Computer Fraud & Security
ISSN (online): 1873-7056

Securing military computing with the blockchain

DR RAJEEV KUMAR

PROF RAEES AHMAD KHAN

Abstract: In an era defined by technological advancements and digital interconnectivity, securing military computing infrastructure is of paramount importance. The integration of blockchain technology has emerged as a potential solution to mitigate evolving cyberthreats, offering a decentralised and tamper-resistant framework. This article provides a comprehensive examination of blockchain's capabilities, challenges and implications for defence strategies. Through a synthesis of relevant literature and case studies, it elucidates blockchain's key principles, potential advantages in military settings, and its impact on data security and accountability. As militaries worldwide seek to protect sensitive information and critical systems, the integration of blockchain offers a promising avenue for bolstering security, contributing to the development of more robust defence systems in the digital age.

In the rapidly evolving landscape of modern warfare and defence, the secure and efficient management of sensitive military data and computing resources is paramount. As military operations increasingly rely on advanced technologies such as cloud computing, Internet of Things (IoT) devices and artificial intelligence, the vulnerabilities within the digital infrastructure become more pronounced.[1] Cyberthreats, espionage and unauthorised access pose significant risks to national security and military operations. To address these challenges, and ensure the utmost protection of sensitive information and critical systems, the integration of cutting-edge technologies is imperative.

Blockchain technology, initially designed as the underpinning technology for crypto-currencies such as Bitcoin, has garnered attention for its potential to enhance security and integrity in various sectors.[2] Its decentralised and tamper-resistant nature offers a unique solution to the vulnerabilities inherent in centralised military computing systems. This research article delves into the application of blockchain technology as a robust framework for securing military computing, aiming to provide a comprehensive understanding of its capabilities, challenges and potential impact on defence strategies.

In this era of digital warfare, military institutions worldwide must adapt and adopt innovative approaches to safeguard their assets and information. The integration of blockchain technology into military computing systems holds the promise of enhancing data security, integrity and transparency while also addressing issues of trust and accountability. By exploring the synergies between blockchain technology and military operations, this research article seeks to contribute to the ongoing discourse surrounding the modernisation and fortification of military computing infrastructure in the face of evolving threats in cyberspace.

Key blockchain concepts

Blockchain is a decentralised and tamper-resistant ledger that records transactions across a network of nodes.[3] Here we will outline some key concepts.

Decentralisation: The core concept of decentralisation in the context of blockchain technology in the military is to distribute and secure sensitive military data, communications and operations across a network of decentralised nodes rather than relying on a centralised authority or server. This approach enhances security by reducing single points of failure and vulnerability to cyber attacks, ensures data integrity through cryptographic verification, and allows for trustless interactions among military entities. Decentralisation also fosters transparency and auditability, as all transactions and activities are recorded on an immutable blockchain, ultimately enabling more-resilient and efficient military operations while minimising the risk of unauthorised access or data manipulation.

Immutability: This is a core concept in blockchain technology when applied to military systems. It refers to the inherent property of a blockchain ledger, where once data is recorded in a block and added to the chain, it becomes tamper-proof and unalterable. This feature ensures that critical military information, such as mission plans, logistics data and personnel records, remains secure and unmodifiable, reducing the risk of unauthorised access, data manipulation or cyber attacks. Immutability enhances trust, transparency and the integrity of military operations, making blockchain an attractive technology for safeguarding sensitive military data and enhancing overall security.

Vol: 2024 | Iss: 2 | 2024 | 10.12968/S1361-3723(24)70007-4 | © 2024 MA Business Ltd

Downloaded from magonlinelibrary.com by 043.248.074.032 on September 15, 2024.

