - Tecnologías de Registro Distribuido) para trazabilidad, aduanas y financiamiento del comercio.

- Análisis de perspectivas macroeconómicas y de gobernanza: Con base en el informe del FMI (2024), se evalúan implicaciones institucionales, éticas y estratégicas en la convergencia tecnológica cuántica-Blockchain.

- Estudio de simulación cuántica aplicada a logística: A partir de la literatura en arXiv (2024), se consultan aplicaciones de simulación cuántica y algoritmos de optimización, especialmente QAOA (Quantum Approximate Optimization Algorithm - Algoritmo Cuántico Aproximado de Optimización), en redes logísticas y gestión de inventarios.

- Revisión de iniciativas de colaboración regional: Se analiza la documentación de la red CYTED-RIBCi para identificar oportunidades de cooperación iberoamericana en Blockchain, seguridad y aplicaciones emergentes cuánticas.

Este enfoque metodológico permitió articular tendencias globales, marcos regulatorios y escenarios de adopción tecnológica en el Comercio Internacional.

RESULTADOS

Objetivos Específicos:

- Examinar el estado del arte y los avances globales en Criptografía Post-Cuántica (PQC) y su impacto en la protección de datos y operaciones del comercio internacional.

- Analizar el potencial de la simulación cuántica en redes logísticas globales, especialmente en optimización de rutas, inventarios y trazabilidad.

- Explorar la evolución de los contratos inteligentes hacia contratos cuánticos, evaluando casos de uso emergentes y capacidades criptográficas resistentes a ataques cuánticos.

- Evaluar los desafíos y oportunidades de la interoperabilidad híbrida entre DLT (Distributed Ledger Technologies - Tecnologías de Registro Distribuido), sistemas legacy y redes cuánticas, contrastando avances entre regiones.

- Revisar el papel de las certificaciones internacionales y estándares ISO en un entorno Blockchain–Cuántico orientado a la trazabilidad y la seguridad regulatoria.

- Analizar las implicaciones de políticas públicas, gobernanza y ética frente a la convergencia cuántico–Blockchain y su impacto en la brecha regional, especialmente en América Latina.

BIBLIOGRAFÍA

[1] NIST (2024). Criptografía Post-Cuántica (PQC) Selected Algorithms. Recuperado de https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2024.

[2] European Commission (2023). A Coor-dinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. Recuperado de https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[3] European Commission. EBSI Overview [Web page]. Recuperado de https://ec.europa.eu/cefdigital/wiki/display/EBSICOM/EBSI+Overview.

[4] IDB (2020). Blockchain y comercio internacional. en América Latina. Recuperado de https://publications.iadb.org/publications/es/document/Revista-Integracion--Comercio-Ano-24-No-46-Octubre-2020-Blockchain-y-comercio-internacional-Nuevas-tecnologias-para-una-mayor-y-mejor-insercion-internacional-de-America-Latina.pdf.

[5] FMI (2024). La economía mundial transformada por la inteligencia artificial ha de beneficiar a la humanidad [Blog]. Recuperado de https://www.imf.org/es/Blogs/Articles/2024/01/14/ai-will-transform-the-global-economy-lets-make-sure-it-benefits-humanity.

[6] arXiv (2024). Quantum Computing in Logistics and Supply Chain Management - an Overview. Recuperado de https://arxiv.org/html/2402.17520v1.

[7] CYTED - RIBCi (n.d.). Red Iberoamericana de Blockchain y Ciberseguridad. Recuperado de https://www.cyted.org/rede/red-iberoamericana-de-blockchain-y-ciberseguridad-ribci.

CONFIANZA DIGITAL Y CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS

Ferney Martínez Ossa,
Science and Technology Corporation for the Development of the Naval, Maritime and Riverine Industry, Colombian Navy (COTECMAR). Colombia.
fmartinez@cotecmar.com

Luis Enrique Sánchez, Antonio Santos-Olmo, David G. Rosado y Eduardo Fernández-Medina,
Universidad de Castilla-La Mancha. España.

