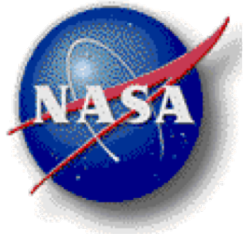


Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy

Ron Reisman
NASA Ames Research Center

AIAA Science and Technology Forum and Exposition 2019
Session ICC-02, Information and Command and Control Systems

San Diego, CA January 11, 2019

Not Presented due to Government Shutdown

Outline

- FAA NextGen Surveillance Mandate Challenges
- Air Traffic Use-Cases & Enterprise Blockchain
- Cryptographic Remedies

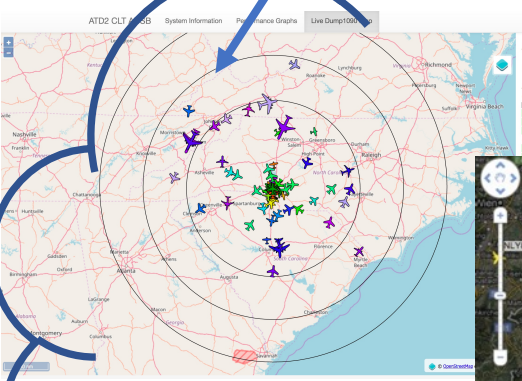
Automatic Dependent Surveillance – Broadcast (ADS-B)

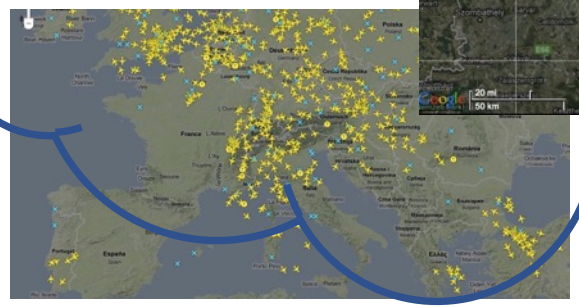
Plaintext

Plaintext

ADS-B Out

Air Traffic Management





FAA Mandate: ADS-B by January 1, 2020
ADS-B (plaintext) Security Concerns

- Privacy: FAA redacted ~10% Air Traffic from publication
    - Military (~4.7 %)
    - Corporate (~4.4.%)
- Authentication
- Signal Injection vulnerabilities (spoofing, denial-of-service)

Government Accounting Office Conclusions:

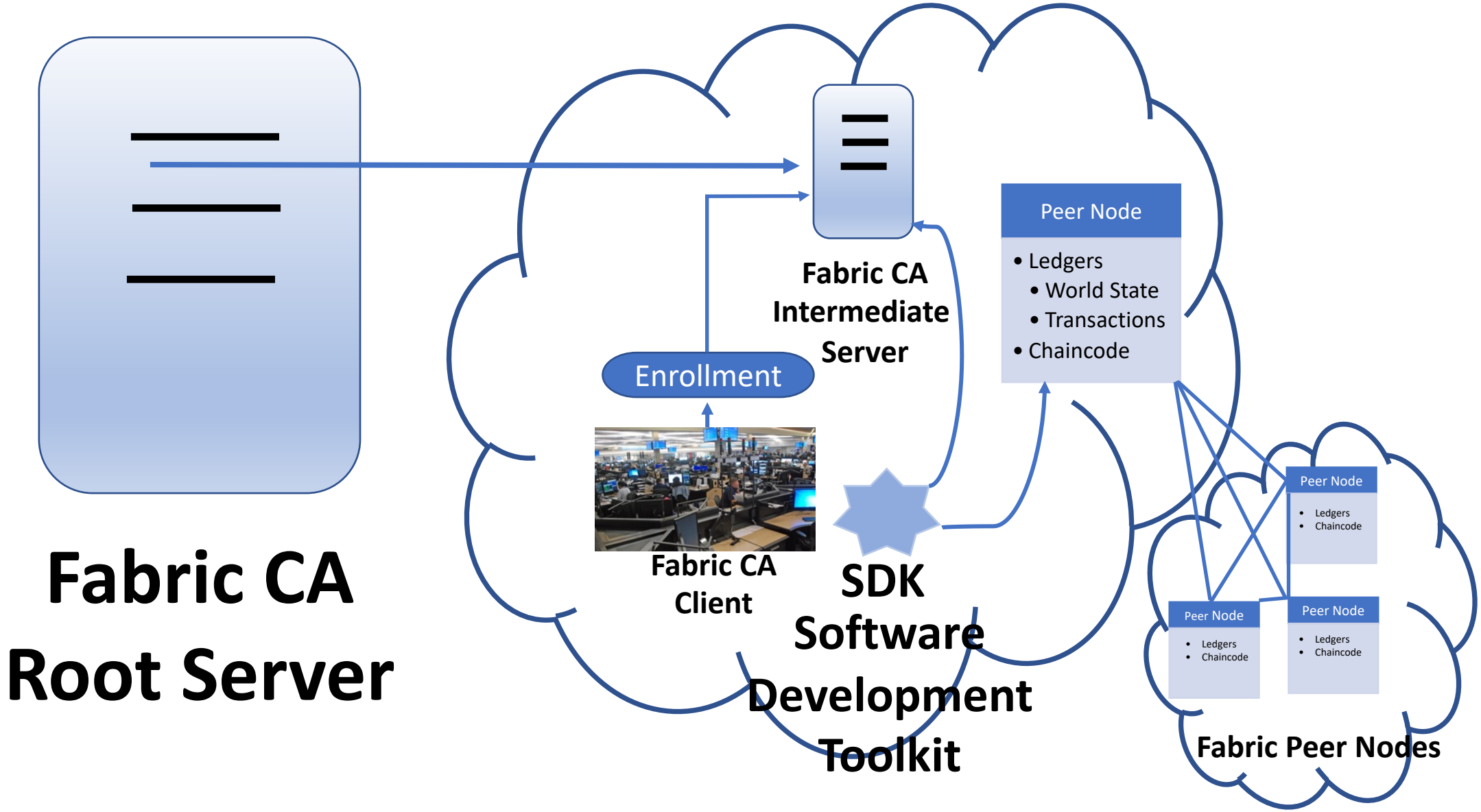
- *No approved solutions for ADS-B related risks*
- *DOD is not integrating NextGen requirements*
- *FAA will require ADS-B for Air Traffic Services*
- *Unresolved issues between DOD & DOT*

