AIAA SciTech Forum
January 3-7, 2022, San Diego, CA & Virtual
AIAA SCITECH 2022 Forum

10.2514/6.2022-1092

Immutable Secure Data Exchange and Storage for Urban Air Mobility Environments

Kenneth Freeman[1], Norbert Gillem[2], Aidan R. Jones[3]
Banavar Sridhar[4], Nishant Sharma[5],
NASA Ames Research Center, Moffett Field, CA, USA

Urban air mobility (UAM) is a concept that proposes to develop short-range aerial vehicles to overcome increasing surface congestion. Within the UAM 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) support flight operations within the UAM environment. The development of UAM systems and the associated data exchange and service interactions will be at risk due to numerous cybersecurity attacks. 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.

The UAM architecture is leveraged from the Unmanned Traffic Management (UTM) concept of operations [1]. Within the UAM 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) 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).

Urban air mobility (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 [3]. 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 development of UAM systems and the associated data exchange and service interactions will be at risk due to numerous cybersecurity attacks. As these threats evolve, the UAM cybersecurity capabilities must also adapt to these changes [4].

I. Motivation

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, independent PSU operators and supplemental data service providers (SDSP) will exchange data with UAM operators. Figure 1 shows a notional UAM architecture depicting the interaction between different entities.

[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] Principal Engineer, USRA, Moffett Field, CA 94035, USA, Fellow AIAA
[5] Systems Engineer, Intrinsyx Technologies Corporation, Moffett Field, CA 94035, USA.

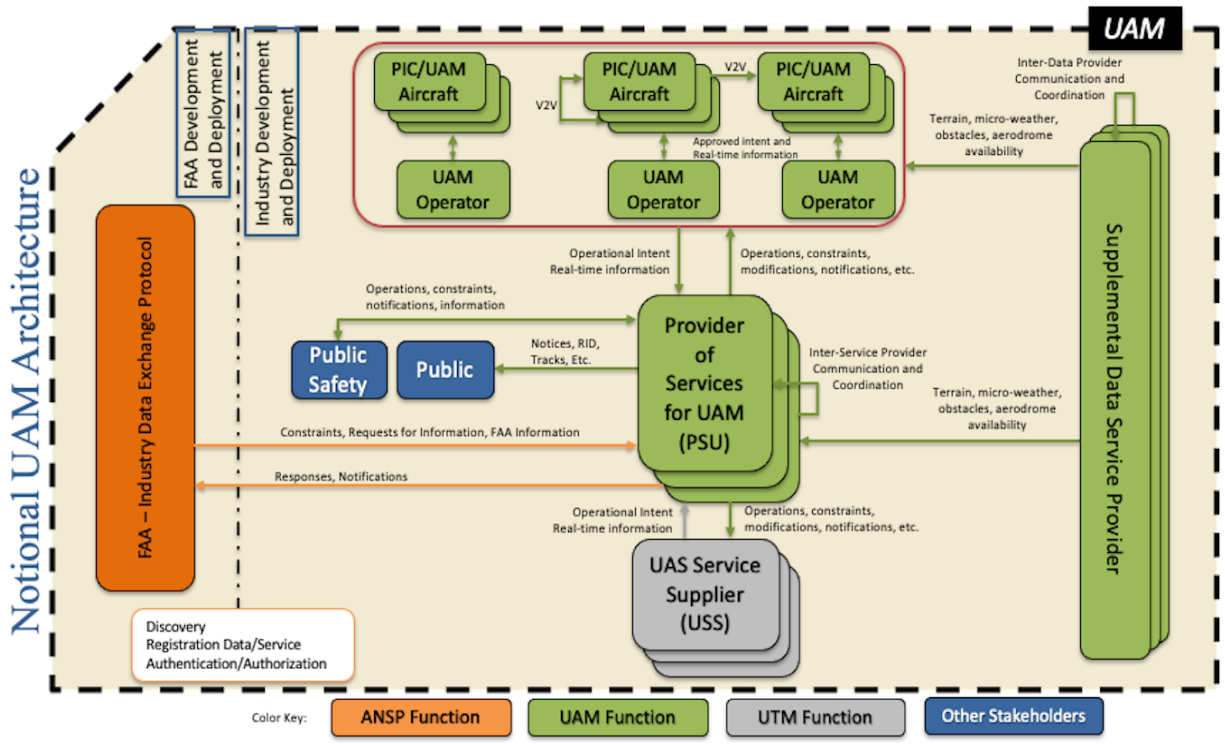

Figure 1 – Notional UAM Architecture

The decentralized community of UAM operators, PSU operators, and SDSPs will likely operate their services on local or cloud environments that require security. This research focuses on the secure data exchange and storage of this decentralized UAM environment to address these challenges. This research intends 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 and data corruption
- The exploitation of valid accounts, leading to the loss of credentials and unauthorized system and data access
- The exploitation of public-facing applications, leading to data corruption

