SADIO Electronic Journal of Informatics and Operations Research (EJS) Vol. 25 No. 1 (2026) e-ISSN 1514-6774
https://revistas.unlp.edu.ar/ejs | https://doi.org/10.24215/15146774e096

Convergence of Artificial Intelligence and Blockchain for Security Enhancement on FinTech Platforms.

Gabriel A. Ibarra[1] and Francisco Gindre[2,3]

[1] Centro de Altos Estudios en Tecnología Informática (CAETI), Facultad de Tecnología Informática, Universidad Abierta Interamericana, CABA, 1069AAB, Argentina
[2] Facultad de Informática, Universidad Nacional de La Plata, La Plata, 1900, Argentina
[3] Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), La Plata, 1900, Argentina

Abstract. The convergence of artificial intelligence (AI) and blockchain technology has become a central pillar of financial security within the FinTech ecosystem. This work is grounded in a systematic analysis of the literature that examines the contribution of both technologies to critical areas such as fraud detection, protection of sensitive data, regulatory compliance (KYC/AML), traceability, and risk management. The results indicate that the integration of AI and blockchain strengthens the resilience of financial platforms and streamlines regulatory processes, although challenges remain regarding scalability, interoperability, algorithmic bias, and incomplete regulatory frameworks. This study synthesizes the current state of the field, the main limitations, and the opportunities these technologies offer to enhance security in FinTech.

Keywords: fintech, artificial intelligence, blockchain, financial cybersecurity, regTech, fraud prevention, traceability

Convergencia de Inteligencia Artificial y Blockchain para el Fortalecimiento de la Seguridad en Plataformas FinTech

Abstract. La convergencia entre inteligencia artificial (IA) y tecnología blockchain se ha consolidado como un eje central de la seguridad financiera en el ecosistema FinTech. Este trabajo se basa en un análisis sistemático de la literatura que examina el aporte de ambas tecnologías en áreas críticas como la detección de fraudes, la protección de datos sensibles, el cumplimiento regulatorio (KYC/AML), la trazabilidad y la

Received August 2025; Accepted November 2025; Published February 2026

gestión de riesgos. Los resultados muestran que la integración de IA y blockchain fortalece la resiliencia de las plataformas financieras y optimiza procesos regulatorios, aunque persisten desafíos de escalabilidad, interoperabilidad, sesgos algorítmicos y marcos regulatorios incompletos. El trabajo sintetiza el estado actual, las principales limitaciones y las oportunidades de estas tecnologías para mejorar la seguridad en FinTech.

Keywords: fintech, inteligencia artificial, blockchain, ciberseguridad financiera, regtech, prevención de fraudes, trazabilidad

1 Introducción

El sector FinTech ha experimentado una transformación acelerada en la última década, impulsada por la adopción de tecnologías emergentes como la inteligencia artificial (IA) y la cadena de bloques (blockchain). La literatura muestra que la digitalización financiera, la innovación en productos y el uso de analítica avanzada han modificado la gestión de la seguridad, la verificación de identidades, la trazabilidad de datos y el cumplimiento normativo (Li & Xu, 2022; Nofie, 2020; Qi & Xiao, 2018). Diversos estudios coinciden en que la convergencia de IA y blockchain constituye un avance clave para reforzar la resiliencia de las plataformas financieras digitales, en un contexto de incremento del fraude, mayor sofisticación de los ciberataques y complejidad regulatoria creciente (Faccia et al., 2020; Nicholls et al., 2023; Samonte & Navarro, 2024; Samonte et al., 2024).

La IA ha demostrado capacidades destacadas para identificar patrones anómalos en grandes volúmenes de datos, anticipar riesgos y automatizar decisiones bajo condiciones cambiantes. Los modelos de aprendizaje automático superan las limitaciones de los sistemas basados en reglas fijas al adaptarse a amenazas en evolución (Samonte & Navarro, 2024). En mercados descentralizados, la IA también ha sido efectiva para identificar actividades ilícitas mediante análisis de grafos transaccionales (Nicholls et al., 2023). Estas capacidades se complementan con enfoques explicables y sistemas de alerta temprana que contribuyen a la evaluación continua de riesgos (Wei & Floreti, 2022; Wen, 2024), reduciendo pérdidas operativas y fortaleciendo la confianza de usuarios y entidades reguladoras (Zakaria et al., 2023).

Blockchain aporta propiedades esenciales para la integridad y seguridad de la información financiera. Su estructura descentralizada e inmutable dificulta la manipulación de datos y facilita auditorías transparentes, lo cual es fundamental en sectores donde la trazabilidad es crítica (Garanina et al., 2021; Wu et al., 2024). La inmutabilidad de los registros, junto con mecanismos criptográficos avanzados, favorece la consistencia de las transacciones y amplía la capacidad de supervisión en entornos con múltiples actores (Zhang et al., 2019). Asimismo,

los contratos inteligentes permiten automatizar procesos como la verificación de identidad, la evaluación de riesgos y la ejecución de políticas regulatorias (Liu et al., 2021; R. & Ravi, 2021).

La literatura también identifica desafíos significativos. La escalabilidad limita la aplicación de blockchain en escenarios que requieren alto rendimiento, y la interoperabilidad entre sistemas tradicionales y redes distribuidas continúa siendo un problema técnico relevante (Ahmadjee et al., 2022; Lohachab et al., 2021). La opacidad de algunos modelos de IA, los sesgos algorítmicos y la ausencia de marcos regulatorios homogéneos dificultan una adopción masiva (McCarthy, 2023; Paterson, 2021). La tensión entre privacidad y trazabilidad, especialmente en procesos KYC/AML, evidencia la necesidad de arquitecturas híbridas que equilibren eficiencia, transparencia y protección de datos (Gunasinghe et al., 2019; Liang et al., 2024; Nokhbeh Zaeem et al., 2022; Soltani et al., 2021).

En este contexto, la integración IA–blockchain representa una oportunidad estratégica para fortalecer la seguridad financiera. La IA aporta análisis predictivo, monitoreo inteligente y respuesta automatizada, mientras que blockchain garantiza integridad, auditabilidad y confiabilidad de los datos. La literatura del mapeo sistemático muestra beneficios concretos: la detección de fraudes mejora significativamente (Alarab et al., 2020; Faccia et al., 2020), el monitoreo de riesgos se vuelve más robusto cuando se aplican modelos inteligentes sobre infraestructuras distribuidas (Habib Ullah Khan & Maliha, 2024), y procesos como la verificación de identidad y la automatización del cumplimiento normativo se optimizan mediante arquitecturas híbridas basadas en IA y blockchain (Chen, 2022; Ren et al., 2023). En conjunto, esta complementariedad permite diseñar infraestructuras más resilientes frente a amenazas emergentes (Becker et al., 2020; Lagerwaard, 2023).

