Analysis of the Issues Related to the Problem of Enhanced Data Security in Space

Dina Aldanazarova[1] and S. Ospanov[2]
[1]Kazakh-British Technical University, Almaty, Kazakhstan
[2]National Center for Space Research and Technology, Integration of Kaz Kosmos with universities (Corporate Academy), Almaty, Kazakhstan

d_aldanazarova@kbtu.kz
ospanoff1956@gmail.com

Abstract: As space exploration and use expands, the need for strong data security measures becomes increasingly important. This article explores the unique challenges of protecting data in space-based systems and proposes solutions to address these challenges. The vulnerability of space-based communications networks, satellite systems, and terrestrial infrastructure to cyber threats and potential attacks is studied. An overview of the literature on space data security reveals a variety of existing vulnerabilities and challenges in protecting sensitive information transmitted to and from space. Issues such as data interception, unauthorized access, and the impact of space weather events are prominent concerns that have been documented. Overview of a comprehensive framework for improving data security in space environments based on encryption, authentication, security protocols, intrusion detection, and physical security principles. By implementing these solutions, space agencies and organizations can ensure confidentiality, integrity, and availability of data and ensure safe operations in the space sector.

Key words: Satellites, Network, Data security, Space, Space sector

1. Introduction

With the development of space technology and aerospace, the issue of data security in space is becoming increasingly important.(Kang,et al 2013) The aim of this review is to analyze the research conducted on the issue of data protection and security in space technology and engineering, identify the main challenges, and explore solutions in the space sector.

According to Mayence (2010), there are three main aspects of space security:

1. security in space (i.e., protecting space systems);
2. space for security (i.e., military space operations); and
3. security from space (i.e., protecting Earth from space-based threats).

Due to advances in navigation systems, satellite communications, research missions, and commercial space projects, the amount of data transmitted and processed in the space industry is increasing significantly. This emphasizes the importance of securing data from cybersecurity threats and physical damage.(Plotnek,et al 2022)

The space industry represents a multifaceted ecosystem characterized by dynamic shifts, evolving technologies, and innovative concepts. Originating during the Cold War period, it was controlled by a select few nations and operated at the state level, focusing on the creation of sizable and costly satellites designed for extended operational durations. Information sharing was restricted to essential needs, primarily to impede adversaries' military prowess, establishing a framework of secrecy in developmental approaches. These methodologies, prevalent during this era, epitomize what is commonly referred to as "Old Space." (Manulis, et al., 2021)

Before we discuss data security, let's define it as the protection of data against unauthorized disclosure, modification, restriction, or destruction. (Winkler, et al 1974)

The increasing frequency of security attacks on assets in space is causing the lines between space security and cyber security to become less distinct. As the space sector becomes more commercialized and militarized, the appeal of targeting space assets grows, necessitating a broader and more diverse approach to cyber security for space infrastructure. (Varadharajan,2023)

The objective of our research is to investigate these unique data security challenges in space and propose corresponding solutions to address them. We aim to develop a comprehensive framework for enhancing data security in space conditions, encompassing the application of encryption methods, authentication protocols, security frameworks, intrusion detection systems, and principles of physical security. (Kreilina,2023) (Salykov, et.al 2023)

By implementing the proposed solutions, space agencies and organizations can ensure the confidentiality, integrity, and availability of data, thereby facilitating safe operations in the space sector and bolstering trust in space technologies.

2. Related Work

2.1 Challenges and Innovations in Data Security in Space

2.1.1 Securing space information networks

Earth observations rely mainly on single satellites or satellite constellations, making continuous information capture and transmission difficult. Satellite ground stations cannot be deployed globally, and the lack of collaborative management reduces information acquisition and transmission efficiency. Rapid development in space technologies has led to the emergence of space information networks, composed of geosynchronous Earth orbit (GEO) satellites, medium Earth orbit (MEO) satellites, low Earth orbit (LEO) satellites, and high-altitude platform stations (HAPSs). These networks can improve the coverage area and effectiveness of emergency monitoring, making them crucial for disaster prevention, rescue, global location and navigation, and space tracking. However, security requirements in space information networks are increasing, and key secure technologies such as secure handoff, secure transmission control, key management, and secure routing should be integrated into the network architecture. Despite extensive research on space network structure, convergence, network management, routing, mobility management, and transmission control, security-related issues have not been thoroughly investigated. (Salykov, et.al 2023)

The space information network, heavily reliant on information networks, is vulnerable to cyberspace attacks based on offensive information access(Jiang,et al 2015). Falco (2019) analyzes the characteristics and security requirements of space information networks, proposing a new situation awareness and information defense strategy combining multi-domain approaches. The research results can serve as a reference for space information network security research and cyberspace defense technology research.

