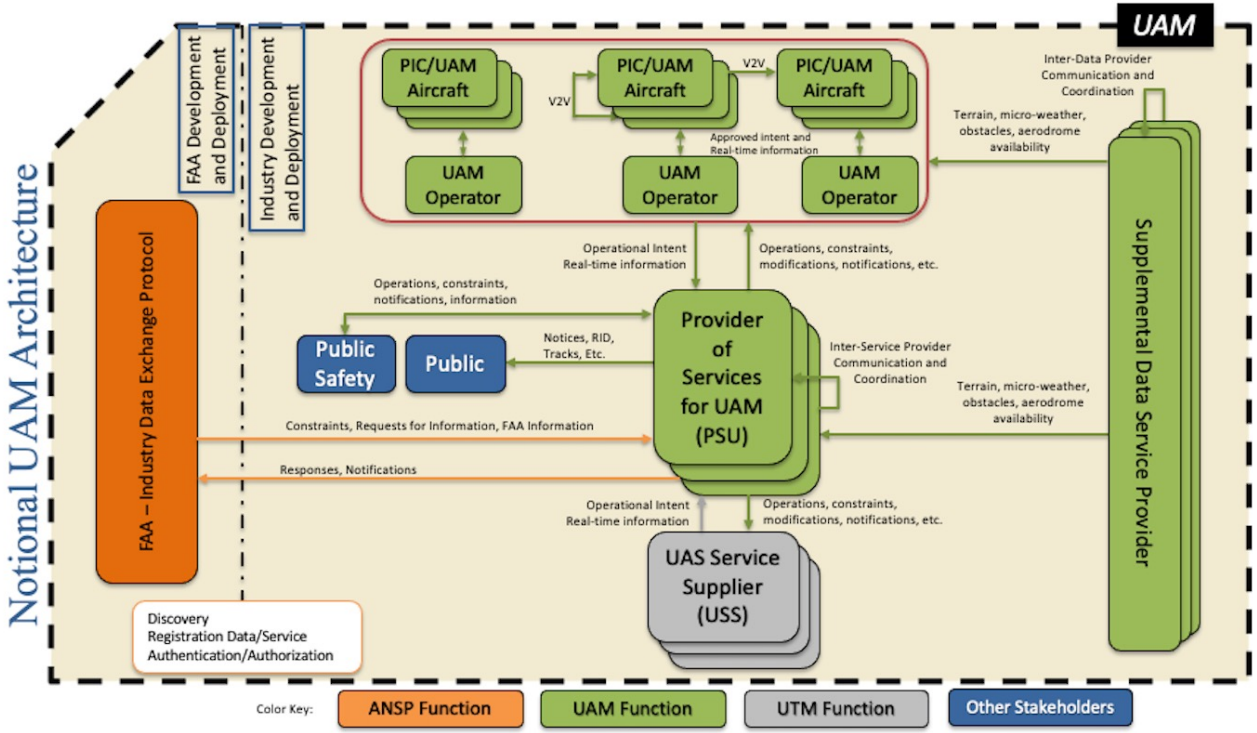



Immutable Secure Data Exchange and Storage for UAM Environments

Kenneth Freeman
NASA Ames Research Center

Overview / Motivation

Urban Air Mobility (UAM), leveraging a service-based architecture for Secure Airspace solutions



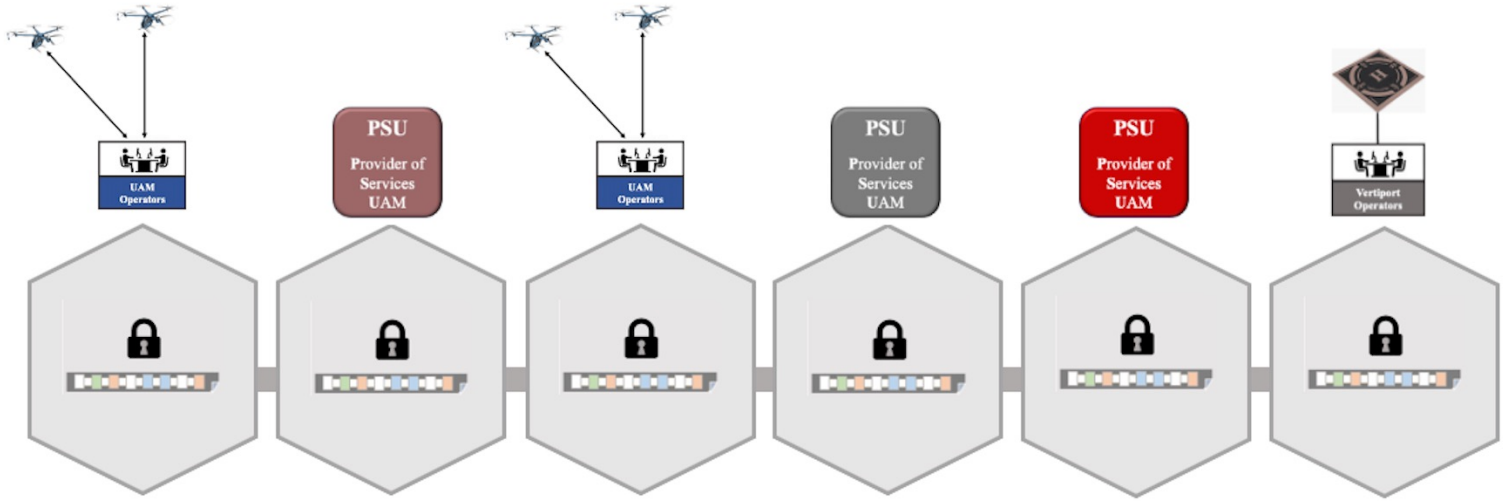
UAM Environment :

