BLOCKCHAIN FOR AVIATION OPERATIONS CONCEPT: MITIGATING ADS-B DATA SPOOFING, JAMMING, AND INTERCEPTION WITH PROOF OF LOCATION CONSENSUS NETWORK

Richard S. Walsh, MSc., A.A.E., a3i global aeronautics advisors, LLC

The intent of this research paper is to provide an informed pathway to enable new capabilities in aviation through the application of blockchain technology within the National Airspace System, addressing specific functional and data sharing needs in support of both Unmanned Aircraft Systems and Advanced Air Mobility. Specifically, this paper explores the application of blockchain technology in an operational environment, a first. Specifically, leveraging blockchain toward resolving ADS-B vulnerabilities of data spoofing, jamming, and interception. Once defined, the problem space was further refined through a literature review and subsequent analysis of the limitations of that research. Informed by the literature review, the opportunity space was explored with emphasis given to blockchain technology's capacity to resolve operational barriers to scale Advanced Air Mobility. Protentional challenges to deploying blockchain technology are addressed and uncertainties identified where applicable. Two sets of recommendations are provided and should be considered cumulatively. Proof of Location Consensus Network seeks to mitigate ADS-B vulnerabilities of data spoofing, jamming, and interception. Elimination of these vulnerabilities will decrease operational risk, enhance ADS-B reliability, and enable increasingly autonomous and ubiquitous operations.

Nomenclature

ADS-B Type Code	(TC)	Internet(s) of Things	(IoT)
Advanced Air Mobility	(AAM)	Long Short-Term Memory	(LSTM)
Air Traffic Control	(ATC)	Machine Learning	(ML)
Air Traffic Management	(ATM)	Maximum Power Emitted While Transmitting	(TX)
Air Traffic Operations Simulation	(ATOS)	Minimum Aviation Safety Performance Standards	(MASPS)
Airspace Development Program-2	(ATD-2)	NASA Aeronautics Research Mission Directorate	(ARMD)
American Institute of Aeronautics and Astronautics	(AIAA)	National Airspace System	(NAS)
Artificial Intelligence	(AI)	Next Generation Air Transportation System	(NextGen)
Automatic Dependent Surveillance-Broadcast	(ADS-B)	Performance-Based Navigation	(PBN)
Beyond Visual Line of Sight	(BVLOS)	Practical Byzantine Fault Tolerance	(PBFT)
Bitcoin	(BTC)	Proof of Authority	(PoA)
Command, Control, and Communications	(C3)	Proof of Location Consensus Network	(PLCN)
Community of Interest	(CoI)	Proof of Stake	(PoS)
Compound Annual Growth Rate	(CAGR)	Proof of Work	(PoW)
Convergent Aeronautics Solutions	(CAS)	pulse-position modulation	(PPM)
Decentralized Applications	(dApps)	Sense-and-Avoid	(SAA)
Deep Learning	(DL)	Small Unmanned Aircraft System	(sUAS)
Detect and Avoid	(DAA)	Terawatt-hours of energy	(TWh)
Distributed Air-Ground Traffic Management	(DAG-TM)	Terminal Sequencing and Spacing	(TSS)
Federal Aviation Administration	(FAA)	Time Distance of Arrival	(TDoA)
Global Navigation Satellite System	(GNSS)	Transactions per second	(TPS)
Gross Domestic Product	(GDP)	Unmanned Aerial Vehicles	(UAV)
Human-In-The-Loop	(HITL)	Unmanned Aircraft System	(UAS)
Inertial Navigation Systems	(INS)	Unmanned Aircraft System Traffic Management	(UTM)
International Air Transport Association	(IATA)	Urban Air Mobility	(UAM)

I. INTRODUCTION

Automatic Dependent Surveillance-Broadcast (ADS-B) infrastructure requires that all surveillance be open communications. ADS-B signals are unauthenticated and unencrypted, and therefore non-secure. “Spoofing” or inserting a fake aircraft into the ADS-B system is relatively easy and thereby can adversely impact safe and efficient flight. Malicious manipulation of ADS-B signals transmits false information about an aircraft’s position, velocity, and identification, which interferes with Detect and Avoid (DAA) and Air Traffic Control (ATC). Spoofing a target into the real ADS-B system would be a simple matter of transmitting the signal on the ADS-B frequencies (978 and 1090 MHz) [1]. While the Federal Aviation Administration (FAA) has procedures for identifying and eliminating spoofed targets via ground stations (air-to-ground), there is currently no mitigation capability between transmitting/receiving aircraft (air-to-air). In its effort to remedy this technical barrier, the FAA is applying resources through research into new technologies such as encryption, use of multiple receivers to verify signal authenticity, algorithmic data integrity check, and data source authentication. Machine Learning (ML) algorithms used in pattern recognition, geolocation of signal source, and determination of signal strength are additional research areas being explored to further alleviate spoofing.

A. ADS-B and Next Generation Air Transportation System

ADS-B is a core technology in the Next Generation Air Transportation System (NextGen). NextGen is an air space modernization effort designed to improve the efficiency, safety, and environmental impact of the U.S. air transportation system. As surveillance technology, ADS-B uses satellites to determine the position of aircraft and broadcast that information to air traffic controllers and other aircraft in real-time. This information is used to track aircraft, provide traffic information to pilots, and create more efficient flight paths. Advantages of ADS-B over traditional radar surveillance include its precision and immunity to weather. As airspace becomes increasingly congested with new technologies such as semi- and (fully) autonomous air vehicles, the unimpeded capabilities of ADS-B are essential toward ensuring a safe, efficient, and secure air space system.

B. ADS-B and Urban Air Mobility

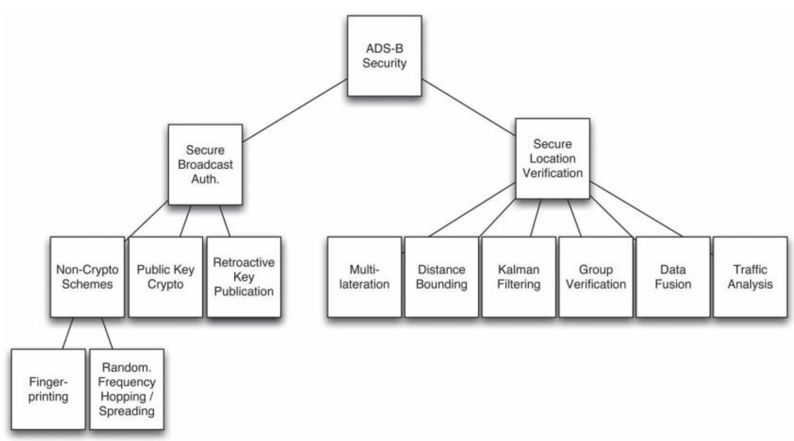
The FAA defines Urban Air Mobility (UAM) as a safe and efficient aviation transportation system utilizing highly automated aircraft that will operate and transport passengers and cargo at lower altitudes within urban and suburban areas. UAM relies on ADS-B in many ways to include providing a way for UAM aircraft to see and avoid each other. Given the complexity and operational density envisioned from UAM operations, ADS-B is essential for operational safety. Further, ADS-B allows UAM aircraft to communicate with ATC and can also be used to collect data about UAM operations. This data can then be used to improve the safety and efficiency of UAM operations.

II. PROBLEM STATEMENT

ADS-B vulnerabilities of data spoofing, jamming, and interception increase operational risk, inhibit ADS-B reliability, and undermine ADS-B use for UAM and autonomous operations which may limit UAMs scalability.

A. ADS-B Cybersecurity Literature Review

The field of ADS-B cybersecurity research is prolific in the number of publications produced. This is a problem space that is well understood, however no one solution set has yet to emerge as superior to the field. A sampling of more recent research provides insight into the investigative direction to mitigate certain ADS-B vulnerabilities. In their paper, *Actual TDoA-based augmentation system for enhancing cybersecurity in ADS-B*, Ahmed Abdelwahab Elmarady et al., proposes a new system for enhancing the cybersecurity of ADS-B. The system uses a crowdsourced network of ADS-B receivers to collect data, which is then used to train a machine learning model to detect spoofing attacks. The model can detect spoofing attacks with a high accuracy, even when the attacker is using a sophisticated spoofing device [2]. Saulius Rudys et al., discuss physical layer vulnerabilities of ADS-B and propose several techniques for mitigation. The techniques include using spread spectrum modulation, frequency hopping, and authentication [3]. Wang et al., offer a new method for detecting ADS-B spoofing attacks using Long Short-Term Memory (LSTM) neural networks. The method uses the LSTM network to learn the normal patterns of ADS-B messages, and then uses this knowledge to detect anomalies that may indicate a spoofing attack [4]. A new method for detecting Global Navigation Satellite System (GNSS) spoofing of ADS-B equipped aircraft using Inertial Navigation Systems (INS) is proposed by Birendra Kujur et al. The method uses the INS to estimate the aircraft's position and velocity, and then compares this estimate to the position and velocity reported by the ADS-B receiver. If the two estimates are significantly different, then a spoofing attack is likely [5]. In their paper, Martin Strohmeier et al., survey security vulnerabilities of the ADS-B protocol and discuss possible countermeasures. Several security features are proposed that could be added to the ADS-B protocol, such as message authentication, message encryption, and access control. Challenges of implementing these security features in the ADS-B protocol are discussed as well and focus on the protocols broadcast signal in the open and in real-time. ADS-B is broadcast in the open, sent to all receivers within range making it difficult to ensure that only authorized parties can receive ADS-B messages. ADS-B is a real-time protocol requiring messages to be processed quickly, making it difficult to implement some security features, such as message encryption, which can add latency to the protocol. Figure 1 delineates the results of the author's literature review; two distinct approaches to securing ADS-B are distilled: secure broadcast authentication and secure location verification [6].



<u>Source</u>: *Strohmeier et al.: On The Security Of The ADS-B Protocol*

Fig. 1 Taxonomy of ADS-B Security Research

Figure 1 is instructive in its categorization of method relative to ADS-B data security barrier resolution. Currently, there is no one accepted solution to securing ADS-B broadcast signal authenticity. For secure location verification, multilateration, also known aa hyperbolic positioning, is the method by which ADS-B signal authenticity is verified. Multilateration additionally solves for identification and resolution of ADS-B noncompliant aircraft by way of radar and air traffic control.

