Review

Blockchain Applications in the Military Domain: A Systematic Review

Nikos Kostopoulos , Yannis C. Stamatiou , Constantinos Halkiopoulos * , Hera Antonopoulou

Posted Date: 28 November 2024

doi: 10.20944/preprints202411.2266.v1

Keywords: Blockchain Technology; Military Operations; Data Security; Secure Communication; Supply Chain Management; Smart Contracts; Cybersecurity; Scalability; Interoperability; Operational Efficiency

 doi:10.20944/preprints202411.2266.v1

Review

Blockchain Applications in the Military Domain: A Systematic Review

Nikos Kostopoulos [1], Yannis C. Stamatiou [2], Constantinos Halkiopoulos [1,*] and Hera Antonopoulou [1]

[1] Department of Management Science and Technology, University of Patras, 26334 Patras, Greece
[2] Computer Technology Institute and Press "Diophantus", University of Patras Campus, 26504 Patras, Greece
* Correspondence: halkion@upatras.gr

Abstract: *Background:* Blockchain technology can be transformative in military operations, increasing security, transparency, and gaining efficiency. It addresses many of the problems related to data security, privacy, communication, and supply chain management. Those aspects that have been most researched are its integration with emerging technologies, such as artificial intelligence, IoT, application in unmanned aerial vehicles, and secure communications; *Methods:* A systematic review of 43 peer-reviewed articles was performed to find out the applications of blockchain in defense. Key areas analyzed include the role of blockchain in securing communications, fostering transparency, promoting real-time data sharing, and using smart contracts for maintenance management. Challenges were assessed, including scalability, interoperability, and integration with the legacy system, alongside possible solutions, such as sharding and optimized consensus mechanisms; *Results*: In the case of blockchain, great potential benefits were shown in enhancing military operations, including secure communication, immutable record-keeping, and real-time integration of data with IoT and AI. Smart contracts optimized resource allocation and reduced maintenance procedures. However, challenges remain, such as in scalability, interoperability, and high energy requirements. Proposed solutions like sharding and hybrid architecture show promise to address these issues; *Conclusions*: Blockchain is set to revolutionize the efficiency and security of the military. Its potential is huge, but it must overcome issues of scalability, interoperability, and integration. Further research and strategic adoption will thus allow blockchain to become one of the cornerstones of future military operations.

Keywords: blockchain technology; military operations; data security; secure communication; supply chain management; smart contracts; cybersecurity; scalability; interoperability; operational efficiency

1. Introduction

In the evolving landscape of military operations, technology has played an increasingly important role in the digital platforms of today. Our military decision-making process relies heavily on the algorithms and the digital platforms that support complex decision-making processes. In the last few decades, information technology and communication have made rapid strides in the administrative, economic, and financial sectors. The same revolution has largely bypassed the military camp, even though it has been a crucial facilitator in peacekeeping operations. The growing dependency of commanders on technology and electronic information systems for accurate, time-critical operational decisions has been identified in recent years as a call for secure electronic operations in the information age. In the military domain, time is often the most valuable resource. Therefore, efficiency, security, and confidentiality are essential [1–6]. Upgrading computer networking systems and software provides new opportunities for the military domain. Blockchain's advantages could be seamlessly integrated to help solve a myriad of modern military problems and digitize systems that historically operated in non-interoperable and isolated technological environments. It focuses on applications of blockchain technology in military operations, log

 doi:10.20944/preprints202411.2266.v1

management, health records, supply, logistics, equipment, training and exercises, defense production, and acquisition and procurement [7–14].

Background and Overview of Blockchain Technology

While originally created as a basis for cryptocurrencies such as Bitcoin, Blockchain technology has, gradually, transformed into a general-purpose distributed computational structure with a wide range of applications beyond cryptocurrencies. Today's military environment is shaped by continual technological growth, complicated operational environments, and an increasing reliance on evidence and data to inform decisions across the military. Established systems of record maintenance, accountability, communication, and logistics generally face challenges related to security, efficiency, and precision. Thus, military establishments around the world are testing new data technologies that meet these challenges head-on. One candidate, blockchain technology, has continued to emerge, with its distributed, secure, and transparent functionality, as one that may improve multiple aspects of military operations [13–17]. In general, the Blockchain is a decentralized ledger structure that supports the secure, transparent, and tamper-free archiving of information and data among a set of nodes (e.g. individual or agencies) in a communications network. In the military domain trust, information and data security, data integrity, and transaction transparency are considered priority issues. Blockchain's tamper-free properties can significantly enhance the security and safety of military actions, promoting operations efficiency and ensuring fast access to reliable information [18–26]. The primary objective of this paper is to conceptually explore potential applications of blockchain technology in the military domain. That is to say, the identification of important application areas within the military domain where blockchain could be useful to enhance and secure key operations; consideration of the key benefits and challenges in the implementation of blockchain in those areas; and recommendations for future research and development goals that can overcome the challenges impeding a wider adoption of blockchain in the military domain.

2. Military Applications of Blockchain Technology

Blockchain technology has gained significant popularity in recent years across various non-defense sectors. It has recently shown a significant influence in the military domain and is depicted as having a broad scope of practice. Here, blockchain technology improves military information technology and assists in the development of data management. Supply chain problems are reduced considerably through robust and tender transmission of funds to different vendors and further utilize blockchain for protecting log data. Blockchain technology is also utilized for secure password transmission to various users by reducing unauthorized use. Likewise, blockchain might also render secure communication between establishments during coordination in multiple settings. It has developed privacy-preserving frameworks that are essential for military data transmission and multidisciplinary approaches that enhance precision weapons for efficient strikes, making the program more efficient and effective like several other defense and scientific applications [27–29]. Blockchain technology is of significant interest in enhancing defense operations for a more effective research foundation, new initiative creation, and commercialized technology application. Successful military forces need steady support and adequately coordinated assets in terms of additional resources, logistics, manpower, and money. Innovations like blockchain are particularly important for the military supply chain that is under challenging environments. This global assessment discusses the adoption rate and actual operational efficiency of this technology. There are various blockchain applications in the military domain. A plan has been set forth to utilize monitoring games in terms of implementation after a detailed blockchain technology analysis by eliminating significant cost burdens. Additionally, blockchain technology has operational efficiency. However, such an application could face security issues and cyber threats in the future. This application is currently experiencing slow adoptions [30–35].

 doi:10.20944/preprints202411.2266.v1

2.1. Supply Chain Management

In military applications, blockchain technology can revolutionize the way in which the supply chain is managed. Traditional supply chains are vulnerable to various types of fraud and misuse, which include theft, smuggling, and fraudulent transactions. Consequently, supply chains face issues of transparency, availability, and delay. Blockchain technologies can maintain a secure distributed ledger of all transactions that can be accessed by authorized individuals, which can help reduce delays and provide near-real-time information on the movement of supplies. When new transactions occur, they are added to existing ledger blocks in a secure way, making this technology tamper-proof. Many commercial organizations use blockchain for tracking products in the supply chain to ensure their supplies, such as food, are fresh [36–41]. For several years, managing military logistics has been recognized as one of the key driving areas for integrating blockchain in the military domain. Military logistics require the provision of all necessary military supplies and inputs to support military operations, including manpower, food, equipment, and ammunition. Some of the challenges in military logistics include the need for a large logistics workforce, dealing with uncertainties and natural disasters in the environment, the need for remote logistics management, and the need to postpone the need for logistics resources in a possible contingency case. Blockchain technology can help in this context by first enabling a more cost-efficient allocation of resources. Real-time visibility and insight into peacetime activities and resources can make future planning more informed and accurate than before. A variety of case studies have been summarized in the literature on the application of blockchain technology to optimize military logistics, including but not limited to food supply chain case studies, inventory management, and supply chain finance. Several military organizations have also undertaken blockchain pilots in logistics to test the effectiveness of these approaches. The UK army has conducted internal exercises on the potential use of blockchain for logistics support. Blockchain can make military logistics more resilient and cost-effective by improving connectivity and trust between different members of the global military logistics network [42–44].

2.2. Secure Communication and Data Sharing

Sharing data is critical in joint military operations. Lack of information can lead to mission failure. The promise of blockchain for secure communication and data sharing in a military domain stem from the vulnerabilities of traditional methods of data and communication. Blockchain ensures tamper-evident and authenticated end-to-end communication by encrypting the data payload and storing the encrypted key on the ledger. End users hold the private keys, and only they can unlock the data. End-to-end encryption reduces the attack surface as the attacker has fewer places to attack. Communication can be further hardened with the addition of decentralized communication channels using peer-to-peer or client-server architecture. Unlike traditional communication systems, the blockchain-based secure communication system can provide an end-to-end communication authentication service, ensuring confidentiality, availability, integrity, and authenticity of messages, which can significantly reduce the occurrence of misinformation. Implications on Decision Making and Operational Effectiveness: Secure communication and data sharing methods have communication and decision-making benefits that are important when trying to work as a group. In the military, secure communication means that leaders can make decisions based on timely information, and all of the people on whom the decision depends on are working from the most up-to-date and accurate information. Blockchain enables secure data sharing across multiple organizations and systems. This shift will find value in tools for secure messaging for military units, in ad-hoc groups, or as one-on-one messaging. Tools like secure messaging apps will be used in areas with low or unreliable infrastructure. The apps will enable coalition partners, non-governmental organizations, and military branches to create secure and collaborative groups, further enabling them to plan and execute missions together. Data shared in one tool would automatically be available to those with the needed privileges in other systems. However, lack of trust in a blockchain and using the blockchain are the biggest enemies against its successful adoption. Developing trust in a

 doi:10.20944/preprints202411.2266.v1

blockchain application is daunting, and the best solution is to create a blockchain time-stamped service with fully reviewed, verified, and validated code to further increase the trust in it [45–49].

2.3. Research Questions

In the context of exploring the role of blockchain technology in military applications, this study aims to address several key questions that arise from existing literature. These questions focus on the intersection of blockchain's potential with military operations, addressing both opportunities and challenges. The research questions for this review are as follows:

[RQ1] How can blockchain technology enhance data security and privacy in military communication systems?

This question seeks to explore blockchain's ability to facilitate secure communication within military networks by preventing unauthorized access and ensuring data integrity. Current research indicates that blockchain can provide robust solutions for privacy preservation, especially in sensitive communications where data breaches pose significant risks.

[RQ2] What are the primary challenges and opportunities for deploying blockchain in military supply chain management?

Blockchain's distributed ledger can potentially transform military logistics and supply chains by enhancing transparency, reducing fraud, and improving traceability. This question investigates the key benefits, as well as the implementation challenges, when introducing blockchain technology into complex, multi-layered military supply chains.

[RQ3] What role can smart contracts play in improving maintenance management frameworks within military operations?

With the increasing complexity of military equipment maintenance, blockchain-enabled smart contracts offer a potential solution to automate and streamline maintenance tasks. This research question addresses how smart contracts can improve operational efficiency, reduce human error, and ensure timely updates in military asset management.

[RQ4] How effective are current blockchain frameworks in mitigating cyber threats within military networks and systems?

The military's reliance on interconnected digital systems makes it vulnerable to cyberattacks. This question explores how blockchain can be integrated into cybersecurity frameworks to protect against external threats, unauthorized access, and data manipulation within military infrastructures.

[RQ5] What are the potential use cases of blockchain in enhancing military operational transparency and accountability?

Blockchain's immutability and transparency could enhance the military's accountability in both operational and administrative functions. This research question investigates how blockchain can be employed to track operations, manage resource allocation, and ensure audit trails, fostering a culture of transparency within military organizations.

[RQ6] How can blockchain-enabled frameworks be integrated with other emerging technologies (e.g., AI, IoT) in military contexts to enhance decision-making processes?

As military operations become increasingly reliant on advanced technologies, this question examines the integration of blockchain with other cutting-edge technologies, such as artificial intelligence (AI) and the Internet of Things (IoT). The goal is to understand how these technologies can work in tandem to enhance decision-making and operational efficiency in the military domain.

To answer the research questions in a structured manner, the design research methodology is followed as depicted in the flowchart of the methodology (Figure 1). This systematic approach ensures a structured exploration of blockchain's transformative potential in military operations while addressing the specific challenges put forth by the research questions.

 doi:10.20944/preprints202411.2266.v1

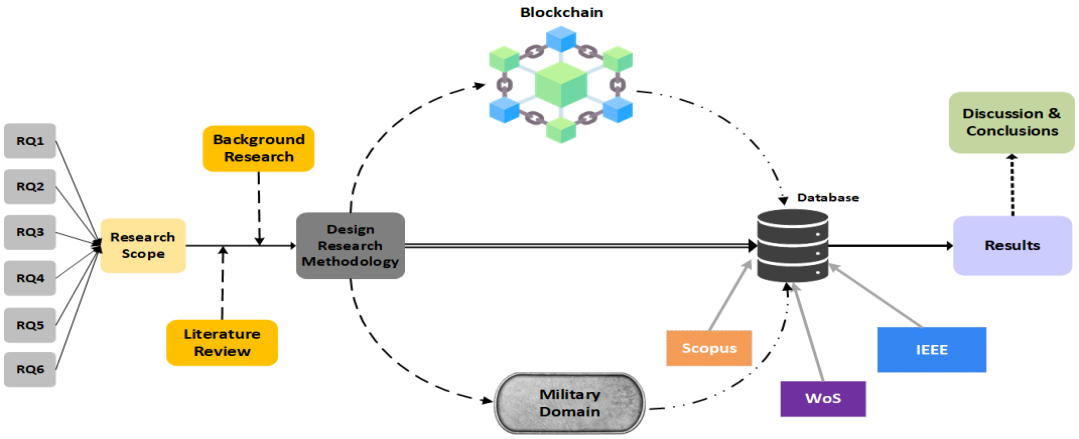

Figure 1. Methodology Flowchart for Blockchain Applications in the Military Domain.

3. Materials and Methods

This systematic review was conducted following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure transparency and rigor. The process consisted of four stages: identification, screening, eligibility, and inclusion, as detailed below [50]. A comprehensive search was conducted across multiple academic databases, including Scopus, IEEE Xplore, and Web of Science. This search yielded 120 records, complemented by 10 additional records identified through other sources such as grey literature, reference lists, and conference proceedings. After removing 15 duplicates, a total of 115 records remained for screening. The titles and abstracts of the 115 records were screened to assess their relevance to blockchain applications in the military domain. Articles were excluded if they did not focus on military-specific applications, lacked discussions of blockchain technology, or were non-peer-reviewed. This step excluded 60 records, leaving 55 articles for full-text review. The remaining 55 full-text articles were assessed against the inclusion and exclusion criteria. Articles were excluded for the following reasons:

- 5 articles were unrelated to blockchain applications in the military domain.
- 4 articles had methodological limitations, such as insufficient data or lack of rigor.
- 3 articles presented redundant or overlapping content.

A total of 43 articles met the inclusion criteria and were included in the final qualitative synthesis. These articles comprehensively address blockchain applications in the military, focusing on areas such as security, logistics, supply chain management, and privacy. This systematic process is summarized in the PRISMA flowchart (Figure 2), which illustrates the progression from the initial identification of records to the final inclusion of 43 studies in the review.

3.1. Search Strategy

We conducted a detailed, multi-stage search to ensure every relevant paper was collected. This consisted of an automated search of academic journals and digital libraries supplemented with hand searches of key academic journals and enlisting the help of our professional networks to identify additional papers. A comprehensive search was conducted across major academic databases, including Scopus, IEEE Xplore, Web of Science, PubMed, and Google Scholar, to ensure broad coverage of relevant literature. The search terms included "Blockchain," "Distributed Ledger Technology," "Military," "Defense," "Armed forces," "Battlefield," "Tactical," "Supply chain," "Cybersecurity," "Privacy," "Data protection," "Logistics," "Resource management," "UAV," "Drone," "IoT," and "Internet of Things." Boolean operators were used to refine the searches, combining terms such as ("Blockchain" OR "Distributed Ledger Technology") AND ("Military" OR "Defense" OR "Armed forces") and ("Blockchain") AND ("Supply chain" OR "Logistics" OR "Cybersecurity" OR "Privacy"). Search terms were adjusted as needed to fit the requirements of individual databases.

 doi:10.20944/preprints202411.2266.v1

3.2. Inclusion and Exclusion Criteria

The inclusion criteria required studies to focus on blockchain applications in the military or defense sector, be peer-reviewed, written in English, and discuss relevant use cases such as cybersecurity, supply chain, privacy, and resource management in military contexts. Exclusion criteria eliminated studies unrelated to blockchain technology, general applications without military relevance, and non-peer-reviewed or incomplete studies. The search yielded an initial set of 130 records, which were screened and assessed for duplicates, relevance, and methodological rigor. Following the removal of duplicates, 115 records were screened based on title and abstract, and 60 records were excluded for not meeting inclusion criteria. Of the 55 full-text articles assessed, 12 were excluded due to irrelevance, methodological issues, or redundancy. This resulted in 43 studies meeting the criteria for inclusion in the systematic review. In addition to database searches, backward citation tracking was performed by reviewing references of included studies, and forward citation tracking was used to examine studies citing the included papers. This approach ensured comprehensive coverage and minimized the risk of missing key studies relevant to blockchain applications in the military domain.