El presente artículo se basa en un análisis sistemático de la literatura (Ibarra & Gindre, 2025) con el propósito de ofrecer una visión integral del impacto combinado de la inteligencia artificial y la tecnología blockchain en la seguridad de plataformas FinTech. El trabajo examina beneficios, limitaciones técnicas, desafíos operativos y aspectos regulatorios asociados con su implementación. Asimismo, organiza los hallazgos en función de las preguntas de investigación, compara enfoques, identifica brechas persistentes y presenta una síntesis crítica orientada a investigadores, profesionales del sector y entidades reguladoras.

No obstante, es importante reconocer ciertas limitaciones en la literatura analizada. La evidencia disponible presenta una notable heterogeneidad metodológica: numerosos estudios de inteligencia artificial aplicados a la detección de anomalías se sustentan en simulaciones o en conjuntos de datos restringidos, lo que dificulta extrapolar sus resultados a entornos operativos reales (Chen, 2022; Samonte & Navarro, 2024). Por su parte, buena parte de las contribuciones sobre blockchain se concentra en modelos teóricos o arquitecturas conceptuales con escasa validación empírica, lo que limita evaluar su aplicabilidad en plataformas FinTech sujetas a requisitos regulatorios estrictos (Garanina et al., 2021; Wu et al., 2024). Además, solo una fracción acotada de trabajos aborda de manera integrada la convergencia IA–blockchain, lo que deja vacíos en torno

a los desafíos prácticos asociados con su implementación conjunta, tales como interoperabilidad, gobernanza y sincronización de datos (Ahmadjee et al., 2022; Lohachab et al., 2021). Estas limitaciones no reducen la relevancia del análisis, pero sí señalan la necesidad de investigaciones aplicadas que evalúen soluciones híbridas en entornos FinTech reales y regulados.

Este artículo aporta una articulación comparativa entre IA y blockchain que permite comprender, desde una perspectiva unificada, sus complementariedades, limitaciones y desafíos para la seguridad en entornos FinTech.

2 Marco Teórico

La integración de inteligencia artificial y tecnología blockchain en el sector financiero se apoya en marcos conceptuales que convergen en objetivos orientados a la integridad de los datos, la seguridad computacional y la confiabilidad operativa. Estos fundamentos permiten analizar su papel en la arquitectura de plataformas FinTech modernas y su potencial para fortalecer procesos de supervisión, auditoría y gestión de riesgos.

2.1 IA en Finanzas: bases técnicas y rol en seguridad

La inteligencia artificial aplicada a las finanzas se basa en modelos diseñados para procesar grandes volúmenes de datos, identificar patrones y asistir en la toma de decisiones bajo incertidumbre. Sus enfoques fundamentales incluyen el aprendizaje supervisado, no supervisado y profundo, que optimizan funciones de pérdida para clasificar eventos, detectar anomalías o anticipar comportamientos futuros (Samonte & Navarro, 2024).

Los modelos de aprendizaje profundo, estructurados en arquitecturas neuronales de múltiples capas, permiten extraer representaciones jerárquicas de datos transaccionales complejos, habilitando análisis más precisos en escenarios dinámicos y de alta frecuencia (Chen, 2022). La teoría de grafos ha adquirido relevancia en la representación de relaciones entre entidades financieras, al permitir analizar redes transaccionales y detectar vínculos atípicos asociados a posibles esquemas ilícitos (Nicholls et al., 2023).

La IA incorpora además principios de explicabilidad y transparencia algorítmica, esenciales en entornos regulados donde las decisiones automatizadas deben poder auditarse. Estas aproximaciones buscan reducir riesgos derivados de comportamientos opacos o difíciles de justificar (Wei & Floreti, 2022). Estudios bibliométricos confirman que la IA se ha consolidado como un componente transversal en la gestión de riesgos, el análisis predictivo y la automatización de servicios financieros (Samonte et al., 2024; Zakaria et al., 2023).

2.2 Blockchain: arquitectura de confianza y registro seguro

Blockchain constituye un modelo de registro distribuido sustentado en criptografía, consenso descentralizado e inmutabilidad estructural. Su diseño encadena bloques mediante funciones hash, de modo que cualquier alteración del

contenido sea detectable y el historial permanezca íntegro (Wu et al., 2024). La transparencia y verificabilidad de este esquema facilitan auditorías continuas y permiten supervisar procesos sensibles con múltiples actores (Garanina et al., 2021; Zhang et al., 2019).

Los contratos inteligentes representan un pilar central de este modelo. Definidos como programas autoejecutables almacenados en la cadena de bloques, permiten automatizar reglas de negocio, reducir intervención humana y estandarizar operaciones bajo condiciones verificables (R. & Ravi, 2021). En contextos financieros, este mecanismo resulta relevante para procesos de verificación de identidades, cumplimiento normativo y gestión de activos (Liu et al., 2021).

Blockchain involucra decisiones arquitectónicas sobre topología de red, niveles de permisos, mecanismos de consenso y gobernanza distribuida. Estas decisiones determinan sus capacidades de escalabilidad, su interoperabilidad con infraestructuras financieras tradicionales y su resiliencia frente a amenazas externas (Ahmadjee et al., 2022; Lohachab et al., 2021). El análisis de estos elementos permite explicar por qué blockchain opera como infraestructura base para aplicaciones de auditoría, trazabilidad y seguridad en sistemas financieros contemporáneos.

2.3 Convergencia IA–Blockchain y motivación del estudio

IA y blockchain pueden articularse bajo un marco de complementariedad tecnológica. Diversos estudios sostienen que la IA depende de datos íntegros y resistentes a manipulaciones para generar predicciones robustas, mientras que blockchain proporciona integridad, auditabilidad y persistencia verificable en los registros que alimentan los modelos (Faccia et al., 2020; Wu et al., 2024). Esta interdependencia fundamenta su estudio conjunto en escenarios financieros que requieren tanto inteligencia adaptativa como garantías criptográficas de seguridad, habilitando arquitecturas híbridas que refuerzan la supervisión y la mitigación de riesgos (Becker et al., 2020; Truby et al., 2020).

En este marco, blockchain actúa como proveedor de datos confiables, mientras que la IA agrega mecanismos de análisis predictivo, clasificación y detección temprana. El uso de contratos inteligentes abre la posibilidad de automatizar reglas derivadas de modelos analíticos y ejecutar políticas de verificación de forma continua y auditable (Truby et al., 2020). Estos fundamentos permiten sentar las bases teóricas para arquitecturas orientadas a mejorar la detección de fraudes, fortalecer la integridad de los datos y optimizar la gobernanza digital en el ecosistema financiero.