Additional approaches used in mitigating spoofing and jamming of the ADS-B signal involve machine learning and neural networks. Both machine learning and neural networks are algorithms used in artificial intelligence. Machine learning refers to developing algorithms that can analyze and learn from data to make decisions while the neural networks is a group of algorithms in machine learning that perform computations similar to neurons in the human brain [7]. Rudys et al., proposes physical layer protection techniques e.g., spread spectrum modulation and jamming detection and mitigation algorithm, to provide security against message injection attacks, such as spoofing, and partial security against jamming. Simulations evaluated the proposed structure, verifying effective protection of ADS-B against spoofing and jamming attacks [8][9]. Utilizing deep neural networks, Ying et al., presents a deep learning-based approach for detecting ADS-B spoofing attacks. The proposed approach consists of two stages: a message classifier and an aircraft classifier. The message classifier uses a deep neural network to classify each incoming ADS-B message as either legitimate or spoofed. The aircraft classifier then uses a separate deep neural network to identify the aircraft that is associated with the message. The approach was evaluated utilizing a dataset of real-world ADS-B messages, achieving high accuracy in detecting spoofing attacks. This approach correctly identified 99.34% of the spoofing attacks in the dataset [10].

B. NASA and ADS-B Research

NASA's research regarding ADS-B has been instrumental in the development and application of what the FAA has described as a core technology for NextGen. NASA has conducted research on ADS-B in the areas of performance, interoperability, cost, and safety and has evaluated ADS-B performance in a variety of environments, including dense airspace, mountainous terrain, and areas with high levels of interference. NASA has worked to ensure that ADS-B systems from different manufacturers are able to communicate with each other or are interoperable. NASA has evaluated the safety benefits of ADS-B, including its ability to improve traffic surveillance and conflict detection and its research has contributed to cost containment of ADS-B systems, making them more affordable for small aircraft operators helping to make ADS-B a viable technology for the future of aviation.

1. ADS-B Sense-and-Avoid System

In their 2017 presentation to the American Institute of Aeronautics and Astronautics (AIAA) entitled *Automatic Dependent Surveillance Broadcast ADS-B Sense-and-Avoid System*, NASA researchers Ricardo Arteaga, et al. provide results, benefits and compliance to the FAA mandate that aircraft operating in airspace that now requires a Mode C transponder must be equipped with ADS-B Out by January 1, 2020 in order to have clear guidelines to show aircraft designers how to integrate ADS-B technology into future Unmanned Aircraft System (UAS) vehicles [11]. The authors describe the design and implementation of an ADS-B sense-and-avoid system for a UAS. The system uses ADS-B data to construct a state-based airspace model, which is used to predict future aircraft trajectories. The system also uses a conflict resolution algorithm to generate new flight paths that avoid potential collisions. Results of flight tests that were conducted to evaluate the performance of the ADS-B sense-and-avoid system validate that the system was able to successfully sense and avoid other aircraft, obstacles, and weather hazards and demonstrate that the ADS-B sense-and-avoid system is a promising technology for improving the safety of UAS operations.

2. **ADS-B Distributed Air-Ground Traffic Management**

In a paper titled *ADS-B within a Multi-aircraft Simulation for Distributed Air-Ground Traffic Management*, authors Richard Barhydt et al., discuss the use of ADS-B in a multi-aircraft simulation for Distributed Air-Ground Traffic Management (DAG-TM). DAG-TM is a concept of operations for the National Airspace System (NAS) that relies on ADS-B and other technologies to improve safety and efficiency. The authors of the paper conducted a simulation of a 100-aircraft scenario using NASA Langley Research Center's PC-based Air Traffic Operations Simulation (ATOS). The simulation included both ADS-B-equipped and non-ADS-B-equipped aircraft. The results of the simulation showed that ADS-B can be used to improve traffic surveillance and conflict detection in a multi-aircraft environment. However, the authors also noted that there are some challenges associated with using ADS-B in a NAS environment, such as message collision and interference. The authors conclude that ADS-B is a promising technology for DAG-TM, but that further research is needed to address the challenges associated with its use in the NAS [12].

3. **ADS-B use for Beyond Visual Line of Sight**

ADS-B is used to provide situational awareness to the ground pilot and the chase pilot in studies conducted by NASA. *Demonstration of Two Extended Visual Line of Sight Methods for Urban UAV Operations* by Nicholas Rymer et al., demonstrate that ADS-B is instrumental for increased situational awareness, reduction of collision risk, and improved efficiency of Beyond Visual Line of Sight (BVLOS) operations by reducing the need for the pilot to constantly monitor a small, unmanned aircraft system's (sUAS) position. This can free up the pilot to focus on other tasks, such as planning the sUAS's flight path or monitoring the sUAS's systems. In their study, the ground pilot and the chase pilot use ADS-B data to track the position of the sUAS and to avoid collisions with other aircraft and obstacles. ADS-B data is also used to monitor the sUAS's flight path and to ensure that the sUAS is not flying in restricted airspace. The authors found ADS-B to be an essential tool for safe and reliable BVLOS operations and recommend that ADS-B be used in all BVLOS operations to provide situational awareness to the pilot and to help prevent collisions [13].

4. **ADS-B use of Blockchain Technology**

In his research paper *Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy*, Ronald J. Reisman proposes using ADS-B data to feed a blockchain-based air traffic management system. The blockchain would provide a secure and tamper-proof way to store and share ADS-B data. This would allow air traffic controllers to have a real-time view of the air traffic situation and would also help to improve safety and efficiency. To mitigate privacy concerns of aircraft operators and passengers, the author proposes using a permissioned blockchain, which would allow only authorized users to access data. Smart contracts to automate certain tasks, such as the processing of flight plans and the issuance of clearances, are also proposed. The author posits that the use of ADS-B in a blockchain-based air traffic management system has the potential to revolutionize air traffic control. By providing a secure, reliable, and efficient way to store and share data, blockchain could help to improve safety, efficiency, and environmental performance and would provide a secure and tamper-proof way to store and share ADS-B data. This would allow air traffic controllers to have a real-time view of the air traffic situation, helping to improve safety and efficiency of the NAS. The blockchain could help to improve efficiency by automating certain tasks, such as the processing of flight plans and the issuance of clearances and could help reduce costs by eliminating the need for some existing systems and processes [14].

C. Summary of Problem/Need

ADS-B requires a reliable and secure network infrastructure to support the exchange of data between aircraft and ground stations. This network infrastructure must be able to handle the large volume of data that is generated by ADS-B transmissions, and it must be secure from unauthorized access. ADS-B is considered a vulnerability feature as it can be used to track aircraft movements and identify aircraft identities. This information could be used by malicious actors to plan attacks on aircraft and disrupt air traffic control. Mitigation of the risks associated with ADS-B vulnerabilities include encryption thereby introducing additional complexity into the identification and tracking of aircraft. Additionally, combining other technologies with ADS-B, such as radar and air traffic control make it more difficult for malicious actors to exploit ADS-B vulnerabilities but may increase human workload, cost, and complexity. These strategies may further negatively impact system efficiency, possibly burdening the system with delay, impacting efficiency for the price of safety. Ensuring the validity of ADS-B data is paramount to reliability. Reliability requires guarding ADS-B data from malicious intent without adversely impacting its in-time capability. Therefore, risk reduction associated with ADS-B vulnerabilities must include mitigation of data spoofing, jamming, and interception.

D. Societal Importance, Benefit

UAM and autonomous operations hold the promise of improving air transportation, reducing traffic congestion, improving air quality, and making transportation more accessible. Achieving these goals however requires surmounting regulatory, safety, public acceptance, and technological barriers. Technological barriers include aircraft design, propulsion, avionics, air traffic management, battery technology, crashworthiness, and security. ADS-B is central to air traffic management for NextGen and, as such, a core technology that UAM is dependent upon. Addressing the challenges of UAM and autonomous operations will have a significant positive impact on society as these technologies have the potential to improve safety through human error reduction, enhanced systemwide efficiency by way of time and fuel reduction, increased system flexibility by ensuring a more agile and responsive transportation system, and the creation of new transportation services and providers. Addressing ADS-B vulnerabilities ensures that UAM and autonomous operations will be safe and reliable as well as providing a societal benefit. Benefits include reduction of noise pollution, increased access to rural areas that are difficult or impossible to reach by road and rail, and improved disaster response.

E. NASA Convergent Aeronautical Solutions

The Convergent Aeronautics Solutions (CAS) project invests in seemingly improbable ideas that might lead to solutions to the problems that plague aviation and impact safety, environmental and community impact, and the global growth in air traffic [15]. Originating with the advancement of ADS-B, the problem as defined herein remains a complex and challenging space that has yet to be resolved. UAM and autonomous operations will increasingly add complexity to an already intricate air space. Reliance on ADS-B requires resolution of this problem set to ensure NextGen's mission of improving aviation operational efficiency is met. Air Traffic Management (ATM) is a core expertise for NASA [16]. Ensuring aircraft are safely separated and enhancing the efficiency of the NAS system continues to be central to NASA research. Combined, NASAs modeling and simulation expertise with decades of experience innovating air traffic management and performing key research with government, academic and industry partners underpin the advancement of NextGen. With its capability to seed improbable ideas, CAS is well positioned to advance concepts that may facilitate the development of initiatives and technologies in support of NextGen. Further, this concept is consistent with NASA Aeronautics Research Mission Directorate (ARMD) vision for aeronautical research encompassing a broad range of technologies to meet future needs of the aviation community, the nation, and the world for safe, efficient, flexible, and environmentally sustainable air transportation [17]. Last, research of this concept is consistent with NASA Strategic Thrusts 1 – Safe and Efficient Growth in Global Operations, 4 – Safe, Quiet, and Affordable Vertical Lift Air Vehicles, 5 - In-Time System-Wide Safety Assurance, and 6 - Assured Autonomy for Aviation Transformation [18].

1. **Transformative Potential**

Resolving ADS-B vulnerabilities of data spoofing, jamming, and interception will reduce operational risk, increase ADS-B reliability, and strengthen ADS-B use for UAM and autonomous operations. De-risking the NAS and enhancing operational efficiency contributes to NextGen's modernization toward a safer, more efficient, and more predictable NAS.

2. **New insights into the problem**

The development of small, lightweight, and low-cost automatic surveillance broadcast transceivers for unmanned aerial vehicles is the latest trend in the ADS-B market space [19]. The trend is anticipated to drive market valuation to $2.8 billion by 2028 from $848 million in 2020 representing a compound annual growth rate of 18% over the planning horizon [20]. Modernization of air traffic management infrastructure, expansion of new airports, and growing demand for Unmanned Aerial Vehicles (UAV) are drivers of this global trend. Increased reliance on ADS-B combined with increased demand adds to the complexity of operations. As legacy and autonomous operations merge in a finite airspace, less risk tolerance is required. Unauthorized access and manipulation of the ADS-B signal will restrain the ADS-B market's growth. If left unresolved, ADS-B vulnerabilities create a barrier to UAM scalability and increasingly autonomous operations.

