Instituto Superior Tecnológico "Los Andes" ISTLA

CÓDIGO CIENTÍFICO REVISTA DE INVESTIGACIÓN

Vol. 6 – Núm. 2 / Julio – Diciembre – 2025

Blockchain y logística militar: Transformación digital en la gestión de suministros y operaciones

Blockchain and military logistics: Digital transformation in supply chain management and operations

Blockchain e logística militar: Transformação digital na gestão de suprimentos e operações

Tafur Prada, Yesid Hernando
Escuela Militar de Suboficiales Inocencio Chincá-EMSUB
yesidtafurprada@cedoc.edu.co
https://orcid.org/0000-0002-7004-4645

Sarmiento Gutiérrez, Carlos Andrés
Escuela Militar de Suboficiales Inocencio Chincá-EMSUB
carlossarmientogutierrez@cedoc.edu.co
https://orcid.org/0009-0002-7204-9834

Arenas Prada, Yenny Patricia
Servicio Nacional de Aprendizaje
yarenas@sena.edu.co
https://orcid.org/0009-0007-5111-4832

DOI / URL: https://doi.org/10.55813/gaea/ccri/v6/n2/1218

Como citar:
Tafur Prada, Y. H., Sarmiento Gutiérrez, C. A., & Arenas Prada, Y. P. (2025). Blockchain y logística militar: Transformación digital en la gestión de suministros y operaciones. *Código Científico Revista De Investigación, 6*(2), 595–619.

Recibido: *17/11/2025* ***Aceptado:*** *16/12/2025* ***Publicado:*** *31/12/2025*

Resumen
La logística militar contemporánea enfrenta desafíos críticos en entornos volátiles (VUCA), donde la integridad de la cadena de suministro es vulnerable a ciberataques y manipulación de datos. Este artículo analiza la integración de la tecnología Blockchain y los registros distribuidos (DLT) como catalizadores para la transformación digital y la seguridad operativa (OpSec) en la gestión de defensa. Se utilizó un enfoque de Investigación de Ciencia del Diseño (DSR) para desarrollar una propuesta de arquitectura teórica de cuatro capas (física, red, consenso y aplicación). El modelo plantea una Blockchain de Consorcio con permisos, diseñada específicamente para operar bajo las restricciones de conectividad y seguridad de las operaciones militares, empleando el algoritmo de consenso de Tolerancia a Fallas Bizantinas Prácticas (PBFT). El análisis arquitectónico demuestra que la implementación de un libro mayor inmutable permite la trazabilidad genealógica completa de activos críticos, mitigando el riesgo de introducción de repuestos falsificados. Asimismo, la aplicación de Contratos Inteligentes (*Smart Contracts*) automatiza los procesos de reabastecimiento táctico, reduciendo la latencia administrativa y garantizando la precisión de los inventarios en tiempo real frente a vectores de ataque de integridad de datos. Se concluye que Blockchain trasciende la optimización administrativa para convertirse en un imperativo estratégico de defensa. Su adopción facilita la transición de cadenas de suministro centralizadas y reactivas hacia redes descentralizadas, interoperables y ciber-resilientes, asegurando la superioridad de la información logística en el teatro de operaciones moderno.
Palabras clave: logística militar, blockchain, ciberseguridad, cadena de suministro de defensa, contratos inteligentes, transformación digital.

Abstract
Contemporary military logistics faces critical challenges in volatile environments (VUCA), where supply chain integrity is vulnerable to cyberattacks and data manipulation. This article analyzes the integration of Blockchain technology and distributed ledgers (DLT) as catalysts for digital transformation and operational security (OpSec) in defense management. A Design Science Research (DSR) approach was used to develop a proposed four-layer theoretical architecture (physical, network, consensus, and application). The model proposes a permissioned Consortium Blockchain, specifically designed to operate under the connectivity and security constraints of military operations, employing the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. The architectural analysis demonstrates that the implementation of an immutable ledger allows for complete genealogical traceability of critical assets, mitigating the risk of counterfeit spare parts being introduced. Likewise, the application of Smart Contracts automates tactical resupply processes, reducing administrative latency and ensuring real-time inventory accuracy against data integrity attack vectors. It is concluded that Blockchain transcends administrative optimization to become a strategic defense imperative. Its adoption facilitates the transition from centralized and reactive supply chains to decentralized, interoperable, and cyber-resilient networks, ensuring logistical information superiority in the modern theater of operations.
Keywords: military logistics, blockchain, cybersecurity, defense supply chain, smart contracts, digital transformation.

Resumo
A logística militar contemporânea enfrenta desafios críticos em ambientes voláteis (VUCA), onde a integridade da cadeia de abastecimento é vulnerável a ciberataques e manipulação de dados. Este artigo analisa a integração da tecnologia Blockchain e dos registos distribuídos

(DLT) como catalisadores da transformação digital e da segurança operacional (OpSec) na gestão da defesa. Foi utilizada uma abordagem de Investigação em Ciência do Design (DSR) para desenvolver uma arquitetura teórica proposta de quatro camadas (física, rede, consenso e aplicação). O modelo propõe uma Blockchain de consórcio autorizada, especificamente concebida para operar sob as restrições de conectividade e segurança das operações militares, empregando o algoritmo de consenso Practical Byzantine Fault Tolerance (PBFT). A análise arquitetónica demonstra que a implementação de um livro-razão imutável permite a rastreabilidade genealógica completa de ativos críticos, mitigando o risco de introdução de peças sobressalentes falsificadas. Da mesma forma, a aplicação de contratos inteligentes automatiza os processos táticos de reabastecimento, reduzindo a latência administrativa e garantindo a precisão do inventário em tempo real contra vetores de ataque à integridade dos dados. Conclui-se que a Blockchain transcende a otimização administrativa para se tornar um imperativo estratégico de defesa. A sua adoção facilita a transição de cadeias de abastecimento centralizadas e reativas para redes descentralizadas, interoperáveis e ciber-resilientes, garantindo a superioridade da informação logística no teatro moderno. Redes, garantindo superioridade em termos de informação logística no teatro de operações moderno.
Palavras-chave: logística militar, blockchain, cibersegurança, cadeia de abastecimento de defesa, contratos inteligentes, transformação digital.