PALABRAS CLAVES

Infraestructuras críticas, ciberseguridad marítima, análisis de riesgos

RESUMEN

El Marco MARISMA-SHIPS atiende la necesidad crítica de proteger la Infraestructura Crítica marítima mediante una gestión de riesgos dinámica y basada en patrones, asegurando la resiliencia operacional de las plataformas. Esta capacidad de análisis continuo y actualizado es fundamental para el Comercio Internacional, ya que la seguridad de las rutas marítimas y de la información a bordo es crucial para la estabilidad de la cadena de suministro global. La implementación de este framework (especialmente en el desarrollo de POSEIDÓN) permite una visibilidad avanzada del riesgo, esencial para el comercio. Al proporcionar una evaluación rigurosa de la ciberseguridad del activo físico marítimo, se mitigan interrupciones que podrían paralizar el flujo de mercancías a nivel mundial. El objetivo final es establecer una protección integral de extremo a extremo que salvaguarde no solo la operación naval, sino también la confianza y la continuidad de las transacciones comerciales y logísticas que dependen de esta infraestructura.

OBJETIVOS

El objetivo primordial del modelo MARISMA-SHIPS es establecer una gestión de riesgos de ciberseguridad sistemática y eficiente para las Infraestructuras Críticas (IC) marítimas. Esto se logra mediante la adaptación de estándares internacionales en un patrón de riesgos especializado que se centra en los activos navales esenciales, lo que permite la evaluación rigurosa de vulnerabilidades y la reducción significativa del tiempo necesario para el análisis en la industria. Un segundo objetivo clave es garantizar la resiliencia operacional continua de estas IC mediante un enfoque dinámico. El sistema está diseñado para que los incidentes de seguridad retroalimenten continuamente el análisis de riesgo, manteniendo la evaluación actualizada en tiempo real, facilitando así la implementación de planes de mitigación efectivos.

METODOLOGÍAS / HERRAMIENTAS

Esta ponencia aborda la necesidad urgente de estrategias de mitigación de riesgos y presenta el Marco de Análisis de Riesgos POSEIDÓN como una solución sistemática diseñada para fortalecer la resiliencia en este sector vital. La metodología MARISMA-SHIPS es un sistema dinámico y basado en patrones para la gestión de riesgos de ciberseguridad en Infraestructuras Críticas (IC) Marítimas.

1. Metodología Base: Se fundamenta en la aplicación de un “patrón de riesgos” especializado para activos críticos a bordo de buques, garantizando un análisis sistemático y eficiente. Ciclo Dinámico: Implementa una gestión de riesgo en tiempo real. Los incidentes y eventos de seguridad retroalimentan continuamente el sistema, lo cual es esencial para mantener la validez del análisis en un entorno de IC en constante amenaza.

2. Herramienta Usada Herramienta Principal: El marco MARISMA, y por ende su extensión MARISMA-SHIPS, se implementa utilizando la plataforma eMarisma (o MARISMA 2.0) que se distingue por: -Gestión de Eventos Dinámica: Actualiza el riesgo del proceso en cada momento con base en las incidencias. -Patrones Reutilizables: Permite la creación de modelos personalizados (como el patrón SHIPS) para reducir el tiempo de análisis. -Generación Automática: Implementa una gestión integral que genera automáticamente el mapa de riesgos y el plan de tratamiento.

RESULTADOS

La investigación se centró en el diseño, desarrollo y aplicación del modelo MARISMA-SHIPS en un entorno marítimo real, validando su eficacia en la identificación y gestión de riesgos de ciberseguridad a bordo de buques. Enfoque Integral: El modelo integra metodologías y estándares internacionales con innovaciones adaptadas específicamente a las necesidades del sector marítimo. Viabilidad Industrial: Los resultados demuestran que la implementación de MARISMA-SHIPS es viable para su integración en la línea de producción de un astillero, destacando su utilidad práctica para la industria marítima. Esta experiencia ha sido esencial para cerrar la brecha entre la academia y la industria, permitiendo al grupo de investigación desarrollar patrones con un mayor nivel de especificación y lograr análisis de riesgo más precisos. El modelo integra estándares globales con innovaciones específicas para el sector naval, demostrando en un caso de estudio real su viabilidad y utilidad para mejorar la resiliencia operacional y ser integrado en líneas de producción.

