

# A Blockchain Case Study for Urban Air Mobility Operational Intent

Kenneth Freeman<sup>1</sup>, Norbert Gillem<sup>2</sup>, Aidan R. Jones<sup>3</sup>  
Nishant Sharma<sup>4</sup>

*NASA Ames Research Center, Moffett Field, CA, USA*

## Extended Abstract

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. 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.

### A. 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.

UAM operations will be leveraging a service-based architecture for airspace solutions. The UAM environment will leverage independent UAM operators utilizing diverse communications and system access approaches. Additionally,

---

<sup>1</sup> Aerospace Engineer, NASA Ames Research Center, Moffett Field, CA 94035, USA.

<sup>2</sup> Aerospace Engineer, NASA Ames Research Center, Moffett Field, CA 94035, USA.

<sup>3</sup> Aerospace Engineer, NASA Ames Research Center, Moffett Field, CA 94035, USA.

<sup>4</sup> Systems Engineer, Intrinsic Technologies Corporation, Moffett Field, CA 94035, USA.

there will be independent Provider of Services for UAM (PSU) operators and supplemental data service providers (SDSP) exchanging data between themselves and UAM operators.

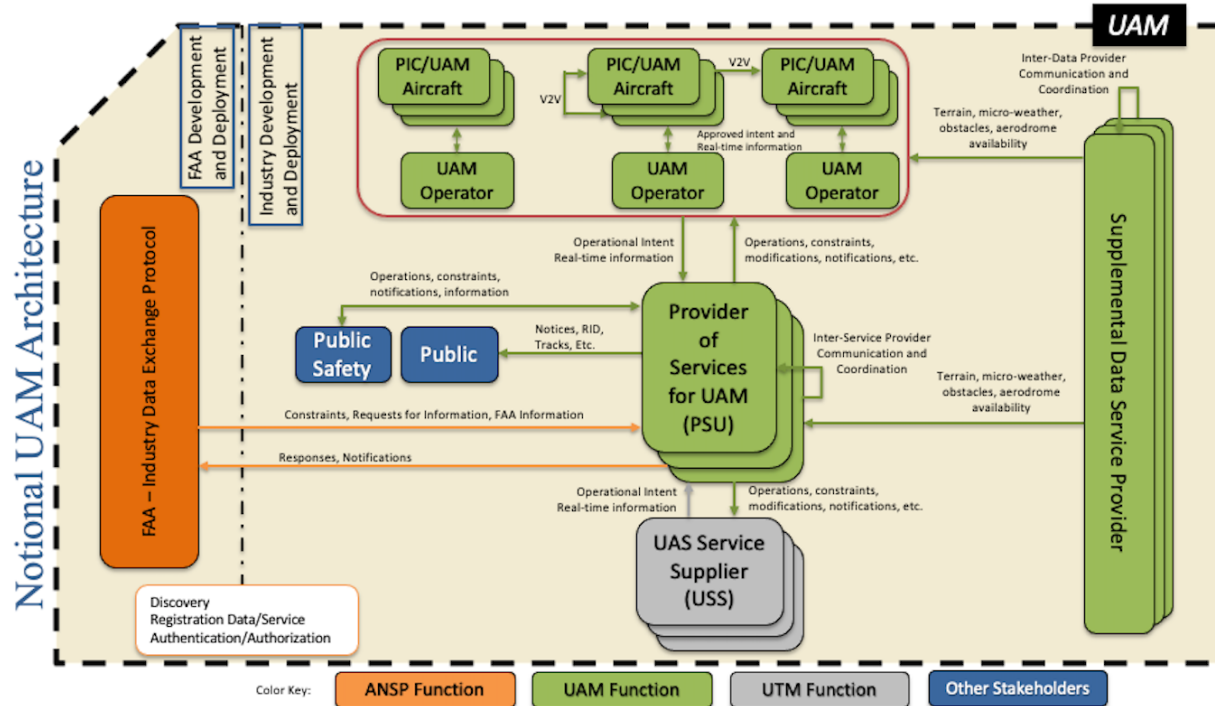


Figure 1 – Notional UAM Architecture

### B. 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 research is to address four cybersecurity threats that may impact a UAM environment:

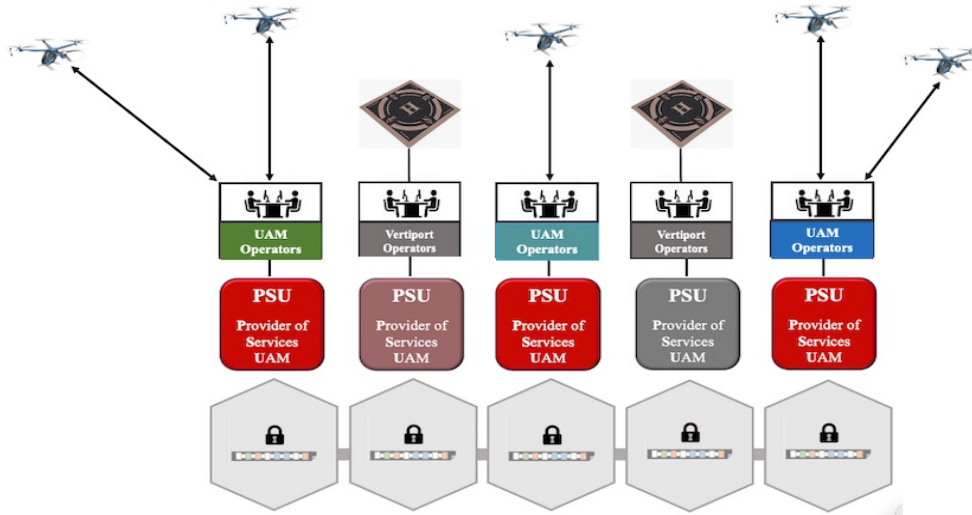
- Man-in-the-middle attacks, leading to data manipulation
- Victims of spear phishing, leading to the interaction with malicious content
- Exploitation of valid accounts, leading to the loss of credentials and system access
- Exploitation of public facing application, leading to corruption of data

The intent of this work is to leverage a permissioned blockchain approach, to simulate secure data exchange and storage, to mitigate these cybersecurity threats.

### C. 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. [4]

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. The transaction is verified by all the nodes with their blockchain consisting of a copy of the chained blocks of all transactions. [4]

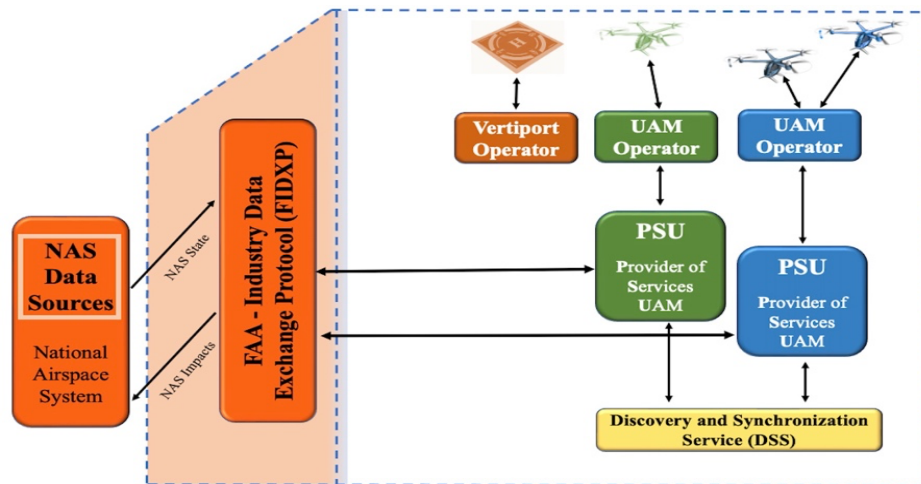


**Figure 2 – Notional Blockchain Distributed Ledger**

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. Since blockchains have an append-only feature, the data on a blockchain is immutable. Also, immutability ensures that the no one can alter the state of the blockchain data.

#### **D. 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 [5]. 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.



**Figure 3 – Operational Intent Case Study**

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. The DSS which provides a high-level strategic conflict detection capability, enables an UAM Operator to register into an airspace, be aware of other operators in the airspace, and post operations to the airspace. 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. 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.

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. 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 [6]. Smart contracts will 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](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] Sridhar, B., Chatterji, G., Freeman, K. Simulation and Modeling Concepts for Secure Airspace Operations, *accepted for publication at the 2021 AIAA Aviation Forum*
- [5] Urban Air Mobility Concept of Operations v 1.0
- [6] <https://www.hyperledger.org/use/fabric>