Consensus mechanisms: In military blockchain technology, consensus mechanisms are fundamental protocols that enable distributed and decentralised networks to achieve agreement on the state of the blockchain ledger without relying on a central authority. In military applications, where security, trust and resilience are paramount, consensus mechanisms ensure that all participants in the network, which could include various military units or agencies, validate and confirm the validity of transactions and data. The core concept is to establish a robust and tamper-resistant method for achieving agreement within the military blockchain, thereby enhancing data integrity, security and the overall reliability of critical military operations and communications. Popular consensus mechanisms in this context may include Proof of Work (PoW) or more energy-efficient alternatives like Proof of Stake (PoS) or Delegated Proof of Stake (DPoS), all adapted to meet the stringent security and performance demands of military applications.

Smart contracts: In the context of military blockchain technology, smart contracts represent self-executing, tamper-resistant digital agreements that automate and enforce predefined rules and conditions within a secure and decentralised network. These contracts enable military organisations to streamline and enhance various operational processes, such as procurement, supply chain management and logistics, by eliminating intermediaries, reducing administrative overhead, ensuring transparency and enhancing data integrity. Smart contracts in the military can play a pivotal role in improving accountability, trust and efficiency while safeguarding sensitive data and mission-critical operations within the blockchain ecosystem.

Security features

Blockchain technology offers several security features that make it suitable for military computing.[4]

Data integrity: In blockchain security features for military applications, data integrity is a fundamental concept that ensures the accuracy and immutability of sensitive information within a decentralised ledger. By utilising cryptographic hashing and consensus algorithms, blockchain technology guarantees that once data is recorded, it cannot be altered or deleted without consensus from the network participants, providing an immutable audit trail for military operations. This robust data integrity helps safeguard critical military information, enhancing transparency, trust and security in mission-critical scenarios while reducing the risk of unauthorised tampering or data manipulation.

Authentication: Authentication in blockchain security involves the verification of the identity of users or entities participating in the blockchain network through cryptographic mechanisms. It ensures that only authorised participants can access and interact with the blockchain, thereby enhancing the integrity and confidentiality of military operations and sensitive data. This core concept in military security features employs cryptographic keys and digital signatures to validate the authenticity of transactions and smart contracts, preventing unauthorised access and malicious activities within the blockchain network, and enabling secure and tamper-resistant record-keeping for mission-critical information and communication.

Confidentiality: In blockchain security features within military applications, confidentiality revolves around ensuring that sensitive information, such as troop movements, classified intelligence and operational strategies, remains private and accessible only to authorised personnel. This is achieved through the use of cryptographic techniques, including private and public key encryption, to restrict access to data on the blockchain ledger. Additionally, smart contracts and access control mechanisms can be implemented to enforce strict permission levels, ensuring that only individuals with the appropriate clearance can view or modify specific data, thereby safeguarding military operations and national security interests from unauthorised disclosure or tampering.

Transparency: For military implementations of blockchain security features, transparency revolves around the core concept of utilising distributed ledger technology to enhance the integrity, traceability and auditability of sensitive data, communications and logistics within military operations. By recording transactions and activities on an immutable and decentralised ledger, blockchain ensures that all relevant stakeholders have real-time access to accurate and tamper-proof information, thereby reducing the risk of unauthorised access, data manipulation and cyber attacks. This transparency fosters trust among military entities, enhances situational awareness, and supports secure and efficient decision-making processes critical to national defence and security.

Military applications of blockchain

Secure communications: The core concept of secure communications in applications of blockchain in military computing revolves around leveraging blockchain technology to ensure the confidentiality, integrity and authenticity of sensitive military data and communications. By employing decentralised and immutable ledger systems, blockchain can create a tamper-resistant environment where military operations, logistics and intelligence data can be securely transmitted and stored. Smart contracts can automate and enforce access controls, ensuring that only authorised personnel have access to classified information.

Additionally, cryptographic techniques, such as public-private key pairs, can be integrated into blockchain networks to encrypt

Downloaded from magonlinelibrary.com by 043.248.074.032 on September 15, 2024.

and secure communications, safeguarding military operations from cyberthreats and unauthorised access, thereby enhancing the overall security and trustworthiness of military computing systems.