Aunque la literatura ofrece numerosos aportes sobre IA y blockchain de forma independiente, son menos frecuentes los estudios que integran ambas perspectivas en un marco coherente y orientado específicamente a la seguridad financiera. Esta brecha motiva el presente trabajo, que se fundamenta en un análisis sistemático de la literatura para examinar cómo la convergencia entre ambas tecnologías puede fortalecer la protección de datos, la detección de fraudes y el cumplimiento regulatorio en plataformas FinTech.

3 Estado del Arte

La literatura reciente evidencia un crecimiento sostenido en la adopción de inteligencia artificial y tecnología blockchain dentro del sector financiero. Los estudios recopilados en el mapeo sistemático muestran una transición desde aplicaciones exploratorias hacia implementaciones funcionales en plataformas FinTech, pero persisten desafíos en escalabilidad, interoperabilidad, privacidad y gobernanza que condicionan su adopción a gran escala (Li & Xu, 2022; Qi & Xiao, 2018).

La investigación actual puede agruparse en tres líneas principales: (1) aplicaciones de IA para análisis de riesgos y detección de actividades ilícitas; (2) uso de blockchain para garantizar integridad, trazabilidad y automatización confiable; y (3) arquitecturas híbridas que integran ambas tecnologías para reforzar la seguridad y el cumplimiento regulatorio.

En la primera línea, los modelos de aprendizaje automático y profundo han demostrado eficacia para identificar patrones anómalos en flujos transaccionales, superando las limitaciones de los sistemas basados en reglas estáticas (Chen, 2022; Samonte & Navarro, 2024). En contextos descentralizados, el análisis de grafos permite detectar actividades ilícitas en redes de criptomonedas mediante modelos estructurales capaces de identificar conexiones encubiertas (Nicholls et al., 2023). Estas propuestas se complementan con técnicas supervisadas aplicadas a AML y KYC, que permiten segmentar clientes, detectar anomalías y automatizar verificaciones (Alarab et al., 2020; Habib Ullah Khan & Maliha, 2024; Zakaria et al., 2023).

En la segunda línea, blockchain se utiliza como infraestructura para reforzar la integridad y transparencia de los procesos financieros. Estudios recientes describen sus mecanismos criptográficos y arquitecturas distribuidas (Wu et al., 2024), mientras que otros trabajos muestran cómo la descentralización fortalece la resistencia a manipulaciones (Zhang et al., 2019). Los contratos inteligentes permiten automatizar procesos críticos, tales como verificación de identidad, ejecución de reglas regulatorias y gestión de activos (Liu et al., 2021; R. & Ravi, 2021). A pesar de estos avances, se mantienen desafíos en rendimiento, latencia, interoperabilidad y gobernanza, especialmente al integrar registros distribuidos con infraestructuras bancarias tradicionales (Ahmadjee et al., 2022; Lohachab et al., 2021).

La tercera línea explora modelos híbridos que combinan análisis inteligente con registros inmutables. Los estudios evidencian que los modelos predictivos que operan sobre datos almacenados en blockchain mejoran la confiabilidad del análisis, y que los registros distribuidos facilitan auditorías sobre decisiones generadas por modelos de IA (Chen, 2022; Faccia et al., 2020). En el ámbito antifraude, se proponen infraestructuras distribuidas combinadas con técnicas inteligentes para reforzar la seguridad transaccional (Ren et al., 2023). Desde una perspectiva regulatoria, se destaca que los contratos inteligentes pueden automatizar funciones de cumplimiento y activar mecanismos de supervisión continua (Becker et al., 2020; Lagerwaard, 2023; Truby et al., 2020). Propuestas orientadas a AML confirman la utilidad de combinar aprendizaje supervisado con monitoreo *on-chain*

para detectar actividades ilícitas en criptomonedas y activos digitales (Alarab et al., 2020; van Wegberg et al., 2018).

En conjunto, esta literatura muestra que la convergencia IA–blockchain constituye una evolución hacia sistemas de seguridad financiera más robustos, aunque aún requiere avances en interoperabilidad, privacidad, explicabilidad y gobernanza para consolidarse en producción.

4 Metodología

La metodología aplicada se basa en un mapeo sistemático de la literatura (MSL) orientado a identificar, clasificar y sintetizar la evidencia existente sobre la integración de inteligencia artificial y blockchain en la seguridad de plataformas FinTech. Este enfoque permite obtener una visión amplia del campo, diferenciar líneas de investigación consolidadas y emergentes, y detectar brechas relevantes.

El proceso metodológico se diseñó de acuerdo con principios clásicos de revisiones sistemáticas: (1) definición explícita de preguntas de investigación; (2) construcción de una cadena de búsqueda; (3) selección de bases de datos reconocidas; (4) aplicación de criterios de inclusión y exclusión; (5) filtrado por títulos, resúmenes y texto completo; y (6) extracción y síntesis de la evidencia.

4.1 Bases de datos y cadena de búsqueda

La búsqueda bibliográfica se realizó en cinco repositorios académicos de referencia internacional: IEEE Xplore, ACM Digital Library, Taylor & Francis, Wiley Online Library y Emerald Insight. La selección de estas fuentes garantiza la cobertura de estudios revisados por pares, publicados en conferencias y journals tecnológicos relevantes para el ámbito FinTech.

La cadena de búsqueda se construyó a partir de combinaciones booleanas de términos relacionados con inteligencia artificial, blockchain, seguridad financiera, fraude, trazabilidad, RegTech (soluciones tecnológicas que se usan para automatizar y agilizar las operaciones de cumplimiento en las organizaciones) y FinTech (por ejemplo, *"artificial intelligence"*, *"machine learning"*, *"blockchain"*, *"financial security"*, *"fraud detection"*, *"FinTech"*, *"KYC/AML"*). El proceso inicial arrojó 667 resultados entre 2010 y 2024.

4.2 Criterios de inclusión y exclusión

Tras la obtención de resultados preliminares, se aplicaron criterios de inclusión y exclusión para garantizar la relevancia del corpus. Entre los criterios de inclusión se consideraron:

- Estudios publicados entre 2010 y 2024.
- Artículos revisados por pares, en inglés o español.
- Investigaciones que abordaran explícitamente IA, blockchain o la combinación de ambas en el contexto FinTech.

– Trabajos centrados en seguridad financiera, fraude, gestión de riesgos, identidad digital, cumplimiento normativo o protección de datos.

Como criterios de exclusión se descartaron:

– Estudios no relacionados con el dominio financiero.
– Trabajos que mencionaran IA o blockchain de forma tangencial sin vinculación con seguridad.
– Documentos incompletos, duplicados o sin revisión por pares.
– Publicaciones centradas exclusivamente en criptomonedas sin análisis de seguridad ni aplicaciones FinTech.

