TADOREA

KNOWLEDGE DISCOVERY FOR AVIATION

OPEN DATA

VS

CRYPTO-ECONOMICS

IN AVIATION

TADOREA

KNOWLEDGE DISCOVERY FOR AVIATION

innaxis

"Progress in science depends on
new techniques, new discoveries and new ideas,
probably in that order"

Sydney Brenner, biologist, 2002 Nobel Prize Winner

THE PROBLEM: BUILDING DATA-DRIVEN SYSTEMS

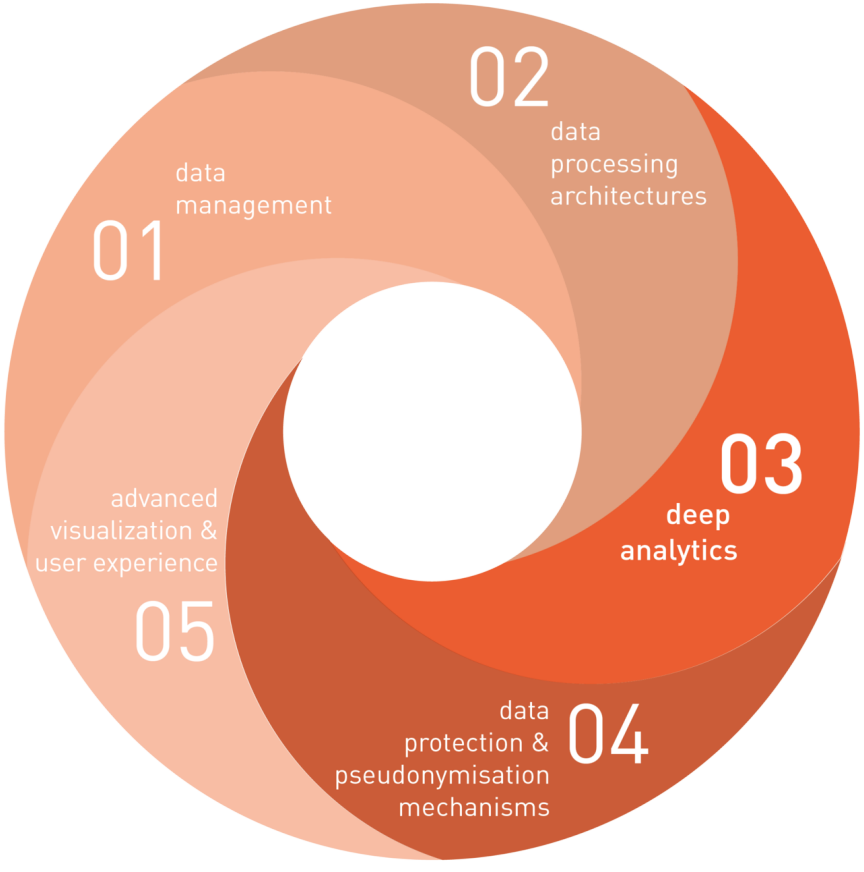
1 NON-OPEN DATA AND DATA INTELLIGENCE
2 A WORKAROUND: DATA MODELS

A SOLUTION: THE CRYPTO-ECONOMIC WAY

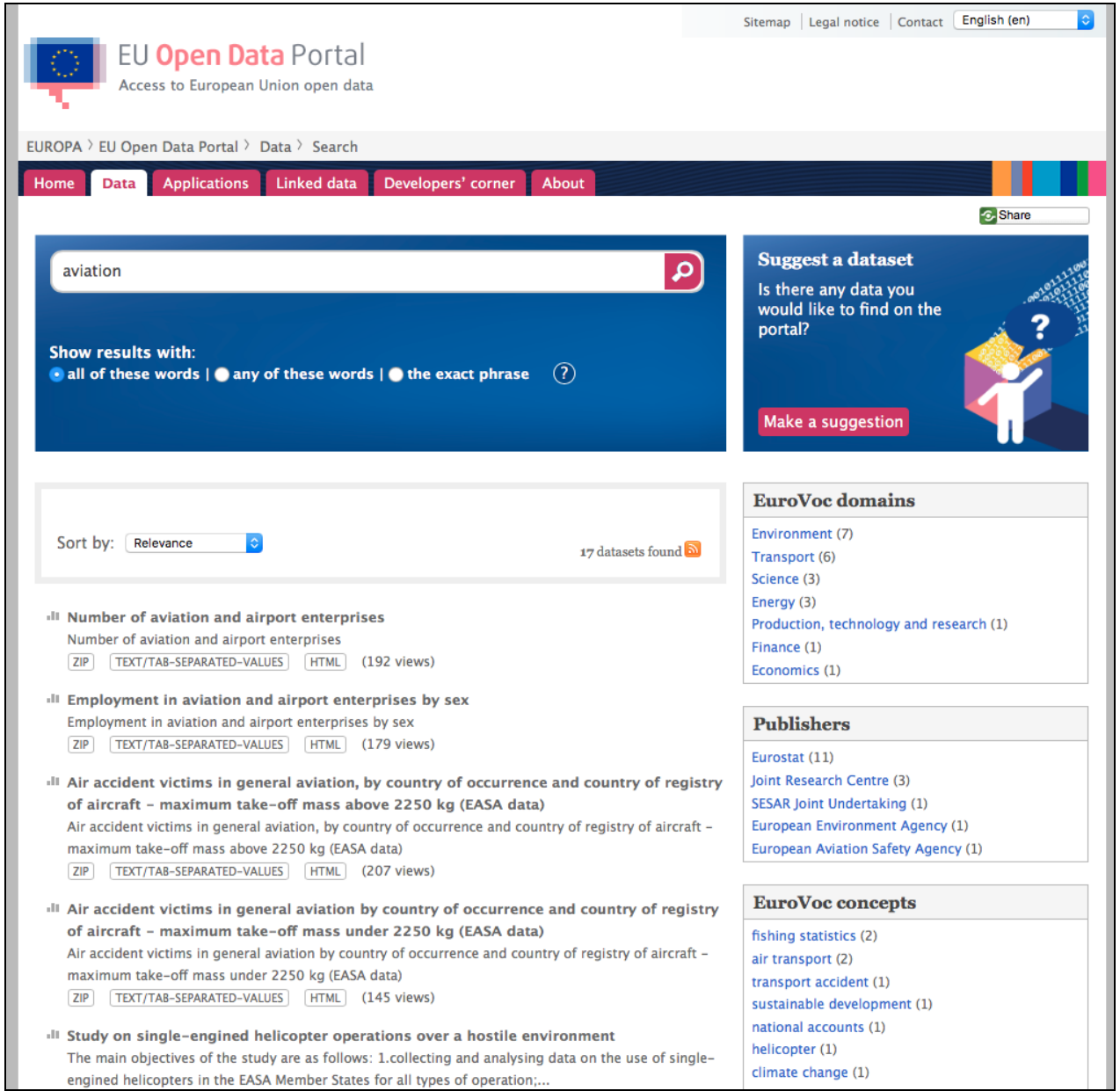
3 CONTEXT: THE BLOCKCHAIN
4 INFORMATION SECURITY - DEFINITION & TOOLBOX
5 GOVERNANCE PROTOCOLS

1
OPEN DATA AND DATA INTELLIGENCE

02
data
processing
architectures
data
management
01
03
deep