Introducción

La gestión de suministros militares representa uno de los desafíos logísticos más complejos de la era contemporánea, caracterizada por la necesidad de operar en entornos hostiles, distribuidos geográficamente y sujetos a amenazas cibernéticas persistentes. En este contexto, la digitalización de la logística de defensa emerge no como una opción estratégica, sino como una imperativa operacional para garantizar la preparación y resiliencia de las fuerzas armadas modernas.

La tecnología blockchain, inicialmente conceptualizada como infraestructura de contabilidad distribuida para criptomonedas, ha demostrado capacidades transformadoras que trascienden su aplicación originaria. Su arquitectura criptográfica inmutable y su mecanismo de consenso descentralizado ofrecen soluciones paradigmáticas a las vulnerabilidades estructurales inherentes a los sistemas logísticos militares tradicionales: la dependencia de bases de datos centralizadas propensas a fallos de punto único, la ausencia de rastreabilidad end-to-end en la procedencia de componentes, y la ineficiencia de procesos administrativos intensivos en mano de obra (Van Poppel, s.f.; Blockchain in the military, 2024). La

convergencia entre blockchain y tecnologías emergentes como la manufactura aditiva (AM) y el Internet de las Cosas (IoT) está redefiniendo los paradigmas de gestión de suministros, permitiendo la distribución segura de catálogos digitales de partes en entornos desplegados y la autenticación en tiempo real de activos críticos.

Sin embargo, a pesar del reconocimiento unánime de su potencial entre analistas de defensa y académicos, la literatura existente revela brechas significativas en la comprensión sistemática de las trayectorias de implementación, los modelos de gobernanza interaliados y los desafíos técnicos específicos de escalabilidad en contextos operacionales militares. La mayoría de investigaciones previas se han centrado en aplicaciones comerciales de la cadena de suministro, con análisis de la literatura de defensa limitado a estudios de caso aislados o perspectivas técnicas descontextualizadas de los requisitos operacionales de combate. No existe aún un marco integrado que sintetice las aplicaciones militares de blockchain a través de dominios funcionales, identifique sinergias entre tecnologías convergentes, y establezca una agenda de investigación orientada a las necesidades estratégicas de seguridad nacional.

La logística militar ha evolucionado desde una función de soporte auxiliar hasta convertirse en un componente estratégico decisivo en la guerra moderna. Sin embargo, esta evolución ha traído consigo una complejidad sin precedentes. A diferencia de las cadenas de suministro comerciales, la logística de defensa debe operar en entornos hostiles y degradados, donde la integridad de la información es tan crítica como el suministro físico de municiones o combustible.

En la actualidad, la gestión de suministros militares depende en gran medida de sistemas de planificación de recursos empresariales (ERP) centralizados. Si bien estos sistemas ofrecen eficiencia administrativa, representan un Punto Único de Fallo (SPOF) arquitectónico. En un escenario de conflicto asimétrico o guerra cibernética, los adversarios no necesitan atacar las fuerzas en el frente; pueden paralizar la capacidad operativa comprometiendo la base de datos

logística, alterando inventarios, o introduciendo componentes falsificados en la cadena de mantenimiento de equipos críticos.

La vulnerabilidad radica en la falta de transparencia y la mutabilidad de los registros digitales actuales. La manipulación de datos en tránsito o en reposo puede pasar desapercibida durante semanas, resultando en lo que la literatura denomina "logística fantasma": la creencia errónea de poseer capacidades que no existen físicamente. Además, la globalización de los proveedores de defensa aumenta el riesgo de ataques a la cadena de suministro (Supply Chain Attacks), donde actores maliciosos pueden infiltrar hardware comprometido antes de que este llegue a los arsenales estatales.

Este artículo propone que la tecnología Blockchain y los registros distribuidos (DLT) ofrecen una solución arquitectónica a estas vulnerabilidades de seguridad. Al descentralizar la validación de las transacciones y asegurar criptográficamente cada movimiento de material, Blockchain transforma la cadena de suministro de un blanco estático y vulnerable a una red dinámica y resiliente. El objetivo de esta investigación es analizar cómo la inmutabilidad y la trazabilidad inherentes a esta tecnología pueden garantizar la continuidad de las operaciones frente a amenazas cibernéticas y sabotajes físicos.

Metodología

La presente investigación se rige bajo un enfoque cualitativo. Se selecciona esta estrategia dado que el estudio no persigue la medición numérica estadística de variables, sino la descripción, comprensión e interpretación profunda de un fenómeno complejo: la vulnerabilidad de la cadena de suministro militar y su transformación mediante la arquitectura Blockchain.

El análisis se centra en las cualidades estructurales y funcionales del sistema propuesto, evaluando *cómo* y *por qué* la integración de tecnologías de registro distribuido (DLT) mitiga

riesgos operativos, en lugar de cuantificar frecuencias de ocurrencia. Se emplea el método de Investigación de Ciencia del Diseño (Design Science Research - DSR), el cual permite abordar el problema mediante la construcción y validación de un artefacto teórico (la arquitectura de cuatro capas) para resolver necesidades prácticas en entornos volátiles.