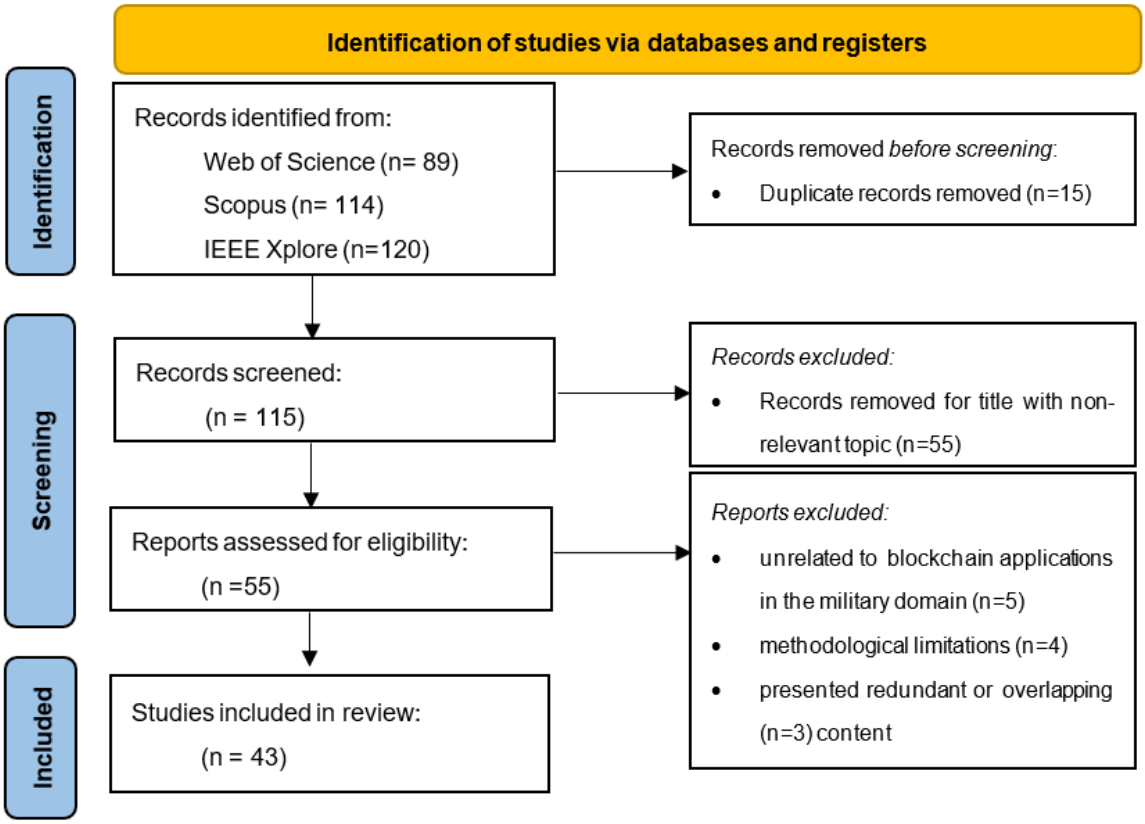

Figure 2. Flowchart of Prisma Methodology.

 doi:10.20944/preprints202411.2266.v1

Table 1. This is a table. Tables should be placed in the main text near to the first time they are cited.

Authors	Study Objectives	Main Findings
Abed et al., (2020) [51]	1. To develop a secure file approach using blockchain technology to protect against unauthorized access and manipulation of log files. 2. To provide proof of log file manipulation and non-repudiation. 3. To test the effectiveness of the proposed blockchain-based approach by comparing it to a scenario without blockchain protection.	- The blockchain technique prevents log file manipulation because the attacker cannot determine the correct hash value. - Without blockchain, the log file can be manipulated by the attacker without being detected. - The blockchain technique provides proof of log manipulation and non-repudiation.
Abualigah et al., (2021) [52]	- Provide a comprehensive review of the Internet of Drones (IoD) and its applications - Examine the deployments and integration of IoD, including areas such as privacy protection, security, neural networks, blockchain, and optimization - Identify and discuss the hot research topics and problems in the IoD domain to guide future research	- The paper provides a comprehensive review of the applications of the Internet of Drones (IoD) in various domains, including smart cities, cloud and fog computing, unmanned aerial vehicles, wireless sensor networks, mobile computing, and business paradigms. - The paper also reviews the integration of IoD with technologies such as privacy protection, security authentication, neural networks, blockchain, and optimization-based methods. - The paper discusses the current hot research topics and problems in the field of IoD to help guide future research in this area.
Aggarwal et al., (2021) [53]	1. Provide a broad survey of 6G technology and its architecture, requirements, and use cases 2. Present a solution taxonomy for UAV communication applications 3. Propose a blockchain-envisioned security solution and 6G-enabled network connectivity for UAV communication	- The paper presents a survey of the architecture, requirements, and use cases of 6G technology for UAV communication. - The paper proposes a blockchain-envisioned security solution and 6G-enabled network connectivity for UAV communication to address the challenges of traditional UAV communication methods. - The paper provides a solution taxonomy based on the applications of UAV communication.
Akter et al., (2023) [54]	- Develop a blockchain-integrated CNN-based framework (IoMT-Net) for identifying and tracking unauthorized/illegal UAVs in the Internet of Military Things (IoMT) system - Use blockchain technology to prevent illicit access, data manipulation, and illegal intrusions in the IoMT system - Utilize a CNN model to analyze RF signals from an antenna array to determine the Direction of Arrival (DoA) for localizing illegal UAVs	- The study proposes a blockchain-integrated framework to prevent unauthorized access and data manipulation in the Internet of Military Things (IoMT) system. - The study proposes a convolutional neural network (CNN) model to analyze RF signals and localize unauthorized UAVs in the IoMT system. - The proposed CNN model achieved high accuracy (97.63%) in estimating the direction of arrival of the RF signals, outperforming other state-of-the-art models.

 doi:10.20944/preprints202411.2266.v1

Aldossri et al., (2024) [55]	- Investigating the integration of lightweight blockchain and fog computing technologies to enhance the security of drone operations - Investigating the integration of lightweight blockchain and fog computing technologies to enhance the operational efficiency of drone operations - Providing a thorough summary of existing research on the application, challenges, and potential of integrating lightweight blockchain and fog computing into drone systems	- The paper presents a systematic review of the integration of lightweight blockchain and fog computing technologies to enhance the security and operational efficiency of drones. - The review highlights the significant potential of this integration to advance the capabilities and reliability of drones in critical applications. - The paper aims to provide a comprehensive summary of the existing research on how the integration of lightweight blockchain and fog computing can redefine the security and operational frameworks of drone usage.
Amran et al., (2022) [56]	1. Investigate using UAVs with wireless repeaters to boost weak signals in remote/isolated areas during emergencies 2. Protect the transmitted data from interference and manipulation using blockchain technology 3. Optimize the localization and clustering of UAVs using a swarm intelligence algorithm (SIL)	- Increasing the number of UAVs reduces execution time, redundancy, and localization inaccuracy. - Syncing data via blockchain may save time. - Exploring other nature-inspired localization algorithms in combination with blockchain could lead to further improvements in the future.
Asuncion et al., (2021) [57]	1. Identify a specific Department of Defense use case for blockchain technology 2. Extrapolate the requirements for this use case 3. Assess the different layers of the blockchain stack to identify the existing state of the art 4. Undertake a gap analysis of the technology for this context 5. Describe and implement a platform that addresses the identified challenges and requirements for the Department of Defense use case	- The paper describes the development of a platform that connects transactions from two separate blockchain systems (Consensys Quorum and Hyperledger Fabric) to enable transparent part tracking across the military and supplier networks. - The platform uses a graph-based approach to preserve privacy while enabling full transparency. - The paper also discusses the evolution of blockchain technology and the emergence of enterprise-level blockchain systems.
Bera et al., (2020) [58]	- Identify the challenges and issues in applying blockchain technology to 5G-based IoT-enabled Internet of Drones (IoD) environments - Propose and analyze a new blockchain-based secure framework for data management among IoD communication entities	- The paper identifies challenges and issues with applying blockchain technology in a 5G-IoT-enabled Internet of Drones (IoD) environment. - The paper proposes and analyzes a new blockchain-based secure framework for data management in the IoT-enabled IoD environment. - The proposed blockchain-based framework is able to resist several potential attacks and offers better security, functionality, and lower communication and computation overhead compared to other related schemes.

 doi:10.20944/preprints202411.2266.v1

Deebak et al., (2023) [59]	- Develop a blockchain-based remote mutual authentication (B-RMA) system for IoT devices and cloud networks - Evaluate the security efficiency and privacy protection of the proposed B-RMA system - Analyze the communication metrics (execution time, throughput, overhead ratio) of the B-RMA system	- The proposed blockchain-based remote mutual authentication (B-RMA) system can be integrated with IoT environments and decentralize user authentication. - The paper evaluates the security and privacy benefits of the proposed B-RMA system through an informal security analysis. - The results show the B-RMA system achieves a scalable environment.
Dubey et al., (2022) [60]	- Examine the effects of blockchain technology (BCT) on information alignment and coordination in humanitarian supply chains - Investigate the moderating effect of intergroup leadership on the relationships between BCT, information alignment, and coordination	- Blockchain technology (BCT) has a significant positive effect on information alignment and coordination among humanitarian organizations. - Intergroup leadership does not have a significant moderating effect on the relationship between BCT and information alignment/coordination. - Interdependence among humanitarian organizations has a significant positive effect on information alignment and coordination.
Ghimire et al., (2021) [61]	- Integrate blockchain technology with software-defined Internet of Unmanned Vehicles (IoUV) for military/battlefield applications - Provide trustworthy command and control operations in IoUV using blockchain - Increase trust, accountability, and reduce friction among different military units in the battlefield	- The paper proposes a sharding-enabled blockchain framework for software-defined Internet of Unmanned Vehicles (IoUV) in the battlefield. - The blockchain technology helps to provide trustworthy command and control operations in IoUV and stores those operations in tamper-resistant digital ledgers. - The proposed framework aims to increase the trust and accountability, and to reduce business friction among different units involved in the battlefield.
Gumaei et al., (2021) [62]	- Develop a framework that combines blockchain, deep recurrent neural networks (DRNN), and edge computing for 5G-enabled drone identification and flight mode detection - Remotely sense and collect raw RF signals of drones under different flight modes, use this data to train a DRNN model, and distribute the trained model on edge devices for drone and flight mode detection - Use blockchain to ensure data integrity and secure data transmission	- The DRNN model developed in the proposed framework can accurately detect drones and their flight modes from real-world RF signals. - The framework involves collecting drone RF signal data, training a DRNN model on a cloud server, and deploying the model on edge devices for real-time detection. - Blockchain is used in the framework to ensure the integrity and security of the data transmission.
Gupta et al., (2020) [63]	1. Present a comprehensive survey on securing drone communication 2. Propose a blockchain-based secure and intelligent drone communication architecture	- The authors propose a blockchain-based secure and intelligent drone communication architecture that utilizes 5G and AI technologies. - The proposed architecture uses IPFS for data storage, which improves network performance,

 doi:10.20944/preprints202411.2266.v1

	that utilizes 5G and AI techniques 3. Incorporate a healthcare-based case study using the proposed architecture	security, privacy, and reduces transaction costs. - The proposed architecture enables efficient drone communication with dynamic, flexible, and real-time decision-making capabilities through 5G and AI technologies.
Han et al., (2022) [64]	- Propose a blockchain-based UAV identity management model (B-UIM-M) to address security issues like single point of failure and lack of reliable authentication - Design a blockchain-based distributed identity authentication scheme based on the B-UIM-M model - Develop a secure communication architecture and protocols based on blockchain to ensure secure data transmission	- The paper proposes a blockchain-based UAV identity management model (B-UIM-M) to address security issues such as single point of failure and lack of reliable authentication mechanisms. - The paper establishes a distributed identity authentication scheme based on distributed identity identifiers (DIDs) under the B-UIM-M model. - The paper proposes a secure communication architecture based on blockchain and a set of secure transmission protocols to ensure the secure transmission of UAV communication data.
Harbi et al., (2022) [65]	- Analyze the current research on using blockchain technology to secure Internet of Drones (IoD) environments - Classify the reviewed studies based on blockchain type - Compare the reviewed studies on various factors - Identify how blockchain can provide security for IoD - Discuss open issues and challenges in combining blockchain and IoD	- Blockchain technology can provide fundamental security features for IoD networks, including authentication, privacy-preserving, confidentiality, integrity, and access control. - The paper compares the reviewed studies on blockchain for IoD security across different factors. - The paper identifies open issues and challenges in combining blockchain and IoD technologies.
Hassija et al., (2020) [66]	- Develop a framework for secure and reliable energy trading between UAVs and charging stations - Enable UAVs to buy energy from charging stations using tokens - Allow UAVs to borrow tokens from charging stations if they don't have enough to buy energy	- The proposed model allows UAVs to buy energy from charging stations using tokens, and to borrow tokens if needed, with interest or late fees. - A game-theoretic model is used to decide the energy buying strategy for UAVs. - The proposed framework provides increased utility for both UAVs and charging stations in a secure and cost-optimal manner, compared to conventional approaches.
Hu et al., (2021) [67]	- Propose a new type of UAV network architecture that combines SDN and blockchain technology (named SUV) - Ensure the SUV network can quickly build and adjust UAV networks based on application requirements and communication environment - Ensure the SUV network has desirable features like flexibility, survivability, security, and programmability, making it suitable for 5G-oriented UAV networking	- The main finding is the proposal of a new UAV network architecture called SUV, which combines SDN and blockchain technology to address the limitations of traditional mobile self-organizing networks. - SUV can quickly build UAV networks according to application requirements and has features such as flexibility, survivability, security, and programmability, making it suitable for 5G-oriented UAV networking.

 doi:10.20944/preprints202411.2266.v1

Hughes et al., (2017) [68]	1. Discuss the need to consider the societal impact of blockchain technology 2. Highlight the importance of inclusivity in the development of blockchain to avoid widening the digital divide 3. Explore the moral obligation to develop blockchain in a way that prevents abuse of trust by states and institutions 4. Examine the potential for blockchain to enable civil intervention in human rights issues	- Blockchain technology should be developed with the broader societal needs in mind, not just the interests of a few. - Inclusivity is crucial in the development of blockchain technology to avoid exacerbating digital divides. - Blockchain technology could be leveraged to support human rights and civil intervention in certain contexts.
Jadav et al., (2023) [69]	- Develop a secure and efficient system for data acquisition and dissemination in military operations using UAVs - Propose a blockchain and machine learning-based secure and intelligent UAV communication system (called "Block-USB") that can handle large amounts of data and secure sensitive military data from intruders and malicious actors	- The proposed "Block-USB" system, which combines blockchain and machine learning (ML) technologies, can secure UAV-based military operations and data dissemination in 6G networks. - The Block-USB system uses off-chain storage (IPFS) to improve the blockchain's storage capacity. - The Block-USB system outperforms traditional 4G/5G and non-IPFS-based systems in terms of classification accuracy, communication latency, and data scalability.
Javed et al., (2022) [70]	- Propose a blockchain-based authentication scheme that uses blockchain as a certificate authority and transactions as certificates, in order to reduce the high maintenance costs associated with traditional certificate-based authentication schemes. - Develop an authentication scheme based on Hyperelliptic Curve Cryptography (HECC), which provides the same level of security as other cryptographic schemes but with a smaller key size. - Provide a security analysis of the proposed scheme, demonstrating its resistance to various active and passive attacks. - Compare the performance of the proposed scheme with existing similar schemes, and show that the proposed scheme is more efficient in terms of computation and communication costs.	- The proposed scheme has significantly lower computation cost (40.479 ms) compared to two existing schemes (107.962 ms and 81.295 ms). - The proposed scheme has lower communication overhead (320 bits) compared to two existing schemes (1952 bits and 3040 bits). - The lower computation cost and communication overhead of the proposed scheme make it more practical for resource-constrained IoD networks compared to the existing schemes.
Koulianos et al., (2023) [71]	- Develop a secure and efficient system for drone swarms to exchange data and coordinate movements using blockchain technology - Introduce a novel leader-election mechanism for drone swarms using blockchain nodes - Develop a smart contract for decentralized decision-making on swarm formation based	- The proposed blockchain-based system for secure communication and formation control in drone swarms was successfully implemented and tested through simulation, with highly encouraging results. - The blockchain-based approach has the potential to enhance the security and decision-making capabilities of drone swarm systems.

 doi:10.20944/preprints202411.2266.v1

	on mission requirements - Design the smart contract to be lightweight and easily deployable	- The simulation results suggest that the proposed model could serve as a starting point for developing advanced, secure drone swarm systems.
Lis et al., (2019) [72]	- Analyze the economic aspects of cybersecurity for critical infrastructure - Evaluate the economic implications of cybersecurity efforts and cyberattacks - Explore methods to determine optimal investment in critical infrastructure cybersecurity - Propose solutions to develop sustainable, efficient and resilient critical infrastructure systems	- A comprehensive economic analysis of cybersecurity must consider both direct and indirect costs of cybersecurity measures as well as the expected damages from cyberattacks. - Developing a holistic economic framework to capture the costs, benefits, and consequences of cyberattacks and cybersecurity efforts can inform future policymaking. - Critical infrastructure providers often lack sufficient incentive to invest in cybersecurity beyond their own organization, necessitating government intervention through regulation and standards.
Manikandan et al., (2022) [73]	- Develop a new algorithm called RUPOA that can provide an optimal path for a swarm of UAVs - Integrate concepts of UAV energy rate and authentication to enhance secure and efficient path planning - Ensure the algorithm can generate an optimal path in less time and adapt to generate a new optimal path under security attacks - Achieve a higher attack mitigation percentage compared to existing algorithms	- The proposed RUPOA algorithm generates an optimal path in less execution time and is capable of generating the next optimal path under security attacks. - The proposed algorithm aims to reduce the distance of communication among the neighbor nodes and maintains a routing table to track the position and energy of all the neighbor nodes. - The attack mitigation percentage of the proposed algorithm is optimal compared to existing algorithms.
Mohril et al., (2021) [74]	- Develop a comprehensive maintenance management framework for military equipment that addresses military-specific maintenance challenges - Maintain maintenance data with high granularity and accuracy, including for the lowest maintainable units - Store maintenance data in a highly secure environment - Leverage blockchain technology to make the maintenance management framework "comprehensive and future ready"	- The proposed blockchain-enabled maintenance management framework aims to maintain highly detailed and accurate maintenance data for military equipment. - The framework discusses how blockchain technology can be used to address the challenges of military equipment maintenance. - The framework utilizes smart contracts to automate monitoring and validation of maintenance data with minimal human intervention.
Nyangaresi et al., (2024) [75]	- To address the security vulnerabilities of the Internet of Drones (IoD) system, particularly the insecure wireless communication channels and the risk of drone capture and cloning - To develop a secure authentication protocol for IoD that uses Physically Unclonable Function (PUF) and biometrics to withstand typical IoD attacks such as impersonation, replay, de-synchronization and spoofing	- A new PUF and biometric-based authentication protocol for the Internet of Drones is presented. - The protocol is formally proven to have a robust negotiated session key using the Real or Random (RoR) model. - The protocol is shown to be able to withstand common IoD attacks like impersonation, replay, de-synchronization, and spoofing.