La aplicación de estos criterios redujo la muestra a 175 artículos para la etapa de revisión detallada.

4.3 Clasificación asistida y muestra final

Para mejorar la eficiencia del proceso de selección se empleó la plataforma Scolr, que permitió gestionar los artículos, registrar decisiones editoriales y etiquetar cada entrada como *incluido*, *excluido* o *pendiente*. Además, se desarrollaron herramientas en Python utilizando Selenium y *web scraping* para automatizar tareas como la captura de metadatos, la verificación de duplicados y el almacenamiento estructurado de la información relevante.

Luego del filtrado por títulos y resúmenes, se realizó una revisión a texto completo de los estudios que cumplían los criterios de inclusión. A partir de este proceso se obtuvo un conjunto consolidado de trabajos con aportes sustantivos en al menos uno de los siguientes ejes: (1) aplicación de IA para la detección de amenazas y gestión de riesgos; (2) uso de blockchain para garantizar integridad, trazabilidad o automatización de procesos; (3) análisis de la sinergia IA–blockchain en contextos FinTech; o (4) investigaciones orientadas al cumplimiento regulatorio, auditoría o percepción del usuario en entornos financieros digitales.

4.4 Preguntas de investigación y categorías de análisis

Los artículos seleccionados se organizaron en categorías temáticas derivadas de patrones observados en la literatura. Estas categorías incluyen: (1) prevención de fraudes; (2) protección de datos sensibles; (3) identidad digital y KYC/AML; (4) trazabilidad y auditoría; (5) RegTech y cumplimiento normativo; y (6) modelos híbridos IA–blockchain.

En paralelo, se formularon siete preguntas de investigación (PI1–PI7) orientadas a analizar cómo IA y blockchain contribuyen a la seguridad financiera, quiénes se benefician, qué desafíos persisten y qué vacíos se observan en la literatura. Para cada artículo se extrajeron datos como objetivos, tecnologías utilizadas, marcos analíticos, resultados, limitaciones y contribuciones, sintetizados en la sección de resultados.

5 Resultados por preguntas de investigación

El análisis sistemático de la literatura permitió examinar cómo los estudios abordan las siete preguntas de investigación propuestas. Esta sección sintetiza los hallazgos más relevantes, articulando contribuciones, tendencias y limitaciones observadas en el conjunto de trabajos seleccionados.

5.1 PI1: ¿Cómo mejora la IA la seguridad frente a métodos tradicionales?

La literatura muestra que la inteligencia artificial supera a los sistemas de seguridad basados en reglas fijas en términos de precisión, adaptabilidad y capacidad de respuesta. Diversos estudios evidencian que los modelos de aprendizaje automático permiten detectar patrones emergentes de fraude difíciles de identificar mediante enfoques convencionales, especialmente en escenarios donde las tácticas de ataque evolucionan rápidamente (Samonte & Navarro, 2024). Los modelos de aprendizaje profundo reducen tasas de falsos positivos y mejoran la identificación de comportamientos anómalos mediante análisis contextuales más ricos (Chen, 2022).

El uso de análisis de grafos complementa estas capacidades, particularmente en escenarios donde los atacantes buscan ocultar conexiones entre cuentas o establecer redes ilícitas complejas. La caracterización estructural de relaciones transaccionales permite identificar patrones encubiertos en redes de criptomonedas, fortaleciendo el monitoreo financiero (Nicholls et al., 2023). Estos avances se articulan con estudios que aplican aprendizaje supervisado a AML y KYC, reforzando la capacidad de la IA para adaptarse a patrones cada vez más sofisticados (Alarab et al., 2020; Habib Ullah Khan & Maliha, 2024).

En conjunto, la evidencia indica que la IA incrementa la eficacia de los mecanismos de detección y habilita respuestas más ágiles, monitoreo continuo y capacidades predictivas que los sistemas tradicionales no igualan.

5.2 PI2: ¿Qué aporta blockchain en la gestión de datos y transacciones?

La literatura identifica que blockchain aporta inmutabilidad, descentralización y trazabilidad verificable en la gestión de datos y transacciones financieras. Los registros distribuidos reducen la posibilidad de manipulación, fortalecen la integridad de la información y permiten auditorías más confiables, aspectos esenciales en entornos donde la confiabilidad del dato es crítica (Wu et al., 2024; Zhang et al., 2019). Los contratos inteligentes automatizan procesos como la validación de transacciones, la ejecución de políticas regulatorias y el seguimiento de activos, reduciendo errores humanos y mejorando la consistencia operativa (Liu et al., 2021; R. & Ravi, 2021).

Estudios en contabilidad y finanzas corporativas muestran que la adopción de registros distribuidos redefine prácticas de control y reporte, ofreciendo fuentes

de información más transparentes y verificables (Garanina et al., 2021). En síntesis, blockchain proporciona un soporte estructural para garantizar integridad y verificabilidad de la información, particularmente en ecosistemas con múltiples actores o procesos que requieren auditorías recurrentes.

5.3 PI3: ¿Qué desafíos implica la integración conjunta de IA y blockchain?

La integración entre inteligencia artificial y tecnología blockchain presenta oportunidades importantes, pero también desafíos técnicos y operativos. Uno de los principales obstáculos es la escalabilidad: los tiempos de procesamiento característicos de blockchain pueden limitar aplicaciones que requieren análisis en tiempo real. A ello se suma la complejidad de arquitecturas híbridas en las que modelos de IA intensivos en cómputo deben coexistir con infraestructuras distribuidas sujetas a restricciones de latencia y capacidad (Ahmadjee et al., 2022; Lohachab et al., 2021).

Otro desafío central es la interoperabilidad. Muchos sistemas financieros dependen de infraestructuras heredadas que no se integran fácilmente con redes distribuidas, lo que dificulta la adopción de soluciones híbridas. La transparencia de los registros distribuidos puede entrar en tensión con la necesidad de proteger datos sensibles utilizados por modelos de IA, especialmente en aplicaciones vinculadas con procesos KYC/AML e identidad digital (Liang et al., 2024; Nokhbeh Zaeem et al., 2022; Soltani et al., 2021).

En el plano operativo, las soluciones híbridas requieren capacidades computacionales elevadas, modelos de gobernanza claros y estrategias explícitas para mitigar sesgos algorítmicos. La literatura enfatiza que, sin marcos normativos robustos y mecanismos adecuados de auditoría, la integración IA–blockchain podría reproducir o amplificar riesgos existentes en el sistema financiero (Saleh et al., 2023; Truby et al., 2020).