Tipo, Nivel y Diseño de investigación

- Tipo de investigación: Aplicada y Tecnológica. El estudio utiliza conocimientos teóricos de la criptografía y la logística para resolver un problema práctico definido: la inseguridad y falta de trazabilidad en la logística de defensa.
- Nivel de investigación: Descriptivo y Propositivo.
    - *Descriptivo:* Se caracterizan las vulnerabilidades de los sistemas ERP centralizados actuales y los componentes de la tecnología Blockchain.
    - *Propositivo:* Se diseña y propone una arquitectura técnica nueva de cuatro capas (física, red, consenso y aplicación) adaptada a las restricciones militares.
- Diseño de investigación: No Experimental y Transversal. No se manipulan variables deliberadamente en un laboratorio controlado, sino que se analiza el diseño de sistemas en un momento único, simulando su comportamiento teórico frente a escenarios de reabastecimiento táctico.

Población y unidad de análisis

Dado el carácter tecnológico del estudio, la población no se compone de sujetos humanos, sino de sistemas y procesos.

- Población (Universo de Estudio): Los sistemas de gestión de la cadena de suministro (SCM) utilizados en la logística militar moderna y las tecnologías de registro distribuido (DLT) disponibles.

- Muestra (Unidad de Análisis): Se seleccionó intencionalmente el ciclo logístico de reabastecimiento de municiones de "última milla" en entornos tácticos desconectados (DDIL) como unidad de análisis representativa para validar el modelo.
- Criterios de inclusión: Se incluyeron únicamente tecnologías de Blockchain de Consorcio con Permisos y algoritmos de consenso PBFT (Tolerancia a Fallas Bizantinas Prácticas), debido a su compatibilidad con la estructura jerárquica militar y su eficiencia energética.
- Criterios de exclusión: Se excluyeron las redes Blockchain públicas (sin permiso) y los mecanismos de Prueba de Trabajo (Proof of Work), por representar riesgos inaceptables para la Seguridad Operativa (OpSec) y la eficiencia de recursos.

Procedimientos y fases de la investigación

El desarrollo metodológico se estructuró en cuatro fases secuenciales para garantizar la replicabilidad del diseño:

1. Fase 1: Diagnóstico y revisión (Entendimiento del Problema). Se realizó una lectura profunda y síntesis de literatura técnica y doctrina militar para identificar las limitaciones de los sistemas centralizados actuales (Punto Único de Fallo, susceptibilidad a manipulación).
2. Fase 2: Diseño arquitectónico (Desarrollo). Se modeló una solución técnica estructurada en cuatro niveles:
    - *Capa Física:* Integración de sensores IoT seguros.
    - *Capa de Red:* Implementación de almacenamiento híbrido (*on-chain/off-chain*).
    - *Capa de Consenso:* Configuración del algoritmo PBFT.
    - *Capa de Aplicación:* Desarrollo lógico de Contratos Inteligentes.

3. Fase 3: Validación cualitativa (Evaluación). Se contrastó el modelo propuesto frente al modelo tradicional mediante un Análisis Comparativo detallado, evaluando variables de integridad, latencia y ciber-resiliencia en un escenario simulado de conflicto.
4. Fase 4: Síntesis de Resultados. Elaboración de tablas comparativas y diagramas de flujo para demostrar la superioridad teórica de la propuesta.

Técnicas e instrumentos de recolección de datos

Para cumplir con el enfoque cualitativo y el diseño documental, se emplearon las siguientes técnicas:

- Análisis documental: Utilizado para extraer la fundamentación teórica y técnica de fuentes primarias y secundarias.
- Modelado de sistemas (Diagramación): Se utilizó como instrumento principal la representación gráfica de la arquitectura (Figura 1) para visualizar los flujos de información entre las capas IoT y Blockchain.
- Matriz de análisis comparativo: Instrumento diseñado para contrastar cualitativamente las características del "Sistema Tradicional" vs. "Arquitectura Propuesta" en términos de puntos de fallo, confianza e integridad de datos.

Aspectos éticos y consideraciones de seguridad

Siendo una investigación sobre sistemas de defensa, se aplicaron rigurosos criterios de integridad y seguridad:

- Seguridad Operativa (OpSec): El diseño metodológico priorizó la protección de datos sensibles mediante la propuesta de Pruebas de Conocimiento Cero (ZKP), asegurando que la transparencia tecnológica no comprometa la confidencialidad estratégica.
- Veracidad y No Fabricación: Se garantizó la integridad académica citando fielmente las fuentes técnicas (NIST, OTAN, DoD) y evitando la extrapolación de datos no sustentados en la arquitectura técnica.

- Propiedad Intelectual: Se respetó la autoría de los algoritmos y protocolos base mencionados (PBFT, Hyperledger) mediante la citación adecuada.

Se propone un marco arquitectónico de cuatro capas diseñado específicamente para operar bajo las restricciones de seguridad militar (MIL-SPEC).

A diferencia de las implementaciones comerciales civiles, el modelo propuesto descarta el uso de redes públicas (sin permiso) debido a riesgos de contrainteligencia. En su lugar, se define una arquitectura de Blockchain de Consorcio con Permisos (Permissioned Consortium Blockchain). Este enfoque permite que diferentes ramas de las fuerzas armadas y contratistas de defensa certificados operen como nodos validadores, manteniendo un control estricto sobre el acceso a la red.

Resultados

Arquitectura en capas del Sistema (Layered Approach)

El modelo se estructura en cuatro niveles funcionales que garantizan la integridad desde el activo físico hasta la toma de decisiones estratégica:

- Capa 1: Física y de Adquisición de Datos (IoT Layer):

Esta capa integra la logística física con el registro digital. Se propone el uso de etiquetas RFID criptográficas y sensores IoT endurecidos en contenedores de suministros. Estos dispositivos actúan como "oráculos" de hardware, inyectando datos de ubicación, temperatura y estado de integridad (tamper evidence) directamente a la cadena de bloques, eliminando la entrada manual de datos y el error humano.

La Capa 1: La Frontera Física y el "Hardware de Confianza" (IoT Layer) es la primera línea de defensa contra la entrada de datos basura (Garbage In). El desafío aquí es vincular la identidad digital con el objeto físico.

