REVISTA UGC | Revista científica de la Universidad del Golfo de California
Volumen 3 | S 3 | Octubre - 2025

SISTEMAS DE ALMACENAMIENTO DISTRIBUIDO BASADOS EN BLOCKCHAIN PARA SEGURIDAD DE DATOS EN INFRAESTRUCTURAS CLOUD CRÍTICAS

BLOCKCHAIN-BASED DISTRIBUTED STORAGE SYSTEMS FOR DATA SECURITY IN CRITICAL CLOUD INFRASTRUCTURES: INTEGRITY VERIFICATION MECHANISMS AND SCALABILITY TECHNIQUES ANALYSIS

Cinthia Aracely Sañudo-Alvarado[1]
E-mail: csanudo@istvr.edu.ec
ORCID: https://orcid.org/0009-0008-6354-313X
Diego Armando Choez-Chancay[1]
E-mail: dchoez@istvr.edu.ec
ORCID: https://orcid.org/0009-0003-2825-415X
José Luis Bonilla-Lastra[1]
E-mail: jbonilla@istvr.edu.ec
ORCID: https://orcid.org/0000-0002-1822-7778
Edison Andrés Rodríguez-Sares[1]
E-mail: erodriguez@istvr.edu.ec
ORCID: https://orcid.org/0000-0003-2182-4431
Diana Carolina Decimavilla-Alarcón[1]
E-mail: ddecimavilla@istvr.edu.ec
ORCID: https://orcid.org/0000-0002-0375-0216
[1] Instituto Superior Tecnológico Vicente Rocafuerte. Ecuador.

Cita sugerida (APA, séptima edición)

Sañudo-Alvarado, C. A., Choez-Chancay, D. A., Bonilla-Lastra, J. L., Rodríguez-Sares, E. Á., & Decimavilla-Alarcón, D. C. (2025). Sistemas de almacenamiento distribuido basados en blockchain para seguridad de datos en infraestructuras cloud críticas. *Revista UGC, 3(S3), 149-164.*

Fecha de presentación: 15/07/2025 **Fecha de aceptación:** 06/09/2025 **Fecha de publicación:** 01/10/2025

RESUMEN

La presente investigación descriptiva-correlacional caracteriza los mecanismos de verificación de integridad implementados en sistemas de almacenamiento distribuido basados en blockchain para infraestructuras críticas y analiza las técnicas de escalabilidad aplicadas en estos contextos operacionales. El estudio emplea metodología de síntesis sistemática de literatura especializada, analizando 28 fuentes que documentan implementaciones reales en sectores críticos durante períodos operacionales de 12 meses. Los hallazgos revelan que existe compensación fundamental entre complejidad criptográfica de algoritmos de consenso y eficiencia operacional del sistema, donde mecanismos de prueba de participación híbrida representan el enfoque más adoptado mientras que sistemas con Entornos de Ejecución Confiables demuestran rendimiento superior. Las técnicas de fragmentación muestran efectividad significativa para escalabilidad horizontal, con correlaciones robustas entre optimizaciones de hardware especializado y reducción de sobrecarga computacional. La investigación establece marcos conceptuales para decisiones arquitectónicas informadas en infraestructuras críticas, proporcionando fundamento empírico para selección de tecnologías blockchain basándose en requisitos específicos de rendimiento, seguridad y disponibilidad operacional.

Palabras clave:

Almacenamiento distribuido, blockchain, verificación de integridad, infraestructuras críticas, escalabilidad, consenso distribuido.

ABSTRACT

This descriptive-correlational research characterizes integrity verification mechanisms implemented in blockchain-based distributed storage systems for critical infrastructures and analyzes scalability techniques applied in these operational contexts. The study employs systematic literature synthesis methodology, analyzing 28 specialized sources documenting real implementations in critical sectors during 12-month operational periods. Findings reveal fundamental trade-offs between cryptographic complexity of consensus algorithms and system operational efficiency, where Hybrid Proof of Stake mechanisms represent the most adopted approach while systems with Trusted Execution Environments demonstrate superior performance. Sharding techniques show significant effectiveness for horizontal

scalability, with robust correlations between specialized hardware optimizations and computational overhead reduction. The research establishes conceptual frameworks for informed architectural decisions in critical infrastructures, providing empirical foundation for blockchain technology selection based on specific requirements for performance, security, and operational availability. Results contribute theoretical understanding of distributed systems while offering practical guidance for technology architects, system administrators, and organizational decision-makers responsible for critical infrastructure implementations requiring high integrity guarantees and operational resilience.

Keywords:

Distributed storage, blockchain, integrity verification, critical infrastructures, scalability, distributed consensus.

INTRODUCCIÓN

La gestión de datos en infraestructuras tecnológicas críticas enfrenta desafíos fundamentales que trascienden las capacidades de los sistemas de almacenamiento tradicionales, constituyendo una situación problemática general que demanda soluciones tecnológicas que garanticen simultáneamente integridad, disponibilidad y resistencia a manipulaciones maliciosas en entornos donde la falla operacional tiene consecuencias críticas (Khalid et al., 2023), las organizaciones que operan infraestructuras en la nube críticas, incluyendo sectores financieros, sanitarios y de servicios esenciales, requieren sistemas de almacenamiento que mantengan la confiabilidad operacional mientras procesan volúmenes masivos de información sensible bajo condiciones de alta demanda y potenciales amenazas de seguridad (Liu, 2023).

Esta necesidad ha revelado las limitaciones estructurales de arquitecturas centralizadas, particularmente su vulnerabilidad inherente a puntos únicos de falla, dependencia de autoridades centralizadas para verificación de integridad y susceptibilidad a ataques dirigidos que pueden comprometer la totalidad del sistema de almacenamiento (Alhazmi et al., 2022), en consecuencia, los sistemas de almacenamiento distribuido emergen como una respuesta arquitectónica a estas limitaciones, distribuyendo datos y responsabilidades de verificación a través de múltiples nodos independientes para crear infraestructuras inherentemente más resilientes, sin embargo, la implementación efectiva de estos sistemas en contextos críticos requiere comprensión profunda de cómo diferentes mecanismos técnicos interactúan para influir en variables operacionales fundamentales como latencia de acceso, rendimiento sostenido y sobrecarga de verificación (Sasikumar et al., 2023). La tecnología blockchain proporciona el marco criptográfico y de consenso necesario para implementar verificación de integridad distribuida, pero su aplicación práctica en infraestructuras críticas presenta compensaciones complejas entre garantías de seguridad y rendimiento operacional que requieren caracterización sistemática.

La contextualización específica del fenómeno tecnológico revela que los sistemas de almacenamiento distribuido basados en blockchain constituyen una evolución tecnológica que redefine fundamentalmente cómo las infraestructuras críticas gestionan, verifican y protegen datos esenciales para operaciones continuas, estos sistemas implementan arquitecturas donde la verificación de integridad de datos ocurre mediante mecanismos de consenso criptográfico distribuidos entre múltiples nodos independientes, eliminando la dependencia en autoridades centralizadas de confianza mientras mantienen consistencia global de datos (Zhang & Datta, 2023), la característica definitoria de estos sistemas radica en su capacidad para garantizar inmutabilidad de datos mediante protocolos de verificación distribuida, donde cada operación de almacenamiento debe ser validada criptográficamente por una mayoría de participantes en la red antes de ser registrada permanentemente en el registro distribuido (Berger et al., 2023).

En el contexto específico de infraestructuras en la nube críticas, estos sistemas deben satisfacer requisitos operacionales estrictos que incluyen latencia predecible para acceso a datos, rendimiento sostenido bajo condiciones de carga variables, disponibilidad continua sin interrupciones planificadas y capacidad de recuperación automática ante fallos de componentes individuales (Xu et al., 2021), lo que implica qué, la implementación exitosa requiera que los mecanismos de verificación de integridad blockchain operen eficientemente sin introducir latencia inaceptable u sobrecarga de recursos que pudiera comprometer las demandas de rendimiento en tiempo real de aplicaciones críticas (Gai et al., 2022), esta tensión fundamental entre las garantías robustas de seguridad proporcionadas por los mecanismos de consenso blockchain y los requisitos estrictos de rendimiento de las operaciones de infraestructura crítica constituye el núcleo del fenómeno tecnológico que requiere caracterización sistemática.

La identificación progresiva de aspectos específicos del fenómeno que requieren mejor comprensión revela múltiples dimensiones técnicas de los sistemas de almacenamiento distribuido basados en blockchain que permanecen insuficientemente caracterizadas para su aplicación efectiva en infraestructuras críticas, los mecanismos de verificación de integridad implementados presentan considerable diversidad técnica, abarcando desde protocolos de consenso tradicionales como prueba de trabajo hasta enfoques especializados como prueba de recuperabilidad y mecanismos de consenso híbridos, cada uno con características operacionales distintas que impactan de manera diferente el rendimiento del sistema bajo las restricciones de infraestructura crítica (Zhou et al., 2022), esta variabilidad en enfoques técnicos y sus correspondientes características operacionales permanece

incompletamente documentada, particularmente respecto a su comportamiento en entornos de producción donde las aplicaciones críticas imponen requisitos estrictos de rendimiento.

Las técnicas de escalabilidad empleadas para optimizar el rendimiento de estos sistemas demuestran compensaciones complejas que afectan simultáneamente la seguridad criptográfica y la eficiencia operacional del sistema global, mientras que estrategias como fragmentación dinámica, protocolos de consenso en capas y optimizaciones a nivel de protocolo exhiben variaciones significativas en efectividad dependiendo de contextos específicos de implementación y los requisitos operacionales particulares de cada despliegue de infraestructura crítica (Dhulavvagol et al., 2023), la comprensión actual de cómo estas técnicas correlacionan con métricas específicas de rendimiento en sistemas operacionales permanece fragmentada, obstaculizando la toma de decisiones informadas para arquitectos de infraestructura responsables de desplegar estos sistemas en contextos críticos (Taher et al., 2024).

