Análisis de superficies de ataque en blockchain y estrategias de mitigación para el fortalecimiento de la seguridad y resiliencia en entornos digitales

Carlos Marino Santacruz Aguirre

Asesora

Yenny Stella Núñez Álvarez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Agradecimientos

A la Gobernación del Valle del Cauca, quien a través del Departamento Administrativo de Desarrollo Institucional y la Secretaría de las TIC, me ha facilitado los tiempos y espacios necesarios para complementar mis estudios profesionales.

A la Universidad Nacional Abierta y a Distancia (UNAD), por darme la oportunidad de volver en calidad de egresado para continuar con mi proceso de profesionalización.

A mi estimada directora Yenny Stella Núñez Álvarez, por darme la oportunidad de trabajar con ella en la temática elegida para mi opción de grado.

A los demás directores y tutores de los diferentes cursos, por orientarme asertiva y oportunamente en las diferentes actividades desarrolladas a lo largo de mi proceso formativo.

Dedicatoria

A Dios, mi señor, mi todo, quien me ha guiado, inspirado y me ha dado la fuerza necesaria para llegar a la meta.

A la Iglesia Bautista Reformada Siervos de la Palabra, nuestro Pastor y hermanos en la fe, por acogerme y permitirme crecer en conocimiento y verdad, a la luz de las Sagradas Escrituras.

A mi querida Gilma, mi compañera fiel, mi confidente, mi ayuda idónea, quien me ha apoyado incondicionalmente en cada momento vivido.

A mi familia, por todo su gran amor y acompañamiento motivacional que me ha permitido avanzar en medio de las dificultades.

También a mis compañeros de trabajo, por refutar mis opiniones y permitirme ver nuevas formas de resolver las diferentes problemáticas de la vida.

Y, finalmente, a los quienes no confiaron en mí, porque gracias a ellos aprendí a dejar a un lado lo que no edifica, obteniendo la fuerza necesaria para avanzar.

Resumen

La tecnología blockchain ha sido promovida como una solución segura y transparente para la gestión de datos y transacciones digitales. No obstante, diversas vulnerabilidades documentadas han sido aprovechadas por ciberatacantes, afectando la integridad de sistemas basados en esta tecnología. Esta monografía presenta un estudio investigativo-documental sobre las superficies de ataque en blockchain, mediante el análisis de literatura científica arbitrada, informes técnicos y casos de seguridad reportados. A lo largo del estudio, se examinan de forma teórica herramientas como las auditorías de código, los análisis forenses sobre cadenas de bloques y las pruebas de penetración aplicadas a contratos inteligentes, con el fin de comprender su utilidad como mecanismos de evaluación. Con base en estos hallazgos, se formulan recomendaciones y buenas prácticas orientadas al fortalecimiento de la seguridad y resiliencia de las implementaciones Blockchain en entornos digitales.

Palabras clave: Blockchain, Ciberseguridad, Vulnerabilidad.

Abstract

Blockchain technology has been promoted as a secure and transparent solution for managing digital data and transactions. However, various documented vulnerabilities have been exploited by cyber attackers, compromising the integrity of systems based on this technology. This monograph presents an investigative-documentary study on attack surfaces in Blockchain through the analysis of peer-reviewed scientific literature, technical reports, and documented security cases. Throughout the study, theoretical examinations are conducted on tools such as code audits, forensic analysis of Blockchain records, and penetration testing applied to smart contracts, in order to understand their relevance as evaluation mechanisms. Based on these findings, this research proposes technical recommendations and best practices aimed at strengthening the security and resilience of Blockchain implementations in digital environments.

Keywords: Blockchain, Cybersecurity, Vulnerability.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Glosario

Blockchain. Sistema de almacenamiento de datos basado en una red descentralizada de bloques enlazados, diseñado para garantizar la seguridad y transparencia transaccional digital.

Ciberseguridad. Prácticas y tecnologías encargadas de proteger sistemas de información contra ataques digitales.

Contrato inteligente. Programa de autoejecución en una cadena de bloques que automatiza acuerdos entre partes sin necesidad de intermediarios.

Criptografía. Técnica de codificación de información utilizada para garantizar la seguridad de la información en ambientes digitales.

DeFi (Finanzas Descentralizadas). Ecosistema de aplicaciones financieras basadas en Blockchain que operan sin la intervención de instituciones tradicionales.

Interoperabilidad. Capacidad de diferentes redes de Blockchain para comunicarse y transferir información o activos entre sí de manera segura.

Nodo. Computadora conectada a una red Blockchain que almacena y valida transacciones y bloques.

Superficie de ataque. Conjunto de puntos vulnerables en un sistema Blockchain que pueden ser explotados por actores malintencionados.

Token. Representación digital de un activo o derecho en una Blockchain, que puede tener distintos usos como medio de pago, acceso a servicios o gobernanza.

Vulnerabilidad. Debilidad de un sistema, expuesto a explotación por ciberdelincuentes.

Introducción

La tecnología Blockchain ha crecido exponencialmente en los últimos años, prometiendo transformar diversos sectores mediante mecanismos de descentralización, transparencia y seguridad criptográfica, sin embargo, sus múltiples debilidades han puesto en riesgo la integridad de los sistemas y la confianza de los usuarios (Saad et al., 2020). Los ataques recientes a las plataformas de cadena de bloques aprovechan las vulnerabilidades de los contratos inteligentes y los protocolos de red, lo que genera problemas como el doble gasto, la congestión de las transacciones y la posible manipulación de las operaciones de la cadena de bloques (Nzuva, 2024).

Los datos recientes sobre las fallas de interoperabilidad entre cadenas de bloques destacan importantes vulnerabilidades en los puentes de comunicación y los contratos inteligentes. Los puentes entre cadenas, esenciales para la transferencia de activos entre diferentes cadenas de bloques, han sido cada vez más atacados por los atacantes, lo que ha ocasionado importantes pérdidas financieras, cómo en el caso del hackeo del puente Ronin de Axie Infinity, el cual provocó una pérdida de casi 600 millones de dólares, lo que supuso una de las mayores infracciones de seguridad de 2023 (Belenkov et al., 2025). Por otro lado, los puentes entre cadenas se enfrentan a protocolos complejos que aumentan la vulnerabilidad a los ataques, incluidos los problemas relacionados con las fallas en los contratos inteligentes y las manipulaciones de los oráculos, a su vez que el marco SmartAxe ha identificado 88 vulnerabilidades entre cadenas (CCV) derivadas de ataques reales, que afectan a activos por un valor aproximado de 1,88 millones de dólares (Liao et al., 2024).

El análisis de estos incidentes revela un patrón de explotación que subraya la necesidad urgente de mejorar las medidas de seguridad y evidencian la necesidad crítica de abordar las

amenazas a la seguridad en los sistemas Blockchain, lo que demanda la generación de acciones efectivas para mitigar estos riesgos, con la propuesta de buenas prácticas que fortalezcan la seguridad y resiliencia de estas tecnologías.

Lo anterior dio origen a esta investigación, estructurada en tres capítulos que contienen la identificación de las principales vulnerabilidades en los sistemas Blockchain, el análisis de las amenazas cibernéticas más relevantes que pueden afectar esta tecnología, los riesgos asociados y las estrategias de mitigación para garantizar su implementación de forma confiable y efectiva.

Al finalizar se dan a conocer una serie de conclusiones y referencias bibliográficas usadas para brindar un argumento sólido sobre los diferentes puntos desplegados a lo largo de la presente investigación.

Planteamiento del Problema

A pesar de su diseño descentralizado y seguro, Blockchain enfrenta varios retos de ciberseguridad, lo que compromete su confiabilidad y adopción en sectores críticos. Diversas investigaciones han identificado vulnerabilidades significativas en distintos niveles, desde ataques a la capa de red hasta errores en contratos inteligentes y riesgos en la interoperabilidad entre cadenas (Noor & Mustafa, 2024b). Esto ha facilitado incidentes como el robo de activos digitales, la manipulación de transacciones y la interrupción de servicios clave en plataformas basadas en Blockchain (Rosa et al., 2023).

El problema se centra en que las vulnerabilidades de Blockchain siguen evolucionando y siendo explotadas por ciberdelincuentes y como ejemplo de ello, en el 2022 los ataques a protocolos DeFi basados en Blockchain generaron pérdidas superiores a los 3,000 millones de dólares, lo que representó un incremento del 56% en comparación con el año anterior (He et al., 2025). En particular, los contratos inteligentes, empleados en diversas aplicaciones Blockchain, han sido un vector recurrente de ataques debido a fallos en su programación, lo que ha resultado en pérdidas significativas para distintos proyectos (Pu & Qiao, 2025). Además, los puentes intercadena han demostrado ser puntos de alto riesgo, permitiendo la sustracción de grandes sumas de activos digitales cuando son vulnerados (Kouki et al., 2025). Estos problemas no solo afectan la seguridad de quienes dependen de Blockchain, sino que también limitan su expansión y aceptación en sectores donde la confianza es importante (finanzas, logística, gestión de datos sensibles, entre otros).

A medida que los mecanismos de protección evolucionan, también lo hacen las técnicas de ataque. En las redes basadas en Proof of Stake, basadas en validadores que se seleccionan en función de la cantidad de criptomonedas que poseen y que crean un sistema plutocrático en el

que la concentración de la riqueza conduciendo a un control oligopolístico (Sus, 2022), se han identificado estrategias de manipulación de nodos validadores que, mediante la acumulación de participación o la colusión entre actores, logran influir indebidamente en la producción de bloques.

Por otro lado, la explotación de fallos en los mecanismos de consenso, como inconsistencias en la validación o bifurcaciones intencionadas, permite a los atacantes generar condiciones de doble gasto o interrupción de servicio. Las implicaciones económicas de este tipo de ataques pueden ser graves y afectar no solo al grupo objetivo, sino también a la confiabilidad de la red en general (Bhudia et al., 2022).

Asimismo, la ingeniería inversa aplicada a contratos inteligentes se ha convertido en una práctica común para identificar errores lógicos antes de su explotación directa, utilizando herramientas automáticas para extraer y analizar el código desplegado en Blockchain pública. Se han propuesto técnicas como el análisis de gráficos de control del flujo para detectar vulnerabilidades, pero muchos métodos existentes aún presentan altas tasas de falsos positivos (Ali, 2022).

También es importante mencionar que más del 60% de las empresas que han adoptado Blockchain en su infraestructura reportan preocupaciones relacionadas con la seguridad y la escalabilidad de la tecnología (Lotfi et al., 2025; Fernández López, 2021). Por ello, es imprescindible analizar en profundidad las superficies de ataque en Blockchain, identificando sus vulnerabilidades más críticas y diseñando estrategias de mitigación que favorezcan su resistencia y protección en entornos digitales.

Justificación

El estudio de las superficies de ataque en Blockchain es necesario para asegurar su implementación protegida y eficiente en múltiples industrias. El crecimiento y diversificación de esta tecnología han incrementado la complejidad de los desafíos de seguridad. La falta de estrategias de mitigación adecuadas no solo expone a los sistemas a ataques cibernéticos, sino que también genera desconfianza en su uso (Díaz, 2019).

Esta investigación busca aportar un análisis detallado de las amenazas que afectan a los sistemas Blockchain, proporcionando información clave para fortalecer su seguridad. Al centrarse en la identificación de vulnerabilidades críticas y en la implementación de estrategias de mitigación, el estudio contribuirá a mejorar la resistencia de Blockchain frente a ataques emergentes (Llamas Covarrubias, 2021).

Se estima que más del 40% de las vulnerabilidades detectadas en sistemas Blockchain pueden mitigarse con auditorías de código más rigurosas y la implementación de mecanismos de detección temprana (He et al., 2025). Esta investigación será útil tanto para desarrolladores y expertos en ciberseguridad como para organizaciones y tomadores de decisiones que buscan implementar Blockchain de manera segura. La documentación de mejores prácticas ayudará a consolidar infraestructuras más sólidas, minimizando riesgos y aumentando la confianza en la tecnología.

La solidez de este trabajo se refleja en la alineación con marcos normativos ampliamente aceptados que orientan la seguridad en sistemas distribuidos, entre los que resalta la guía NIST SP 800-183, la cual plantea principios de diseño para arquitecturas confiables, abordando componentes clave como nodos, mecanismos de consenso y canales de comunicación en redes descentralizadas. Por su parte, la norma ISO/IEC 27001 ha sido adoptada en implementaciones

Blockchain para establecer políticas de gestión de riesgos, protección de activos digitales y continuidad operativa. A ello se suman las directrices desarrolladas por la Cloud Security Alliance (CSA), centradas en el aseguramiento de contratos inteligentes, la gobernanza técnica de plataformas descentralizadas y la administración de identidades digitales. La consideración de estos estándares no solo aporta validez técnica, sino que también garantiza su aplicabilidad en entornos organizacionales que exigen altos niveles de cumplimiento y seguridad.

Asimismo, este estudio no solo abordará las amenazas existentes, sino que también propondrá soluciones novedosas que pueden ser adaptadas a diversos sectores, como las finanzas, la administración pública y la gestión de la cadena de suministro (Mejía et al., 2023). Se prevé que este estudio aporte al diseño de sistemas Blockchain más confiables y resilientes, facilitando su integración en entornos digitales con altos estándares de seguridad.

Objetivos

Objetivo General

Analizar las superficies de ataque en sistemas basados en Blockchain mediante la identificación de vulnerabilidades y amenazas cibernéticas, desarrollando estrategias de mitigación efectivas que mejoren la seguridad y resiliencia de estas tecnologías en entornos digitales.

Objetivos Específicos

Identificar las superficies de ataque que afectan los sistemas basados en Blockchain, mediante el análisis de vulnerabilidades específicas relacionadas con contratos inteligentes y redes descentralizadas, proporcionando un entendimiento claro de los puntos críticos de seguridad, clasificándolas por su frecuencia, impacto y nivel de exposición.

Elegir las amenazas cibernéticas más relevantes que afectan a los sistemas Blockchain, utilizando datos sobre los ataques más frecuentes empleados por adversarios, con la revisión del impacto potencial en la seguridad de estos sistemas, considerando su frecuencia, impacto y complejidad técnica en los entornos descentralizados.

Definir los riesgos asociados con las superficies de ataque en sistemas Blockchain, mediante la identificación, clasificación y priorización de vulnerabilidades, estableciendo su probabilidad de ocurrencia e impacto, que permita a las organizaciones una gestión eficiente de la seguridad digital.

Desarrollar estrategias para la mitigación de riesgos en tecnologías Blockchain, mediante la implementación de controles técnicos y organizativos, evaluados en función de su aplicabilidad, eficacia y alineación con estándares reconocidos, que fortalezcan su seguridad y resiliencia, garantizando una implementación confiable y efectiva en diversos entornos digitales.