- Independent UAM operators leveraging diverse communications
- Interactions (data exchange) between multiple PSUs and operators
- Decentralized local computing and cloud environments requiring security

Motivation: Research a methodology for providing secure data exchange and storage

What is Blockchain?

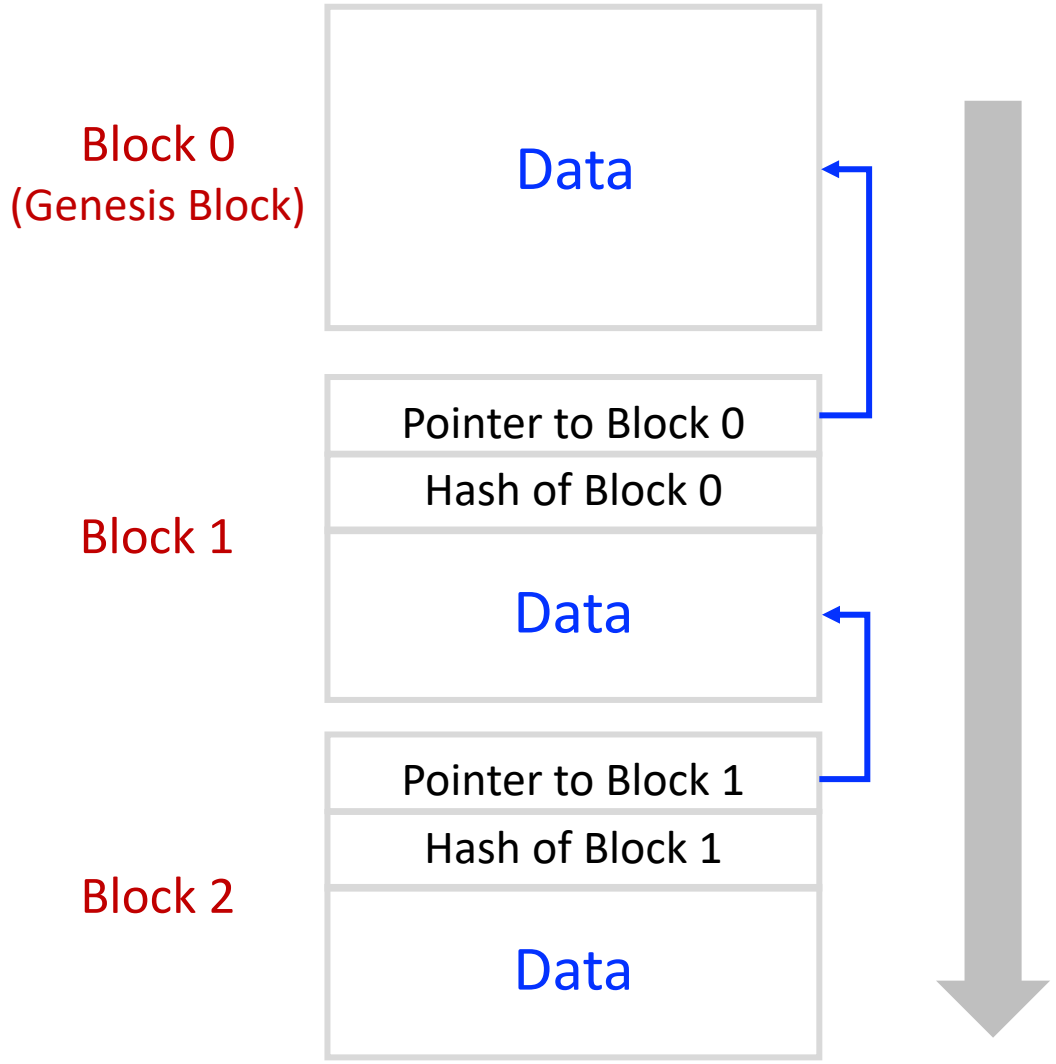
Blockchain is not cryptocurrency



- Blockchain is the technology behind cryptocurrencies like Bitcoin
- Blockchain provides an immutable distributed ledger made up of blocks
- Blockchain technology provides is a method of maintaining security of transactions without the presence of a central authority

What is Blockchain?