3. **Potential and shortcomings of available means for solution**

Mitigating certain ADS-B vulnerabilities without introducing additional complexity is central to industry acceptance. Any offered solution must work within the existing system without interference of its primary mission. ADS-B is based on satellite communication to determine aircraft position. Aircraft determine their position by communicating with satellites, then broadcast this to ATC to enable it to be tracked. Solutions to mitigate security concerns must enhance the reliability of aircraft position without inducing increased system risk. Artificial Intelligence (AI) and Machine Learning (ML) based methodologies for resolving ADS-B vulnerabilities may introduce complexity that we are neither aware of nor understand. While not uncommon in complex systems, the introduction of uncertainty is unacceptable in human-centric systems that are increasingly reliant upon increasingly autonomous systems. Caution in implementation of AI/ML solutions require consideration of their limitations:

a) Only as smart as people teach them to be [21].
b) Algorithms may perform well when solving easy problems but not as successful with more challenging, real-world problems [22].
c) Using AI/ML or Deep Learning (DL) models may be inappropriate, not meaningful, and add an unnecessary degree of complexity without delivering new insight [23].
d) Threat actors have the same access to AI/ML tools as defenders [24].

III. OPPORTUNITY

As stated in section 2 of this document, ADS-B vulnerabilities of data spoofing, jamming, and interception increase operational risk, inhibit ADS-B reliability, and undermine ADS-B use for UAM and autonomous operations which may limit UAMs scalability. Elimination of these vulnerabilities is therefore the preferred state and may be achievable through the application of Blockchain Technology.

A. Summary of the targeted opportunity

Blockchain allows for peer-to-peer transactions without centralized management, which is why it is attractive for an aviation system use case. Trust is established through protocols, cryptography, and computer code. Once established. trust greatly strengthens the capacity for communication and collaboration between organizations and individuals within peer-to-peer networks, enabling the potential for global networks without centralized formal institutions.

1. Relevance to aviation/aeronautics

The adoption of blockchain technology in the aviation industry is still in its early stages, but it has the potential to revolutionize the way the industry operates. In their paper, *The Role of Blockchain Technology in Aviation Industry*, authors Raja Wasim Ahmad et al., discuss potential applications of blockchain technology in the aviation industry. Applications include tracking aircraft lifecycle, managing aircraft parts supply chain, securing customer loyalty programs, and digitizing crew certificates. All reviewed applications are advantaged by blockchain technologies inherent security, transparency, efficiency, and cost savings relative to alternative technologies [25]. Organizations affiliated with the aviation industry have similarly explored blockchain technology deployment. IATA's *The Future of the Airline Industry 2035* study aims to help airlines and other key aviation stakeholders anticipate the key risks and opportunities that their businesses could face between now and 2035 [26]. The influence of external forces—from geopolitics to technological innovation and environmental concerns—in shaping aviation's future are studied. Five key technology drivers for change are identified: cybersecurity, Internet(s) of Things (IoT), tensions between data privacy and surveillance, alternative modes of rapid transit, and robotics and automation. The main technology recommendations include further exploration of how to take advantage (and manage risks) of new technologies such as blockchain. In its 2018 white paper entitled *Blockchain in Aviation, Exploring the Fundamentals, Use Cases, and Industry Initiatives*, IATA explores five areas of application:

a) Certification – streamlining certification for safety and security.
b) Smart Contracts – codifying agreements with emphasis on the procure-to-pay area.
c) Tokenization – turning assets into pervasive digital twins.
d) Provenance – tracking of valuable physical and virtual assets.
e) Digital ID – managing digital identities of entities across the value chain [27].

As a trade organization, IATAs focus is on the business of the Airline industry and as such its study of blockchain technology strongly aligns with issues affecting that industry, its stakeholders, and member organizations business. However, the five identified areas of application are readily extensible to all sectors of aviation including aviation operations, a field yet explored for blockchain technology. Scalability, governance, and cost of usage have been identified as the main obstacles to global adoption of blockchain however, these obstacles are being addressed thereby unburdening the technology from widespread adoption. Some examples of blockchain use in aviation include:

a) Airlines - Airlines are using blockchain technology to help manage take-off and landing slots. The EU-funded SlotMachine consortium is using blockchain technology to develop a cost-efficient solution which will enable airlines to swap take-off and landing slots more efficiently [28].
b) Aircraft- Boeing supports TrustFlight aircraft maintenance project using blockchain. TrustFlight announced a new digital aircraft maintenance platform in collaboration with Boeing, Canada's RaceRocks, and the University of British Columbia. The university will provide its blockchain expertise for the project. Other companies are using blockchain technology for secure record management of maintenance, flight logs, parts supplies, and other safety critical use cases.
c) Tourism – Applications in the travel domain include reservations, identity verification, loyalty programs, digital payments, and inventory management.
d) Supply chain - Blockchain provides all parties within a respective supply chain with access to the same information, potentially reducing communication or transfer data errors. Less time can be spent validating data and more can be spent on delivering goods and services—either improving quality, reducing cost, or both. Integration of blockchain technology in supply chain has helped overcome three main issues of supply chain: process optimization, data visibility, and demand management [29].

As evidenced by IATAs efforts, industry seems focused on blockchain technology application primarily within business and finance silos and has yet to explore the full capabilities of blockchain technology as applied to resolving specific barriers to flight operations and scalability. Application of blockchain technology to flight operations and scalability may surmount multiple barriers currently faced within this domain. Some of which may be considered "wicked" problems affecting multiple areas of concern. Wicked problems as a concept can be used to highlight limitations of reductionistic approaches for addressing complex societal and environmental problems [30][31]. Utilization of blockchain technology within this domain and for this express purpose may provide pathways toward resolving challenges associated with data provenance, security, latency, certification and regulatory enforcement, and command, control, and communications (C3) during flight operations. Ultimately, the promise of blockchain technology in this space must underpin and advance a secure, efficient, and reliable NAS.

2. Relevance to government lab

The Federal Aviation Act of 1958 established the FAA and made it responsible for the control and use of navigable airspace within the United States. The NAS was created by the FAA to protect persons and property on the ground, and to establish a safe and efficient airspace environment for civil, commercial, and military aviation [32]. Any proposed modification to the NAS, its systems, and operations requires approval from the FAA. ADS-B is a foundational technology for NextGen and as such, any proposed modification to that system requires the attention of the governing agency. Utilization of blockchain technology to mitigate ADS-B vulnerabilities has yet to be researched by government or industry. Certification of blockchain technology for use in aviation operations requires research for it to be meaningfully integrated into future systems and operations that will inevitably evolve with time and need. Evaluation of technology towards industry integration and adoption and relative to safe, secure, and ubiquitous operations must be accommodated within the bounds of government due in large measure to the public safety and public good implications. NASA explores the unknown in air and space, innovates for the benefit of humanity, and inspires the world through discovery. Research goals of blockchain technology relative to aviation are therefore aligned with the NASA mission.

3. Alignment with NASA Aeronautics Research Mission Directorate

NASA ARMD conducts high-quality, cutting-edge research that generates innovative concepts, tools, and technologies to enable revolutionary advances in our Nation's future aircraft, as well as in the airspace in which they will fly [33]. Revolutionary advances in technology tend to carry with them higher degrees of uncertainty and risk. While the elimination of risk in aviation operations is impossible, research into how risk mitigation technologies will affect operational safety, as well as technologies economic viability, is essential toward widespread adoption.

a) ARMD Vision

Introduced in year 2013, ARMDs vision sets forth a plan for aeronautical research for the next quarter century, encompassing a broad range of technologies to meet future needs of the aviation community, the nation, and the world for safe, efficient, flexible, and environmentally sustainable air transportation [34]. ARMDs Strategic Implementation Plan consists of six strategic thrusts; 1. Safe, Efficient Growth in Global Operations, 2. Innovation in Commercial Supersonic Aircraft, 3. Ultra-Efficient Subsonic Transports, 4. Safe, Quiet, and Affordable Vertical Lift Air Vehicles, 5. In-Time System-Wide Safety Assurance, and 6. Assured Autonomy for Aviation Transformation. Resolving ADS-B vulnerabilities of data will reduce operational risk, increase ADS-B reliability, and build confidence in ADS-B use for UAM and autonomous operations which will enable scalability. These outcomes align with ARMD strategic thrusts 1, 4, 5, and 6.

b) Advanced Air Mobility

On May 17, 2023, a request for information on Advanced Air Mobility (AAM) was issued by the Department of Transportation [35]. The purpose of which is to seek the public's input on the development of a national strategy on AAM as required by the Advanced Air

Mobility Coordination and Leadership Act [36]. The act directs the Department of Transportation to establish an Advanced Air Mobility interagency working group to plan and coordinate efforts related to the safety, infrastructure, physical security, cybersecurity, and federal investment necessary to bolster the AAM ecosystem, particularly passenger-carrying aircraft, in the United States. NASA has been assigned to lead the Automation Strategy which focuses "*on understanding the acceleration of the desired transition from initial AAM operations with conventionally qualified, onboard pilots through advanced capabilities proposed by the AAM industry, such as simplified vehicle operations, remotely piloted operations, autonomous operations, and remotely supervised flight operations. This group is considering automation strategy with a comprehensive view related to vehicle, airspace, and enabling communication, navigation, and surveillance (CNS) capabilities to enable various automation/autonomy stages.*"

c) Next Generation Air Transportation System

The Next Generation Air Transportation System, or NextGen, is the ongoing transformation of air traffic control. This transformation includes the transition from primarily ground-based to primarily satellite-enabled surveillance and navigation, from analog voice to digital communication, and from limited data exchange to fully integrated information management [37]. ADS-B is one of NextGen's most important underlying technologies and as such, essential to the promise of AAM.

4. Assessment of current efforts

As listed in Table 1, the most recent research concerning proposed methodologies to mitigate ADS-B vulnerabilities of spoofing, jamming, and interception were evaluated, and limitations of the proposed methods identified. Research was primarily conducted within simulated environments, assessing minimal vulnerabilities. Conclusions were broadly layered or generalized covering aspects of the problem space insufficiently studied. Herein lies an opportunity to further explore these proposed methodologies as well as offer alternative methodologies that consider those areas lacking in the referenced research. To provide a more comprehensive and informative assessment of the potential of any proposed method attempting to address ADS-B vulnerabilities, future research must include:

a) Real world testing, additional to simulation.
b) Evaluation against all types of malicious spoofing attacks, jamming, and interception
c) Specifics of algorithms and data structures.
d) Consideration of the impact of noise on method performance where applicable.
e) Consideration of the impact of multipath propagation on method performance where applicable.
f) Consideration of the impact of different signal strengths on method performance where applicable.
g) Clear definitions of what constitutes spoofing, jamming, and interception attacks.
h) Discussion of the trade-offs between accuracy and false alarm rate where applicable.
i) Discussion of the scalability of proposed method.
j) Discussion of environmental conditions (weather) effect on method performance where applicable.