Marco Referencial

Antecedentes

El desarrollo de Blockchain ha transformado el uso de la información y las transacciones digitales en diversos sectores, incluyendo las finanzas, la logística, la salud y la administración pública. Esta tecnología descentralizada ha demostrado ser una solución viable para garantizar la seguridad, la inmutabilidad y la trazabilidad de los datos (He et al., 2025).

La acogida y demanda de Blockchain en los últimos años ha sido exponencial. Según *Annals of Operations Research*, la inversión global en esta tecnología ha superado los 10.000 millones de dólares, con una proyección de alcanzar los 39.700 millones para el año 2025 (Lotfi et al., 2025). Su implementación en la industria financiera ha permitido optimizar procesos de pago, reducir costos operativos y minimizar el fraude bancario (Pandey & Kushwaha, 2025). Adicionalmente, en la cadena de suministro, Blockchain ha facilitado la trazabilidad de productos y la verificación de su autenticidad, reduciendo en un 30% las irregularidades en documentación (Lotfi et al., 2025).

A pesar de estos avances, la implementación de Blockchain también ha revelado riesgos críticos. Entre ellos, se destacan los ataques del 51%, en los que un actor malintencionado controla la mayoría de la red para manipular transacciones (Saad et al., 2020). También se han registrado ataques Sybil, en los que los atacantes crean múltiples identidades falsas para influir en la red (Zalte et al., 2023). Según *Concurrency and Computation: Practice and Experience*, los ciberataques en Blockchain generaron pérdidas superiores a los 3.800 millones de dólares en 2023, evidenciando la necesidad de fortalecer los mecanismos de protección (Noor & Mustafa, 2024a).

***Casos Recientes de Ataques y Fallos en Redes Blockchain*.**

Hackeo a Binance Smart Chain (BSC) – Octubre 2022. Binance Smart Chain sufrió un ataque debido a una vulnerabilidad en su puente de cadena cruzada, lo que resultó en el robo de aproximadamente 2 millones de BNB, valorados en $570 millones. Los atacantes explotaron una falla en el contrato inteligente del puente, permitiéndoles acuñar nuevos BNB sin respaldo. Este incidente subrayó la importancia de realizar auditorías exhaustivas en los contratos inteligentes y reforzar la seguridad en los puentes de cadena cruzada.

Compromiso de Carteras en Solana – Agosto 2022. Más de 8,000 carteras de usuarios en la red Solana fueron comprometidas, resultando en el robo de aproximadamente $5 millones en criptomonedas. El ataque se atribuyó a una vulnerabilidad en las carteras móviles, donde los atacantes lograron acceder a las claves privadas de los usuarios. Este evento destacó la importancia de la seguridad en las aplicaciones de cartera y la necesidad de que los usuarios mantengan prácticas seguras en la gestión de sus claves privadas.

Ataque a Curve Finance – Julio 2023. Curve Finance, una plataforma de intercambio descentralizado en Ethereum, fue atacada debido a una vulnerabilidad en la versión 0.2.15 del compilador Vyper utilizada en algunos de sus contratos inteligentes. Este fallo permitió a los atacantes drenar fondos de varios pools de stablecoins, resultando en pérdidas de alrededor de $73.5 millones. Posteriormente, parte de los fondos fueron recuperados, pero el incidente resaltó la necesidad de utilizar herramientas de desarrollo seguras y mantener actualizados los entornos de ejecución.

Ataque a Mixin Network – Septiembre 2023. Mixin Network, un proveedor de transacciones peer-to-peer, sufrió un ataque en el que se comprometió la base de datos de su proveedor de servicios en la nube, resultando en la pérdida de aproximadamente $200 millones.

El incidente llevó a la suspensión de todos los servicios de retiro y depósito, subrayando la necesidad de asegurar las infraestructuras de terceros y evaluar continuamente la seguridad de los proveedores externos.

Ataque a CoinEx – Septiembre 2023. CoinEx fue hackeado debido a la filtración de la clave privada de su cartera caliente, lo que resultó en una pérdida de $70 millones. Investigaciones posteriores sugirieron la posible implicación del Grupo Lazarus, destacando la necesidad de implementar medidas robustas de gestión de claves y monitoreo continuo de actividades sospechosas.

Lecciones Aprendidas.

Auditorías de Seguridad Rigurosas. Es esencial realizar auditorías exhaustivas y periódicas de los contratos inteligentes y las infraestructuras asociadas para identificar y mitigar vulnerabilidades potenciales.

Gestión Segura de Claves Privadas. Implementar prácticas sólidas para la generación, almacenamiento y uso de claves privadas es crucial para prevenir accesos no autorizados y posibles robos de fondos.

Actualización y Mantenimiento Constante. Mantener actualizados los entornos de desarrollo y las herramientas utilizadas, así como monitorear continuamente las dependencias externas, ayuda a protegerse contra vulnerabilidades conocidas y emergentes.

Evaluación de Proveedores Externos. Es fundamental evaluar y supervisar la seguridad de los proveedores de servicios externos, especialmente aquellos que manejan datos sensibles o infraestructuras críticas.

Incorporar estas lecciones en el diseño y operación de sistemas Blockchain puede fortalecer la resiliencia y confianza en estas tecnologías emergentes.

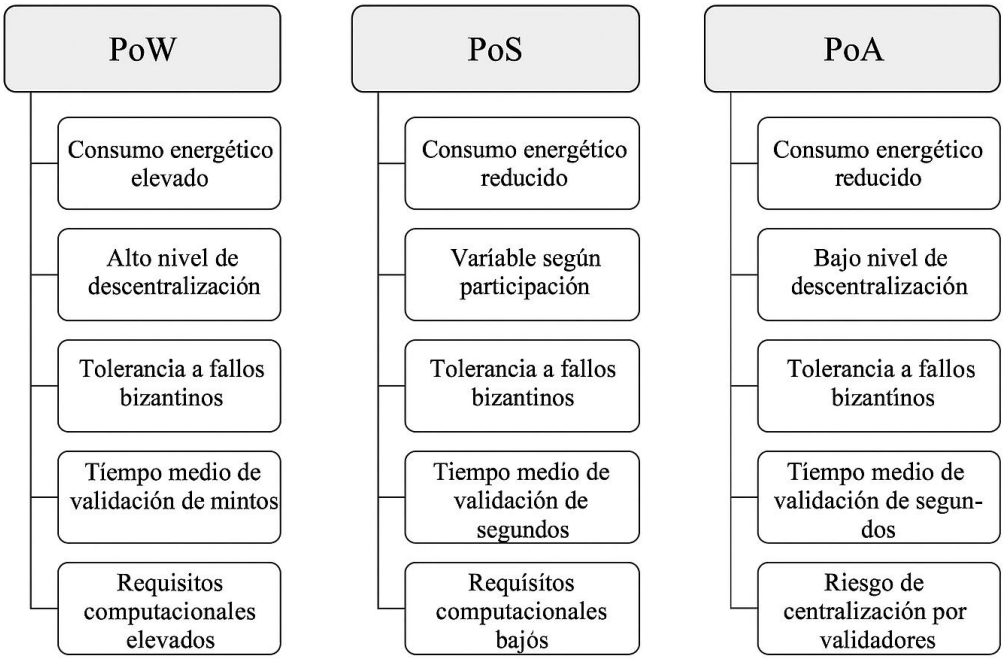
Marco Conceptual

La tecnología Blockchain ha evolucionado como una solución para la gestión de transacciones seguras en un entorno descentralizado. Para comprender la aplicación de esta tecnología en diferentes ámbitos, es necesario tener en cuenta los conceptos asociados a su funcionamiento y seguridad.

Algoritmos de Consenso. Los algoritmos de consenso son fundamentales para la validación de transacciones en Blockchain.

Figura 1

Esquema Comparativo de Algoritmos de Consenso



Nota. Comparación entre PoW, PoS y PoA, con métricas como consumo energético, descentralización, seguridad y requisitos.

Existen diversos mecanismos cómo los que se muestran en la Figura 1, entre ellos:

Proof of Work (PoW). Utilizado en Bitcoin, requiere una gran cantidad de poder computacional para resolver problemas matemáticos y validar transacciones (Saad et al., 2019).

Proof of Stake (PoS). Selecciona validadores en función de la cantidad de criptomonedas que poseen, reduciendo el consumo energético en comparación con PoW (He et al., 2025).

Proof of Authority (PoA). Se emplea en Blockchain privadas, donde un grupo selecto de validadores aprobados garantiza la seguridad y eficiencia de la red (Legerén-Molina, 2019).

Blockchain. Blockchain es una tecnología basada en la descentralización, la criptografía y la verificación distribuida. Cada transacción registrada en la cadena es validada por una red de nodos y almacenada en bloques enlazados mediante algoritmos criptográficos, lo que garantiza la inmutabilidad de los datos (Díaz, 2019). Esta estructura ha permitido revolucionar la gestión de los activos digitales, ofreciendo mayor transparencia y seguridad en procesos financieros y comerciales. Actualmente, Blockchain no solo se limita a criptomonedas, sino que también es utilizada en sistemas de votación electrónica, gestión de identidad digital, cadenas de suministro y aplicaciones en el sector salud (Rosa et al., 2023).

Contratos Inteligentes. Los contratos inteligentes son programas de autoejecución guardados en Blockchain para la automatización de acuerdos sin la necesidad de intermediarios. Han sido ampliamente adoptados en sectores como las finanzas, la logística y la administración pública debido a su capacidad de reducir costos operativos y aumentar la transparencia en los procesos.

A pesar de sus ventajas, los contratos inteligentes también presentan vulnerabilidades. Por ejemplo, los errores en el código pueden ser explotados por atacantes para realizar ataques de reentrada, permitiendo la extracción no autorizada de fondos (Noor & Mustafa, 2024b). Para mitigar estos riesgos, se han desarrollado auditorías de seguridad en contratos inteligentes y se

recomienda el uso de herramientas de verificación formal para evitar errores en su implementación (Mejía et al., 2023).

Criptografía y Hashing en Blockchain. La seguridad en Blockchain se basa en la criptografía asimétrica y los algoritmos de hashing. La criptografía asimétrica utiliza claves públicas y privadas para autenticar transacciones y evitar accesos no autorizados (Díaz, 2019). Los algoritmos de hashing, como SHA-256, permiten verificar la integridad de los datos, validando que cualquier cambio en la información sea identificado de inmediato (Chen et al., 2025).

Con el avance de la criptografía aplicada se han desarrollo mecanismos especializados que mejoran la privacidad en sistemas Blockchain sin comprometer la seguridad estructural ni la validación distribuida. Dos enfoques relevantes son los zk-SNARKs y las firmas de anillo.

Los zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) son pruebas criptográficas que permiten verificar la validez de una transacción sin revelar los datos que la componen. Gracias a esta tecnología, es posible garantizar el anonimato del emisor, el receptor y el valor de la operación, lo cual es particularmente útil en plataformas públicas. Este tipo de mecanismos ha sido adoptado en redes como Zcash, permitiendo la validación de operaciones sin exposición de información confidencial (Santoso & Christyono, 2023).

A su vez, las firmas de anillo permiten que un participante firme digitalmente una transacción dentro de un grupo, sin que se pueda identificar cuál de los miembros lo hizo. Esto proporciona anonimato plausible al firmante, dificultando la trazabilidad directa (Han et al., 2022). Este enfoque ha sido implementado en sistemas como Monero, fortaleciendo la privacidad de los usuarios sin requerir confianza en terceros.

Ambos mecanismos, aunque complejos en su estructura matemática, representan avances significativos para permitir aplicaciones más confidenciales en Blockchain, como los sistemas de

votación, la protección de identidad digital y las operaciones financieras sensibles. Su integración evidencia cómo la criptografía evoluciona para responder a las crecientes exigencias de privacidad en entornos distribuidos.

También es importante mencionar que uno de los principales beneficios de la criptografía en Blockchain es la creación de un sistema seguro y resistente a manipulaciones. Sin embargo, existen riesgos asociados, como los ataques de colisión, en los que dos entradas diferentes generan el mismo hash, poniendo en peligro la seguridad de la cadena. Para mitigar estos riesgos, se han desarrollado nuevos protocolos de hashing y se investiga la posibilidad de integrar criptografía cuántica en los sistemas Blockchain (Kouki et al., 2025).

Escalabilidad en Blockchain. La escalabilidad es un reto clave para Blockchain, ya que las redes congestionadas pueden presentar tiempos de confirmación elevados y costos operativos altos. Soluciones como la fragmentación (sharding) y las cadenas laterales (sidechains) han sido desarrolladas para mejorar la capacidad de procesamiento de transacciones y optimizar el rendimiento de la red (Kouki et al., 2025).

Identidad Digital en Blockchain. Blockchain se ha convertido en una excelente alternativa para el aseguramiento de identidad digital. Almacenar credenciales verificadas en una Blockchain permite a los usuarios controlar su información personal sin depender de intermediarios (Rosa et al., 2023). Este enfoque mejora la seguridad y la privacidad en procesos de verificación de identidad, reduciendo el fraude y la suplantación de identidad en transacciones en línea (Pu & Qiao, 2025).

Interoperabilidad en Blockchain. Uno de los mayores desafíos en la expansión de Blockchain es la interoperabilidad entre diferentes redes. Actualmente, muchas Blockchain operan de manera independiente, lo que limita la transferencia de datos y activos entre plataformas. La falta de

estandarización impide que Blockchain públicas y privadas interactúen eficientemente, dificultando su integración en sistemas empresariales (Noor & Mustafa, 2024b).

Para abordar este problema, se han desarrollado protocolos de interoperabilidad como Polkadot y Cosmos, que permiten la comunicación entre múltiples Blockchain sin comprometer la seguridad de las transacciones (Mejía et al., 2023).

Privacidad y Gobernanza en Blockchain. Si bien Blockchain ofrece transparencia y descentralización, también presenta desafíos en cuanto a privacidad. En redes públicas, las transacciones son visibles para todos los participantes, lo que puede comprometer la confidencialidad de los datos. Investigaciones recientes han propuesto soluciones como transacciones confidenciales y direcciones encriptadas para mejorar la protección de datos en Blockchain (Rosa et al., 2023).

La gobernanza de Blockchain varía según el tipo de red. En las Blockchain públicas, las decisiones se realizan de forma descentralizada a través de mecanismos de consenso. En cambio, en las Blockchain privadas, una entidad centralizada regula la red, lo que permite mayor eficiencia, pero reduce la descentralización (Pu & Qiao, 2025). Además, algunos proyectos han implementado sistemas de gobernanza híbridos, combinando la descentralización con mecanismos de control que garantizan el cumplimiento de normativas legales y de seguridad.