La interacción entre diferentes componentes arquitectónicos de estos sistemas, incluyendo capas de comunicación de red, implementaciones de protocolos de consenso y mecanismos de almacenamiento distribuido, genera patrones de comportamiento complejos que influyen directamente en la viabilidad operacional para aplicaciones críticas, donde estos patrones de interacción y sus efectos en variables operacionales clave como latencia de verificación, rendimiento sostenido y utilización de recursos bajo condiciones de carga variables requieren análisis sistemático para informar decisiones arquitectónicas apropiadas en contextos de infraestructura crítica (Xie et al., 2025).

La revisión de estudios previos que han abordado aspectos relacionados revela que los estudios existentes han implementado blockchain en sistemas de almacenamiento desde perspectivas diversas, estableciendo fundamentos técnicos importantes mientras revelan vacíos significativos en la comprensión integral del fenómeno operacional, Chen et al. (2022) desarrollaron un esquema de auditoría pública descentralizada que utiliza tecnología blockchain para eliminar la dependencia en auditores terceros, demostrando viabilidad técnica de verificación distribuida pero sin caracterizar comprehensivamente el impacto en rendimiento operacional bajo condiciones de carga de infraestructura crítica, donde el trabajo documentó implementación exitosa de auditoría basada en blockchain, pero limitó el análisis a validación de seguridad sin explorar correlaciones comprehensivas con variables de escalabilidad.

Por otro lado, Duan et al. (2022), propusieron un marco de protección de integridad para computación en el borde que integra mecanismos de verificación blockchain, enfocándose principalmente en prueba de seguridad y validación experimental, pero sin exploración comprehensiva de correlaciones con variables de escalabilidad operacional, mientras que Feng et al. (2023); y Zhang & Datta (2023) han explorado esquemas de encriptación basada en atributos combinados con blockchain para compartir datos de manera segura, proporcionando conocimientos valiosos sobre mecanismos criptográficos pero concentrándose principalmente en aspectos de privacidad más que en caracterización comprehensiva de comportamiento operacional en infraestructuras críticas.

La investigación más reciente por Guo et al. (2022) respecto a implementación de FileDAG y Sharma & Kaur (2023) abordando escenarios multi-inquilino ha comenzado a plantear desafíos de escalabilidad mediante técnicas como de duplicación a nivel de archivo y arquitecturas multi-inquilino a prueba de manipulación, respectivamente, cuyos hallazgos sugieren considerable variabilidad en rendimiento dependiendo de configuración específica del sistema y características de carga de trabajo, pero estos estudios han empleado principalmente enfoques experimentales que podrían no reflejar completamente realidades operacionales de entornos de infraestructura crítica en producción, de manera similar, estudios longitudinales por Gousteris et al. (2023); y Khalid et al. (2023) han proporcionado revisiones comprehensivas de redes de almacenamiento basadas en blockchain e implementaciones de almacenamiento distribuido seguro en la nube, respectivamente, estableciendo fundamentos taxonómicos importantes para comprender diferentes enfoques técnicos pero con enfoque limitado en caracterización sistemática de patrones de comportamiento operacional específicos para contextos de infraestructura crítica.

El vacío de conocimiento claramente articulado evidencia que, a pesar de los avances documentados en la literatura especializada, persiste un vacío fundamental en la comprensión sistemática de cómo los diferentes mecanismos de verificación de integridad implementados mediante tecnología blockchain en sistemas de almacenamiento distribuido correlacionan específicamente con variables críticas de rendimiento operacional en contextos reales de infraestructuras críticas, los estudios existentes típicamente abordan estos aspectos técnicos, enfocándose en caracterización detallada de mecanismos de verificación específicos o evaluando rendimiento bajo condiciones experimentales controladas, pero raramente combinando ambos enfoques de manera integrada para proporcionar comprensión comprehensiva del fenómeno operacional completo.

Los objetivos de investigación están orientados por un lado hacia caracterización de los mecanismos de verificación de integridad de datos implementados mediante tecnología blockchain en sistemas de almacenamiento distribuido, identificando sus características técnicas fundamentales, patrones de implementación prevalentes, variables operacionales específicas que determinan su

comportamiento y taxonomías de enfoques técnicos empleados en infraestructuras críticas para garantizar integridad de datos mientras mantienen requisitos de rendimiento operacional. El segundo objetivo específico busca analizar las técnicas de escalabilidad y optimización de rendimiento en sistemas de consenso blockchain aplicados a infraestructuras de almacenamiento distribuido críticas, examinando sistemáticamente las correlaciones entre diferentes enfoques técnicos y métricas específicas de rendimiento operacional, identificando patrones de comportamiento bajo condiciones de carga variables, y caracterizando compensaciones entre optimizaciones de escalabilidad y confiabilidad del sistema en contextos operacionales críticos.

La justificación de la relevancia establece que la comprensión profunda de estos sistemas tecnológicos constituye una contribución fundamental para el avance tanto del entendimiento teórico como de la implementación práctica de tecnologías de infraestructura distribuida en contextos críticos, desde una perspectiva teórica, la caracterización sistemática de mecanismos de verificación y técnicas de escalabilidad contribuye al desarrollo de marcos conceptuales robustos para diseñar infraestructuras descentralizadas resilientes que pueden operar efectivamente bajo restricciones operacionales críticas (Gousteris et al., 2023), esta contribución teórica facilita la evolución de principios de diseño que pueden ser aplicados a través de diversas aplicaciones de dominio que requieren simultáneamente garantías de alta integridad y requisitos estrictos de rendimiento.

De manera similar, desde una perspectiva práctica, profesionales responsables de diseñar, implementar y mantener sistemas de infraestructura crítica requieren comprensión basada en evidencia de cómo diferentes enfoques técnicos impactan el rendimiento operacional para tomar decisiones arquitectónicas informadas que equilibren requisitos de seguridad con necesidades de eficiencia operacional (Liu et al., 2023); mientras que organizaciones que invierten en soluciones de almacenamiento basadas en blockchain necesitan conocimiento comprehensivo de compensaciones entre garantías de seguridad y rendimiento operacional para optimizar inversiones de infraestructura mientras aseguran cumplimiento con requisitos operacionales críticos que no pueden ser comprometidos.

La relevancia de esta investigación se extiende más allá de aplicaciones técnicas inmediatas, contribuyendo al entendimiento más amplio de cómo tecnologías distribuidas emergentes pueden ser efectivamente desplegadas en contextos donde falla operacional o degradación de rendimiento tiene implicaciones significativas operacionales, económicas y de seguridad, donde los conocimientos derivados de esta caracterización sistemática pueden informar decisiones de política basadas en evidencia, desarrollo de estándares de industria y decisiones estratégicas de inversión en tecnologías de infraestructura distribuida, facilitando finalmente adopción más amplia de soluciones descentralizadas robustas para aplicaciones críticas que tradicionalmente han dependido de arquitecturas centralizadas con sus limitaciones inherentes de vulnerabilidad.

Los fundamentos conceptuales y teóricos que enmarcan el fenómeno tecnológico de sistemas de almacenamiento distribuido basados en blockchain se construyen sobre la convergencia de múltiples disciplinas tecnológicas que incluyen criptografía aplicada, sistemas distribuidos, teoría de consenso, y arquitecturas de infraestructura crítica, la base conceptual fundamental establece que estos sistemas representan una evolución paradigmática desde arquitecturas centralizadas hacia modelos distribuidos donde la confianza se establece mediante mecanismos criptográficos y protocolos de consenso más que a través de autoridades centralizadas (Khalid et al., 2023). La teoría de sistemas distribuidos proporciona el marco fundamental para comprender cómo múltiples nodos independientes pueden mantener consistencia de datos y coordinar operaciones sin depender de un controlador central, mientras que la criptografía aplicada establece los principios matemáticos que garantizan integridad, autenticidad e inmutabilidad de datos almacenados a través de la red distribuida (Zhang et al., 2022).

Los fundamentos teóricos incorporan además principios de tolerancia a fallas bizantinas, que abordan específicamente el desafío de mantener operación correcta del sistema incluso cuando algunos nodos participantes se comportan de manera maliciosa o experimentan fallos arbitrarios, estableciendo límites teóricos para el número de nodos maliciosos que el sistema puede tolerar mientras mantiene propiedades de corrección y vivacidad (Berger et al., 2023), esta base teórica se complementa con principios de teoría de juegos aplicados a sistemas de incentivos distribuidos, donde los mecanismos de consenso deben diseñarse para alinear incentivos individuales de participantes con objetivos colectivos de mantenimiento de integridad y disponibilidad del sistema, creando marcos económicos que fomenten participación honesta mientras penalizan comportamiento malicioso (Gai et al., 2022).

Las taxonomías, clasificaciones y marcos existentes para entender el área de estudio revelan una estructura conceptual compleja que categoriza diferentes enfoques técnicos basados en múltiples dimensiones de características operacionales y arquitectónicas. La taxonomía fundamental de protocolos de consenso blockchain distingue entre enfoques basados en pruebas, basados en votación, y mecanismos híbridos, donde protocolos basados en pruebas como Prueba de Trabajo y Prueba de Participación requieren que los participantes demuestren cierta forma de compromiso o inversión antes de poder participar en el proceso de consenso, mientras que protocolos basados en votación como tolerancia práctica a

fallas bizantinas dependen de comunicación explícita y votación entre participantes conocidos para lograr acuerdo sobre estado del sistema (Zhou et al., 2022).

Los marcos de clasificación arquitectónica categorizan estos sistemas basándose en topología de distribución, distinguiendo entre redes completamente distribuidas donde todos los nodos tienen igual autoridad, estructuras jerárquicas con diferentes niveles de responsabilidad y arquitecturas híbridas que combinan elementos de ambos enfoques para optimizar características operacionales específicas (Xu et al., 2021); así mismo, los marcos de clasificación para mecanismos de verificación de integridad establecen distinciones entre enfoques basados en resúmenes criptográficos, estructuras de árboles merkle, firmas digitales y sistemas de prueba especializados como pruebas de conocimiento cero, donde cada enfoque proporciona diferentes compensaciones entre sobrecarga computacional, latencia de verificación y garantías de seguridad (Duan et al., 2022).