2.2 New Space

The space industry is undergoing significant transformation due to advancements in technologies, attitudes, and investment. New and proposed constellations are increasing the in-orbit satellite population, expanding the threat landscape. Manulis (2021) analyzes past satellite security threats and incidents to assess the motivations and characteristics of adversarial threats to satellites. Ground and radio frequency communications were the most favored targets, but the boom of satellite constellations in the upcoming years may shift this focus towards the space segment. Key technology advancements and open issues in the satellite industry related to security and operational requirements are also discussed. The term "New Space" is characterized by incorporating standard modules and components while making space travel cheaper and more widespread across industries. Companies are taking more risks with their satellites, leading to more innovative applications and technologies. Major applications of New Space include the academic sector pushing the innovative boundaries of New Space by exhibiting new technologies in space, such as smart phone electronics in satellites, investment in the Earth observation market, and global broadband services. (Manulis, et al., 2021)

Varadharajan, et.al 2023 discusses the security challenges faced by space-borne systems, such as communication satellites, sensory, surveillance, and GPS, as they merge with cyberspace. The increasing commercialization and militarization of the space sector have blurred the boundaries between space security and cyber security. As terrestrial critical infrastructures, such as communications, financial services, transport, logistics, and weather monitoring, are intrinsically dependent on space-based assets, preventing their compromise is a critical and urgent need. The space sector is expected to grow even faster in the future, driven by falling launch costs and rapid technological developments. Despite the complexity of the space industry and increasing dependency on space infrastructure, cyber security issues are somewhat under-recognized by infrastructure providers and policymakers. Varadharajan, et.al 2023 examines the current threat landscape of space infrastructure and security challenges, outlining the issues that need to be tackled in the formulation of cyber security solutions for space and providing recommendations for developing a policy framework for space security. Space organizations are organizations that build, operate, maintain, or own space systems, which are somewhat more complex than terrestrial digital infrastructures from a technology perspective. (Varadharajan, et.al 2023)

3. Case Study

Space systems, including satellites and mission control centers, are frequently targeted by cyberattacks. Despite their technical sophistication, the space industry's cybersecurity efforts have lagged those of other high-technology sectors. Space systems face unique cybersecurity risks that complicate their remediation capabilities. (Falco, et.al 2019) explores factors leading to the space sector's poor cybersecurity posture, various cyberattacks against space systems, and existing mitigation techniques employed by the sector. Several security principles for satellites and space assets are proposed to help reorient the sector toward designing, developing, building, and managing cyber secure systems. These principles address both technical and policy issues to address all space system stakeholders. Despite efforts to improve cybersecurity in the United States, there has been little focus on cybersecurity for space systems. (Falco, et.al 2019)

Cyberspace countermeasures aim to contest and maintain control of information by adopting electromagnetic and network attack methods. The space information network is mainly composed of satellite TELEMETRY, TRACK CONTROL networks (TT&C) and space communication networks. These networks are scattered across land, sea, air, and space, connected by wireless or wired data links. Standardized network operation mechanisms and unified information transmission formats are widely adopted, and numerous control and communication tasks require collaboration among network nodes. Distributed dynamic self-organizing networks, such as Ad-Hoc, are increasingly used in space communication networks. System specification and compatibility are focused, with standard technical specifications like the IP protocol gradually being promoted and used.

Space information networks are more vulnerable to cyberspace attacks due to their unique characteristics. The cyberspace threat includes detection and attack, including electromagnetic spectrum and network property information. Attack methods include sensor access, performance-oriented MAC protocol attacks, performance-oriented LLC protocol attacks, service-oriented routing protocol attacks, false information deception, and decision jams based on false cyberspace situations.