 doi:10.20944/preprints202411.2266.v1

		- The protocol has lower computation, energy, and communication costs compared to other approaches.
Oláh et al., (2023) [76]	- Develop a secure and scalable registration protocol for the Internet of Drones (IoD) using PUF and blockchain technology - Provide a formal security analysis of the proposed registration protocol using the ProVerif tool - Provide an informal security analysis of the proposed protocol - Evaluate the efficiency and practicality of the proposed solution through a proof-of-concept implementation and analysis	- The proposed solution was evaluated against existing solutions in terms of key exchange, efficiency, physical security, data security, and availability of security analysis and implementation. - The paper presents a real-world implementation and prototype of the proposed solution, as well as a comparison of the LoRa technology used against other communication alternatives.
Pandey et al., (2022) [77]	- Provide a comprehensive survey of security issues in UAV-aided networks - Describe a taxonomy of security intrusions and secrecy performance metrics - Discuss techniques to mitigate security threats using various wireless communication technologies - Explore the role of emerging technologies like machine learning, SDN, and blockchain in UAV security	- The paper provides a comprehensive review of security issues and mitigation techniques in UAV communications. - It discusses how various wireless communication technologies, such as mmWave, NOMA, and MIMO, can be used to enhance the security of UAV communications. - The paper also explores the potential of emerging technologies, like machine learning, software-defined networks, and blockchain, to improve the security of UAV-aided communications.
Salor et al., (2023) [78]	1. Identify emerging 5G and 6G technologies that can enhance tactical communications 2. Provide a comprehensive overview of these technologies and their potential military applications 3. Offer a framework for understanding how these technologies can be applied in various tactical scenarios or use cases 4. Serve as a starting point for future research on using civilian technologies to advance military development	- Emerging technologies like network virtualization, software-defined networks, IoT, blockchain, AI, semantic communications, and neuromorphic processors can enhance the security, performance, and practicality of tactical communications and military applications. - The paper serves as a foundational analysis and analytical framework to guide future research initiatives in improving tactical communications.
Samanth et al., (2022) [79]	- Review recent UAV frameworks that have been designed and tested using the AirSim simulator - Review different secure IoD communication frameworks that have used various cryptography concepts and have been implemented in real-time or using network simulators	- UAV frameworks should be tested in simulators like AirSim before real-world deployment. - There is a need for secure IoD communication frameworks that do not compromise performance. - The study reviewed various secure IoD communication frameworks that have been implemented using different cryptographic techniques.

 doi:10.20944/preprints202411.2266.v1

Sarkar et al., (2023) [80]	- To devise a technique to share k secret images among n participants (n ≥ k) such that only k or more participants can collaborate to recover the original k secret images - To use a spanning tree approach with Prufer sequences to generate the share images for each participant - To store the share images in a blockchain using the interplanetary file system to provide distributed storage and eliminate single points of failure	- The paper proposes a blockchain-based (k,n) multi-secret image sharing scheme that uses Prufer sequences to generate share images for each participant. - The scheme stores the share images in a blockchain, which provides distributed storage and prevents cheating by allowing participants to verify each other's shares. - The scheme allows for lossless reconstruction of the original k secret images, making it suitable for sensitive applications where data integrity is critical.
Shahidinejad et al., (2024) [81]	- Develop a cost-effective blockchain-based key exchange protocol for secure communication between drones in different domains of the Internet of Drones (IoD) - Use Chebyshev's chaotic map as the cryptographic system and store only the public keys of the drones on the blockchain ledger to reduce storage and computational overhead - Ensure the proposed protocol meets the essential security requirements for IoD, such as anonymity and unlinkability, while complying with the Canetti and Krawczyk adversary model	- The paper presents a new blockchain-assisted authentication protocol for secure cross-domain communications in the Internet of Drones (IoD) that aims to address the limitations of previous approaches. - The proposed protocol uses Chebyshev's chaotic map as the cryptographic system and stores only the public keys of the drones on the blockchain, which reduces the storage and computational overhead compared to previous approaches. - The paper claims that the proposed protocol meets the security requirements of the Canetti and Krawczyk adversary model and provides anonymity and unlinkability, which are essential for IoD applications.
Shahzad et al., (2022) [82]	1. Discuss the need for faster and more secure 6G communication networks to support real-time applications. 2. Propose a blockchain-based solution to enhance security and privacy in 6G communication networks. 3. Describe a novel smart contract mechanism and a digital signature methodology to authenticate and secure the blockchain.	- The paper proposes a novel smart contract mechanism and a digital signature methodology to enhance the security and authentication of blockchain-based systems for 6G communication in tactile networks. - The paper emphasizes the importance of securing sensitive data and eliminating design flaws in order to achieve robust security in blockchain-based systems. - The paper proposes the use of cryptographic algorithms such as SHA-256, SHA-512, and ZK-SNARKS to achieve authenticity and integrity in the proposed blockchain-based solution.
Sobb et al., (2020) [83]	- Examine the uniqueness of military supply chains 4.0 and their integration with new technologies - Outline the emerging concepts of Supply Chain 4.0 and link them to commercial and military needs - Highlight the need for semantic modeling to understand threats and opportunities in this	- Supply chain 4.0 integrates manufacturing and IT processes but suffers from cyber risks like lack of standards and security issues. - Military supply chains have unique requirements like readiness and flexibility compared to commercial supply chains.

 doi:10.20944/preprints202411.2266.v1

	space - Outline the underpinning technologies and their intersections in the context of increasing technological interdependence	- The paper discusses the impact of emerging technologies like blockchain, IoT, and AI on supply chain 4.0 and the associated cyber security challenges.
Stanley-Lockman et al., (2019) [84]	1) Build on the concept of the Revolution in Military Logistics (RML) defined by the U.S. Army in 1999. 2) Analyze how emerging critical technologies may facilitate a paradigmatic shift in land-based combat service support. 3) Assess the merits, vulnerabilities, and cultural difficulties of transforming future military logistics by integrating these technologies.	- The chapter discusses how emerging technologies, including AI, alternative energy, AR, additive manufacturing, robotics, blockchain, and IoT, can enable a transformation of military logistics to make it more agile, modular, seamless, controlled, and sustainable. - The chapter assesses the potential benefits as well as the vulnerabilities and cultural challenges of integrating these technologies into operational concepts and organizational structures to transform future military logistics. - The chapter conceives of logistics transformation as a prerequisite for broader military transformation at the tactical, operational, and strategic levels.
Torky et al., (2022) [85]	1. Optimize the scheduling of drone charging to maximize the number of charged drones and minimize the number of "dead" drones. 2. Investigate the use of a novel blockchain protocol to authenticate and verify drone charging transactions.	- The PSO algorithm was effective in optimizing drone routes and preventing collisions during charging flights with low error rates. - The proposed scheduling methodology achieved a 96.8% success rate in drone charging cases. - The proposed blockchain protocol was efficient in managing drone charging transactions with low latency, allowing rapid and valid transactions.
Vashistha et al., (2022) [86]	- To develop a blockchain-based solution called eChain to address the problem of counterfeit electronic devices - To transform the existing supply chain into a trustworthy distributed ledger framework using eChain - To generate device provenance records from the blockchain that can be used to classify authentic and counterfeit electronic devices	- eChain generates blockchain-based device provenance records that can be used to classify authentic and counterfeit electronic devices. - A fully functional prototype of the eChain system was developed to demonstrate the feasibility and efficacy of the proposed blockchain-based solution for electronic device authenticity verification.
Vestergaard et al., (2021) [87]	Not mentioned (the abstract does not explicitly state any "study objectives" or goals of the paper)	Not mentioned (the abstract does not present any specific "main findings" or conclusions)
Wang et al., (2022) [88]	- Develop a blockchain-based solution to protect 3D printing models from unauthorized tampering - Create a whitelist of approved 3D models that can be verified before printing	- The paper proposes using blockchain technology to store the "fingerprints" of 3D models and verify the "fingerprints" before printing to prevent illegal tampering. - The blockchain-based approach can ensure the security and credibility of 3D-printed products by

 doi:10.20944/preprints202411.2266.v1

	- Demonstrate the feasibility of the proposed solution through an attack-defense experiment	creating a whitelist of approved models. - The combination of blockchain and 3D printing can help build a trusted manufacturing environment and realize more flexible manufacturing.
Wu et al., (2020) [89]	- Review existing blockchain-based solutions for privacy preservation in 5G-enabled drone communications - Introduce the architecture for 5G-enabled drone communications and blockchain	- 5G-enabled drones have potential applications in military and civilian settings, such as monitoring and tracking individuals. - There are security and privacy considerations that need to be addressed in 5G-enabled drone communications. - The paper reviews existing blockchain-based solutions for facilitating privacy preservation in 5G-enabled drone communications, and discusses relevant legislation, regulations, challenges, and open issues.
Yang et al., (2022) [90]	1) Conduct a comprehensive review of security issues and solutions for the Internet of Drones (IoD) 2) Discuss IoD-related security requirements 3) Identify the latest advancements in IoD security research	- The paper reviews various security technologies for the Internet of Drones (IoD), with a focus on authentication techniques and blockchain-based solutions. - The paper identifies the challenges faced by current IoD security methodologies and provides recommendations for future research directions in this area. - The paper concludes that appropriate security measures are necessary to address IoD security issues, and that new security solutions should balance the level of security and cost efficiency.
Yazdinejad et al., (2020) [91]	- Integrate blockchain and SDN to address challenges in IoT networks - Propose a secure and energy-efficient blockchain-enabled SDN architecture for IoT networks - Use a cluster structure and new routing protocol in this architecture - Use public and private blockchains for P2P communication, eliminating proof-of-work - Implement an efficient authentication method with distributed trust for resource-constrained IoT devices	- The proposed routing protocol based on a cluster structure has higher throughput, lower delay, and lower energy consumption compared to several classic routing protocols. - The proposed blockchain-enabled SDN architecture outperforms classic blockchain approaches.
Yazdinejad et al., (2020) [92]	- Develop a secure authentication model with low latency for drones in smart cities using blockchain technology - Apply a zone-based architecture and a customized decentralized consensus (DDPOS) to	- The proposed architecture improves security and reduces latency for the Internet of Drones. - The proposed architecture outperforms other models in terms of performance metrics like packet loss, throughput, and latency. - The proposed architecture can detect 97.5% of attacks by malicious drones while airborne.

 doi:10.20944/preprints202411.2266.v1

	enable drones to authenticate without requiring reauthentication - Improve security and reduce latency in the Internet of Drones (IoD)	
Zhu et al., (2020) [93]	- Provide a systematic understanding of cyberattacks and cyber defenses related to the Internet of Battlefield Things (IoBT) - Improve cybersecurity awareness for IoBT - Advance the development of appropriate security mechanisms for IoBT	- The paper identifies and characterizes three main types of cyberattacks on military IoBT systems: multiple entry-point and single device hacking, risks from unmanned aerial vehicles, and collateral damage. - The paper also identifies three main types of cyber defense strategies to address these threats: comply to connect, blockchain, and artificial cyber hunters. - The overall goal of the paper is to provide a systematic review of cyberattacks and cyber defenses related to the Internet of Battlefield Things (IoBT) in order to improve cybersecurity awareness and advance the development of appropriate security mechanisms.

 doi:10.20944/preprints202411.2266.v1

4. Results

The results of this systematic review highlight the multifaceted potential of blockchain technology in military applications, underscoring its transformative role across key domains such as security, transparency, operational efficiency, and decision-making processes. Drawing insights from the analyzed literature, this section synthesizes findings on blockchain's ability to address critical challenges in military contexts, including data integrity, supply chain management, autonomous systems, and cybersecurity as follows.

Figure 3 visually encapsulates the multifaceted applications of blockchain technology in military operations. At its core, blockchain serves as an enabler for diverse military functionalities, spanning logistics management, secure communication, UAV operations, AI integration, IoT connectivity, and maintenance automation. Each relationship highlights the technology's transformative impact: from enhancing supply chain traceability and ensuring encrypted data sharing to enabling autonomous system accountability and predictive maintenance efficiency. The scheme further emphasizes blockchain's integration with emerging technologies, such as AI and IoT, providing a robust framework for real-time monitoring and data-driven decision support. These connections underscore the potential for blockchain to revolutionize military operations by addressing critical challenges in security, transparency, and operational efficiency.

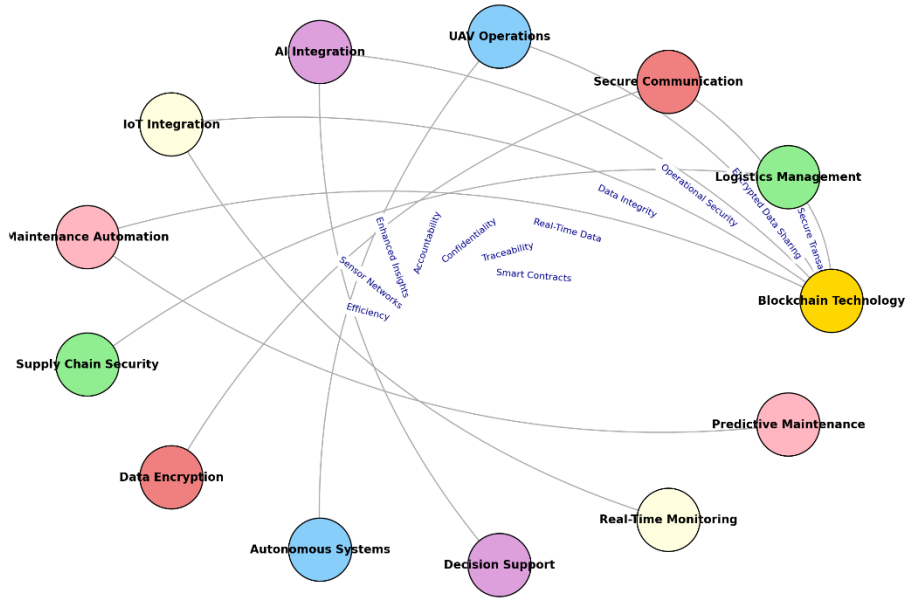

Figure 3. Visualizing Blockchain Applications in Military Contexts.

Additionally, the heatmap in Figure 4 illustrates the distribution of the 43 studies analyzed across various methodologies and application domains. The methodologies considered include systematic reviews, case studies, experimental studies, and theoretical analyses, while the application domains encompass supply chain management, secure communication, UAV operations, AI integration, and IoT applications. Notably, systematic reviews and case studies dominate research in supply chain management and secure communication, reflecting their critical importance in military logistics and data security. Experimental studies and theoretical analyses show balanced representation across emerging domains such as UAV operations, AI integration, and IoT applications, highlighting efforts to test and conceptualize blockchain's integration with advanced technologies. The heatmap provides a comprehensive view of the research landscape, showcasing the methodological rigor and domain-specific focus in exploring blockchain applications for military contexts.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 November 2024 doi:10.20944/preprints202411.2266.v1

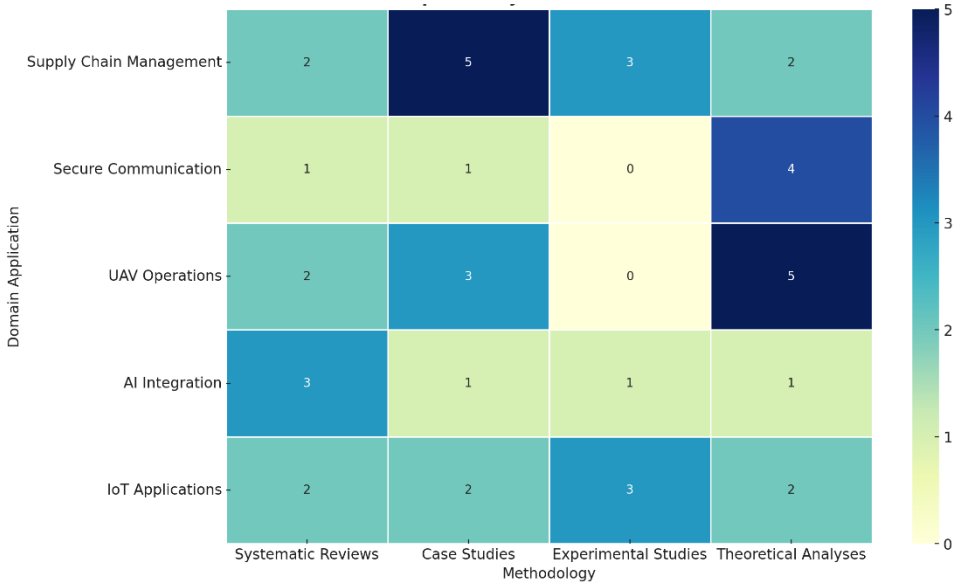

Figure 4. Heatmap of Studies (N=43) Focus Across Methodologies and Application Domains.

Moreover, the graph below (Figure 5) visualizes the hierarchical relationships and dependencies between various applications of blockchain technology in military contexts. Each node represents a specific domain or subdomain, such as Logistics, Cybersecurity, IoT, UAVs, or Smart Contracts, color-coded uniquely for distinction. Larger nodes highlight key concepts or categories, while the connecting edges represent functional relationships or technological integrations between them. The legend to the right explains the color-coded nodes, making the graph more intuitive and interpretable. This representation emphasizes the interconnected nature of blockchain applications in enhancing military operations, security, and efficiency.