Marco Teórico

La tecnología Blockchain ha sido estudiada en áreas como la ciberseguridad, la economía digital y la informática distribuida, mostrando su impacto en la transformación digital de diversas industrias (Mejía et al., 2023).

Orígenes y Evolución de Blockchain. La tecnología Blockchain fue definida inicialmente en 1991 por Stuart Haber y W. Scott Stornetta, con una propuesta que la describió como un sistema criptográficamente seguro para el estampado de tiempo en documentación digitalizada. Aun así, su uso práctico surgió con el nacimiento de Bitcoin en 2008, estableciendo la primera red Blockchain descentralizada (Saad et al., 2020). Desde entonces, la tecnología ha evolucionado hacia aplicaciones en múltiples sectores, como las finanzas descentralizadas (*DeFi*), los contratos inteligentes y la seguridad de la información (He et al., 2025).

Estructura y Funcionamiento de Blockchain. Blockchain está basado en interconexión de bloques, donde cada bloque alberga una cantidad determinada de transacciones validadas. Su funcionamiento depende de la combinación de tres elementos clave:

Descentralización. La información no está almacenada en un solo servidor, sino distribuida entre múltiples nodos, reduciendo el riesgo de ataques (Díaz, 2019).

Inmutabilidad. Una vez que una transacción es validada e incluida en un bloque, no puede ser alterada sin modificar toda la cadena (Chen et al., 2025).

Seguridad Criptográfica. El uso de firmas digitales y funciones hash garantiza la integridad y autenticidad de las transacciones (Kouki et al., 2025).

Aplicaciones de Blockchain en Diversos Sectores.

Sector Financiero. Blockchain ha revolucionado los servicios financieros a través de criptomonedas, pagos transfronterizos y contratos inteligentes. Se estima que más del 60% de las

instituciones bancarias están explorando su adopción para mejorar la seguridad y eficiencia en las transacciones digitales (Pandey & Kushwaha, 2025).

Cadenas de Suministro. La trazabilidad de productos es uno de los mayores beneficios de Blockchain en la logística. Empresas han implementado esta tecnología para reducir fraudes y mejorar la transparencia en la distribución de bienes (Lotfi et al., 2025).

Salud y Protección de Datos. Blockchain asegura el almacenamiento de historiales médicos, garantizando la privacidad y accesibilidad solo a partes autorizadas (Rosa et al., 2023). En 2024, más del 20% de los hospitales en economías avanzadas adoptaron esta tecnología para mejorar la interoperabilidad de los registros médicos electrónicos (Pu & Qiao, 2025).

Desafíos y Futuro de Blockchain.

Escalabilidad y Consumo Energético. Uno de los principales desafíos que enfrenta Blockchain es la escalabilidad, ya que redes como Bitcoin solo pueden procesar aproximadamente siete transacciones por segundo. Soluciones como las cadenas laterales (*sidechains*) y la fragmentación (*sharding*) buscan abordar estos problemas, mejorando la eficiencia de las redes descentralizadas (Kouki et al., 2025).

Regulación y Marco Legal. La falta de regulaciones globales es otro obstáculo para la adopción masiva de Blockchain. Algunos países han desarrollado marcos normativos específicos para criptomonedas y contratos inteligentes, mientras que otros han prohibido su uso debido a preocupaciones sobre el lavado de dinero y la financiación ilícita.

Interoperabilidad. Dado que existen múltiples plataformas Blockchain operando de manera independiente, se han desarrollado protocolos como Polkadot y Cosmos para facilitar la interoperabilidad entre ellas (Noor & Mustafa, 2024b). Esto permitirá una mayor integración de Blockchain en distintos ecosistemas empresariales y gubernamentales.

Marco Legal

Las regulaciones sobre Blockchain han evolucionado de manera diferente en cada país y sector. La adopción de esta tecnología en ámbitos financieros, comerciales y gubernamentales ha impulsado la creación de marcos normativos para garantizar su uso seguro y conforme a la legislación vigente (Fernández López, 2021).

Normativas y Regulaciones Internacionales. A nivel global han desarrollado regulaciones sobre legalidad y seguridad de Blockchain.

Unión Europea (UE). Ha establecido normativas como el Reglamento de Mercados de Criptoactivos (*MiCA*), que regula el uso de criptomonedas y Blockchain en transacciones digitales (Llamas Covarrubias, 2021).

Estados Unidos. Diferentes agencias, como la Comisión de Bolsa y Valores (*SEC*), han implementado regulaciones para garantizar la transparencia y evitar fraudes financieros en Blockchain (Pu & Qiao, 2025).

Asia. Países como China y Japón han desarrollado legislaciones específicas que buscan controlar el uso de criptomonedas y fomentar el desarrollo de Blockchain en sectores estratégicos (Lotfi et al., 2025).

Protección de Datos y Privacidad. Uno de los principales desafíos regulatorios de Blockchain es su compatibilidad con normativas de protección de datos. La inmutabilidad de Blockchain entra en conflicto con el derecho al olvido, lo que ha llevado a la exploración de soluciones híbridas que permitan la eliminación de información sin comprometer la integridad de la red (Llamas Covarrubias, 2021).

Uso de Blockchain en Contratos y Documentación Legal. Los contratos inteligentes han despertado el interés de la comunidad legal debido a su capacidad para automatizar acuerdos sin

necesidad de intermediarios. Sin embargo, su validez jurídica sigue siendo un área de debate. En países como EE.UU. y la UE, ya existen marcos que reconocen la validez de los contratos inteligentes en ciertas jurisdicciones (Fernández López, 2021). Además, Blockchain ha sido utilizada en la notarización digital de documentos, garantizando su autenticidad y evitando falsificaciones (Mejía et al., 2023).

Desafíos y Perspectivas Regulatorias. A pesar de los avances normativos, existen desafíos que deben abordarse para una adopción más amplia de Blockchain:

Falta de Armonización Legal. Diferencias en las regulaciones internacionales dificultan el comercio global basado en Blockchain (Pandey & Kushwaha, 2025).

Responsabilidad Legal. Determinar la responsabilidad en transacciones automatizadas y contratos inteligentes sigue siendo un tema sin resolución clara (Noor & Mustafa, 2024b).

Cumplimiento Fiscal. La integración de Blockchain en sistemas fiscales requiere nuevas metodologías para la tributación de activos digitales y transacciones en criptomonedas (Legerén-Molina, 2019).

La proyección apunta a que, en los siguientes años, los gobiernos y organismos internacionales seguirán desarrollando marcos regulatorios que equilibren la innovación tecnológica con la seguridad y el cumplimiento legal.

Marco Contextual

El impacto de Blockchain varía según el sector y la región en la que se implemente. Su adopción ha crecido exponencialmente en industrias como la financiera, la salud, la administración pública y la cadena de suministro, pero también enfrenta desafíos técnicos y regulatorios que afectan su integración (Pu & Qiao, 2025).

Blockchain en el Sector Financiero. En el ámbito financiero, Blockchain ha innovado la operación de pagos, transferencias y contratos. Su aplicación en criptomonedas y sistemas de pago transfronterizos ha permitido reducir costos y tiempos de procesamiento, además de mejorar la seguridad en las transacciones. Se estima que más del 60% de las instituciones bancarias están explorando su adopción para aumentar la eficiencia en los sistemas financieros tradicionales (Pandey & Kushwaha, 2025). Sin embargo, la volatilidad de las criptomonedas y la falta de regulaciones han dificultado su aceptación generalizada. Algunos gobiernos han implementado monedas digitales de banco central (CBDC) basadas en Blockchain para aprovechar sus beneficios sin los riesgos asociados a las criptomonedas descentralizadas (Fernández López, 2021).

Blockchain en la Administración Pública. Gobiernos de diversas partes del mundo han comenzado a implementar Blockchain para optimizar la seguridad y transparencia en la gestión de datos. Aplicaciones como la votación electrónica, la emisión de documentos digitales y el control del gasto público han demostrado que esta tecnología puede reducir la corrupción y aumentar la eficiencia administrativa (Pu & Qiao, 2025).

En Estonia, por ejemplo, Blockchain es utilizada para garantizar la integridad de los registros notariales y de salud, asegurando que solo los ciudadanos autorizados puedan acceder a su información. En América Latina, algunos países han comenzado a explorar su uso en registros

de propiedad y administración tributaria para evitar fraudes y errores en la documentación (Lotfi et al., 2025).

Blockchain en la Salud. El sector salud ha encontrado en Blockchain una solución efectiva para mejorar la interoperabilidad de los sistemas médicos y asegurar los datos de los pacientes. La descentralización permite a los profesionales de la salud acceder a historiales clínicos sin comprometer la privacidad de los pacientes, reduciendo el riesgo de pérdida o manipulación de la información (Rosa et al., 2023).

Además, Blockchain ha sido utilizada para optimizar la cadena de suministro de medicamentos, asegurando la autenticidad de los productos y reduciendo el fraude en la distribución de fármacos (Llamas Covarrubias, 2021). En 2024, se reportó que más del 20% de los hospitales en economías avanzadas han implementado sistemas Blockchain para gestionar historiales médicos electrónicos y mejorar la seguridad de los datos clínicos (Pu & Qiao, 2025).

Blockchain en la Industria y la Cadena de Suministro. Empresas de manufactura y logística han implementado Blockchain para respaldar la trazabilidad de los productos evitando fraudes en la cadena de suministro. La posibilidad de registrar cada paso de un producto, desde su fabricación hasta su entrega, ha permitido optimizar la eficiencia y reducir la falsificación de productos en industrias como la alimentaria, automotriz y tecnológica (Lotfi et al., 2025).

En el comercio internacional, Blockchain ha reducido en un 40% el tiempo de verificación de documentos aduaneros, mejorando la velocidad y confiabilidad de las operaciones de importación y exportación (Mejía et al., 2023). Además, su implementación ha permitido una reducción del 30% en costos administrativos relacionados con la logística global.

Desafíos y Perspectivas de Blockchain en Diferentes Contextos. A pesar de los avances en la implementación de Blockchain, existen desafíos que afectan su adopción a gran escala:

Regulación Incierta. La falta de marcos normativos claros en muchas regiones dificulta la inversión en tecnologías basadas en Blockchain (Fernández López, 2021).

Costos de Implementación. La infraestructura necesaria para operar redes Blockchain puede ser costosa para empresas y gobiernos, lo que limita su adopción en economías emergentes (Noor & Mustafa, 2024b).

Escalabilidad. A medida que más usuarios se suman a una red Blockchain, la capacidad de procesamiento de transacciones puede verse afectada, generando tiempos de espera más largos y mayores costos (Kouki et al., 2025).

A futuro, se espera que la adopción de Blockchain continúe expandiéndose con la mejora de protocolos de interoperabilidad y soluciones de escalabilidad. La combinación de Blockchain con inteligencia artificial y computación cuántica podría abrir nuevas oportunidades para su aplicación en sectores emergentes y consolidar su papel en la transformación digital global (Pandey & Kushwaha, 2025).

Diseño Metodológico

Enfoque de la Investigación

Se adoptará un enfoque cualitativo, ya que se centra en el análisis teórico y documental de la tecnología Blockchain, sus aplicaciones y su marco regulatorio. Se busca interpretar la información existente para extraer conclusiones fundamentadas sobre su impacto en diferentes sectores.

Tipo de Investigación

Se aplicará una investigación documental y descriptiva, pues se basa en la revisión de literatura científica arbitrada y fuentes especializadas. Se analizarán artículos, libros y normativas para describir el estado actual de Blockchain y sus implicaciones en ámbitos como la seguridad, la economía y la legislación.

Método de Investigación

Se aplicará el método hermenéutico y analítico, permitiendo la interpretación de textos académicos y normativas existentes para establecer relaciones entre las teorías y aplicaciones prácticas de Blockchain.

Fuentes de Información

Se usarán fuentes alternas, incluyendo artículos indexados en bases de datos científicas (SCOPUS, IEEE, Springer, Elsevier), normativas gubernamentales y libros especializados en la temática.

Técnicas de Recolección de Información

La recopilación de datos partirá de una revisión sistemática de la documentación existente sobre el tema a investigar, priorizando estudios publicados en los últimos cinco años para garantizar actualidad y relevancia.

Análisis de Datos

Se aplicará un **análisis cualitativo** mediante la categorización de la información relacionada con los aspectos relevantes de la investigación (seguridad, gobernanza, escalabilidad, regulaciones, aplicaciones prácticas).

Criterios de Validación

La validez del estudio se garantizará mediante la triangulación de fuentes, contrastando diferentes perspectivas y estudios para evitar sesgos.

Superficies de Ataque y Vulnerabilidades Críticas en Blockchain

La tecnología Blockchain ha sido adoptada en diversos sectores debido a sus propiedades de descentralización, inmutabilidad y transparencia. No obstante, su creciente implementación ha expuesto nuevas superficies de ataque que pueden ser aprovechadas por actores malintencionados. La seguridad en estos sistemas no solo depende de sus principios criptográficos, sino también de la robustez del software y la infraestructura que los soporta.

Ante este panorama, resulta necesario examinar las vulnerabilidades que afectan a Blockchain, abarcando contratos inteligentes, nodos y red P2P, protocolos de consenso y almacenamiento de datos. En este capítulo, se identifican los principales puntos de exposición en estos entornos, se analizan ejemplos de ataques documentados y se presentan códigos CVE relevantes. Asimismo, se plantean enfoques de mitigación basados en auditorías de seguridad, mejoras en los protocolos y el uso de inteligencia artificial para la detección temprana de amenazas. La información aquí expuesta servirá de base para el desarrollo de estrategias que fortalezcan la protección de los sistemas Blockchain en capítulos posteriores.

Superficies de Ataque en Blockchain

La seguridad en Blockchain ha sido objeto de estudio debido a las múltiples vulnerabilidades documentadas en sus diferentes componentes. Estas vulnerabilidades han sido recopiladas y reportadas en bases de datos de seguridad informática, como la lista Common Vulnerabilities and Exposures (CVE), administrada por MITRE, y en informes de organismos especializados en ciberseguridad, pueden derivarse de errores en el código, fallos en la implementación de los mecanismos de consenso o vulnerabilidades en la red de nodos.

La explotación de estas fallas ha generado pérdidas millonarias y afectado la confianza en esta tecnología.