Network security situation awareness is crucial for preventing or reducing cyberspace threats to space information networks. Key technologies include a space information network security model, security situation element extraction, multi-hierarchy information fusion, network security situation evaluation, and network security situation prediction. Current models struggle to build a unified model that integrates electromagnetic spectrum and network properties, and most models are designed for specific prediction methods.

Multi-hierarchy information fusion technology can fuse electromagnetic spectrum and network property information synchronously, generating accurate and reliable cyberspace network security elements. Network security situation evaluation and prediction are based on extracted situation elements and can assist in decision-making and performance evaluation. (Falco, et.al 2019)

4. Protocols

CCSDS has created a set of protocols for telemetry, telecommand, and OSI model layers (application, transport, etc.). Adapted to support protocols from the IP suite, CCSDS is making data communications more accessible and familiar for new enterprises in the space industry. The implementation and demonstration of these protocols have been noted in over a thousand missions listed on the CCSDS website, with several commercial telecommunication satellites using CCSDS command and control capabilities.(Manulis, et.al 2021)

The CCSDS Space Data Link Security (SDLS) protocol extends its data link protocols to include confidentiality services by encrypting the frame data, authentication, and integrity through authenticated and non-authenticated message authentication codes (MACs), respectively, and anti-replay protection using sequence numbers. The design and analysis of the scheme follow the security concerns outlined in ISO 7498-2. The protocol aims to ensure the confidentiality, integrity, and/or authenticity of the transmitted data. However, it does not offer protection against DDoS attacks such as jamming, traffic flow analysis, and data substitution if the encryption lacks authentication . (Manulis, et.al 2021)

The Space Domain Cybersecurity (SPADOCS) framework was introduced to bridge the space and cyber domains with the goal of improving collaboration and information sharing across mission, enterprise, international, and government boundaries. The Space Domain Cyber Security (SpaDoCs) framework provides a comprehensive and systematic model for understanding and solving space domain cyber security. The SpaDoCs framework is a process framework for organizing, understanding, and learning. The SpaDoCs framework describes the main challenges of cybersecurity in the space domain.

The framework describes the space domain layer by layer, starting with the enterprise layer and then drilling down to the mission, system, and DevSecOps layers. Threats and vulnerabilities at each level are highlighted, recognizing that confidentiality, integrity, and availability (also known as the CIA triad) are foundational and critical goals of cybersecurity.(Quiquet,2023)

