

Simulating Secure Data Exchange and Storage for Urban Air Mobility Environments

Aidan Jones*

NASA Ames Research Center, Moffet Field, CA 94035, USA.

Norbert Gillem†

NASA Ames Research Center, Moffet Field, CA 94035, USA.

Abdullah Abdul‡

Morgan State University, Baltimore, MD 21251.

Nishant Sharma§

Intrinsyx Technologies Corporation, Moffet Field, CA 94035, USA.

Chaz Chang¶

San Jose State University, San Jose, CA 95152, USA.

Kenneth Freeman||

NASA Ames Research Center, Moffet Field, CA 94035, USA.

Extended Abstract

I. Background

Urban Air Mobility (UAM) defines an environment for managing the operations of vertical takeoff and landing (VTOL) and short takeoff and landing (STOL) vehicles in an urban environment [1]. Within a UAM environment, UAM operators manage vehicle operations, relying on Providers of Services for UAM (PSUs) and Supplemental Data Service Providers (SDSPs) for support. In addition, the Federal Aviation Administration (FAA) must maintain certain controls over UAM environments in order to coordinate UAM and National Airspace System (NAS) operations. The FAA accomplishes this through the Flight Information Management System (FIMS), for which the primary interface for UAM participants is the FAA-Industry Exchange Protocol (FIDXP). As UAM environments are cooperative in nature, with multiple organizations participating, there is a need for synchronization and conflict management among the different entities. The primary mechanism in place for this is the Discovery and Synchronization Service (DSS), which tracks the organizations' operations within different airspaces. The notional architecture for UAM can be seen in figure 1.

Ensuring a strong cybersecurity posture is paramount to successful UAM operations. In order to achieve public acceptance of aerial transportation in densely populated areas, strong security and safety guarantees must be made. Cybersecurity in UAM is required to secure both physical infrastructure as well as data. In this case, data can belong to individual customers, operating organizations, or even be public.

II. Motivation

The objective of this work is to leverage a permissioned blockchain for secure data exchange and storage in a simulated UAM environment. UAM environments are federated in nature, meaning there are multiple organizations managing their own services, identities, and infrastructure. However, these entities often need to interoperate, necessitating a secure way to exchange data. Blockchain is ideal for such use cases, allowing multiple organizations fine tuned and granular control over shared data in a consistent manner. Examples of such data are identities, flight plans, customer and

*Software Engineer, NASA Ames Research Center, Moffet Field, CA 94035, USA.

†Aerospace Engineer, NASA Ames Research Center, Moffet Field, CA 94035, USA.

‡Intern, Morgan State University, Baltimore, MD 21251.

§Systems Engineer, Intrinsyx Technologies Corporation, Moffet Field, CA 94035, USA.

¶Intern, San Jose State University, San Jose, CA 95152, USA.

||Aerospace Engineer, NASA Ames Research Center, Moffet Field, CA 94035, USA.

employee data, logs, and vehicle telemetry. The simulation discussed in this paper focuses on identities, flight plans, and telemetry data.

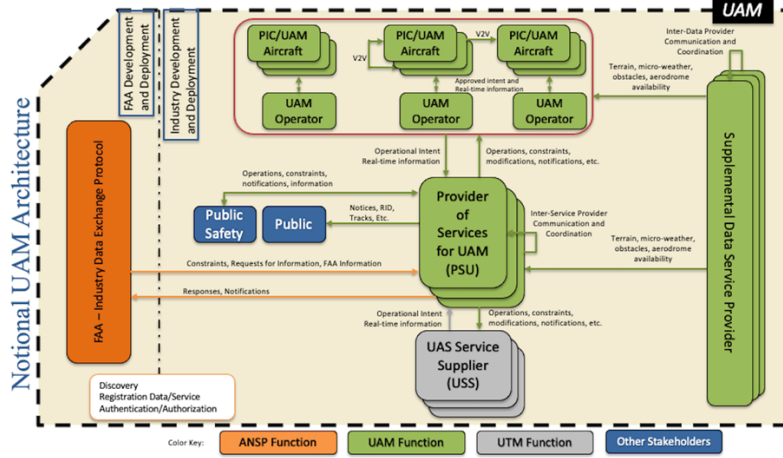


Fig. 1 Notional UAM Architecture

Previous research [2] into using blockchain for UAM data exchanges focused on the general feasibility of such an approach, as well as addressing various cybersecurity concerns. In contrast, this paper aims to better simulate an actual UAM environment, mocking many of the core services. Specifically, this paper focuses on information exchanged between UAM operators, PSUs, and a DSS during the process of a UAM operator claiming a specific airspace for a flight. The flight plan, also referred to as operational intent in this paper, is saved on the blockchain, as are any constraints imposed by other organizations who have their own claims on said airspace. This paper also explores the process of generating and recording realistic telemetry data after the flight plan is accepted.