TITLE	Ref.	APPROACH	CONCLUSIONS	LIMITATIONS
Actual TDoA-based augmentation system for enhancing cybersecurity in ADS-B	[2]	Utilize actual Time Differences of Arrival (TDoA) verses traditional theoretical TDoA	Able to detect malicious ADS-B messages with a high degree of accuracy and reduce computational complexity of verifying ADS-B messages	1. simulation only, non-real world 2. evaluated against only one type of malicious attack 3. does not provide specifics of algorithms and data structures
Physical layer protection for ADS-B against spoofing and jamming	[3]	Method uses physical layer signal analysis to verify the authenticity of ADS-B messages	The proposed method is effective against spoofing and jamming attacks	1. simulation only, non-real world 2. evaluated against only one type of malicious spoofing and jamming attack 3. does not provide specifics of algorithms and data structures 4. does not consider the impact of noise on the performance of the proposed method 5. does not consider the impact of multipath propagation on the performance of the proposed method 6. does not consider the impact of different signal strengths on the performance of the proposed method
ADS-B spoofing attack detection method based on LSTM	[4]	Uses a long short-term memory (LSTM) network, trained on a dataset of simulated ADS-B messages (legitimate and spoofed messages). The LSTM classifies new messages as either legitimate or spoofed.	The proposed method is effective against spoofing attacks	1. simulation only, non-real world 2. evaluated against only one type of malicious spoofing attack 3. does not provide specifics of algorithms and data structures 4. does not consider the impact of noise on the performance of the proposed method 5. does not consider the impact of multipath propagation on the performance of the proposed method 6. does not consider the impact of different signal strengths on the performance of the proposed method, 7. does not provide a clear definition of what constitutes a "spoofing attack". 8. Does not discuss the trade-offs between accuracy and false alarm rate, 9. Does not discuss scalability of proposed method
Detecting GNSS spoofing of ADS-B equipped aircraft using INS	[5]	Method uses the inertial navigation system (INS) to generate a reference trajectory for the aircraft, and then compares this trajectory to the trajectory obtained from the GNSS signal. If the two trajectories do not match, then the system can conclude that the GNSS signal is being spoofed.	The proposed method is effective at detecting GNSS spoofing attacks	1. simulation only, non-real world, 2. evaluated against only one type of malicious spoofing attack, 3. specific parameters of the INS, 4. does not consider the impact of noise on the performance of the proposed method, 5. does not consider the impact of multipath propagation on the performance of the proposed method, 6. does not consider the impact of different signal strengths on the performance of the proposed method, 7. does not provide a clear definition of what constitutes a "spoofing attack". 8. Does not discuss the trade-offs between accuracy and false alarm rate, 9. Does not discuss scalability of proposed method, 10. Does not consider the impact of environmental factors, such as turbulence, on the performance of the proposed method. This is an important consideration, as environmental factors can degrade the performance of both the INS and the GNSS signal.
Physical layer protection for ADS-B against spoofing and jamming	[6]	Proposed method uses physical layer signal analysis to verify the authenticity of ADS-B messages	The proposed method is effective against spoofing and jamming attacks	1. simulation only, non-real world 2. evaluated against only one type of malicious spoofing attack 3. does not provide specifics of algorithms and data structures 4. does not consider the impact of noise on the performance of the proposed method 5. does not consider the impact of multipath propagation on the performance of the proposed method 6. does not consider the impact of different signal strengths on the performance of the proposed method, 7. does not provide a clear definition of what constitutes a "spoofing attack". 8. Does not discuss the trade-offs between accuracy and false alarm rate, 9. Does not discuss scalability of proposed method
Detecting ADS-B Spoofing Attacks using Deep Neural Networks	[10]	The Deep Neural Network (DNN) is trained on a dataset of simulated ADS-B messages, including both legitimate and spoofed messages. The network is then used to classify new messages as either legitimate or spoofed	The proposed method is effective against spoofing attacks	1. simulation only, non-real world 2. evaluated against only one type of malicious spoofing attack 3. does not provide specifics of implementation such as specifics of the DNN, 4. does not consider the impact of noise on the performance of the proposed method 5. does not consider the impact of multipath propagation on the performance of the proposed method 6. does not consider the impact of different signal strengths on the performance of the proposed method, 7. does not provide a clear definition of what constitutes a "spoofing attack". 8. Does not discuss the trade-offs between accuracy and false alarm rate, 9. Does not discuss scalability of proposed method
ADS-B within a Multi-aircraft Simulation for Distributed Air-Ground Traffic Management	[12]	The study considers a scenario in which aircraft are equipped with ADS-B and communicate with ground stations. The ground stations then use this information to track the aircraft and provide traffic information to the pilots	ADS-B can be used to improve the efficiency and safety of air traffic management	1. The paper consider only one scenario, 2. did not consider the impact of noise on ADS-B performance, 3. did not consider multipath propagation on ADS-B performance, 4. Did not consider a wider range of scenarios, including different traffic densities and weather conditions, 5. Did not provide sufficient details about the implementation of the simulation study, such as the specific parameters of the ADS-B system, 6. Does not consider the impact of spoofing attacks on ADS-B, 7. Does not consider the scalability of ADS-B for real-world deployment

Table 1 Select Research Review Limitations

The lack of authentication, encryption, and integrity protection of the ADS-B protocol make it vulnerable to several attacks, including spoofing, jamming, and data corruption. Enhancement of the ADS-B protocol with security features, such as authentication, encryption, and integrity protection will work to de-risk the protocols use as it becomes increasingly relied upon with the advent of AAM. However, ensuring a more robust protocol requires research into the universe of potential attacks or, at a minimum, the population of likely attacks. Any suggested security enhancements must be sufficiently detailed to warrant consideration of implementation. Further, the potential impact of the vulnerabilities, not just on the ADS-B protocol but on the safety of air traffic i.e., the system, must be addressed. In so doing, confidence in recommendations to adjust or alter the ADS-B protocol is established, ensuring community acceptance, industry adoption, and widespread deployment.

5. Relevant internal expertise and capabilities

ADS-B is a secondary surveillance radar system used for ATC. It is recognized by the FAA and industry as an important enabler for future trajectory-based air traffic management [38]. NASA's involvement in researching air traffic management dates back almost a quarter of a century, exploring how weather and congestion disruptions affect the NAS. At NASA Ames and Langley Centers, researchers explore technologies, operations, and methodologies toward ensuring the NextGen environment is safe, efficient, and reliable. NASA's research in this field is extensive. In the research paper, *Evaluation of the Terminal Sequencing and Spacing System for Performance-Based Navigation Arrivals*, Jane Thipphavong et al., evaluated the performance of the Terminal Sequencing and Spacing (TSS) system in human-in-the-loop (HITL) simulations. The TSS system is a suite of advanced arrival management technologies that combines time-based scheduling and controller precision spacing tools. The goal of the TSS system is to enable Performance-Based Navigation (PBN) arrivals, while maintaining high throughput rates and reducing controller workload [39]. Commencing in 2017, and in collaboration with the FAA and Airlines, NASA showcased air traffic management tools through Airspace Development Program-2 (ATD-2). NASA has helped to transition the country's air traffic control network from a limited ground-based system of radar sites to an expanded space-based system of satellites, helping to move the ever-increasing volume of American air traffic in and out of the nation's airports more quickly and safely [40]. Most recently, ARMD established the AAM Mission Integration Office and the AAM Research Institute to coordinate and communicate the AAM ecosystem and to forge collaborative opportunities with industry and partners [41]. The AAM mission is a vision to help emerging aviation markets to safely develop an air transportation system that moves people and cargo between places previously not served or underserved by aviation using revolutionary new aircraft [42]. With the advent of AAM, the NAS will grow increasingly complex. Compounding congestion of the NAS will be UAS. While the FAA has yet to determine the use of ADS-B relative to UAS - ADS-B is a Part 91 regulation, and most small UAS or drones operate under Part 107, some type of remote identification may be required but it is uncertain what the requirements for such a system are or even how the system would work. Here again, NASA, in collaboration with the FAA, other governmental agencies, and industry partners, have devised a framework to enable the autonomous operation of UAS at low altitudes in airspace where FAA air traffic services are not provided. The framework is called Unmanned Aircraft System Traffic Management (UTM). UTM is a "traffic management" ecosystem for uncontrolled operations that is separate from, but complementary to, the FAA's ATM system. UTM development will ultimately identify services, roles and responsibilities, information architecture, data exchange protocols, software functions, infrastructure, and performance requirements for enabling the management of low-altitude uncontrolled drone operations.

IV. IDENTIFIED SOLUTION PATH AND APPROACH

Section III.A.4, *Assessment of Current Efforts* and Table 1 illustrate the limitations of current ADS-B vulnerabilities research. This examination reveals an opportunity to advance the reviewed research toward more fully addressing ADS-B vulnerabilities in non-simulated environments as well as addressing other specified research limitations. Research on this topic to date seemingly has had a narrow focus and while the methods explored have yielded positive results in simulated environments toward mitigating ADS-B vulnerabilities - perhaps a larger opportunity is being missed? Expanding on existing research is an obvious solution path that could be advanced by the original authors, industry, and the FAA. Given the lapse in time since this research was published, it is uncertain if the methods advanced are viewed as capable of addressing future ADS-B requirements for an increasingly operationally complex, congested, and autonomous NAS. Securing ADS-B against malicious attacks, while laudable and necessary, enhances reliance on ADS-B. However, it does not expand ADS-B capabilities. Enhanced capabilities of ADS-B may be necessary as AAM takes hold and continues its evolution. In his paper, *Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy,* NASA Computer Scientist, Ronald J. Reisman lays out a compelling argument for the adoption of blockchain technology as a solution to ADS-B vulnerabilities and to ensure AAMs scalability. As then announced on NASAs website, the paper describes a new infrastructure that would allow for the management of security, privacy, and authentication of information for air traffic services in the United States. On January 14, 2019, CryptoCoin.News published an article elaborating on the announcement, *"NASA's initiative proposes to use an encryption method via blockchain and Hyperledger Fabric for the ADS-B information. The document further describes how the platform will be able to adapt to air traffic, thanks to its previous implementation in business transactions"* [43].

A. AAM Market

According to Future Business Insights, the current AAM market, which is largely limited to drones for photography, recreation, and limited package delivery, is around US$8.1 billion [44]. Deloitte expects the AAM market for passenger and cargo mobility in the United States to reach approximately US$115 billion by 2035. This is equivalent to 30% of the US commercial aerospace market and 0.5% of the country's Gross Domestic Product (GDP) in 2019 [45]. More recently, custom market insights published a report forecasting the AAM market valuation at US$68 billion by 2032, at a Compound Annual Growth Rate (CAGR) of 35%, with the Asia Pacific market being the fastest growing market and Europe the largest AAM market [46]. While forecasts vary, they indicate an undeniable growth trend for AAM. As AAM scales, dependence on ADS-B will grow and with it, malicious attacks. Mitigation of ADS-B vulnerabilities leads to trust – trust in aircraft position (location). Once firmly established, trust in location enables Sense-and-Avoid (SAA) and BVLOS operations which will naturally evolve into ubiquitous independent autonomous operations.