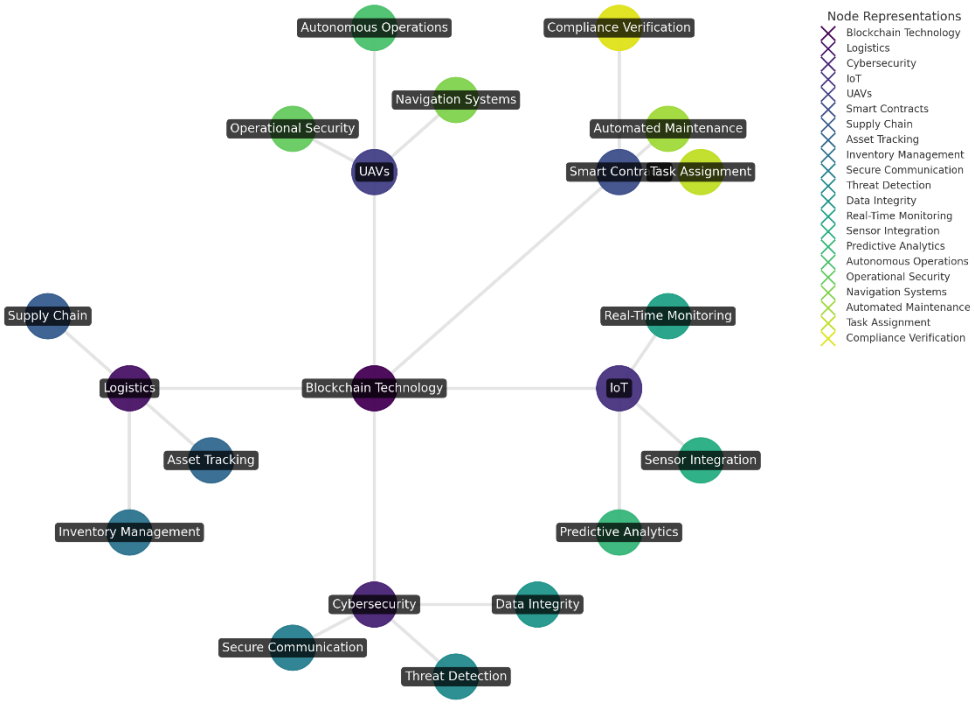

Figure 5. Graph Representation of Blockchain Applications in Military Domains.

[RQ1] How can blockchain technology enhance data security and privacy in military communication systems?

 doi:10.20944/preprints202411.2266.v1

The decentralized architecture of blockchain, its cryptographic foundations, and tamper-resistant ledger system hold the promise of bringing transformative capabilities in enhancing data security and privacy in the communication systems of the military. All these features guarantee strong protection against unauthorized access, data breaches, and cyber-attacks, where integrity and confidentiality are maintained within sensitive communications. In this context, various research works have described how security can be enhanced with blockchain in the diverse scenarios of military communication. For instance, authors [58] presented a secure blockchain framework for the management of communication entities in IoT-enabled drone environments. This is able to enhance the level of security and functionality while reducing operational overheads [58].

Similarly, the privacy-preserving feature of blockchain is underlined for 5G-enabled drone communications [89], a very critical feature considering the great volume of sensitive data collected and disseminated in such systems. In this regard, the study [91] presented an architecture of a blockchain for IoT networks based on a hybrid public-private blockchain approach for peer-to-peer communication between IoT devices and SDN controllers. Their proposed system eliminates the Proof-of-Work consensus but instead adopts a low-latency mechanism tailor-made for resource-constrained IoT devices in a military setting. The decentralized nature of their design thereby significantly reduces authentication delay but provides distributed trust, hence suitable for dynamic environments like the IoD. Another study [92] further proposed a drone-based delegated proof-of-stake (DDPOS) consensus mechanism, to enhance security over IoD, that achieves 97.5% detection rates for malicious drones while airborne and reduced latency [92].

The proposed block-chain-based system for IoUV was lately given by another study [61] with his colleagues. To ensure trustworthy command and control operations for battlefield applications, their sharding-enabled blockchain approach attempts to resolve the scalability issues while also ensuring that blockchain systems continue if a number of battlefield nodes are compromised or destroyed. This approach enhances the integrity and accountability of the critical operations going on in the battlefield scenarios [61]. The decentralized architecture of blockchain eliminates single points of failure, making it more resilient to attacks on the communication systems. According to the study [93] this feature is very important for military systems where the distributed nature of data storage across many nodes significantly raises the bar for an adversary to compromise entire networks [93]. Further, blockchain possesses good confidentiality and integrity guaranteed by cryptographic techniques. Furthermore, researchers [65] have emphasized the fact that blockchain's immutable ledger prevents unauthorized data tampering, providing a reliable and traceable record of military communications [65].

Blockchain will allow the military units and allied forces to share data securely across domains. Also, the study [81] proposed a framework for interoperable blockchain-based communication, characterized by strict access control and security critical to effective collaboration between forces in joint multi-domain operations [81]. Additionally, researchers [69] have shown how blockchain could provide greater data transparency and auditability for military organizations by tracing and verifying information flow from one unit to another, thereby tracing any kind of anomalies in the process [69].

The cryptographic foundations of blockchain assure secure data exchange mechanisms and authentication for military IoT and UAV networks. One of the studies [66] illustrated how blockchain safeguards UAV communication systems, through cryptographic hashing and distributed consensus, in order to secure the system from unauthorized access and possible data breaches [66]. Another related study presented an architecture for SDN-based blockchain that allows flexibility, survivability, and security for improving the resilience of communication networks [67].

Smart contracts further automate the policies of access control, ensuring homogeneous enforcement of security protocols across communication networks. The potential of Samanth et al. has been pointed out in key management agreements, authentication, encryption, and digital signatures—features very essential toward secure military communication systems [79]. Another piece of research underlined the immutability of blockchain and its cryptographic linkages, leaving any tampering attempts detectable and thus allowing trustworthy records of all communications [88]. Challenges remain, however, in scalability and integration with current military infrastructure. The

 doi:10.20944/preprints202411.2266.v1

study's [61] approach to sharding-enabled blockchain is just one of the solutions that could bring improvement in terms of scalability by distributing processing load among all shards [61]. Moreover, high computational intensity of blockchain and resistance to quantum cryptographic methods urge further research in the area of lightweight consensus mechanisms and advanced cryptographic techniques [56,72]. In general, its inherent features of decentralization, cryptography, and immutability can highly qualify blockchain to be a great stride in enhancing data security and privacy in military communication systems. If the current challenges are properly addressed and the innovative frameworks proposed by researchers are further developed, blockchain can substantially reinforce the confidentiality, integrity, and resilience of military networks to assure secure and efficient operations in dynamic environments.

[RQ2] What are the primary challenges and opportunities for deploying blockchain in military supply chain management?

Blockchain technology represents a formidable confluence of both opportunities and challenges in improving military supply chain management, providing solutions to some of the most critical issues of security, transparency, and interoperability. However, successful implementation means overcoming numerous technical, operational, and resource-based constraints. Integration of this technology with the legacy logistics systems is one of the major challenges in the deployment of blockchain in military supply chains. Furthermore, the study [57] highlighted the challenges of aligning the blockchain systems with the legacy infrastructure, which generally requires huge modification and resource investments [57]. Adding to this challenge, at the scale of military operations, huge volumes of data, and transactions can be overwhelming for traditional blockchain technologies.

Moreover, the study [69] indicated that the current blockchain systems have scalability limitations, which may lead to poor performance in real-time supply chain scenarios [69]. Researchers [61] therefore proposed a sharding-enabled blockchain solution that distributes the computational load into several shards to maintain its operability even under resource-constrained battlefield environments [61]. Security and privacy have always been the major concerns for military logistics systems. Also, researchers [89] pointed out that managing sensitive data in blockchain systems could give rise to risks, especially when unauthorized access or tampering would compromise critical operations [89]. Additionally, the study [65] indicated that blockchain can mitigate such risks through its immutability of records, if there is strong encryption and mechanisms for access control to provide security against emerging cyber threats [65]. Another critical challenge pertains to energy consumption linked with certain blockchain consensus mechanisms, such as Proof-of-Work, to perform transactions.

Also, researchers [91] have stated that more energy-efficient mechanisms—like Delegated Proof-of-Stake—may provide workable alternatives in resource-constrained environments—for example, related to drones or battlefield supply chains [91]. Another big challenge faced with the supply chain management of the military is interoperability. Furthermore, the study [60] underlined that the coordination among such diverse entities as military units, allied forces, and government agencies needs a standard framework for the secure and efficient sharing of data [60].

In this respect, blockchain's decentralized nature presents a potential solution by taking out the requirement for a central authority, yet guaranteeing seamless integration with heterogeneous systems continues to be a technical and operational challenge [83]. Moreover, researchers [81] proposed a blockchain-based framework to address this issue by allowing interoperable and secure communication among several stakeholders involved in military operations [81]. With those challenges, blockchain presents opportunities that could be transformational in the enhancement of military supply chain management. The immutability that it brings forth offers the prospect of increased tracing and tracking of military assets, offering real-time visibility and guaranteeing accountability. Also, researchers [89] addressed the potential of blockchain in creating tamper-resistant records that enable detection and prevention of fraud or counterfeiting of supplies ([89]. The study [86] reflected on the importance of provenance tracking in guaranteeing authenticity in military

 doi:10.20944/preprints202411.2266.v1

equipment and supplies, as well as in mitigating risks involved with counterfeit parts in critical applications [86].

Another big avenue is smart contracts, which automate some of the most important supply chain procedures, which reduce administrative overhead and minimizes human error. Other authors in their study [68] alluded to how smart contracts can smoothly carry out procurement flow, thereby enhancing efficiency and ensuring constant application of policy across a military logistics network [68]. The study [92] proved how blockchain-based authentication methods could secure unmanned vehicles and other supply chain components, ensuring that access to critical systems is granted only to authorized entities [92]. Furthermore, the decentralized nature of blockchain also provides resilience against disruptions, for example, cyberattacks or natural disasters. Also, researchers [85] commented that blockchain systems based on a decentralized architecture are more resilient to single points of failure because the system remains operational when parts of the network are compromised [85]. Similarly, the sharding-enabled approach by the study [61] would ensure that military supply chains are able to continue running even if nodes are destroyed or damaged in hostile environments [61].

Furthermore, blockchain can also enable the efficient and secure sharing of data between different military units and allied forces, improving coordination and information alignment during complex supply chain operations. Additionally, researchers [60] emphasized that the transparency and auditability of blockchain can increase collaboration among stakeholders while maintaining strict access controls over sensitive information. Still, some of these challenges require further investigation and development. In resource-constrained scenarios—like drones with limited battery life, the high computational requirements of blockchain systems may be quite inapt. Also, researchers [66] have suggested optimizing the implementation of blockchains to reduce energy consumption without affecting security [66]. This also includes the need for future-proofing blockchain against emerging fast threats, for example, quantum computing [51,62]. Furthermore, researchers [72] pointed out that quantum resistant cryptographic algorithms must be used to provide long term viability in military applications [72].

In conclusion, blockchain technology can be seen as having tremendous potential for revolutionizing military supply chain management by increasing security, transparency, and operational efficiency. While the challenges regarding scalability, energy efficiency, and interoperability remain at play, innovative solutions like sharding, smart contracts, and energy-efficient consensus mechanisms provide pathways toward those challenges. With continuing research and development, blockchain can become a keystone of resilient, secure, and efficient military logistics systems.

[RQ3] What role can smart contracts play in improving maintenance management frameworks within military operations?

Smart contracts, a core feature of blockchain technology, hold transformative potential for improving maintenance management frameworks within military operations by enhancing automation, efficiency, security, and traceability. These programmable contracts can automatically execute predefined actions based on specified conditions, removing the need for constant human intervention while ensuring rigorous adherence to maintenance protocols. One big application of smart contracts is to automate the scheduling and execution of maintenance activities by encoding maintenance protocols and schedules in a blockchain, which then automatically triggers a maintenance request based on equipment usage metrics, sensor data, or elapsed time since the last service. This automation ensures that the military assets are kept up to date on time, thereby avoiding the risk of failure during important operations [72,74]. Combining IoT sensors with smart contracts will be able to build a framework for predictive maintenance. Under such a framework, real-time analysis of equipment performance data can provide a mechanism for identifying and resolving potential problems before they lead to failures [77,93].

This proactive approach will not only increase the reliability and readiness of military equipment but also extend its operational life. Another critical advantage of smart contracts is that they create an immutable, auditable history for all maintenance activities. All maintenance actions,

 doi:10.20944/preprints202411.2266.v1

including inspection, repair, and replacement of parts, are made in an unalterable form on the blockchain and hence create an unalterable history for each piece of equipment [58,74]. This traceability enhances accountability since each maintenance task can be traced back to specific personnel or units.

It also enforces the requirements of military maintenance standards by directly flagging any deviation from prescribed protocols by the smart contract itself [79]. The possibility of auditing maintenance activities due to an immutable ledger eases the tracking of compliance and increases transparency in high-stakes environments, where operational safety is a must [65]. Similarly, smart contracts will enable effective resources allocation through prioritization of maintenance activities according to operational needs, criticality of equipment, and resources availability. Smart contracts ensure that activities of maintenance personnel, tools, and spare parts are efficiently performed even under resource-constrained environments, such as battlefield conditions, through automation [61,69].

For example, equipment tagged for maintenance automatically triggers the smart contract to assign the most suitable personnel and resources required to perform the maintenance in a manner that minimizes downtime and maximizes mission readiness. Integration of smart contracts in the larger military supply chain adds efficiency. In case specific parts or supplies are needed for the maintenance activities, then the smart contracts automatically trigger the procurement order based on the level of inventory, meaning that at the required time, the necessary components will be available [67,86]. In this way, one avoids delay in obtaining and ensures continuous availability of critical supplies.

Smart contracts can also assure quality in the supply chain, proving that the parts and materials used are authentic, hence mitigating the risks of counterfeit components that would compromise military operations [86]. When smart contracts are in use, interoperability is achieved since the standardization of maintenance procedures and data formats across various units or participating nations in joint military operations or coalition forces. This feature offers ample coordination of maintenance activities for effective efficiency of operations and cooperation amongst the various stakeholders [57,59,60]. Smart contracts also enable the sharing of data in a secure way between entities with strong mechanisms of encryption to ensure sensitive maintenance-related information is only accessible to the person with authority while maintaining the integrity of shared data [81]. While the application of smart contracts has a lot of advantages, their use in military maintenance management comes with its challenges. Smart contract codes need to be secure; otherwise, vulnerabilities might expose sensitive operations to cyber threats. Researchers [91] state that a strong security mechanism will be needed in order not to let smart contracts be exploited in some environments, such as the IoD where maintenance management concerns unmanned systems.

Moreover, the technical challenges in integration of smart contracts into the legacy system must be well-planned and implemented. Second, there are issues regarding scalability since huge volumes of maintenance tasks and data are usually created in complicated military operations [90]. In a nutshell, smart contracts can revolutionize maintenance management frameworks in military operations by automating processes, tracing, better resources allocation, and through strict maintenance standards observance. While security, scalability, and system integration remain challenges, these can be met primarily by ensuring that rigorous planning and testing, that is, in close collaboration with a range of stakeholders—will enable successful smart contract deployment in a military context. Each of these advancements finally culminates in better operational readiness, higher efficiency, and greater reliability of military assets, to make sure that they meet the demanding requirements of modern warfare.

[RQ4] How effective are current blockchain frameworks in mitigating cyber threats within military networks and systems?

Current blockchain frameworks show great potential in the mitigation of cyber threats within military networks and systems through decentralization, cryptographic foundations, and tamper-proof data management. These properties enable improved security, privacy, and resilience against different cyber threats in sensitive military environments. Their effectiveness does depend on the

 doi:10.20944/preprints202411.2266.v1

details of implementation, though, as well as the nature of the threat and possible integration challenges with the existing systems.

This decentralized architecture is one of the major assets of blockchain in the mitigation of cyber threats. Unlike the traditional centralized systems with known single points of failure, blockchain spreads its data across a multitude of nodes, thus being resilient to DDoS attacks by its very nature, where an adversary attempts to disable the system by overwhelming it with traffic. Also, researchers [71,93] have highlighted the fact that, by its very nature, blockchain is distributed and continues operations even when parts of the network are compromised. Such robustness is a bonus for military systems, which could be operating in adversarial environments where the integrity of communications and operations is paramount.

For instance, blockchain immutability guarantees the integrity of sensitive information stored in military systems. Once data is recorded on a blockchain, it cannot be altered without detection and is thus highly resistant to tampering or manipulation. The importance lies here, with this capability of maintaining authenticity throughout the chain of command-and-control operations under battlefield scenarios. Also, researchers [61] showed the application of blockchain on the IoUV, where operational data can be stored in tamper-resistant ledgers to achieve a reliable and accountable environment between units. Along the same lines, the studies [72,77] highlighted the use of immutable ledgers in securing military communications through ensuring that unauthorized changes are not permitted.

The blockchain frameworks also excel in the security of communications, given the end-to-end encryption and the strong authentication mechanism. In blockchain systems, public and private key cryptography ensures that sensitive communications are accessible only to the authorized entities. Also, the study [64] showed how blockchain encrypts military data during its transmission, so it becomes almost impossible to intercept or alter. In drone operations, the study [92] proposed a tailored consensus mechanism, called Drone-Based Delegated Proof of Stake (DDPOS), which combined low latency and high security. The system proved to detect 97.5% of malicious drone attacks, which showed the potential of blockchain technology in securing airborne military communications.

Another critical area in which blockchain enhances cybersecurity is authentication. These blockchain-based systems perform decentralized identity verification and thus ensure that access to military systems and data is granted only to authorized personnel. Also the study [92] demonstrated the effectiveness of blockchain on drone networks through secure authentication mechanisms that denied access to unauthorized entities while keeping delays at a minimum. Additionally, the studies [70,82] have further noted that the embedding of smart contracts in blockchain systems could enforce access controls and automate authentication protocols in a manner to reduce insider threats and unauthorized activities.