analytics
advanced
visualization &
user experience
05
data
protection &
pseudonymisation
mechanisms
04


02
data
processing
architectures
data
management
01
03
deep
analytics
advanced
visualization &
user experience
05
data
protection &
pseudonymisation
mechanisms
04

EUROPEAN COMMISSION ON OPEN DATA



WHO OWNS THE DATA?

WHICH DATA "SHOULD BE" CONFIDENTIAL OR SECRET?

EXAMPLES NON-OPEN DATA IN AVIATION

Airlines

Safety incidents	sensible
Fuel consumption	competitive
Passengers, or passenger connectivity	competitive
Sources of delay	competitive

ANSP's

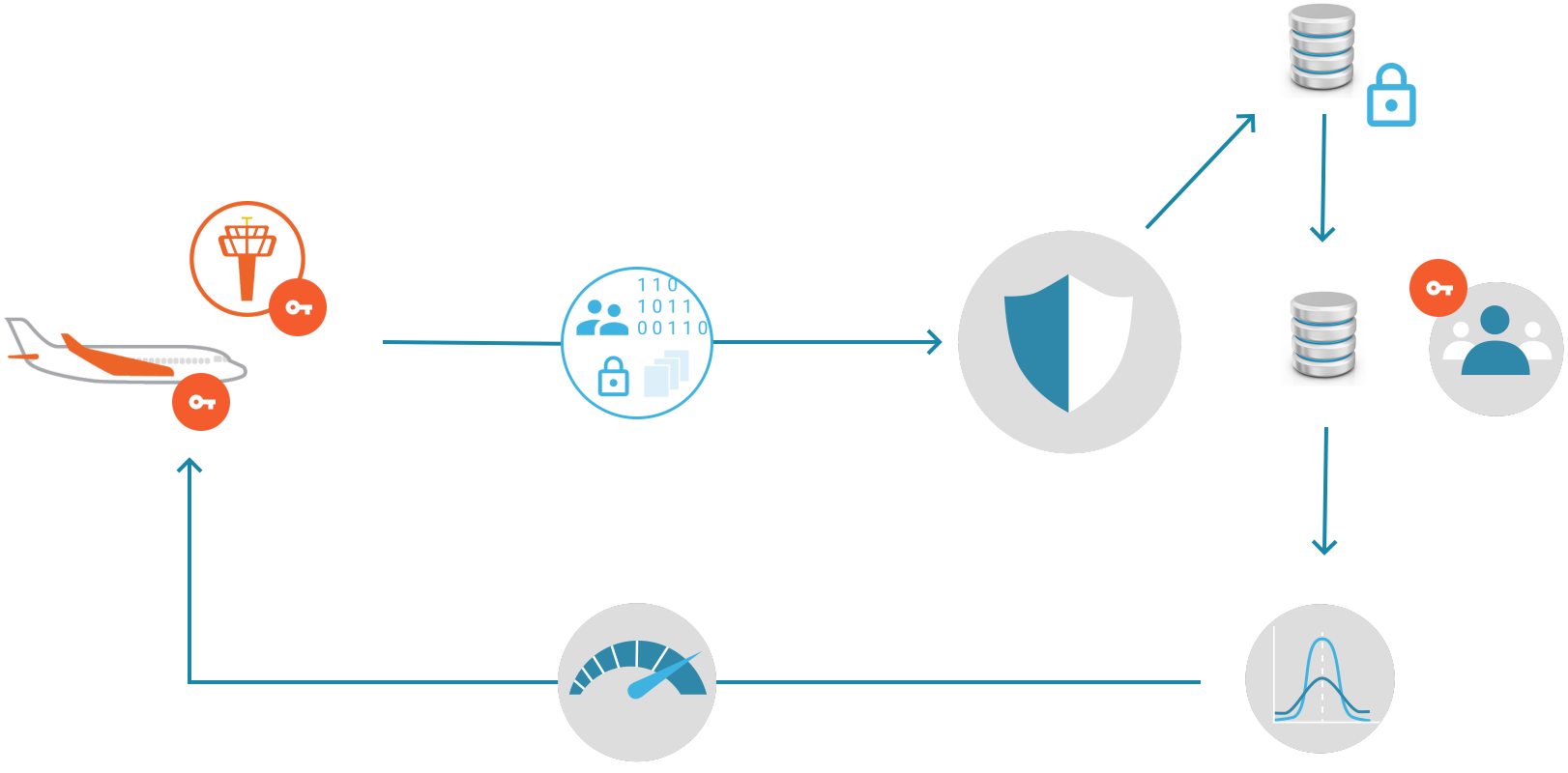
Safety incidents	sensible
Staff allocations, regulations	sensible
Capacity constraints	sensible
ATCO workloads	sensible