5.4 PI4: ¿Cómo mejora la integración el cumplimiento normativo y procesos KYC/AML?

La integración de inteligencia artificial y tecnología blockchain aporta mejoras al cumplimiento regulatorio y a los procesos KYC/AML. La IA permite detectar comportamientos sospechosos, clasificar perfiles de riesgo y automatizar la verificación de identidad a partir del análisis de documentos y patrones transaccionales, reduciendo errores y acelerando procedimientos tradicionalmente manuales (Habib Ullah Khan & Maliha, 2024; Samonte & Navarro, 2024). Revisiones bibliométricas y mapeos sistemáticos evidencian una incorporación progresiva de estas capacidades en el sector financiero (Qudah et al., 2024; Zakaria et al., 2023).

Blockchain ofrece una base inmutable y trazable para el registro de información utilizada en procesos regulatorios. Los contratos inteligentes permiten automatizar la ejecución de reglas, garantizando transparencia, consistencia y auditabilidad en la aplicación de políticas (R. & Ravi, 2021). Propuestas basadas en identidad auto-soberana refuerzan estas capacidades al permitir la gestión de

credenciales reutilizables, verificables y controladas por el usuario (Liang et al., 2024; Soltani et al., 2021).

Estudios recientes sostienen que esta integración habilita modelos RegTech donde el cumplimiento puede operar como un mecanismo continuo y programable en lugar de un proceso exclusivamente reactivo (Truby et al., 2020). Investigaciones orientadas a vigilancia financiera, regulación de fintechs y diseño de unidades de inteligencia financiera destacan que estas capacidades son relevantes para la prevención del lavado de dinero y otros delitos financieros (Becker et al., 2020; Lagerwaard, 2023).

5.5 PI5: ¿Qué impacto tiene la integración en la percepción del usuario?

La percepción del usuario es crítica para la adopción de tecnologías financieras emergentes. La IA puede mejorar la experiencia mediante sistemas explicables, asistentes inteligentes y mecanismos adaptativos que facilitan la interacción con servicios digitales, incrementando la confianza cuando las decisiones automatizadas se perciben comprensibles (Huang et al., 2021).

Blockchain contribuye mediante transparencia, trazabilidad y verificabilidad, características que refuerzan la sensación de seguridad al interactuar con plataformas financieras digitales. Sin embargo, su complejidad técnica puede generar incertidumbre si no se acompaña de interfaces claras y mecanismos de explicación accesibles para usuarios no especializados (Nofie, 2020). En el caso de las monedas digitales de banco central y otros activos tokenizados, las percepciones sobre privacidad, vigilancia y control estatal influyen directamente en la aceptación pública (Kaur, 2024; Wong et al., 2024).

Los estudios revisados muestran que la percepción del usuario mejora cuando ambas tecnologías se implementan de forma complementaria y la experiencia de uso oculta la complejidad técnica subyacente, preservando a la vez transparencia, control sobre los datos y protección de la privacidad.

5.6 PI6: ¿Qué casos de éxito existen en la literatura?

Aunque muchos trabajos se encuentran en etapas experimentales, varios estudios reportan implementaciones exitosas o prototipos validados en contextos financieros reales. Algunos muestran resultados directos en la reducción de riesgos y mejora de la eficiencia operativa. Se documentan escenarios donde la IA permitió disminuir pérdidas operativas mediante la detección temprana de transacciones fraudulentas en plataformas de pago (Samonte & Navarro, 2024). Complementariamente, se demuestra la eficacia del análisis de grafos para identificar esquemas de lavado de dinero en entornos reales de criptomonedas (Nicholls et al., 2023), mientras que comparativas de métodos supervisados para AML evidencian mejoras respecto a enfoques tradicionales (Alarab et al., 2020).

En relación con blockchain, se presentan casos donde la trazabilidad distribuida fortalece procesos de auditoría y reduce disputas en transacciones financieras (Wu et al., 2024). Estudios en contabilidad y finanzas corporativas

sugieren que la adopción progresiva de registros distribuidos está redefiniendo prácticas de control y verificación (Garanina et al., 2021; Liu et al., 2021).

Estos casos evidencian el potencial de ambas tecnologías, aunque la literatura coincide en que aún es necesaria una validación más amplia en entornos productivos bancarios y FinTech, especialmente en arquitecturas híbridas IA–blockchain.

5.7 PI7: ¿Qué marcos teóricos predominan en los estudios revisados?

Los marcos teóricos predominantes pueden agruparse en tres líneas:

- **Modelos basados en aprendizaje automático y profundo**, aplicados a tareas de clasificación, detección de anomalías y análisis predictivo en entornos financieros (Chen, 2022; Samonte & Navarro, 2024; Zakaria et al., 2023).
- **Modelos de trazabilidad e integridad**, sustentados en estructuras distribuidas y mecanismos criptográficos propios de blockchain, orientados a garantizar inmutabilidad y verificabilidad de transacciones (Wu et al., 2024; Zhang et al., 2019).
- **Enfoques regulatorios y de gobernanza digital**, centrados en la aplicación de tecnologías emergentes en procesos de supervisión, cumplimiento normativo y gestión de identidades (Becker et al., 2020; Saleh et al., 2023; Truby et al., 2020).

La literatura evidencia una tendencia creciente hacia modelos híbridos en los que la IA opera sobre datos verificados mediante blockchain, mientras que los contratos inteligentes ejecutan reglas derivadas de análisis automatizados. Estudios sobre identidad auto-soberana, privacidad en redes distribuidas y técnicas criptográficas avanzadas amplían la base conceptual para el diseño de arquitecturas de seguridad más robustas (Liang et al., 2024; Oude Roelink et al., 2024; Soltani et al., 2021).

6 Discusión

Los resultados obtenidos permiten identificar tensiones, complementariedades y limitaciones que caracterizan el uso de inteligencia artificial y blockchain en la seguridad de plataformas FinTech. A continuación se sintetizan las principales observaciones críticas organizadas en torno a desafíos técnicos, regulatorios, operativos y socio–organizacionales.

En términos prácticos, los resultados permiten orientar a instituciones financieras y reguladores respecto de cómo la convergencia IA–blockchain puede fortalecer mecanismos de detección de fraudes, trazabilidad y cumplimiento regulatorio. La síntesis presentada ofrece criterios técnicos y operativos para evaluar soluciones híbridas en contextos reales, considerando restricciones de escalabilidad, gobernanza y viabilidad normativa.

6.1 Complementariedad y límites

Los estudios revisados coinciden en una marcada complementariedad entre inteligencia artificial y blockchain. La IA aporta capacidades de predicción, monitoreo y respuesta automatizada, mientras que blockchain asegura integridad, trazabilidad y resistencia frente a manipulaciones (Chen, 2022; Wu et al., 2024). Esta articulación tecnológica resulta especialmente valiosa en procesos como KYC/AML, auditorías y detección de fraudes (Habib Ullah Khan & Maliha, 2024; Samonte & Navarro, 2024).