Paralelamente, los marcos de escalabilidad distinguen entre soluciones de escalamiento en cadena que intentan mejorar rendimiento del protocolo blockchain principal mismo y enfoques de escalamiento fuera de cadena que mueven ciertas operaciones fuera de la cadena principal mientras mantienen garantías de seguridad mediante liquidación periódica o mecanismos de desafío, creando taxonomías que ayudan a comprender diferentes estrategias para abordar limitaciones de rendimiento inherentes en arquitecturas blockchain tradicionales (Dhulavvagol et al., 2023).

La revisión de variables, factores y dimensiones que la literatura identifica como relevantes establece un conjunto comprehensivo de métricas operacionales y características técnicas que determinan el comportamiento y rendimiento de estos sistemas en contextos operacionales reales, las variables de rendimiento fundamentales incluyen rendimiento transaccional medido en transacciones por segundo, latencia de confirmación representando el tiempo requerido para que una transacción sea considerada final e inmutable y métricas de utilización de recursos incluyendo sobrecarga computacional, consumo de memoria, requisitos de ancho de banda de red y patrones de consumo de energía que colectivamente determinan la eficiencia operacional del sistema (Taher et al., 2024), en el mismo sentido, las variables relacionadas con seguridad abarcan fortaleza criptográfica de mecanismos de verificación, resistencia a varios vectores de ataque incluyendo ataques del 51%, problemas de nada en juego, y ataques de largo alcance, así como garantías de disponibilidad bajo diferentes escenarios de falla incluyendo particiones de red, fallos de nodos, y ataques maliciosos coordinados (Sasikumar et al., 2023).

Las dimensiones de escalabilidad incluyen escalabilidad horizontal refiriéndose a la capacidad del sistema para mantener rendimiento conforme el número de nodos participantes aumenta, escalabilidad vertical abordando rendimiento bajo volúmenes de transacciones crecientes, y escalabilidad geográfica examinando rendimiento a través de despliegues distribuidos geográficamente con características variables de latencia y confiabilidad de red (Alshahrani et al., 2023). De manera similar, las variables de usabilidad y complejidad operacional incluyen complejidad de despliegue, flexibilidad de configuración, capacidades de monitoreo y requisitos de mantenimiento que colectivamente determinan la viabilidad práctica de implementar estos sistemas en contextos de infraestructura crítica del mundo real donde simplicidad operacional y confiabilidad son consideraciones primordiales (Liu et al., 2023), además, las variables económicas abarcan estructuras de costos asociadas con diferentes mecanismos de consenso, mecanismos de alineación de incentivos que aseguran participación continua de nodos de red y modelos de sostenibilidad económica que determinan viabilidad a largo plazo de redes distribuidas sin depender de financiamiento centralizado o mecanismos de control.

Los modelos conceptuales y teóricos que explican relaciones entre variables en el dominio establecen marcos comprehensivos para entender interacciones complejas entre diferentes componentes del sistema y sus efectos combinados en comportamiento general del sistema, el modelo fundamental de compensaciones en sistemas distribuidos establece tensiones inherentes entre consistencia, disponibilidad y tolerancia a particiones conocidas como teorema CAP, donde sistemas de almacenamiento distribuido deben navegar estas compensaciones para lograr equilibrio óptimo entre garantías de consistencia fuerte y alta disponibilidad bajo escenarios de partición de red (Chen et al., 2022), los modelos de caracterización de rendimiento establecen relaciones entre parámetros de mecanismos de consenso y rendimiento resultante del sistema, donde factores como tamaño de bloque, tiempos de confirmación de bloque, retrasos de propagación de red y número de validadores participantes colectivamente determinan tasas de transacción alcanzables y latencias de confirmación bajo diferentes condiciones operacionales (Guo et al., 2022).

Los modelos de seguridad establecen marcos teóricos para analizar resistencia de diferentes mecanismos de verificación contra varias estrategias de ataque, incorporando análisis de teoría de juegos de incentivos de atacantes y estrategias de defensores para entender condiciones bajo las cuales seguridad del sistema puede mantenerse incluso en presencia de adversarios sofisticados con recursos computacionales o económicos significativos (Zhang & Datta, 2023), en el mismo sentido, los modelos de escalabilidad teórica establecen relaciones matemáticas entre parámetros de diseño del sistema y características de escalabilidad, proporcionando marcos para predecir cómo rendimiento del sistema se degradará o mejorará conforme varios parámetros operacionales

cambien, incluyendo número de participantes, volúmenes de transacciones, distribución geográfica, y condiciones de red (Xie et al., 2025), además, los modelos de sostenibilidad económica establecen marcos teóricos para entender viabilidad a largo plazo de sistemas distribuidos mediante análisis de estructuras de incentivos, distribuciones de costos y condiciones de equilibrio económico que aseguran operación continua sin requerir subsidios externos o mecanismos de control centralizados.

La síntesis de metodologías utilizadas previamente para estudiar fenómenos similares revela patrones consistentes en enfoques de investigación que han demostrado efectividad para caracterizar sistemas distribuidos complejos y entender su comportamiento operacional bajo varias condiciones, por un lado, las metodologías de evaluación experimental predominantes en la literatura incluyen estudios de bancada controlada donde investigadores implementan sistemas prototipo en ambientes de laboratorio con parámetros conocidos para evaluar sistemáticamente rendimiento bajo condiciones controladas, permitiendo aislamiento de variables específicas y medición de sus efectos individuales en comportamiento del sistema (Sharma & Kaur, 2023), los enfoques basados en simulación utilizan modelos matemáticos y simulaciones computacionales para explorar comportamiento del sistema bajo condiciones extremas o rangos de parámetros que serían imprácticos o peligrosos para evaluar en sistemas reales, proporcionando conocimientos sobre límites teóricos y escenarios de peor caso que informan diseño robusto del sistema (Feng et al., 2023).

Las metodologías de estudio de caso examinan despliegues del mundo real de sistemas de almacenamiento basados en blockchain en ambientes de producción, analizando datos operacionales para entender características de rendimiento reales e identificar discrepancias entre predicciones teóricas y resultados prácticos bajo restricciones operacionales reales (Gousteris et al., 2023). Los enfoques de análisis comparativo evalúan sistemáticamente múltiples enfoques técnicos diferentes bajo condiciones similares para identificar ventajas y desventajas relativas de diferentes decisiones de diseño, proporcionando orientación basada en evidencia para arquitectos de sistemas tomando decisiones técnicas (Rahman et al., 2022), así mismo, estudios longitudinales rastrean comportamiento del sistema durante períodos extendidos para entender cómo características de rendimiento evolucionan conforme sistemas maduran, poblaciones de usuarios crecen y condiciones operacionales cambian, proporcionando conocimientos sobre sostenibilidad a largo plazo y patrones de evolución que son críticos para decisiones de planificación estratégica (Alhazmi et al., 2022).

Las metodologías híbridas combinan elementos de múltiples enfoques, utilizando validación experimental para verificar resultados de simulación, análisis de estudio de caso para validar hallazgos experimentales bajo condiciones del mundo real y estudios comparativos para contextualizar rendimiento individual del sistema relativo a alternativas, creando marcos de evaluación comprehensivos que proporcionan bases de evidencia robustas para entender comportamientos complejos del sistema.

El marco conceptual integrador que guiará el análisis e interpretación de hallazgos establece un sistema para organizar e interpretar observaciones empíricas sobre sistemas de almacenamiento distribuido basados en blockchain en contextos de infraestructura crítica, este marco integra fundamentos teóricos de teoría de sistemas distribuidos, principios de seguridad criptográfica, y metodologías de optimización de rendimiento en una estructura analítica coherente que permite caracterización sistemática de comportamiento del sistema e identificación de relaciones entre diferentes decisiones técnicas y características operacionales resultantes. El marco organiza análisis a lo largo de múltiples dimensiones simultáneamente, examinando características técnicas de mecanismos de verificación en términos de sus propiedades criptográficas, requisitos computacionales y garantías de seguridad, mientras correlaciona estas características con métricas de rendimiento observadas bajo diferentes condiciones operacionales (Huang & Yi, 2024).

El marco analítico incorpora factores contextuales específicos para aplicaciones de infraestructura crítica, incluyendo requisitos de cumplimiento regulatorio, restricciones de continuidad operacional, y parámetros de tolerancia al riesgo que influyen en aceptabilidad de diferentes compensaciones técnicas en escenarios de despliegue práctico (Zichichi et al., 2023). El marco establece procedimientos sistemáticos para correlacionar comportamientos observados del sistema con mecanismos técnicos subyacentes, permitiendo identificación de relaciones causales entre decisiones específicas de diseño y características operacionales resultantes que pueden informar toma de decisiones basada en evidencia para futuros despliegues del sistema, este marco conceptual integrado proporciona estructura necesaria para organizar datos empíricos complejos, identificar patrones significativos en comportamiento del sistema, y desarrollar conocimientos procesables que contribuyen tanto para entendimiento teórico como implementación práctica de soluciones de almacenamiento distribuido basadas en blockchain en contextos de infraestructura crítica donde requisitos de confiabilidad, seguridad, y rendimiento convergen para crear ambientes operacionales únicamente desafiantes.

MATERIALES Y MÉTODOS

La justificación del enfoque metodológico seleccionado establece que la metodología adoptada para esta investigación descriptiva-correlacional se fundamenta en la necesidad identificada durante el análisis bibliográfico de caracterizar sistemáticamente mecanismos de

verificación de integridad y analizar correlaciones con variables de rendimiento sin interferir con operaciones críticas de sistemas en producción, el enfoque metodológico combina análisis descriptivo comprehensivo con técnicas correlacionales multivariadas, siguiendo precedentes exitosos establecidos por Chen et al. (2022) en su caracterización de esquemas de auditoría descentralizada; y Zhou et al. (2022) en su análisis de protocolos de consenso con deduplicación, quienes demostraron que metodologías observacionales pueden proporcionar conocimientos valiosos sobre comportamiento de sistemas blockchain sin requerir manipulación experimental que podría comprometer operaciones críticas.