BIBLIOGRAFÍA

[1] U. N. C. on Trade, Development, Review of Maritime Transport 2023, 2023. URL https://unctad.org/publication/review-ma-

ritime-transport-2023

[2] G. A. Weaver, B. Feddersen, L. Marla, D. Wei, A. Rose, M. V. Moer, Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach, Transportation Research Part C: Emerging Technologies 137 (2022) 103423. doi:10.1016/J.TRC.2021.103423.

[3] C. Mascarenas, A. I. Vázquez, Notes on maritime cybersecurity in ship design, RINA, Royal Institution of Naval Architects - International Conference on Marine Design 2020, Papers (2020) 91–99.

[4] D. Heering, Ensuring cybersecurity in shipping: Reference to estonian shipowners, TransNav 14 (2020) 271–278. doi:10.12716/1001.14.02.01.

[5] V. Greiman, Navigating the cyber sea: Dangerous atolls ahead, 14th International Conference on CyberWarfare and Security, ICCWS 2019 (2019) 87–93.

[6] IEEE, 2021 world automation congress, wac 2021, World Automation Congress Proceedings 2021-August.

[7] B. Xing, J. Dai, S. Liu, Enforcement of opacity security properties for ship information system, International Journal of Naval Architecture and Ocean Engineering 8 (2016) 423–433. doi:10.1016/j.ijnaoe.2016.05.012.

[8] C.-H. Chang, S. Wenming, Z. Wei, P. Changki, C. A. Kontovas, Evaluating cybersecurity risks in the maritime industry: a literature review, in: Proceedings ofthe International Association ofMaritime Universities (IAMU) Conference, International Association of Maritime Universities, 2019, pp. 79–86. URL https://researchonline.ljmu.ac.uk/id/eprint/11929/

[9] E. Cassi, J. P. Cavanna, P. Scialla, The cyber risk and its management in the marine industry, Technology and Science for the Ships of the Future - Proceedings of NAV 2018: 19th International Conference on Ship and Maritime Research (2018) 950–959doi:10.3233/978-1-61499-870-9-950. URL https://ebooks.iospress.nl/doi/10.3233/978-1-61499-870-9-950

[10] F. Martınez, L. E. Sánchez, A. Santos-Olmo, D. G. Rosado, E. Fernández-Medina, Maritime cybersecurity: protecting digital seas, International Journal of Information Security 23 (2024) 1429–1457. doi:10.1007/S10207-023-00800-0/TABLES/7. URL https://link.springer.com/article/10.1007/s10207-023-00800-0

DELITOS CON CRIPTOMONEDAS. ESTRATEGIAS DESDE LA JUSTICIA ARGENTINA

Herminia Beatriz Parra de Gallo

Universidad Católica de Salta. Argentina

bgallo@ucasal.edu.ar

PALABRAS CLAVES

Criptomonedas, Delitos Informáticos, Herramientas forenses basadas en Blockchain

RESUMEN

El presente trabajo aborda la problemática de los delitos vinculados con el uso de criptomonedas y los desafíos que estos representan para el sistema judicial argentino. Las criptomonedas, caracterizadas por su naturaleza descentralizada, la ausencia de intermediarios y su operatoria transnacional, han generado nuevas modalidades delictivas que complejizan la investigación, la obtención de pruebas y la persecución penal. En este contexto, se analizan los principales tipos de delitos asociados, el marco normativo vigente en la Argentina y las instituciones internacionales que también abordan la problemática, así como los desafíos probatorios que enfrenta la Justicia, haciendo especial énfasis en las herramientas que están disponibles desde una perspectiva empírica y teórica. Asimismo, se presentan metodologías, protocolos y herramientas tecnológicas que permiten fortalecer las capacidades institucionales para la investigación de estos delitos, promoviendo la cooperación interinstitucional y el uso de soluciones tecnológicas especializadas.