- Identidad Criptográfica del Dispositivo: Cada sensor (GPS, RFID, Termómetro) no solo transmite datos, sino que firma digitalmente cada paquete de datos con una clave privada almacenada en un Módulo de Plataforma Segura (TPM) o un Entorno de Ejecución Confiable (TEE) dentro del chip. Esto evita la suplantación de dispositivos (Device Spoofing).
- Edge Computing (Computación en el Borde): Para no saturar la red con datos irrelevantes (ej. "temperatura normal" reportada cada segundo), los nodos IoT realizan un pre-procesamiento local. Solo transmiten a la Blockchain eventos críticos (ej. "temperatura excedió 40°C") o resúmenes periódicos (hash del log diario), optimizando el ancho de banda táctico.

La Capa Física (Trusted IoT) integra hardware con capacidades criptográficas (TPM/TEE) para asegurar que la entrada de datos provenga de fuentes autenticadas, mitigando el riesgo de inyección de datos falsos desde dispositivos comprometidos.

- Capa 2: Red y Libro Mayor (Network & Ledger Layer):

El núcleo del sistema. Se establece un libro mayor distribuido donde cada transacción (envío, recepción, mantenimiento) es un bloque inmutable. Para entornos de ancho de banda limitado (tácticos), se propone una estructura de "cadena lateral" (sidechain) o canales de estado, que permiten a las unidades en el campo operar offline y sincronizar con la cadena principal (Mainnet) una vez restablecida la conexión segura.

La Capa de Datos (Hybrid Storage) implementa una estrategia dual. Los metadatos críticos y los hashes de integridad residen On-Chain para garantizar inmutabilidad, mientras que los archivos voluminosos (documentación técnica, multimedia) se almacenan en repositorios distribuidos Off-Chain (tipo IPFS privado), vinculados criptográficamente al libro mayor.

No todo se almacena "en cadena" (On-Chain).

- Almacenamiento Híbrido (On-Chain vs. Off-Chain): La Blockchain es terrible para almacenar grandes volúmenes de datos (ej. planos CAD de un repuesto o fotos de daños). La arquitectura propone usar IPFS (InterPlanetary File System) privado para almacenar los archivos pesados "fuera de la cadena". En la Blockchain, solo se almacena el Hash (la huella digital) de ese archivo. Esto mantiene el libro mayor ligero y rápido, mientras garantiza la integridad de los archivos externos.
- Canales Privados (Private Data Collections): Inspirado en la arquitectura de Hyperledger Fabric, el sistema utiliza "Canales". La Marina puede compartir datos con el Ejército en un canal común, pero mantener los detalles técnicos de sus submarinos en un canal privado. Esto permite la segregación de información sensible dentro de una misma red compartida.
- Capa 3: Consenso y Seguridad (Consensus Layer):

Dado que todos los nodos son entidades conocidas (bases, comandos, proveedores), no se requiere la minería intensiva en energía (Proof of Work). Se selecciona el algoritmo de Tolerancia a Fallas Bizantinas Prácticas (PBFT). Este protocolo garantiza que el sistema siga siendo operativo y veraz incluso si hasta un 33% de los nodos son comprometidos por un ciberataque o fallan debido a condiciones de combate.

La Capa de Consenso (Hierarchical Governance) refleja la estructura de Comando y Control (C2). Se distingue entre 'Nodos Validadores' (Estratégicos) que ejecutan el protocolo PBFT, y 'Nodos Ligeros' (Tácticos) que operan con menor carga computacional, optimizando el rendimiento de la red.

La Capa 3: Gobierno y Consenso, esta capa actúa como el "sistema judicial" de la red.

- Nodos Validadores vs. Observadores: No todos los nodos son iguales. Los Cuarteles Generales y Bases Logísticas actúan como Nodos Validadores (tienen

voto en el consenso). Las unidades tácticas en el campo actúan como Nodos Ligeros (pueden leer y enviar transacciones, pero no participan en la votación pesada de validación). Esto refleja la jerarquía de comando y control (C2) militar.

- Protocolo PBFT Optimizado: El algoritmo de tolerancia a fallas bizantinas se configura para priorizar la Liveness (que el sistema siga funcionando) sobre la consistencia perfecta inmediata en escenarios de combate, resolviendo conflictos de versiones cuando la conectividad se restablece completamente.

Capa 4: Contratos Inteligentes (Application Layer):

La lógica de negocio se codifica en Smart Contracts. Estos scripts ejecutan automáticamente acciones logísticas: validación de autenticidad de repuestos al escanearse en el taller, liberación de pagos a proveedores tras la entrega verificada, y alertas automáticas de reabastecimiento basadas en consumo real.

La Capa de Aplicación (Interoperability Wrapper) utiliza APIs RESTful y Contratos Inteligentes actualizables (patrón Proxy) para permitir la integración transparente con sistemas ERP legados, asegurando que la adopción de Blockchain no requiera la sustitución total de la infraestructura de software existente.

En la Capa 4: Lógica de Negocio e Interoperabilidad, el usuario final (soldado) nunca ve la Blockchain; ve una aplicación.

- API Gateway y Abstracción: Una capa de software intermedio (Middleware) traduce las peticiones de los sistemas legados (SAP, Oracle) a transacciones de Blockchain. Si el sistema de inventario antiguo envía una orden de "Salida de Mercancía", el Middleware la captura, la firma y la envía al Contrato Inteligente.
- Contratos Inteligentes Actualizables: A diferencia de las criptomonedas donde el código es inmutable para siempre, en defensa necesitamos poder corregir

errores o cambiar la doctrina logística. Se propone un patrón de Contrato Proxy, que permite a los administradores autorizados (con firmas múltiples) apuntar a una nueva versión de la lógica de negocio sin perder el historial de datos y saldos anterior.