III. Blockchain

At its core, a blockchain is a distributed and immutable ledger [3]. That is, it is a data structure that records transactions between various entities in a distributed environment, where each transaction is appended. It should be noted that the term transaction here refers to an arbitrary addition of data recorded on the blockchain. Each transaction is signed by the private key of the entity submitting the transaction, so that other users can verify with the corresponding public key.

A block in the blockchain consists of a set of transactions grouped together, a hash of the previous block, as well as some additional metadata. Including the hash of the previous block creates a chain of blocks, where the state of data at some block i can be verified by computing the hash of the $i - 1$ block, and so on up the chain. The first block in a blockchain is the only one without a hash, and is called the genesis block. This chaining together of blocks with cryptographic hashes is how blockchains can guarantee immutability, as changing the value of a previous transaction will change the value of the hash. In addition, all nodes in a blockchain network must reach an agreement in terms of which transactions are included in a block. This process is called consensus. There are many different mechanism for consensus, though the most common are proof of work and proof of stake.

Permissioned blockchains, also called private blockchains, restrict access to a specific group of verified users. This is in opposition to public blockchains, such as Bitcoin, where anyone can participate and submit transactions. Hyperledger Fabric (HLF) [4], the blockchain used in this research, leverages traditional public key infrastructure (PKI) for the authentication of users. Also, as permissioned blockchains are not open by nature, they can leverage more centralized and efficient methods of consensus.

IV. Secure Data Exchange Blockchain Network

The blockchain network used in this simulation was created using Hyperledger Fabric, as mentioned in the above section. There are a set of organizations, each possessing a single peer and a certificate authority (CA). A peer refers to

a node in the blockchain network that can submit transactions and host smart contracts. Smart contracts are code that sits on either the blockchain itself as data, or on the peers who can execute it. Executing the contract, which is the same as running the code, can add data to the blockchain, thus generating transactions. Different smart contracts were developed for the different use cases of the simulation. Of note, there is a contract with a set of functions for managing flight plans, as well as one for adding telemetry data.

There is also a single organization representing the FAA. This organization possesses a set of ordering nodes. Ordering nodes, the key component of the ordering service, is how consensus is achieved in HLF. There is a logically centralized service that orders transactions and returns new blocks to peers. While this is a logically centralized service, any number of organizations can participate. However, in this simulation, all ordering nodes belong to a single organization.

The CAs are responsible for issuing identities to users within an organization, as well as verifying identities both internally and externally. Identities outside of an organization can be verified by using the Membership Service Provider (MSP), which defines the preconfigured accepted organizations that can participate in a HLF network. The root certificate from each organizations' CA is shared through the MSP. Identities within an organization are verified using traditional PKI mechanisms.

V. Secure Data Exchange UAM Simulation

The Secure Data Exchange UAM simulation defines multiple services, some of which mock services found in actual UAM environments. There are three primary organizations in the simulation, *Org1*, *Org2*, and *Org3*. *Org1* and *Org2* represent private organizations that own and operate vehicles, a single UAM operator, and a single PSU. There is also DSS used for discovery and synchronization between the two organizations, a FIDXP service to mock FAA authorization of flight plans, and a flight simulation service that generates telemetry data once a flight plan is approved.

Each UAM operator has the capability to submit flight plans to its corresponding PSU. The PSU then ensures the airspace is available, modifying the flight plan and communicating with the DSS and other PSUs if necessary. Once the PSU has a valid flight plan, it returns it back to the UAM operator, which then can notify the flight simulation service to begin the flight. All exchanges, updates to the flight plan, as well as final telemetry data is recorded on the blockchain. This process is transparent to the UAM operator.

The final paper will explore the specifics of the simulation, including the data flow, technology stack, and security considerations. There will also be a thorough evaluation of both the implemented blockchain network, as well as the ability for blockchain to facilitate the secure exchange and storage of data in a UAM environment.

References

- [1] Fontaine, P., "Concept of Operations v2.0 Urban Air Mobility (UAM)," , 2023. URL https://www.faa.gov/sites/faa.gov/files/Urban%20Air%20Mobility%20%28UAM%29%20Concept%20of%20Operations%202.0_0.pdf.
- [2] Freeman, K., Gillem, N., Jones, A. R., Sridhar, B., and Sharma, N., *Immutable Secure Data Exchange and Storage for Urban Air Mobility Environments*, , 2022. URL <https://doi.org/10.2514/6.2022-1092>, URL <https://arc.aiaa.org/doi/abs/10.2514/6.2022-1092>.
- [3] Kolb, J., AbdelBaky, M., Katz, R. H., and Culler, D. E., "Core Concepts, Challenges, and Future Directions in Blockchain: A Centralized Tutorial," *ACM Comput. Surv.*, Vol. 53, No. 1, 2020. <https://doi.org/10.1145/3366370>, URL <https://doi.org/10.1145/3366370>.
- [4] Hyperledger, "Hyperledger Fabric - ReadTheDocs," , 2023. URL <https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html>.