B. Proof of Location Consensus Network

Proof of Location Consensus Network (PLCN) is a Blockchain technology-based concept envisioned to mitigate ADS-B vulnerabilities and extend ADS-B capabilities to enable SAA, BVLOS, and independent autonomous operations. Through the tokenization of validated ADS-B data, ADS-B vulnerabilities are mitigated thus ensuring confidence in aircraft positioning. Once established, ADS-B data tokens are exchanged throughout the network among cooperating aircraft and the larger system i.e., ground stations, ATC. The blockchain network functions as a digital twin of the NAS, enabled via validated ADS-B data. However, to determine this concept's capabilities and limitations, research is required relative to the Minimum Aviation Safety Performance Standards (MASPS) RTCA/DO-242a and more specifically, end-to-end performance verification. The network upon which these validated ADS-B data are tokenized and exchanged (transactions) will necessarily be a permissioned network, affording an additional security layer, preventing unauthorized access to sensitive data unavailable to the public, and accessible only to authorized participants.

C. Key factors and drivers to be considered

Blockchain technology is immutable. Verified data added to a block cannot be altered. Once a transaction is made on a blockchain, the transaction data is stored in a new block, which is then added to the blockchain system. Prior to this process occurring, the information contained in the block must be verified by the network which is made possible by the creation of a hash. Hash functions are used to store and retrieve data from tables and in cryptography to keep information secure. The singular purpose of the hash is to identify data stored in the block and is created when several high-computational computers (nodes) come together to solve complex mathematical problems. For PLCN, an immutable record of validated ADS-B data is secured throughout the flight operation. The ADS-B token is created at the point of validation. Figure 2 illustrates how the hash function turns a random input of data (keys) into a string of bytes with a fixed length and structure (hash value). Hash functions are commonly used data structures in computing systems for tasks such as checking the integrity of messages and authenticating information.

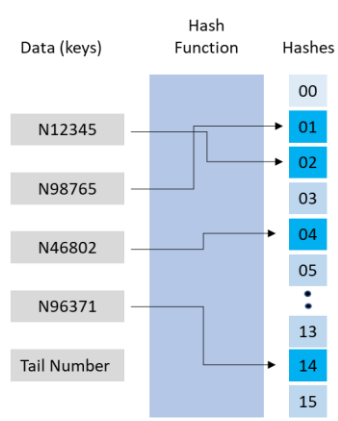


Fig. 2 Hash Map

For a blockchain, tokenization focuses on transforming a real-world asset into a digital token. For PLCN, the real-world asset is validated ADS-B position data. Cryptographic tokens operate on a blockchain, which acts as a medium for the creation and execution of Decentralized

Applications (dApps) and smart contracts. The tokens are used to facilitate transactions on the blockchain. For PLCN, the transaction the ADS-B token is meant to facilitate is the safe (trusted) transit of air space in relation to other conforming aircraft. In a sense, the ADS-B token is 'purchasing' unoccupied airspace along its trajectory or routing, analogous to an aircraft 'owning' the runway once cleared to land by ATC.

For ADS-B, data tokenization and transmission within a blockchain network, energy requirements, and network performance are essential factors requiring research. ADS-B Type Code (TC) broadcast rates are the driving consideration relative to any proposed ADS-B vulnerability mitigation methodology. Additionally, imposing more time onto existing broadcast rates by way of added process, i.e., tokenization, processing time, etc., may adversely affect systemwide safety and therefore systemwide safety must also be considered.

1. Tokenization

Two forms of tokenization are reviewed, data tokenization or non-blockchain tokenization, and blockchain tokenization. Tokenization outside of a blockchain network, non-blockchain tokenization is the process of transforming meaningful data into a random string of letters, numbers, and characters as a security devise to mask sensitive data, whereas blockchain tokenization is the process of transforming a real-world asset i.e., trusted location into a digital token.

2. Non-blockchain tokenization

With non-blockchain tokenization, data format is maintained without sacrificing any strength of security. Non-blockchain tokenization does not use a cryptographic technique to transform sensitive information into ciphertext. Instead of a key or algorithm, non-blockchain tokenization may use a token vault database that stores the relationship between the token and the sensitive value [47]. However, token vaults are high risk targets and while the original data may be encrypted as an additional security layer, centralized pooling of data presents an unnecessary vulnerability. Alternatively, vaultless tokenization does not maintain a database, but instead uses secure ISO 13491-1 cryptographic devices. Secure cryptographic devices use standards-based algorithms to convert sensitive data into non-sensitive data or to generate tokens. With no need to access a database, vaultless tokenization offers reduced latency and increased responsiveness. With no token vault to back up, vaultless tokenization offers increased availability and disaster recovery. With vaultless tokenization, complexity and costs are reduced as there is no need for database licensing, hardware, storage, or maintenance [48]. Tokenized data can be stored in the same size and format as the original data. Tokenization offers a higher level of security if the tokenization system is logically isolated and segmented from data processing systems and applications that process or store the sensitive data replaced by tokens [49]. Non-blockchain tokenization of ADS-B data to mitigate ADS-B vulnerabilities, may offer an efficient and expedited alternative to other solution pathways.

3. Blockchain tokenization

Blockchain tokenization is the process of transforming the value of a real-world asset digitally, to one that resides on the blockchain. Both tangible e.g., gold, and intangible assets e.g., voting rights, can be tokenized, becoming a digital representation of the real-world asset. Tokenization historically has been oriented toward asset commercialization i.e., crypto currency. Typically, the purpose of a token within a dApp or a blockchain network is to incentivize a set of actions that lead to desired outcomes. A dApp token coordinates activity for applications running on top of blockchains that provide services such as trading and lending, data storage, and publishing blogs [50]. The type of token model to use is in part driven by the envisioned outcomes of the blockchain. Tokens can be inflationary, deflationary, or both where one token is used as security to raise funds, and another is used for utility inside the network. Inflationary tokens are continuously produced over time with no maximum supply or capped limit of tokens that can be created. In a deflationary token model, there exists a maximum supply the token is capped at e.g., Bitcoin (BTC) is capped at 21 million. Importantly, not all crypto tokens are currency. Cryptocurrencies are digital representations of value designed to facilitate transactions utilizing blockchain technology. Cryptocurrencies are digital currencies that use encryption techniques to regulate the generation of units of currency and verify the transfer of funds. Tokens are units of value issued by a company or organization that are often used to raise funds for a specific project or purpose. Cryptocurrencies are decentralized and operate independently of a central bank, while tokens are created and managed by a central authority. The process of creating new tokens is called "minting" and it can be done in various ways depending on the token's design. For example, some tokens are designed to be minted continuously over time to incentivize certain behaviors or to reward users for participating in the network. Table 2 provides an outline of the structure and classification of the various token types.

TOKEN TYPE	**DESCRIPTION**
Layer 1	Native to a particular blockchain and are used to power all of its services e.g., BNB, ETH
Layer 2	Utilized in the case of decentralized applications in a specific network e.g., MATIC, ARB
Security	Security tokens or investment contracts, must meet several conditions for the same and are subjected to securities and regulations. Represents an ownership stake in an asset, typically a company, and entitles its holder to a share of profits in the asset. Represents an ownership stake in an asset, typically a company, and entitles its holder to a share of profits in the asset.
Utility	Issued through an initial coin offering (ICO), useful for financing a network e.g., ETH, LTC
CLASSIFICATION	**DESCRIPTION**
Fungible	These tokens are recognized for having the same value as well as replication facility, e.g., ETH
Non-fungible	Non-Fungible Token (NFT) do not share the same value and therefore are unique.

Source: lithtoken.io

Table 2 Structure and Classification of Tokens

PLCN may benefit from an inflationary token model wherein validated ADS-B data is used as the asset and the token, the store of ADS-B value. However, future proofing of the PLCN may require a dual token model wherein the opportunity for a cryptocurrency is preserved until needed. Decarbonization of the aviation industry by 2050 warrants a review of blockchain technology relative to aircraft operations. The Airport and Airway Trust Fund (AATF) is the primary source of funding for the FAA and receives revenues principally from a variety of excise taxes paid by users of the NAS. This includes fuel taxes paid by commercial airline passengers and general aviation users. As the industry moves toward alternative means of powering the fleet, general aviation in the short- to medium-range and commercial more toward the long-range planning horizon, it will be necessary to replace "fuel" taxes with an alternative means of revenue generation. Table 3 provides an outline of aviation taxes and fees for the calendar year 2023. Highlighted in red are the taxes associated with hydrocarbon-based fuel.

Tax or Fee	Rate
Passenger ticket tax (on domestic ticket purchases and frequent flyer awards)	7.50%
Flight segment tax (domestic, indexed annually to Consumer Price Index)	$4.80
Cargo waybill tax	6.25%
Frequent flyer tax	7.50%
General aviation gasoline	*19.3 cents/gallon*
General aviation jet fuel (kerosene)	*21.8 cents/gallon*
Commercial jet fuel (kerosene)	*4.3 cents/gallon*
International departures/arrivals tax (indexed annually to Consumer Price index)	$21.10
(prorated Alaska/Hawaii to/from mainland United States	(Alaska/Hawaii = $10.60)
Fractional ownership surtax on general aviation jet fuel	*14.1 cents/gallon*

Source: *FAA*

Table 3: Aviation Taxes and Fees

As the industry moves away from a NAS funded from various taxation schema partly centered around hydrocarbons, research is needed to determine how the government will replace this source of revenue with a more sustainable and environmentally acceptable one. R. Walsh, et al., *Assessing the Electrification of Aviation's Impact on The Airport and Airway Trust Fund* elaborates on electric aviation's potential impact on the AATF, offering a path forward for government and industry.

4. PLCN Energy Requirements

It is uncertain what the power requirements will be for the PLCN concept. Research is required to determine power usage and impact relative to an aircraft's ADS-B system. The design of the ADS-B transponder is such that it accumulates energy from the input at relative lower power, to burst out at once on the output at high power [51]. The transmission of an ADS-B extended squitter has a duration of 120 microseconds. Since the modulation is pulse-position modulation (PPM) – where a single pulse is encoded by its time shift, the transmitter only transmits for 58 microseconds per message [52]. If the rated maximum power emitted while transmitting (TX) power is 250W, a single ADS-B message costs approximately 0.015 J (assumes 100% efficiency). The maximum squitter rate for ADS-B is 6.2 messages per second, equating to an average of approximately 0.1 Watt of transmitted energy. Other systems hosted by the transponder (Mode S and TCAS) can produce ten times more messages each. Modes A and C use much fewer pulses but can have very high reply rates. This brings the average total transmitted power to over 2 W for congested airspace [53]. While the blockchain network's power consumption is anticipated to grow with scale, it is uncertain the energy requirements of the processes associated with tokenization as previously described.