https://www.gao.gov/assets/690/689478.pdf

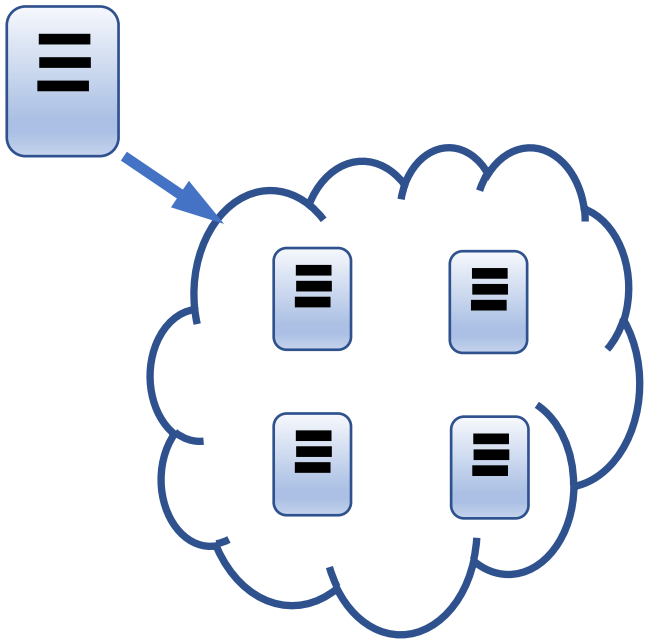
Hyperledger Fabric Differentiating Concepts

- **Private** and **Permissioned**
- **Enrollment** (not “Proof of Work”)
- **Membership Service Provider (MSP)**
- **Ledgers have two parts**
  - **World State**
  - **Transaction Log**
- **Chaincode (smart contracts)**
- **Peer Nodes**
  - **Run chaincode**
  - **Keep copies of ledger**

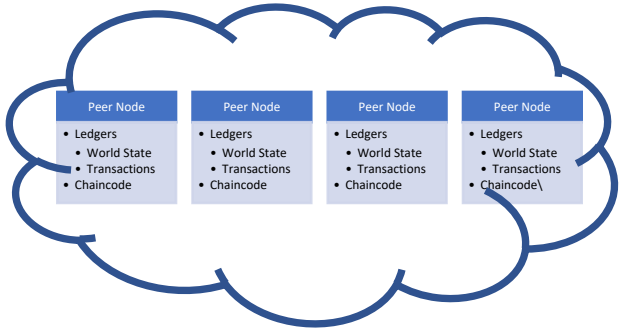
Hyperledger Fabric Certification Authority (CA)



Fab ric CA
Root Server



Geographically Separated
Fabric CA Intermediate Servers



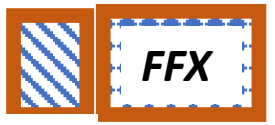
Geographically Separated
Fabric Peer Nodes