Sin embargo, la integración presenta límites prácticos. Problemas de escalabilidad en redes blockchain pueden restringir el uso de arquitecturas híbridas en escenarios que requieren análisis y respuesta de baja latencia (Lohachab et al., 2021). La complejidad computacional de modelos avanzados de IA también dificulta su incorporación directa en infraestructuras distribuidas con recursos limitados (Ahmadjee et al., 2022). Estos desafíos subrayan la importancia de soluciones que equilibren robustez técnica, rendimiento y costos operativos.

6.2 Desafíos regulatorios y de gobernanza

La regulación constituye uno de los desafíos más complejos identificados. Si bien blockchain ofrece trazabilidad y verificabilidad, estas propiedades pueden entrar en conflicto con requisitos de privacidad y confidencialidad. Diversos estudios señalan que esta tensión limita la adopción de redes públicas en aplicaciones que manejan información sensible (Nokhbeh Zaeem et al., 2022). Investigaciones sobre CBDC (Central Bank Digital Currency (Moneda Digital de Banco Central)) y activos tokenizados muestran que el diseño de mecanismos de control y supervisión impacta en la aceptación social y la confianza del usuario (Kaur, 2024; Wong et al., 2024).

La incorporación de IA en procesos de cumplimiento normativo exige marcos capaces de integrar decisiones automatizadas sin comprometer transparencia ni responsabilidad institucional. Esta necesidad se vuelve crítica cuando se emplean modelos opacos para evaluar riesgos o detectar actividades sospechosas (Truby et al., 2020). Los estudios sobre RegTech subrayan que la coordinación entre autoridades supervisoras, entidades financieras y desarrolladores tecnológicos es esencial para evitar la externalización indebida de responsabilidades (Becker et al., 2020; Saleh et al., 2023).

6.3 Limitaciones metodológicas y experiencia de usuario

El análisis revela que gran parte de los estudios se apoya en simulaciones o evaluaciones experimentales en entornos controlados. Solo una fracción limitada documenta implementaciones en escenarios reales, lo que restringe la generalización de resultados (Nicholls et al., 2023; Samonte & Navarro, 2024). Esta brecha entre resultados experimentales y validación práctica es una limitación recurrente.

Asimismo, son pocos los trabajos que analizan en profundidad cómo estas tecnologías impactan la experiencia y percepción del usuario en plataformas FinTech. Dado que la aceptación del usuario final es determinante para la adopción efectiva de soluciones digitales, este vacío constituye una agenda pendiente relevante (Huang et al., 2021; Nofie, 2020).

6.4 Hacia una visión integrada de IA y blockchain

La revisión muestra la necesidad de un marco conceptual que articule los aportes combinados de IA y blockchain en seguridad financiera. Aunque existen propuestas parciales, no se identifican modelos integradores capaces de abordar simultáneamente calidad y verificabilidad de datos, auditoría de decisiones automatizadas, aplicación de contratos inteligentes para cumplimiento regulatorio, mitigación de sesgos y desafíos operativos y regulatorios (Garanina et al., 2021; Lagerwaard, 2023; Truby et al., 2020; Zhang et al., 2019). Aun así, la literatura converge en que la sinergia IA–blockchain representa un camino prometedor para la construcción de plataformas FinTech más seguras, resilientes y auditables (Faccia et al., 2020; Ren et al., 2023).

7 Trabajo Futuro

El análisis de los estudios revisados permitió identificar áreas donde la investigación actual permanece fragmentada o insuficientemente validada. A partir de los vacíos detectados se proponen varias líneas de trabajo futuro.

En primer lugar, se requiere avanzar hacia **evaluaciones en entornos reales de producción**. La mayoría de los trabajos que aplican modelos de IA para detección de anomalías o gestión de riesgos se desarrollan en contextos controlados o con conjuntos de datos históricos limitados (Alarab et al., 2020; Chen, 2022; Samonte & Navarro, 2024). La validación en instituciones financieras, proveedores de pago o plataformas de activos digitales permitiría examinar el desempeño de estas soluciones bajo condiciones reales de volumen, latencia y variabilidad operacional (Deng et al., 2024; Zakaria et al., 2023).

En segundo lugar, se identifica como prioritaria la construcción de **arquitecturas híbridas IA–blockchain plenamente integradas**. Aunque existen avances parciales, la literatura evidencia la ausencia de marcos que articulen de forma coherente gobernanza distribuida, calidad del dato, auditoría automatizada, actualización de modelos y contratos inteligentes sujetos a regulación (Ahmadjee et al., 2022; Lohachab et al., 2021; Truby et al., 2020). El desarrollo de prototipos funcionales con flujos verificables, inferencia en tiempo real y trazabilidad *end-to-end* constituye una dirección crítica.

Otra área necesaria es la creación de **mecanismos de privacidad compatibles con blockchain**. La tensión entre trazabilidad y protección de datos sensibles continúa siendo uno de los principales obstáculos para adoptar redes distribuidas en sectores regulados (Nokhbeh Zaeem et al., 2022). Se requieren

investigaciones orientadas a técnicas criptográficas avanzadas, modelos de compartición segura, particiones *off-chain* y estrategias de anonimización que preserven integridad sin exponer información utilizada por modelos de IA (Liang et al., 2024; Oude Roelink et al., 2024; Soltani et al., 2021).

Asimismo, se observa la necesidad de **estándares de explicabilidad y auditoría automatizada**. Aunque los modelos explicables mejoran la confianza del usuario (Huang et al., 2021), aún no existen mecanismos formales que traduzcan decisiones algorítmicas en reglas verificables registradas en blockchain. El diseño de contratos inteligentes que integren explicabilidad, evidencia criptográfica y auditoría programática representa una oportunidad relevante (Becker et al., 2020; Truby et al., 2020).

Finalmente, se requieren **análisis comparativos de marcos regulatorios** y su efecto sobre la viabilidad de arquitecturas IA–blockchain. La literatura destaca que los avances en RegTech dependen de políticas claras sobre automatización, responsabilidad y supervisión algorítmica (Lagerwaard, 2023; Saleh et al., 2023; Truby et al., 2020). Explorar cómo distintos regímenes condicionan el diseño técnico contribuirá a orientar soluciones compatibles con requisitos legales y operativos.

8 Conclusiones

El análisis realizado evidencia que la convergencia entre inteligencia artificial y tecnología blockchain constituye un eje estratégico para fortalecer la seguridad en plataformas FinTech. La revisión sistemática de la literatura permitió identificar avances significativos, así como vacíos y desafíos persistentes que condicionan su adopción efectiva en entornos financieros reales.