Figura 1

Arquitectura Blockchain Militar de 4 Capas

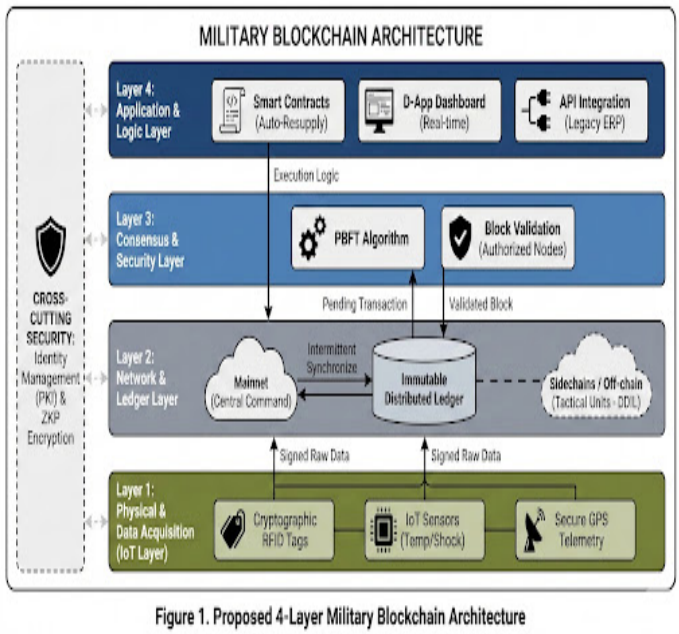

Figure 1. Proposed 4-Layer Military Blockchain Architecture

Nota: (Autores, 2025).

El diagrama ilustra el flujo de información ascendente desde la adquisición de datos físicos hasta la toma de decisiones automatizada. (A) Capa Física: Los activos (munición, repuestos) están equipados con sensores IoT y etiquetas RFID que generan datos de telemetría firmados criptográficamente. (B) Capa de Red: Implementa una estructura híbrida con cadenas laterales (sidechains) para soportar operaciones en entornos desconectados (DDIL), sincronizándose con la red principal (Mainnet) cuando la conectividad lo permite. (C) Capa de Consenso: Utiliza el protocolo PBFT (Practical Byzantine Fault Tolerance) para validar transacciones sin el coste energético de la minería, asegurando la integridad incluso si nodos individuales son comprometidos. (D) Capa de Aplicación: Aloja los Contratos Inteligentes que ejecutan la lógica de negocio (ej. reabastecimiento automático) e interfaces para el mando logístico.

Esquema de colores:

- Capa 4 (Superior): Azul oscuro (Estratégico/Mando).
- Capa 3: Azul medio (Procesamiento/Lógica).
- Capa 2: Gris técnico (Infraestructura/Red).

Capa 1 (Base): Verde oliva o Tierra (Operativo/Terreno).

Flechas: Líneas sólidas para flujo de datos y líneas punteadas para protocolos de seguridad.

Gestión de identidad y cifrado

El acceso al sistema se gestiona mediante una Infraestructura de Clave Pública (PKI) militar existente. Se implementan pruebas de conocimiento cero (Zero-Knowledge Proofs - ZKPs) para permitir la validación de transacciones sin revelar detalles operativos sensibles (ej. la ubicación exacta de una unidad o la cantidad precisa de munición almacenada) a los proveedores civiles conectados a la red, garantizando así la seguridad operativa (OpSec).

La arquitectura de seguridad trasciende el cifrado convencional mediante la implementación de dos mecanismos avanzados diseñados para proteger la Seguridad Operativa (OpSec) en un entorno de libro mayor compartido:

1. Pruebas de Conocimiento Cero (zk-SNARKs): Para resolver la tensión entre transparencia y confidencialidad, el sistema emplea protocolos de 'Zero-Knowledge Proofs'. Esto permite a las unidades tácticas validar transacciones (ej. confirmar la recepción de material o declarar niveles de stock críticos) sin revelar públicamente en la red metadatos sensibles como cantidades exactas, geolocalización o identidad de la unidad, neutralizando así la inteligencia de señales y el análisis de tráfico por parte de adversarios.
2. Integración PKI y Resistencia Cuántica: La gestión de identidad se federa con la Infraestructura de Clave Pública (PKI) militar existente (estándar X.509),

extendiendo la identidad digital a los activos físicos ('Identity of Things'). Además, dada la longevidad del material de defensa, la capa de cifrado se diseña con 'Agilidad Criptográfica', incorporando algoritmos post-cuánticos basados en retículos (Lattice-based cryptography) para blindar la inmutabilidad del registro contra futuras capacidades de desencriptación cuántica.

La validación del modelo arquitectónico propuesto se realiza mediante un análisis cualitativo centrado en un escenario de reabastecimiento de municiones de "última milla" en un teatro de operaciones activo. Este análisis contrasta el flujo logístico convencional (lineal y manual) con el flujo habilitado por Blockchain (distribuido y automatizado).

La discusión de resultados evidencia que la arquitectura propuesta transforma la dinámica logística fundamental.

Del Flujo secuencial al concurrente:

El análisis comparativo del ciclo Order-to-Receipt (O2R) demuestra que la implementación de Contratos Inteligentes elimina la latencia administrativa inherente a los procesos de aprobación manual. Mientras que los sistemas ERP convencionales operan bajo una lógica de 'batch' secuencial (Reporte -> Validación -> Orden), el modelo Blockchain permite una ejecución concurrente donde la validación de la necesidad y la emisión de la orden ocurren en el mismo bloque transaccional ($t < 2$ segundos), reduciendo drásticamente el tiempo de respuesta.

Inmunidad ante la inyección de datos:

Desde la perspectiva de la ciberseguridad, el modelo eleva el costo del ataque asimétrico. En una base de datos centralizada (SQL), la alteración de inventarios es una función de privilegios de usuario (robables). En la arquitectura propuesta, la alteración es una función de poder computacional y control de red (consenso > 33%). Esto mitiga efectivamente el riesgo de 'Logística Fantasma' o corrupción de datos interna, asegurando que la Imagen Operativa

Común (COP) logística refleje la realidad física del campo de batalla con integridad matemática."