II. Blockchain

A blockchain is a distributed system with either a linear or graph-like structure with nodes and links connected without 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 that can 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 its transactions to a full node [5].

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 [5].

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 blockchain maintenance.

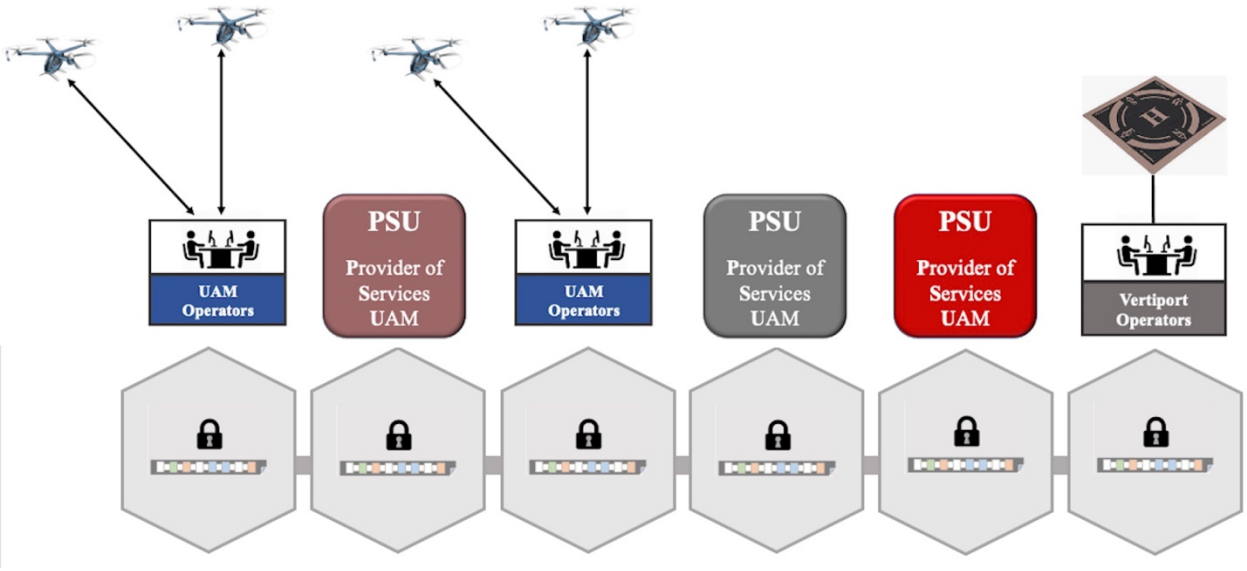

Figure 2 – Notional Blockchain Distributed Ledger

The information recorded to a blockchain is append-only, where a cryptographic technique has been 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 no one can alter the state of the blockchain data.

III. Blockchain Applicability to UAM

This paper examines blockchain technology as a possible solution to secure data transactions and storage. Blockchain technologies can be used for the identity management of vehicles, people, and systems. It could help track transactions and verify negotiated agreements between operators and service providers in UAM environments. For example, the airspace structure for a specific timeframe, the record of the submitted flight plan, and the approved flight plan could be verified using a blockchain-based immutable ledger. Similarly, system and approval logs can be kept in the immutable ledger for audit incidents and even accident investigations. Since the immutable ledger can be leveraged to ensure that the critical information that supports the UAM environment is not altered, the data can be trusted to withstand cybersecurity attacks. Various types of cybersecurity attacks can result in the manipulation or corruption of data. Storing critical UAM information in an immutable blockchain-based ledger would limit the damage from these types of cyber-attacks.