Moreover, the cyber threat mitigation features of blockchain include transparency and traceability. The creation of an auditable trail about all performed actions on the network enables real-time monitoring and post-event forensic analysis. Furthermore, the studies [60,71] highlighted this feature as very essential in detecting suspicious activities, confirming the fulfillment of set or intended cybersecurity protocols, and holding people accountable for their operations. These features give the military networks a better level of trust and reliability. In military logistics, blockchain frameworks help in securing the supply chain by not allowing counterfeit components to enter the system. Also, the role of blockchain in creating a provenance record for military hardware is underlined in study [86], which allows users to verify the authenticity of the equipment and minimizes the risk of sabotage. The application is one of the most critical applications in ensuring the operational readiness and safety of military assets.

These benefits notwithstanding, the current blockchain frameworks cannot be guaranteed to ensure complete mitigation of cyber threats. Scalability is a big challenge, as military networks can have large amounts of transactions and data. For instance, in the study [61], researchers proposed shard-ing-enabled blockchain, where the network is divided into smaller units for the efficient

 doi:10.20944/preprints202411.2266.v1

processing of loads. This framework still needs further development, considering the intricacies involved in large-scale military operations.

Another consideration is energy consumption, especially for computationally intensive consensus mechanisms like Proof-of-Work (PoW). High energy requirements might limit blockchain applicability in resource-constrained environments, such as drone operations. Consequently, researchers [91] have proposed the use of energy-efficient mechanisms, for example, Delegated Proof-of-Stake (DPoS) to overcome such limitations. Integration with the legacy military system and inter-operability across diverse platforms also poses a big challenge. As brought out by the studies [78,83], blockchain adoption requires considerable technical and organizational adjustments, which may be resource-consuming and introduces new vulnerabilities. The new system must be compatible with the already existing cyber security measures and military protocols to not create any security gaps during transition.

Other upcoming threats, such as quantum computing, are a long-term challenge to blockchain frameworks. Quantum computers are theorized to potentially undermine the cryptographic algorithms underpinning current blockchain systems. For example, two studies [75,90] noted the ongoing research on quantum-resistant cryptography in a secure manner by ensuring the long-run viability of blockchain in military applications. In other words, the current architecture of blockchain presents an effective way to mitigate various forms of cyber threats against military networks and systems. They have strong mechanisms that secure data, authenticate users, and increase resilience against attacks. However, their full potential is yet to be realized due to challenges related to scalability, energy consumption, integration, and emerging threats. This would, therefore, require further research and development to adapt blockchain to the special demands of military cybersecurity with knowledge of its effectiveness in such a complex and dynamic threats landscape.

[RQ5] What are the potential use cases of blockchain in enhancing military operational transparency and accountability?

Blockchain technology can be disruptive in enhancing transparency and accountability of military operations, being core features of immutability, de-centralization, and secure data management. Such capabilities do well with the increasing requirement for precision and auditable systems within complex and high-stakes military environments. The following is a selection of use cases where blockchain can be fruitfully employed to enhance transparency and accountability for different dimensions of military operations. Blockchain presents a use case in supply chain management, allowing the military to have a tamper-proof and auditable framework in tracing assets, equipment, and supplies throughout their lifecycle. It assures the authenticity of military materials and prevents counterfeit or tampered items from being introduced into the supply chain. Furthermore, the study [86] emphasized the very important role that blockchain can play in creating tamper-proof device provenance records, which would enable military entities to classify authentic and counterfeit components. This application is essential for the safety and operational reliability of military assets, as counterfeit items can create severe security and functionality issues. Similarly, researchers in their study [60] have shown how blockchain's traceability and mobilization of resources ensure transparency in materials and fund flow, reducing the risks of mismanagement and enhancing overall supply chain accountability. In fact, blockchain transparency can even be applied to communications and command logging in military operations. The immutability of a blockchain ensures that all communications and orders are recorded in such a secure way that posteriors can track changes, enabling the audit trail after operations. Also, researchers [61] emphasized the use of blockchain in storing the data of battlefield command and control in tamper-resistant ledgers to increase trust and accountability between units. To that end, blockchain provides a very secure and traceable log of all mission details, flight paths, and collected data concerning drone operations, where all actions performed by any unmanned system become fully auditable [92].

Blockchain can safely store and update, so to speak, records of training, assignments, and performance evaluations. Blockchain guarantees transparency in any personnel workflows through the development of smart contracts that automatically determine promotions or mission assignments based on pre-established criteria. In the study [72] discussed the potential for blockchain to bring

 doi:10.20944/preprints202411.2266.v1

transparency and accountability in personnel decisions by creating a secure and immutable record of individual activities and certifications. It enables the auditability of personnel decisions and ensures equity within the hierarchical structure in the military. One of the second most salient areas in which blockchain could strengthen operational accountability is that of autonomous systems and unmanned vehicles. Logging and verification, through blockchain, provide assurance that the activities conducted by the system are in accordance with mission protocols and afford an exceptionally powerful mechanism of accountability. The study [92] also revealed that the blockchain-based authentication and logging system for drones, with a delegated proof-of-stake consensus mechanism, could provide a secure and transparent drone operation with minimal security risk [55].

Another area where the abilities of blockchain are transformative is that of financial transparency. Its ledgers can be used to accurately track financial transactions, budgets, and resource allocations, thus preventing fraud and corruption. Researchers in their paper [60] explained how traceability of fund mobilization through blockchain heightens the accountability of military expenditure. In such a way, blockchain comes with an open and auditable system that should instill more public confidence in how the military uses its finances. It also caters to secure and transparent inter-organizational coordination, especially needed during joint military operations or multinational coalitions. To emphasize this further, the same research [60] highlights the value that blockchain can bring into assurance of better alignment and coordination among these different military entities. Such technology will share critical information in a secure manner with a clear audit trail, hence guaranteeing mutual accountability while providing strict access controls.

Hence, tamper-proof records make verification easier and ensure that military protocols and regulations are complied with for auditing. In [74], it was discussed how smart contracts in a blockchain enable the automation of checks for compliance and create immutable records of all actions and transactions for easy auditing. The app not only eases administrative burdens but also guarantees that any non-conformity to previously set protocols is detected and acted upon in a timely manner. While promising, there are some challenges that arise with blockchain implementation in military contexts. One of the major concerns is related to scalability, especially in large-scale operations with a high volume of transactions. Also, as shown in the study [63], current blockchain systems suffer from some limitations regarding high transaction storage cost and issues related to communication latency and bandwidth. Such technical constraints need solution approaches like shar-ding-enabled blockchains or lightweight consensus mechanisms to be widely adopted. In addition, making blockchain interoperable with existing military systems, and thus compatible with different platforms, is a huge technical and organizational undertaking [84,87,91]. It is also of critical importance to balance transparency with operational security. Although blockchain leads to transparency due to the immutability of records, too much openness would reveal sensitive operational details to adversaries. Military organizations need to calibrate access controls accurately and ensure transparency will not jeopardize confidentiality related to strategic information [79,80].

In summary, blockchain technology presents various opportunities for increasing transparency and accountability within military operations. Applications in supply chain management, communication logging, personnel workflows, autonomous systems, financial management, and inter-organizational coordination provide solutions to some of the critical gaps identified in current military processes. Realization of these benefits will, however, depend on the resolution of challenges surrounding scalability, integration, and security. With its growing maturity, blockchain can revolutionize how military operations are conducted and monitored, even audited, by setting new standards for transparency and accountability within the defense sector.

[RQ6] How can blockchain-enabled frameworks be integrated with other emerging technologies (e.g., AI, IoT) in military contexts to enhance decision-making processes?

Blockchain-enabled frameworks, integrated with emerging technologies such as AI and IoT, provide a transformational approach to the improvement of decision-making processes in military contexts. Integration of strengths of these technologies—blockchain for secure, immutable data management; IoT for real-time data collection; and AI for advanced analytics—builds resilience and

 doi:10.20944/preprints202411.2266.v1

efficiency in military systems. Each technology has unique strengths that address different challenges in strategic, operational, and tactical decision-making.

Integration of blockchain and IoT in military applications enhances data security and reliability. In typical military applications, various IoT devices, such as drones, sensors, and communication systems, are usually deployed, enabling a huge amount of real-time data. Blockchain gives a decentralized, tamper-proof ledger to store and validate this immense data. Such integration ensures the integrity of data, which then is immune from unauthorized manipulation or corruption [52,54]. Also, the study [89] pointed out the effectiveness of blockchain in privacy preservation with 5G-enabled drone communications, where data needs to be sent for analysis to some remote centers. Blockchain integration with IoT allows seamless and secure real-time data collection, enabling military decision-makers to act upon reliable and verified information.

Applications in this respect have been seen in the management of supply chains and monitoring of equipment using blockchain-enabled IoT frameworks. Some research works [73,76,91] therefore presented an architecture of IoT networks integrated with the public and private blockchain, which would provide secure peer-to-peer communication between the devices and controllers. The latter provides better visibility and control over military logistics, given that data regarding the status of the equipment and supplies is well recorded and accessible in real time. Integration of IoT with blockchain would help military leaders in tracking resources and monitoring equipment performance for minimal downtime and better resource utilization.

The inclusion of AI in blockchain-enabled systems further enhances decision-making by enabling advanced data analysis and predictive modeling. If the data on a blockchain can be processed, then it enables AI algorithms to detect patterns and hence predict possible problems before optimizing resource distribution. In addition, this study [83] provides some insight into the application of AI in supply chain 4.0 that can be extrapolated to optimize logistics and better conduct strategic planning within military operations. AI analysis of blockchain-validated data ensures that decisions are completely accurate and based on full insight, therefore giving the military more efficiency and effectiveness.

Blockchain frameworks also provide an answer to major concerns in the deployment of AI systems, which guarantee the integrity and accountability of AI models. In a blockchain, the training datasets stored ensure that AI systems, through immutability and traceability of the ledger, prove the authenticity of the training datasets and model updates. In high-stakes military environments, trust in AI systems is a must. For instance, the study [61] highlighted the fact that blockchain combined with AI in autonomous systems, such as drones, creates self-organizing networks, maintaining a secure and auditable log of actions, guaranteeing transparency of operations by unmanned vehicles [53].

This is further advanced with smart contracts, where decision making is automated. Blockchain-based smart contracts can be programmed to execute certain actions under some predefined conditions, such as data from IoT sensors or predictions produced by AI. In this respect, for example, smart contracts can automatically reorder supplies or trigger maintenance work once sensors indicate low levels of stock or wear of equipment. Similarly, researchers [74] have shown the usefulness of smart contracts in automating resource allocation and scheduling—combined with AI and IoT—making military operations much simpler and resulting in less manual intervention.

The integration of blockchain, AI, and IoT increases situational awareness—one of the important elements in military decision-making. IoT sensors sense battlefield data, which is then secured and integrity-ensured through blockchain technology before being analyzed by AI to create actionable insights for commanders to view a holistic and real-time operational picture that enhances response times and decision accuracy. In addition, researchers [91] said that those systems would be invaluable in the battlefields where integrated ones will autonomously choose to complete the human element in supervision.

One of the most promising methods in the integration of blockchain and AI in cybersecurity has been effective at detecting and responding to threats. Blockchain provides security for the military networks through the creation of an immutable security log, which allows AI algorithms to analyze

 doi:10.20944/preprints202411.2266.v1

the log for any anomalies or possible breaches. Also, researchers [65] had presented how blockchain, combined with AI-driven cybersecurity systems, could be used to improve the resilience of military communication networks. This will provide multi-layered protection to ensure strong protection against both external and internal threats.

While blockchain-enabled frameworks provide many benefits when integrated with AI and IoT, there are also some challenges. For instance, one of the major challenges is scalability in such large military operations; otherwise, an overwhelming amount of data might become a big issue for the current system architecture. Ref [63] mentioned the following challenges to integrate them seamlessly: high transaction storage costs, communication latency, and bandwidth limitations. To overcome these constraints, further blockchain consensus mechanism development is required, such as sharding or hybrid systems, to ensure the performance is efficient even under resource-constrained environments.

Interoperability between the blockchain, AI, and IoT systems will be a big challenge, especially in the military context, where there is a lot of technology and legacy systems. Moreover, researchers [91] emphasized the need for standardized protocols to allow smooth communication and integration among platforms. Further, the integration points must be secure, as vulnerabilities at the intersections may compromise the efficiency of the whole system.

This could finally bring a paradigm shift in the way military decisions are reached by integrating blockchain-enabled frameworks with AI and IoT. Integration of the blockchain features of security and transparency, the analytical power of AI, and the real-time data collection of IoT allows military organizations to create strong systems for conducting strategic planning, operational execution, and resource management. However, this realization of benefit is very important by adopting adequate measures related to scalability, interoperability, and security. Further research and development will be important in this area to fully realize the potential of integrated technologies to improve military decision-making and operational effectiveness.

5. Discussion

This paper has conducted a systematic review of the application of blockchain in the military domain, drawing insight from a multidomain search across scientific databases. A total of 43 papers were included for a more in-depth analysis. Table 3 summarized their relevance, frequency of keywords, and identified technical areas. In the next section, these findings are put into context to discuss the implications and future research directions for employing blockchain in the military. The following section discusses the implications of the literature review regarding the application of blockchain in the military domain. Based on classified articles, several opportunities arise when applying blockchain in a military operational environment. As an immutable distributed ledger, the use of blockchain leads to the pursuit of operational efficiencies, while possibly boosting or maintaining the same capabilities at best efforts or improving security. It enables new capabilities, such as machine-to-machine device security, to combat anti-tampering and forensics. As a result, an increased drive in research applies blockchain to industrially relevant problems to incorporate advanced technologies, including distributed ledgers and intelligent systems for problem-solving. Research problems have been defined that address a wide range of issues, such as data privacy and security, connectivity, trust, identity, verification, discipline enablers, data replication and consensus, sharing and exchange, and emergent behaviors such as trust propagation and disambiguation. Technical issues have been identified as barriers to adoption, while possible solutions have been suggested. Integration of the blockchain with existing systems is recognized as a significant challenge, which may be time-consuming, while some research questions remain open, such as staff readiness and resistance to blockchain adoption and the assessment of human capabilities to operate blockchain technology under different threat scenarios. An emerging area of research focuses on hyperconnected platforms, and through strategic alliances or studied alone, there is potential to exploit the internal business cases to accelerate the distributed ledger technology business application landscape in the military domain [94–100].

 doi:10.20944/preprints202411.2266.v1

Scalability Solutions for Blockchain Deployment in Military Supply Chains

Scalability is one of the most critical challenges in the deployment of blockchain into military supply chains, since it entails a large volume of data and transactions. The resolution of such issues demands innovative approaches that will ensure the blockchain systems can successfully handle increasing demands without trading off performance or security. One promising solution is sharding, which divides the blockchain network into smaller, manageable partitions called shards. This way, each share will process a subset of the transactions independently, which increases the throughput and scalability tremendously. Especially in military contexts, where operations span more than one region, the system will keep working even if some shards are compromised or destroyed, as proved by the study [61]. Built on top of a main blockchain, Layer 2 solutions offload transaction processing to reduce congestion and increase speed. With the help of mechanisms like state channels or sidechains, Layer 2 implementations efficiently realize fast and high-frequency transactions. They are especially meaningful for the values in military inventory management applications, where updating is often needed.

Furthermore, another study [91] has shown that Delegated Proof-of-Stake increases scalability and decreases latency in IoT networks of military applications. Interoperability solutions provide various blockchain systems with the ability to interact, share data, and distribute workloads over networks. This is essential in coordinating different military branches and allied forces, which may be using different blockchain systems. Hybrid blockchain architectures combine public and private blockchains in a manner that strikes an optimum for sensitive and insensitive tasks. By segregating critical data onto private chains and less-sensitive operations onto public chains, hybrid architecture reduces the load on the overall system and increases scalability. Off-chain processing eases the load on the primary blockchain in performing computations or storing data off the network. With systems like IPFS, efficient data storage retains blockchain connectivity. Especially effective is the storage of the off chain of detailed military maintenance records and the reflection of summaries on the blockchain.

Tokenization simplifies supply chain operations by enabling assets to be easily represented in tokens, while smart contracts automate processes such as inventory updates and procurement approval, increasing scalability and reducing manual intervention. BaaS platforms give an out-of-the-box, pre-configured infrastructure for the deployment of scalable blockchain systems, hence obliterating the need for custom-built solutions. They have features like auto-scaling, where the capacity of the system adjusts automatically to the network demand. These are particularly useful when there is the need for fast deployment of blockchain systems in emergency cases. The scalability solutions of sharding, Layer 2 networks, optimized consensus mechanisms, and hybrid architecture give answer to the unique demands of the military supply chains. Such innovations ensure that blockchain systems can handle large-scale operations with resource constraints and provide interoperability while meeting the security and efficiency required for critical military logistics. With continued development, block-chain will find a way to transform how militaries manage their supply chains, rendering them resilient, transparent, and effective.

Enhancing Military Logistics with Blockchain Technology: Benefits and Transformations

The transformative benefits of blockchain technology could ensure military logistics of increased security, transparency, efficiency, and resilience throughout the supply chain. These align with the critical requirements from the nature of military operations, which demand logistical processes that are reliable, accountable, and adaptive in nature. The key benefits that blockchain brings to military logistics have to do with improved data security and integrity. First, blockchain forms a decentralized tamper-resistant ledger that ensures no unauthorized access can be gained; hence, it does ensure the security of sensitive logistical information, such as troop movement or supply location. Cryptographic mechanisms underlying blockchain make data virtually im-mutable, free from tampering or cyber-attacks—most critical, given the context of military operations, where even the slightest compromise in logistics data might have critical operational implications.

 doi:10.20944/preprints202411.2266.v1

Blockchain significantly enhances traceability and transparency within the supply chain. Its immutable records allow for the precise tracking of military assets, from procurement to deployment. This capability supports fraud, counterfeiting, and diversion of critical supplies. For example, blockchain can assure the authenticity of military equipment since it allows for provenance tracking, as identified by the researchers [86]. This is of much importance in ensuring that counterfeit components do not find their way into the supply chain, compromising operational effectiveness.