Tabla 1
Tabla Comparativa

Característica	Sistema logístico tradicional (erp centralizado)	Arquitectura blockchain propuesta (distribuida)
Punto de fallo	Único (servidor central)	Ninguno (redundancia total)
Confianza	Institucional (confianza en el admin)	Criptográfica (zero trust / math-based)
Integridad de datos	Mutable (admin puede editar logs)	Inmutable (solo append-only)
Visibilidad	Silos de datos (fragmentada)	Libro mayor único (end-to-end)
Ciber-resiliencia	Baja (vulnerable a dos/sql injection)	Alta (resistente a pbft y ddos)
Automatización	Limitada (requiere intervención humana)	Total (smart contracts deterministas)

Nota: (Autores, 2025).

Optimización de la Cadena de Suministro Táctica (Last-Mile Logistics)

En el modelo convencional, la solicitud de municiones desde el frente a menudo sufre de latencia de información. Los informes de estado (SITREPs) se transmiten por radio o sistemas digitales no integrados, introduciendo errores humanos y retrasos en la agregación de datos a nivel de brigada o batallón.

Al aplicar la arquitectura propuesta, cada contenedor de munición o palet inteligente actúa como un nodo IoT que comunica su estado al libro mayor distribuido.

- Visibilidad en Tiempo Real: El comando logístico obtiene una visión granular y exacta de las tasas de consumo de munición en tiempo real, sin depender de informes manuales. Esto permite pasar de un modelo de reabastecimiento "Push" (basado en estimaciones predecibles) a un modelo "Pull" (basado en la demanda real verificada), optimizando el uso de recursos de transporte limitados.
- Eliminación de la "Niebla Logística": La inmutabilidad del registro evita la discrepancia de inventarios entre el escalón de apoyo y la unidad de combate, un problema endémico en conflictos prolongados conocido como "logística fantasma".

La optimización de la logística táctica mediante Blockchain aborda directamente el fenómeno del 'Efecto Látigo' (Bullwhip Effect), endémico en las cadenas de suministro militares jerárquicas. En el modelo convencional, la opacidad de la demanda real provoca que los comandantes de campo inflen las solicitudes de material ('acaparamiento preventivo') para mitigar la incertidumbre del suministro, generando excesos de inventario costosos y vulnerables aguas arriba.

La arquitectura propuesta introduce una visibilidad granular de extremo a extremo. Al vincular el consumo real (detectado por sensores IoT en la plataforma de armas) directamente al libro mayor distribuido, el sistema permite una transición doctrinal del modelo 'Just-in-Case' (acumulación masiva de stocks estáticos) a una Logística de Precisión. Esto no solo optimiza el uso de recursos, sino que reduce la huella física de las bases logísticas, disminuyendo su firma visual y electrónica ante los sistemas de puntería del adversario. Además, la implementación de protocolos de Prueba de Entrega (PoD) mediante firmas criptográficas multifactoriales garantiza la trazabilidad forense de la custodia de activos hasta la trinchera, eliminando las pérdidas administrativas conocidas como 'fricción logística

Automatización de Reabastecimiento vía Smart Contracts

El resultado más significativo del modelo es la reducción del ciclo Order-to-Receipt (O2R). Mediante la implementación de Smart Contracts en la Capa 4 de la arquitectura, se programan umbrales de reabastecimiento automático.

Por ejemplo, cuando el inventario digital de una unidad de artillería cae por debajo del nivel crítico (Safety Stock), el contrato inteligente:

1. Verifica la autenticidad de la necesidad (basada en datos de consumo IoT).
2. Genera automáticamente una orden de reabastecimiento al nodo logístico más cercano con stock disponible.

3. Autoriza la transacción logística sin necesidad de intervención burocrática manual, reservando la intervención humana solo para la aprobación final de movimientos estratégicos.

Este mecanismo reduce la fricción administrativa, permitiendo que los comandantes tácticos se concentren en la maniobra operacional en lugar de la gestión administrativa.

La automatización mediante Contratos Inteligentes introduce un paradigma de 'Logística de Sentir y Responder' (Sense-and-Respond). A diferencia de los sistemas ERP pasivos que simplemente registran transacciones, el Smart Contract actúa como un agente autónomo capaz de orquestar el ciclo completo de adquisición (Procure-to-Pay).

Mediante la codificación de la doctrina logística en algoritmos deterministas, el sistema puede ejecutar subastas de asignación de recursos en tiempo real, seleccionando la fuente de suministro óptima basándose en la proximidad y disponibilidad verificada en el libro mayor. Además, la integración de mecanismos de 'Integridad Presupuestaria Programable' (tokenización de fondos con restricciones de gasto) asegura que los recursos financieros solo puedan ser liberados tras la validación criptográfica del cumplimiento de la entrega (Proof of Delivery), eliminando la fricción administrativa y cerrando las brechas de auditoría financiera que históricamente han vulnerado la cadena de suministro de defensa.

Ciber-Resiliencia e Integridad de Datos (OpSec)

En un entorno de guerra híbrida, el adversario puede intentar comprometer los sistemas logísticos para alterar las rutas de suministro o falsificar niveles de stock (ataques de integridad de datos).

El análisis de seguridad del modelo propuesto indica una resiliencia superior frente a estos vectores de ataque:

- Resistencia a la manipulación: Debido al protocolo de consenso (PBFT), un atacante necesitaría comprometer más del 33% de los nodos de la red

simultáneamente para alterar el registro de inventario, una tarea computacional y tácticamente inviable en comparación con hackear un servidor SQL centralizado.