Supply chain management: In the context of applications of blockchain in military computing, supply chain management refers to the utilisation of blockchain technology to enhance the transparency, security and efficiency of military supply chain operations. The core concept involves creating a decentralised and immutable ledger that records every step in the procurement, production, distribution and maintenance of military assets, including weaponry, equipment and spare parts. This blockchain-based system ensures that all stakeholders, from defence contractors to military personnel, have real-time access to accurate and tamper-proof data, reducing the risk of fraud, counterfeiting and supply chain disruptions, ultimately bolstering the resilience and effectiveness of military logistics and operations.

Identity and access management (IAM): This plays a crucial role in the application of blockchain technology in military computing by ensuring secure and controlled access to sensitive military data and resources. In this context, IAM encompasses the core concept of establishing and managing digital identities for military personnel and authorised entities within the blockchain network. Through cryptographic techniques and smart contracts, IAM systems enable precise control over who can access and interact with military blockchain applications, enforcing strict access permissions and authentication protocols to safeguard critical information and maintain operational integrity. By integrating IAM into blockchain-based military computing, the armed forces can enhance security, streamline authorisation processes, and ensure that only authorised personnel have access to critical military systems and data.

Data sharing and interoperability: The core concept of data sharing and interoperability in blockchain applications in military computing revolves around leveraging blockchain technology to establish a secure, transparent, and tamper-resistant data ecosystem for military operations.[5] By utilising distributed ledger technology, military organisations can facilitate seamless and trustworthy data sharing among various entities, such as different branches of the armed forces, allied nations and defence contractors, all while ensuring data integrity and confidentiality. This interoperable blockchain framework enhances collaboration, streamlines decision-making processes and improves the overall efficiency and security of military computing systems, ultimately strengthening the military's ability to respond effectively to evolving threats and challenges in the modern era. Furthermore, Table 1 presents a summary of the core concepts in the various applications of blockchain in military computing.

Table 1: Application core concepts of blockchain technology in military computing.

Application	Core concept
Secure communications	Leveraging blockchain for secure, confidential and tamper-resistant military data and communication management.
Supply chain management	Enhancing transparency, security and efficiency in military supply chain operations through blockchain technology.
Identity and access management	Ensuring secure and controlled access to sensitive military data and resources through digital identity management.
Data sharing and interoperability	Establishing a secure and interoperable data ecosystem for seamless collaboration and enhanced military efficiency.

The benefits of blockchain

Enhanced security: The core motivation for employing blockchain technology in military computing lies in its ability to enhance security and trust within military operations and communication networks.[6] By utilising a decentralised and immutable ledger, blockchain ensures the integrity and authenticity of sensitive data, such as communications, logistics and supply chain information. This tamper-resistant infrastructure reduces the risk of cyber attacks, espionage and data breaches, and bolstering national security. Additionally, smart contracts and permissioned blockchain networks enable streamlined and automated processes, improving operational efficiency and reducing the potential for human error, ultimately contributing to a more resilient and secure military computing ecosystem.

Downloaded from magonlinelibrary.com by 043.248.074.032 on September 15, 2024.

Resilience: Blockchain technology offers several key benefits in military computing, primarily by enhancing resilience. Its decentralised and immutable ledger ensures data integrity and security, making it highly resistant to cyber attacks and unauthorised access. In a military context, this means that critical information, such as troop movements, logistics and intelligence, can be securely stored and transmitted. Additionally, blockchain enables efficient and transparent supply chain management, reducing vulnerabilities to fraud and ensuring the availability of essential resources during operations. Furthermore, the redundancy of data across the network enhances fault tolerance, guaranteeing that critical systems continue to function even in the face of disruptions or attacks, ultimately bolstering the resilience of military computing infrastructure.