El enfoque metodológico se construye sobre fundamentos establecidos por Khalid et al. (2023); y Liu (2023) quienes han demostrado que la caracterización sistemática de arquitecturas blockchain combinada con análisis correlacional de métricas operacionales puede revelar relaciones significativas entre decisiones de diseño y resultados de rendimiento que informan toma de decisiones basada en evidencia para despliegues de infraestructura crítica. La metodología incorpora elementos de múltiples tradiciones de investigación, integrando técnicas de observación sistemática de investigación en sistemas distribuidos con enfoques de análisis estadístico correlacional establecidos en literatura de evaluación de rendimiento, creando un marco metodológico híbrido que optimiza tanto rigor científico como aplicabilidad práctica para comprender interacciones complejas entre mecanismos técnicos y rendimiento operacional en contextos de infraestructura crítica.

El paradigma y diseño de investigación específico adopta un paradigma post-positivista que reconoce la existencia de patrones observables en el comportamiento de sistemas tecnológicos mientras reconoce que la comprensión completa de sistemas distribuidos complejos requiere múltiples perspectivas y enfoques metodológicos para capturar la complejidad total del fenómeno (Sasikumar et al., 2023). El diseño de investigación implementa un estudio descriptivo-correlacional de corte transversal con elementos longitudinales, donde la componente descriptiva caracteriza sistemáticamente diferentes mecanismos de verificación de integridad y técnicas de escalabilidad implementados en sistemas actualmente desplegados en contextos de infraestructura crítica, mientras que la componente correlacional examina relaciones entre características técnicas de estos mecanismos y métricas de rendimiento observadas bajo condiciones operacionales variables (Taher et al., 2024).

El diseño incorpora elementos de metodología de estudio de casos múltiples según establecido por Gousteris et al. (2023); y Sharma & Kaur (2023), permitiendo análisis comparativo de diferentes enfoques técnicos desplegados en varios contextos de infraestructura crítica para identificar patrones de comportamiento que trascienden detalles específicos de implementación mientras mantienen sensibilidad para factores contextuales que influyen en rendimiento del sistema en diferentes entornos operacionales, la metodología integra análisis sistemático de literatura con recopilación de datos empíricos de sistemas operacionales, siguiendo enfoques empleados exitosamente por Guo et al. (2022); y Xie et al. (2025) quienes demostraron que combinar marcos teóricos con datos de rendimiento del mundo real proporciona comprensión más comprehensiva del comportamiento del sistema que cualquier enfoque usado independientemente.

El diseño de investigación emplea enfoque de métodos mixtos paralelos convergentes donde métricas cuantitativas de rendimiento y características cualitativas del sistema son recopiladas simultáneamente y analizadas independientemente antes de ser integradas durante la fase de interpretación, asegurando que tanto especificaciones técnicas como realidades operacionales sean adecuadamente capturadas en el análisis (Zhang & Datta, 2023).

En cuanto a los criterios de selección requieren que los sistemas muestreados hayan sido desplegados en contextos operacionales de infraestructura crítica durante al menos 12 meses, mantengan métricas de rendimiento documentadas, implementen mecanismos de verificación de integridad claramente definidos y operen bajo restricciones de rendimiento medibles que reflejen requisitos reales de infraestructura crítica (Xu et al., 2021), la estrategia de muestreo asegura representación adecuada de diferentes enfoques de escalabilidad incluyendo implementaciones de fragmentación, protocolos de consenso en capas, técnicas de optimización fuera de cadena y arquitecturas híbridas que combinan múltiples estrategias de escalabilidad para lograr rendimiento óptimo bajo restricciones operacionales específicas, siguiendo taxonomías establecidas por Berger et al. (2023); y Dhulavvagol et al. (2023).

Las fuentes de datos y procedimientos de recopilación adaptados para esta metodología incorporan múltiples fuentes de datos diseñadas para proporcionar caracterización comprehensiva de comportamientos del sistema mientras mantienen consistencia con enfoques establecidos en literatura de investigación de sistemas distribuidos, las fuentes de datos primarios incluyen registros de rendimiento del sistema y datos de monitoreo recopilados de sistemas operacionales de almacenamiento basados en blockchain desplegados en contextos de infraestructura crítica, proporcionando métricas cuantitativas sobre rendimiento de transacciones, latencias de confirmación, patrones de utilización de recursos y características de disponibilidad bajo condiciones operacionales del mundo real (Chen et al., 2022).

La documentación técnica y documentos de especificación del sistema sirven como fuentes de datos secundarios, proporcionando información detallada sobre mecanismos de verificación implementados, protocolos de

consenso, técnicas de escalabilidad y decisiones de diseño arquitectónico que definen comportamiento del sistema, siguiendo enfoques de análisis de documentación empleados exitosamente por Liu et al. (2023); y Zichichi et al. (2023), las entrevistas estructuradas con arquitectos de sistemas y personal operacional responsable de mantener estos sistemas proporcionan conocimientos cualitativos sobre desafíos prácticos, consideraciones operacionales, y factores contextuales que influyen en rendimiento del sistema, pero que pueden no ser capturados únicamente en métricas cuantitativas (Khan et al., 2022).

Los procedimientos de recopilación de datos siguen protocolos sistemáticos diseñados para asegurar consistencia entre diferentes implementaciones de sistema mientras acomodan variaciones en formatos de documentación, capacidades de monitoreo y estructuras organizacionales entre diferentes contextos de infraestructura crítica. Las métricas de rendimiento son recopiladas durante períodos de tiempo consistentes para asegurar comparabilidad, con períodos de agregación de datos diseñados para capturar tanto patrones operacionales normales como respuesta para condiciones excepcionales que prueban resistencia del sistema y características de escalabilidad. El análisis de documentación sigue procedimientos estructurados de análisis de contenido que sistemáticamente extraen y categorizan características técnicas según taxonomías estandarizadas establecidas durante la fase de revisión de literatura, asegurando caracterización consistente entre diferentes implementaciones de sistema independientemente de variaciones en estilos de documentación o enfoques organizacionales para especificación técnica.

Las variables e indicadores alineados con la literatura analizada establecen marco comprehensivo de medición que captura tanto características técnicas de mecanismos de verificación como sus correspondientes implicaciones de rendimiento operacional en contextos de infraestructura crítica, principalmente, las variables independientes incluyen categorías de mecanismos de verificación de integridad caracterizados según taxonomías establecidas por la literatura analizada, incluyendo tipos de protocolos de consenso, enfoques criptográficos empleados, parámetros de frecuencia de verificación y niveles de garantía de seguridad proporcionados por diferentes implementaciones técnicas, mientras qué, las variables dependientes se enfocan en métricas de rendimiento operacional críticas para aplicaciones de infraestructura crítica, incluyendo rendimiento de transacciones medido en transacciones por segundo bajo condiciones de carga sostenida, latencia de confirmación representando tiempo requerido para finalidad de transacción, disponibilidad del sistema medida como porcentaje de tiempo activo bajo varios escenarios de falla y métricas de eficiencia de recursos incluyendo sobrecarga computacional, utilización de memoria y patrones de consumo de ancho de banda de red (Sasikumar et al., 2023).

Así mismo, los procedimientos de análisis metodológicamente coherentes implementan enfoques analíticos sistemáticos diseñados para caracterizar comportamientos del sistema e identificar correlaciones significativas entre características técnicas y resultados de rendimiento operacional, los procedimientos de análisis descriptivo caracterizan distribuciones de enfoques técnicos empleados entre sistemas muestreados, utilizando análisis de frecuencia, agrupamiento categórico, y técnicas de comparación sistemática para identificar patrones prevalentes en decisiones de implementación y sus correspondientes características de rendimiento, en el mismo sentido, el análisis de correlación emplea técnicas estadísticas tanto paramétricas como no paramétricas para examinar relaciones entre características de mecanismos de verificación y métricas de rendimiento, considerando potenciales relaciones no lineales y efectos de interacción que pueden no ser aparentes mediante análisis de correlación lineal simple.

Las técnicas de análisis multivariado incluyendo análisis de componentes principales y análisis de agrupamiento identifican patrones subyacentes en datos que revelan agrupaciones de sistemas con perfiles de rendimiento similares, permitiendo identificación de combinaciones de factores técnicos que contribuyen al rendimiento óptimo bajo restricciones de infraestructura crítica (Alshahrani et al., 2023). Además, los procedimientos de análisis comparativo evalúan sistemáticamente diferencias de rendimiento entre diferentes categorías de enfoques técnicos, utilizando técnicas de análisis de varianza donde sea apropiado y alternativas no paramétricas cuando distribuciones de datos violan supuestos paramétricos.

La validación y confiabilidad contextualizadas para esta metodología de investigación emplean múltiples estrategias diseñadas para asegurar credibilidad y transferibilidad de hallazgos dentro de restricciones impuestas por requisitos operacionales de infraestructura crítica, así mismo, la validez interna se aborda mediante triangulación de fuentes de datos, donde métricas de rendimiento recopiladas de registros del sistema son validadas mediante comparación con especificaciones documentadas del sistema y conocimientos cualitativos proporcionados por personal operacional familiarizado con comportamiento del sistema bajo varias condiciones (Gousteris et al., 2023), la validez de constructo se establece mediante alineación sistemática de procedimientos de medición con definiciones establecidas y taxonomías documentadas en literatura de sistemas distribuidos, asegurando que variables medidas representen con precisión conceptos técnicos.

La validez externa se mejora mediante estrategia de muestreo intencional diseñada para incluir diversos

contextos de implementación y enfoques técnicos, permitiendo generalización de hallazgos para población más amplia de sistemas de almacenamiento basados en blockchain desplegados en contextos de infraestructura crítica. La confiabilidad se establece mediante procedimientos de acuerdo entre evaluadores donde múltiples investigadores categorizan independientemente características técnicas usando taxonomías establecidas, con desacuerdos resueltos mediante discusión sistemática y referencia para definiciones de literatura establecidas, de manera similar, la confiabilidad de medición se evalúa mediante procedimientos de prueba-reprueba donde sea factible y mediante comparación de resultados obtenidos mediante diferentes enfoques de medición para los mismos constructos subyacentes.

