

A Blockchain Case Study for Urban Air Mobility Operational Intent

Kenneth Freeman¹, Norbert Gillem², Aidan R. Jones³
Nishant Sharma⁴

NASA Ames Research Center, Moffett Field, CA, USA

To realize the potential of Urban Air Mobility (UAM), an assurance of cybersecurity is critical for public acceptance. UAM is a concept that proposes to develop short-range, point-to-point transportation systems in metropolitan areas using vertical takeoff and landing (VTOL) aircraft to overcome increasing surface congestion. The growth in the development of UAM systems, and the associated data exchange and service interactions will be at risk due to numerous types of cybersecurity attacks. The intent of this work is to leverage a permissioned blockchain to simulate secure data exchange and storage for the UAM operational intent use case. In this case study, two vehicle operators are operating in the same airspace. Their intent is to fly vehicles that land at a shared vertiport, securely.

I. Introduction

The next generation of aerial passenger and cargo transportation may leverage the concept of Urban Air Mobility (UAM). UAM is a concept that proposes to develop short-range, point-to-point transportation systems in metropolitan areas using vertical takeoff and landing (VTOL) or short takeoff and landing (STOL) aircraft to overcome increasing surface congestion [1]. The UAM concept leverages a decentralized service-based architecture for airspace solutions, no centralized control by individual, group, or government. Within the environment, UAM operators work collaboratively to manage aerial vehicles in the urban environment. Providers of Services for UAM (PSU), UAM operators, and Supplemental Data Service Providers (SDSP) provide services to support flight operations within the UAM environment. Also, various views of UAM flight information are provided to the public and public safety entities [2]. The Federal Aviation Administration (FAA) can coordinate flight information between the FAA controlled National Airspace System (NAS) and the UAM environments through the FAA-Industry Data Exchange Protocol (FIDXP).

To realize the potential of UAM, an assurance of cybersecurity is critical for public acceptance. Cybersecurity has come to the forefront highlighting the need to protect these networks and systems from cyberattacks. The growth in the development of UAM systems, and the associated data exchange and service interactions will be at risk due to numerous types of cybersecurity attacks. As these threats evolve, the UAM cybersecurity capabilities must adapt to these changes as well [3]. This research focuses on the secure data exchange and storage of this decentralized UAM environment to address these challenges. This research intends to leverage a permissioned blockchain approach to address cybersecurity threats that may impact a UAM environment.

Blockchain technologies can be used for tracking transactions and verifying negotiated agreements between stakeholders in the NAS environment. For example, the record of the submitted flight plan and the approved flight plan could be verified using the Blockchain-based immutable ledger.

¹ Aerospace Engineer, NASA Ames Research Center, Moffett Field, CA 94035, USA.

² Aerospace Engineer, NASA Ames Research Center, Moffett Field, CA 94035, USA.

³ Aerospace Engineer, NASA Ames Research Center, Moffett Field, CA 94035, USA.

⁴ Systems Engineer, Intrinsic Technologies Corporation, Moffett Field, CA 94035, USA.

II. Motivation

A federated enterprise architecture is one which operates collaboratively, where governance is divided between a central authority and constituent units, balancing organizational autonomy with enterprise needs [3]. The role of the central authority is to ensure the well-being of the enterprise, while constituent units have the flexibility to pursue autonomous strategies and independent processes. The UAM airspace system architecture will be federated, with central authority derived largely from the Air Navigation Service Provider (ANSP) (and possibly other entities), and with a distributed constituency of UAM Operators who operate safely and with increasing flexibility as the system evolves.

A UAM Operator is the entity or organization accountable for the overall management and execution of one or more UAM operations. As operators of air taxi services which typically will operate a fleet of UAM aircraft, the UAM Operator is often referred to as the Fleet Operator [4]. Fleet operators will be leveraging a service-based architecture for airspace solutions.

The UAM environment will leverage independent fleet operators utilizing diverse communications and system access approaches. Additionally, there will be independent Provider of Services for UAM (PSU) operators and supplemental data service providers (SDSP) exchanging data between themselves and UAM operators. The PSU is the individual(s) and/or automation responsible for managing the provision of information services associated with airspace operations to the UAM Operator. UAM operators and PSUs use SDSPs to access supporting data including, but not limited to, terrain, obstacle, aerodrome availability, and specialized weather [5].