Las superficies de ataque en Blockchain abarcan diversas capas del sistema, desde el código de los contratos inteligentes hasta la infraestructura de red y los mecanismos de consenso. Identificar y analizar estos puntos de vulnerabilidad permite comprender los riesgos a los que están expuestos los sistemas descentralizados y desarrollar estrategias para mitigarlos.

Contratos Inteligentes. Uno de los principales puntos de exposición en Blockchain son los contratos inteligentes, los cuales pueden contener errores de programación que los vuelven vulnerables a ataques. La reentrada, visualizada en la Figura 2, es una de las fallas más explotadas, permitiendo a los atacantes retirar fondos repetidamente antes de que se actualice el estado del contrato (Vidal et al., 2024). De igual manera, las condiciones de carrera pueden generar inconsistencias en la ejecución de transacciones, comprometiendo la seguridad de los activos digitales (Fernández López, 2021). Estas vulnerabilidades demuestran la importancia de realizar auditorías de código y emplear herramientas automatizadas de verificación formal.

Los contratos inteligentes son programas que se ejecutan en la Blockchain para automatizar acuerdos sin intermediarios. Sin embargo, su código puede contener fallos explotables por atacantes, lo que los convierte en una de las superficies de ataque más estudiadas. Entre las vulnerabilidades más comunes se encuentran:

Reentrada. Un atacante puede explotar esta vulnerabilidad para ejecutar múltiples retiros de fondos antes de que la transacción inicial sea validada (Vidal et al., 2024). Un caso documentado de esta vulnerabilidad es **CVE-2018-10299**, que permitió la extracción indebida de fondos en contratos de Ethereum.

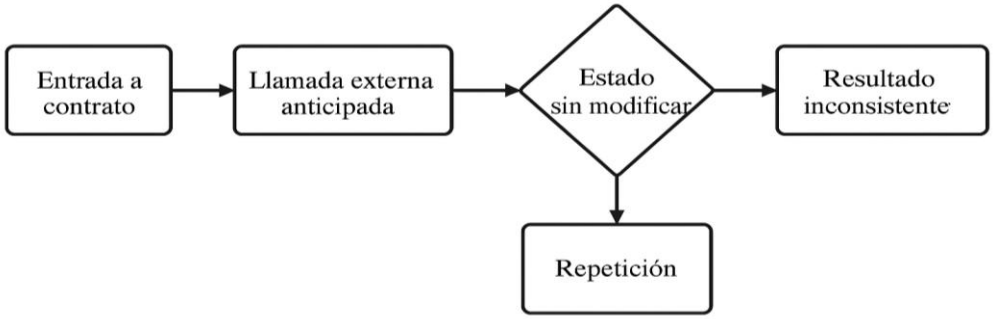
Desbordamiento y Subdesbordamiento de Enteros. Errores en la gestión de valores numéricos pueden permitir manipulaciones indebidas en los cálculos financieros (Pandey &

Kushwaha, 2025). La vulnerabilidad **CVE-2020-26264** evidenció cómo un desbordamiento podía modificar saldos de manera no autorizada.

Condiciones de Carrera. Ocurren cuando múltiples transacciones intentan modificar el mismo estado del contrato simultáneamente, generando inconsistencias (Fernández López, 2021). La explotación de **CVE-2022-3298** permitió que atacantes ejecutaran múltiples transacciones paralelas antes de la actualización del estado del contrato.

Figura 2

Diagrama de Ataque por Reentrada en Contratos Inteligentes



Nota. Flujo lógico del exploit donde un atacante extrae fondos sin actualizar el estado del contrato.

Nodos y Red P2P. Los ataques dirigidos a la infraestructura de red también representan un desafío significativo. La manipulación de nodos a través de ataques Sybil y Eclipse, tal como se muestra en la Figura 3, afecta el mecanismo de consenso y la propagación de transacciones en la red (Mejía et al., 2023). En estos casos, los atacantes crean múltiples identidades falsas o aíslan nodos legítimos, alterando la visión global del estado de la Blockchain. La descentralización y la diversidad de nodos validadores son estrategias clave para mitigar estos riesgos.

Los nodos de la red Blockchain procesan y validan transacciones dentro de una estructura descentralizada. Sin embargo, pueden ser objetivo de ataques que comprometan la seguridad del sistema. Algunas amenazas destacadas incluyen:

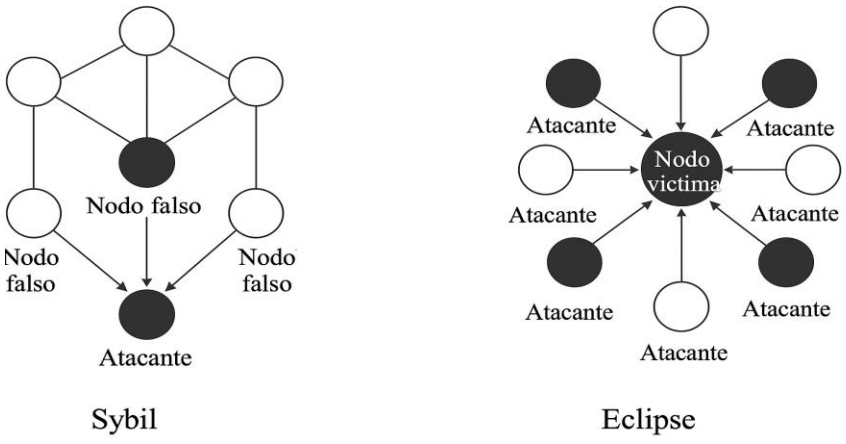
Ataque Sybil. Consiste en la creación de múltiples identidades falsas para influir en el consenso de la red (Mejía et al., 2023). La vulnerabilidad **CVE-2019-6111** permitió la manipulación del consenso a través de la proliferación de nodos maliciosos.

Ataque Eclipse. Aislamiento de un nodo de la red legítima para manipular su visión del estado de la Blockchain (Ding et al., 2024). Un caso documentado es **CVE-2021-31684**, que permitió a los atacantes filtrar y modificar transacciones antes de su confirmación en la red.

Envenenamiento de la Red. Introducción de datos maliciosos que afectan el funcionamiento de la red P2P (Pourrahmani et al., 2023). En **CVE-2020-28348**, se demostró cómo atacantes podían insertar datos dañinos para comprometer la confiabilidad de los nodos.

Figura 3

Ataques Sybil y Eclipse en redes



Nota. Esquema visual que muestra cómo se realiza cada tipo de ataque y sus efectos sobre los nodos.

Protocolos de Consenso. En cuanto a los protocolos de consenso, el ataque del 51% es una de las amenazas más documentadas, especialmente en redes que utilizan Proof of Work (PoW) (Pourrahmani et al., 2023). Este tipo de ataque permite la reorganización de bloques y la reversión de transacciones, lo que puede generar un doble gasto y pérdidas económicas significativas. Por otro lado, los mecanismos de Proof of Stake (PoS) también presentan vulnerabilidades, como la posibilidad de que validadores malintencionados concentren la toma de decisiones dentro de la red, debilitando su seguridad (Hosseini Bamakan & Banaeian Far, 2025).

Los mecanismos de consenso garantizan la validez de las transacciones en Blockchain. Sin embargo, también presentan vulnerabilidades que pueden ser explotadas por actores malintencionados. Algunos de los ataques más relevantes incluyen:

Ataque del 51%. Un actor que controle más del 50% del poder de cómputo en una Blockchain PoW puede reorganizar transacciones y revertir pagos (Lotfi et al., 2025). Un caso emblemático fue el ataque a Bitcoin Gold en 2020, que resultó en pérdidas superiores a los 70 millones de dólares.

Manipulación en Prueba de Participación (PoS). En redes PoS, un atacante con una cantidad significativa de tokens puede influir en la validación de bloques de manera desleal (Hosseini Bamakan & Banaeian Far, 2025). La vulnerabilidad **CVE-2022-23539** permitió que validadores malintencionados ejecutaran ataques de doble gasto en ciertas plataformas PoS.

Almacenamiento y Privacidad de Datos. En términos de almacenamiento y privacidad de datos, Blockchain plantea desafíos únicos. Aunque sus transacciones son seudónimas, técnicas avanzadas de análisis pueden revelar identidades de usuarios mediante la correlación de datos (Padilla Sánchez, 2020). Además, la inmutabilidad de la Blockchain implica que cualquier

información comprometida almacenada en la red no puede ser eliminada, lo que representa un riesgo potencial para la privacidad y la confidencialidad de los datos (Ibáñez Jiménez, 2018).

El almacenamiento de información en Blockchain plantea desafíos en términos de privacidad y exposición de datos sensibles. Algunas amenazas clave incluyen:

Análisis de Patrones de Transacciones. Aunque las transacciones en Blockchain son seudónimas, técnicas avanzadas pueden revelar identidades de los usuarios (Padilla Sánchez, 2020). En **CVE-2023-18247**, se demostró que herramientas de análisis podían rastrear transacciones y vincularlas a usuarios específicos.

Persistencia de Datos Sensibles. Una vez que la información es registrada en la Blockchain, no puede ser eliminada, lo que puede generar riesgos de exposición involuntaria (Ibáñez Jiménez, 2018). La vulnerabilidad **CVE-2021-32456** documentó cómo ciertos datos cifrados almacenados en Blockchain podían ser descifrados con métodos avanzados.

La Tabla 1 presenta un resumen de ataques documentados en Blockchain, destacando las vulnerabilidades explotadas, sus consecuencias y los códigos CVE asociados. Este análisis permite comprender cómo han sido aprovechadas estas debilidades en la práctica y proporciona una base para el desarrollo de estrategias de mitigación efectivas.

Tabla 1

Ejemplos de Ataques Documentados en Blockchain y sus Vulnerabilidades

Vulnerabilidad	Ejemplo Documentado	Impacto	Causa	Código CVE
Reentrada	Ataque a The DAO en Ethereum (2016)	Pérdidas de $50M	Fallo en la gestión del estado del contrato	CVE-2018-10299
Ataque del 51%	Bitcoin Gold (2020)	Pérdidas de $70M	Control mayoritario del poder de cómputo	CVE-2020-28348
Eclipse	Manipulación de nodos en Ethereum	Alteración de la confirmación de transacciones	Aislamiento de nodos de la red legítima	CVE-2021-31684
Desbordamiento de enteros	Explotación en múltiples contratos	Manipulación de valores financieros	Errores en la asignación de memoria	CVE-2020-26264
Condiciones de carrera	Fallo en contratos inteligentes	Modificación del estado antes de confirmación	Ejecución paralela de transacciones	CVE-2022-3298
Envenenamiento de la red	Manipulación de nodos P2P	Saturación de la red con datos corruptos	Inserción de información maliciosa	CVE-2020-28348

Nota. Ataques documentados en Blockchain, con detalle de las vulnerabilidades explotadas, el impacto generado y los códigos CVE correspondientes. Adaptado de Vidal, Ivaki & Laranjeiro (2024); Fernández López 2021); Mejía et al. (2023); Pourrahmani et al. (2023).

Impacto de las Vulnerabilidades en Blockchain

El impacto de las vulnerabilidades en Blockchain se manifiesta en múltiples aspectos, desde pérdidas económicas hasta compromisos en la seguridad y confiabilidad de las redes descentralizadas. El análisis de estas vulnerabilidades permite comprender su alcance y establecer medidas efectivas de mitigación.

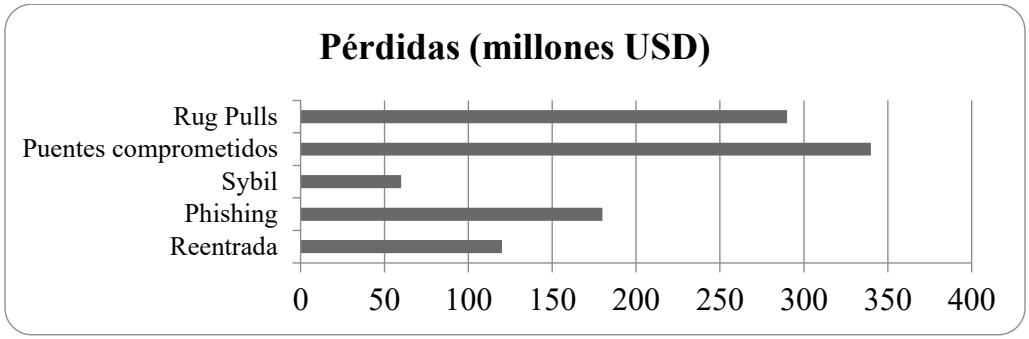
Impacto Económico. Las vulnerabilidades en Blockchain han causado pérdidas millonarias, tal como se muestra en la figura 4, debido a robos de fondos, explotación de contratos inteligentes y ataques a la infraestructura de red. Por ejemplo, en 2022, un ataque a la plataforma Ronin Network resultó en el robo de más de 600 millones de dólares en criptomonedas (Mejía et al., 2023).

Impacto en la Seguridad y Confianza. Los ataques y vulnerabilidades en Blockchain pueden erosionar la confianza de los usuarios y las empresas en la tecnología. Incidentes como la explotación de contratos inteligentes en plataformas DeFi han demostrado que incluso sistemas altamente descentralizados pueden ser vulnerables si no se implementan medidas de seguridad adecuadas (Padilla Sánchez, 2020).

Implicaciones Regulatorias y Legales. El descubrimiento de vulnerabilidades en Blockchain también ha generado preocupaciones regulatorias y legales. Gobiernos y organismos internacionales han intensificado sus esfuerzos para establecer normativas que reduzcan los riesgos asociados a la tecnología (Ibáñez Jiménez, 2018).

Figura 4

Impacto Económico de los Principales Ataques en Blockchain



Nota. Gráfico de barras con montos comprometidos en millones de dólares por tipo de ataque.

Clasificación de Vulnerabilidades en Blockchain según Marcos de Referencia

Diversos marcos han establecido categorías de vulnerabilidades específicas en sistemas distribuidos. A continuación, se presenta en la Tabla 2 una relación entre algunas de las vulnerabilidades más críticas detectadas en Blockchain y su correspondencia con clasificaciones oficiales como OWASP Blockchain Top 10 y NIST SP 800-183.

Este enfoque sistematiza las vulnerabilidades tratadas, alineándolas con los estándares más reconocidos en ciberseguridad para Blockchain.

Tabla 2

Relación entre Vulnerabilidades en Blockchain y Marcos de Referencia

Vulnerabilidad	Categoría OWASP Blockchain (2023)	Capa según NIST SP 800-183
Reentrada	**B10:** Inadequate Contract Isolation	Capa de ejecución de contratos inteligentes
Desbordamiento de enteros	**B03:** Integer Overflow/Underflow	Capa de lógica de aplicación
Ataque del 51%	**B09:** Consensus Manipulation	Capa de consenso
Ataque Sybil	**B02:** Identity Management and Sybil Attacks	Capa de red y autenticación
Análisis de transacciones	**B08:** Privacy Issues and Data Leaks	Capa de almacenamiento
Envenenamiento de red	**B06:** Denial of Service via P2P Messaging	Capa de red P2P

Nota. Adaptado de OWASP (2023); NIST SP 800-183 (2021).