In such blockchain systems, smart contracts can be used to automate all the repetitive tasks of logistics, including those involving procurement approvals, inventory management, and payment settlement. That would reduce the risk of human error and decrease administrative overhead. Also, the study [68] noted the potential of smart contracts in clearing bottlenecks in military logistics workflows, ensuring the operations are executed quickly and reliably. The decentralized architecture of blockchain enhances resilience in military logistics networks. The continuity of operations is guaranteed by removing single points of failure through the implementation of blockchain in view of cyber-attacks or physical disruption. A decentralized approach is better within dynamic and hostile environments where the integrity of supply chains is kept intact.

Blockchain provides a standardized, secure platform for sharing data with military units, allied forces, and suppliers. This interoperability enhances coordination in joint operations while keeping stringent access control over the sensitivity of information. For instance, researchers [60] emphasized the role blockchain could play in information alignment and collaboration among the different stakeholders in the confluence of complex supply chain operations. This will allow real-time tracking of the state of assets and supplies throughout the logistic network. The capability will help with better inventory management, reduce delays, and improved decision-making with accurate and updated information related to the availability and location of resources. Also, other researchers [69] indicated how this real-time tracking capability could ensure that critical supplies are delivered on time during military operations.

Moreover, blockchain adds auditability and accountability, since all transactions and movements within the supply chain are recorded; hence, transparency is provided. This form of traceability supports the identification and proper handling of irregularities since traceability assures resources are actually allocated and used as intended. Possibility of auditing the whole supply chain strengthens accountability and reduces the risk of corruption or misuse of resources. The entire logistics for the military can benefit greatly from blockchain technology in terms of security, efficiency, transparency, and resilience. Blockchain technology, therefore, gives the military real-time tracking, a secure way of sharing data, and record-keeping that is tamper-resistant—all points to making it a transformational tool for managing complex and high-stakes military supply chains. With continued development, blockchain will likely mature into an integral component of military logistics systems and change how resources are managed and deployed in major operations.

Blockchain-Enabled Interoperability in Military Logistics: Challenges and Opportunities

Interoperability is one of the most important aspects in military logistics, which guarantees seamless coordination and integration across different systems, units, and allies. This is where blockchain technology has great potential to help solve the interoperability complexity of military logistic issues by providing standard, secure, and transparent data-sharing and collaboration. Military logistics usually involves several stakeholders, including different branches of the armed forces, allied nations, and civilian agencies. Most of these stakeholders will have separate and sometimes incompatible logistical systems, resulting in a lack of efficiency in information and resources flow. Using blockchain technology, some of these pains are soothed, since it enables cross-system compatibility. Blockchain creates a unified platform where data can be shared securely among the stakeholders, keeping tight control over access to sensitive information.

One of the major benefits blockchain brings to interoperability is standardization of data formats and processes across different entities. With smart contracts, blockchain ensures that all transactions are carried out based on predefined protocols, which reduces discrepancies and allows the interaction between logistics systems to be smoother. For example, another study [81] proposed a blockchain framework that improves communication and data sharing for better integration among

 doi:10.20944/preprints202411.2266.v1

heterogeneous platforms across military supply chains. Blockchain also provides secure mechanisms for sharing data to bring about trust and collaboration among stakeholders. In other words, blockchain is an immutable record, and this guarantees a single source of truth that can be available to all parties, reducing misunderstandings and promoting accountability. This is even more critical in joint military operations, where clear communication and trust among forces must be guaranteed for the operation to succeed. Also, researchers [60] have pointed out the role of blockchain in improving information alignment and coordination, which will ensure logistic operations are in sync and effective.

Furthermore, the decentralized architecture of blockchain further supports interoperability since there is no need to depend on a central authority for managing data exchange. The use of this distributed approach has made logistic networks much more resilient, given that the operation will continue even when some nodes or systems are compromised. Authors [83] also noted that the decentralized aspect of blockchain is valuable in dynamic military settings where operational integrity must be highly maintained. Another big plus to interoperability, in this case through blockchain for military logistics, lies in its ability to provide granular access controls. In other words, the different levels of access are accorded to different stakeholders; sensitive information is only made available to personnel with authorized access, while operations deemed less critical can be shared widely. This feature is expected to improve collaboration without compromising security.

Applying blockchain for interoperability in military logistics is not without its challenges. Compatibility between the blockchain systems and the existing legacy infrastructure requires much technical and organizational effort. Moreover, standardizing protocols across multiple entities with unique operational requirements is a complex task. Such a challenge can be met only by frameworks and agreements in which all stakeholders work together to adopt interoperable blockchain solutions. In a nutshell, there is transformative potential for interoperability with military logistics using blockchain technology. Some of the added advantages of decentralized resilience include standardization of processes and safe data sharing; hence, it is the perfect solution for the integration of diverse logistics systems and stakeholders. Overcoming challenges in protocol standardization and with legacy systems, blockchain will enhance coordination, trust, and efficiency in military logistics operations, therefore supporting more effective and cohesive missions.

Unlocking Blockchain's Potential in Transforming Military Operations

Blockchain technology can be of great importance in the transformation of military operations in view of its characteristics: decentralization, transparency, immutability, and cryptographic security. This would be tailor-made to meet the modern requirements that military systems place on the operational parameters of security, efficiency, and adaptability. In cybersecurity, blockchain will assure strong defenses against data breaches, distributed denial-of-service attacks, and insider threats through the creation of immutable records that protect sensitive information, such as troop movements and intelligence reports. Future integrations of quantum-resistant cryptographic protocols will only seek to further increase the role of blockchain in military cybersecurity. Another area where blockchain could make a transformative difference is interoperability. In multinational military operations or coalition forces, it could provide a standardized, secure, and efficient platform for communications and coordination between countries, branches, or units through the establishment of common protocols, enabling sharing of encrypted data with granular access controls.

Blockchain could also enable the management of autonomous systems and Io DT devices, ensuring that operations of unmanned vehicles, drones, and sensors are secure through decentralized identity verification and tamper-proof mechanisms for command and control. Smart contracts could automate maintenance schedules and resource allocation to further increase the efficiency and readiness of such systems. Blockchain in military logistics can provide the level of transparency, traceability, and security required for supply chains. It will help in the reduction of counterfeiting risks and tampering because immutable provenance records for each item ensure authenticity and accountability. Smart contracts could streamline procurement, inventory management, and delivery processes, which would effectively bring about the elimination of inefficiencies and assurance that

 doi:10.20944/preprints202411.2266.v1

resources are being allocated effectively. Its architecture could also be leveraged to provide secure and resilient communication networks, which would be important in keeping real-time, secure communication channels open in contested environments. For example, blockchain-enabled satellite communications could provide superior reliability for global military operations. Moreover, blockchain transparency and auditability could support strategic decision-making by better tracing resource allocation, mission results, and compliance with protocols governing operations. Indeed, the ability of blockchain to store complete and immutable records could underpin scenario simulations, risk assessments, and strategy optimization in real time.

It will allow the realization of decentralized command and control systems operating in dynamic and hostile environments, where distributed units can be autonomous yet securely connected to the wider network, hence guaranteeing continuity of operations when centralized systems are disrupted. While it has potential, blockchain in military applications faces several challenges, such as scalability, energy efficiency, and integration with prevailing systems. In this regard, standardized frameworks and protocols will be imperative to ensure interoperability among the different military organizations. A new generation of lightweight consensus mechanisms and quantum-resistant cryptography can best scale the application and provide long-term security. The future of blockchain in military applications is bright, and it has the potential to fundamentally change how military forces operate in the digital age. Strategic investment in research, development, and integration will be critical to unleash the full potential of blockchain and helping to address the unique challenges associated with military environments.

Integrating Blockchain Technology into Modern Warfare Strategies

Integration of blockchain in the strategies of warfare can redefine the very way in which military forces operate, coordinate, and execute missions in the digital era. Its decentralized, immutable, and cryptographic features make it a strong solution for enhancing security, efficiency, and resilience in complex and high-stakes environments. Modern warfare, with its increasing dependence on digital infrastructure, is therefore deeply intertwined with the role that blockchain can play in shaping future strategies. Blockchain is one of the basic technologies in cybersecurity, which guarantees the security of communication networks and critical systems from cyber threats. It is decentralized; hence, there are no central points of failure. It makes networks resilient to attacks such as Distributed Denial of Service (DDoS). Plans and intelligence operatively cannot be manipulated or altered in a blockchain due to its immutability. This degree of security is especially important in adversarial environments where data integrity can impact mission success. The integration of quantum-resistant cryptography into blockchain architectures will be imperative to provide this security against the new threats' quantum computers pose. Blockchain will also help command and control operations by letting the system be decentralized, reducing reliance on centralized nodes. This will ensure that operations are continued in case parts of the network are disrupted or compromised. In addition, blockchain-based platforms may provide real-time updating and secure communication between units for effective coordination on the battlefield. Automating mission-critical decisions based on pre-defined conditions using smart contracts can reduce delays in dynamic combat scenarios, thereby helping forces adapt to changed circumstances swiftly.

Military logistics came to integrate blockchain in the supply chain for traceability and authenticity of resources. The immutable ledgers could be used for tracking equipment, ammunition, and other supplies from origination to deployment, reducing the likelihood of counterfeit materials making it into the supply chain. Automated procurement, aided by smart contracts, can increase efficiency in ensuring that troops have access to all necessary resources on time. Blockchain also ensures greater transparency in resource allocation to fight fraud and mismanagement. Interoperability between allied forces is an essential element to coalition warfare. The secure, encrypted sharing of information and data is possible through standardization of data formats, which allows blockchain to increase coordination among otherwise disparate military entities that maintain strict controls over access. More importantly, this becomes exponentially more relevant in any multi-national operation where trust and real-time information exchange are paramount.

 doi:10.20944/preprints202411.2266.v1

Autonomous systems and the Internet of Things are increasingly being integrated with warfighting strategies; blockchain is at the center of their secure deployment. Blockchain could be used to manage identity and communications for unmanned vehicles, drones, and IoT devices, ensuring that they function securely under authorized control. Technology can provide tamper-proof records and automate through smart contracts, enabling predictive maintenance and reducing equipment downtime to improve operational readiness. Blockchain can enable transparent and auditable records to be created. This, therefore, means that the ethical and legal dimensions of warfare will be affected because an immutable record of actions and decisions can support adherence to international laws, including accountability in military operations. Of course, that kind of transparency enhances post-mission analysis and thus helps to refine strategies for better future operations.

Integration of blockchain in the strategy of warfare is confronted with the challenge of scalability, especially in large-scale operations involving a high volume of transactions. Energy efficiency becomes a critical element in resource-constrained environments. Integration with the already existing military systems and protocols requires much effort and coordination. In addition, due to the fast movement of cyber threats, continuous research and adaptation are crucial to keep blockchain technology ahead of emerging vulnerabilities. This is to say, blockchain integration into the strategies of warfare assures transformative opportunities in the realm of security, coordination, and efficiency of military operations. Once the current challenges are overcome and the capabilities of blockchain continue to be built, this will enable military forces to tap into this technology for strategic advantages in an increasingly digital and intertwined battlespace. Blockchain is one of the cornerstones in securing operations, managing resources, and enabling real-time decision-making in future warfare strategies.

Enhancing Military AI Capabilities through Blockchain Integration

Blockchain can be leveraged to bring about important improvements in the deployment, security, and efficiency of AI in military operations. The architecture of blockchain, combined with its decentralized, immutable, and secure nature, in addition to the adaptability and processing power of AI, brings forth systems capable of managing complex, high-stakes environments. This will address challenges of data integrity, decision-making, and operational resilience critical to the process. Blockchain can improve the authenticity of the data on which military AI is trained. The accuracy and quality of the data in AI decision-making, where misinformation or compromised data can lead to disastrous consequences in the military domain, are of paramount importance. Blockchain ledger guarantees the authenticity of the data fed into AI models, and that the data is tamper-proof.

Of special importance are applications in intelligence analysis, autonomous systems, and battlefield decision support, where data quality is critical in making trustworthy decisions for effective operations of AI systems. The integration of blockchain with AI can also enhance data sharing between various military units, allied forces, and autonomous systems. Blockchain allows for secure and transparent sharing of information, making sure that all entities involved in an operation have access to consistent and verified data, enhancing the interoperability of AI systems, which can work together with ease while ensuring security. For example, blockchain could enable secure data exchanges between AI-based drones, unmanned vehicles, and command centers with real-time situational awareness and decision-making capabilities.

In this regard, smart contracts embedded in blockchain systems can automate various AI processes of military operations. Such self-executing contracts can, therefore, trigger AI actions based on predefined conditions, ensuring that tasks are executed efficiently and without delay. For example, resource allocation, mission planning, or activation of defensive measures can be automatized through smart contracts by analyzing real-time battlefield conditions using AI. With such an approach, fewer humans are required to intervene, making the response time faster and more precise in dynamic scenarios. Blockchain enhances the security of AI systems by protecting against cyberattacks. AI systems are vulnerable to adversarial attacks, where malicious actors manipulate input data to influence AI decisions. Blockchain's decentralized and cryptographic nature mitigates

 doi:10.20944/preprints202411.2266.v1

these risks by providing a secure environment for data storage and processing. Additionally, blockchain can create an audit trail for AI decisions, enabling transparency and accountability.

That's especially helpful in high-stakes military applications, where it's important to know the reasoning behind AI-driven decisions. A combination of blockchain with AI can therefore optimize the deployment and management of autonomous military systems. In this respect, blockchain offers decentralized identity management, securing the authentication and monitoring of autonomous systems in a manner that only authorized entities can control them, hence minimizing the possibility of unauthorized access or tampering with unmanned vehicles, drones, or robotic systems. This will even enable predictive maintenance of the systems by blockchain, since the secure recording of operational data and analysis of performance trends through AI guarantees readiness and lowers downtime.

The high computing requirements typically ask for AI to have access to vast, decentralized networks. Blockchain could allow distributed computing frameworks where AI algorithms harness the combined power of several nodes. This distributed approach enhances not only the speed of computations but also the resilience of AI systems, thanks to the decentralization of operations and thus a lower likelihood of targeted attacks. Integration of blockchain with military AI, though having potential, also brings challenges. In this respect, if blockchain is to be integrated into real-time processing of the AI systems involved in critical military operations, it will need to overcome its scalability and latency issues. Besides, the energy-intensive nature of some blockchain consensus mechanisms may not be applied in resource-constrained environments. It will require advances in lightweight consensus protocols and scalable blockchain architecture.

In conclusion, blockchain can complement the military's AI in terms of data integrity, enabling secure sharing of data, automating processes, and protecting against cyber threats. Given its ability to create transparent, secure, and decentralized systems, blockchain complements the analytical and decision-making capabilities of AI by enabling more efficient and resilient military operations. Integration in military strategies and capabilities will be one that defines the future for these technologies.

Blockchain Applications in Defense: Enhancing Security, Transparency, and Efficiency

Blockchain technology has been increasingly applied in defense to enhance the security, transparency, efficiency, and operational integrity of various operations. Specifically, blockchain in supply chain management has been used to provide an authentically guaranteed supply chain for military equipment, spare parts, and materials. The U.S. Department of Defense has researched blockchain in the tracking of logistics processes to provide real-time visibility into the movement of goods and to prevent counterfeit components from entering the supply chain. NATO's Allied Command Transformation has experimented with blockchain technology to enhance trust and interoperability among its member nations, creating tamper-proof records of transactions, precluding fraud, and improving operational efficiency. Blockchain is also being used to address cybersecurity challenges in defense. The U.S. Air Force has partnered with blockchain firms to secure supply chains and data management processes, leveraging the technology's decentralized architecture to reduce cyberattack risks. Similarly, India's Ministry of Defense has explored blockchain to secure defense networks against cyber threats by decentralizing data storage and ensuring tamper-proof and auditable information management.

In autonomous systems, blockchain provides the security of drone and un-manned vehicle operations with decentralized identity management and tamper-proof logging. Those are capabilities that reduce the risk of unauthorized control and ensure the operational protocol is followed. The U.S. Navy has researched blockchain for the protection of IoT networks to make the types of connected systems used in defense operations more reliable and accountable. This has been witnessed with the integration of blockchain in defense systems for secure communication, where data transmission is highly secured. In this regard, Estonia has implemented blockchain to ensure the integrity of sensitive communications within its defense forces, protecting against possible cyber-attacks. NATO has explored blockchain to improve the secure sharing of data among member states, enabling trusted intelligence exchange in coalition operations. Blockchain also brings to defense the added benefits of

 doi:10.20944/preprints202411.2266.v1

financial transparency and accountability. DARPA has researched blockchain in tracking defense expenditure and fraud prevention through immutable records of financial transactions. The United Nations piloted blockchain in peacekeeping missions for the transparent use of resources and funds that are otherwise guaranteed to reach their intended recipients.

Many countries are involved in blockchain-related R&D to explore more applications. The Chinese government has placed the use of blockchain for logistics, cybersecurity, and operation planning on the priorities list for military modernization. Russia has invested in blockchain for its secure communication and data management within its defense infrastructure. These real-life use cases show how blockchain can be a game-changer in defense operations, bringing transparency, security, and efficiency. From securing supply chains to autonomous systems, improving financial accountability, and communication, blockchain addresses some of the critical challenges being faced by modern defense organizations. With continuity in development, it is fast becoming a cornerstone of digital transformation in defense and offering durable solutions to very complex operational needs.