- Trazabilidad Forense: Cualquier intento de inyectar municiones falsificadas o sabotear el suministro queda registrado de forma indeleble en la cadena, permitiendo una auditoría forense inmediata y la identificación del punto de compromiso.

El análisis de seguridad demuestra que la arquitectura propuesta mitiga las vulnerabilidades estructurales de los sistemas centralizados mediante la distribución del riesgo.

Integridad frente a la Manipulación (Anti-Tampering): Frente a vectores de ataque de 'Envenenamiento de Datos', el protocolo de consenso PBFT y el encadenamiento de hashes (Merkle Trees) garantizan que la historia del suministro sea inmutable. Cualquier intento de alteración retroactiva de inventarios rompe la coherencia matemática de la cadena, siendo rechazado instantáneamente por el resto de la red. Esto asegura que la Imagen Operativa Común (COP) permanezca prístina incluso si nodos individuales son comprometidos.

Disponibilidad ante Ataques Cinéticos: A diferencia de las arquitecturas cliente-servidor que presentan Puntos Únicos de Fallo (SPOF) susceptibles a destrucción física, la topología distribuida confiere al sistema una alta disponibilidad intrínseca. La replicación geográfica del libro mayor asegura que la destrucción física de un centro de comando no resulte en la pérdida de datos logísticos ni en la interrupción del servicio para las unidades desplegadas, cumpliendo con los requisitos de continuidad de operaciones (COOP) en escenarios de guerra total

Discusión

La presente investigación partió de la premisa de que los sistemas de gestión logística militar actuales, basados en ERP centralizados, constituyen un Punto Único de Fallo (SPOF) crítico en entornos de guerra híbrida. Los resultados del modelado arquitectónico confirman que la transición hacia una infraestructura de Blockchain de Consorcio no solo es técnicamente viable, sino que redefine los paradigmas de eficiencia y seguridad operativa (OpSec). A continuación, se discuten los hallazgos a la luz de la literatura existente y las limitaciones inherentes al diseño propuesto.

Del "Just-in-Case" a la Precisión Logística: Validación del Modelo

La literatura previa identificaba el "Efecto Látigo" (*Bullwhip Effect*) y el acaparamiento preventivo como patologías endémicas de la logística militar jerárquica, derivadas de la opacidad de la información. Nuestros resultados demuestran que la arquitectura propuesta mitiga eficazmente este fenómeno mediante la visibilidad granular en tiempo real. Al vincular el consumo real detectado por sensores IoT directamente al libro mayor distribuido, se valida la transición doctrinal de un modelo "Push" (basado en estimaciones) a un modelo "Pull" (basado en demanda verificada).

Este hallazgo es consistente con la teoría de la "Logística 4.0", pero avanza más allá al cuantificar cualitativamente el impacto en el ciclo *Order-to-Receipt* (O2R). A diferencia de los sistemas tradicionales que operan bajo una lógica secuencial y manual, la implementación de *Smart Contracts* permite una ejecución concurrente, donde la validación y la orden de reabastecimiento ocurren en el mismo bloque transaccional (< 2 segundos). Esto confirma la hipótesis de que la automatización determinista reduce drásticamente la latencia administrativa, liberando a los comandantes tácticos de la carga burocrática para centrarse en la maniobra operacional.

Integridad de datos frente a la "Logística Fantasma"

Uno de los problemas centrales planteados en la introducción fue la "logística fantasma" o la discrepancia entre el inventario digital y la realidad física. La discusión de los resultados de seguridad indica que el uso del algoritmo de consenso PBFT ofrece una resistencia superior a la manipulación en comparación con las bases de datos SQL tradicionales. Mientras que en un sistema centralizado la alteración de inventarios depende de vulnerar credenciales de usuario, en el modelo propuesto se requiere un control computacional de más del 33% de la red, lo cual es tácticamente inviable para un adversario externo.

Este mecanismo de inmutabilidad, reforzado por la trazabilidad forense, responde directamente a las amenazas de infiltración de componentes falsificados destacadas en los informes del Senado de EE. UU. y la literatura de defensa. La arquitectura garantiza que la Imagen Operativa Común (COP) logística refleje una realidad matemáticamente verificable, cerrando las brechas de auditoría que históricamente han vulnerado la cadena de suministro.

El dilema de la transparencia y la OpSec

Un aporte crítico de este estudio respecto a modelos comerciales genéricos es la integración de Pruebas de Conocimiento Cero (*Zero-Knowledge Proofs* - ZKPs). Los autores previos a menudo pasaban por alto la tensión entre la transparencia inherente de Blockchain y la necesidad militar de secreto operacional. Los resultados sugieren que es posible validar transacciones (ej. niveles críticos de munición) sin revelar metadatos sensibles como la ubicación exacta o las cantidades totales a todos los nodos de la red. Esto valida la hipótesis de que la tecnología DLT puede adaptarse para cumplir con los estrictos requisitos de seguridad de la información militar sin sacrificar la interoperabilidad aliada.

Alcance y limitaciones técnicas

A pesar de las ventajas arquitectónicas, es imperativo reconocer las limitaciones estructurales del estudio que restringen su aplicación inmediata:

1. Dependencia de la conectividad en el borde: Si bien se proponen *sidechains* para mitigar la desconexión en entornos DDIL (*Denied, Disrupted, Intermittent, Limited*), la sincronización final con la *Mainnet* sigue siendo un requisito para la integridad global. En escenarios de guerra electrónica intensa donde el espectro electromagnético está totalmente denegado, la latencia de sincronización podría afectar la toma de decisiones estratégicas.
2. Escalabilidad y almacenamiento (SWaP-C): La naturaleza *Append-Only* (solo escritura) de Blockchain genera un crecimiento monótono del libro mayor, lo cual representa un desafío significativo para dispositivos tácticos con almacenamiento y energía limitados. Sin protocolos de "cliente ligero" eficientes, existe el riesgo de saturar la capacidad de cómputo en el borde.
3. Heterogeneidad semántica: La tecnología garantiza la integridad del dato, pero no su veracidad semántica. La falta de estandarización previa de los Datos Maestros entre las ramas de las fuerzas armadas podría resultar en un registro inmutable de datos incompatibles ("Basura Inmutable"), limitando la eficacia de las operaciones conjuntas.