Principales Amenazas que Afectan la Seguridad de Blockchain

Análisis de Amenazas

El análisis de amenazas es un componente esencial para comprender los riesgos que enfrenta cualquier infraestructura tecnológica, y en el caso de Blockchain, adquiere particular relevancia debido a su estructura distribuida, inmutabilidad y ejecución autónoma de contratos inteligentes. Aunque a menudo se promueve como una tecnología "segura por diseño", la realidad operativa ha demostrado que existen múltiples vectores que pueden ser explotados si no se toman medidas proactivas.

Las amenazas que enfrenta Blockchain no son homogéneas: se manifiestan desde vulnerabilidades lógicas en los contratos hasta ataques de red, compromisos de claves privadas, manipulación de datos externos y saturación de nodos. Algunas de estas amenazas son comunes a otras tecnologías, pero su impacto en entornos descentralizados puede tener consecuencias más graves debido a la ausencia de control centralizado y a la alta dependencia de la integridad del consenso distribuido. Este capítulo realiza un análisis técnico, estructurado y progresivo de dichas amenazas, estableciendo su impacto, clasificación, precedentes y mecanismos actuales de respuesta.

Clasificación de Amenazas según Principios de Seguridad de la Información

En seguridad informática, los principios de confidencialidad, integridad y disponibilidad (CID) se utilizan para determinar cómo un sistema puede verse afectado ante un incidente de seguridad. Blockchain, al tratarse de un sistema criptográficamente robusto pero expuesto por diseño, presenta amenazas que pueden impactar estos tres principios en diferentes capas: desde la infraestructura hasta el usuario final.

La seguridad de la información en Blockchain puede analizarse a partir de la triada CID, que permite visualizar el tipo de impacto generado por cada amenaza identificada, tal como se muestra en la Tabla 3.

Tabla 3

Clasificación de Amenazas según Principios de Seguridad de la Información

Tipo de Amenaza	Confidencialidad	Integridad	Disponibilidad
Robo de claves privadas	✓	✓	✗
Ataques de reentrada	✗	✓	✓
Ataques del 51%	✗	✓	✓
Manipulación de oráculos	✗	✓	✗
DoS / DDoS a nodos	✗	✗	✓
Análisis de patrones transaccionales	✓	✗	✗

Nota: Amenazas que afectan diferentes dimensiones de la seguridad. La integridad es el principio más frecuentemente vulnerado, lo que resalta la necesidad de reforzar el control sobre los flujos internos y lógicos de la red.

La distribución de las amenazas en la tecnología blockchain se puede analizar desde la perspectiva de la tríada de confidencialidad, integridad y disponibilidad (CIA). La naturaleza descentralizada de la cadena de bloques ofrece ventajas únicas a la hora de abordar las amenazas a la ciberseguridad, especialmente en los sistemas colaborativos de detección de intrusiones (CIDS). Sin embargo, también presenta vulnerabilidades que los atacantes pueden aprovechar,

visto en la Figura 5. Las siguientes secciones describen cómo la cadena de bloques interactúa con la tríada de la CIA en el contexto de la distribución de amenazas.

Confidencialidad. El seudoanonimato de la cadena de bloques puede limitar la confidencialidad, ya que los datos de las transacciones son visibles para todos los participantes (Huang, 2023).

Las tecnologías que preservan la privacidad son necesarias para mejorar la confidencialidad en los sistemas de cadenas de bloques, especialmente en aplicaciones sensibles como el IoT y el CPS (Bhattacharjya, 2022).

Integridad. La inmutabilidad de la cadena de bloques garantiza una alta integridad de los datos, lo que dificulta que los atacantes alteren los registros de transacciones (Huang, 2023).

Sin embargo, las vulnerabilidades en los mecanismos de consenso pueden comprometer la integridad, como se ha visto en varios ataques a redes blockchain (Cheng et al., 2021).

Disponibilidad. La disponibilidad de la cadena de bloques depende de la replicación de los datos y la escalabilidad de la red, que pueden verse afectadas por los ataques DDoS (Bhattacharjya, 2022).

Garantizar una alta disponibilidad requiere una infraestructura y estrategias sólidas para mitigar las posibles disrupciones (Huang, 2023).

Figura 5

Triada CIA Aplicada a Amenazas Blockchain

Nota. Representación gráfica que relaciona amenazas con la confidencialidad, integridad y disponibilidad.

Si bien la tecnología blockchain mejora la seguridad a través de su arquitectura descentralizada, no es inmune a las amenazas. El equilibrio entre aprovechar sus puntos fuertes y abordar sus vulnerabilidades sigue siendo un desafío fundamental en materia de ciberseguridad.

Ataques Documentados y Casos Recientes

La teoría de amenazas en Blockchain se complementa con un análisis forense de eventos que han tenido un impacto económico, técnico y social relevante. La documentación de estos ataques, según la Tabla 4, permite identificar patrones comunes, errores de diseño y fallos humanos que han sido aprovechados para comprometer activos digitales, contratos y nodos.

Estos ataques, aunque diversos en su ejecución, comparten una característica clave: explotan vectores específicos que no han sido gestionados correctamente en la arquitectura o configuración de los sistemas Blockchain involucrados. Analizar estos casos ayuda a cerrar la brecha entre la teoría y la práctica, aportando insumos clave para investigaciones futuras y estrategias de mitigación.

Tabla 4

Casos Documentados de Ataques a Sistemas Blockchain

Año	Plataforma	Tipo de Ataque	Consecuencia	Vector Vulnerado
2016	Ethereum (The DAO)	Reentrada	Robo de más de $50 millones	Lógica de contrato
2020	Bitcoin Gold	Ataque del 51%	Reversión de transacciones y doble gasto	Protocolo de consenso
2022	Solana	Compromiso de carteras	Robo de activos desde más de 8,000 wallets	Gestión de claves privadas
2023	Curve Finance	Falla en compilador	Pérdida de $73 millones en contratos	Herramientas de desarrollo
2023	CoinEx	Fuga de clave privada	Robo de más de $70 millones	Almacenamiento inseguro

Nota: Ejemplos que han marcado puntos de inflexión en la evolución de la seguridad Blockchain. Todos los ataques listados se caracterizan por comprometer de manera directa elementos críticos de la infraestructura o la lógica contractual.

Clasificación según Marcos de Referencia

La alineación con marcos como OWASP Blockchain Top 10, MITRE ATT&CK y NIST SP 800-183 permite establecer taxonomías y controles compartidos que faciliten la detección y mitigación de amenazas a nivel organizacional o técnico, tal cómo se puede ver en la Tabla 5.

Tabla 5

Relación entre Amenazas y Marcos de Referencia

Amenaza	OWASP Blockchain Top 10	MITRE ATT&CK (Categoría)	NIST SP 800-183 (Capa Afectada)
Reentrada	B10: Inadecuado aislamiento	T1606: Compromise Application	Capa de ejecución
Robo de claves	B01: Key Management Errors	T1555: Credentials from Password Stores	Capa de autenticación y acceso
Ataque del 51%	B09: Manipulación de consenso	T1499: Resource Hijacking	Capa de consenso
Manipulación de oráculos	B07: Dependencias no verificadas	T1609: Data from Local System	Capa de integración externa (API)
Saturación P2P (DoS)	B06: Denegación de servicio	T1498: Network Denial of Service	Capa de red y disponibilidad
Análisis de patrones	B08: Fugas de privacidad	T1087: Account Discovery	Capa de metadatos / usuario final

Nota: Esta tabla consolida la convergencia entre amenazas técnicas y marcos normativos de seguridad. Permite asociar cada vector con una capa técnica específica, facilitando el diseño de controles específicos y medibles.

Las características descentralizadas de Blockchain dificultan la aplicación de soluciones tradicionales de seguridad. Por ello, han emergido herramientas específicas que permiten realizar análisis automatizado de contratos inteligentes, supervisión de nodos, trazabilidad forense y detección de anomalías en tiempo real.

El uso de sistemas de gestión de eventos de seguridad (SIEM), redes neuronales, auditoría estática y dinámica de código, así como plataformas especializadas en análisis transaccional, ha permitido a las organizaciones identificar comportamientos anómalos y aplicar estrategias de contención más eficaces. Estas soluciones no solo ayudan a detectar amenazas en curso, sino que también generan información valiosa para prevenir ataques similares en el futuro.

A medida que las arquitecturas Blockchain se complejizan con interoperabilidad entre cadenas, contratos con lógica más avanzada y conexiones con sistemas del mundo real, se vuelve indispensable contar con herramientas que puedan escalar, adaptarse y operar sin necesidad de intermediarios centralizados.

El desarrollo y adopción de herramientas especializadas permite fortalecer la postura de ciberseguridad en entornos Blockchain, reduciendo la dependencia de mecanismos de protección genéricos que no consideran la naturaleza descentralizada de esta tecnología.

Técnicas de Mitigación Frente a Amenazas Comunes

La mitigación de amenazas en Blockchain no puede limitarse a medidas reactivas. Se requiere una combinación de controles proactivos, buenas prácticas de desarrollo, mecanismos criptográficos avanzados y defensas distribuidas, cómo se puede ver en la Tabla 6.

Además, la automatización de respuestas y la actualización periódica del código son aspectos clave para reducir la superficie de ataque.

La elección de técnicas de mitigación debe hacerse según el tipo de red (pública, privada, híbrida), el modelo de consenso utilizado, la sensibilidad de los activos, y el nivel de exposición que tenga el sistema hacia entidades externas. Las soluciones más eficaces son aquellas que combinan capas de defensa sin comprometer la transparencia ni la descentralización.

Tabla 6

Técnicas de Mitigación frente a Amenazas Clave

Amenaza	Mitigación Sugerida
Reentradas	Uso de patrones como Checks-Effects-Interactions, verificación formal, simulaciones de ataque.
Ataques del 51%	Incentivos a la descentralización, ajustes de dificultad, uso de pruebas de participación con penalización.
Robo de claves	Almacenamiento seguro mediante HSM, llaves fragmentadas, autenticación multifactor y rotación periódica.
Manipulación de oráculos	Oráculos descentralizados, validación cruzada de datos, mecanismos de reputación y quorum de respuesta.
Análisis de patrones	Técnicas de anonimización (zk-SNARKs, CoinJoin), fragmentación de transacciones, mezcla probabilística.
DoS / congestión de red	Penalización por spam, filtros de reputación, tolerancia a fallos, uso de nodos espejos y balanceadores.

Nota: La tabla presenta un conjunto de técnicas adaptadas al ecosistema Blockchain, que abordan tanto el origen como el impacto de las amenazas. La combinación de varias estrategias refuerza la resiliencia general del sistema ante ataques sofisticados.

Consolidación de Amenazas Críticas

Con base en el análisis técnico y normativo desarrollado en este capítulo, se identifican cinco amenazas que deben considerarse prioritarias para el desarrollo de soluciones defensivas eficaces. Estas amenazas no solo han sido documentadas en múltiples ataques reales, sino que también representan vectores difíciles de contener con técnicas tradicionales.

La consolidación de estas amenazas busca cerrar la brecha entre la identificación genérica de riesgos y la focalización práctica de vectores explotables. Priorizar estas amenazas permite acotar el espectro de análisis, optimizar el uso de recursos defensivos y alinear la investigación futura con necesidades reales del entorno Blockchain.

Las amenazas priorizadas son:

Reentradas en Contratos Inteligentes. Por su presencia reiterada en exploits de alto impacto, dificultad de detección con pruebas convencionales y dependencia de buenas prácticas de programación.

Compromiso de Claves Privadas. Debido a su efecto directo en el control de activos, el gobierno de contratos y la operación de nodos críticos.

Manipulación de Oráculos Externos. Dado que afecta la veracidad de los datos procesados por contratos inteligentes, distorsionando la lógica de ejecución basada en eventos del mundo real.

Ataques del 51%. Con especial preocupación en redes nuevas, de bajo volumen de minería o participación limitada, donde la reorganización de bloques es más factible.

Denegación de Servicio (DoS) Orientada a Nodos Estratégicos. Genera desequilibrios en redes parcialmente descentralizadas, afectando puntos de validación o monitoreo.

La selección de estas amenazas responde a criterios técnicos de impacto, recurrencia, explotabilidad y relevancia en entornos operativos. Su mitigación exige enfoques multidimensionales y herramientas especializadas.

Amenazas Priorizadas y Líneas de Respuesta

En este apartado se sistematizan las amenazas priorizadas junto a sus componentes afectados y las técnicas más recomendadas para su mitigación, de acuerdo al contenido de la Tabla 7. Esta síntesis técnica tiene como propósito orientar futuras investigaciones, evaluaciones de riesgo, auditorías y decisiones de diseño de infraestructura Blockchain segura.

Tabla 7

Amenazas Críticas y Líneas Técnicas de Mitigación

Amenaza Priorizada	Componente Afectado	Línea de Mitigación Avanzada
Reentradas	Contratos inteligentes	Verificación formal, modelado simbólico, revisión por pares, auditoría continua.
Compromiso de claves	Wallets / nodos	Uso de HSM, separación de funciones, autenticación robusta, fragmentación de claves.
Oráculos manipulados	Entrada de datos externos	Validación multi-fuente, oráculos descentralizados, sistemas de reputación, pruebas de consistencia.
Ataques del 51%	Capa de consenso	Participación federada, penalización automática, ajuste de incentivos y prueba de autoridad.
DoS a nodos críticos	Infraestructura de red	Redundancia distribuida, microservicios resilientes, políticas de calidad de servicio y filtrado dinámico.

Nota: Relación directa entre vectores de riesgo, capas funcionales afectadas y estrategias técnicas viables para reducir el impacto o prevenir la ocurrencia de incidentes similares.