Additionally, the service-based architecture leveraged by UAM will be broadly distributed. The infrastructure supporting the independent UAM operators, independent PSU operators, and SDSPs will be controlled by the individual UAM operators and service providers rather than under the day-to-day control of a large-scale entity such as the FAA. As a result, the independent UAM operators, independent PSU operators, and SDSPs will need a mechanism to establish identities and trust across multiple entities within the UAM environment. Blockchain allows individual organizations to exchange information, money, and other assets with one another, without requiring an intermediary to do so.

IV. Secure Data Exchange Blockchain Network

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.

For this work, a permission-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 where anyone can view their daily operations and party to 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.

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 permission architecture, is highly modular, has an open smart contract model, and has a low latency consensus approach [6].

A. Channels

Hyperledger Fabric has a feature called channels, which are a private subset of communication paths between two or more specific network members within a network. Channels are used to conduct private and confidential transactions. For this work, there would be a need to provide privacy for data exchanges between operators and service providers. There may be proprietary pricing or contracting information within these transactions. As shown in Figure 3, a blockchain network was built with two channels to protect the proprietary information of the vertiport operators.

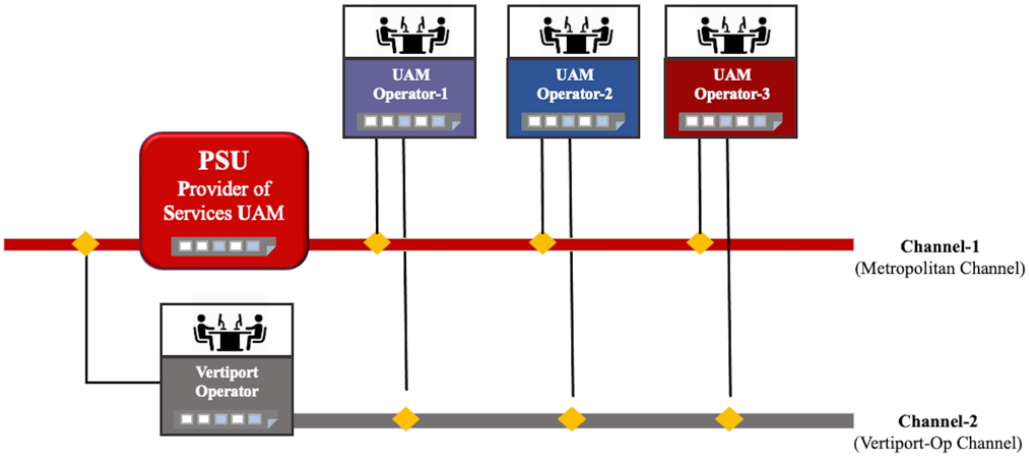

Figure 3– Blockchain Network Channels

As this work progresses, trade-offs will need to be made between the security of multiple channels versus complexity.

B. Blockchain Data Feeder

A smart contract is software defining an asset or assets and the transaction instructions for modifying the asset. Smart contracts in the Hyperledger Fabric framework are referred to as chaincode. Chaincode or smart contracts represent the business logic of the system. Chaincode enforces the rules for reading or altering (adding) information to the distributed ledger. Chaincode execution results in a set of key-value writes (write set) that can be submitted to the network and applied to the ledger on all peers.

The chaincode nomenclature is complex and not easily read by humans. As a result, a blockchain data feeder was developed to input data from a UAM flight simulation into the blockchain. This feeder can collect data from a simulated vehicle transponder and write the chaincode commands to store information on the blockchain. The data feeder provides the speed and accuracy for correct chaincode commands. Chaincode commands are long and contain elements such as permissioned network members' information, the correct ports that each network member can use the correct smart contract function. If the command format is not correct, it will be rejected by the Blockchain network. The data feeder provides an automated interface between the incoming Data and the Hyperledger Fabric Blockchain Network to ensure proper chaincode command entry and operation.

C. Block Sizes

The size of individual blocks on a blockchain can have a potentially large impact on the speed and capacity of the network, but there are always trade-offs. Blockchains get their name from the fact that they are literally composed of an ever-ongoing history of blocks. Blocks themselves are batches of transaction data, and the amount of data contained in each block combined with the chain's block generation speed determines the number of transactions per second, or TPS, that the network can handle. Having a high rate of TPS is more beneficial, so developers are always looking for ways to improve this metric. Because the TPS rate of a blockchain is deeply tied to the size of each block, this becomes a major factor in finding a path to mainstream adoption. However, simply increasing the size indefinitely is only one way to approach the issue, and there are many different philosophies as to how to move forward.