- A blockchain is a growing list of records, called blocks, that are linked using cryptography.
- Each block contains a cryptographic hash of the previous block a timestamp, and transaction data.
- By design, a blockchain is resistant to modification of its data.
- This is because once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks.

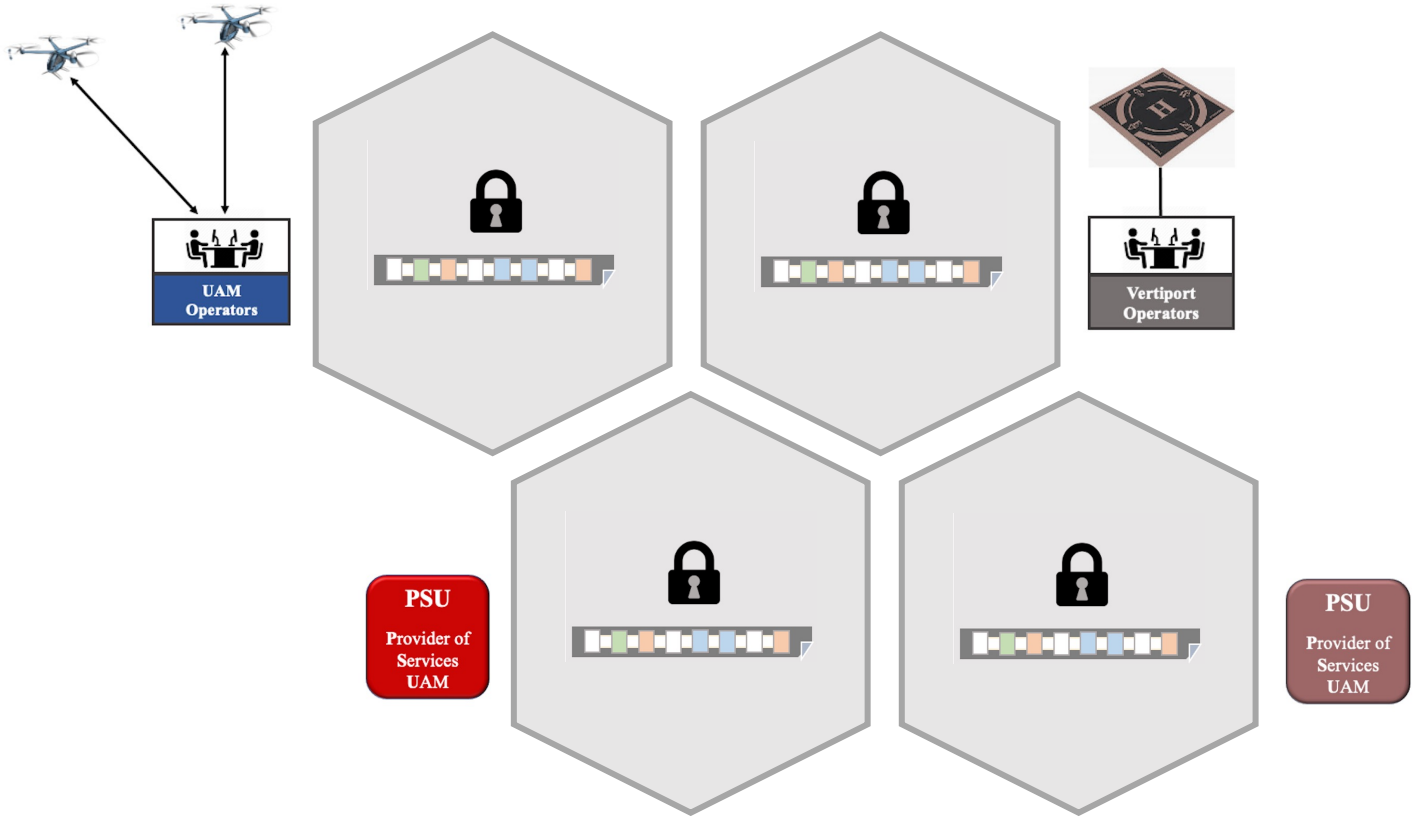


Public vs. Permissioned Blockchains

- 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.
- Permissioned blockchains
  - While transparency is a very desirable trait, enterprises don't want to use a network wherein anyone viewing 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.