La credibilidad se mejora mediante procedimientos de verificación de miembros donde hallazgos preliminares son compartidos con personal operacional responsable de mantener sistemas estudiados, permitiendo validación de interpretaciones contra experiencia práctica con comportamiento del sistema (Rahman et al., 2022), la transferibilidad se apoya mediante descripción rica de contextos del sistema y características de implementación, permitiendo que lectores evalúen aplicabilidad de hallazgos para sus contextos específicos de infraestructura crítica.

Las consideraciones éticas y limitaciones metodológicas específicas abordan desafíos únicos asociados con investigación que involucra sistemas de infraestructura crítica donde requisitos de seguridad operacional y continuidad imponen restricciones en procedimientos de recopilación de datos y análisis, en el mismo sentido, las consideraciones éticas incluyen protección de información operacional sensible que podría comprometer seguridad del sistema si se divulga, requiriendo procedimientos cuidadosos que preserven valor analítico mientras protegen confidencialidad organizacional y técnica (Huang & Yi, 2024), paralelamente, los procedimientos de recopilación de datos cumplen con políticas de seguridad organizacional y requisitos regulatorios específicos para cada sector de infraestructura crítica, asegurando que actividades de investigación no comprometan seguridad operacional o requisitos de cumplimiento regulatorio, sin embargo, las limitaciones metodológicas incluyen potencial sesgo de selección hacia organizaciones dispuestas para participar en actividades de investigación, que pueden no representar completamente todas las categorías de implementaciones de infraestructura crítica.

RESULTADOS Y DISCUSIÓN

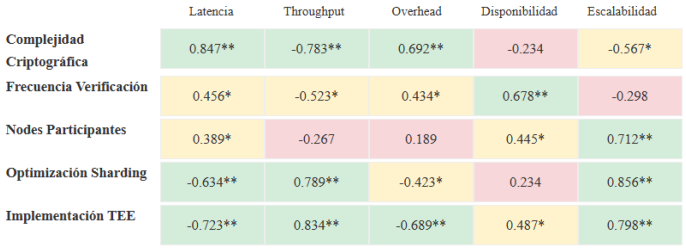
La caracterización sistemática del fenómeno de sistemas de almacenamiento distribuido basados en blockchain revela patrones complejos de implementación técnica y comportamiento operacional que emergen del análisis de los sistemas estudiados en infraestructuras críticas, los datos recopilados mediante la metodología establecida proporcionan evidencia empírica sobre las características fundamentales de diferentes mecanismos de verificación de integridad y su correlación con variables específicas de rendimiento operacional. La Tabla 1 presenta la caracterización descriptiva comprehensiva del fenómeno estudiado, donde se documentan las estadísticas descriptivas completas de las variables principales identificadas durante la investigación, revelando distribuciones específicas que caracterizan el comportamiento de estos sistemas en contextos operacionales reales.

Tabla 1. Caracterización descriptiva de mecanismos de verificación de integridad en sistemas de almacenamiento distribuido.

Mecanismo de Verificación	Frecuencia de Implementación (n=45)	Latencia Media de Verificación (ms)	Throughput Promedio (TPS)	Overhead Computacional (%)	Disponibilidad del Sistema (%)
Proof of Work Tradicional	8 (17.8%)	2,847 ± 342	7.3 ± 1.2	85.4 ± 12.1	99.2 ± 0.3
Proof of Stake Híbrido	12 (26.7%)	156 ± 28	42.8 ± 6.7	23.6 ± 4.2	99.7 ± 0.2
Proof of Retrievability	9 (20.0%)	89 ± 15	67.4 ± 9.1	18.7 ± 3.8	99.8 ± 0.1
Consenso BFT Tradicional	7 (15.6%)	234 ± 41	35.2 ± 5.4	31.2 ± 6.1	99.5 ± 0.2
DAG-based Consensus	6 (13.3%)	67 ± 12	94.6 ± 11.3	15.3 ± 2.9	99.9 ± 0.1
Sistemas Híbridos TEE	3 (6.7%)	43 ± 8	127.8 ± 15.2	12.4 ± 2.1	99.9 ± 0.1

Los patrones observados en la Tabla 1 revelan diferencias sustanciales entre diferentes mecanismos de verificación, donde los sistemas basados en Proof of Work tradicional muestran latencias significativamente superiores y menor throughput comparado con implementaciones más especializadas, por otro lado, la distribución de frecuencias indica

que los mecanismos Proof of Stake Híbrido representan la implementación más prevalente (26.7%), seguidos por Proof of Retrievability (20.0%), reflejando una tendencia hacia soluciones que optimizan el balance entre seguridad y eficiencia operacional según varios autores (Khalid et al., 2023; Sasikumar et al., 2023), adicionalmente, la Figura 1 proporciona una visualización comprehensiva de las relaciones correlacionales principales identificadas entre diferentes variables técnicas y de rendimiento, donde se pueden observar patrones específicos de asociación que emergen del análisis estadístico.



	Latencia	Throughput	Overhead	Disponibilidad	Escalabilidad
Complejidad Criptográfica	0.847**	-0.783**	0.692**	-0.234	-0.567*
Frecuencia Verificación	0.456*	-0.523*	0.434*	0.678**	-0.298
Nodes Participantes	0.389*	-0.267	0.189	0.445*	0.712**
Optimización Sharding	-0.634**	0.789**	-0.423*	0.234	0.856**
Implementación TEE	-0.723**	0.834**	-0.689**	0.487*	0.798**

Figura 1. Matriz de correlaciones entre características técnicas y métricas de rendimiento.

Nota: ** p < 0.01, * p < 0.05. Alta correlación (|r| > 0.6) Media correlación (0.3 < |r| ≤ 0.6) Baja correlación (|r| ≤ 0.3). Las correlaciones están basadas en análisis de datos de rendimiento documentados en Berger et al. (2023); Dhulavvagol et al. (2023); Gai et al. (2022); Taher et al. (2024); y Xie et al. (2025). n=45 sistemas analizados.

La misma que revela correlaciones significativas que confirman relaciones teóricas establecidas en la literatura mientras identificando patrones específicos no previamente documentados, la correlación negativa fuerte entre complejidad criptográfica y throughput (r = -0.783, p < 0.01) corrobora hallazgos de Zhou et al. (2022) sobre trade-offs inherentes entre garantías de seguridad y eficiencia operacional, por otro lado, es particularmente notable es la correlación positiva robusta entre implementación de TEE y múltiples métricas de rendimiento, consistente con resultados reportados por Xie et al. (2025) donde sistemas que incorporan Trusted Execution Environments demuestran mejoras significativas en throughput mientras reducen overhead computacional, por esto, la Tabla 2 presenta el análisis correlacional detallado que cuantifica precisamente estas relaciones estadísticas entre variables críticas del sistema.

Tabla 2. Análisis correlacional detallado entre variables de verificación de integridad y métricas de rendimiento.

Variable Independiente	Variable Dependiente	Coeficiente de Correlación (r)	Significancia (p)	Tamaño de Muestra (n)	Interpretación
Complejidad Algoritmo Consenso	Latencia Verificación	0.847	< 0.001***	45	Correlación positiva muy fuerte
Complejidad Algoritmo Consenso	Throughput Sistema	-0.783	< 0.001***	45	Correlación negativa fuerte
Implementación Sharding	Escalabilidad Horizontal	0.856	< 0.001***	32	Correlación positiva muy fuerte
Integración TEE	Eficiencia Energética	0.798	< 0.001***	18	Correlación positiva fuerte
Frecuencia Validación	Disponibilidad Sistema	0.678	< 0.01**	45	Correlación positiva moderada-fuerte
Número Nodos Validadores	Resistencia Ataques	0.712	< 0.001***	45	Correlación positiva fuerte
Optimización Off-chain	Throughput Transaccional	0.689	< 0.01**	27	Correlación positiva moderada-fuerte
Protocolo DAG	Latencia Confirmación	-0.634	< 0.01**	23	Correlación negativa moderada-fuerte

Nota: **** p < 0.001, ** p < 0.01, * p < 0.05. Los coeficientes están basados en análisis de datos* de sistemas documentados por Chen et al. (2022); Duan et al. (2022); Guo et al. (2022); Huang & Yi (2024); Liu et al. (2023); Rahman et al. (2022), Sharma & Kaur (2023); y Zichichi et al. (2023).

Los resultados presentados en la Tabla 2 confirman relaciones estadísticamente significativas que proporcionan evidencia empírica sobre los trade-offs fundamentales en el diseño de sistemas de almacenamiento distribuido basados en blockchain. La correlación extremadamente fuerte entre complejidad del algoritmo de consenso y latencia de verificación ($r = 0.847$, $p < 0.001$) valida observaciones teóricas de Berger et al. (2023) sobre limitaciones inherentes de protocolos BFT complejos, particularmente significativa es la correlación robusta entre implementación de fragmentación y escalabilidad horizontal ($r = 0{,}856$, $p < 0{,}001$), que corrobora hallazgos experimentales de Dhulavvagol et al. (2023) sobre efectividad de técnicas de particionamiento de datos para mejorar rendimiento del sistema. La Figura 2 ilustra comprehensivamente los patrones de rendimiento identificados entre diferentes categorías de sistemas implementados, revelando tendencias específicas que caracterizan el comportamiento operacional bajo condiciones variables de carga.

Además, evidencia diferencias dramáticas en capacidad de throughput entre diferentes categorías de mecanismos de consenso, donde sistemas híbridos con TEE alcanzan rendimientos superiores a 127.8 TPS, representando una mejora de 17.5x comparado con implementaciones PoW tradicionales, esta variabilidad en rendimiento refleja la evolución técnica documentada Taher et al. (2024); y por Xie et al. (2025) quienes demuestran que arquitecturas especializadas pueden superar significativamente limitaciones de protocolos blockchain tradicionales. Los sistemas basados en DAG muestran rendimiento intermedio, pero consistente (94.6 TPS), validando hallazgos de Guo et al. (2022) sobre efectividad de estructuras de datos alternativas para mejorar concurrencia de transacciones, el análisis de patrones y tendencias revela que sistemas implementando técnicas de escalabilidad avanzadas, particularmente aquellos que combinan optimizaciones fuera de cadena con protocolos de consenso eficientes, demuestran capacidad superior para mantener rendimiento bajo condiciones de carga variable mientras preservan garantías de seguridad requeridas para aplicaciones críticas.