OBJETIVOS

El objetivo general de este trabajo es analizar las estrategias adoptadas por la Justicia Argentina frente a los delitos con criptomonedas, identificando los principales desafíos y las herramientas disponibles para su abordaje.

Como objetivos específicos se plantean:

- Describir las características fundamentales de las criptomonedas que impactan en su uso delictivo.
- Identificar la tipología de delitos más frecuentes vinculados con criptoactivos.
- Analizar el marco normativo nacional e internacional aplicable a estos delitos.
- Examinar los principales desafíos probatorios asociados a la investigación de criptoactivos.
- Presentar metodologías, protocolos y herramientas tecnológicas utilizadas en la preservación de evidencia y la forensia de blockchain.

METODOLOGÍAS / HERRAMIENTAS

Se realiza una revisión conceptual sobre las criptomonedas y su funcionamiento, destacando aquellos aspectos que dificultan su control por parte de la justicia.

Además de describir brevemente la evolución lograda en la incorporación de Blockchain en ámbitos financieros de Latinoamérica [1], se describe el uso de las criptomonedas en la comisión de delitos informáticos.

A continuación, se aborda la normativa judicial argentina tomándose como ejemplo el "PROTOCOLO GENERAL DE ACTUACIÓN DESTINADO A PRIMEROS INTERVINIENTES PARA LA IDENTIFICACIÓN Y SECUESTRO DE POTENCIALES ELEMENTOS DE PRUEBA DE CRIPTOACTIVOS" (Resolución 117/2025 del Ministerio de Seguridad de la Nación Argentina) [2], para explicar cómo se está encarando este delito desde la Justicia Argentina. Dicho protocolo establece lineamientos claros para la intervención judicial y policial, contemplando la cadena de custodia digital, la trazabilidad de la evidencia y los distintos tipos de actuación según la naturaleza del soporte (billeteras físicas, billeteras en papel, aplicaciones, plataformas de intercambio, entre otros), y resulta de mucha utilidad para enmarcar los delitos vinculados a las criptomonedas pues incluye instancias de aprendizaje para el neófito en el tema a partir de un glosario de términos técnicos y diagramas de actividades que explican -ante un delito de estas características- como debe actuar y las responsabilidades que le caben al primer interviniente y a los restantes actores.

Se describe una metodología clásica para el análisis forense Blockchain [3], basadas en el análisis del ciclo de vida de la evidencia digital, que incluye las etapas de identificación, recolección, preservación, examen, análisis y reporte, garantizando la integridad y validez probatoria de la información obtenida.

Se presenta además diversas herramientas tecnológicas que resultan de interés para la investigación de delitos con criptomonedas. Entre ellas se destacan:

- Plataformas de computación en la nube orientadas a la investigación forense, como BlockSLaaS [4], que permiten compartir información de manera segura entre las partes involucradas, evitando colisiones y fortaleciendo la seguridad de los datos.
- Soluciones específicas como Block-4Forensic [5], diseñadas para la forensia de vehículos conectados, que aportan un entorno confiable y trazable para el análisis posterior a incidentes.

En particular se muestra el “Prototipo para la Detección y Análisis de Perfiles Transaccionales de Billeteras Tron” [5] orientadas al análisis de transacciones e identificaciones de direcciones, que permiten reconstruir flujos financieros y detectar vínculos entre billeteras.

Estas herramientas, combinadas con protocolos claros de actuación y cooperación interinstitucional, constituyen un soporte fundamental para la Justicia en el abordaje de delitos complejos vinculados con criptoactivos.

RESULTADOS

Del análisis realizado se desprende que los delitos con criptomonedas representan un desafío creciente para la Justicia Argentina, tanto por la complejidad técnica de las tecnologías involucradas como por su carácter transnacional.