Why Use Blockchain?

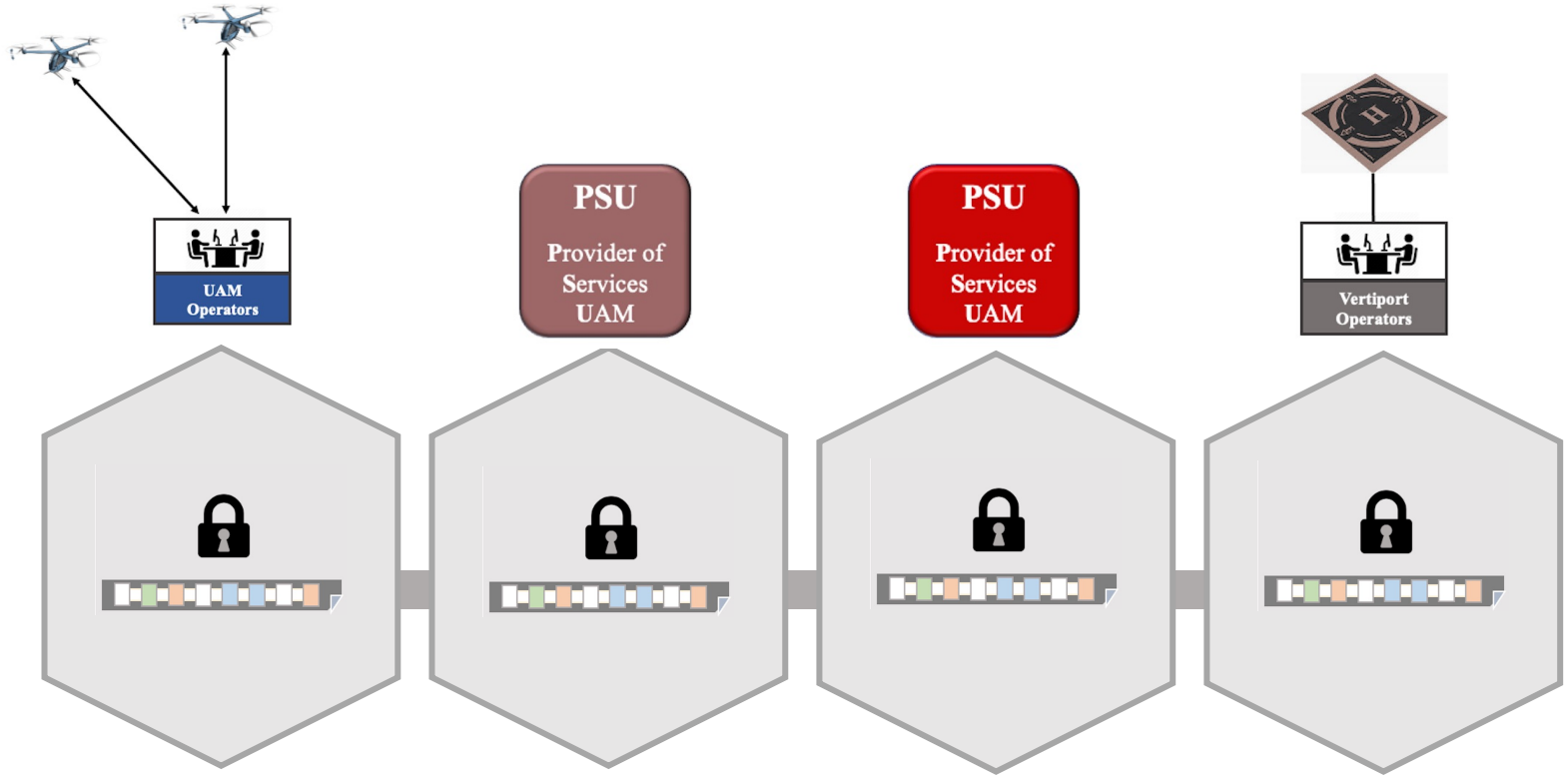
- A blockchain is a distributed ledger that records all the transactions that take place on the network
- A blockchain ledger decentralized
  - It is replicated across many network participants
  - Each participant collaborates in the blockchain maintenance
- The information recorded to a blockchain is append-only
  - A cryptographic techniques is used that guarantees that once a transaction has been added to the ledger it cannot be modified.



