Aero-Knowledge Proof

Privacy Preserving Proof-of-Compliance
for Aircraft Maintenance

Aviation Market

China Aviation Market
$2.7 trillion

Global Aircraft Fleet
31,000

Global Aircraft Fleet
38,000

China Aircraft Fleet
7690

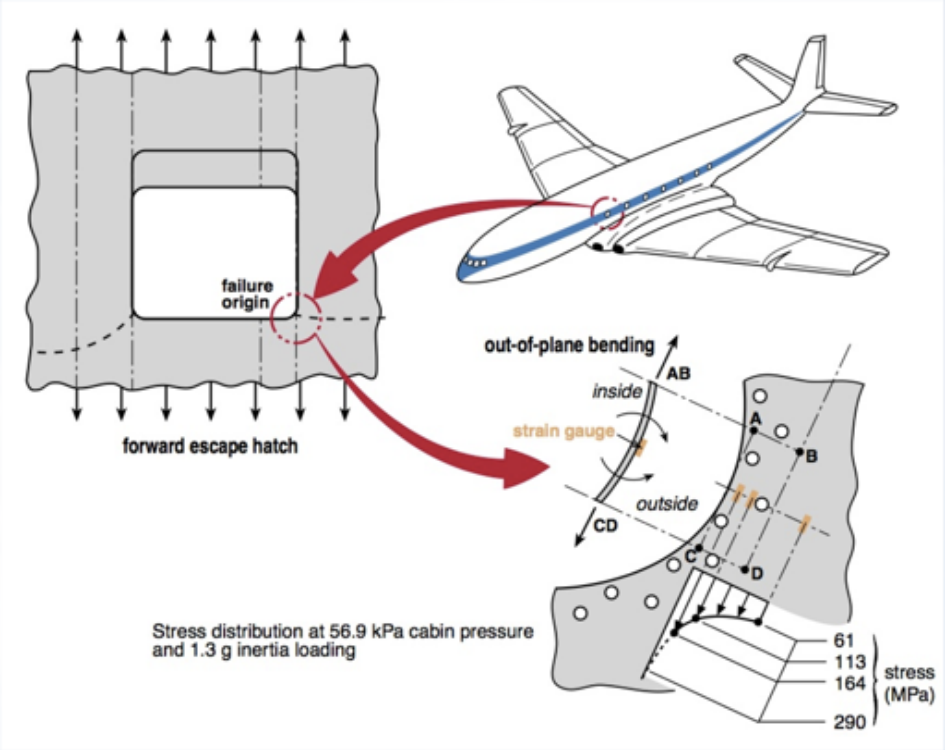
2017 **2028** **2039**

Global MRO Market
$115 billion

China MRO Market
$1.2 trillion

[1] Units of aircraft, i.e. any machine that flies, including helicopters and gliders
[2] All monetary amounts in US Dollars

Aviation Safety



Everyone cares

- No one would buy in an unsafe aircraft
- No one would fly in an unsafe aircraft

Everyone contributes

- Every incident is a learning experience
- Every investigation creates better regulations

TIMELY COMPLIANCE ENFORCEMENT CAN SAVE MORE LIVES

Air traffic man stabbed to death after jet crash

Air traffic controllers monitor flights at Zurich airport

By Fiona Fleck in Geneva and Dan McLaughlin in Moscow
12:01AM GMT 26 Feb 2004

An air traffic controller in charge in Switzerland when **two aircraft collided**, killing scores of Russian schoolchildren, has been stabbed to death in his home in a suspected revenge killing.

Peter Nielsen, 36, was on duty alone in the Zurich control room two years ago when he gave only 44 seconds' warning to a Bashkirian Airlines aircraft and a DHL cargo craft that they were too close.

Preliminary accident reports said he told the passenger plane to descend, overruling its crash avoidance system, and the two aircraft collided over southern Germany. All 71 people on board, including 45 children from Bashkortostan, an autonomous Russian republic 1,000 miles east of Moscow, were killed.

Switzerland
News » Russia »

EXTERNAL LINKS

Murder clouds skies over Zurich airport [25 Feb '04] - Neue Zürcher Zeitung

Skyguide in a state of shock [25 Feb '04] - Skyguide

Bashkortostan Today

In Switzerland

The private jet set

Alpine sheep herding

Extreme climbing

Kaloyev found guilty of intentional killing

OCT 26, 2005 - 17:19

PRIVACY IS IMPORTANT

A Russian man who lost his family in a plane crash has been found guilty by a Zurich court of the intentional killing of the air traffic controller on duty.

