

Inteligencia Artificial y Blockchain: Impactos en la Mejora de la Seguridad en Plataformas Fintech

Gabriel Alejandro Ibarra¹ and Francisco Gindre^{2,3}

¹ Facultad de Tecnología Informática. Universidad Abierta Interamericana UAI,
Avenida San Juan 951 - 1er piso, CABA, Argentina

Gabriel.ibarra@alumnos.uai.edu.ar,
<https://www.uai.edu.ar>

² LIFIA, Facultad de Informática, Universidad Nacional de La Plata, calle 50 S/N
esquina 120, La Plata, Argentina,

fgindre@lifia.info.unlp.edu.ar,
<https://lifia.info.unlp.edu.ar/>

³ CONICET

Resumen La convergencia de inteligencia artificial (IA) y blockchain está revolucionando el sector Fintech al ofrecer soluciones innovadoras en seguridad, cumplimiento normativo y transparencia operativa. Esta revisión sistemática de la literatura abarca 667 estudios publicados entre 2010 y 2024, seleccionando alrededor de 175 artículos relevantes. Los resultados preliminares resaltan que estas tecnologías permitiría optimizar procesos críticos como ‘Know Your Customer’ (KYC) y la prevención de fraudes, aunque enfrentan limitaciones en escalabilidad e interoperabilidad, así como desafíos regulatorios. El objetivo de trabajo es proporcionar una perspectiva integral sobre el impacto actual y futuro de estas tecnologías en Fintech. **Keywords:** Fintech, Inteligencia

Artificial, Blockchain, Ciberseguridad Financiera, Interoperabilidad Tecnológica **Abstract.** The convergence of artificial intelligence (AI) and blockchain is revolutionizing the Fintech sector by offering innovative solutions in security, regulatory compliance, and operational transparency. This systematic literature review will analyze 667 studies published between 2010 and 2024, selecting approximately 175 relevant articles. The preliminary results indicate that these technologies could enable the optimization of critical processes such as ‘Know Your Customer’ (KYC) and fraud prevention, although they face limitations in scalability and interoperability, as well as regulatory challenges. The objective of this research is to provide a comprehensive perspective on the current and future impact of these technologies in Fintech.

Keywords: Fintech, Artificial Intelligence, Blockchain, Financial Cybersecurity, Technological Interoperability

1. Introducción

En los últimos años, el sector FinTech creció con rapidez, incorporando tecnologías como inteligencia artificial (IA) y *blockchain* para mejorar seguridad, eficiencia y transparencia en servicios financieros [6,7]. Una de las grandes ventajas de la IA ha sido su capacidad para detectar fraudes, automatizar procesos y analizar grandes volúmenes de datos en tiempo real, lo que incrementa la velocidad y precisión de las decisiones.

Por su parte, *blockchain* aporta trazabilidad, inmutabilidad e integridad a las transacciones y registros digitales, minimizando riesgos de manipulación [10]. Si bien se observan beneficios concretos, aun persisten dudas sobre su impacto real, limitaciones técnicas y desafíos regulatorios. Este trabajo en desarrollo presenta un mapeo sistemático de literatura (2010–2024), sintetizando hallazgos dispersos y abordando las siguientes preguntas de investigación: **(1)** ¿Cómo mejora la IA la seguridad frente a métodos tradicionales? **(2)** ¿Qué aporta *blockchain* en la gestión de datos y transacciones? **(3)** ¿Qué desafíos implica su integración conjunta? **(4)** ¿Cómo mejora el cumplimiento normativo y procesos KYC? **(5)** ¿Qué impacto tiene en la percepción del usuario? **(6)** ¿Qué casos de éxito existen? **(7)** ¿Qué marcos teóricos predominan?

2. Metodología

Se realizó un mapeo sistemático de literatura siguiendo un enfoque estructurado y reproducible. La búsqueda se llevó a cabo en cinco bases académicas reconocidas por su impacto (IEEE, ACM, Taylor & Francis, Wiley, Emerald), abarcando el período 2010–2024, y focalizándose en estudios relacionados con IA, *blockchain* y seguridad en el contexto FinTech. Se incluyeron únicamente artículos revisados por pares, publicados en inglés o español, mientras que se descartaron investigaciones sin enfoque financiero, como aquellas centradas en IoT u otras tecnologías aisladas. La búsqueda inicial arrojó 667 resultados. Tras eliminar duplicados y aplicar criterios de inclusión y exclusión a títulos y resúmenes, 175 trabajos fueron seleccionados para una revisión detallada. Luego de la lectura completa, se definió una muestra final de 105 artículos pertinentes. Para facilitar este proceso, se utilizó la plataforma Scopr, junto con herramientas automatizadas programadas en Python utilizando bibliotecas como Selenium y BeautifulSoup, que permitieron clasificar y etiquetar los documentos en las categorías *incluido*, *excluido* y *pendiente*. Durante la revisión, uno de los desafíos fue clasificar estudios que abordaban la inteligencia artificial de forma transversal, sin centrarse específicamente en seguridad, lo que obligó a tomar decisiones editoriales cuidadosas para mantener el enfoque del análisis.