Transparency and accountability: Another key application of blockchain technology in military computing lies in its capacity to enhance transparency and accountability across various aspects of defence operations.[7] By employing decentralised, immutable ledgers, blockchain ensures that sensitive data – such as supply chain information, equipment maintenance records and personnel credentials – can be securely and transparently tracked in real-time. This not only reduces the risk of fraud, unauthorised access and data tampering but also fosters a heightened level of trust among stakeholders, both internal and external.

Furthermore, blockchain's smart contract capabilities can automate and enforce predefined rules and agreements, streamlining procurement processes, and facilitating swift, auditable transactions. Overall, blockchain serves as a powerful tool in modernising and fortifying military infrastructure, promoting efficiency, security and accountability in defence operations.

Reduced administrative overhead: The ability to reduce administrative overhead through decentralised and secure data management is a significant factor in the adoption of blockchain technology in military applications. By implementing blockchain, military organisations can streamline and automate various administrative processes, such as logistics, supply chain management and personnel records, all while ensuring data integrity and security. The distributed ledger nature of blockchain eliminates the need for centralised intermediaries, reducing the risk of data manipulation or unauthorised access. This not only enhances operational efficiency but also bolsters trust and transparency within military operations, making it a compelling solution for improving overall effectiveness and security in military computing environments. Table 2 provides a comprehensive summary of the benefits of blockchain technology in military computing.

Table 2: Summary of the benefits.

Aspect	Benefit
Enhanced security	Using blockchain to enhance security, integrity and authenticity of military data, reducing cyberthreats and breaches.
Resilience	Leveraging blockchain's decentralised and immutable nature to ensure data availability and system resilience in military operations.
Transparency and accountability	Enhancing transparency, trust and accountability in defence operations through secure and auditable blockchain records.
Reduced administrative overhead	Streamlining administrative processes and reducing overhead by automating tasks and ensuring secure data management with blockchain technology.

Challenges and Considerations

Blockchain technology has garnered significant attention in recent years for its potential to enhance security, transparency and efficiency in various sectors. However, in military computing, the adoption of blockchain technology presents unique challenges and considerations. This section explores the key challenges and considerations associated with integrating blockchain into military computing, highlighting the potential benefits and risks.

Security concerns: Blockchain technology, touted for its security features, is not immune to attacks. Military computing must consider the possibility of 51% attacks or other novel threats that could compromise the integrity of the blockchain. Additionally, the emergence of quantum computing poses a significant threat, necessitating a plan for post-quantum cryptography to protect

Downloaded from magonlinelibrary.com by 043.248.074.032 on September 15, 2024.

sensitive data.

Privacy and confidentiality: In the military, dealing with highly classified information is routine. Thus, integrating blockchain technology must ensure that data remains confidential and only accessible to authorised personnel. Balancing transparency with data privacy presents a challenge, as the inherent transparency of blockchain can conflict with the need to keep certain military operations and data hidden.

Scalability: Military operations generate massive volumes of data and transactions. Ensuring that the blockchain can handle this volume without compromising performance is crucial. Moreover, in diverse military environments, where connectivity is limited, addressing blockchain's latency issues is essential for effective operations.

Interoperability: Military computing relies on a vast network of legacy systems. Integrating blockchain with these systems can be complex and costly. Additionally, in multinational military operations, ensuring interoperability with blockchain systems from different countries becomes paramount.

Regulatory compliance: Military operations often transcend international borders. Adhering to various international laws and regulations while using blockchain can be an intricate issue. Furthermore, data stored on a blockchain may be subject to data sovereignty laws, which can vary significantly between countries.

Resource constraints: Blockchain networks can be energy-intensive, posing challenges in the resource-constrained environments typical of military field operations. Deploying and maintaining blockchain infrastructure in remote or hostile environments may be logistically challenging.

Smart contract risks: Smart contracts on blockchains can have vulnerabilities that, if exploited, can lead to significant security breaches. Enforcing smart contracts in military operations may also have legal implications that need careful consideration.

Training and education: To use blockchain technology effectively and securely, military personnel need adequate training. Moreover, adopting blockchain technology may require a cultural shift in the military's approach to data management and security.