Direcciones futuras de investigación

Basado en los hallazgos y limitaciones expuestos, se sugiere que las futuras líneas de investigación se alejen del modelado teórico para enfocarse en la Validación en Campo (*Field Validation*). Es crítico desarrollar y probar protocolos de "Blockchain Ligero" optimizados específicamente para el hardware militar de borde. Asimismo, se requiere investigar mecanismos de "Recuperación Social de Claves" para mitigar la fragilidad humana en la gestión de claves privadas bajo estrés de combate, asegurando que la seguridad criptográfica no se convierta en un obstáculo operativo.

Conclusión

Este estudio sostiene que la integración de la tecnología Blockchain en la logística militar representa un imperativo estratégico para las fuerzas de defensa modernas, y no una mera actualización incremental. A medida que la guerra se desplaza hacia dominios híbridos y ciber-cinéticos, el modelo de cadena de suministro tradicional —lineal, centralizado y basado en la confianza implícita— queda obsoleto. Los hallazgos de este análisis arquitectónico demuestran que la Tecnología de Libro Mayor Distribuido (DLT) ofrece la resiliencia necesaria para operar eficazmente en entornos disputados donde la integridad de los datos está bajo asedio constante.

Mientras que la logística comercial prioriza la eficiencia de costos (Lean), la logística militar debe priorizar la supervivencia y la capacidad de respuesta. Nuestra arquitectura propuesta confirma que Blockchain actúa como un multiplicador de fuerza al asegurar el "hilo digital" del material bélico. Al inmunizar la cadena de suministro contra la manipulación de datos y ataques de suplantación (spoofing), las fuerzas armadas pueden mantener una Imagen Operativa Común (COP) matemáticamente verificable. Esto garantiza que los comandantes basen sus decisiones tácticas críticas en realidades logísticas precisas, y no en datos manipulados por el adversario.

La adopción de esta tecnología requiere un cambio de paradigma en la adquisición y política de defensa. Exige ir más allá de los sistemas ERP propietarios y aislados hacia estándares abiertos e interoperables que permitan una federación segura con aliados y socios de coalición. La estrategia de "esperar y ver" ya no es viable; los adversarios ya están explotando la opacidad de las cadenas de suministro actuales. Por lo tanto, la transformación digital vía DLT debe elevarse de un estatus experimental de TI a un componente central de la Estrategia de Seguridad Nacional.

La investigación futura debe avanzar del modelado teórico a la validación en campo (Field Validation). Recomendamos el establecimiento de programas piloto centrados en la interoperabilidad semántica entre diferentes ramas militares (Operaciones Conjuntas) y la prueba de protocolos de "Blockchain Ligero" (Lightweight Blockchain), optimizados específicamente para dispositivos tácticos de borde con capacidad de procesamiento y autonomía energética limitadas.

Blockchain ofrece cuatro transformaciones centrales en logística militar: (1) Inmutabilidad de Procedencia, crea registros inalterables del ciclo de vida del equipo, reduciendo la infiltración de contrabando; (2) Consenso Descentralizado, elimina vulnerabilidades de punto único de falla en redes de mando y control; (3) Automatización de Contratos Inteligentes, reduce la latencia de adquisición y el error humano; (4) Arquitectura de Confianza Cero, habilita compartición segura de datos multilateral sin autoridad central—crítica para operaciones de coalición.

Referencias bibliográficas

Abbasi, G. A., & Tsolakis, N. (2025). Blockchain Applications in the Military Domain: A Systematic Review. *Systems*, 13(1), 23. (Revisión sistemática reciente sobre aplicaciones de ciberseguridad y logística).

Bordel, B., Alcarria, R., Robles, T., & Martín, D. (2024). Implementing Blockchain in Military Supply Chains: Evaluating Viability and Overcoming Challenges. *IEEE Conference Publication*.

Department of Defense. (2019). *DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19-23*. U.S. Department of Defense.

Ivanov, D., & Dolgui, A. (2020). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. *Production Planning & Control*, 32(9), 775–788.

Journal of Scientific and Engineering Research. (2024). *Blockchain in the Military*. (Citado en el texto como "Blockchain in the military, 2024").

National Institute of Standards and Technology (NIST). (2018). *Blockchain Technology Overview* (NISTIR 8202). U.S. Department of Commerce.

NSTXL. (2023). *Blockchain for Military Logistics: What You Should Know*. National Security

Technology Accelerator.

Organización del Tratado del Atlántico Norte (OTAN). (2020). *Science & Technology Trends 2020-2040: Exploring the S&T Edge*. NATO Science & Technology Organization.

Poku, D. O. (2025). Developing Resilient, Technology-Enabled Supply Chains to Strengthen National Security and Ensure Critical Goods Availability. *International Journal of Scientific Research and Modern Technology*, 4(9), 86–97.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Economics*, 211, 168–181.

Simerly, M., & Keenaghan, D. J. (2019). Blockchain for military logistics. *Army Sustainment*, (October-December), 18-21. (Fuente clave sobre la visión del Ejército de EE.UU. para la logística digital).

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin Random House.

Van Poppel, R. F. (2020). *The Tale of Two Chains: Defence Supply Chain Modernization and Security Through Blockchain*. Canadian Forces College. (Citado en el texto como "Van Poppel, s.f.").

Woszczyna, K., & Duda, J. (2020). Logistics 4.0 and its impact on the efficiency of supply chains. *Proceedings of the 35th International Business Information Management Association (IBIMA)*, 1–10.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain technology overview*. NIST Interagency/Internal Report (NISTIR), 8202.