As the blockchain network is being configured, a decision needs to be made on selecting the sizes of the individual blocks in the ledger. In selecting the block sizes, there is a trade-off between performance and security. Selecting larger blocks lead to better performance when adding information to the blockchain. However, smaller blocks support enhanced security. The riskiest aspect of blockchain networks comes when Data is added to the chain. As a result, larger amounts of data have increased risk when being added.

V. Secure Data Exchange Blockchain Verification

Two use cases were identified for verifying the functionality of the blockchain for a UAM scenario and defining the best operational configurations for the blockchain.

A. Use Cases

For this stage of the secure data exchange work, two use cases were considered to verify the capabilities and performance of blockchain networks:

1. Enrollment: The use case focused on the enrollment of UAM operators, vertiport operators, and pilots.
2. Telemetry: The use case simulated the collection of vehicle telemetry while in flight and during takeoff and landing.

An early step related to building a blockchain network that supports the Enrollment use case was to establish the business logic. For this case, three UAM operators and one vertiport operator were identified. Data tables were established to represent the information required to enroll a UAM operator or a vertiport operator onto the blockchain network. Additionally, business logic and data tables were established for the enrollment of UAM pilots, as well. A blockchain network was built that met the requirements of the Enrollment use case. It is assumed that this use case could mitigate threats from the exploitation of public-facing applications, credential loss, and spearfishing.

Next, the Telemetry use case was identified. It is assumed that this use case could mitigate threats from man-in-the-middle attacks. For the purposes of the engineering evaluation of this use case, routes from the Dallas-Fort Worth airspace were used. Some routes connected the large airports like Dallas-Fort Worth (DFW), Dallas-Love Field (DAL), and Addison (ADS) [7]. The intent was to add business logic to the blockchain network that would support the collection of vehicle telemetry as they flew within the DFW airspace. As shown in Figure 4 below, DFW routes were leveraged to simulate vehicle movement. The number of routes were based on low demand volumes. For the Telemetry use case, the number of vehicles simulated ranged from 4 – 50. Based on this, the transmission of vehicle telemetry was simulated, assuming Automatic Dependent Surveillance-Broadcast (ADS-B) as the method of secondary surveillance.

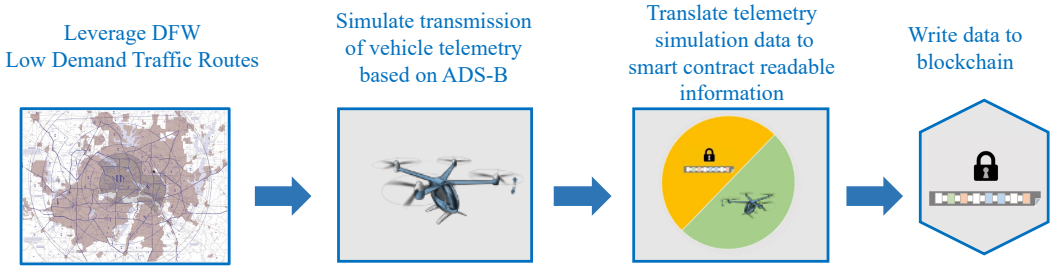

Figure 4 – Telemetry Use Case Approach

Each simulated vehicle reported its location approximately once per second. The data from the simulation was then sent to a feeder program that translated the information in a way that could be leveraged by a smart contract. The smart contract is then leveraged to write the information to the blockchain. The use case intends to show and validate that multiple vehicles flying in traffic routes can transmit telemetry recorded on the blockchain network. Once the telemetry is stored on the blockchain network, the information can be viewed as trusted records by local air traffic control or the vehicle operators.

B. Enrollment Use Case

The intent of this use case was to verify the function of the blockchain. The goal of this verification testing for the enrollment use case was to verify the following: (1) Data can be inserted into both blockchain and world state database. (The world state holds the current value of the attributes of a blockchain ledger state.), (2) data can be queried from the world state database, and (3) data can be queried from the blockchain.