Why Use Blockchain?

A definition for immutability: *the state of not changing, or being unable to be changed*

- Immutability ensures that the no one can alter the state of the blockchain data
- Immutability also ensures that no one can intrude on the system



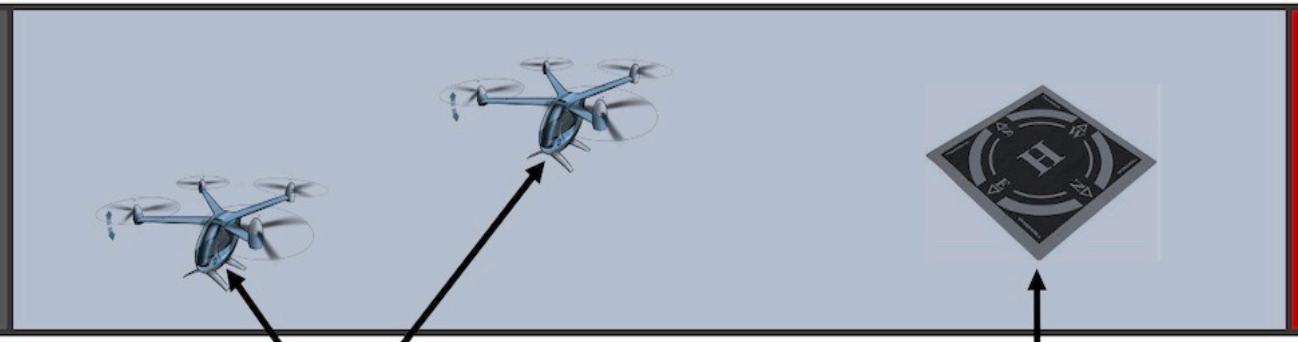
Consensus

- A key question is how parties in a blockchain reach consensus on how to agree to whether a transaction is valid and how changes can be made.
- The proof-of-work is a optional consensus model used in blockchain networks where a publishing node is allowed to publish the next block by expending time, energy, and computational cycles to solve a hard-to-solve, but easy-to-verify problem.
- The publishing node sends the block with a valid nonce to full nodes in the blockchain network. The full nodes can easily verify the solution using the nonce, add the block to their copy of the blockchain and distribute it to their peer nodes.

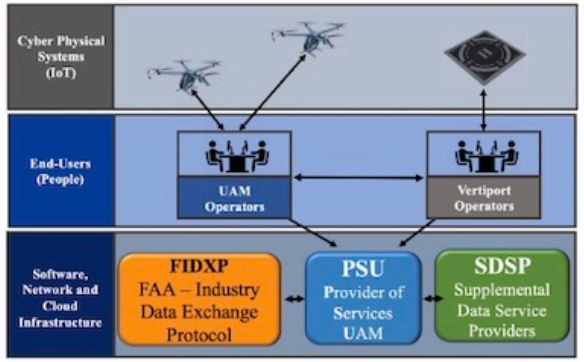
Why Use Blockchain for UAM

Blockchain Use Cases	Relevance
Identity Management	• Identity of the UAM system, pilot, vertiport or service
Payment/Settlement	• Charges related to leveraging UAM vehicle flights, vertiport take-off, landing and other UAM services
Provenance	• Immutable order of business transactions, leveraged in cases of conflict or accidents
Data Tracking	• Data tracking for flight scheduling, vertiport resources, UAM participant licensing, registration and UAM system identification characteristics

Threat Landscape

Cyber Physical Systems (IoT)		Cyber Physical Systems Threats	• Man-in-the-middle attack, leading to unauthorized access or data manipulation • Jamming, leading to the limitation of available data • Rogue UAS attempting to access UAM network
End-Users (People)	UAM Operators Vertiport Operators	End-Users (People) Threats	• Victim of spear phishing, leading to the interaction with malicious content • Exploitation of valid accounts, leading to the loss of credentials and system access
Software, Network and Cloud Infrastructure	FIDXP FAA – Industry Data Exchange Protocol PSU Provider of Services UAM SDSP Supplemental Data Service Providers	Software, Network and Cloud Infrastructure Threats	• Exploitation of valid accounts, leading to the loss of credentials and system access • Exploitation of public facing application, leading to corruption of data