3. Resultados Preliminares

La integración de IA y *blockchain* mejora notablemente la seguridad en FinTech, especialmente en detección de fraudes, gestión de riesgos y protección de

datos sensibles. Los algoritmos de aprendizaje profundo han demostrado superar métodos tradicionales al identificar transacciones fraudulentas en tiempo real [2]. El análisis de grafos en *blockchain* ha demostrado detectar esquemas ilícitos con mayor precisión, como el lavado de dinero [5]. También se reportan casos exitosos donde la IA reduce pérdidas y mejora la confianza en plataformas de pago [8]. La adopción de *blockchain* refuerza la integridad de los datos mediante registros inmutables, mejorando la transparencia financiera. Algunos autores proponen modelos de seguridad de “confianza cero” basados en consensos distribuidos para prevenir brechas [1]. La combinación IA-*blockchain* permite automatizar procesos regulatorios (KYC/AML) y evaluar riesgos de criptoactivos de forma predictiva [2]. Además, estas tecnologías mejoran la experiencia del usuario: chatbots inteligentes y sistemas de identidad digital segura elevan la percepción de protección. Estudios como [4] y [3] destacan que la criptografía y la detección proactiva no solo fortalecen la confianza del usuario y previenen actividades sospechosas, sino que también permiten anticiparse a posibles amenazas mediante sistemas de monitoreo en tiempo real. Esta capacidad predictiva y preventiva representa un cambio de paradigma en la gestión de la seguridad financiera.

Cuadro 1. Tendencias en la aplicación conjunta de IA y Blockchain en FinTech

Área de aplicación	Contribución de IA	Contribución de Blockchain
Prevención de fraudes	Algoritmos predictivos, detección en tiempo real	Registro inmutable de transacciones
Cumplimiento normativo (KYC/AML)	Automatización, monitoreo de comportamiento	Contratos inteligentes, trazabilidad
Protección de datos sensibles	Análisis proactivo, detección de anomalías	Criptografía, control de acceso distribuido
Confianza y experiencia del usuario	Chatbots, sistemas explicables	Identidad digital descentralizada

4. Discusión

Los resultados preliminares sugieren que la sinergia entre IA y *blockchain* tiene alto potencial para fortalecer la seguridad en FinTech. Ambas tecnologías se complementan: la IA identifica amenazas complejas mediante aprendizaje automático, mientras *blockchain* garantiza la inmutabilidad de los datos. Esta sinergia resulta particularmente útil en procesos críticos como la verificación de identidad (KYC), reduce fraudes y facilita la automatización regulatoria (*Reg-Tech*), disminuyendo costos y errores. No obstante, persisten desafíos. La **escalabilidad** afecta el rendimiento de *blockchain* con grandes volúmenes de datos, y los modelos de IA requieren alto poder de cómputo. La **interoperabilidad**

también es crítica: integrar IA y *blockchain* en sistemas financieros tradicionales exige superar barreras técnicas y de estandarización. Además, surgen tensiones entre **privacidad** y **trazabilidad**, ya que la IA necesita datos sensibles y *blockchain* los almacena de forma transparente [4,9]. Se plantean marcos legales que permitan una adopción segura [9], mientras que la confianza del usuario sigue siendo esencial: errores de seguridad o sesgos pueden comprometer su aceptación. En resumen, la integración de estas tecnologías pueden mejorar la resiliencia del sector financiero, siempre que su implementación considere estrategias que mitiguen riesgos. La colaboración entre industria, academia y reguladores será clave para escalar estas soluciones de forma segura. Por ello, se hace necesario seguir generando evidencia empírica que fundamente mejores prácticas y fortalezca la adopción responsable de estas tecnologías disruptivas en el sector financiero.