4.1 SPADoc Framework

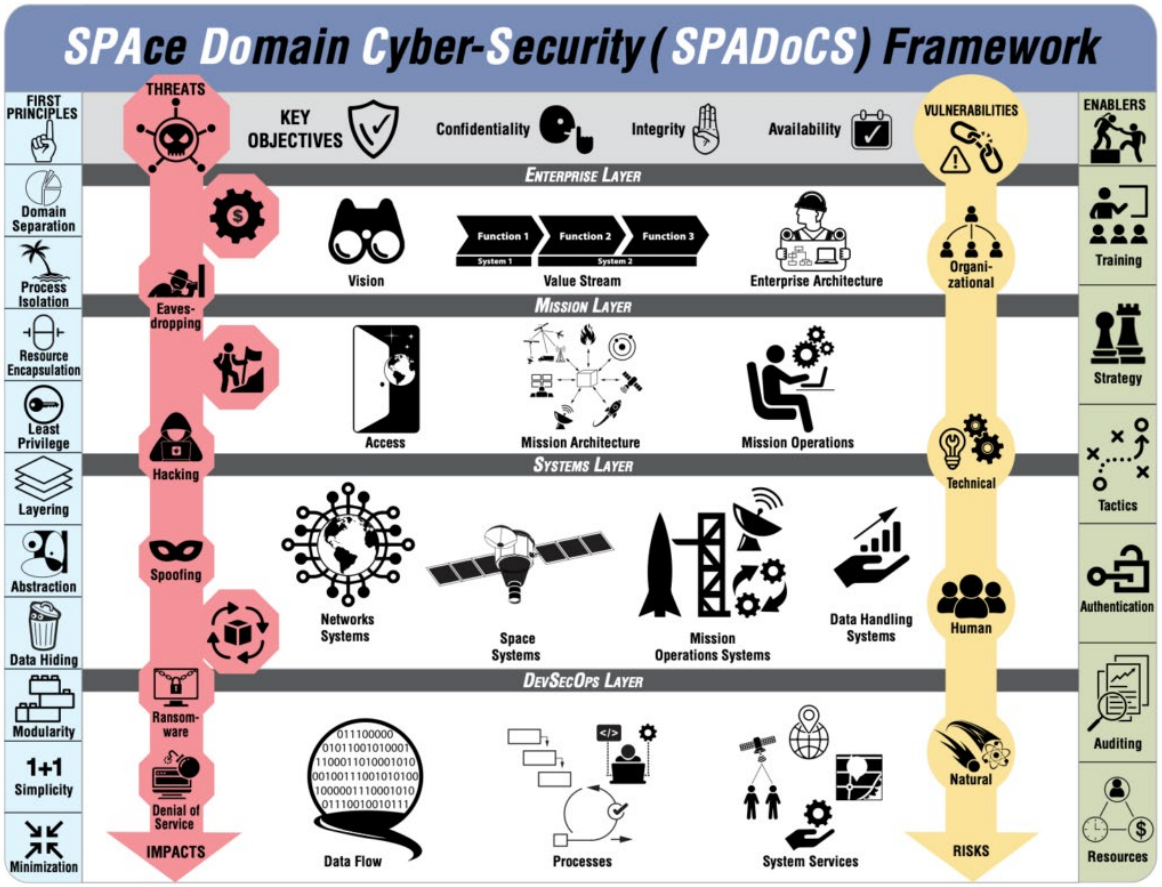

Figure 1: Space Domain Cyber-Security Framework. The SpaDoCs framework describes the main challenges of cybersecurity in the space domain

This framework was integrated into the course (Plotnek,et al 2022) to give cybersecurity professionals the specialized skills they need to manage and secure systems in the space domain. By leveraging the SPADOCS framework, the course (Plotnek,et al 2022) addresses the unique cybersecurity requirements of space missions and prepares professionals for the complexities of securing space assets in an evolving threat landscape.

5. Blockchain in Space

The rapid growth of satellite communications has broad application prospects for space information networks, which are based on various aerospace and ground equipment. However, these networks are susceptible to various cyber and physical attacks, making security a significant concern. This paper proposes the application of blockchain in space information network security, focusing on areas, advantages, and challenges. Blockchain is a decentralized and distributed database invented by Satoshi Nakamoto in 2008, composed of blocks linked using cryptography. The development of blockchain can be divided into three phases: blockchain 1.0, which is a decentralized transparent ledger with transaction records of digital currency, blockchain 2.0, which decentralizes markets through smart contracts, and blockchain 3.0, which includes coordination applications beyond currency, economics, and markets, such as government, health, science, and education. The paper concludes by analyzing the challenges of blockchain application in space information network security and highlighting the need for additional methods to strengthen the security of centralized nodes in the space information network.

Blockchain technology has made progress in space, with Blockstream leasing bandwidth on satellites to broadcast real-time Bitcoin blockchain data. The Blockstream Satellite network consists of three

geosynchronous satellites, covering two-thirds of Earth's landmass and enabling Bitcoin users in Africa, Europe, South America, and North America to download Bitcoin blockchain data. Blockstream plans to lease a fourth satellite to cover Asia, allowing 99.999996% of the world's population to receive blockchain data from Blockstream Satellites. Nexus Earth plans to deploy its own low-earth orbit satellite network to support the distribution and use of its NXS cryptocurrency. The network would consist of two layers: a relay layer and an outer processing and storage layer, with an estimated 300 cubesats achieving global coverage. Nexus satellites would act as nodes of the Nexus blockchain, and third-party applications could be hosted on satellites, with customers paying for these services using NXS cryptocurrency. Blockchain applications in space information networks include identification, self-reconfiguration, and smart contracts to improve network resilience.(Cheng,2019)

By offering decentralized and secure tools for processing and manipulating space resources in the form of space digital tokens, blockchain technology has the potential to have a major impact on space business and scientific research. The numerous uses of space mining are reflected in the tokenization of space resources, including orbits, satellites, spacecraft, orbital debris, asteroids, and other space objects, in the form of digital tokens based on blockchain technology. All space transactions and communications may be tracked in a visible, verifiable, and secure manner using blockchain algorithms built on smart contracts. Based on the idea of space digital currencies, this paper is one of the first attempts to theoretically investigate the application of blockchain theory in the space business. (Torky,et.al 2020)