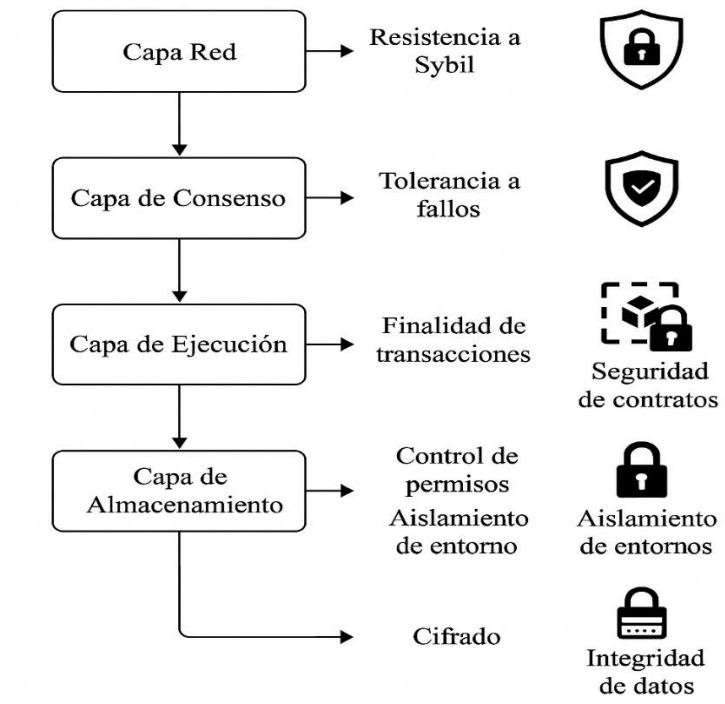
Riesgos Emergentes en Blockchain

Revisión de Marcos de Seguridad y Normativas Aplicables a Blockchain

La integración de Blockchain en entornos organizacionales exige el cumplimiento de normativas internacionales que orienten su despliegue seguro. Esta tecnología no opera en el vacío: sus componentes funcionales deben alinearse con marcos de seguridad consolidados que permitan identificar riesgos, aplicar controles y validar su efectividad. Diversas guías técnicas han sido adaptadas a la lógica descentralizada de las cadenas de bloques, permitiendo su integración con marcos como ISO/IEC 27001, NIST SP 800-183, OWASP Blockchain Top 10 y el repertorio táctico MITRE ATT&CK.

Figura 6

Mapa de Capas Funcionales de Blockchain y Controles de Seguridad Aplicables



Nota. Visualización por capas (red, consenso, ejecución, almacenamiento) con sus respectivos controles.

Cada capa técnica de un sistema Blockchain relacionadas en la Figura 6, ya sea el motor de contratos, la red de nodos, el almacenamiento o los oráculos, presenta desafíos específicos que pueden ser correlacionados con controles recomendados por estos marcos. Esta armonización permite construir arquitecturas seguras sin sacrificar la descentralización ni la eficiencia operativa.

Tabla 8

Relación entre Marcos de Referencia y Capas Funcionales en Sistemas Blockchain

Capa funcional	ISO/IEC 27001	NIST SP 800-183	OWASP Blockchain Top 10	MITRE ATT&CK
Contratos inteligentes	A.14.2.1, A.14.2.5	Capa de ejecución	B10, B03	T1606, T1203
Red y nodos P2P	A.13.1.1, A.13.2.3	Capa de red	B06, B02	T1498, T1557
Almacenamiento de datos	A.8.2.1, A.9.4.1	Capa de almacenamiento	B08	T1005, T1530
Mecanismos de consenso	A.6.1.1, A.18.2.3	Capa de consenso	B09	T1499, T1562
Interoperabilidad y oráculos	A.15.1.1, A.14.2.7	Capa de integración externa	B07	T1609, T1195

Nota. La tabla presenta una correspondencia entre capas técnicas de Blockchain y estándares de ciberseguridad. Su objetivo es facilitar el diseño de controles específicos por capa funcional.

Además de los controles ya mapeados en la Tabla 8, resulta pertinente incluir referencias al Anexo A de la norma ISO/IEC 27001:2022, particularmente aquellos que guardan relación directa con la gestión de seguridad en entornos descentralizados.

A.5.23 Gestión de Identidades y Credenciales. Aplicable al control de acceso en nodos y carteras.

A.8.16 Gestión de Registros de Actividad. Esencial para la trazabilidad en cadenas públicas y privadas.

A.5.15 Seguridad Física de Equipos. Crítica en la protección de hardware wallets y nodos locales.

A.7.4 Gestión de Capacidades de Seguridad en la Nube. Relacionada con servicios Blockchain-as-a-Service.

Estos controles complementan la cobertura técnica y organizacional, permitiendo integrar Blockchain en Sistemas de Gestión de Seguridad de la Información (SGSI) bajo estándares formales.

Evaluación del Riesgo Residual en Sistemas Blockchain

Toda implementación segura de Blockchain debe incluir una valoración clara del riesgo residual: es decir, el riesgo que persiste tras aplicar controles técnicos u organizativos. Esta valoración permite tomar decisiones informadas sobre la tolerancia al riesgo y sobre los recursos que deben destinarse a reforzar los mecanismos de protección.

En sistemas Blockchain, el riesgo residual suele estar subestimado debido a la falsa percepción de seguridad automática derivada de la criptografía o la descentralización. Sin

embargo, muchos incidentes recientes han demostrado que fallas en contratos inteligentes, validadores o servicios externos pueden escapar a controles superficiales.

Para abordar esta problemática, las organizaciones deben construir matrices específicas que contemplen el tipo de ataque, su impacto en términos financieros y reputacionales, la probabilidad de ocurrencia y la cobertura efectiva de los controles implementados. De este modo, es posible identificar vulnerabilidades que requieren medidas adicionales como rediseño de arquitectura, segregación de funciones o refuerzo de monitoreo.

Aplicación del Modelo Zero Trust en Arquitecturas Descentralizadas

El modelo Zero Trust, tradicionalmente aplicado a infraestructuras de red corporativas, puede ser adaptado a sistemas Blockchain con notables ventajas. Este modelo se basa en la premisa de que ningún nodo, usuario o contrato debe ser confiado por defecto, independientemente de su ubicación en la red o su rol asignado.

Al aplicarlo en Blockchain, se propone que cada transacción, interacción con contratos o validación de bloques esté sujeta a múltiples verificaciones independientes. Esto incluye controles como validación de estados intermedios, uso de pruebas criptográficas, y auditorías dinámicas por nodos externos.

Gobernanza Técnica en Ecosistemas Blockchain Empresariales

La gobernanza técnica en Blockchain no se limita a la gestión de claves o a la validación de bloques. Implica la toma de decisiones sobre el ciclo de vida del software desplegado, los parámetros del consenso, la inclusión o expulsión de validadores, y la gestión de incidentes.

Una adecuada gobernanza requiere la existencia de comités técnicos con autoridad para auditar cambios en los contratos, definir políticas de despliegue, aprobar actualizaciones del protocolo y establecer mecanismos de resolución ante errores lógicos o ataques. Además, se

deben contemplar mecanismos de transparencia que permitan auditar las decisiones tomadas sin comprometer la seguridad de la red.

En redes empresariales, esto se traduce en implementar manuales de gobierno, protocolos de votación con quorum, y métricas de desempeño por nodo o módulo funcional. La gobernanza no es opcional: es la base de la sostenibilidad operativa en entornos descentralizados con impacto real en procesos de negocio.

Modelo de Madurez de Ciberseguridad Aplicado a Blockchain

Para evaluar la evolución de la seguridad en sistemas Blockchain, se recomienda implementar un modelo de madurez adaptado que permita diagnosticar el nivel de control y preparación de la organización frente a incidentes y amenazas.

Tabla 9

Modelo de Madurez de Seguridad Aplicado a Blockchain

Nivel	Descripción	Características Clave
1	Inicial	No existen controles documentados; respuestas informales ante incidentes
2	Repetible	Algunos controles establecidos, pero sin monitoreo ni mejora continua
3	Definido	Controles formales; existe documentación y procesos reactivos
4	Gestionado	Supervisión activa; análisis de amenazas; respuesta coordinada
5	Optimizado	Seguridad integrada desde el diseño; auditorías dinámicas; automatización

Nota. El modelo permite realizar diagnósticos internos y establecer planes de mejora continua alineados con riesgos Blockchain.

Si bien el modelo de madurez propuesto en la Tabla 9 y complementado con la Figura 7, permite evaluar el nivel de desarrollo organizacional frente a la seguridad en Blockchain, es necesario complementarlo con una estructura funcional de gestión que integre procesos, roles, políticas y ciclos de mejora continua.

Figura 7

Modelo de Madurez de Seguridad Blockchain

Nota. Niveles de sistemas inmaduros hasta resilientes.

A continuación, se presenta una propuesta de modelo estructurado de gestión, adaptable a redes públicas, privadas o híbridas, que articula las funciones estratégicas, técnicas y operativas requeridas para sostener un esquema de ciberseguridad efectivo.

A partir del modelo de madurez, se debe generar un modelo estructurado de gestión de la ciberseguridad en Blockchain con los siguientes componentes:

Gobernanza. Comité técnico multidisciplinar, con atribuciones para definir políticas, auditar contratos y gestionar incidentes.

Evaluación Continua. Aplicación de marcos como NIST CSF o MAGERIT, adaptados al ciclo de vida de contratos y validadores.

Ciclo PHVA (Planificar-Hacer-Verificar-Actuar). En despliegues, actualizaciones, monitoreo y respuesta.

Integración DevSecOps. Auditoría automática de contratos en etapas CI/CD.

Segmentación de Roles. Entre administradores, validadores, desarrolladores y usuarios finales.

Este modelo busca adaptarse a entornos privados, públicos o híbridos, con controles personalizables por tipo de red.

Controles Técnicos Comparados según Tipo de Blockchain

Las redes Blockchain se pueden clasificar según su estructura de acceso y participación: públicas, privadas e híbridas. Cada una de ellas enfrenta riesgos particulares y, por tanto, requiere controles específicos ajustados a su naturaleza, de acuerdo a la Tabla 10.

Tabla 10

Controles Técnicos Sugeridos según el Tipo de Red Blockchain

Tipo de Blockchain	Riesgo principal	Controles técnicos recomendados
Pública	Ataques Sybil, exploits en contratos	Mecanismos de reputación, auditoría formal, oráculos descentralizados
Privada	Fallos en gobernanza, acceso privilegiado	Segmentación de funciones, control de cambios, monitoreo interno
Híbrida	Falla en puentes intercadena	Validación cruzada, redundancia de datos, control federado de nodos

Nota. La tabla permite diferenciar los enfoques de seguridad según el modelo de red Blockchain adoptado.

Para fortalecer las capacidades reactivas, se sugiere adoptar un esquema de respuesta ante incidentes alineado con ISO/IEC 27035, tal como se muestra en la Figura 8, compuesto por:

Detección. Sensores distribuidos, SIEM, alertas por anomalías.

Notificación. Registros en nodos, oráculos y wallets vinculadas.

Evaluación Inicial. Identificación del tipo de ataque (reentrada, fuga, DoS, etc.)

Contención. Interrupción de contratos, aislamiento de nodos, revocación de claves.

Análisis Forense. Trazabilidad en la cadena, revisión de logs, correlación de eventos.

Recuperación. Ejecución de forks, restauración de estados previos, revalidación.

Lecciones Aprendidas. Retroalimentación al modelo de madurez y controles preventivos.

Figura 8

Ciclo de Respuesta ante Incidentes en Entornos Blockchain según ISO/IEC 27035

Nota. Esta figura ilustra las fases propuestas para la gestión de incidentes en sistemas distribuidos, desde la detección hasta las lecciones aprendidas, aplicadas específicamente a arquitecturas Blockchain con alineación a ISO/IEC 27035.

Ataques Avanzados y Emergentes en Blockchain y su Evolución Reciente

El ecosistema Blockchain ha sido blanco de ataques cada vez más sofisticados, muchos de los cuales no se basan en vulnerabilidades criptográficas, sino en debilidades lógicas, errores

humanos y vectores externos a la red. Estos ataques han evolucionado desde simples estafas por phishing hasta sofisticadas manipulaciones de contratos inteligentes y exploits en puentes intercadena.

En apartados anteriores se ha dado a conocer algunos aspectos relevantes de las superficies de ataque en Blockchain y las amenazas más frecuentes que enfrentan estos entornos, no obstante, en los últimos años, múltiples vectores tradicionales han evolucionado hacia formas mucho más complejas, aprovechando la creciente sofisticación de los sistemas Blockchain, la expansión de plataformas DeFi y la interoperabilidad entre redes. Lo anterior sugiere la necesidad de profundizar en cómo han mutado técnica y operativamente los ataques más representativos, adoptando formas emergentes de alto impacto que desafían los mecanismos de defensa convencionales.

Entre los más representativos se encuentran:

Reentradas Encadenadas y Contratos Proxy. La reentrada, inicialmente visible en el ataque a *The DAO*, ha evolucionado hacia estructuras encadenadas que se aprovechan de contratos delegados (proxy). En lugar de una simple llamada recursiva, ahora se utiliza lógica delegada para burlar los controles de estado y ejecutar múltiples operaciones dentro de una misma transacción (Vidal et al., 2024).

Esta evolución revela que no basta con validar el orden lógico de llamadas; se requiere verificación formal del flujo simbólico y simulaciones dinámicas.

Ataques en Puentes Intercadena. Casos como el de Ronin Network reflejan cómo los puentes intercadena pueden ser vulnerados mediante la manipulación de validadores, errores en contratos de verificación cruzada o el compromiso de firmas en nodos clave. Estas estructuras representan uno de los mayores vectores actuales de riesgo económico y técnico (Mejía et al., 2023).

Estos ataques no solo vulneran contratos, sino también mecanismos externos de confianza entre redes, lo cual amplifica su impacto.

Maximal Extractable Value (MEV) y Front-Running Algorítmico. Con el auge de DeFi, los ataques tipo MEV se han convertido en una amenaza latente. Mediante bots especializados, los atacantes reordenan el mempool para ejecutar transacciones antes y después de una víctima, explotando el orden de inclusión y obteniendo ventaja económica (Pandey & Kushwaha, 2025).

Este tipo de explotación no altera la lógica del contrato, pero manipula el entorno operativo donde se ejecutan, introduciendo asimetrías técnicas en un sistema supuestamente equitativo.

Denegación de Servicio Mediante Congestión Económica (Gas Dos). El Gas DoS representa una evolución de los ataques de denegación de servicio clásicos. En lugar de saturar la red con peticiones, el atacante eleva los costos operativos enviando transacciones con altos límites de gas, impidiendo la inclusión de operaciones legítimas en los bloques (Fernández López, 2021).

Este ataque no explota vulnerabilidades de software, sino los propios incentivos económicos del sistema, afectando su disponibilidad funcional.

Manipulación de Oráculos y Falsificación de Precios. Los contratos que dependen de entradas externas han sido explotados a través de la manipulación de oráculos. Casos como bZx o Mango Markets mostraron cómo la falta de verificación cruzada puede ser aprovechada para distorsionar precios y desencadenar ejecuciones arbitrarias (Mejía et al., 2023).