No obstante, se observa un avance significativo en la adopción de marcos normativos, protocolos de actuación y herramientas tecnológicas que fortalecen las capacidades de investigación y persecución penal.

La implementación de metodologías de forensia de blockchain, junto con la preservación adecuada de la cadena de custodia digital, permite mejorar la calidad de la prueba y aumentar las probabilidades de éxito en los procesos judiciales.

Asimismo, la cooperación internacional y el trabajo coordinado con organismos especializados resultan esenciales para enfrentar un fenómeno que trasciende las fronteras nacionales.

En conclusión, si bien los delitos con criptomonedas plantean desafíos relevantes, la articulación entre normativa, metodologías y herramientas tecnológicas ofrece a la Justicia Argentina un marco promisorio para su abordaje, contribuyendo a una respuesta más eficaz frente a este tipo de criminalidad emergente.

BIBLIOGRAFÍA

[1] Castillo Vanegas, A. C., & Avila Zambrano, F. L. (2023). Uso de criptomonedas como moneda de curso legal en los paises Latinoamericanos.

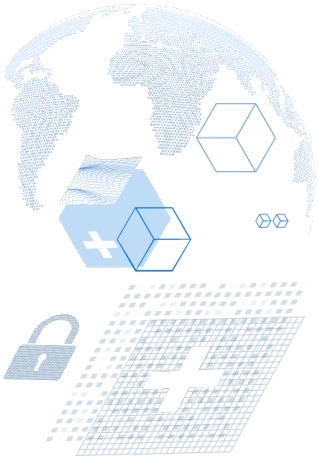
[2] Ministerio de Seguridad de la Nación, Argentina, Protocolo General de Actuación para la identificación, preservación y secuestro de potenciales elementos de prueba vinculados con Criptoactivos https://www.boletinoficial.gob.ar/detalleAviso/primera/320271/20250129.

[3] Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions.Electronics,13(17), 3568. https://www.mdpi.com/2079-9292/13/17/3568.

[4] S. Rane, A. Dixit, Blockslaas: registro seguro como servicio asistido por blockchain para análisis forense en la nube. En Conferencia Internacional sobre Seguridad y Privacidad, pp. 77-88, Springer, 2019.

[5] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, S. Uluagac, Block4forensic: un marco de blockchain ligero integrado para aplicaciones forenses de vehículos conectados. IEEE Commun. Mag. 56(10), 50–57 (2018).

[6] Terrile, R. (2025). Prototipo para la Detección y Análisis de Perfiles Transaccionales de Billeteras Tron. https://drive.google.com/file/d/13B7jau638xcLNblUP9_h0lH-CyhJdFATm/view?usp=drive_link.



PILARES DE SEGURIDAD INTEGRAL PARA DISPOSITIVOS MÉDICOS

Marcela Ulloa

Universidad Mayor. Chile.

marcela.ulloa@umayor.cl

PALABRAS CLAVES

Dispositivos médicos, Ciberseguridad, Sistema de salud

RESUMEN

La ciberseguridad en sistemas de salud enfrenta una fuerte fragmentación del conocimiento debido a la diversidad y dispersión de normas, marcos regulatorios y evidencia científica aplicada a dispositivos médicos interconectados. Para demostrar esta complejidad, se integraron múltiples estándares (ISO, NIST, HIPAA, ENISA, GDPR y HITRUST), además de literatura científica y vulnerabilidades documentadas. Con base en esta revisión, se proponen pilares que sustentan un modelo integral y adaptable de seguridad, orientado a fortalecer la infraestructura digital sanitaria, apoyar auditorías continuas y mejorar la resiliencia frente a amenazas emergentes.

OBJETIVOS

Desarrollar una herramienta práctica de apoyo para la implementación de estrategias de seguridad en dispositivos médicos.

METODOLOGÍAS / HERRAMIENTAS

El método empleado en la investigación es exhaustivo, con un enfoque integrado y estructurado orientado a desarrollar un modelo teórico sólido para la seguridad de la información en dispositivos médicos.