This diagram shows the recommended process operations model, which shows how to use the Consortium's blockchain (i.e. a blockchain system that is 'semi-private' and has a controlled miner's group, but can work across different organizations) to store, manage and protect satellite flight data at all stages of the satellite launch lifecycle. At each stage, the blockchain will be updated with new blocks of data that will be available 3 Figure 2. Blockchain satellite mission data life cycle using a consortium blockchain. (Torky,et.al 2020)

This diagram shows the recommended process operations model, which shows how to use the Consortium's blockchain (i.e. a blockchain system that is 'semi-private' and has a controlled miner's group, but can work across different organizations) to store, manage and protect satellite flight data at all stages of the satellite launch lifecycle. At each stage, the blockchain will be updated with new blocks of data that will be available 3.

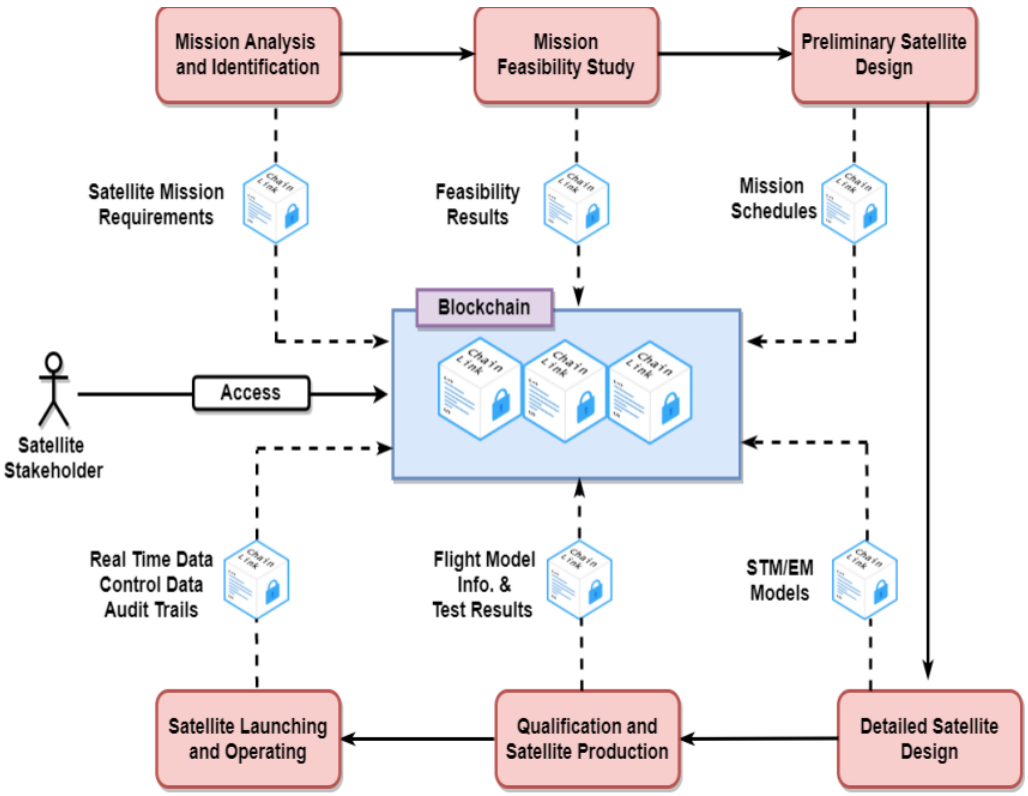

Figure 2: Blockchain satellite mission data life cycle using a consortium blockchain. (Torky, et.al 2020))

This diagram shows the recommended process operations model, which shows how to use the Consortium's blockchain (i.e. a blockchain system that is 'semi-private' and has a controlled miner's group, but can work across different organizations) to store, manage and protect satellite flight data at all stages of the satellite launch lifecycle. At each stage, the blockchain will be updated with new blocks of data that will be available 3 Figure 2. Blockchain satellite mission data life cycle using a consortium blockchain.((Torky,et.al 2020))