Leveraging the enrollment use case, data was successfully written to the blockchain ledger. Additionally, information could be read from the blockchain ledger. Due to the success of the enrollment use case, use cases supporting UAM regulatory data collection, performance measurements, and the business transaction could be considered.

C. Telemetry Use Case

In this use case, several tests were run to simulate an actual UAM environment with multiple vehicles flying and reporting their location. Testing was performed, setting the number of simulated vehicles to the following values: 4, 8, 10, 20, 30, 40, 50. Each simulated vehicle should report the simulated location approximately once per second.

The data used in these tests are simulation data from the DFW area. Possible UAV routes were produced in the DFW area, as well as simulated flights along those routes. Each route had a beginning, an end, and a set of waypoints. Each point on the route had a latitude, longitude, and altitude. The simulated flights had information about the start time, end time, and average speed. From this information, various points along the routes were extrapolated by assuming the UAVs traveled in a straight line and at a constant speed between waypoints.

Latency is the time it takes for a piece of data to be transferred across a network. Generally, the transaction latency increased as the number of vehicles increased. However, this does not hold true for all values. Specifically, the average latency when there are 20 simulated vehicles had a high variance, ranging from 1.7 seconds to 2.67 seconds. Oddly, the general trend for the maximum latency decreased as simulated vehicles were added. While the maximum latency was consistently high regardless of the number of simulated vehicles, the significantly smaller average latency suggests that most transactions had less latency than the reported average, as shown in Figure 5.

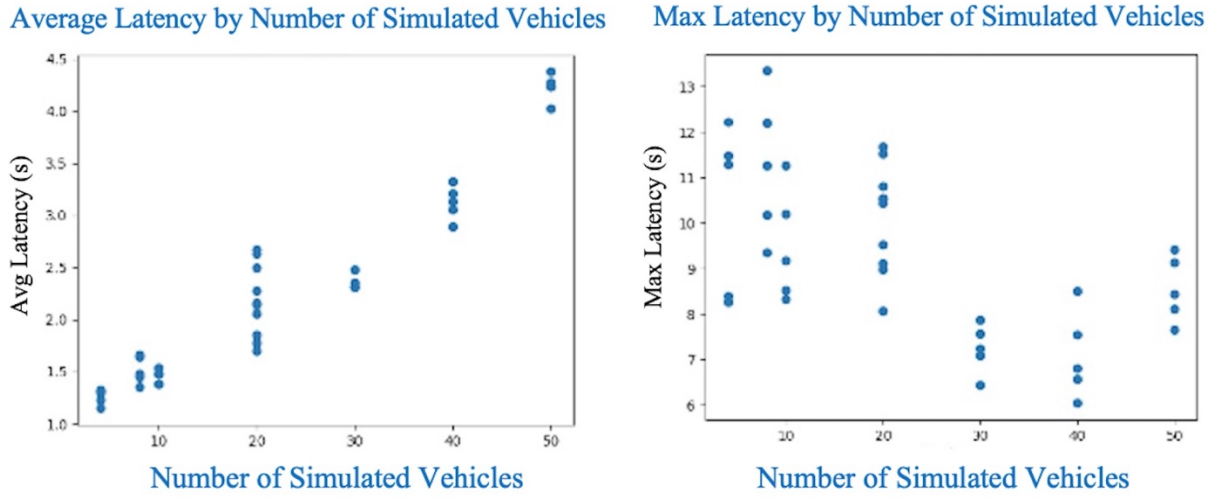

Figure 5 – Average and Max Latency by the Number of Simulated Vehicles

Throughput is the amount of data being sent and received within a specified timeframe. The throughput increased as the number of simulated vehicles increased. That is expected as there are simply more vehicles reporting their

location simultaneously. To understand the impact of multiple simulated vehicles, the drop from send rate to recorded throughput should be considered. The tool used to measure the blockchain performance, Hyperledger Caliper [9].

Figure 6 shows that as the number of simulated vehicles increased, the gap between send rate and throughput increased. The blockchain network had a more difficult time keeping up with the transactions, beyond 30 simulated vehicles transmitting telemetry every second.