RESULTADOS

Los resultados derivados de la aplicación de la metodología de revisión integral, estructurada en cuatro fases. Cada etapa permitió la organización y el análisis sistemático de la información, contribuyendo a una comprensión clara y bien fundamentada del tema investigado.

- **Planteamiento del Problema:**

  La información sobre riesgos y vulnerabilidades en dispositivos médicos está dispersa, lo que dificulta decisiones coherentes y aumenta las brechas de seguridad. Aunque existen normas como ISO, NIST y HITRUST, su aplicación es desigual. Por ello, se requiere un modelo integrado que unifique y organice esta información para mejorar la protección y la gestión de la ciberseguridad en salud.

- **Revisión de regulaciones, estudios de ciberseguridad y vulnerabilidades comunes:**

  Detalla información sobre regulaciones y vulnerabilidades, y la revisión de la literatura científica permite realizar un análisis exhaustivo.

- **Presentación de los datos y análisis de los resultados:**

  La presentación de los datos y el análisis de los resultados tienen como objetivo ofrecer una comprensión detallada y clara de la información recopilada. Mediante el uso de tablas y gráficos, se visualizan variables clave, lo que permite identificar de manera intuitiva patrones, relaciones y tendencias significativas. Los gráficos proporcionan una representación visual de los datos, facilitando la comparación, la distribución y la evolución de las variables a lo largo del tiempo. Las tablas, por su parte, aportan precisión y detalle, permitiendo un análisis de los valores numéricos.

- **Desarrollo del modelo de pilares de seguridad:**

  Como resultado del desarrollo de los *Pilares de Seguridad Integral para Dispositivos Médicos: Un Análisis Integral*, se creó una representación simplificada y abstracta del diseño. Esto se realizó con el fin de seleccionar los elementos críticos y definir sus relaciones. Para cada elemento se establecieron diversos atributos que permitieron visualizar la estructura y las conexiones del modelo derivado del proceso de revisión, asegurando claridad y coherencia. Esta representación fue acompañada de información que facilita su comprensión y aplicación.

Los resultados se desarrollaron en función de pilares y bajo un enfoque integral para garantizar tanto claridad estructural como cobertura completa. Desde una perspectiva de ingeniería, los pilares se refieren a componentes fundamentales que sostienen la integridad y funcionalidad de un sistema, permitiendo un análisis modular y mejoras específicas. El término integral enfatiza la unificación y concentración de la información, permitiendo que el mode-

lo agregue y centralice aspectos críticos de seguridad en un marco coherente que facilite su evaluación e implementación de forma holística.

Elementos de los cuatro pilares de seguridad:

- Regulaciones
- Modelo vs. Fabricante
- Análisis de Vulnerabilidades y Amenazas
- Tendencias y Tecnologías Emergentes

BIBLIOGRAFÍA

[1] Yazid, A. Cybersecurity and Privacy Issues in the Internet of Medical Things (IoMT). Eig. Rev. Sci. Technol. 2023, 7, 1–21.

[2] Ogu, E.C. Cybersecurity for eHealth: A Simplified Guide to Practical Cybersecurity for Non-Technical Healthcare Stakeholders & Practitioners; Routledge: London, UK, 2021.

[3] Wong, J.; Tong, R.K. (Eds.) Medical Regulatory Affairs: An International Handbook for Medical Devices and Healthcare Products; CRC Press: Boca Raton, FL, USA, 2022.

[4] Wirth, A.G. Medical Device Cybersecurity for Engineers and Manufacturers; Artech House: Norwood, MA, USA, 2020.

[5] Arnab, R. Chapter Three: Regulatory overview. In Cybersecurity for Connected Medical Devices; Arnab, R., Ed.; Elsevier Inc.:Amsterdam, The Netherlands, 2022; pp. 46–64.

[6] ISO. Available online: https://www.iso.org/es/home (accessed on 24 June 2024).

[7] Hitrustalliance. HITRUST. Available online: https://hitrustalliance.net/ (accessed on 24 June 2024). Appl. Sci. 2025, 15, 6634 27 of 29.