Supply chain management: Enhancing supply chain security is crucial for military operations. Blockchain can help prevent counterfeits, but implementing it effectively requires overcoming challenges related to verifying the authenticity of supplies and equipment.

Long-term viability: Given the rapidly evolving nature of technology, the military must consider the long-term viability of blockchain solutions. Planning for potential transitions to new technologies is essential to ensure continued effectiveness in military computing.

Table 3: Comparative analysis of the challenges and considerations.

Challenge/ consideration	Description	Implications and mitigations
Security concerns	Resilience to attacks: Potential vulnerabilities.	Employ robust cyber security measures.
	Quantum computing: Threats to encryption.	Research and implement post-quantum cryptography.
Privacy and confidentiality	Sensitive data: Protecting classified information.	Implement strict access controls and encryption.
	Privacy concerns: Balancing transparency and privacy.	Develop permissioned blockchains for restricted access.
Scalability	Transaction volume: Handling high data volumes.	Explore scalable consensus mechanisms.
	Network latency: Performance in remote locations.	Optimise network architecture for low latency.
Interoperability	Integration with legacy systems: Compatibility.	Develop adapters/interfaces for legacy system integration.
	Multinational collaboration: Cross-border	Establish international standards for

Downloaded from magonlinelibrary.com by 043.248.074.032 on September 15, 2024.

Challenge/ consideration	Description	Implications and mitigations
	operations.	blockchain interoperability.
Regulatory compliance	International laws: Compliance with laws.	Legal counsel and international collaboration for compliance.
	Data sovereignty: Data stored in different countries.	Choose blockchain solutions that align with local data sovereignty.
Resource constraints	Energy consumption: High energy usage.	Opt for energy-efficient consensus mechanisms.
	Infrastructure: Deploying in remote locations.	Plan logistics for infrastructure maintenance in remote areas.
Smart contract risks	Vulnerabilities: Smart contract security.	Conduct thorough code audits and testing.
	Legal implications: Legal enforcement of smart contracts.	Consult legal experts to navigate legal complexities.
Training and Education	Personnel training: Adequate blockchain knowledge.	Develop training programmes for military personnel.
	Cultural shift: Adapting to new data management.	Promote a culture of data security and blockchain adoption.
Supply chain management	Counterfeit prevention: Ensuring authenticity.	Implement blockchain-based tracking for supply chain security.
Long-term viability	Future-proofing: Ensuring relevance over time.	Continuously assess and adapt blockchain solutions to evolving needs.

Table 3 provides a snapshot of the challenges and considerations associated with integrating blockchain into military computing, along with potential mitigations and solutions. Military decision-makers must carefully evaluate each factor to make informed choices regarding the adoption and implementation of blockchain technology in their operations.

Real-world use cases

Leveraging blockchain technology in military computing can enhance security, streamline operations and improve overall efficiency. Here are some pertinent real-world use cases of blockchain in military computing, inspired by the initiatives of various countries and organisations.

Secure communications

Enhanced encryption: Blockchain can be used to enhance secure communication channels. Messages can be encrypted and stored on the blockchain, ensuring that only authorised personnel have access to sensitive information.

Decentralised communication networks: In the event of a cyber attack or network disruption, blockchain-based decentralised communication networks can enable military units to maintain communication, ensuring mission-critical information flow.

Supply chain management

Inventory tracking: The US Department of Defense's initiative can be extended to create an immutable ledger for tracking military equipment, spare parts and ammunition. This ensures transparency and minimises the risk of counterfeits.

Logistics optimisation: Smart contracts on a blockchain can automate and optimise logistics operations, including procurement, transportation and distribution, reducing costs and ensuring timely delivery of essential supplies.

Personnel records and identity management

Immutable service records: As demonstrated by the Estonian Defence Forces, blockchain can secure military personnel records, ensuring the integrity and authenticity of service history, qualifications and training certifications.