La sofisticación radica en que el atacante no interactúa directamente con el contrato, sino que manipula su entorno de datos, afectando su lógica desde el exterior.

Compromiso de Infraestructura Externa. Ataques como el ocurrido en Mixin Network evidencian que la vulnerabilidad puede no estar en la lógica on-chain, sino en la infraestructura

de soporte: bases de datos en la nube, compiladores, entornos CI/CD o APIs externas. En Curve Finance, una falla en el compilador Vyper permitió un drenaje masivo de fondos (Fernández López, 2021).

Estos ataques exigen ampliar el enfoque defensivo más allá de la lógica on-chain e incluir en el análisis de riesgo toda la arquitectura asociada (CI/CD, claves en servidores, compiladores, APIs).

Subversión del Consenso en Redes Pos. En redes basadas en *Proof of Stake*, algunos validadores han logrado reorganizar bloques mediante colusión o concentración de poder sin ser penalizados. Estos ataques, que alteran la integridad del consenso, se han documentado especialmente en plataformas con bajo número de participantes activos (Hosseini Bamakan & Banaeian Far, 2025).

Estos vectores, aunque silenciosos, ponen en peligro el corazón de la integridad Blockchain: la confianza distribuida en el mecanismo de validación.

Estos ataques no solo representan una progresión técnica, sino una transformación conceptual de los riesgos en Blockchain. Lo que antes se consideraba un sistema seguro por diseño, ahora requiere defensas adaptativas que consideren la interacción entre componentes internos y externos, lógica de negocio, actores automatizados y estructuras de validación descentralizadas. Comprender estos comportamientos emergentes es fundamental para anticiparse a nuevas amenazas y fortalecer la resiliencia de las arquitecturas Blockchain.

Estrategias de Mitigación en Blockchain

Mitigación de Riesgos

La mitigación de riesgos en Blockchain requiere un enfoque integral que combine auditorías de seguridad, optimización de protocolos de consenso y la integración de tecnologías avanzadas como la inteligencia artificial, entre otras estrategias.

Auditorías y Verificación de Código. Las auditorías de seguridad desempeñan un papel crucial en la detección y corrección de vulnerabilidades antes de que sean explotadas. Herramientas como CertiK, OpenZeppelin y MythX permiten analizar contratos inteligentes en busca de errores lógicos y vulnerabilidades de ejecución (Saad et al., 2020).

Mejoras en los Protocolos de Consenso. Los protocolos de consenso han evolucionado para mejorar la seguridad y eficiencia de Blockchain. Algunos avances incluyen la combinación de prueba de trabajo (PoW) y prueba de participación (PoS), lo que permite reducir el consumo energético sin comprometer la seguridad (Pu & Qiao, 2025).

Implementación de Soluciones de Privacidad. Para mitigar los riesgos en la privacidad y el almacenamiento de datos, se han desarrollado soluciones como las pruebas de conocimiento cero (ZKP) (Llamas Covarrubias, 2021).

Inteligencia Artificial para la Detección de Amenazas. La inteligencia artificial (IA) se ha integrado en la seguridad de Blockchain para detectar patrones de comportamiento anómalos y prevenir ataques (Hosseini Bamakan & Banaeian Far, 2025).

Tabla 11

Comparativo de Vulnerabilidades y Estrategias de Mitigación en Blockchain

Vulnerabilidad	Código CVE	Impacto Principal	Estrategia de Mitigación
Reentrada	CVE-2018-10299	Extracción indebida de fondos	Uso del patrón “checks-effects-interactions”; verificación formal con herramientas como MythX o Slither.
Desbordamiento de enteros	CVE-2020-26264	Manipulación de cálculos financieros	Utilizar bibliotecas seguras como SafeMath; pruebas de límites y auditorías automáticas.
Condiciones de carrera	CVE-2022-3298	Ejecución paralela inconsistente	Diseñar lógica de contratos con exclusión mutua; aplicar pruebas concurrentes en entornos simulados.
Ataque Sybil	CVE-2019-6111	Manipulación del consenso	Uso de mecanismos de reputación y validación mediante prueba de identidad (PoI) o mecanismos federados.
Ataque Eclipse	CVE-2021-31684	Aislamiento de nodos legítimos	Aleatoriedad en la selección de pares; inclusión de nodos de confianza y monitoreo activo de la red.
Envenenamiento de red	CVE-2020-28348	Saturación y propagación de datos maliciosos	Aplicar filtros criptográficos en protocolos P2P; supervisión constante con sistemas de detección de anomalías.
Análisis de patrones transaccionales	CVE-2023-18247	Riesgo de deanonimización del usuario	Empleo de técnicas como CoinJoin, zk-SNARKs y firmas de anillo para preservar la privacidad.

Nota. Elaboración propia a partir de Vidal et al. (2024); Mejía et al. (2023); Hosseini Bamakan & Banaeian Far (2025); Pourrahmani et al. (2023).

La identificación de vulnerabilidades en sistemas Blockchain se enfoca en la formulación de estrategias de mitigación orientadas a reducir la superficie de ataque. En la Tabla 11 se relaciona algunas de las vulnerabilidades más relevantes con sus respectivas estrategias de mitigación, considerando la clasificación de CVE (Common Vulnerabilities and Exposures) y recomendaciones derivadas de marcos como NIST y OWASP.

Herramientas para la Detección de Amenazas en Blockchain

El monitoreo de amenazas en sistemas Blockchain requiere tecnologías avanzadas capaces de detectar comportamientos anómalos en tiempo real. Entre estas herramientas se destacan:

Sistemas de Gestión de Información y Eventos de Seguridad (SIEM). Soluciones como Splunk, IBM QRadar o Elastic SIEM permiten el monitoreo y correlación de eventos generados por nodos Blockchain. Estos sistemas facilitan la detección de actividades inusuales, como intentos de bifurcación no autorizada o patrones de transacción atípicos (Mejía et al., 2023).

Redes Neuronales y Machine Learning. La implementación de algoritmos de aprendizaje profundo permite identificar transacciones sospechosas, fraudes o ataques en contratos inteligentes. Se han desarrollado modelos de detección basados en redes LSTM (Long Short-Term Memory) y algoritmos de clasificación para discriminar entre actividades legítimas y maliciosas (Chen et al., 2025). Herramientas como DeepLearning4J o TensorFlow Blockchain Toolkit han sido aplicadas con éxito en análisis predictivos sobre redes descentralizadas.

Frameworks Especializados.

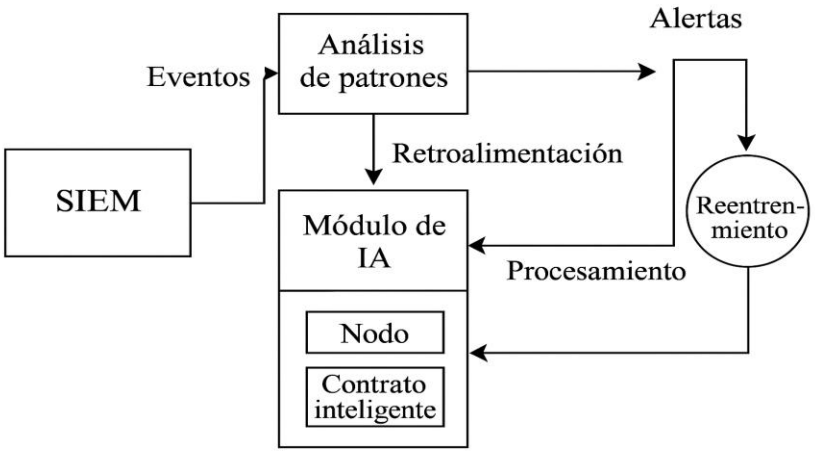
MythX, **Oyente**, **Slither**. Utilizados para escaneo de vulnerabilidades en contratos inteligentes, incluyendo detección de reentradas, errores de gas y condiciones de carrera.

SmartCheck. Herramienta estática que permite encontrar errores comunes en Solidity.

Chainalysis y CipherTrace. Permiten rastreo forense y evaluación de riesgos financieros en transacciones Blockchain.

Figura 9

Arquitectura de Seguridad Integrada con SIEM e IA en Blockchain



Nota. Diagrama técnico que representa SIEM, nodos, contratos y módulos IA colaborando en tiempo real.

La integración de estas herramientas dentro de arquitecturas de seguridad basadas en Zero Trust y marcos como NIST SP 800-207, tal como se muestra en la Figura 9, potencia la protección proactiva frente a amenazas emergentes.

Asimismo, el uso de Blockchain Analytics complementado con IA ofrece una visión integral del comportamiento de la red, reduciendo el tiempo de respuesta ante incidentes.

Aplicación de Inteligencia Artificial en la Detección de Amenazas Blockchain

Frente a la velocidad y variedad de ataques en Blockchain, las técnicas tradicionales de monitoreo resultan insuficientes. Por esta razón, muchas plataformas están integrando módulos de inteligencia artificial (IA) que permiten detectar patrones anómalos, predecir posibles fallos y

responder de forma automatizada a comportamientos maliciosos. Los sistemas de IA pueden ser entrenados para:

Detectar movimientos inusuales de activos en wallets específicas.

Reconocer patrones de ataque antes de que se consoliden.

Analizar código fuente de contratos y generar alertas ante estructuras sospechosas.

Clasificar amenazas por nivel de criticidad y sugerir respuestas inmediatas.

Este enfoque proactivo, aunque poderoso, requiere curación constante de los datos de entrenamiento y supervisión humana para evitar falsos positivos o decisiones desalineadas con los objetivos de negocio.

Mecanismos para Trazabilidad y Recolección de Evidencia Digital

La naturaleza inmutable de Blockchain convierte a esta tecnología en una fuente rica para la recolección de evidencias en investigaciones forenses digitales. Sin embargo, esta trazabilidad puede verse limitada si no existen mecanismos adecuados para asociar eventos on-chain con identidades o acciones específicas del mundo real.

La disciplina conocida como *Blockchain forensics* ha desarrollado herramientas para analizar transacciones, reconstruir caminos de fondos, identificar mezcladores y generar pruebas admisibles en entornos judiciales. Estas herramientas permiten auditar registros de forma transparente y verificar acciones sin posibilidad de alteración.

Es recomendable que las organizaciones adopten estructuras que permitan generar logs interpretables desde sus implementaciones Blockchain, sin comprometer privacidad, pero garantizando trazabilidad operativa y cumplimiento normativo.

Criptografía Poscuántica Aplicada a Blockchain: Necesidad Futura de Adaptación

La amenaza potencial de la computación cuántica sobre los algoritmos criptográficos actuales representa un desafío real para Blockchain. Muchos de los mecanismos de firma digital usados hoy podrían ser vulnerables ante ataques cuánticos, comprometiendo la validez de las transacciones pasadas y futuras.

El desarrollo de algoritmos resistentes a la computación cuántica ha comenzado a ser explorado en redes como Ethereum y Cardano, aunque su implementación masiva aún está en fases preliminares. La preparación ante este escenario debe incluir:

Monitoreo activo del avance de tecnologías cuánticas.

Flexibilidad para reemplazar algoritmos sin perder integridad histórica.

Pruebas piloto con mecanismos híbridos que incluyan firmas resistentes como Lattice, NTRU o hash-based signatures.

Protección de la Identidad Digital en Entornos Descentralizados

La gestión de la identidad digital es un aspecto crítico en Blockchain, donde los usuarios operan mediante claves criptográficas que no siempre están protegidas de forma adecuada. La pérdida, robo o suplantación de claves puede implicar no solo la pérdida de activos, sino también el acceso no autorizado a funciones críticas del sistema. Las estrategias más efectivas en este campo incluyen:

Uso de billeteras multifirma o de custodia compartida.

Aplicación de autenticación multifactor en nodos autorizados.

Registros de actividad asociados a identificadores descentralizados (DID).

Segmentación de privilegios según nivel de autorización y duración de sesiones.

Estas medidas refuerzan la resistencia ante ataques de apropiación de identidad y permiten una trazabilidad funcional sin comprometer el anonimato.

Comparativo entre Estrategias Reactivas y Proactivas en la Mitigación Blockchain

En el contexto de la ciberseguridad aplicada a entornos Blockchain, resulta necesario diferenciar entre enfoques **proactivos**, orientados a la prevención y disuasión de ataques, y enfoques **reactivos**, centrados en la detección, contención y recuperación posterior al incidente. Ambos modelos son complementarios y deben integrarse en el diseño de soluciones robustas. La Tabla 12 presenta un comparativo entre estas dos estrategias, considerando su aplicación práctica en el ciclo de vida de sistemas basados en tecnología Blockchain.

Tabla 12

Comparativo entre Estrategias Reactivas y Proactivas en Blockchain

Enfoque	Características	Ejemplos en Blockchain	Ventajas	Limitaciones
Reactivo	Actúa después del incidente	Rescate de tokens, forks, congelamiento de contratos	Rápida contención	No previene daños previos
Proactivo	Previene y reduce la probabilidad de ataque	Auditorías, verificación formal, monitoreo predictivo	Reduce ocurrencia de incidentes	Alto costo inicial y complejidad técnica

Nota. La tabla compara las estrategias reactivas y proactivas con aplicación en entornos Blockchain organizacionales.

Buenas Prácticas por Capas Técnicas

La implementación segura de soluciones basadas en Blockchain no depende únicamente del uso de criptografía avanzada o de arquitecturas descentralizadas, sino también de la correcta integración de buenas prácticas a lo largo de todas las capas técnicas del sistema. Estas prácticas permiten reducir la superficie de ataque, minimizar vulnerabilidades explotables y mejorar la respuesta ante incidentes.

En la Tabla 13 se consolidan algunos controles y recomendaciones aplicables en diferentes niveles de una arquitectura Blockchain, con el fin de apoyar la gestión técnica y operativa de la seguridad en entornos organizacionales.

Tabla 13

Buenas Prácticas en Seguridad Blockchain por Capa Técnica

Capa	Buenas Prácticas Recomendadas
Contratos inteligentes	Auditoría formal, pruebas unitarias, patrón CEI, revisión por pares
Red P2P	Encriptación de tráfico, listas blancas de nodos, protección anti-DoS
Almacenamiento	Fragmentación, cifrado local, validación de hashes
Consenso	Rotación de validadores, penalización, tolerancia a fallos
Oráculos e integración	Múltiples fuentes, reputación, quorum, contratos de verificación cruzada

Nota. Esta tabla presenta una lista estructurada de controles y acciones recomendadas para cada capa funcional en arquitecturas Blockchain, considerando criterios de evaluación técnica, seguridad operacional y resiliencia criptográfica.