La evidencia revisada muestra que la **IA aporta mejoras sustanciales** en detección de anomalías, identificación de patrones de fraude y evaluación predictiva de riesgos. Los modelos de aprendizaje automático y profundo destacan por su capacidad para adaptarse a escenarios dinámicos y reducir falsos positivos (Chen, 2022; Samonte & Navarro, 2024). Otros trabajos enfatizan el rol de la explicabilidad y los sistemas de alerta temprana como mecanismos que incrementan la transparencia y la confianza operativa (Wei & Floreti, 2022; Wen, 2024).

Por su parte, **blockchain se consolida como infraestructura de integridad**, aportando inmutabilidad, trazabilidad y verificación distribuida. Estas propiedades resultan valiosas en auditorías continuas y en entornos con múltiples actores (Wu et al., 2024). Investigaciones previas también destacan que la descentralización mejora la resistencia a manipulaciones e inconsistencias regulatorias (Zhang et al., 2019). Adicionalmente, los contratos inteligentes reducen errores operativos y permiten automatizar reglas de cumplimiento (Liu et al., 2021; R. & Ravi, 2021).

Si bien la convergencia IA–blockchain presenta un **potencial significativo**, su adopción plena continúa limitada por problemas de escalabilidad, tensiones entre privacidad y trazabilidad, falta de interoperabilidad y ausencia de están-

dares para arquitecturas híbridas (Lohachab et al., 2021). Estas restricciones explican por qué numerosos estudios permanecen en fases experimentales y aún no se observan despliegues generalizados en producción (Ahmadjee et al., 2022; Nokhbeh Zaeem et al., 2022).

En el ámbito regulatorio, los trabajos revisados indican que ambas tecnologías pueden **transformar procesos de supervisión y cumplimiento**, habilitando auditorías más frecuentes, verificables y programables (Truby et al., 2020). No obstante, su implementación requiere marcos claros de gobernanza y transparencia algorítmica, así como políticas robustas de protección de datos (Becker et al., 2020; Saleh et al., 2023). Estudios sobre privacidad, CBDC y activos tokenizados subrayan que los mecanismos de control inciden directamente en la percepción y aceptación del usuario (Kaur, 2024; Wong et al., 2024).

El análisis revela **brechas persistentes**: escasa validación en entornos reales, limitada consideración de la experiencia del usuario y ausencia de modelos híbridos robustos que integren calidad del dato, explicabilidad y gobernanza distribuida (Deng et al., 2024). Resolver estas brechas constituye una dirección clave para la investigación futura.

En conjunto, los resultados permiten concluir que la convergencia entre IA y blockchain representa un eje estratégico para el fortalecimiento de la seguridad financiera. Aunque persisten desafíos técnicos y normativos, la evidencia disponible sugiere que los enfoques híbridos ofrecen un camino consistente hacia plataformas FinTech más seguras, auditables y confiables.

Como agenda futura, se requieren estudios empíricos que validen prototipos híbridos en entornos operativos, así como análisis comparativos que profundicen en interoperabilidad, gobernanza y efectos regulatorios de soluciones conjuntas basadas en IA y blockchain.

Disclosure of Interests. Los autores declaran que no presentan conflictos de interés.

References

Ahmadjee, S., Mera-Gómez, C., Bahsoon, R., & Kazman, R. (2022). A study on blockchain architecture design decisions and their security attacks and threats. *ACM Trans. Softw. Eng. Methodol.*, *31*(2), 36e. https://doi.org/10.1145/3502740

Alarab, I., Prakoonwit, S., & Nacer, M. I. (2020). Comparative analysis using supervised learning methods for anti-money laundering in bitcoin. *Proceedings of the 2020 5th International Conference on Machine Learning Technologies*, 11–17. https://doi.org/10.1145/3409073.3409078

Becker, M., Merz, K., & Buchkremer, R. (2020). Regtech—the application of modern information technology in regulatory affairs: Areas of interest in research and practice [ISAFM-19-052.R1]. *Intelligent Systems in Accounting, Finance and Management*, *27*(4), 161–167. https://doi.org/10.1002/isaf.1479

Chen, S. (2022). Cryptocurrency financial risk analysis based on deep machine learning. *Complexity*, *2022*(1), 2611063. https://doi.org/10.1155/2022/2611063

Deng, R., Jiang, J., Ou, C., Chen, Z., & Li, H. (2024). Current status and prospects of risk management research in the era of big data intelligence. *Proceedings of the 2023 3rd International Conference on Big Data, Artificial Intelligence and Risk Management*, 859–864. https://doi.org/10.1145/3656766.3656908

Faccia, A., Moşteanu, N. R., Cavaliere, L. P. L., & Mataruna-Dos-Santos, L. J. (2020). Electronic money laundering, the dark side of fintech: An overview of the most recent cases. *Proceedings of the 2020 12th International Conference on Information Management and Engineering*, 29–34. https://doi.org/10.1145/3430279.3430284

Garanina, T., Ranta, M., & Dumay, J. (2021). Blockchain in accounting research: Current trends and emerging topics [Ahead of print]. *Accounting, Auditing & Accountability Journal*. https://doi.org/10.1108/AAAJ-10-2020-4991

Gunasinghe, H., Kundu, A., Bertino, E., Krawczyk, H., Chari, S., Singh, K., & Su, D. (2019). Prividex: Privacy preserving and secure exchange of digital identity assets. *The World Wide Web Conference*, 594–604. https://doi.org/10.1145/3308558.3313574

Habib Ullah Khan, M. Z., & Maliha. (2024). Identifying the ai-based solutions proposed for restricting money laundering in financial sectors: Systematic mapping. *Applied Artificial Intelligence*, *38*(1), 1–18. https://doi.org/10.1080/08839514.2024.2344415

Huang, H., Pin-Hsuan Chang, B., Zhou-Peng Liao, C., & Chen, D.-Y. (2021). A matter of risk management: The effects of the innovation sandboxes on citizens' risk perceptions. *Proceedings of the 22nd Annual International Conference on Digital Government Research*, 281–285. https://doi.org/10.1145/3463677.3463738

Ibarra, G. A., & Gindre, F. (2025). Inteligencia artificial y blockchain: Impactos en la mejora de la seguridad en plataformas fintech. *JAIIO, Jornadas Argentinas de Informática*, *11*(7), 62–66. https://revistas.unlp.edu.ar/JAIIO/article/view/20072

Kaur, G. (2024). Privacy implications of central bank digital currencies (cbdcs): A systematic review of literature. *EDPACS*, *69*(9), 87–123. https://doi.org/10.1080/07366981.2024.2376794

Lagerwaard, P. (2023). Financial surveillance and the role of the financial intelligence unit (fiu) in the netherlands. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-09-2022-0134