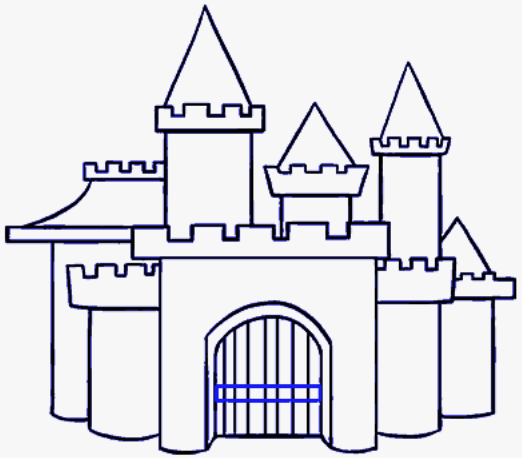
Threat Landscape



Cyber Physical Systems Threats	• Man-in-the-middle attack, leading to unauthorized access to sensitive data or data manipulation • Jamming, leading to the limitation of available data • Rogue UAS attempting to access UAM network
End-Users (People) Threats	• Victim of spear phishing, leading to the interaction with malicious content • Exploitation of valid accounts, leading to the loss of credentials and system access
Software, Network and Cloud Infrastructure Threats	• 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 research is to address four of the threats that may impact a UAM environment:
  - Man-in-the-middle attack, leading to data manipulation
  - Victim 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

Two Generals Problem



- Two armies, each led by a different general, are preparing to attack a fortified city.
- The armies are encamped near the city, each in its own valley.
- A third valley separates the two hills, and the only way for the two generals to communicate is by sending messengers through the valley.
- The valley is occupied by the city's defenders and there's a chance that any given messenger sent through the valley will be captured.