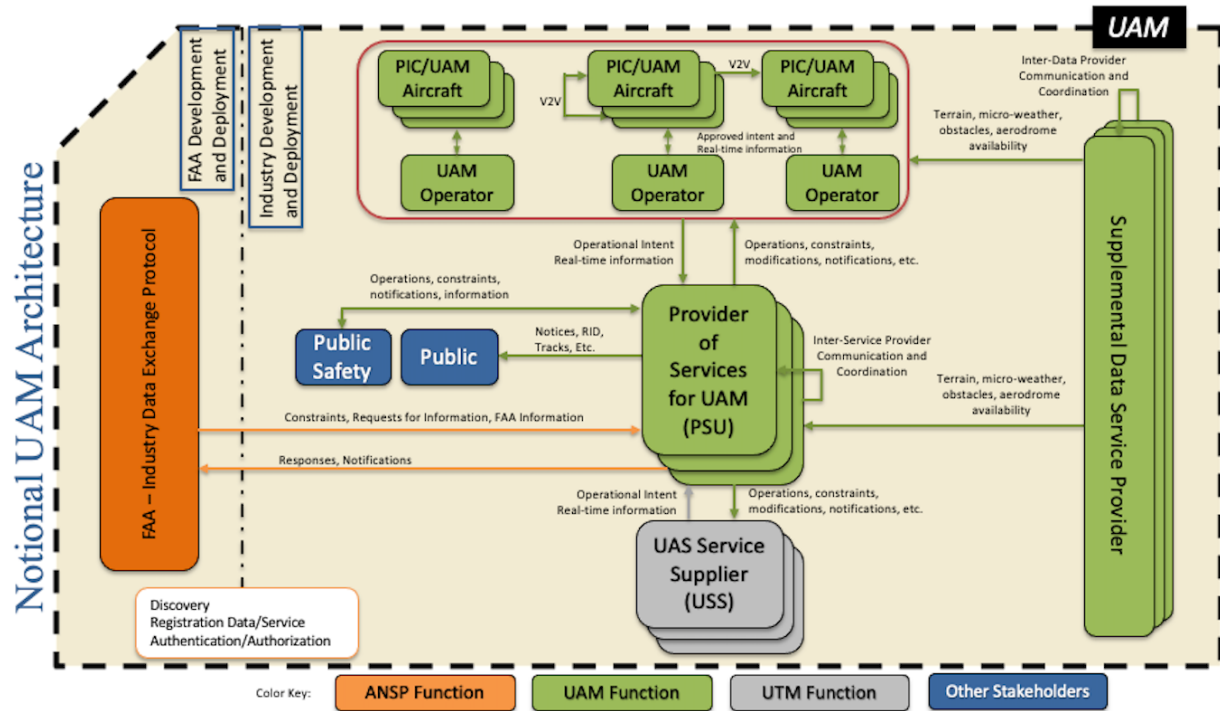


Figure 1 – Notional UAM Architecture

In 2020, the Federal Aviation Administration (FAA) published its version 1 of the UAM Concept of Operations [5] which described the envisioned operational environment that supports the expected growth of flight operations in and around urban areas. Figure 1 shows the notional UAM architecture, from the UAM Concept of Operations, which shows the interaction of the elements of the UAM ecosystem, such as the PSUs, SDSPs and UAM operators. The data exchanges between these entities will need to be secure, to ensure the operational safety of vehicles flying within the UAM ecosystem.