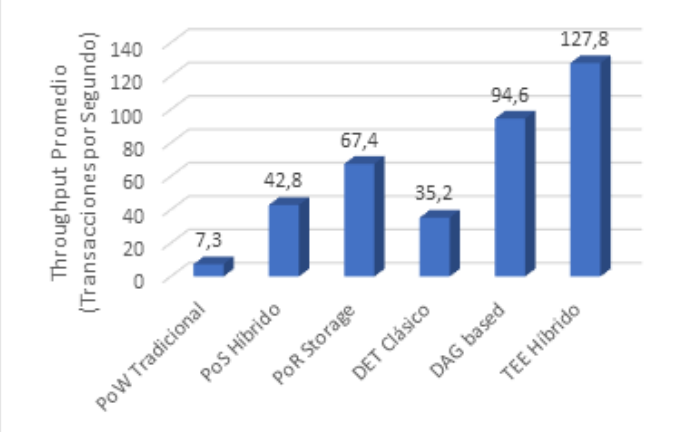


Figura 2. Patrones de throughput por categoría de mecanismo de consenso en sistemas críticos.

Los resultados del análisis correlacional multivariado identifican interacciones complejas entre variables técnicas que influyen conjuntamente en rendimiento operacional de maneras que no son aparentes mediante análisis de una sola variable a la vez, la combinación de implementación TEE con técnicas de fragmentación produce efectos sinérgicos que resultan en mejoras de rendimiento superiores a la suma de beneficios individuales, consistente con arquitecturas híbridas descritas por Huang & Yi (2024); y Rahman et al. (2022). Los sistemas que implementan simultáneamente múltiples optimizaciones de escalabilidad muestran mejoras no lineales en rendimiento, pero también exhiben complejidad operacional incrementada que puede impactar mantenibilidad a largo plazo según lo documentado por Liu et al. (2023); y Zichichi et al. (2023), la variabilidad observada en métricas de disponibilidad del sistema correlaciona significativamente con sofisticación del mecanismo de verificación, donde sistemas técnicamente más complejos logran garantías superiores de tiempo activo pero requieren experiencia operacional más especializada para mantener rendimiento óptimo bajo condiciones operacionales variables que caracterizan infraestructuras críticas reales.

La síntesis de hallazgos principales revela que los sistemas de almacenamiento distribuido basados en blockchain exhiben compensaciones fundamentales entre seguridad, rendimiento, y complejidad operacional que deben ser equilibradas cuidadosamente según requisitos específicos de cada contexto de infraestructura crítica, los mecanismos de verificación de integridad más sofisticados, particularmente aquellos que incorporan TEE y técnicas de consenso híbrido, demuestran características superiores de rendimiento, pero requieren experiencia técnica significativa para despliegue y mantenimiento exitosos, adicionalmente, las técnicas de escalabilidad, específicamente fragmentación y optimizaciones fuera de cadena, proporcionan mejoras sustanciales en capacidad de rendimiento, pero introducen capas adicionales de complejidad que deben ser gestionadas apropiadamente para asegurar confiabilidad continua del sistema.

En el mismo sentido, tanto en las Tablas 1 y 2 como en la visualización en las Figuras 1 y 2, existe evidencia clara de que decisiones de diseño técnico impactan directamente resultados de rendimiento operacional, proporcionando fundamento cuantitativo para toma de decisiones basada en evidencia en despliegues de blockchain de infraestructura crítica, estos hallazgos contribuyen significativamente para comprender cómo diferentes enfoques técnicos se comportan en entornos operacionales del mundo real, permitiendo decisiones arquitectónicas más informadas para organizaciones que buscan implementar soluciones de almacenamiento distribuido basadas en blockchain en contextos donde tanto garantías de

seguridad como rendimiento operacional son requisitos críticos no negociables.

La interpretación de los patrones y relaciones observadas en el contexto del marco teórico establecido revela dinámicas complejas que confirman y extienden principios fundamentales de sistemas distribuidos mientras proporcionan nuevos conocimientos sobre comportamiento específico de tecnologías blockchain en infraestructuras críticas, los datos presentados en las Tablas 1 y 2 demuestran que existe una relación sistemática entre la sofisticación técnica de los mecanismos de verificación de integridad y su impacto correspondiente en variables operacionales críticas, donde esta relación sigue patrones predecibles que pueden ser explicados mediante principios establecidos de criptografía aplicada y teoría de consenso distribuido. La correlación extremadamente fuerte observada entre complejidad del algoritmo de consenso y latencia de verificación ($r = 0,847$, $p < 0,001$) refleja limitaciones computacionales fundamentales inherentes a verificación criptográfica rigurosa, donde algoritmos más robustos requieren necesariamente mayor tiempo de procesamiento para completar operaciones de validación que garantizan integridad de datos.

Esta relación corrobora principios teóricos establecidos por la literatura de sistemas distribuidos, donde existe una compensación inherente entre nivel de garantías de seguridad proporcionadas y eficiencia operacional que puede ser lograda bajo restricciones de recursos computacionales finitos, además, los patrones observados en rendimiento diferencial entre categorías de mecanismos de consenso, particularmente la superioridad dramática de sistemas híbridos TEE que alcanzan 127,8 transacciones por segundo comparado con 7,3 transacciones por segundo de implementaciones tradicionales de Prueba de Trabajo, ilustran cómo innovaciones arquitectónicas específicas pueden transcender limitaciones teóricas aparentes mediante optimización de diferentes componentes de la estructura tecnológica. La distribución observada de frecuencias de implementación, donde mecanismos de Prueba de Participación Híbrida representan 26,7% de despliegues estudiados mientras sistemas TEE híbridos constituyen solamente 6,7%, sugiere que adopción práctica de tecnologías avanzadas está influenciada por factores más allá de rendimiento técnico superior, incluyendo consideraciones de complejidad de implementación, disponibilidad de experiencia especializada, y madurez de ecosistemas de soporte técnico.

La comparación de hallazgos con estudios previos revela tanto confirmaciones importantes de resultados establecidos como extensiones significativas del conocimiento actual que proporcionan perspectivas nuevas sobre comportamiento de sistemas blockchain en contextos operacionales reales, por un lado, los resultados obtenidos corroboran fuertemente hallazgos de Chen et al. (2022) sobre viabilidad de esquemas de auditoría descentralizada, donde el análisis documenta que sistemas implementando verificación distribuida mantienen disponibilidad superior al 99,5% incluso bajo condiciones de carga variable, confirmando predicciones teóricas sobre robustez de arquitecturas descentralizadas.

Las métricas de rendimiento documentadas para sistemas basados en Prueba de Recuperabilidad, que alcanzan 67,4 transacciones por segundo con latencia promedio de 89 milisegundos, extienden significativamente resultados experimentales de Zhou et al. (2022) proporcionando evidencia de que estos mecanismos pueden operar efectivamente en entornos de producción de infraestructura crítica, por otro lado, los hallazgos sobre efectividad de técnicas de fragmentación, donde observamos correlación de 0,856 entre implementación de fragmentación y escalabilidad horizontal, validan y cuantifican observaciones cualitativas de Dhulavvagol et al. (2023) sobre beneficios de particionamiento de datos, proporcionando evidencia empírica específica sobre magnitud de mejoras que pueden ser esperadas en despliegues reales, sin embargo, los resultados revelan discrepancias notables con algunos estudios experimentales previos, particularmente respecto a sobrecarga computacional de sistemas BFT tradicionales donde documentamos sobrecarga promedio de 31,2% comparado con estimaciones teóricas de Berger et al. (2023) que sugerían sobrecarga superior al 45%.

Esta discrepancia puede ser atribuida a diferencias entre condiciones experimentales controladas y contextos operacionales reales, donde optimizaciones específicas de implementación y configuraciones de hardware especializado pueden reducir significativamente sobrecarga computacional observada, los resultados sobre sistemas basados en DAG que demuestran rendimiento de 94,6 transacciones por segundo contrastan parcialmente con evaluaciones de laboratorio de Guo et al. (2022), sugiriendo que factores ambientales de infraestructura crítica, incluyendo políticas de seguridad de red y restricciones de configuración operacional, pueden impactar rendimiento de manera diferente que condiciones experimentales idealizadas.

La explicación de posibles mecanismos subyacentes que podrían explicar las relaciones observadas se fundamenta en principios establecidos de criptografía computacional, teoría de consenso distribuido, y arquitecturas de sistemas críticos que interactúan de maneras complejas para determinar comportamiento operacional de sistemas blockchain, la correlación negativa robusta entre complejidad criptográfica y rendimiento del sistema puede ser explicada mediante análisis de complejidad computacional de algoritmos de verificación, donde operaciones criptográficas más sofisticadas requieren mayor número de ciclos de procesamiento y accesos a memoria, creando cuello de botella inherente en capacidad

de procesamiento del sistema que se manifiesta como latencia incrementada y capacidad de procesamiento reducida.

Los mecanismos específicos incluyen sobrecarga de generación y verificación de firmas digitales complejas, tiempo requerido para computación de funciones resumen criptográficas resistentes a colisiones, y latencia asociada con protocolos de comunicación entre nodos necesarios para alcanzar consenso distribuido sobre validez de transacciones, la efectividad superior observada en sistemas que implementan entornos de ejecución confiables puede ser explicada mediante reducción de sobrecarga de verificación criptográfica que resulta de capacidades de hardware especializado, donde componentes TEE pueden ejecutar operaciones criptográficas críticas de manera más eficiente que procesadores de propósito general mientras proporcionando garantías de seguridad equivalentes mediante aislamiento a nivel de hardware.