Space Challenges and Solutions: A Blockchain Framework As noted in recent studies and discussed in this paper (Torky,et.al 2020) ,blockchain technology stands to make significant advances in the space industry. In 2017, NASA awarded a $330,000 grant to Dr. Jin Wei Kocsis to develop a blockchain-based spacecraft system, known as the Resilient Networking and Computing Paradigm (RNCP). This project marks NASA's initial exploration of blockchain's potential within space ap plications. Blockchain enables the tokenization of space assets such as satellites, spacecraft, space debris, orbits, and asteroids, managing them as digital tokens. Converting these assets into tokens allows global transactions involving space resources through blockchain protocols and smart contracts. Blockchain can also introduce greater autonomy for spacecraft, empowering them to make critical decisions without reliance on ground stations. This vision supports the development of a blockchain framework to create new models that illustrate the unique benefits of blockchain in the space industry.

Torky,et.al 2020 proposes a blockchain-based framework that includes models to address space industry challenges, such as:

- Tracking and Data Relay Satellites (TDRS): Blockchain enables the management of complex satellite network connections by using digital tokens, optimizing user queries and enhancing response efficiency.
- Satellite Launch Logistics: A blockchain-based peer-to peer network can streamline the complex, multi-stakeholder satellite launch process. Blockchain offers a transparent and decentralized way to manage logistics, funding, and communication between entities involved in satellite launches.
- Orbital Asset Tokenization: Space assets like satellites and debris can be tokenized, allowing real-time tracking and management through smart contracts. This tokenization aids stakeholders in monitoring space activities and ensuring asset security.
- Satellite Swarm Communications: Blockchain helps secure satellite swarm communications by creating virtual trusted zones and enabling decentralized, secure data sharing between satellites, especially important in scenarios like avoiding space debris collisions.

5.1 Limitations of using Blockchain Technology

Blockchain technology, while promising, faces several challenges and limitations in space applications. Some key limitations include:

- Latency and Bandwidth Constraint: Space communication suffers from high latency and limited bandwidth, especially for assets far from Earth. Blockchain relies on rapid consensus among nodes, but long delays in data transmission between space nodes and Earth-based nodes can disrupt this process, complicating real-time data synchronization and consensus.
- Energy Consumption: Blockchain processes, particularly proof-of-work (PoW) consensus algorithms, can be highly energy-intensive. This is impractical in space, where energy is a scarce resource, as spacecraft and satellites have limited power supplies and rely primarily on solar energy. Alternative consensus mechanisms (like proof-of-stake) might be needed, but they are less established in blockchain for space applications.
- Computational Power Limitations: Spacecraft and satellites have limited computational capacity due to constraints on weight, energy, and thermal dissipation. Blockchains, particularly those requiring extensive cryptographic calculations or large data processing, could exceed the processing capabilities of space-based systems.
- Data Storage Constraints: Blockchain systems require storing data across multiple nodes, which can lead to a large cumulative storage requirement. In space applications, storage space on satellites is limited, making it challenging to maintain the entire blockchain ledger. Pruning or optimized storage solutions would be necessary to manage this issue.
- Security Risks in Decentralized Networks: While blockchain enhances data security through its decentralized structure, it also opens challenges like the risk of network partitioning. In the event of communication disruption between satellite nodes or between satellites and Earth, network partitioning can result in data silos, potentially impacting security and data integrity.

- Regulatory and Interoperability Challenges: The space industry is highly regulated, and blockchain adoption may require new standards and regulations. Furthermore, inter-operability among different blockchain systems and legacy space infrastructure presents additional technical challenges, particularly when integrating decentralized systems across international and multi-agency collaborations.
- Cost and Complexity of Upgrades: Spacecraft and satellites have long development cycles and upgrading them in space is logistically and financially challenging. Blockchain technology, especially if implemented on hardware, could require periodic updates or modifications to maintain security or performance, which may be impractical in space.

Addressing these limitations may involve modifying consensus algorithms, developing specialized blockchain architectures for low-resource environments, and creating hybrid blockchain models that combine centralized and decentralized elements to suit space-based operations

6. Results and Recommendations for Future Work

The results of this research demonstrate an understanding of data security challenges in space and provide a set of proposed solutions to enhance data protection in this domain.