III. Security Risks

The decentralized community of UAM operators, PSU operators and SDSPs will likely operate their services on local or cloud environments that require security. The focus of this work is on the secure data exchange and storage of this decentralized UAM environment. The intent of this work is to leverage a permissioned blockchain to simulate secure data exchange and storage, and to mitigate the following four cybersecurity threats that may impact a UAM environment:

- Man-in-the-middle attacks, leading to data manipulation
- Victims of spear phishing, leading to the interaction with malicious content
- Exploitation of valid accounts, leading to the loss of credentials and system access
- Exploitation of public facing application, leading to corruption of data

Data manipulation can result in the alteration of vital information, leading to erroneous results or decisions. Additionally, malicious content can be used to exploit vulnerabilities in software or systems, allowing attackers to gain unauthorized access to sensitive information. Also, when credentials are stolen or lost, attackers can utilize them to gain unauthorized access to UAM systems. Attackers can steal or modify sensitive data or even install additional malware once they have gained access to the UAM systems.

IV. Blockchain

A blockchain is a distributed system with either a linear structure or a graph-like structure with nodes and links connected without any centralized authoritative nodes or hierarchy. A user or an individual system is represented as a node within the blockchain network. A full node stores the entire blockchain made up of blocks. A publishing node is a full node which has the capability to extend the blockchain by creating and publishing new blocks. A lightweight node does not store or maintain a copy of the blockchain and must pass their transactions to a full node [6].

Each block in the blockchain has a header containing metadata about the block, block data containing a set of transactions and other related data. Every block header (except the first one in the chain) contains a cryptographic link to the header of the previous block. Each transaction involves one or more blockchain users, a recording of the changes and is digitally signed by the user submitting the transaction. Each node then verifies the transaction using their local copy of the blockchain, which is a complete log of all previous transactions [6].

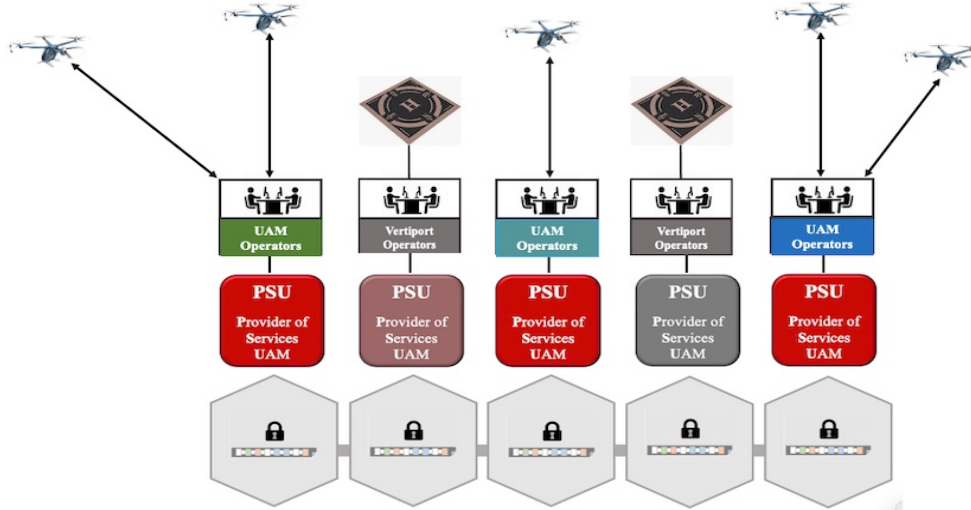


Figure 2 – Notional Blockchain Distributed Ledger

As shown in Figure 2, a blockchain is a distributed ledger that records all the transactions that take place on the network. A blockchain ledger decentralized, is replicated across many network participants. Additionally, each participant collaborates in the blockchain maintenance. The information recorded to a blockchain is append-only, where a cryptographic technique is used that guarantees that once a transaction has been added to the ledger it cannot be modified. Also, immutability ensures that the no one can alter the history of the blockchain data.

For this work, a permissioned-based blockchain was selected for implementation. Blockchains can either be Public or Permissioned. Public blockchains are open protocols. Anyone can join the network and participate in the protocol and take care of the overall network consensus. The data stored in the blockchain is visible since everything is public. While transparency is a very desirable trait, enterprises don't want to use a network wherein anyone can view their daily operations and be a party to some confidential information. As a result, enterprises prefer using a unique form of blockchain called permissioned chains, limiting the number of nodes entering the network. Permissioned blockchains are applicable to UAM environments since there will be UAM security and privacy requirements for limiting access to the data.