Kaloyev received an eight-year sentence for killing the Danish air traffic controller

(Keystone)

Vitaly Kaloyev was sentenced to eight years in prison. Russian authorities said they would seek his extradition so that he can serve his sentence in Russia.

The Zurich cantonal court judged that the accused wanted to kill his victim, at least after the first blows with the knife. Kaloyev's wife and two children were killed in the 2002 Überlingen crash.

The victim, a 36-year-old Dane, was on duty when two jets collided in mid-air in Swiss airspace in July 2002. He was stabbed to death in front of his wife at the family home near Zurich on February 24, 2004.

Kaloyev acknowledged in court that he must have killed the victim but said he could not remember the incident. The 49-year-old told the court that he never wanted to cause physical suffering to anybody.

Ulrich Weder, the Zurich cantonal prosecutor, had asked the court to sentence Kaloyev to 12 years' imprisonment. He argued that the crime was clearly premeditated homicide, but fell short of murder because Kaloyev had not acted out of malice.

Call for leniency

Kaloyev was arrested the day after the killing in Zurich. His lawyers pleaded for manslaughter, saying that the defendant was tormented by great psychological distress at the time of the crime. They asked for a more lenient sentence of three years.

The crash killed 71 people, including Kaloyev's wife and his two children who were on their way to visit him in Spain.

The trial is being closely followed in Russia, especially in Bashkortostan and North Ossetia, where most of the victims, including Kaloyev's family, came from.

Problem

Air regulation compliance: <u>complete</u>, but not <u>private</u> nor <u>timely</u>

CURRENTLY
Compliance enforcement is intermittent or reactive [to incidents]

CURRENTLY
Compliance enforcement may inadvertently reveal sensitive information of aircraft operators

CURRENTLY
Compliance enforcement does not respect nor protect the privacy of workers[1]

IDEALLY
Compliance enforcement should be timely, i.e. "real-time"

IDEALLY
Compliance enforcement does not reveal any confidential & linkable data

IDEALLY
Compliance enforcement keeps their identities secret but keeps them accountable

[1] such as Maintenance, Repair, Overhaul (MRO) workers, ATC staff, pilots, etc

Solution

BLOCKCHAIN

Traceable
Provenance
+
Automatic
Reconciliation

↓

Timely
Complete
Records

ACCOUNTABLE
ANONYMOUS

CRYPTOGRAPHY

Zero-Knowledge Range Proofs
for data that proves
an aircraft is still compliant
+
Accountable Ring Signatures
for data attesters
that preserve their identities
unless an investigation triggers
full revelation

↓

Private
Records

Example:
A part that does not need to be replaced because the miles flown is under the trigger to replace it

Example:
technicians, engineers, ATC, pilots, etc

Stakeholders

Issuers

issue attestations on aircraft flight and maintenance data to satisfy the regulations

Stewards

steward (i.e., are in control of) attested data to prove compliance

Verifiers

verify that regulated entities are compliant and updates rules when risks evolve

Beneficiaries

benefit from cost-effective, real-time proof-of-compliance for aircraft assets

Stakeholders

Issuers

also known as

Aircraft Data Attesters ("Attesters")

Stewards

also known as

Aircraft Operators ("Operators")

Verifiers

from governments are

Civil Aviation Administrative Authorities ("Regulators")

Verifiers

with business goals are

Entities that buy and sell aircraft, including leasing and financing ("Financiers")

Stakeholders: Attesters

Issuers ("Attesters") issue attestations on aircraft flight and maintenance data to satisfy regulations

Manufacturers

whose equipment provide signed readings of sensors

Technicians and Engineers

who attest to the state of examined components

Air-Traffic Controllers

who attest to aircraft departure and arrival at various locations

Stakeholders: Operators

Stewards ("Operators") steward (i.e., are in control of) attested data to prove compliance

Airline Operators

operate aircraft
for moving people

Logistics Companies

operate aircraft
for moving things

Civil Reserve Air Fleet

operate civilian aircraft
for emergency military reasons

Stakeholders: Risk-Bearers

Verifiers ("Risk-Bearers") verify compliance of regulated entities & updates rules when risks evolve

Regulators

regulate all aspects of civil aviation over a jurisdiction's airspace and adjacent waters