[8] ISO/IEC 27701:2019; Security Techniques-Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management-Requirements and Guidelines. ISO: Genewa, Switzerland, 2019.

BLOCKCHAIN: DO PARADIGMA DE CONSENSO BIZANTINO À TRANSFORMAÇÃO ALGORÍTMICA DO COMÉRCIO GLOBAL E A CONVERGÊNCIA COM A INTELIGÊNCIA ARTIFICIAL

Ana Paula Afonso y Jéssica Carneiro,
Instituto Politécnico do Porto. Portugal.
{apafonso, jessicacarneiro}@iscap.ipp.pt

Feriel Selaimia y Manuel Pérez-Cota,
Universidade de Vigo. Espanha.
{feriel.selaimia, mpcota}@uvigo.gal

PALABRAS CLAVES

Blockchain; Tolerância a Falhas Bizantinas (BFT); Inteligência Artificial; Smart Contracts; Comércio Internacional; Governação Algorítmica.

RESUMEN

A tecnologia Blockchain representa uma das mudanças de paradigma mais profundas na computação distribuída desde a invenção da Internet. Originalmente concebida para resolver o Problema dos Generais Bizantinos — um dilema lógico onde os componentes de um sistema devem concordar com uma estratégia comum apesar da presença de atores maliciosos — a Blockchain evoluiu para uma infraestrutura de confiança universal. Este resumo analisa a transposição desta fundação técnica para a comércio global, onde a opacidade das cadeias de abastecimento e a fricção burocrática historicamente impediam a eficiência.

O ponto de inflexão atual reside na convergência com a Inteligência Artificial (IA). Enquanto a Blockchain garante a integridade e a imutabilidade dos dados, a IA fornece a capacidade analítica e preditiva para interpretar esses mes-

mos dados. Esta simbiose permite a transição de contratos estáticos para smart contracts dinâmicos, capazes de gerir fluxos comerciais internacionais com intervenção humana mínima. A investigação conclui que esta transformação algorítmica não é apenas técnica, mas sim uma reconfiguração da economia política global, onde o código assume o papel de garante das trocas comerciais.

OBJETIVOS

Objetivo Geral:

Investigar a trajetória evolutiva da Blockchain, partindo da sua base teórica em sistemas distribuídos até à sua aplicação prática como motor de automação e inteligência no comércio global contemporâneo.

Objetivos Específicos:

- Análise Teórica: decompor o conceito de Tolerância a Falhas Bizantinas (BFT) e como este sustenta a segurança em redes comerciais descentralizadas.
- Exploração Tecnológica: avaliar os mecanismos de integração entre Large Language Models (LLMs) e tokens de Blockchain para a gestão de contratos internacionais.
- Impacto Setorial: Identificar ganhos de eficiência na logística global, com foco na redução de custos de transação e eliminação de intermediários financeiros.
- Estudo de Governação: Analisar os desafios éticos e regulamentares da "lei algorítmica" (Lex Cryptographia) face às normas comerciais vigentes [1].

METODOLOGIAS E FERRAMENTAS

A metodologia adotada foi a Revisão Sistemática da Literatura Integrativa, combinada com a análise de tendências tecnológicas recentes (2023-2025).

- Critérios de Seleção – foram selecionados artigos científicos que abordam especificamente a dualidade "IA + Blockchain" e relatórios de instituições como a UNCTAD [2] e a Organização Mundial do Comércio [3].
- Enquadramento Teórico – Utilizamos a Teoria dos Custos de Transação de Coasse para medir o impacto da desintermediação.
- Ferramentas Analíticas – Análise de Protocolos:
  - Estudo comparativo entre algoritmos de consenso Proof-of-Stake (PoS) e;
  - Directed Acyclic Graphs (DAG).
- Modelagem de Casos – Simulação de fluxos de Smart Contracts para cartas de crédito digitais.
- Bibliometria – Uso de ferramentas como VOSviewer para mapear a densidade de publicações sobre "AI-Driven Blockchain" no período pós-2023.