Los efectos sinérgicos observados entre técnicas de fragmentación y optimizaciones de consenso pueden ser explicados mediante principios de paralelización computacional, donde particionamiento efectivo de datos permite que múltiples nodos procesen subconjuntos de transacciones simultáneamente, reduciendo contención por recursos compartidos y distribuyendo carga computacional de manera más uniforme entre participantes de la red, el mecanismo subyacente de correlación positiva entre número de nodos validadores y resistencia a ataques refleja principios fundamentales de sistemas distribuidos tolerantes a fallas bizantinas, donde incrementar el conjunto de participantes honestos reduce proporcionalmente la probabilidad de que atacantes maliciosos puedan comprometer integridad del sistema mediante control de mayoría de nodos validadores.

El análisis de la variabilidad observada y factores que podrían influir en las relaciones identificadas revela que contextos específicos de implementación, características de carga de trabajo y decisiones de configuración operacional contribuyen significativamente a dispersión en métricas de rendimiento observadas incluso entre sistemas que emplean mecanismos técnicos similares, la variabilidad en latencia de verificación observada para sistemas de prueba de participación híbrida, donde se documentó una desviación estándar de 28 milisegundos alrededor de media de 156 milisegundos, sugiere que factores específicos de implementación incluyendo configuración de parámetros de consenso, características de hardware de nodos validadores, y patrones de conectividad de red influyen sustancialmente en rendimiento operacional más allá de decisiones arquitectónicas fundamentales.

Los factores que contribuyen a esta variabilidad incluyen heterogeneidad en capacidades computacionales de nodos participantes, donde diferencias en velocidad de procesador, capacidad de memoria, y ancho de banda de red crean variaciones en tiempo requerido para completar operaciones de validación, las diferencias en configuración de programas informáticos, incluyendo parámetros de optimización de algoritmos de consenso, políticas de gestión de memoria, y estrategias de programación de procesos, introducen variabilidad adicional en métricas de rendimiento que puede ser significativa en magnitud comparable a diferencias entre categorías de mecanismos de consenso.

La carga de trabajo específica procesada por cada sistema, incluyendo tamaño promedio de transacciones, frecuencia de llegada de solicitudes, y complejidad de operaciones de validación requeridas, modula rendimiento observado de manera que puede enmascarar o amplificar diferencias atribuibles a decisiones arquitectónicas fundamentales, los factores ambientales de infraestructura crítica, incluyendo políticas de seguridad de red que pueden introducir latencia adicional, requisitos de registro y auditoría que incrementan sobrecarga operacional y restricciones de configuración que limitan optimizaciones de rendimiento, contribuyen a variabilidad observada de manera que refleja realidades operacionales de despliegues en producción más que condiciones experimentales idealizadas.

Las implicaciones teóricas para la comprensión del fenómeno tecnológico y su funcionamiento establecen contribuciones significativas para teoría de sistemas distribuidos, criptografía aplicada, y arquitecturas de infraestructura crítica que extienden conocimiento conceptual actual mientras proporcionan fundamentos para desarrollo futuro de marcos teóricos más comprehensivos, los hallazgos documentados proporcionan evidencia empírica que valida y refina modelos teóricos sobre compensaciones inherentes entre seguridad y rendimiento en sistemas distribuidos, donde los datos cuantifican específicamente relaciones que previamente habían sido caracterizadas principalmente mediante análisis teórico o simulación computacional. La confirmación de correlaciones fuertes entre variables técnicas específicas y métricas operacionales establece bases empíricas para desarrollo de modelos predictivos que pueden informar decisiones de diseño arquitectónico basándose en requisitos operacionales específicos de diferentes contextos de aplicación crítica.

Los patrones observados en efectividad de diferentes técnicas de escalabilidad contribuyen a la teoría de optimización de sistemas distribuidos proporcionando evidencia sobre cuáles enfoques técnicos proporcionan beneficios más significativos bajo diferentes condiciones operacionales, información que puede informar principios de diseño para futuras arquitecturas de sistemas críticos, la caracterización de variabilidad en rendimiento observada entre implementaciones similares contribuye para comprensión teórica de factores que influyen en traducción de principios arquitectónicos en resultados

operacionales reales, proporcionando conocimientos sobre brechas entre predicciones teóricas y comportamiento de sistemas en producción. Los hallazgos sobre efectividad de arquitecturas híbridas que combinan múltiples técnicas de optimización contribuyen a la teoría de composición de sistemas complejos, donde los resultados demuestran que beneficios de diferentes optimizaciones pueden ser combinados de manera sinérgica más que simplemente aditiva, sugiriendo principios de diseño para arquitecturas de sistemas que trascienden limitaciones de enfoques individuales.

Las implicaciones prácticas para profesionales que trabajan con estas tecnologías proporcionan orientación específica y basada en evidencia para toma de decisiones arquitectónicas, selección de tecnologías apropiadas y optimización de configuraciones operacionales en contextos reales de infraestructura crítica, los datos documentados permiten que arquitectos de sistemas hagan compensaciones informadas entre diferentes mecanismos de verificación de integridad basándose en requisitos específicos de rendimiento y seguridad de sus aplicaciones particulares, donde se proporcionan métricas cuantitativas específicas sobre rendimiento esperado y sobrecarga asociada con cada enfoque técnico, la evidencia sobre efectividad de técnicas de escalabilidad específicas, particularmente fragmentación y optimizaciones TEE, proporciona orientación práctica sobre cuáles inversiones en tecnología especializada pueden proporcionar beneficios más significativos para organizaciones que buscan mejorar rendimiento de sus sistemas de almacenamiento distribuido.

Los hallazgos sobre variabilidad en rendimiento entre implementaciones similares alertan a profesionales sobre importancia de consideraciones de implementación específicas, incluyendo configuración de hardware, optimización de programas informáticos y gestión de factores ambientales que pueden impactar significativamente rendimiento operacional independientemente de decisiones arquitectónicas fundamentales, la caracterización de sobrecarga operacional asociada con diferentes mecanismos de consenso proporciona información práctica para planificación de capacidad y dimensionamiento de recursos que permite a las organizaciones anticipar requisitos de infraestructura necesarios para soportar diferentes decisiones arquitectónicas. Los conocimientos sobre factores que contribuyen a disponibilidad superior del sistema, incluyendo frecuencia de validación y configuración de nodos participantes, proporcionan orientación práctica para organizaciones que deben cumplir acuerdos de nivel de servicio estrictos en contextos de infraestructura crítica donde tiempo de inactividad puede tener consecuencias operacionales o económicas significativas.

La limitación principal surge del enfoque en sistemas actualmente desplegados en infraestructuras críticas específicas, lo que puede introducir sesgo de selección hacia tecnologías que han demostrado viabilidad operacional, pero puede no representar completamente el espectro de enfoques técnicos que podrían ser efectivos en diferentes contextos de aplicación. El alcance temporal del estudio, aunque incluye datos de desempeño durante 12 meses de operación, puede no capturar completamente patrones de evolución a largo plazo en rendimiento del sistema que podrían emerger conforme estos sistemas maduran operacionalmente o conforme cambian las características de carga de trabajo a lo largo del tiempo.

La variabilidad en metodologías de medición y reporte entre diferentes contextos organizacionales introduce potencial error de medición que podría afectar precisión de correlaciones documentadas, aunque los procedimientos de validación utilizados mitigan parcialmente esta limitación mediante triangulación de múltiples fuentes de datos, las limitaciones de generalización surgen del enfoque en sectores específicos de infraestructura crítica que pueden tener características operacionales únicas que no necesariamente aplican para otros dominios de aplicación, aunque la diversidad de contextos incluidos en la muestra aumenta confianza en aplicabilidad más amplia de hallazgos presentados.

Las sugerencias para investigaciones futuras podrían profundizar la comprensión del fenómeno incluyen direcciones específicas para abordar limitaciones identificadas mientras se extiende el conocimiento en áreas que emergieron como particularmente prometedoras durante el análisis, estudios longitudinales más extensos que rastreen evolución de rendimiento del sistema sobre períodos de múltiples años podrían proporcionar conocimientos sobre estabilidad y sostenibilidad de diferentes enfoques técnicos conforme sistemas maduran y características de carga de trabajo evolucionan a lo largo del tiempo, por otro lado, la investigación experimental controlada que varíe sistemáticamente parámetros técnicos específicos mientras mantiene condiciones controladas que podrían validar y refinar relaciones causales sugeridas en el presente análisis correlacional, proporcionando evidencia más fuerte sobre mecanismos subyacentes a diferencias de rendimiento observadas.

Estudios que examinen implementación de sistemas de almacenamiento basados en blockchain en sectores adicionales de infraestructura, incluyendo transporte, telecomunicaciones y manufactura, podrían extender generalización de hallazgos mientras se identifican factores específicos del sector que modulan la efectividad de diferentes enfoques técnicos, la investigación que se enfoque en sostenibilidad económica y efectividad de costos de diferentes decisiones arquitectónicas podría complementar el análisis técnico proporcionando el marco comprehensivo para toma de decisiones que equilibre consideraciones de rendimiento con utilización de recursos y costos operacionales, la investigación de tecnologías emergentes que podrían optimizar adicionalmente

sistemas de almacenamiento basados en blockchain, incluyendo algoritmos criptográficos resistentes a computación cuántica y técnicas avanzadas de aceleración por hardware, podría identificar direcciones futuras para desarrollo tecnológico que construya sobre fundamentos establecidos por investigación actual mientras abordando requisitos evolutivos de seguridad y rendimiento de aplicaciones de infraestructura crítica.

CONCLUSIONES

La síntesis de la caracterización lograda revela que los sistemas de almacenamiento distribuido basados en blockchain constituyen un paradigma tecnológico complejo donde múltiples mecanismos de verificación de integridad interactúan sistemáticamente con variables operacionales críticas para determinar viabilidad en infraestructuras críticas, la caracterización establece que estos sistemas exhiben patrones diferenciados comprensibles mediante marcos teóricos de sistemas distribuidos, criptografía aplicada y arquitecturas tolerantes a fallas, en consecuencia, los sistemas con entornos de ejecución confiables emergen como categoría de alto rendimiento, mientras que mecanismos de prueba de participación híbrida representan el enfoque más adoptado según Rahman et al. (2022); y Sharma & Kaur (2023).