5. Network Performance

Centralized blockchain networks are faster and more efficient than decentralized networks, but they are also more vulnerable to attack. Decentralized blockchain networks are slower but more secure, as they have comparatively fewer chances of being compromised. ADS-B broadcast rate requirements indicate the necessity for a network capable of managing high operational density with speed and efficiency. As indicated in Table 4, ADS-B message framework is comprised of six groupings. Focus is given to Type Code (TC) broadcast rates in

Table 5 illustrating the acceptable broadcast rates for each TC. Radars can take anywhere from 5 to 12 seconds to update an aircraft's position, ADS-B equipment provides ATC with updated aircraft information almost every second. Safety is enhanced by making aircraft visible in near real time to ATC. Mitigating ADS-B vulnerabilities must consider implications to broadcast rates and the corresponding effect on systemwide safety.

nBits*	Bits	Abbreviation	Name
5	1 - 5	DF	Downlink Format (17)
3	6 - 8	CA	Capability (additional identifier)
24	9 - 32	ICAO	ICAO aircraft address
56	33 - 88	DATA	Data
	[33 - 37]	[TC]	Type code
24	89 - 112	PI	Partity/Interrogator ID

* nBits, or Target Threshold is the threshold below which a block header hash must be in order for the block to valid, and nBits is the encoded form of the target threshold as it appears in the block header.

<u>Source</u>: *ADS-B Decoding Guide Release 0.3*

Table 4: ADS-B Message Framework

TC	Content	Broadcast Rate (seconds)	
		Airborne	Surface
1 - 4	Aircraft identification (ID and Type)	5.0	10.0
5 - 8	Surface position*	0.5	5.0
9 - 18	Airborne position (w/barrometric altitude)	0.5	na
19	Airborne velocities	0.5	na
20 - 22	Airborne position (w/GNSS height)	0.5	na
28	Aircraft status e.g., emergency/priority	1.0	
31	Aircraft operational status	1.7	

* ADS-B broadcast rate listed is while in motion and when stationary in columns Airborne and Surface respectively

<u>Source</u>: *ADS-B Decoding Guide Release 0.3 modified*

Table 5: ADS-B Type Code Content and Nominal Broadcast Rates

6. Network Scalability

An important aspect of a network's ability to scale is the transaction processing time. The transaction processing time equals time necessary to update the state database. The scalability of the PLCN will be determined by the speed at which ADS-B data validation and token exchanges (transactions) are conducted. These metrics will determine the PLCNs scalability and thereby, future capability. A blockchain network requires reliable metrics to measure and quantify performance. Transactions per second (TPS), or throughput rate is a computer software and hardware measurement that represents the number of transactions completed in one second by an information system. While TPS should be considered, other network performance metrics should be assessed relative to future acceptable performance. Table 6 provides the logical grouping of key metrics that may be used to assess network performance.

Metrics Group	Metrics
Blockchain node	number of produced blocks, number of processed transactions, processing time, finality time
Peer-to-peer subsystem	number of hit/miss requests, number of active peers, volume and structure of peer-to-peer traffic
System node	CPU, memory, storage, network

Source: *Hackernoon*

Table 6: Key Metrics to Measure Blockchain Network Performance

7. Systemwide Safety

Blockchain technology can be transformative for aviation operations if strategically deployed. As envisioned, PLCN seeks to first mitigate ADS-B vulnerabilities and secondly, expand its capabilities to enable autonomous control. Therefore, it is necessary to assess PLCN against the requirements of the future NAS, namely, NextGen, Info-Centric NAS, defined as a collaborative environment utilizing service-oriented architecture for tailored mission services, e.g., Machine Learning, Internet of Things, and Sky for All, defined as a highly automated for complexity and scalability and oriented toward dynamic adaptation e.g., digital mesh, Artificial Intelligence, Internet of Things. All goals must be assessed in tandem for the intrinsic value of blockchain technology to be evidenced. To do so requires research into the affects blockchain technology will have on aviation operations and how they may impact systemwide safety.

D. Limiting factors

ADS-B is a real-time protocol requiring messages to be processed quickly, making it difficult to implement some security features, such as message encryption, which can add latency to the protocol. Blockchain technology has yet to be deployed in an aviation operational environment and as such, there are assumed many unknowns.

1. Performance

Blockchain networks can be slow and inefficient due to the high computational requirements needed to validate transactions. As the network grows relative to the number of users, transactions, and applications, performance is impacted. However, consumer demand for high performing networks is driving the technology toward more efficient means of finalizing transactions at scale. Networks are increasingly more efficient and capable, which in turn is driving more demand. The consensus mechanism used by a blockchain network is a critical factor in determining its performance. When a transaction is to be validated it must be broadcast to all network nodes and their response must then be collated for majority-based consensus. The latency of the network is measured in milliseconds, commonly referred to as the ping rate. The lower the ping rate the better the performance. A ping rate of less than 100ms is considered acceptable but for optimal performance, latency in the range of 30-40ms is desirable [54].

2. Energy consumption

Blockchain has garnered much attention regarding energy consumption. Most of which centers around mining activities relative to cryptocurrencies. According to the University of Cambridge's bitcoin electricity consumption index, bitcoin miners are expected to consume roughly 130 Terawatt-hours of energy (TWh), which is roughly 0.6% of global electricity consumption [55]. The vast majority of Bitcoin's energy consumption happens during the mining process. Once coins have been issued, the energy required to validate transactions is minimal [56]. The high demand for energy arises due to an algorithm called Proof of Work (PoW). Designed as a proving mechanism to secure public blockchains, such as Bitcoin, it incentivizes blockchain participants (miners) to spend large amounts of electricity in exchange for Bitcoin [57]. Alternatively, permissioned blockchain networks utilize more energy-efficient consensus mechanisms like Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA), or Proof of Stake (PoS). These mechanisms don't rely on computational power for validation, but on predetermined validators (a blockchain network that is responsible for verifying transactions on the network), which consume less energy [58]. An analysis of current scientific knowledge shows that the energy consumption of blockchain technology is not as high as it is often claimed to be [59]. Blockchain-based systems are often more automated than traditional systems, which can further reduce costs. The increased efficiency of blockchain can also help reduce energy consumption and save businesses money [60].

E. Means of assessing feasibility of solution

Once the determination has been reached to pursue the PLCN concept, refinement of the objective and scope for its design must precede development of a proof of concept. Once accomplished, computer simulation is needed to test PLCN's capabilities and limitations relative to the MASPS and more specifically, end-to-end performance verification.

V. RECOMMENDATIONS

PLCN is a concept methodology premised on blockchain tokenization of ADS-B data. It is theorized that blockchain tokenization affords a higher level of security, serving to protect against ADS-B vulnerabilities, thereby instantiating locational trust, de-risking ADS-B, and enabling AAM to scale. Future NAS readiness is factored-in to PLCN through the establishment of a blockchain network specifically adapted for future aviation operations and aligned with the requirements of NextGen, Info-Centric NAS, Sky for All and UTM. Table 7 provides recommendations and associated resources.

PHASE	RECOMMENDATION	DURATION (months)	RESOURCES	
			NASA	OTHER
1	Circulate PLCN concept document among community of interest (CoI) to gage desirability and interest in collaborating on the construction and testing of the PLCN proof of concept	1	CAS Leadership	CoI
	Refine requirements develop key metrics by which to measure concept viability	1 - 2	CAS PI, CS01, CS(int), SimLabs ATM	CoI PI, CoI others
	Construct PLCN proof of concept	6	CAS PI, CS01, CS(int), SimLabs ATM	CoI PI, CoI others
2	Develop operational uses case series to measure capability i.e., end-to-end performance	1	CAS PI, CS01, CS(int), SimLabs ATM	CoI PI, CoI others
	Construct and run computer-based simulation model based on operational use cases to determine feasibility of concept as measured against MASPS	3	CAS PI, CS01, CS(int), SimLabs ATM	CoI PI, CoI others
	Analyze results against performance criteria	1	CAS PI	CoI PI
3	Construct and run physical simulation(s) to verify computer simulation results and to advance understanding of concept performance in real-world operational environment	6	CAS PI, CS01, CS(int), UAS Test Range	CoI PI, CoI others
	Analyze results against performance criteria	1	CAS PI	CoI PI

Table 7 PLCN Project Recommendations and Resources

As identified in Table 7, resident NASA expertise from CAS, Computer Science, combined with personnel from NASA SimLabs Air Traffic Management Laboratory round out human and physical resources from NASA. Additional resources from the Community of Interest (CoI) are anticipated, however the extent to which the CoI choose to participate is unknown. The schedule is an approximation pending positive consensus from the CoI and selection of identified personnel for this project.

A. Secondary Recommendation

Alternatively, should the PLCN concept prove unfavorable, Table 8 lists alternative solution pathways with corresponding proposed actions for consideration. Reviewing the problem space of ADS-B vulnerabilities in consideration of the PLCN methodology, additional solution pathways were revealed that may be equally impactful toward resolving ADS-B vulnerabilities.

Solution Pathway	Proposed Action
Identified ADS-B Research	Re-asses ADS-B research listed in Table 1 against identified limitations and relative to current and future NAS needs. Rank order and assess further research needs to determine viability of proposed solution. Test solution through additional computer simulation regarding capabilities and limitations relative to the MASPS and more specifically, end-to-end performance verification and, where warranted, physical simulation.
Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy	Should a blockchain solution to mitigate ADS-B vulnerabilities be given consideration, this NASA research deserves renewed focus. Assess further research needs to determine feasibility of proposed methodology. Test methodology through computer simulation regarding capabilities and limitations relative to the MASPS and more specifically, end-to-end performance verification, advancing to physical simulation if warranted.
Non-blockchain tokenization	Determination of desirability, viability, and feasibility as a potential low-technology solution to mitigate ADS-B vulnerabilities. Subsequent to DVF determination, a more in-depth concept feasibility study with associated computer simulation to determine technical feasibility regarding capabilities and limitations relative to the MASPS and more specifically, end-to-end performance verification to determine the viability of this proposed methodology. Should this methodology prove feasible, progress to physical simulation.

Table 8 Alternative Solution Pathways

VI. CONCLUSION

Blockchain technology carries with it several attributes beneficial for AAM and UAS. Advantages include immutability, traceability, security, privacy, and interoperability. It is envisioned that, when applied to aviation operations, blockchain technology can resolve barriers to scale revolving around secure transfer of data and increasingly autonomous operations. As illustrated in Appendix A, PLCN seeks to mitigate ADS-B vulnerabilities of data spoofing, jamming, and interception. Elimination of these vulnerabilities will decrease operational risk, enhance ADS-B reliability, and enable increasingly autonomous and ubiquitous operations. PLCN concept seeks to address three additional system-level problem areas:

1. <u>Need for trust across a decentralized operational environment</u> - Shift to non-governmental distributed information technologies and reliance upon information received from others requiring mechanisms to enable trust of information products.
2. <u>Autonomous flight operations will drive the need to ensure information integrity</u> - Increased reliance on automation for flight operational decision-making and actions moving toward increasingly autonomous flight with reduced direct human oversight and situation awareness thereby increasing dependence on information integrity to ensure acceptable outcomes.
3. <u>Operations concept migration from centralized to decentralized</u> - Decentralization of information and decision making away from "government" (trusted source) toward commercial third-party provider will require a federated operational concept.