Limitaciones observadas en la literatura. A partir del proceso de selección y análisis de los artículos incluidos, se identificaron algunas debilidades recurrentes en la literatura revisada. En particular, muchos estudios presentan enfoques teóricos o simulaciones sin validación empírica en entornos financieros reales. Además, en varios casos se aborda inteligencia artificial y blockchain de forma separada, sin tratar los desafíos concretos que implica su integración técnica y operativa. También se observa una cobertura limitada de los marcos regulatorios existentes, lo cual dificulta evaluar la viabilidad de adopción en contextos normativos complejos. Por último, se destaca la escasa representación de estudios en regiones emergentes, lo que limita la generalización de los hallazgos a nivel global.

5. Trabajo futuro

Este estudio se encuentra en desarrollo, por lo que aún restan líneas por profundizar. En lo inmediato, se completará la revisión sistemática incorporando estudios recientes y afinando la clasificación según las preguntas de investigación. En una siguiente etapa, se planea realizar un análisis cuantitativo de tendencias (por ejemplo, técnicas de IA por año, subdominios FinTech tratados) y una síntesis cualitativa que permita proponer un marco conceptual del área. También se explorarán tecnologías emergentes como la computación cuántica, las pruebas de conocimiento cero y los contratos inteligentes avanzados, evaluando su aplicabilidad para superar limitaciones actuales de seguridad, escalabilidad y privacidad en entornos financieros [4]. Otro objetivo será formular recomendaciones regulatorias basadas en buenas prácticas detectadas en casos de éxito, priorizando aquellas que favorezcan la adopción responsable y sostenible de estas tecnologías. Finalmente, se contempla la posibilidad de realizar encuestas a expertos y estudios de caso en instituciones financieras reales, con el fin de validar empíricamente los hallazgos y contrastar las propuestas teóricas en escenarios concretos. Este artículo representa un trabajo en curso, cuyo análisis detallado se encuentra en desarrollo. Como siguiente paso, se prevé la publicación de los resultados definitivos de la revisión sistemática.

Referencias

1. Umair B. Chaudhry and Aysha K. M. Hydros. Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm. *IET Blockchain*, 3(2):98–115, 2023.
2. Si Chen. Cryptocurrency financial risk analysis based on deep machine learning. *Complexity*, 2022(1):2611063, 2022.
3. Muhammad Zia Habib Ullah Khan and Maliha. Identifying the ai-based solutions proposed for restricting money laundering in financial sectors: Systematic mapping. *Applied Artificial Intelligence*, 38(1):1–18, 2024.
4. Hsini Huang, Brian Pin-Hsuan Chang, Calvin Zhou-Peng Liao, and Don-Yun Chen. A matter of risk management: The effects of the innovation sandboxes on citizens' risk perceptions. In *Proceedings of the 22nd Annual International Conference on Digital Government Research*, dg.o '21, pages 281–285, New York, NY, USA, 2021. Association for Computing Machinery.
5. Jack Nicholls, Aditya Kuppa, and Nhien-An Le-Khac. Fraudlens: Graph structural learning for bitcoin illicit activity identification. In *Proceedings of the 39th Annual Computer Security Applications Conference, ACSAC '23*, page 324–336, New York, NY, USA, 2023. Association for Computing Machinery.
6. Ali Saleh, Jassim Bejani, and Daragh Tooski. Fintech cybersecurity challenges and regulations: Bahrain case study. *Journal of Computer Information Systems*, 2023.
7. Mary Jane C. Samonte and Aaron Luis Emmanuel S. Navarro. Unleashing the power of ai: Seeking the impact of artificial intelligence in the fintech industry. In *Proceedings of the 2024 6th International Conference on Management Science and Industrial Engineering, MSIE '24*, pages 196–201, New York, NY, USA, 2024. Association for Computing Machinery.
8. Mary Jane C. Samonte, Drew Antoni E. Villasor, Ken Francisco M. Sudo, and Renilda S. Layno. Analyzing artificial intelligence as business strategy in fighting fraud in the fintech industry. In *Proceedings of the 2024 10th International Conference on Computing and Artificial Intelligence, ICCAI '24*, pages 319–324, New York, NY, USA, 2024. Association for Computing Machinery.
9. Jon Truby, Rafael Brown, and Andrew Dahdal. Banking on ai: Mandating a proactive approach to ai regulation in the financial sector. *Law and Financial Markets Review*, 14(2):110–120, 2020.
10. Hanjie Wu, Qian Yao, Zhenguang Liu, Butian Huang, Yuan Zhuang, Huayun Tang, and Erwu Liu. Blockchain for finance: A survey. *IET Blockchain*, 4(2):101–123, 2024.