The paper focuses on enhancing data security in space-based systems, which face significant vulnerabilities in satellite communications, sensors, and infrastructure due to threats like jamming, spoofing, and data interception. To counter these, the authors propose a security framework incorporating low-bandwidth encryption, distributed network authentication, and space-specific intrusion detection systems. They emphasize lightweight, latency-sensitive security measures that also protect ground infrastructure from both cyber and physical threats. This holistic approach aims to preserve data confidentiality, integrity, and availability across mission-critical operations in space, preparing for the increasing risks as space activities expand.

The results highlight that blockchain technology could offer substantial benefits for data protection within space information networks, though challenges such as latency, bandwidth constraints, and energy consumption remain. Future exploration and technology adaptation are recommended to fully address these limitations and further strengthen the cybersecurity posture of space systems.

This paper establishes a foundational discussion of cybersecurity for the space domain, particularly emphasizing the integration of blockchain technology. While the abstract effectively outlines the desired goals, there is room for a more rigorous and detailed exploration of blockchain applications in space systems. Key points for enhancing the study are outlined below

Enhanced Analysis of Blockchain Applications for Space Systems

Detailed Use Cases:

Blockchain technology can support space systems in the following ways:

- **Satellite Data Management:** Blockchain-enabled decentralized ledgers can securely store and manage satellite telemetry, tracking, and control (TT&C) data across mission lifecycles.
- **Space Asset Tokenization:** Transforming space resources (e.g., satellites, orbital slots, debris) into digital tokens allows for secure and transparent management via smart contracts.
- **Supply Chain and Launch Coordination**: Blockchain facilitates a transparent, tamper-proof network for managing satellite assembly, testing, and launch logistics among multiple stakeholders.
- **Inter-Satellite Communication:** Decentralized networks enhance security in satellite swarm communications and data relay operations, ensuring resistance to jamming and malicious alterations.

Advanced Operational Scenarios: To improve reliability, blockchain frameworks should incorporate adaptive consensus mechanisms like Proof-of-Stake or Delegated Proof-of-Stake for reduced energy consumption in space environments.

Limitations of Blockchain for Space Systems

A comprehensive exploration of blockchain's limitations in the space domain reveals the following challenges:

Latency and Bandwidth Constraints: High latency in space communications hampers real-time consensus, while limited bandwidth restricts data transmission needed for blockchain synchronization.

Energy Consumption: Resource-intensive consensus algorithms, such as Proof-of-Work, are impractical due to energy limitations on satellites and spacecraft relying on solar power.

Computational Capacity: Space-based systems with constrained hardware capabilities may struggle to handle computationally intensive cryptographic processes required by blockchain.

Data Storage and Ledger Maintenance: Blockchain's decentralized structure demands substantial storage across multiple nodes. Space systems, with limited memory, require optimized or pruned blockchain solutions to maintain ledger integrity.

Interoperability and Regulation: Integrating blockchain into international space operations necessitates cross-border agreements on standards, frameworks, and compliance mechanisms.

Modification of Standards to Enable Blockchain Adoption

Adaptation of CCSDS Protocols: The CCSDS Space Data Link Security (SDLS) protocol should be expanded to incorporate blockchain functionalities such as decentralized identity management and ledger-based authentication.

New Space-Specific Blockchain Standards:

Development of lightweight blockchain standards tailored for the space domain, including:

- Consensus algorithms optimize for low-latency, low-power environments.
- Pruning strategies to minimize storage requirements on satellites.
- Interoperable frameworks for seamless integration with legacy space systems.

Security Certification and Compliance: Establishing a standardized certification process for blockchain-based space applications ensures alignment with international cybersecurity norms.

Integration of Blockchain into the SPADOCS Framework

Layer-Specific Integration: Blockchain technology should be embedded at multiple levels of the SPADOCS framework:

Mission Layer: Tokenized tracking of satellite resources and mission-critical data for real-time management.

System Layer: Decentralized protocols to enhance security in inter-satellite and ground-to-space communications.

DevSecOps Layer: Blockchain-based logs and secure coding practices to ensure resilience against cyber threats during system development and operation.