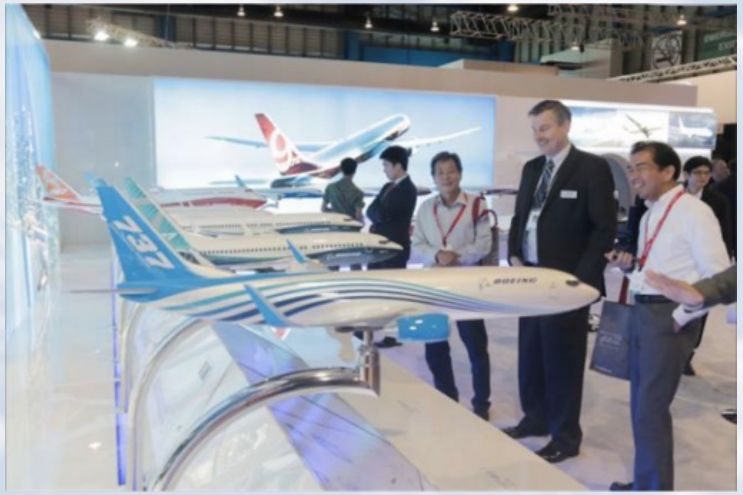
Auditors

investigates civil aircraft accidents within a jurisdiction's airspace and adjacent waters

Financiers

buy and sell aircraft, including leasing and financing for profit or as collateral

Why Corda



Each aircraft has unique sets of stakeholders

Not all nodes have the same access nor validation privileges

Flexibility in adding and removing specific stakeholders

Corda Nodes Design

	Type A	**Type B**	**Type C**
Who	Attesters	Operators	Risk-Bearers
Mission	Creation of records	Administration of records	Inspection of records
Role	• Attest data • Adds commitment not by encryption (which is "plaintext") • Signs attestation with ring signature	• Keeps data • Counter-signs commitments • Generates zero-knowledge proofs for verification requests	• Requests data via de-commitment scheme • Inspects zero-knowledge proofs for proof-of-compliance
Relations	Type B only	Type A and Type C	Type B only