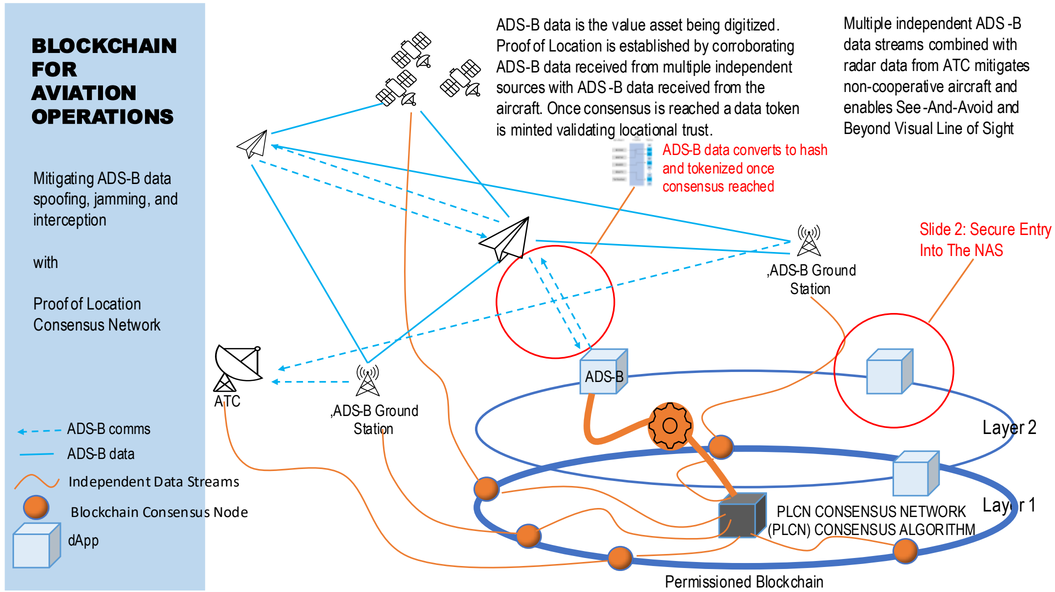
REFERENCES

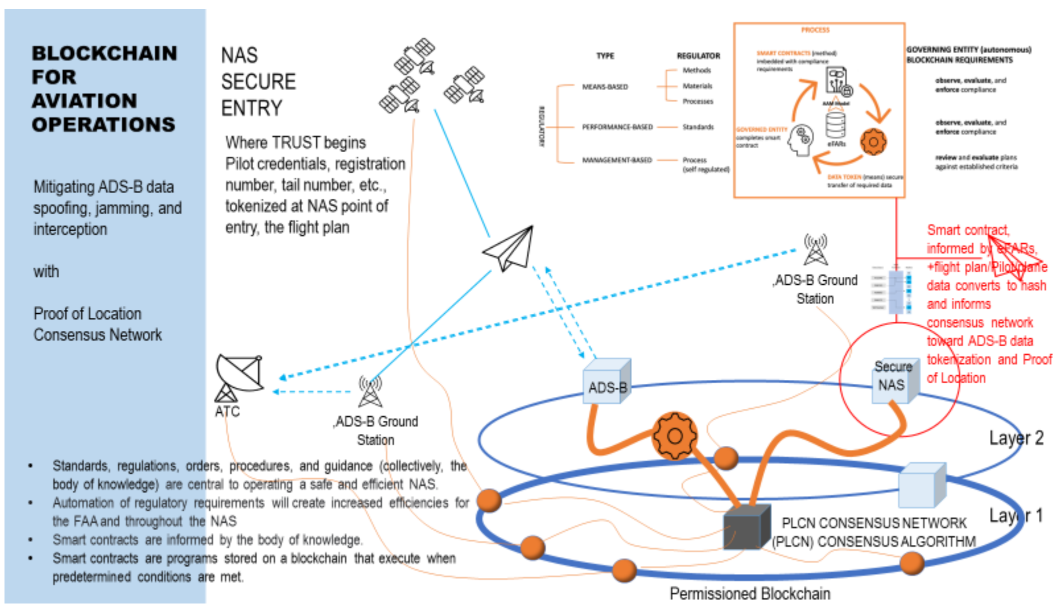
[1] Thurber M. ADS-B is insecure and easily spoofed, say hackers. Aviation International News. 2012;44(9):1-2. Accessed March 6, 2023.
[2] Elmarady AA, Rahouma K. Actual TDoA-based augmentation system for enhancing cybersecurity in ADS-B. Chinese Journal of Aeronautics. 2021;34(2):217-228. doi: 10.1016/j.cja.2020.11.015.
[3] Rudys S, Aleksandravicius J, Aleksiejunas R, Konovaltsev A, Zhu C, Greda L. Physical layer protection for ADS-B against spoofing and jamming. International Journal of Critical Infrastructure Protection. 2022;38:100555. doi: 10.1016/j.ijcip.2021.100555.
[4] Wang J, Zou Y, Ding J. ADS-B spoofing attack detection method based on LSTM. Journal of Wireless Communications and Networks. 2020;160:1-9. doi: 10.1186/s13638-020-01798-5.
[5] Kujur B, Khanafseh S, Pervan B. Detecting GNSS spoofing of ADS-B equipped aircraft using INS. In: 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS). Portland, OR, USA; 2020:548-554. doi: 10.1109/PLANS46316.2020.9117317.
[6] Strohmeier M, Lenders V, Martinovic I. On the security of the Automatic Dependent Surveillance-Broadcast protocol. IEEE Communication Surveys & Tutorials. 2015;17(2):1066-1087. doi: 10.1109/COMST.2014.2383115.
[7] IBM Data and AI Team. AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the difference? IBM.com. 2023. Accessed March 15, 2023.
[8] Ridgeway R. Why is Layered Physical Security Important? HS Security. Accessed March 17, 2023.
[9] Rudys S, Aleksandravicius J, Aleksiejunas R, et al. Physical layer protection for ADS-B against spoofing and jamming. International Journal of Critical Infrastructure Protection. 2022;38:100555.
[10] Ying X, Mazer J, Bernieri G, et al. Detecting ADS-B Spoofing Attacks using Deep Neural Networks. 2019.
[11] Arteaga R. Automatic Dependent Surveillance Broadcast: ADS-B Sense-and-Avoid System. AIAA. June 13-17, 2016.
[12] Barhydt R, Palmer MT, Chung WW, Loveness GW. ADS-B within a Multi-aircraft Simulation for Distributed Air-Ground Traffic Management. IEEE/AIAA 23rd Digital Avionics Systems Conference, Salt Lake City, UT, USA. 2004.
[13] Rymer N, Moore AJ, Young S, Glaab L, Smalling K, Consiglio M. Demonstration of Two Extended Visual Line of Sight Methods for Urban UAV Operations. NASA Langley Research Center, Hampton, VA.
[14] Reisman RJ. Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy. AIAA Science and Technology Forum and Exposition 2019 Session ICC-02, Information and Command and Control Systems San Diego, CA. 2019 Not Presented due to Government shutdown.
[15] NASA Convergent Aeronautics Solutions (CAS) Overview | NASA. Published July 13, 2016. Accessed March 29, 2023.
[16] NASA Core Areas of Expertise: Air Traffic Management. Published September 4, 2022. Accessed March 29, 2023.
[17] NASA About Aeronautics Research Mission Directorate. Published October 15, 2015. Accessed March 29, 2023.

[18] NASA Strategic Implementation Plan. Published November 12, 2015. Accessed March 29, 2023.
[19] Skyline: Making BVLOS Missions A Reality. uAvionix. Accessed April 3, 2023.
[20] Fortune Business Insights. Automatic Dependent Surveillance – Broadcast Market Size. Published January 2022. Accessed April 3, 2023.
[21] Poremba S. Experts Weigh In: Pros and Cons of Machine Learning for AI Security. Security Intelligence. Published May 24, 2021. Accessed April 3, 2023.
[22] Biltgen P. AI/ML: Limitations and Possibilities. Security Intelligence. Published November 24, 2021. Accessed April 3, 2023.
[23] Hechler E, Oberhofer M, Schaeck T. Limitations of AI. In: Deploying AI in the Enterprise; pp.299-312; Apress, Berkeley, CA; doi:10.1007/978-1-4842-6206-1_13.
[24] Biltgen P. AI/ML: Limitations and Possibilities. Security Intelligence. Published November 24, 2021. Accessed April 3, 2023.
[25] Ahmad RW, Salah K, Jayaraman R, Hasan HR, Yaqoob I, Omar M. The Role of Blockchain Technology in Aviation Industry. IEEE Aerospace and Electronic Systems Magazine; vol.36; no.3; pp4-15; doi:10.1109/MAES.2020.3043152.
[26] Future of the Airline Industry 2035 | International Air Transport Association (IATA). Accessed April 5, 2023.
[27] Blockchain in Aviation: Exploring the Fundamentals, Use Cases, and Industry Initiatives | International Air Transport Association (IATA). Accessed April 5, 2023.
[28] EU-funded project SlotMachine to use blockchain technology for more cost-efficient flight slot configuration | Frequentis . Accessed April 5, 2023.
[29] Top Companies in the Blockchain Supply Chain Industry | Emergen Research . Published April 21, 2023; accessed May 4, 2023.
[30] Xiang WN.Working with wicked problems in socio-ecological systems: Awareness, acceptance, and adaptation.Journal of Landscape and Urban Planning; volume110; January2; SN0169-2046; doi:10.1016/j.landurbplan2012.11.006
[31] Lönngren J.Wicked Problems in Engineering Education : Preparing Future Engineers to Work for Sustainability (PhD dissertation); Chalmers tekniska högskola; Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-158222
[32] Appendix A | National Airspace System Overview | FAA.gov. Accessed May10;2023.
[33] NASA About Aeronautics Research Mission Directorate. Published October 15, 2015. Accessed May 10, 2023.
[34] NASA About Aeronautics Research Mission Directorate. Published October 15, 2015. Accessed May 10, 2023.
[35] Request for Information on Advanced Air Mobility, A Notice by the Transportation Department on May 17, 2023.
[36] S.516 – Advanced Air Mobility Coordination and Leadership Act. Became Public Law No: 117-203, October 17, 2022.
[37] FAA Next Generation Air Transportation System (NextGen). Accessed June 2, 2023.
[38] FAA Automatic Dependent Surveillance – Broadcast (ADS-B). Accessed June 2, 2023.
[39] Thipphavong J, O'Neill P, Kelly C. Evaluation of the Terminal Sequencing and Spacing System for Performance-Based Navigation Arrivals. In Proceedings of the 2013 IEEE/AIAA 32nd Digital Avionics Systems Conference (DASC), pp6712503-6712510; doi:10.1109/DASC.2013.6712503.