Li, B., & Xu, Z. (2022). A comprehensive bibliometric analysis of financial innovation. *Economic Research-Ekonomska Istraživanja*, *35*(1), 367–390. https://doi.org/10.1080/1331677X.2021.1893203

Liang, W., Liu, Y., Yang, C., Xie, S., Li, K., & Susilo, W. (2024). On identity, transaction, and smart contract privacy on permissioned and permis-

sionless blockchain: A comprehensive survey. *ACM Computing Surveys (ACM Comput. Surv.)*, *56*(12). https://doi.org/10.1145/3676164

Liu, J., Xu, Z., Li, R., Zhao, H., Jiang, H., Yao, J., Yuan, D., & Chen, S. (2021). Applying blockchain for primary financial market: A survey. *IET Blockchain*, *1*(2–4), 65–81. https://doi.org/10.1049/blc2.12009

Lohachab, A., Garg, S., Kang, B., Amin, M. B., Lee, J., Chen, S., & Xu, X. (2021). Towards interconnected blockchains: A comprehensive review of the role of interoperability among disparate blockchains. *ACM Computing Surveys (ACM Comput. Surv.)*, *54*(7). https://doi.org/10.1145/3460287

McCarthy, J. (2023). The regulation of regtech and suptech in finance: Ensuring consistency in principle and in practice. *Journal of Financial Regulation and Compliance*. https://doi.org/10.1108/JFRC-01-2022-0004

Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2023). Fraudlens: Graph structural learning for bitcoin illicit activity identification. *Proceedings of the 39th Annual Computer Security Applications Conference*, 324–336. https://doi.org/10.1145/3627106.3627200

Nofie, I. (2020). The rise and rise of financial technology: The good, the bad, and the verdict. *Cogent Business & Management*, *7*(1), 1725309. https://doi.org/10.1080/23311975.2020.1725309

Nokhbeh Zaeem, R., Chang, K. C., Huang, T.-C., Liau, D., Song, W., Tyagi, A., Khalil, M., Lamison, M., Pandey, S., & Barber, K. S. (2022). Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study. *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, 128–135. https://doi.org/10.1145/3486622.3493917

Oude Roelink, B., El-Hajj, M., & Sarmah, D. (2024). Systematic review: Comparing zk-snark, zk-stark, and bulletproof protocols for privacy-preserving authentication. *Security and Privacy*, *7*(5), e401. https://doi.org/10.1002/spy2.401

Paterson, J. M. (2021). Making robo-advisers careful? duties of care in providing automated financial advice to consumers. *Law and Financial Markets Review*, *15*(3-4), 278–295. https://doi.org/10.1080/17521440.2023.2196027

Qi, Y., & Xiao, J. (2018). Fintech: Ai powers financial services to improve people's lives. *Communications of the ACM*, *61*(11), 65–69. https://doi.org/10.1145/3239550

Qudah, H., Baqila, B. K. A., Albadienah, J. M. O., AlQudah, M. Z., Al Qudah, S., Alrahamneh, S., Ababneh, A., & Qudah, I. (2024). Using bibliometrics to understand algorithmic finance. *Journal of Applied Economics*, *27*(1), 2389497. https://doi.org/10.1080/15140326.2024.2389497

R., V., & Ravi, H. (2021). Innovation in banking: Fusion of artificial intelligence and blockchain. *Asia Pacific Journal of Innovation and Entrepreneurship*. https://doi.org/10.1108/APJIE-09-2020-0142

Ren, Y., Ren, Y., Tian, H., Song, W., & Yang, Y. (2023). Improving transaction safety via anti-fraud protection based on blockchain. *Connection Science*, *35*(1), 2163983. https://doi.org/10.1080/09540091.2022.2163983

Saleh, A., Bejani, J., & Tooski, D. (2023). Fintech cybersecurity challenges and regulations: Bahrain case study. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2023.2251455

Samonte, M. J. C., & Navarro, A. L. E. S. (2024). Unleashing the power of ai: Seeking the impact of artificial intelligence in the fintech industry. *Proceedings of the 2024 6th International Conference on Management Science and Industrial Engineering*, 196–201. https://doi.org/10.1145/3664968.3664993

Samonte, M. J. C., Villasor, D. A. E., Sudo, K. F. M., & Layno, R. S. (2024). Analyzing artificial intelligence as business strategy in fighting fraud in the fintech industry. *Proceedings of the 2024 10th International Conference on Computing and Artificial Intelligence*, 319–324. https://doi.org/10.1145/3669754.3669803

Soltani, R., Nguyen, U. T., & An, A. (2021). A survey of self-sovereign identity ecosystem. *Security and Communication Networks*, *2021*(1), 8873429. https://doi.org/10.1155/2021/8873429

Truby, J., Brown, R., & Dahdal, A. (2020). Banking on ai: Mandating a proactive approach to ai regulation in the financial sector. *Law and Financial Markets Review*, *14*(2), 110–120. https://doi.org/10.1080/17521440.2020.1760454

van Wegberg, R., Oerlemans, J.-J., & van Deventer, O. (2018). Bitcoin money laundering: Mixed results? *Journal of Financial Crime*, *25*(2), 419–435. https://doi.org/10.1108/JFC-11-2016-0067

Wei, L., & Floreti, P. G. (2022). A data-driven explainable case-based reasoning approach for financial risk detection. *Quantitative Finance*. https://doi.org/10.1080/14697688.2022.2118071

Wen, Y. (2024). Research on risk early warning system of financial sharing platform based on neural network model. *Proceedings of the 2024 Guangdong-Hong Kong-Macao Greater Bay Area International Conference on Digital Economy and Artificial Intelligence*, 943–947. https://doi.org/10.1145/3675417.3675573

Wong, M. C. S., Chan, E. K. H., & Yousaf, I. (2024). Cbdcs, regulated stablecoins, and tokenized traditional assets under the basel committee rules on cryptoassets. *Journal of Financial Regulation and Compliance*, *ahead-of-print*(ahead-of-print), ahead-of–print. https://doi.org/10.1108/JFRC-03-2024-0050

Wu, H., Yao, Q., Liu, Z., Huang, B., Zhuang, Y., Tang, H., & Liu, E. (2024). Blockchain for finance: A survey. *IET Blockchain*, *4*(2), 101–123. https://doi.org/10.1049/blc2.12067

Zakaria, N., Sulaiman, A., Min, F. S., & Feizollah, A. (2023). Machine learning in the financial industry: A bibliometric approach to evidencing applica-

tions. *Cogent Social Sciences*, *9*(2), 2276609. https://doi.org/10.1080/23311886.2023.2276609

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys*, *52*(3), 51:1–51:34. https://doi.org/10.1145/3316481