Biometric identity verification: Utilising blockchain for identity management can enhance security by storing and verifying biometric data, ensuring that only authorised personnel gain access to classified areas or systems.

Downloaded from magonlinelibrary.com by 043.248.074.032 on September 15, 2024.

Secure information sharing

Interoperable data sharing: NATO's experiments with blockchain can lead to the development of a secure and interoperable system for sharing sensitive intelligence and information among member nations, reducing the risk of data breaches or leaks.

Cross-national collaboration: Blockchain can facilitate collaborative efforts among multiple nations while maintaining data sovereignty, allowing for joint military exercises and operations with secure information sharing.

Cyber security

Threat intelligence sharing: Blockchain can be used to create a global threat intelligence network, enabling the rapid sharing of cyberthreat data among military agencies and governments, enhancing overall cyber security posture.

Immutable logs: Blockchain can record network activity and system events, providing a tamper-proof audit trail for forensic analysis in the event of cyber attacks or data breaches.

Veterans' benefits and healthcare

Transparent benefits management: Blockchain can ensure transparency in managing veterans' benefits, making it easier to track and distribute pensions, healthcare benefits and other entitlements securely.

Medical records management: Securely storing veterans' medical records on a blockchain can facilitate access to healthcare information for medical professionals while maintaining privacy and security.

By implementing blockchain technology in these real-world use cases, the military can enhance its capabilities, protect sensitive information, and improve operational efficiency while maintaining the highest standards of security.

Suggestions for successful adoption

What follows are our key recommendations for the successful adoption of blockchain technology for securing military computing.

Conduct comprehensive risk assessments and feasibility studies.

> Prioritise a thorough risk assessment before implementing any blockchain solution for military applications.
>
> Evaluate the specific security needs and potential vulnerabilities that blockchain can address.
>
> Conduct feasibility studies to determine whether blockchain is the most suitable technology for the identified security challenges.

Collaborate with industry experts and blockchain developers.

> Seek partnerships with experienced blockchain developers and cyber security experts.
>
> Collaborate with industry leaders to design and implement secure blockchain systems.
>
> Engage in information-sharing and knowledge transfer with blockchain professionals to stay updated on the latest security measures.

Develop clear policies and procedures.

> Create well-defined policies and procedures for the implementation and operation of blockchain solutions.
>
> Ensure that these policies address compliance with relevant military regulations and standards.
>
> Regularly review and update policies to adapt to evolving security threats and technology advancements.

Invest in ongoing research and development.

Downloaded from magonlinelibrary.com by 043.248.074.032 on September 15, 2024.

Allocate resources for ongoing research and development to address scalability issues and cryptographic vulnerabilities.

Stay updated on emerging blockchain technologies and security best practices.

Engage in continuous improvement to enhance the effectiveness of blockchain solutions over time.

Train military personnel.

Provide comprehensive training programmes for military personnel in blockchain technology and security best practices.

Ensure that all relevant personnel, from IT specialists to decision-makers, understand the principles and risks associated with blockchain.

Foster a culture of cyber security awareness and vigilance within the military organisation.

Implement a pilot programme.

Begin with a smaller-scale pilot programme to test the effectiveness and security of blockchain solutions in a controlled environment.

Use the pilot programme to gather feedback and make necessary adjustments before scaling up to full implementation.

This approach can help identify and mitigate potential issues early on.

Perform regular security audits and testing.

Conduct regular security audits and penetration testing of the blockchain systems to identify vulnerabilities.

Use the findings from audits to improve the security posture of the blockchain implementation.

Stay vigilant against emerging threats and adapt security measures accordingly.

Establish clear accountability.

Define roles and responsibilities within the military organisation for overseeing and maintaining the blockchain infrastructure.

Ensure that there is clear accountability for security measures, compliance and incident response.

Maintain a contingency plan.

Develop a comprehensive contingency plan for blockchain security breaches or failures.

Have back-up systems and recovery procedures in place to minimise downtime and data loss in case of a security incident.