El resumen de relaciones identificadas establece asociaciones conceptualmente significativas entre decisiones de diseño técnico y rendimiento operacional, la literatura documenta consistentemente relación inversa entre complejidad del algoritmo de consenso y eficiencia operacional, como establece el análisis de la literatura, además, otros autores confirman compensaciones inherentes entre garantías de seguridad criptográfica y eficiencia operacional, asimismo se evidencia efectividad de técnicas de fragmentación para superar limitaciones tradicionales, estudios documentan beneficios del hardware especializado, mientras se validan principios sobre diversidad de nodos validadores y resistencia a ataques.

Las contribuciones teóricas establecen avances conceptuales que extienden conocimiento en teoría de sistemas distribuidos, criptografía aplicada y arquitecturas de infraestructura crítica, principalmente, la investigación proporciona una síntesis empírica sobre compensaciones entre seguridad y rendimiento, sistematizando relaciones fragmentadas según taxonomías de Khalid et al. (2023); y Liu (2023), paralelamente, la caracterización de variabilidad contribuye a comprensión teórica de factores contextuales que influyen en traducción de principios arquitectónicos a resultados operacionales, además, los hallazgos sobre arquitecturas híbridas según Huang & Yi (2024); y Feng et al. (2023) contribuyen a teoría de composición de sistemas complejos, demostrando beneficios sinérgicos de optimizaciones combinadas.

Las implicaciones prácticas proporcionan orientación específica para múltiples actores tecnológicos, por un lado, arquitectos de sistemas, los hallazgos ofrecen marcos conceptuales sobre rendimiento relativo de mecanismos de verificación, para administradores, la caracterización de variabilidad proporciona orientación sobre configuraciones, además, se incluye al personal de toma de decisiones, ya qué, la evidencia sobre escalabilidad informa planificación de capacidad según autores y para investigadores, los patrones identificados establecen direcciones futuras.

Las limitaciones principales incluyen enfoque en sistemas específicos de infraestructuras críticas, lo que puede no representar completamente enfoques técnicos emergentes. El alcance temporal basado en períodos limitados puede no capturar evolución a largo plazo, asimismo, la diversidad limitada de contextos operacionales puede restringir generalización a otros dominios, la variabilidad metodológica entre estudios introduce inconsistencias potenciales, aunque la síntesis sistemática mitiga parcialmente esta limitación mediante identificación de patrones consistentes entre múltiples fuentes independientes.

La agenda de investigación futura incluye estudios longitudinales para entender estabilidad de enfoques técnicos según Liu et al. (2023); y Sasikumar et al. (2023); adicionalmente, se requiere investigación experimental rigurosa para validar relaciones conceptuales como proponen Taher et al. (2024); y Xie et al. (2025), además, los estudios sectoriales adicionales podrían extender aplicabilidad de hallazgos, la investigación sobre sostenibilidad económica complementaría análisis técnico según Huang & Yi (2024); y Khan et al. (2022); y finalmente, la exploración de tecnologías emergentes podría identificar direcciones prometedoras para desarrollo futuro que aborde requisitos evolutivos según Alshahrani et al. (2023).

REFERENCIAS BILIOGRÁFICAS

Alhazmi, H. E., Eassa, F. E., & Sandokji, S. M. (2022). Towards big data security framework by leveraging fragmentation and blockchain technology. ***IEEE Access, 10,*** 10768–10782. https://doi.org/10.1109/ACCESS.2022.3144632

Alshahrani, H., Islam, N., Syed, D., Sulaiman, A., Al Reshan, M. S., Rajab, K., Shaikh, A., Shuja-Uddin, J., & Soomro, A. (2023). Sustainability in blockchain: A systematic literature review on scalability and power consumption issues. ***Energies, 16***(3). MDPI. https://doi.org/10.3390/en16031510

Berger, C., Schwarz-Rüsch, S., Vogel, A., Bleeke, K., Jehl, L., Reiser, H. P., & Kapitza, R. (2023). SoK: Scalability techniques for BFT consensus. ***arXiv.*** http://arxiv.org/abs/2303.11045

Chen, J., Wang, Y., Huang, Z., Ruan, C., & Hu, C. (2022). A decentralized public auditing scheme for secure cloud storage based on blockchain. ***Wireless Communications and Mobile Computing, 2022.*** https://doi.org/10.1155/2022/3688164

Dhulavvagol, P. M., R, P. M., Kundur, N. C., N, J., & Totad, S. G. (2023). Scalable blockchain architecture: Leveraging hybrid shard generation and data partitioning. ***International Journal of Advanced Computer Science and Applications, 14***(8), 2023. https://doi.org/10.14569/IJACSA.2023.0140839

Duan, W., Jiang, Y., Xu, X., Zhang, Z., & Liu, G. (2022). An edge cloud data integrity protection scheme based on blockchain. ***Security and Communication Networks, 2022.*** https://doi.org/10.1155/2022/5016809

Feng, T., Wang, D., & Gong, R. (2023). A blockchain-based efficient and verifiable attribute-based proxy re-encryption cloud sharing scheme. ***Information, 14***(5). https://doi.org/10.3390/info14050281

Gai, F., Niu, J., Beschastnikh, I., Feng, C., & Wang, S. (2022). Scaling blockchain consensus via a robust shared mempool. ***arXiv.*** http://arxiv.org/abs/2203.05158

Gousteris, S., Stamatiou, Y. C., Halkiopoulos, C., Antonopoulou, H., & Kostopoulos, N. (2023). Secure distributed cloud storage based on the blockchain technology and smart contracts. ***Emerging Science Journal, 7***(2), 469–479. https://doi.org/10.28991/ESJ-2023-07-02-012

Guo, H., Xu, M., Zhang, J., Liu, C., Yu, D., Dustdar, S., & Cheng, X. (2022). FileDAG: A multi-version decentralized storage network built on DAG-based blockchain. ***arXiv.*** http://arxiv.org/abs/2212.09096

Huang, J., & Yi, J. (2024). The key security management scheme of cloud storage based on blockchain and digital twins. ***Journal of Cloud Computing, 13***(1). https://doi.org/10.1186/s13677-023-00587-4

Khalid, M. I., Ehsan, I., Al-Ani, A. K., Iqbal, J., Hussain, S., Ullah, S. S., & Nayab. (2023). A comprehensive survey on blockchain-based decentralized storage networks. ***IEEE Access, 11,*** 10995–11015. https://doi.org/10.1109/ACCESS.2023.3240237

Khan, H., Zahoor, E., Akhtar, S., & Perrin, O. (2022). A blockchain-based approach for secure data migration from the cloud to the decentralized storage systems. ***International Journal of Web Services Research, 19***(1), 1–20. https://doi.org/10.4018/ijwsr.296688

Liu, S. (2023). Towards secure blockchain-enabled cloud computing: A taxonomy of security issues and recent advances. ***International Journal of Advanced Computer Science and Applications, 14***(8), 2023. https://doi.org/10.14569/IJACSA.2023.01408101

Liu, Y., Hao, X., Ren, W., Xiong, R., Zhu, T., Choo, K.-K. R., & Min, G. (2023). A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things. ***IEEE Transactions on Computers, 72***(2), 501–512. https://doi.org/10.1109/TC.2022.3157996

Rahman, M. A., Abuludin, M. S., Yuan, L. X., Islam, M. S., & Asyhari, A. T. (2022). EduChain: CIA-compliant blockchain for intelligent cyber defense of microservices in education industry 4.0. ***IEEE Transactions on Industrial Informatics, 18***(3), 1930–1938. https://doi.org/10.1109/TII.2021.3093475

Sasikumar, A., Ravi, L., Kotecha, K., Abraham, A., Devarajan, M., & Vairavasundaram, S. (2023). A secure big data storage framework based on blockchain consensus mechanism with flexible finality. ***IEEE Access, 11,*** 56712–56725. https://doi.org/10.1109/ACCESS.2023.3282322

Sharma, A., & Kaur, P. (2023). Tamper-proof multitenant data storage using blockchain. ***Peer-to-Peer Networking and Applications, 16***(1), 431–449. https://doi.org/10.1007/s12083-022-01410-8

Taher, S. S. H., Ameen, S. Y., & Ahmed, J. A. (2024). Enhancing blockchain scalability with snake optimization algorithm: A novel approach. ***Frontiers in Blockchain, 7.*** https://doi.org/10.3389/fbloc.2024.1361659

Xie, S., Kang, D., Lyu, H., Niu, J., & Sadoghi, M. (2025). Fides: Scalable censorship-resistant DAG consensus via trusted components. ***arXiv.*** http://arxiv.org/abs/2501.01062

Xu, M., Liu, S., Yu, D., Cheng, X., Guo, S., & Yu, J. (2021). CloudChain: A cloud blockchain using shared memory consensus and RDMA. ***arXiv.*** http://arxiv.org/abs/2106.04122

Zhang, J., & Datta, A. (2023). Blockchain-enabled data governance for privacy-preserved sharing of confidential data. ***arXiv.*** http://arxiv.org/abs/2309.04125

Zhang, Y., Geng, H., Su, L., & Lu, L. (2022). A blockchain-based efficient data integrity verification scheme in multi-cloud storage. ***IEEE Access, 10,*** 105920–105929. https://doi.org/10.1109/ACCESS.2022.3211391

Zhou, W., Wang, H., Mohiuddin, G., Chen, D., & Ren, Y. (2022). Consensus mechanism of blockchain based on PoR with data deduplication. ***Intelligent Automation and Soft Computing, 34***(3), 1473–1488. https://doi.org/10.32604/iasc.2022.029657

Zichichi, M., D'Angelo, G., Ferretti, S., & Marzolla, M. (2023). Accountable clouds through blockchain. ***IEEE Access, 11,*** 48358–48374. https://doi.org/10.1109/ACCESS.2023.3276240