A blockchain network is comprised primarily of a set of peer nodes (or, simply, peers). Peers are a fundamental element of the network because they host ledgers and smart contracts. A smart contract defines the rules between different organizations in executable code. Applications invoke a smart contract to generate transactions that are recorded on the ledger. Blockchain technology can be used to track transactions and verify negotiated agreements using smart contracts, which are self-executing contracts that are stored and run on a blockchain network. Smart contracts can be programmed to automatically execute certain actions once certain conditions are met, such as the transfer of aeronautics related information between federated entities across a UAM environment. When a transaction is initiated on a blockchain network, it is broadcast to all nodes on the network and verified by a consensus mechanism, where peers approve the transaction. Once the transaction is verified, it is added to a block, which is then added to the blockchain, creating an immutable and transparent record of the transaction. This level of transparency and immutability makes blockchain technology particularly useful for tracking transactions and verifying agreements, as it provides an auditable and tamper-proof record of all actions taken on the network. Additionally, the use of smart contracts can help to automate many of the processes involved in negotiating and executing agreements, making the process more efficient and secure.

V. Case Study – Operational Intent

In this case study, two vehicle operators are operating in the same airspace. Their intent is to fly vehicles that land at a shared vertiport. Each vehicle operator will coordinate its flight intent through a PSU. A PSU is an entity that provides services to the UAM Operator to help them meet UAM operational requirements that enable safe, efficient, and secure use of the airspace [7].

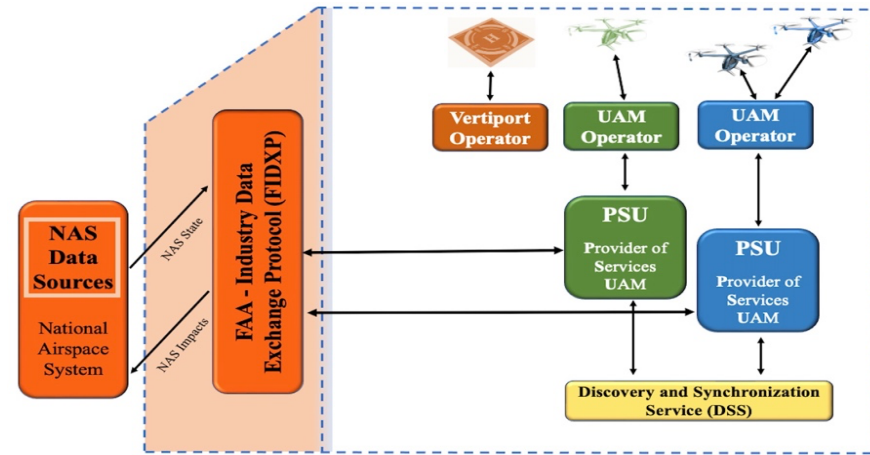


Figure 3 – Operational Intent Case Study

As shown in Figure 3, multiple PSUs employed by different operators will be part of a network and subject to interoperability requirements. The PSU is the trusted source for some of the traditional ANSP services, such as distribution of notifications, confirmation of flight intent, and confirmation of authorized access to airspace.

Since the PSUs may have independent operational intent that has conflicts, there needs to be a process of automatically detecting relevant concurrent flight information on the PSU Network. The Discovery Synchronization Service (DSS) enables PSUs to identify other PSUs with active operations around the area of interest during the noted planned flight times. A DSS can be utilized by all participating PSUs to facilitate automated data exchanges between one another. Specifically, it enabled UAM Operators to register into an airspace, be aware of other UAM Operators in the airspace, and to submit operations, via the PSU. Additionally, it validates that the PSU had obtained

all relevant data from other PSUs. The intent of the DSS was to guarantee that the PSU supporting the UAM Operator possessed comprehensive and current data concerning the surrounding operations and airspace restrictions within the operation's vicinity [8]. Additionally, the FAA-Industry Data Exchange Protocol (FIDXP) is an interface for data exchange between FAA systems and UAM participants.