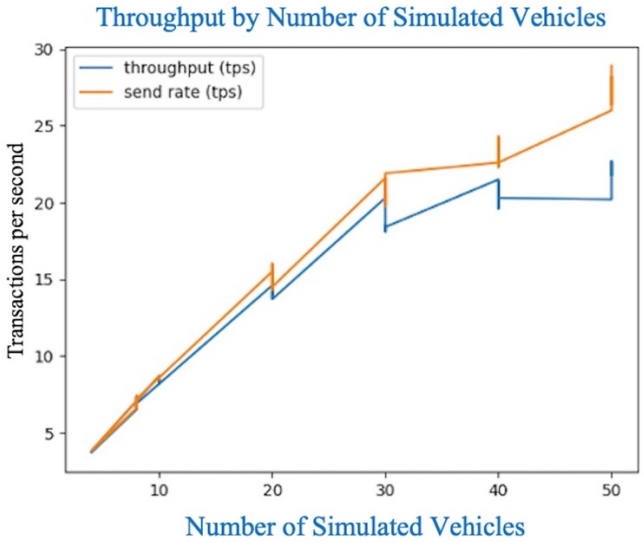

Figure 6 - Throughput by Number of Simulated Vehicles

D. Overall Verification Findings

This blockchain approach does perform and scale nicely, given the right compute and networking infrastructure. There were no transactions lost in any of the tests. However, it can also yield results that are inadequate for some UAM applications. The data proves that the Transaction Per Seconds will deteriorate as the stress on the network is increased. For these tests, one CPU was used with the following parameters: 16 MB RAM, Intel Xeon CPU E5-2686 2.30GHz, Cores 2 leveraging Amazon Web Services.

The enrollment use case was tested using 200 records, representing the enrollment of new vehicles, pilots, vertiports, or UAM operators into the UAM environment. There were no performance concerns when writing to or reading from the blockchain network. For the telemetry use case, there was no discernable variance for the reading data from the blockchain as Data is added to the network. However, as the number of simultaneous vehicles increased, the gap between the telemetry sent to the blockchain and the write time increased. This performance can be increased by increasing the underlying computing power. Initial UAM operations will be designed to minimize interactions with existing ATM operations, with operational tempo expected to be on the order of 3-15 operations per vertiport per hour and simultaneous operations in the tens (10-50) per metropolitan area [10]. A combination of underlying blockchain technology selection, blockchain technology parameter tuning, and an increase in computational capabilities will be required to meet the telemetry use case requirements for initial UAM operations.

VI. Future Work

The approach for immutable secure data exchange has been established. The next steps are to expand the use cases to validate the blockchain functions for secure data exchange, to cover areas that apply across multiple UAM areas that could be applicable to future simulations. Additionally, simulations will be built to validate the principles of these use cases on blockchain networks.

Also, there will be work in determining how to integrate blockchain concepts into a reference PSU and other reference airspace services. Additionally, other blockchain technologies will be considered to increase performance. Also, penetration testing will be included in the testing to verify the blockchain technology's abilities to mitigate cyber security attacks.

VII. References

[1] Kopardekar, P., Rios, J. Prevot, T. Johnson, M. Jung, J & E. Robinson, J. Unmanned Aircraft System Traffic Management (UTM) Concept of Operations. NASA Ames Research Center.

[2] Whitley, Pamela, FAA UTM Concept of Operations – v2.0, Federal Aviation Administration, [online] Available: ttps://www.faa.gov/uas/research_development/traffic_management/media/UTM_ConOps_v2.pdf

[3] 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.

[4] Freeman, K., Garcia, S., Cyber Threats and Security Controls Analysis for Urban Air Mobility Environments, AIAA SciTech 2021 Forum

[5] Sridhar, B., Chatterji, G., Freeman, K. Simulation and Modeling Concepts for Secure Airspace Operations, AIAA Aviation 2021 Forum

[6] https://www.hyperledger.org/use/fabric

[7] Verma, V.A. et al. "Lessons Learned: Using UTM Paradigm for Urban Air Mobility", 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)

[8] "VFR Raster Charts," Federal Aviation Administration, Jan. 31, 2017. https://www.faa.gov/air_traffic/flight_info/aeronav/digital_products/vfr/

[9] https://www.hyperledger.org/use/caliper

[10] Goodrich, K., and Theodore, C. "Description of the NASA Urban Air Mobility Maturity Level (UML) Scale," AIAA 2021-1627. AIAA Scitech 2021 Forum. January 2021