By following these recommendations, military organisations can increase the likelihood of successfully adopting blockchain technology to enhance the security of their computing systems.

Conclusion

This article has explored the promising application of blockchain technology in enhancing the security of military computing systems. Through an extensive review of existing literature and practical use cases, several key findings have emerged. These findings underscore the potential advantages of blockchain, including heightened security, transparency, resilience and data

Downloaded from magonlinelibrary.com by 043.248.074.032 on September 15, 2024.

integrity. By shedding light on these benefits, the article aims to contribute to informed decision-making within the military sector, fostering awareness of the transformative potential of blockchain.

It is important to raise awareness and provide practical insights into the integration of blockchain technology into military operations. This research highlights the significance of blockchain's transparent and accountable nature, which can fortify security in military computing environments. Additionally, we can clearly see the potential efficiency gains through smart contract automation, further illustrating the advantages of blockchain adoption in the military context.

Nevertheless, in this article we have primarily focused on the conceptual advantages of blockchain in military computing, without delving deeply into the technical challenges or regulatory complexities that may hinder its widespread adoption. Future research should address these concerns, focusing on technical solutions, robust security testing, regulatory frameworks, cost-benefit analysis and education and training programmes to fully unlock the potential of blockchain technology in securing military computing systems. In doing so, the military can remain at the forefront of technological innovation while safeguarding critical data and operations.

About the authors

Dr Rajeev Kumar is currently working as an assistant professor at the Centre for Innovation and Technology at the Administrative Staff College of India, Hyderabad, Telangana, India. He has authored over 80 papers published in SCI/Scopus indexed journals. At present, his total Google Scholar citations exceed 2,200, accompanied by an h-index of 28.

Prof Raees Ahmad Khan is currently working as a professor in the Department of Information Technology at the Babasaheb Bhimrao Ambedkar University (a Central University), Lucknow, Uttar Pradesh, India. He has authored over 350 papers published in SCI/Scopus indexed journals. Presently, his total Google Scholar citations exceed 4,000, accompanied by an h-index of 32.

References:

1.Zhu, Y; Zhang, X; Zh, Y Ju; Wang, Ch Ch. 'A study of blockchain technology development and military application prospects'. The 2020 Spring International Conference on Defence Technology, 2020. Accessed Feb 2024. https://iopscience.iop.org/article/10.1088/1742-6596/1507/5/052018/pdf.

2.Sanchez, Salvador. 'Blockchain technology in defence'. European Defence Matters. Accessed Feb 2024. https://eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence.

3.Cornella, A; Zamengo, L; Delepierre, A; Clementz, G. 'Blockchain in defence: a breakthrough?'. Finabel, Sep 2020. Accessed Feb 2024. https://finabel.org/wp-content/uploads/2020/09/FFT-Blockchain.pdf.

4.'How blockchain is being used by global militaries'. Analytics Insight, 27 Oct 2022. Accessed Feb 2024. www.analyticsinsight.net/how-blockchain-is-being-used-by-global-militaries/.

5.Woodfield, Daryl. 'The emerging impacts of blockchain technology on DoD asset cyber security'. Air Command and Staff College, Air University. Accessed Feb 2024. https://apps.dtic.mil/sti/pdfs/AD1107534.pdf.

6.James, Kelroy. 'Blockchain: Disruptive innovation for defence transformation'. Data Driven Investor, 26 Sep 2022. Accessed Feb 2024. www.datadriveninvestor.com/2022/09/26/blockchain-disruptive-innovation-for-defence-transformation/.

7.'Enabling NATO's Collective Defense: Critical infrastructure security and resiliency (NATO COE-DAT Handbook 1)'. US Army War College, 15 Nov 2022. Accessed Feb 2024. www.coedat.nato.int/publication/researches/12-Enabling%20NATO_s%20Collective%20Defense_%20Critical%20Infrastructure%20Secur

Downloaded from magonlinelibrary.com by 043.248.074.032 on September 15, 2024.