If any of the systems supporting UAM operations, such as the PSUs, DSS or FIDXP, succumb to a cybersecurity attack, then there could be a loss of data integrity that impacts flight operations. The UAM data integrity concern is like the "Two Generals Paradox" in computer science. The "Two Generals Paradox" explores the challenges of reliable communication in a distributed computing environment [9]. For the paradox, two generals are leading separate armies that are planning to attack a common enemy. Since the generals are located far away from each other, they can only communicate via messengers. However, there is a risk that the messengers can be intercepted, and their messages can be tampered with or lost. The challenge is to devise a strategy that guarantees that both generals agree on a coordinated attack plan, even in the presence of communication failures.

Blockchain technology does not rely on a central authority. Since blockchain technology uses a distributed and decentralized ledger which allows for reliable and secure communication between different entities, it is a potential solution to the Two Generals Problem for the UAM data integrity concern. With a solution, based on blockchain technology, for the Two Generals Problem, the generals can use a consensus mechanism to agree on a synchronized attack plan without relying on a central authority. Similarly, two UAM operators can communicate with the DSS to deconflict any planned flight plans, that may merge. The blockchain consensus mechanism ensures that all parties involved in the communication agree on the same data or message, or in this case, the operational intent of the two UAM operators. This is achieved through a process of validation and verification of transactions or messages by network participants.

Blockchain networks, either embedded or adjacent to UAM PSUs, DSS or the FIDXP can be utilized to mitigate cybersecurity attacks. By replicating the information from the DSS and the FIDXP across blockchain networks, the blockchain immutability feature will prevent loss of data integrity after any cyber-attacks. As a result, as the vehicle operators check their flight plans against the DSS and FIDXP, the integrity of the flight operations can be trusted.

The Hyperledger Fabric open source permissioned blockchain framework was selected to meet the secure data exchange for UAM objectives. Hyperledger Fabric provides a distributed ledger that has a permissioned architecture, is highly modular, has an open smart contract model, and has a low latency consensus approach [10]. Smart contracts can be leveraged to collect information from the DSS and FIDXP. Additionally, they will also gather operational intent from the PSUs and support their checking the DSS and FIDXP for flight deconfliction.

References

- [1] Vascik, P. D., Hansman, R. J., & Dunn, N. S. (2018). Analysis of urban air mobility operational constraints. *Journal of Air Transportation*, 26(4), 133-146.
- [2] Whitley, Pamela, FAA UTM Concept of Operations – v2.0, Federal Aviation Administration, [online] Available: https://www.faa.gov/uas/research_development/traffic_management/media/UTM_ConOps_v2.pdf
- [3] The MITRE Corporation, "Architectures Federation", <https://www.mitre.org/publications/systemsengineering-guide/enterprise-engineering/engineering-informationintensiveenterprises/architectures-federation>, accessed July 2021
- [4] Levitt, I., Phojanamongkolkij, N., Horn, A., Witzberger, K., "UAM Airspace Research Roadmap v2.0", NASA/TM-20230002647, March 2023.
- [5] Federal Aviation Administration, NextGen Concept of Operations for Urban Air Mobility (UAM) v1.0, Jun 2020. https://nari.arc.nasa.gov/sites/default/files/attachments/UAM_ConOps_v1.0.pdf.
- [6] Sridhar, B., Chatterji, G., Freeman, K., Simulation and Modeling Concepts for Secure Airspace Operations, 2021 *AIAA Aviation Forum*
- [7] Freeman, K., Gillem, N., Jones, A., Sridhar, B., Sharma, N., Immutable Secure Data Exchange Data Model Test Results, 2021 *AIAA SciTech 2022 Forum*
- [8] Cheng, A., Witzberger, K., Isaacson, D., Verma, S., Arneson, H., Lee, H., Seah, C., "National Campaign (NC)-1 Strategic Conflict Management Simulation (X4) Final Report", NASA/TM- -2022-0018159
- [9] Gmytrasiewicz, Piotr J.; Edmund H. Durfee (1992). "Decision-theoretic recursive modeling and the coordinated attack problem". *Proceedings of the First International Conference on Artificial Intelligence Planning Systems*.
- [10] <https://www.hyperledger.org/use/fabric>