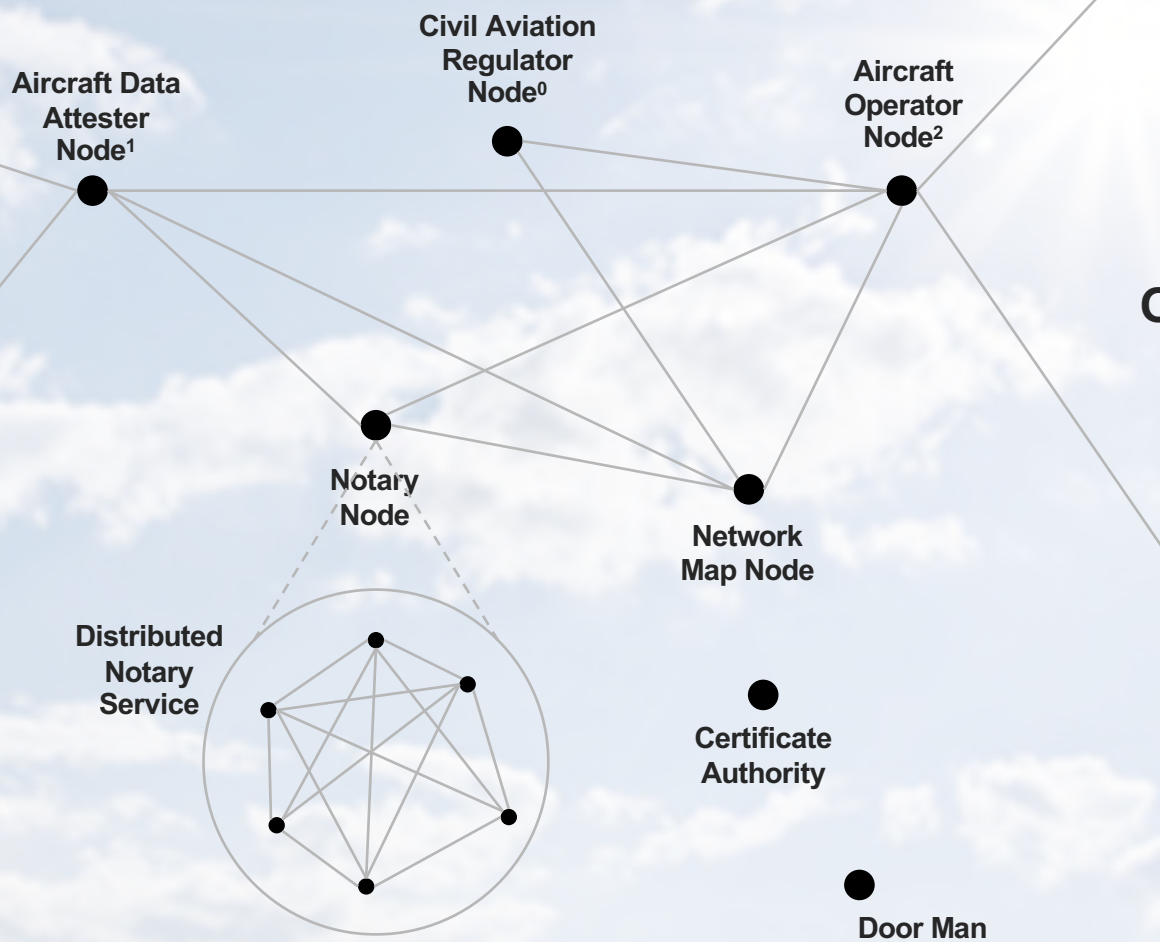
System Nodes

- Notary Node: may be provided by some regulators
- Certificate Authority: may use existing CA or self-sovereign CA
- Door Man: recommend an auditor or compliance body

Corda Network Design

Self-Sovereign Identity
1. Provide proof-of-credentials
2. Oversee authentication
3. Manage access control

Record Management Module
1. Sign-off new data via smart contract
2. Supervise disputes or clarifications
3. Accommodate requests for audits



AIRCRAFT MAINTENANCE

AIRCRAFT OPERATIONS

Record Management Module
1. Verify data attester's identity and role
2. Access aircraft record information
3. Submit new data via smart contract

Assets Oracle[3]

Transmit relevant information to smart contract for aircraft record upkeep

[0] Multiple Civil Aviation Regulators exist
[1] Multiple Aircraft Data Attesters exist
[2] Multiple Aircraft Operators exist
[3] Each Aircraft Operator has its own Assets Oracle

Record Attestation Process

Issuer

1. $ATC_{Airport\ A}$ observes the departure of an aircraft; ATC_A commits data and signs a new flight record entry with ring signature.

Steward

2. Operator receives attestation of aircraft departure from *Airport A*; Operator signs the new flight record.

Previous flight record is invalidated as new values are expected

3. $ATC_{Airport\ B}$ observes aircraft has arrived; ATC commits new flight record entry and signs with ring signature.

4. Operator receives attestation of aircraft arrival at *Airport B*; Operator signs the new flight record.

Maintenance records expect new values

5. MRO inspects and works on the aircraft; for each part inspection or part replacement, a relevant technician attests to data for new maintenance record, commits, and ring-signs.

6. Operator receives attestation of aircraft maintenance state; Operator signs on the new maintenance record.

Record Inspection Process

Steward

Verifier

1. Verifier requires a proof-of-airworthiness for an aircraft

2. Verifier requests aircraft by referencing identifiers of relevant components

3. Operator confirms stewardship over requested aircraft

4. Verifier requests **de-commitment** of specific and relevant data

5. Operator approves de-commitment of requested data, then generates the **proof of linkability** of commitment and de-commitment, and the **zero-knowledge range proof** of requested data

6. Verifier inspects requested all proofs of the requested aircraft

Benefits

Real-Time Accountability

Reducing risk of aircraft accidents
Reducing risk of unexpected devaluation

Accountable records with Anonymity

Protecting sensitive information of operators
Protecting identities of individual workers

Risks

All-or-nothing adoption

Network requires regulators

Network requires operators

Network requires MRO companies

Regulatory risk

Civil aviation regulators may not be enthusiastic about changes

Geopolitics may affect adoptions across jurisdictions

Next Steps: Go-to-Market

- Small Market: private or business aviation
- Small Jurisdiction: Macau SAR
- All of the above?

Next Steps: R&D

PROBLEM	SOLUTION	CHALLENGE	FUTURE
Compliance enforcement is intermittent or reactive, but should be in "real-time".	Blockchain: automatic reconciliation of flight and maintenance records.	Corda as of now has no framework for zero-knowledge proofs nor ring signatures.	Corda needs a cryptography library to support zk-proofs and commitment schemes in general.
Compliance enforcement may reveal sensitive information and breach personal privacy of workers, but all data should prserve privacy.	Cryptography: commitment schemes of records with zero-knowledge range proofs and accountable ring signatures for data attesters.	Corda CA and network map nodes are omnipotent and omnipresent, so Corda needs a framewwork for privacy-preserving cryptography.	Corda needs to support signing by ring signature rather than just the traditional signing with public-key infrastructure.