Two Generals Problem – Unreliable Communications

Attack at dawn

Not sure if message received

Not sure if ACK is received

ACK

Not sure if ACK² is received

ACK²

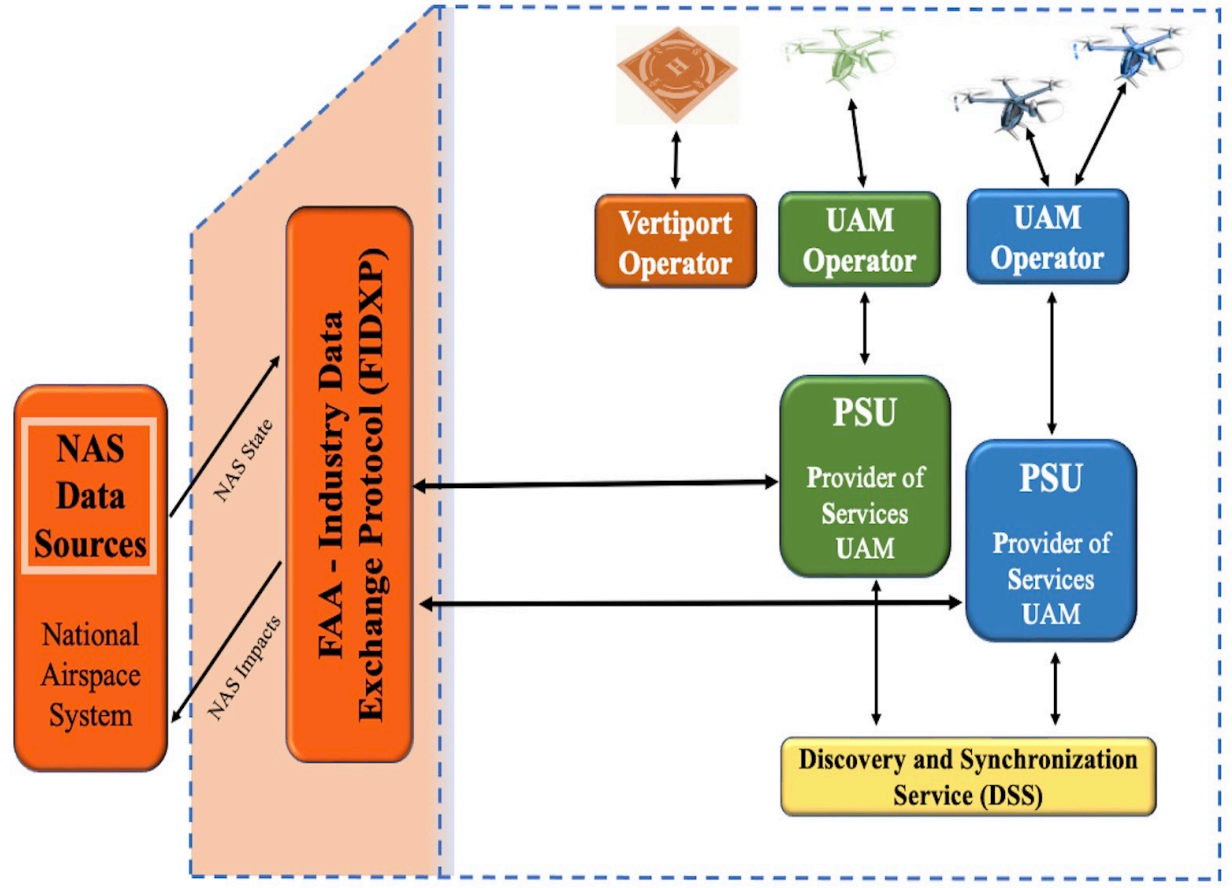
Not sure if ACK³ is received

ACK³

Never reach agreement

UAM Blockchain Use Case

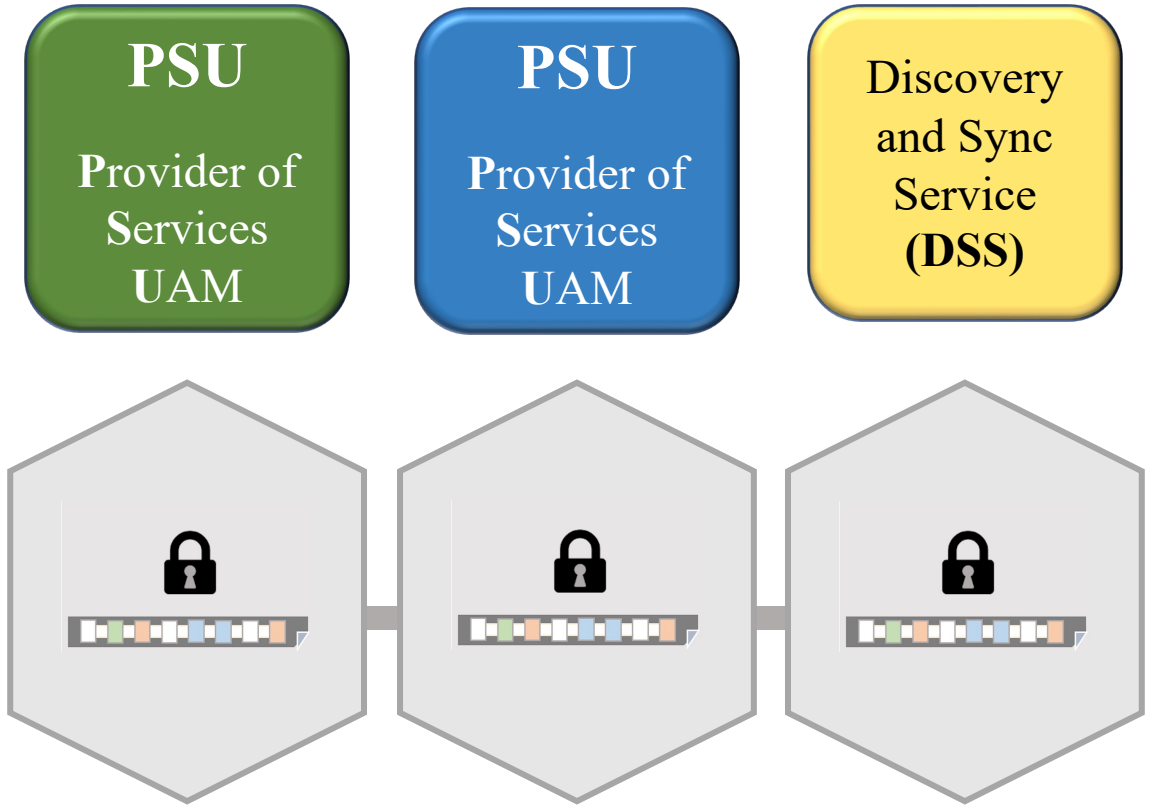
- Two UAM operators have flights planned to land at the same vertiport
- Pre-flight the UAM operator (green) will need to send flight intent via PSU to the DSS to determine if the flight plan is acceptable
- If flying in FAA controlled airspace, then pre-flight intent will need to also be approved by the ANSP function
- Risk: Any data compromise that leads to a loss of data integrity would put this operation at risk.