RESULTADOS E DISCUSSÃO

1. Do Consenso Bizantino à Confiança Digital

O problema dos Generais Bizantinos, formulado originalmente por Lamport [4], serviu de base para o desenvolvimento do Bitcoin e, posteriormente, de redes corporativas. Em 2024, observa-se que a segurança do comércio global já não depende exclusivamente de jurisdições nacionais, mas de algoritmos de consenso que garantem que todos os intervenientes na cadeia de valor (exportadores, bancos, alfândegas) visualizam a mesma "verdade" digital [5].

2. A Convergência com a Inteligência Artificial

A convergência tecnológica atua em três frentes principais:

A. Tokens Inteligentes – A IA atua como uma ponte que valida dados do mundo real (p.ex: temperatura de um contentor detetada por sensores IoT) antes de serem inseridos na Blockchain.
B. Segurança e Auditoria – Algoritmos de IA monitorizam a rede Blockchain para detetar padrões de fraude em tempo real, algo impossível de realizar manualmente em volumes de comércio global [6].
C. Execução Autónoma – A união de LLM com código de contrato permite que a Blockchain interprete cláusulas contratuais complexas e execute pagamentos automaticamente quando as condições são verificadas [7].

3. Transformação do Comércio Global

As evidências recolhidas mostram que a digitalização via Blockchain reduz os custos operacionais em cerca de 15% a 30% no setor logístico [3]. Além disso, a «Transformação Algorítmica» permite a inclusão de pequenas e médias empresas (PME) no comércio internacional, uma vez que a confiança é garantida pelo protocolo e não por históricos de crédito extensos.

BIBLIOGRAFIA

[1] Andersen, M., & Silva, J. P. (2024). Descentralização e Inteligência. Artificial: O novo tecido da economia digital. Lisboa: Editorial Académica Portuguesa.

[2] United Nations Conference on Trade and Development (UNCTAD). 2024. Digital Economy Report 2024: Harnessing AI and Blockchain for Sustainable Development. Nova Iorque: Nações Unidas.

[3] Organização Mundial do Comércio (OMC). (2023). Relatório sobre o Comércio Mundial: Ferramentas digitais e a resiliência das cadeias de abastecimento global. Genebra: Publicações da OMC.

[4] The Byzantine Generals Problem LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE SRI International.

[5] Fernandes, R. L. (2025). Sistemas Distribuídos e o Futuro do Consenso: De Bizâncio à Web3. Porto: Imprensa Universitária da Invicta.

[6] Zhang, Y., Gupta, S., & Müller, H. (2023). Deep Learning meets Blockchain: Emerging trends in supply chain automation. Journal of Global Trade and Technology, 15(2), 112-134. https://www.google.com/search?q=https://doi.org/10.1016/jgtt.2023.05.004.

[7] Santos, T. M., & Costa, L. F. (2024). A convergência entre Blockchain e Machine Learning na gestão logística 4.0. Revista Lusófona de Tecnologia e Sociedade, 12(1), 45-67.

Agradecimientos

Los autores agradecen a CEPAL, al Instituto de Estudios Internacionales de la Universidad de Chile y al programa CYTED, por medio de la Red RIBCi, el apoyo financiero que hizo posible la realización de este Simposio en Santiago de Chile (2025) y la vinculación internacional de su equipo de investigadores.

Agradecimentos

Os autores agradecem à CEPAL, ao Instituto de Estudios Internacionales da Universidad de Chile e ao programa CYTED, por meio da Rede RIBCi, pelo apoio financeiro que possibilitou a realização deste Simpósio em Santiago do Chile (2025) e a articulação internacional de sua equipe de pesquisadores.


Naciones Unidas
United Nations

CEPAL


Red RIBCi
Red Iberoamericana de
Blockchain y Ciberseguridad


PROGRAMA
IBEROAMERICANO
CYTED
CIENCIA Y TECNOLOGÍA PARA EL DESARROLLO


UNIVERSIDAD
DE CHILE
Instituto
de Estudios
Internacionales