Limitations of Blockchain Technology in Defense Applications

Blockchain technology—while dramatically increasing the security, transparency, and efficiency of defense— does have some limitations that affect feasibility and effectiveness within the military context. These limitations result from the inherent technological constraints, integration challenges, and operational considerations peculiar to defense environments. Among all the major limitations of blockchain in defense, scalability is nearest to the top. Military operations create large volumes of data and require real-time processing, which current blockchain systems cannot handle in most cases. Traditional blockchain consensus mechanisms, like Proof of Work, are slow and resource-intensive—thus not fitting well with applications requiring real-time responses, including battlefield communications or dynamic supply chain management. High transaction storage costs, communication latency, and the demands on bandwidth further degrade the scalability concerns, particularly in resource-constrained environments such as remote deployments or conflict zones [63]. Energy consumption is another major limitation, more so for blockchain networks based on PoW. The operations are often carried out in environments with a dearth of, or required to be preserved for core functions, energy resources. High energy requirements, therefore, render traditional blockchain implementations impractical for certain defense applications, like drone swarms or edge devices on the Internet of Things (IoT) networks [92].

Integration challenges also impede the adoption of blockchain in defense. The military systems are mostly based on old infrastructure which is not compatible with modern blockchain solutions. Integration of blockchain with the existing systems faces challenges in terms of extensive technical efforts, resource investment, and planning to ensure seamless operations. The lack of standardization of blockchain protocols further deteriorates interoperability challenges, especially in multinational defense operations or coalition environments where diverse technologies must work cohesively [91]. Integration points bring other risks to security. Whereas the blockchain is highly secured, the vulnerabilities of blockchain appear at the integration points where blockchain will interact with other technologies such as IoT sensors, AI systems, communication networks, etc. Blockchain systems, in general, might be put at risk when cyber-attacks target these integration points [65].

Finally, the latency in blockchain transactions may also create issues within the time-sensitive defense operation. Since blockchain is based on a validation process that is decentralized, transaction confirmation is relatively slow and might not be attuned to the fast-decision-making needs within military contexts, such as real-time threat response or tactical adjustments during combat operations [63]. Another concern is the potential for adversarial exploitation of blockchain technology. In fact, despite being secure, blockchain could still stand the test of time against sophisticated adversaries seeking to discover new methods for breaching or exploiting blockchain networks; for example, quantum computing represents a potential threat to the cryptographic foundations of current blockchain systems. Advances in quantum computing technology could eventually make it possible to break encryption algorithms, which would leave blockchain networks vulnerable if countermeasures such as quantum-resistant cryptography are not developed and implemented [72].

 doi:10.20944/preprints202411.2266.v1

Further barriers to blockchain adoption in defense include operational secrecy and data sensitivity. Whereas blockchain's transparency and immutability are great advantages when it comes to accountability, they may become liabilities where the military operation needs to curtail information visibility. The amount of data put on the blockchain and who can access it have to be weighed very carefully to balance transparency with operational security [77].

Third, it is prohibitively expensive to implement and maintain blockchain systems in defense contexts. The costs of initial set-up, continued maintenance, and specialized technical expertise may become inhibitive to widespread adoption. This especially becomes an issue in budget-constrained environments where resources need to be carefully allocated across numerous defense priorities [75]. In other words, blockchain technology, while promising in its potential to transform defense operations, still faces major scalability, energy efficiency, integration, security, and operational practicality challenges that need to be overcome if the full potential of this technology is to be realized. This will require further research and development into more efficient consensus mechanisms and techniques for integration.

Ethical Considerations of Blockchain Technology in Military Applications

Integration of blockchain in military applications raises several ethical concerns. These should be very well considered, especially as its integration increases in critical areas such as command and control, supply chain management, autonomous systems, and intelligence operations. Ethical considerations range from privacy and accountability to security and potential misuse of technology. This would give rise to a very serious moral concern in the effects it would have on privacy: whereas blockchain is feted for its transparency and immutability, these could inadvertently lay bare sensitive military data. For example, using blockchain to maintain personnel or track supplies might give up information that could compromise operational security or put military personnel at risk if an adversary accessed the data.

Even in the so-called permissioned blockchain systems, problems of unauthorized access or accidental disclosures are among the critical ethical concerns [72]. Another great ethical challenge will be accountability and decision-making within autonomous military systems. Blockchain-enabled frameworks, used in conjunction with AI and IoT, may create decentralized decision-making systems where responsibility for specific actions becomes hard to trace. For example, if a blockchain-audited autonomous drone makes a critical decision in combat, tracing who is accountable—be it a developer, an operator, or a system architect—becomes very difficult.

This lack of clear accountability might undermine trust and create moral dilemmas in military operations [91]. Although operational transparency is normally considered an advantage, it can also become an ethical conflict. The immutable records of blockchain are ideal for accountability, but the transparency requirement may come into conflict with the need of the military to keep some operations confidential. Balancing accountability and operational secrecy continue to be a challenge, especially in coalition or joint-force operations where access levels may have to be differentiated [77].

Another concern is that the blockchain might be misused. Characteristics of blockchain—all upholding promises to provide secure, anonymous, and decentralized systems—may be used by malicious actors or rogue states to obscure illegal or unethical activities within military operations. For instance, blockchain could potentially be used to launder arms transfers not approved by the United Nations, fund covert operations, or obscure accountability in human rights abuses [72].

Automation and smart contracts elevate ethical questions around issues of proportionality and discrimination in combat scenarios. It becomes ambiguous whether international humanitarian laws can be followed once the smart contracts trigger automated actions according to predefined conditions, for instance, starting an autonomous strike due to sensor data. One of the critical ethical imperatives is how blockchain-based systems maintain the principles of distinction and proportionality, specifically in the decision between life and death [65].

Blockchain technologies, especially those dependent on energy-intensive consensus mechanisms such as Proof of Work, pose an ethical issue in military contexts due to their environmental impact. If implemented in resource-scarce environments, these could further drain energy supplies needed for other critical operations, which raises questions on the responsible use of

 doi:10.20944/preprints202411.2266.v1

resources [63]. Another challenge in coalition operations includes trust and equitability. Where multiple nations or entities are involved, the blockchain-enabled military system will need to ensure equitable access and assurance of transparency in trust and decision-making. Lopsidedness in capability, technological or control over the blockchain systems could create unequal power dynamics and undermine trust between allies [78].

Lastly, there are long-term risks of technological dependency that raise ethical concerns. Heavy reliance on blockchain systems for critical military operations could create vulnerabilities if adversaries were to develop disruptive technologies like quantum computing, which might compromise the very basis of blockchain's cryptographic security. This reliance may also stifle the development of alternative systems and create a dangerous monoculture in military technology [90]. It is therefore concluded that blockchain brings transformative potential to military operations, but its ethical implications must be observed with the greatest care. If the integration in the military is to conform to ethical norms and international laws, addressing concerns about privacy protection, accountability, transparency, misuse, and environmental impact will be of utmost importance. Strong regulation, ethical frameworks, and continuing dialogue among stakeholders will be very important in dealing with these challenges responsibly.

Future Directions

For a deeper understanding of these and upcoming blockchain applications in the military domain, more research and pilot projects need to be conducted in various sections. For instance, intermediate agents such as the Federal Office of Defense Technology and Procurement or military alliances are conceivable. Interestingly, Sweden and Denmark share the same Joint Support Service; they are using a blockchain-based system that might be a potential cooperation opportunity. A further necessary step towards the adoption of technology is the conduction of real-world pilot projects. Apart from the technological considerations, legislation and ethical concerns need to be captured upfront. Therefore, interdisciplinary research is needed. It is the endeavor to involve, compromise, and discipline alike: politicians and military staff, national and international stakeholders, private entities and academies, knowledge experts, front-runners, and those showing a certain reluctance to agree [101–106].

Interesting research questions include: What tasks and procedures in the logistics sector of the military domain are suitable to be executed on a blockchain decentralized solution? In how far are blockchain and other decentralized solutions suitable in military supply chains and military operations, regarding flexibility and resilience towards outages and cyberattacks? Are there perspectives for military supply chain sustainability by deploying blockchain or similar technology? How can interdisciplinary blockchain strategies ensure compatibility, connective platforms, and interoperability between various stakeholders, military services, allied countries, partners, and contractors in military operations? The emergence of processes and information technology has resulted in the evolution of blockchain platforms with AI for IoT solutions. In the warfare scenario today and in the future, that is the capability of influence blockchain platforms, but the combined platform is rarely mentioned. Finally, interdisciplinary research is needed into the broad applicability of blockchain techniques and decentralized applications. Additionally, legal issues, costs, and ethical considerations should be investigated, as they are relevant to the approval and implementation of the technique. Therefore, a framework for security and cyber risk management with respect to legal issues and ethical considerations must be developed. Representatives of different fields should come together to apply these regulations, because security is a common property of attacking, drawing, and living [107–111].

Furthermore, to allow the implementation of the concept of exclusive logistics, the concept must be implemented by economic and academic research. The first step is to establish a test diamond in the zoo of virtual worlds, which could already be derived from practical military currents such as unmanned aerial vehicles and drones. Policymakers, military planners, and civilian society are increasingly looking at potentialities and future landscapes. Blockchain or a valorization of the concept of distributed information and publicity could also be sniffed at an exclusive functional

 doi:10.20944/preprints202411.2266.v1

manageability of services, since it has been proven that a huge number of large entities do not trust one another unconditionally [112–115].

6. Conclusions

In conclusion, this research paper underscores the transformational capability of blockchain technology to enhance military operations across all domains, especially in the areas of data security, supply chain management, and secure communication. The inherent features of decentralization, transparency, and immutability of blockchain are especially valuable solutions to some of the most critical challenges in a military context, including data integrity, operational transparency, and the resilience of systems. Still, it also faces some challenges in blockchain integration, such as issues of scalability, energy consumption, and compatibility with the already existing military infrastructure. It contributes to the requirements of further research and development to overcome such challenges and to optimize the employment of blockchain in the military. Moreover, the potential for the integration of blockchain with emerging technologies, such as AI and IoT, has been identified to further improve decision-making, situational awareness, and operational management. The successful implementation of blockchain in military operations will need to address the security and ethical considerations together with the technical and operational constraints. The results of this research indicate that blockchain can revolutionize military logistics, cybersecurity, and communication in a way that supports increased strategic planning and operational effectiveness. Thus, future research should focus on the improvement of consensus mechanisms, interdisciplinary approaches, legislative, and ethical implications of blockchain technologies to extract the maximum possible benefit for the military sector.

Author Contributions: Conceptualization, N.K. and H.A.; methodology, C.H.; software, I.S.; validation, I.S. and C.H.; formal analysis, C.H.; investigation, N.K. and C.H..; resources, I.S.; data curation, C.H.; writing—original draft preparation, N.K. and H.A.; writing—review and editing, I.S. and C.H.; visualization, C.H.; supervision, I.S.; project administration, H.A.; funding acquisition, H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Davis, S. I. (2022). Artificial intelligence at the operational level of war. Defense & Security Analysis. https://doi.org/10.1080/14751798.2022.2031692
2. Mattingsdal, J., Johnsen, B. H., & Espevik, R. (2023). Threat conditions on police and military commanders' preferences for urgent and offensive actions: An analysis of decision-making at the operational level of war. Military Psychology. https://doi.org/10.1080/08995605.2023.2277609
3. Mattingsdal, J., Espevik, R., Johnsen, B. H., & Hystad, S. (2023). Exploring why police and military commanders do what they do: An empirical analysis of decision-making in hybrid warfare. Armed Forces & Society. https://doi.org/10.1177/0095327X231160711
4. Johnson, J. (2023). Automating the OODA loop in the age of intelligent machines: Reaffirming the role of humans in command-and-control decision-making in the digital age. Defence Studies. https://doi.org/10.1080/14702436.2022.2102486
5. Horyń, W., Bielewicz, M., & Joks, A. (2021). AI-supported decision-making process in multidomain military operations. In Artificial Intelligence and Its Contexts: Security, Business, and Governance (pp. 93-107). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-88972-2_7
6. Bolton, C. R., & Prescott, M. R. (2024). Commander's critical information requirements: Crucial for decision-making and joint synchronization. Joint Force Quarterly.
7. Theodorakopoulos, L., Theodoropoulou, A., & Halkiopoulos, C. (2024). Enhancing Decentralized Decision-Making with Big Data and Blockchain Technology: A Comprehensive Review. Applied Sciences, 14(16), 7007. https://doi.org/10.3390/app14167007

8. Halkiopoulos, C., Antonopoulou, H., & Kostopoulos, N. (2023). Utilizing Blockchain Technology in Various Applications to Secure Data Flows. A Comprehensive Analysis. Technium: Romanian Journal of Applied Sciences and Technology, 11, 44–55. https://doi.org/10.47577/technium.v11i.9132
9. Aoun, A., Ilinca, A., Ghandour, M., & Ibrahim, H. (2021). A review of Industry 4.0 characteristics and challenges, with potential improvements using blockchain technology. Computers & Industrial Engineering, 162, 107746. https://doi.org/10.1016/j.cie.2021.107746
10. Khan, A. A., Laghari, A. A., Li, P., Dootio, M. A., & Karim, S. (2023). The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises. Scientific Reports. https://doi.org/10.1038/s41598-023-28707-9
11. Reghunadhan, R. (2020). Ethical considerations and issues of blockchain technology-based systems in war zones: A case study approach. In Handbook of Research on Blockchain Technology. https://doi.org/10.1016/B978-0-12-819816-2.00001-0
12. 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
13. Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for modern applications: A survey. *Sensors*. https://doi.org/10.3390/s22145274
14. Kassen, M. (2022). Blockchain and e-government innovation: Automation of public information processes. *Information Systems*. https://doi.org/10.1016/j.is.2021.101862
15. Abdulrahman, Y., Arnautović, E., Parezanović, V., & Svetinovic, D. (2023). AI and blockchain synergy in aerospace engineering: An impact survey on operational efficiency and technological challenges. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3305325
16. Khoshavi, N., Tristani, G., & Sargolzaei, A. (2021). Blockchain applications to improve operation and security of transportation systems: A survey. *Electronics*. https://doi.org/10.3390/electronics10050629
17. Lee, S., & Kim, S. (2021). Blockchain as a cyber defense: Opportunities, applications, and challenges. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3136328
18. Shahzad, K., Aseeri, A. O., & Shah, M. A. (2022). A blockchain-based authentication solution for 6G communication security in tactile networks. *Electronics*. https://doi.org/10.3390/electronics11091374
19. Jain, A., Barke, S., Garg, M., Gupta, A., Narwal, B., Mohapatra, A. K., ... & Srivastava, G. (2024). A walkthrough of blockchain-based internet of drones architectures. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2024.3447465
20. Kendall, A., Das, A., Nagy, B., Johnson, B., & Ghosh, A. (2022). Using hyperledger fabric blockchain to improve information assurance of IoT devices for AI model development. In *Advances in Blockchain Technology for Cyber Physical Systems* (pp. 233-259). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-93646-4_11
21. Aljohani, M., Mukkamala, R., & Olariu, S. (2024). Autonomous strike UAVs in support of homeland security missions: Challenges and preliminary solutions. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3420235
22. Bothra, P., Karmakar, R., Bhattacharya, S., & De, S. (2023). How can applications of blockchain and artificial intelligence improve performance of Internet of Things?-A survey. *Computer Networks*. https://doi.org/10.1016/j.comnet.2023.109634
23. Theodorakopoulos, L., Theodoropoulou, A., & Stamatiou, Y. (2024). A State-of-the-Art Review in Big Data Management Engineering: Real-Life Case Studies, Challenges, and Future Research Directions. Eng, 5(3), 1266–1297. https://doi.org/10.3390/eng5030068
24. Bagga, P., Das, A. K., Chamola, V., & Guizani, M. (2022). Blockchain-envisioned access control for internet of things applications: A comprehensive survey and future directions. *Telecommunication Systems*. https://doi.org/10.1007/s11235-022-00938-7
25. Stamatiou, Y., Halkiopoulos, C., & Antonopoulou, H. (2023). A Generic, Flexible Smart City Platform focused on Citizen Security and Privacy. Proceedings of the 27th Pan-Hellenic Conference on Progress in Computing and Informatics. https://doi.org/10.1145/3635059.3635095
26. Mohan, D., Alwin, L., Neeraja, P., Lawrence, K. D., & Pathari, V. (2022). A private Ethereum blockchain implementation for secure data handling in Internet of Medical Things. *Journal of Reliable Intelligent*