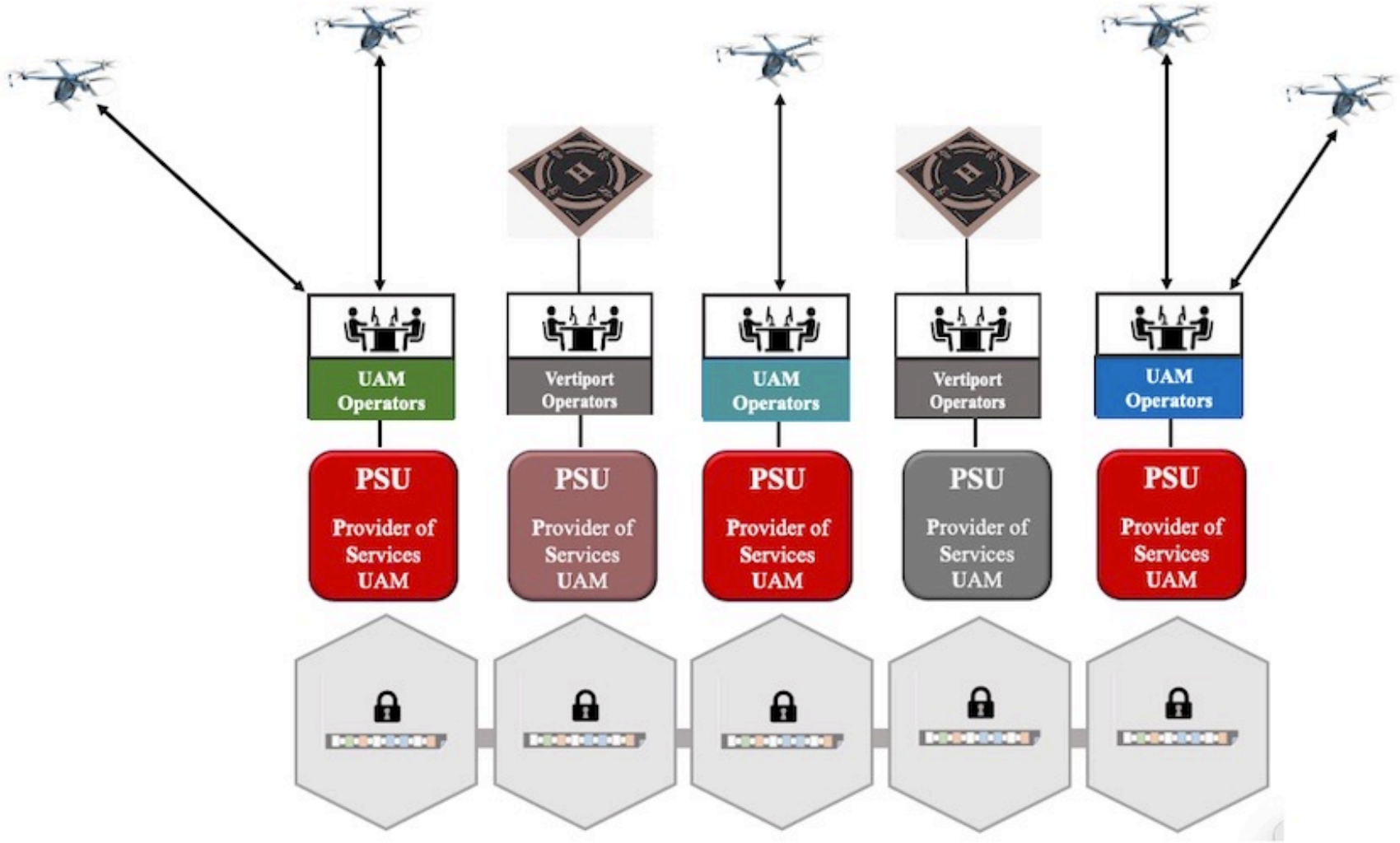
ANSP = Air navigation service provider

UAM Blockchain Use Case

- Blockchain embraces a peer-to-peer decentralized design that eliminates central authority (replaced by consortium authority)
- Blockchain distributed ledger technology provides independently verifiable ledger copies
- Once the data is in the ledger, it cannot be altered, by a cyber attack
- Enables parties that don't trust each other to work together off of a single version of shared truth



Questions


UAM Operators
Vertiport Operators
UAM Operators
Vertiport Operators
UAM Operators
PSU
Provider of Services UAM
PSU
Provider of Services UAM
PSU
Provider of Services UAM
PSU
Provider of Services UAM
PSU
Provider of Services UAM