Conclusiones

El análisis de las superficies de ataque en Blockchain muestra que, a pesar de sus ventajas, sigue siendo vulnerable a ataques avanzados. Se han identificado códigos CVE específicos que han afectado la seguridad de contratos inteligentes, nodos y protocolos de consenso. La implementación de auditorías de código, seguridad en nodos y mejoras en los mecanismos de consenso resulta esencial para mitigar estos riesgos.

El análisis de vulnerabilidades en Blockchain demuestra que, si bien esta tecnología ofrece altos niveles de seguridad, aún existen amenazas significativas. La identificación y documentación de estos riesgos permite desarrollar mejores estrategias de mitigación y reforzar la seguridad en implementaciones futuras.

La evolución de las amenazas en entornos Blockchain exige una redefinición permanente de las estrategias de defensa. No basta con aplicar buenas prácticas genéricas: se requiere una comprensión profunda del funcionamiento de la red, sus capas técnicas, vectores de ataque y mecanismos de recuperación.

La incorporación de herramientas avanzadas como redes neuronales y sistemas SIEM en el monitoreo de Blockchain demuestra que la convergencia entre inteligencia artificial y ciberseguridad no solo es posible, sino necesaria para anticiparse a amenazas emergentes. Esta integración permite detectar patrones complejos de ataque y generar alertas en tiempo real, mejorando los tiempos de respuesta en redes distribuidas.

Los marcos de referencia como OWASP Blockchain Top 10, NIST SP 800-183 y MITRE ATT&CK, al ser adaptados específicamente a la lógica funcional de Blockchain, proporcionan un soporte metodológico útil para alinear controles técnicos con objetivos organizacionales, reduciendo la brecha entre la auditoría tradicional y la seguridad en entornos descentralizados.

A pesar de los avances normativos internacionales, persisten vacíos regulatorios que afectan la adopción segura de Blockchain. La ausencia de una armonización legal sobre privacidad, trazabilidad y responsabilidad contractual limita el desarrollo de soluciones interoperables y conformes a normativas de protección de datos como el RGPD o la Ley 1581 en Colombia.

El estudio evidencia que las amenazas más críticas en Blockchain no son únicamente de naturaleza técnica, sino que también surgen de debilidades en la gobernanza, la capacitación del personal y la falta de integración de controles organizativos. Por tanto, la seguridad en Blockchain debe abordarse como un proceso transversal que involucra diseño, implementación, operación y evaluación permanente.

A partir de los hallazgos obtenidos, se identifican líneas futuras de acción orientadas a mejorar la detección de amenazas mediante enfoques automatizados, actualizar marcos regulatorios que acompañen la evolución tecnológica y aplicar buenas prácticas en contextos donde Blockchain se utilice para procesos críticos y de alta disponibilidad.

Recomendaciones

Este apartado presenta una serie de sugerencias prácticas para mejorar la seguridad en los sistemas Blockchain, tomando como base los hallazgos de la investigación, dirigido a investigadores, estudiantes y el público en general interesado en esta tecnología.

Los desarrolladores de contratos inteligentes deben incorporar prácticas de diseño que impidan la repetición no autorizada de operaciones, así como utilizar herramientas que analicen el código de forma automática para identificar posibles fallos antes de su implementación. Esto ayudará a prevenir ataques que aprovechan debilidades en la programación.

Es aconsejable que las organizaciones que emplean redes Blockchain establezcan mecanismos para verificar la identidad de los participantes y monitoreen constantemente la salud de los nodos. De esta manera, se reduce el riesgo de que actores malintencionados tomen control de la red o aíslen a otros participantes legítimos.

Se recomienda a los usuarios y administradores de sistemas Blockchain proteger de forma robusta las claves privadas, que son como la "llave" de acceso a los activos digitales. Implementar métodos de autenticación adicionales y guardar estas claves en dispositivos seguros puede prevenir robos significativos.

Los responsables de proyectos Blockchain deberían considerar que las fuentes de información externas, conocidas como oráculos, pueden ser manipuladas. Por ello, se aconseja utilizar múltiples fuentes para verificar los datos y establecer sistemas de reputación que aseguren la veracidad de la información que entra a la cadena de bloques.

Las organizaciones que implementan Blockchain, deberían establecer una valoración continua de los riesgos que persisten incluso después de aplicar las medidas de seguridad

iniciales. Esto implica identificar las vulnerabilidades que aún podrían ser explotadas y destinar recursos para fortalecer esas áreas.

En el contexto de las redes Blockchain empresariales, se considera beneficioso definir claramente los roles y responsabilidades del personal técnico involucrado en la gestión del sistema. Esto incluye establecer procesos para la aprobación de cambios en los contratos, la gestión de actualizaciones y la forma de actuar ante posibles incidentes de seguridad.

Se propone a los equipos de desarrollo integrar Inteligencia Artificial en los sistemas de monitoreo de Blockchain, para detectar patrones de comportamiento inusuales y alertar sobre posibles amenazas en tiempo real, mejorando la capacidad de respuesta ante ataques.

Para garantizar la capacidad de investigar incidentes de seguridad, se aconseja a las implementaciones de Blockchain que generen registros detallados de actividad. Estos registros, combinados con herramientas de análisis forense, facilitarán la reconstrucción de eventos y la recolección de pruebas digitales sin comprometer la privacidad.

Referencias

Ali, A. (2022, diciembre 31). *CFG Analysis for Detecting Vulnerabilities in Smart Contracts (2022) | Abdelrahman Ali | 1 Citations*. https://scispace.com/papers/cfg-analysis-for-detecting-vulnerabilities-in-smart-27l4qevy

Belenkov, N., Callens, V., Murashkin, A., Bak, K., Derka, M., Gorzny, J., & Lee, S.-S. (2025, enero 6). *SoK: A Review of Cross-Chain Bridge Hacks in 2023*. SciSpace - Paper; Cornell University. https://doi.org/10.48550/arxiv.2501.03423

Bhattacharjya. (2022). A Holistic Study on the Use of Blockchain Technology in CPS and IoT Architectures Maintaining the CIA Triad in Data Communication. *International Journal of Applied Mathematics and Computer Science*, *32*, 403-413. https://doi.org/10.34768/amcs-2022-0029

Bhudia, A., Cartwright, A., Cartwright, E., Hernandez Castro, J. C., & Hurley Smith, D. (2022). Extortion of a Staking Pool in a Proof-of-Stake Consensus Mechanism. *SciSpace - Paper*, 1-6. https://doi.org/10.1109/COINS54846.2022.9854946

Chen, Z., Zhu, L., Jiang, P., He, J., & Zhang, Z. (2025). Tackling Data Mining Risks: A Tripartite Covert Channel Merging Blockchain and IPFS. *IEEE Transactions on Network Science and Engineering*. Scopus. https://doi.org/10.1109/TNSE.2025.3539909

Cheng, J., Xie, L., Tang, X., Tang, X., Xiong, N., & Liu, B. (2021). A survey of security threats and defense on Blockchain. *Multimedia Tools and Applications*, *80*(20), 30623-30652. https://doi.org/10.1007/S11042-020-09368-6

Díaz, J. M. (2019). Risks and vulnerabilities of the denial of service distributed on the internet of things. *Revista de Bioetica y Derecho*, *46*, 85-100. Scopus. https://doi.org/10.1344/rbd2019.0.27068

Ding, S., Hu, H., Xu, F., Chai, Z., & Wang, W. (2024). Blockchain-based security-minded information-sharing in precast construction supply chain management with scalability, efficiency and privacy improvements. *Automation in Construction*, *168*, 105698. https://doi.org/10.1016/j.autcon.2024.105698

Fernández López, R. I. (2021). EL DERECHO TRIBUTARIO ANTE UNA NUEVA REALIDAD VIRTUAL: LA TECNOLOGÍA BLOCKCHAIN APLICADA A LOS CONTRATOS INTELIGENTES. *Revista Técnica Tributaria*, *132*, 17-55. https://doi.org/10.48297/rtt.v1i132.613

Han, X., Zhang, D., Huang, Z., Yao, S., & Wu, Z. (2022). Revocable One-Time Ring Signature from Pairings. *Wireless Communications and Mobile Computing*, *2022*, 1-14. https://doi.org/10.1155/2022/8021267

He, L., Zhang, X., Huo, B., & Zhang, Y. (2025). Platform pricing and blockchain adoption for capacity sharing with cross-network externality and supply risk. *Annals of Operations Research*, *344*(2), 793-823. Scopus. https://doi.org/10.1007/s10479-024-05850-8

Hosseini Bamakan, S. M., & Banaeian Far, S. (2025). Distributed and trustworthy digital twin platform based on blockchain and Web3 technologies. *Cyber Security and Applications*, *3*. Scopus. https://doi.org/10.1016/j.csa.2024.100064

Huang, K. (2023). The C.I.A Properties of Web3 System. *Future of Business and Finance*, 3-29. https://doi.org/10.1007/978-3-031-39288-7_1

Ibáñez Jiménez, J. W. (2018). *Blockchain: Primeras cuestiones en el ordenamiento español.* Dykinson. https://research.ebsco.com/linkprocessor/plink?id=6d0fc4a6-4cb8-33e9-ba24-867b1caaef04

Kouki, F., Mengash, H. A., Alruwais, N., Miled, A. B., Aljabri, J., & Salama, A. S. (2025). IMPROVING FRACTALS FINANCIAL CREDIT RISK EVALUATION BASED ON DEEP LEARNING TECHNIQUES AND BLOCKCHAIN-BASED ENCRYPTION. *Fractals*. Scopus. https://doi.org/10.1142/S0218348X2540033X

Legerén-Molina, A. (2019). Legal challenges about blockchain. *Revista de Derecho Civil*, *6*(1), 177-237. Scopus.

Liao, Z., Nan, Y., Liang, H., Sun, H., Zhai, J., Wu, J., & Zheng, Z. (2024, junio 22). *SmartAxe: Detecting Cross-Chain Vulnerabilities in Bridge Smart Contracts via Fine-Grained Static Analysis*. SciSpace - Paper; Cornell University. https://doi.org/10.1145/3643738

Llamas Covarrubias, J. Z. (2021). TRANSPARENCY AND PROTECTION OF PERSONAL DATA IN THE BLOCKCHAIN. *Estudios en Derecho a la Informacion*, *2021*(11), 27-63. Scopus. https://doi.org/10.22201/iij.25940082e.2021.11.15299

Lotfi, R., Rajabzadeh, M., Zamani, A., & Rajabi, M. S. (2025). Viable supply chain with vendor-managed inventory approach by considering blockchain, risk and robustness. *Annals of Operations Research*, *344*(2), 575-594. Scopus. https://doi.org/10.1007/s10479-022-05119-y

Mejía, J. C. G., Zuluaga, J. G., Agudelo, F. A. V., Duran, D. E. S., & Gamboa, A. R. (2023). Blockchain Monitoring with Machine Learning. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2023*(E56), 621-637. Scopus.

Noor, M. A. F., & Mustafa, K. (2024a). A taxonomy of endpoint vulnerabilities and affected blockchain architecture layers. *Concurrency and Computation: Practice and Experience*, *36*(19). Scopus. https://doi.org/10.1002/cpe.8158

Noor, M. A. F., & Mustafa, K. (2024b). Mitigating Blockchain Endpoint Vulnerabilities: Conceptual Frameworks. *International Journal of Computer Networks and Applications*, *11*(6), 933-953. Scopus. https://doi.org/10.22247/ijcna/2024/56

Nzuva, S. M. (2024). Revisiting Blockchain Technologies and Smart Contracts Security: A Pragmatic Exploration of Vulnerabilities, Threats, and Challenges. *Asian Journal of Research in Computer Science*, *17*(7), 11-30. https://doi.org/10.9734/ajrcos/2024/v17i7474

Padilla Sánchez, J. A. (2020). Blockchain y contratos inteligentes: Aproximación a sus problemáticas y retos jurídicos. *Revista de Derecho Privado*, *39*, 175-201. https://doi.org/10.18601/01234366.n39.08

Pandey, V., & Kushwaha, G. S. (2025). From risk minimisation to trust building: An empirical study on blockchain technology in digital payment system. *Journal of Modelling in Management*. Scopus. https://doi.org/10.1108/JM2-03-2024-0080

Pourrahmani, H., Yavarinasab, A., Monazzah, A. M. H., & Van herle, J. (2023). A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain. *Internet of Things*, *23*, 100888. https://doi.org/10.1016/j.iot.2023.100888

Pu, G., & Qiao, W. (2025). Relational risk, knowledge sharing and supply chain resilience: The complementary role of blockchain governance and relational governance. *Journal of Knowledge Management*, *29*(2), 301-341. Scopus. https://doi.org/10.1108/JKM-12-2023-1244

Rosa, B. M. G., Anastasova, S., & Yang, G. Z. (2023). NFC-Powered Implantable Device for On-Body Parameters Monitoring With Secure Data Exchange Link to a Medical

Blockchain Type of Network. *IEEE Transactions on Cybernetics*, *53*(1), 31-43. Scopus. https://doi.org/10.1109/TCYB.2021.3088711

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C. A., Nyang, D. H., & Mohaisen, A. (2019). Overview of attack surfaces in blockchain. En *Blockchain for Distributed Systems Security* (pp. 51-65). Scopus. https://doi.org/10.1002/9781119519621.ch3

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, D. (2020). Exploring the Attack Surface of Blockchain: A Comprehensive Survey. *IEEE Communications Surveys and Tutorials*, *22*(3), 1977-2008. Scopus. https://doi.org/10.1109/COMST.2020.2975999

Santoso, I., & Christyono, Y. (2023). Zk-SNARKs As A Cryptographic Solution For Data Privacy And Security In The Digital Era. *International Journal of Mechanical Computational and Manufacturing Research*, *12*(2), 53-58. https://doi.org/10.35335/computational.v12i2.122

Sus, V. (2022). Proof-of-Stake Is a Defective Mechanism. *Social Science Research Network*, *2022*, 409-409. https://doi.org/10.2139/ssrn.4067739

Vidal, F. R., Ivaki, N., & Laranjeiro, N. (2024). Vulnerability detection techniques for smart contracts: A systematic literature review. *Journal of Systems and Software*, *217*, 112160. https://doi.org/10.1016/j.jss.2024.112160

Zalte, S., Bhatia, H., Deshmukh, R., Gupta, N., & Kamat, R. (2023). Overview of attack surfaces in blockchain. En *Blockchain Applications in Cybersecurity Solutions* (pp. 62-80). Scopus. https://doi.org/10.2174/9789815080599123010007