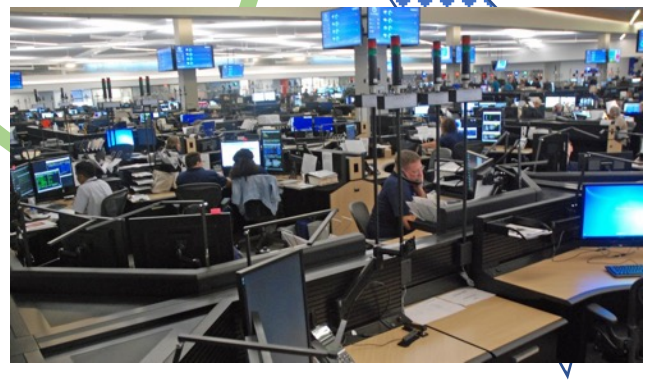
ADS-B transmitting Cyphertext

Membership

Membership

Air Traffic Management Services



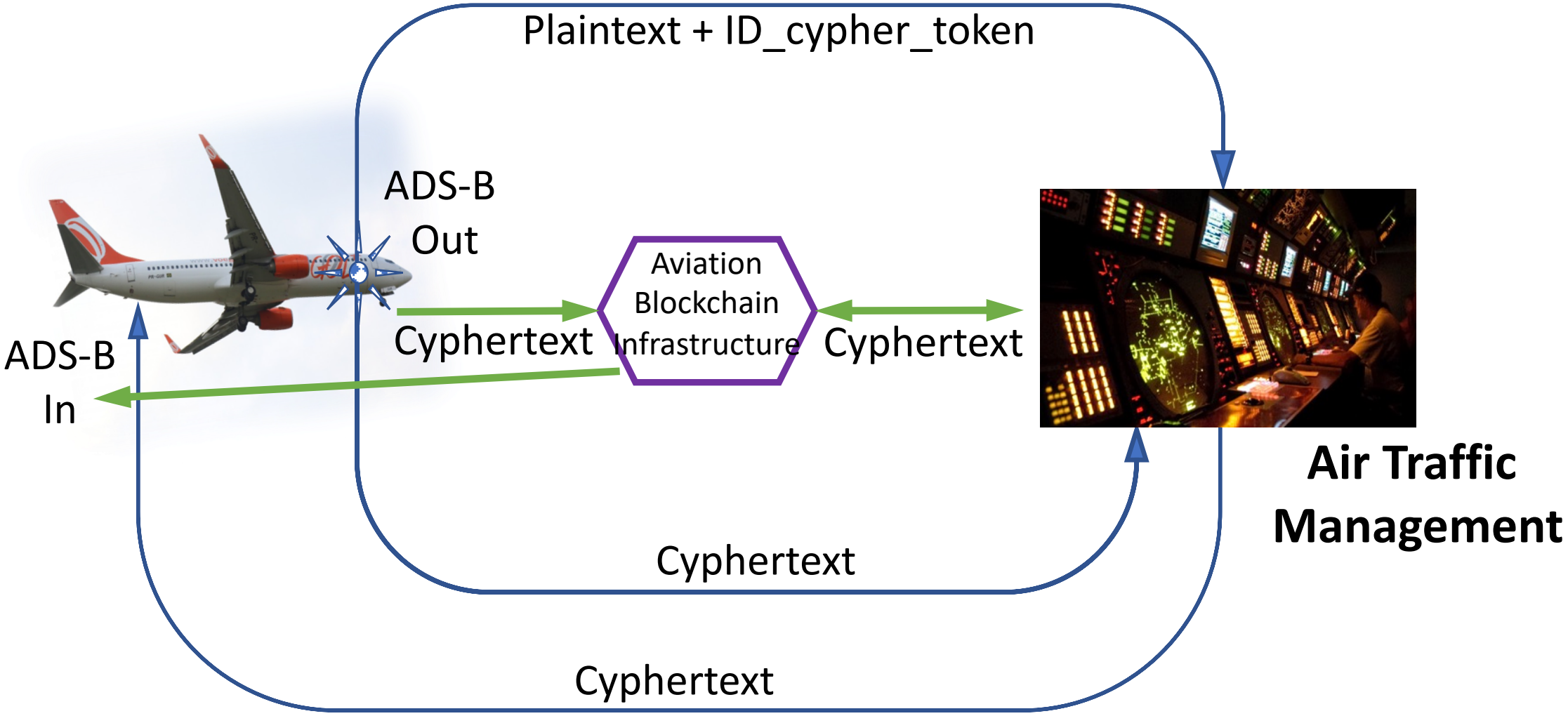


Airline Operation Services

!@#@%^
&*)_(_)(_
)}&^%$%
^&$^&%$

Unauthorized recipients see only unintelligible cyphertext

Aviation Blockchain Infrastructure (ABI) Enables ADS-B Authentication & Privacy



Concluding Remarks

- Open-source enterprise-oriented blockchain platform (Hyperledger Fabric) may be leveraged as a practical cryptographic solution to provide security and privacy for ADS-B
- Demonstration Needed: ADS-B hardware running cryptographic codes without any additional expense or modification
- Research Issue: How will future Collision Avoidance technology work reliably with encrypted surveillance signals?