[40] NASA Air Traffic Operations Lab Answering Big Questions About the Future of Air Travel. Published November 21, 2014. Accessed June 10, 2023.
[41] NASA Advanced Air Mobility Mission Overview. Published January 27, 2021. Accessed June 10, 2023.
[42] NASA Advanced Air Mobility Project. Published July 9, 2021. Accessed June 10, 2023.
[43] NASA Announces Blockchain-Based Platform For Air Traffic Control - CryptoCoin.News. Published January 14, 2019. Accessed June 11, 2023.
[44] Fortune Business Insights, Commercial Drone Market Size. Published May 2023; accessed June 11, 2023.
[45] Deloitte insights, Advanced air mobility | Deloitte Insights. Published January 26, 2021; accessed June 11, 2023.
[46] Custom Market Insights, Global Advanced Air Mobility Market 2023-2032; Published July 2023; accessed August 2, 2023.
[47] Vyas K., Data Security: Tokenization vs Encryption | IT Business Edge; Published July1; accessed August2;2023.
[48] FutureX; The Demise of Vaulted Tokenization? (futurex.com); Published June12; accessed August3;2019.
[49] Kovacs E., Tokenization: Benefits and Challenges for Securing Transaction Data - SecurityWeek; Published November4; accessed August3;2014.
[50] Ehrlich S. What Are DApp Tokens? Forbes. Published March 10, 2023. Accessed August 3, 2023.
[51] Why is the input power of an ADS-B Transponder much lower than its rated transmission output power? Aviation Stack Exchange. Published May 2021. Accessed August 4, 2023.
[52] Pulse-position modulation - Wikipedia. Accessed August 4, 2023.
[53] Why is the input power of an ADS-B Transponder much lower than its rated transmission output power? Aviation Stack Exchange. Published May 2021. Accessed August 4, 2023.
[54] IBM. What is latency? Accessed August 4, 2023.
[55] Bitcoin consumes 'more electricity than Argentina' - BBC News. Published February 10, 2021. Accessed August 4, 2023.
[56] Carter N. How Much Energy Does Bitcoin Actually Consume? Harvard Business Review. Published May 5, 2021. Accessed August 4, 2023.
[57] Blockchains and energy consumption | Provenance. Published May 2, 2019. Accessed August 4, 2023.
[58] Eshghi B. Difference Between Permissioned and Permissionless Blockchain | AIMultiple.com. Published May 2, 2023. Accessed August 4, 2023.
[59] Sedlmeir J, Buhl HU, Fridgen G et al. The Energy Consumption of Blockchain Technology: Beyond Myth; Bus Inf Syst Eng; vol62; pp599-608; doi:10.1007/s12599-020-00656-x.
[60] Timbo R., Blockchain Cloud Computing: Benefits and Examples | Revelo.com; Published March1; accessed August4;2023.

Appendix A


BLOCKCHAIN FOR AVIATION OPERATIONS
Mitigating ADS-B data spoofing, jamming, and interception
with
Proof of Location Consensus Network
ADS-B data is the value asset being digitized. Proof of Location is established by corroborating ADS-B data received from multiple independent sources with ADS-B data received from the aircraft. Once consensus is reached a data token is minted validating locational trust.
Multiple independent ADS-B data streams combined with radar data from ATC mitigates non-cooperative aircraft and enables See-And-Avoid and Beyond Visual Line of Sight
ADS-B data converts to hash and tokenized once consensus reached
Slide 2: Secure Entry Into The NAS
ADS-B Ground Station
ATC
ADS-B Ground Station
ADS-B
Layer 2
Layer 1
PLCN CONSENSUS NETWORK (PLCN) CONSENSUS ALGORITHM
Permissioned Blockchain
ADS-B comms
ADS-B data
Independent Data Streams
Blockchain Consensus Node
dApp


BLOCKCHAIN FOR AVIATION OPERATIONS
Mitigating ADS-B data spoofing, jamming, and interception
with
Proof of Location Consensus Network
NAS SECURE ENTRY
Where TRUST begins
Pilot credentials, registration number, tail number, etc., tokenized at NAS point of entry, the flight plan
Smart contract, informed by eFARs, +flight plan/Pilot/plane data converts to hash and informs consensus network toward ADS-B data tokenization and Proof of Location
ADS-B Ground Station
ATC
ADS-B Ground Station
ADS-B
Secure NAS
Layer 2
Layer 1
PLCN CONSENSUS NETWORK (PLCN) CONSENSUS ALGORITHM
Permissioned Blockchain
Standards, regulations, orders, procedures, and guidance (collectively, the body of knowledge) are central to operating a safe and efficient NAS.
Automation of regulatory requirements will create increased efficiencies for the FAA and throughout the NAS
Smart contracts are informed by the body of knowledge.
Smart contracts are programs stored on a blockchain that execute when predetermined conditions are met.

Appendix B

Glossary

1. *Multilateration*, also known as hyperbolic positioning, is the process of locating an object by accurately computing the time difference of arrival (TDOA) of a signal emitted from the object to three or more receivers.
2. *Peer-to-peer computing* or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent (i.e., having equal potencies) participants in the application.
3. *Smart contract* is a computer program or protocol that runs on a blockchain and executes the terms of an agreement between parties automatically when certain conditions are met. Smart contracts aim to reduce the need for intermediaries, cost, and risk of fraud and exceptions. Smart contracts involve the transfer of digital assets, is trackable, and irreversible. Smart contracts have a high potential to enable streamlining of business-to-business interactions (e.g., invoicing, reconciliation, settlement, and accounting.
4. *Tokenization* is the process of converting physical or non-physical assets into digital tokens on a blockchain network. This allows users to transfer real-world value onto the blockchain and create, exchange, and trade tokens securely and decentralized.
5. *Wicked problems* are problems with many interdependent factors making them seem impossible to solve. Because the factors are often incomplete, in flux, and difficult to define, solving wicked problems requires a deep understanding of the stakeholders involved, and an innovative approach provided by design thinking.
6. *Command, control, and communications* (C3) systems are fundamental to all military operations, delivering the critical information necessary to plan, coordinate, and control forces and operations across the full range of Department of Defense (DoD) missions. Some forms of command and control (C2) are primarily procedural or technical in nature—such as the control of air traffic and air space, the coordination of supporting arms, or the fire control of a weapons system.
7. *Spoofing attacks* may target aircraft and ground systems exploiting ADS-B message interception, jamming or injection. Attacks can be classified into: (i) Aircraft reconnaissance; (ii) Flood denial of ground station or aircraft; (iii) Target ghost injection of ground station or aircraft.
8. *Noise* or frequency noise refers to random fluctuations of the instantaneous frequency of an oscillating signal.
9. *Multipath propagation* results from radio signals reaching the receiving antenna by two or more paths, while a multipath topology results from having multiple paths through a network between a source and a destination node.
10. *Unmanned Aircraft System Traffic Management* (UTM) is a "traffic management" ecosystem for uncontrolled operations that is separate from, but complementary to, the FAA's Air Traffic Management (ATM) system. UTM development will ultimately identify services, roles and responsibilities, information architecture, data exchange protocols, software functions, infrastructure, and performance requirements for enabling the management of low-altitude uncontrolled drone operations.

11. *Sense-and-Avoid* is the ability of Unmanned Aircraft Systems (UAS) to "sense" and "avoid" other aircraft, including airplanes, rotorcraft, gliders, balloons, blimps, and parachutes.
12. *Beyond Visual Line of Sight* (BVLOS), refers to operations where the person or people responsible for operating a drone cannot physically see it during some, or all of its flight.
13. *Permissioned blockchain* is a distributed ledger that is not publicly accessible. A private blockchain providing only users with permission to access it. Users are required to self-identify through certificates or other digital means.
14. *Decentralized application* (dApps) are digital programs that run on a peer-to-peer network or blockchain instead of a single computer or server. dApps are free from the control and interference of a single authority and have no single point of failure. dApps can have various functions and interfaces but they communicate with their corresponding blockchain, which manages the state of all network actors.
15. *Cryptographic techniques* are methods of coding information to make it unintelligible to anyone who does not have the key to decrypt it. Cryptographic techniques are based on mathematical concepts and algorithms that can provide data security, authentication, and confidentiality.
16. *Ciphertext* is a series of randomized letters and numbers. It is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it.
17. *Secure Cryptographic Device* (SCD), according to ISO 13491-1, is defined as a device that provides physically and logically protected cryptographic services and storage. Such devices can be a PIN Entry Device (PED), a smartcard, or a hardware security module (HSM). The HSM is a special “trusted” network computer performing a variety of cryptographic operations: key management, key exchange, encryption, etc.
18. *GPS-Squitter* is a technology for aircraft surveillance in which aircraft broadcast their GPS determined positions to all listeners via the Mode S data link, It can be used to provide aircraft traffic, displays, on the ground for controllers, and in the cockpit for pilots.
19. *Mode S* is a datalink technology that uses discretely addressed interrogations. Mode S equipment includes ground stations with sensors, and transponders aboard aircraft. Mode S equipment has altitude capability and also permits data exchange. The interrogations that ground sensors send planes include the identification information of the target plane.
20. *Traffic Collision Avoidance System* (TCAS) purpose is to minimize the risk of mid-air collisions between aircraft. The ICAO requires all aircraft with a capacity of more than 19 passengers to be fitted with this safety measure. The rule also applies to aircraft with a maximum takeoff weight (MTOW) of more than 5,700 kg.
21. *Mode A* equipment transmits an identifying code only. Mode C equipment enables ATC to see the aircraft altitude or flight level automatically.
22. *Centralized digital network* is a network in which collective data is processed and stored by a single node.
23. *Decentralized digital network* is a network in which multiple nodes store and process data.
24. *Info-Centric NAS* is defined as a collaborative environment utilizing service-oriented architecture for tailored mission services, e.g., Machine Learning, Internet of Things.

25. *Sky for All* is defined as a highly automated for complexity and scalability and oriented toward dynamic adaptation e.g., digital mesh, Artificial Intelligence, Internet of Things.
26. *Total system safety approach* considers the entire aviation industry as a system. All service providers, and their systems for the management of safety, are considered as sub-systems. This allows a State to consider the interactions, and cause and effect, throughout the whole system.
27. *Validator* is a node on a blockchain network that is responsible for verifying transactions on the network. Validator nodes use a set of rules and algorithms to validate transactions and create new blocks. As a result of the consensus mechanism used by the blockchain network, these rules are predetermined.