Collaboration Enhancement: Blockchain can improve collaboration and transparency across mission, enterprise, and international boundaries by securely linking multiple stakeholders through a shared, immutable ledger.

Dynamic Threat Monitoring: The SPADOCS framework can leverage blockchain-enabled analytics for predictive threat monitoring and anomaly detection across distributed space assets.

7. Conclusions

This revised paper highlights the potential of blockchain to revolutionize cybersecurity in the space domain while addressing its limitations and necessary standard modifications. A deeper integration into the SPADOCS framework provides a systematic approach to mitigating threats and fostering resilience in space operations.

Future work should focus on:

- Designing experimental models to test blockchain performance in space-like environments.
- Collaborating with international space agencies to establish interoperable standards.
- Developing hybrid blockchain models to combine the benefits of decentralized security with the efficiency of centralized systems.

By extending prior work with rigorous analysis and practical implementation strategies, blockchain can transform space cybersecurity, ensuring safe, transparent, and efficient operations in the rapidly evolving space sector.

References

Cheng, S., Gao, Y., Li, X., Du, Y., Du, Y., and Hu, S., 2019. Blockchain Application in Space Information Network Security. In: Yu, Q., ed., *Space Information Networks*. SINC 2018. Communications in Computer and Information Science, vol. 972, Singapore: Springer. https://doi.org/10.1007/978-981-13-5937-8_1.

Falco, G., 2019. Cybersecurity principles for space systems. *Journal of Aerospace Information Systems*, 16(2).

Jiang, C., Wang, X., Wang, J., Chen, H.-H., and Ren, Y., 2015. Security in space information networks. *IEEE Communications Magazine*, 53, pp.82–88.

Kang, S., Qiaozhong, D., and WeiQiang, Z., 2013. Space Information Security and Cyberspace Defense Technology. *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, Beijing, China, pp.1509–1511. doi: 10.1109/GreenCom-iThings-CPSCom.2013.267.

Krelina, M., 2023. The Prospect of Quantum Technologies in Space for Defence and Security. *Space Policy*, 65, p.101563.

Manulis, M., Bridges, C.P., Harrison, R., Sekar, V., and Davis, A., 2021. Cyber security in New Space: Analysis of threats, key enabling technologies and challenges. *International Journal of Information Security*, 20(3), pp.287–311.

Plotnek, J. and Slay, J., 2022. Space Systems Security: A Definition and Knowledge Domain for the Contemporary Context.

Quiquet, F., 2023. The Space Domain Cybersecurity framework, also known as SpaDoCs. Available at: https://www.spacesecurity.info/en/space-domain-cybersecurity-framework-also-known-as-spadocs/#:~:text=What%20is%20SpaDoCs%20Framework%20%3F%20SpaDoCs%20Framework%20describes,drilling%20down%20through%20mission%2C%20system%20and%20DevSecOps%20layers [Accessed 12 Mar. 2024].

Salykov, A., Aimbetov, A., Yesmagulova, N., and Jussibaliyeva, A., 2023. Factors and trends in the development of the space industry in the context of the digitalization of the economy of the Republic of Kazakhstan. *Environment, Development and Sustainability*.

Seenivasan, M., Krishnasamy, V., and Muppudathi, S.S., 2022. Data division using Fuzzy Logic and Blockchain for data security in cyber space. *Procedia Computer Science*, 215, pp.452–460. doi: 10.1016/j.procs.2022.12.047.

Thangavel, K., Plotnek, J., Gardi, A., and Sabatini, R., 2022. Understanding and Investigating Adversary Threats and Countermeasures in the Context of Space Cybersecurity. *2022 IEEE/AIAA Digital Avionics Systems Conference (DASC)*. doi: 10.1109/DASC55683.2022.9925759.

Varadharajan, V. and Suri, N., 2023. Security challenges when space merges with cyberspace. *Space Policy*.

Wang, R., Taleb, T., Jamalipour, A., and Sun, B., 2009. Protocols for reliable data transport in space internet. *IEEE Communications Surveys & Tutorials*, 11(2), pp.21–32. doi: 10.1109/SURV.2009.090203.

Winkler, S. and Danner, L., 1974. Data Security in the Computer Communication Environment. *Computer*, 7(2).