Environments, 8(4), 379-396. https://doi.org/10.1007/s40860-021-00153-2

27. Surya, S., Elakya, R., & Selvanayaki, S. (2024). Synergizing aerospace efficiency: Blockchain and AI integration for enhanced security in flight data management. In *AI and Blockchain Optimization Techniques in Aerospace Engineering* (pp. 181-192). IGI Global. https://doi.org/10.4018/979-8-3693-1491-3.ch009
28. Kumari, S., & Muthulakshmi, P. (2023). Artificial intelligence-blockchain-enabled technology for Internet of Things: Research statements, open issues, and possible applications in the near future. *Privacy Preservation of Genomic and Medical Data* (pp. 433-480). https://doi.org/10.1002/9781394213726.ch18
29. Khan, M., Imtiaz, S., Parvaiz, G. S., Hussain, A., & Bae, J. (2021). Integration of Internet of Things with blockchain technology to enhance humanitarian logistics performance. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3054771
30. Rahimi, A., Akhavan, P., Philsofian, M., & Darabi, A. (2022). Investigating the effect of using blockchain technology on collaborative interactions and performance improvement in the defense industry supply chain. *The Journal of Industrial Management Perspective, 12*(45), 109-134. https://doi.org/10.52547/jimp.12.1.109
31. Ahmad, R. W., Hasan, H., Yaqoob, I., Salah, K., Jayaraman, R., & Omar, M. (2021). Blockchain for aerospace and defense: Opportunities and open research challenges. *Computers & Industrial Engineering, 151*, 106982. https://doi.org/10.1016/j.cie.2020.106982
32. Dubey, R., Gunasekaran, A., & Foropon, C. R. (2024). Improving information alignment and coordination in humanitarian supply chain through blockchain technology. *Journal of Enterprise Information Management, 37*(3), 805-827. https://doi.org/10.1108/JEIM-07-2022-0251
33. Zhang, S., Li, Y., Ge, W., & Shen, X. (2022, July). Military application of blockchain technology for future battlefield operations. In *International Conference on Cloud Computing, Internet of Things, and Computer Applications (CICA 2022)* (Vol. 12303, pp. 352-362). SPIE. https://doi.org/10.1117/12.2642579
34. Reyes, P. M., Gravier, M. J., Jaska, P., & Visich, J. K. (2022). Blockchain impacts on global supply chain operational and managerial business value processes. *IEEE Engineering Management Review, 50*(3), 123-140. https://doi.org/10.1109/EMR.2022.3187729
35. Sani, S., Schaefer, D., & Milisavljevic-Syed, J. (2022). Strategies for achieving pre-emptive resilience in military supply chains. *Procedia CIRP*. https://doi.org/10.1016/j.procir.2022.05.186
36. Raja Santhi, A., & Muthuswamy, P. (2022). Influence of blockchain technology in manufacturing supply chain and logistics. *Logistics*. https://doi.org/10.3390/logistics6010015
37. Park, A., & Li, H. (2021). The effect of blockchain technology on supply chain sustainability performances. *Sustainability*. https://doi.org/10.3390/su13041726
38. Al-Zaqeba, M., Jarah, B., Ineizeh, N., Almatarneh, Z., & Jarrah, M. A. A. L. (2022). The effect of management accounting and blockchain technology characteristics on supply chains efficiency. *Uncertain Supply Chain Management, 10*(3), 973-982. https://doi.org/10.5267/j.uscm.2022.2.016
39. Batwa, A., & Norrman, A. (2020). A framework for exploring blockchain technology in supply chain management. *Operations and Supply Chain Management: An International Journal, 13*(3), 294-306. https://doi.org/10.31387/oscm0420271
40. Agarwal, U., Rishiwal, V., Tanwar, S., Chaudhary, R., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Blockchain technology for secure supply chain management: A comprehensive review. *IEEE Access, 10*, 85493-85517. https://doi.org/10.1109/ACCESS.2022.3194319
41. Hariguna, T., Durachman, Y., Yusup, M., & Millah, S. (2021). Blockchain technology transformation in advancing future change. *Blockchain Frontier Technology, 1*(01), 13-20. https://doi.org/10.34306/bfront.v1i01.4
42. Andrii, D., Zarina, P., Oleh, S., Olena, P., & Dmytro, R. (2024, April). Management of Transport and Logistics Systems: Problems Under Conditions of Military Operations. In *International Conference on Business and Technology* (pp. 363-373). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-67444-0_35
43. Katina, P. F., & Gheorghe, A. V. (2023). Blockchain-enabled resilience: An integrated approach for disaster supply chain and logistics management. https://doi.org/10.1201/9781003336082

44. Wamba, S. F., & Queiroz, M. M. (2020). Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. *International Journal of Information Management*. https://doi.org/10.1016/j.ijinfomgt.2019.102064
45. Kumar, R., Wang, W., Kumar, J., Yang, T., Khan, A., Ali, W., & Ali, I. (2021). An integration of blockchain and AI for secure data sharing and detection of CT images for the hospitals. *Computerized Medical Imaging and Graphics, 87*, 101812. https://doi.org/10.1016/j.compmedimag.2020.101812
46. Wan, P. K., Huang, L., & Holtskog, H. (2020). Blockchain-enabled information sharing within a supply chain: A systematic literature review. *IEEE Access*. https://doi.org/10.1109/ACCESS.2020.2980142
47. Wang, Z., Zheng, Z., Jiang, W., & Tang, S. (2021). Blockchain-enabled data sharing in supply chains: Model, operationalization, and tutorial. *Production and Operations Management, 30*(7), 1965-1985. https://doi.org/10.1111/poms.13356
48. Shen, M., Duan, J., Zhu, L., Zhang, J., Du, X., & Guizani, M. (2020). Blockchain-based incentives for secure and collaborative data sharing in multiple clouds. *IEEE Journal on Selected Areas in Communications, 38*(6), 1229-1241. https://doi.org/10.1109/JSAC.2020.2986619
49. Liu, H., Crespo, R. G., & Martínez, O. S. (2020). Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. *Healthcare*. https://doi.org/10.3390/healthcare8030243
50. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Moher, D. Updating guidance for reporting systematic reviews: Development of the PRISMA 2020 statement. *J. Clin. Epidemiology* **2021**, *134*, 103–112. https://doi.org/10.1016/j.jclinepi.2021.02.003.
51. Abed, N., & Hasan, S. (2020). A Proactive Secure File Approach Using a Blockchain Technique. DOI: https://doi.org/10.1080/09720529.2020.1727610
52. Abualigah, L., Diabat, A., Sumari, P., & Gandomi, A. (2021). Applications, Deployments, and Integration of Internet of Drones (IoD): A Review. DOI: https://doi.org/10.1109/JSEN.2021.3114266
53. Aggarwal, P., & Dixit, S. (2021). Blockchain-Envisioned UAV Communication Using 6G Networks: Open Issues, Use Cases, and Future Directions. DOI: https://doi.org/10.1109/JIOT.2020.3020819
54. Akter, F., Malik, M., & Rahman, S. (2023). IoMT-Net: Blockchain-Integrated Unauthorized UAV Localization Using Lightweight Convolution Neural Network for Internet of Military Things. DOI: https://doi.org/10.1109/JIOT.2022.3176310
55. Aldossri, K., & Saleh, H. (2024). Advancing Drone Operations Through Lightweight Blockchain and Fog Computing Integration: A Systematic Review. DOI: https://doi.org/10.3390/drones8040153
56. Amran, R., & Hassan, N. (2022). Efficient and Secure WiFi Signal Booster via Unmanned Aerial Vehicles WiFi Repeater Based on Intelligence-Based Localization Swarm and Blockchain. DOI: https://doi.org/10.3390/mi13111924
57. Asuncion, A., Hernandez, D., & Sato, K. (2021). Connecting Supplier and DoD Blockchains for Transparent Part Tracking. DOI: https://doi.org/10.1016/j.bcra.2021.100017
58. Bera, B., Saha, S., Das, A., & Kumar, N. (2020). Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment. DOI: https://doi.org/10.1109/TVT.2020.3000576
59. Deebak, B., & Al-Turjman, F. (2023). A Lightweight Blockchain-Based Remote Mutual Authentication for AI-Empowered IoT Sustainable Computing Systems. DOI: https://doi.org/10.1109/JIOT.2022.3152546
60. Dubey, R., Bryde, D., & Kapur, R. (2022). Improving Information Alignment and Coordination in Humanitarian Supply Chain Through Blockchain Technology. DOI: https://doi.org/10.1108/jeim-07-2022-0251
61. Ghimire, N., & Kumar, P. (2021). Sharding-Enabled Blockchain for Software-Defined Internet of Unmanned Vehicles in the Battlefield. DOI: https://doi.org/10.1109/MNET.011.2000214
62. Gumaei, A., & Khalil, I. (2021). Deep Learning and Blockchain with Edge Computing for 5G-Enabled Drone Identification and Flight Mode Detection. DOI: https://doi.org/10.1109/MNET.011.2000204
63. Gupta, S., Jain, V., & Aggarwal, P. (2020). Fusion of Blockchain and Artificial Intelligence for Secure Drone Networking Underlying 5G Communications. DOI: https://doi.org/10.1002/ett.4176
64. Han, D., Kim, S., & Choi, J. (2022). Identity Management and Authentication of a UAV Swarm Based on Blockchain. DOI: https://doi.org/10.3390/app122010524
65. Harbi, S., Alshammari, M., & Ahmed, A. (2022). A Systematic Literature Review of Blockchain Technology for Internet of Drones Security. DOI: https://doi.org/10.1007/s13369-022-07380-6
66. Hassija, V., Gupta, A., & Singh, R. (2020). A Distributed Framework for Energy Trading Between UAVs and Charging Stations for Critical Applications. DOI: https://doi.org/10.1109/TVT.2020.2977036
67. Hu, X., Zhang, J., & Li, Z. (2021). Building Agile and Resilient UAV Networks Based on SDN and Blockchain. DOI: https://doi.org/10.1109/MNET.011.2000176

68. Hughes, J., & Smith, T. (2017). Blockchain, The Greater Good, and Human and Civil Rights. DOI: https://doi.org/10.1111/META.12271
69. Jadav, S., Patel, D., & Sharma, N. (2023). Blockchain-Based Secure and Intelligent Data Dissemination Framework for UAVs in Battlefield Applications. DOI: https://doi.org/10.1109/MCOMSTD.0005.2200052
70. Javed, F., Iqbal, K., & Raza, M. (2022). An Efficient Authentication Scheme Using Blockchain as a Certificate Authority for the Internet of Drones. DOI: https://doi.org/10.3390/drones6100264
71. Koulianos, S., & Papadopoulos, E. (2023). Blockchain Technology for Secure Communication and Formation Control in Smart Drone Swarms. DOI: https://doi.org/10.3390/fi15100344
72. Lis, M., & Balogh, G. (2019). Cyberattacks on Critical Infrastructure: An Economic Perspective. DOI: https://doi.org/10.18559/ebr.2019.2.2
73. Manikandan, M., & Narayanan, S. (2022). Optimized Path Planning Strategy to Enhance Security Under Swarm of Unmanned Aerial Vehicles. DOI: https://doi.org/10.3390/drones6110336
74. Mohril, R. S., Solanki, B. S., & Lad, B. K. (2021). Blockchain Enabled Maintenance Management Framework for Military Equipment. DOI: https://doi.org/10.1109/TEM.2021.3099437
75. Nyangaresi, P., & Mutunga, R. (2024). A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. DOI: https://doi.org/10.1016/j.prime.2024.100471
76. Oláh, J., & Kovács, P. (2023). Secure Registration Protocol for the Internet of Drones Using Blockchain and Physical Unclonable Function Technology. DOI: https://doi.org/10.3390/sym15101886
77. Pandey, R., & Mishra, K. (2022). Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey. DOI: https://doi.org/10.1109/ACCESS.2022.3215975
78. Salor, H., & Wong, L. (2023). Harnessing the Potential of Emerging Technologies to Break down Barriers in Tactical Communications. DOI: https://doi.org/10.3390/telecom4040032
79. Samanth, R., Gupta, N., & Sharma, P. (2022). Security in Internet of Drones: A Comprehensive Review. DOI: https://doi.org/10.1080/23311916.2022.2029080
80. Sarkar, S., & Mukherjee, R. (2023). Blockchain-Based Authenticable (k,n) Multi-Secret Image Sharing Scheme. DOI: https://doi.org/10.1117/1.JEI.32.5.053019
81. Shahidinejad, A., & Davoodi, M. (2024). Anonymous Blockchain-Assisted Authentication Protocols for Secure Cross-Domain IoD Communications. DOI: https://doi.org/10.1109/TNSE.2023.3347594
82. Shahzad, A., & Malik, F. (2022). A Blockchain-Based Authentication Solution for 6G Communication Security in Tactile Networks. DOI: https://doi.org/10.3390/electronics11091374
83. Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. DOI: https://doi.org/10.3390/electronics9111864
84. Stanley-Lockman, Z., & Greenberg, M. (2019). Revisiting the Revolution in Military Logistics: Technological Enablers Twenty Years On. DOI: https://doi.org/10.1007/978-3-030-28342-1_11
85. Torky, M., & Hassanein, A. (2022). Scheduling and Securing Drone Charging System Using Particle Swarm Optimization and Blockchain Technology. DOI: https://doi.org/10.3390/drones6090237
86. Vashistha, M., Raj, P., & Shukla, K. (2022). eChain: A Blockchain-Enabled Ecosystem for Electronic Device Authenticity Verification. DOI: https://doi.org/10.1109/tce.2021.3139090
87. Vestergaard, J., Jensen, T., & Andersen, M. (2021). Blockchain for International Security: An Introduction. DOI: https://doi.org/10.1007/978-3-030-86240-4_1
88. Wang, Z., Liu, Y., & Li, Q. (2022). Using Blockchain to Protect 3D Printing from Unauthorized Model Tampering. DOI: https://doi.org/10.3390/app12157947
89. Wu, Y., Dai, H., Wang, H., & Ruan, K. K. (2020). Blockchain-Based Privacy Preservation for 5G-Enabled Drone Communications. DOI: https://doi.org/10.1109/MNET.011.2000166
90. Yang, C., Zhou, X., & Lin, H. (2022). A Review on Security Issues and Solutions of the Internet of Drones. DOI: https://doi.org/10.1109/OJCS.2022.3183003
91. Yazdinejad, A., & Gandomi, A. (2020). An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security. DOI: https://doi.org/10.1109/tsc.2020.2966970
92. Yazdinejad, A., & Gandomi, A. (2020). Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security. DOI: https://doi.org/10.1109/JIOT.2020.3015382
93. Zhu, Y., Lu, Z., & Li, S. (2020). An invisible warfare with the internet of battlefield things: A literature review. DOI: https://doi.org/10.1002/hbe2.231
94. Al Sadawi, A., Hassan, M. S., & Ndiaye, M. (2021). A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3070555
95. Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. *International Journal of Information Management*. https://doi.org/10.1016/j.ijinfomgt.2020.102120

96. Wang, T., Hua, H., Wei, Z., & Cao, J. (2022). Challenges of blockchain in new generation energy systems and future outlooks. *International Journal of Electrical Power & Energy Systems, 135*, 107499. https://doi.org/10.1016/j.ijepes.2021.107499
97. Akram, S. V., Malik, P. K., Singh, R., Anita, G., & Tanwar, S. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. *Security and Privacy, 3*(5), e109. https://doi.org/10.1002/spy2.109
98. Alam, S., Shuaib, M., Khan, W. Z., Garg, S., Kaddoum, G., Hossain, M. S., & Zikria, Y. B. (2021). Blockchain-based initiatives: current state and challenges. *Computer Networks, 198*, 108395. https://doi.org/10.1016/j.comnet.2021.108395
99. Zou, J., He, D., Zeadally, S., Kumar, N., Wang, H., & Choo, K. R. (2021). Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges. *ACM Computing Surveys (CSUR), 54*(8), 1-36. https://doi.org/10.1145/3456628
100. Durneva, P., Cousins, K., & Chen, M. (2020). The current state of research, challenges, and future research directions of blockchain technology in patient care: Systematic review. *Journal of Medical Internet Research*. https://doi.org/10.2196/18619
101. Rissanen, R., Pulli, P., Sinkkonen, M., & Vaittinen, S. (2023). Lessons learned in cross-border data exchange in health services across Nordic and Baltic countries. *Reference incomplete; data unavailable.*
102. Kifokeris, D., & Koch, C. (2022). The proof-of-concept of a blockchain solution for construction logistics integrating flows: Lessons from Sweden. *Blockchain for Construction*. https://doi.org/10.1007/978-981-19-3759-0_7
103. Proskurovska, A. (2023). Re-inventing housing finance with blockchain: The case of Sweden. *Geoforum*. https://doi.org/10.1016/j.geoforum.2023.103884
104. Karaszewski, R. (2021). The use of blockchain technology in public sector entities management: An example of security and energy efficiency. https://doi.org/10.3390/en14071873
105. Holm, K., & Goduscheit, R. C. (2023). Exploring the opportunities of blockchain-enabled coopetition: Learnings from the wind turbine industry. *International Journal of Technology Management, 93*(3-4), 295-315. https://doi.org/10.1504/IJTM.2023.133927
106. Theodorakopoulos, L., Karras, A., Theodoropoulou, A., & Kampiotis, G. (2024). Benchmarking Big Data Systems: Performance and Decision-Making Implications in Emerging Technologies. Technologies, 12(11), 217. https://doi.org/10.3390/technologies12110217
107. Al-Swidi, A. K., Al-Hakimi, M. A., Al Halbusi, H., Al Harbi, J. A., & Al-Hattami, H. M. (2024). Does blockchain technology matter for supply chain resilience in dynamic environments? The role of supply chain integration. *PLOS ONE, 19*(1), e0295452. https://doi.org/10.1371/journal.pone.0295452
108. Meidute-Kavaliauskiene, I., Yıldız, B., Çiğdem, Ş., & Činčikaitė, R. (2021). An integrated impact of blockchain on supply chain applications. *Logistics, 5*(2), 33. https://doi.org/10.3390/logistics5020033
109. Stamatiou, Y. C., Halkiopoulos, C., Giannoulis, A., & Antonopoulou, H. (2022). Utilizing a Restricted Access e-Learning Platform for Reform, Equity, and Self-development in Correctional Facilities. Emerging Science Journal, 6, 241–252. https://doi.org/10.28991/esj-2022-sied-017
110. Adrian Gheorghe, F. S. A. P., & Unal Tatar, O. F. K. (2021). Blockchain for a resilient, efficient, and effective supply chain: Evidence from cases.
111. GOODS, N. O. N. C. (2023). Mobilizing military supply chains with distributed ledger technologies-Volume 2. *DRDC-RDDC*.
Wenger, A., Cavelty, M. D., & Jasper, U. (2020). The politics and science of the future: Assembling future knowledge and integrating it into public policy and governance. In *The Politics and Science of Prevision* (pp. 229-251). Routledge. https://doi.org/10.4324/9781003022428
112. Kimbell, L., & Vesnić-Alujević, L. (2020). After the toolkit: Anticipatory logics and the future of government. *Policy Design and Practice*. https://doi.org/10.1080/25741292.2020.1763545
113. King, J., Holmes, R., Burkholder, S., Holzman, J., & Suedel, B. (2022). Advancing nature-based solutions by leveraging Engineering With Nature® strategies and landscape architectural practices in highly collaborative settings. *Integrated Environmental Assessment and Management, 18*(1), 108-114. https://doi.org/10.1002/ieam.4473
114. Sánchez, M. L., Cabrera, A. T., & Del Pulgar, M. L. G. (2020). Guidelines from the heritage field for the integration of landscape and heritage planning: A systematic literature review. *Landscape and Urban*

Planning, 204, 103931.
https://doi.org/10.1016/j.landurbplan.2020.103931