EXAMPLES OF DATA-DRIVEN SYSTEMS THAT WOULD BENEFIT OF CONFIDENTIAL DATA

Emission policies
Fuel policies
Prioritisation in departure, flow or arrival
Safety policies
Resource allocation
ATM procedures effectiveness
??? ???

THE DEFAULT APPROACH

the "trust" issue



THE DEFAULT APPROACH

the software supply chain attack issue

FORTUNE

DATA SHEET

CYBER SATURDAY EDITION BY ROBERT HACKETT

SHARE THIS | SHARE THIS | FOLLOW | SUBSCRIBE | ANON TIP

SEPTEMBER 23, 2017

An insidious attack trend has been catching my eye lately. It's called the software supply chain attack.

The scheme goes like this: Hackers compromise a trusted software vendor, subvert its products with their own malicious versions, and then use the tainted formulation to infect customers — thereby bypassing internal security controls and easily spreading malware far and wide. Customers, careful to keep their software up to date, don't think twice about downloading the latest iterations. That's good digital hygiene, after all.

At least that's what we've been trained to think. Cisco researchers exposed one of these sneaky incursions earlier this week. The hacking operation sabotaged CCleaner, a popular piece of computer cleaning software distributed by Avast, a Czech antivirus firm. (Morphisec, an Israeli cybersecurity startup, had discovered the compromise too.)

Here's what happened: In August, some unknown hacking group inserted a backdoor into the CCleaner software, which was then dutifully installed on more than 700,000 machines. With that foothold, the attackers then attempted to drill down deeper into the networks of at least 18 big tech company targets, including Google, Intel, Microsoft, Samsung, HTC, and Cisco. Presumably, the intruders sought trade secrets.

This is only the most recent example of such an attack. Earlier this year hackers compromised MeDoc, a piece of accounting software developed by a Ukrainian tech firm, in order to spread a destructive strain of ransomware, dubbed NotPetya, through its update mechanism. The attack crippled operations at big companies, ranging from Danish shipping giant Maersk to U.S. pharma company Merck. Similarly, Kaspersky Labs, the lately besieged Russian cybersecurity firm, found a backdoor in server management software from the U.S. and South Korean tech firm NetSarang that infected hundreds of banks and other

fortune.com/newsletter/cybersaturday/?scrape=1

CONCLUSION: DATA "MINING"

2
A WORKAROUND: DATA MODELS

DATA MODELS: EXAMPLES

ATM Seminar USA & Europe
AIR TRAFFIC MANAGEMENT
RESEARCH AND DEVELOPMENT

Fuel Burn Estimation Modeling for ATM Benchmark Applications Perspectives from an International Collaboration
Authors: *Gabriele Enea (MITRE), Jesper Bronsvoort (Airservices Australia), Hartmut Fricke , Christian Seiß, Judith Rosenow, (TU Dresden), Almira Ramadani, Mike Paglione (FAA)*

A Bayesian Network Model of Pilot Response to TCAS Resolution Advisories
Authors: *Robert Moss, Edward Londner (MIT Lincoln Laboratory)*

Bayesian Inference of Aircraft Initial Mass
Authors: *Junzi Sun, Joost Ellerbroek, Jacco Hoekstra (Delft University of Technology)*

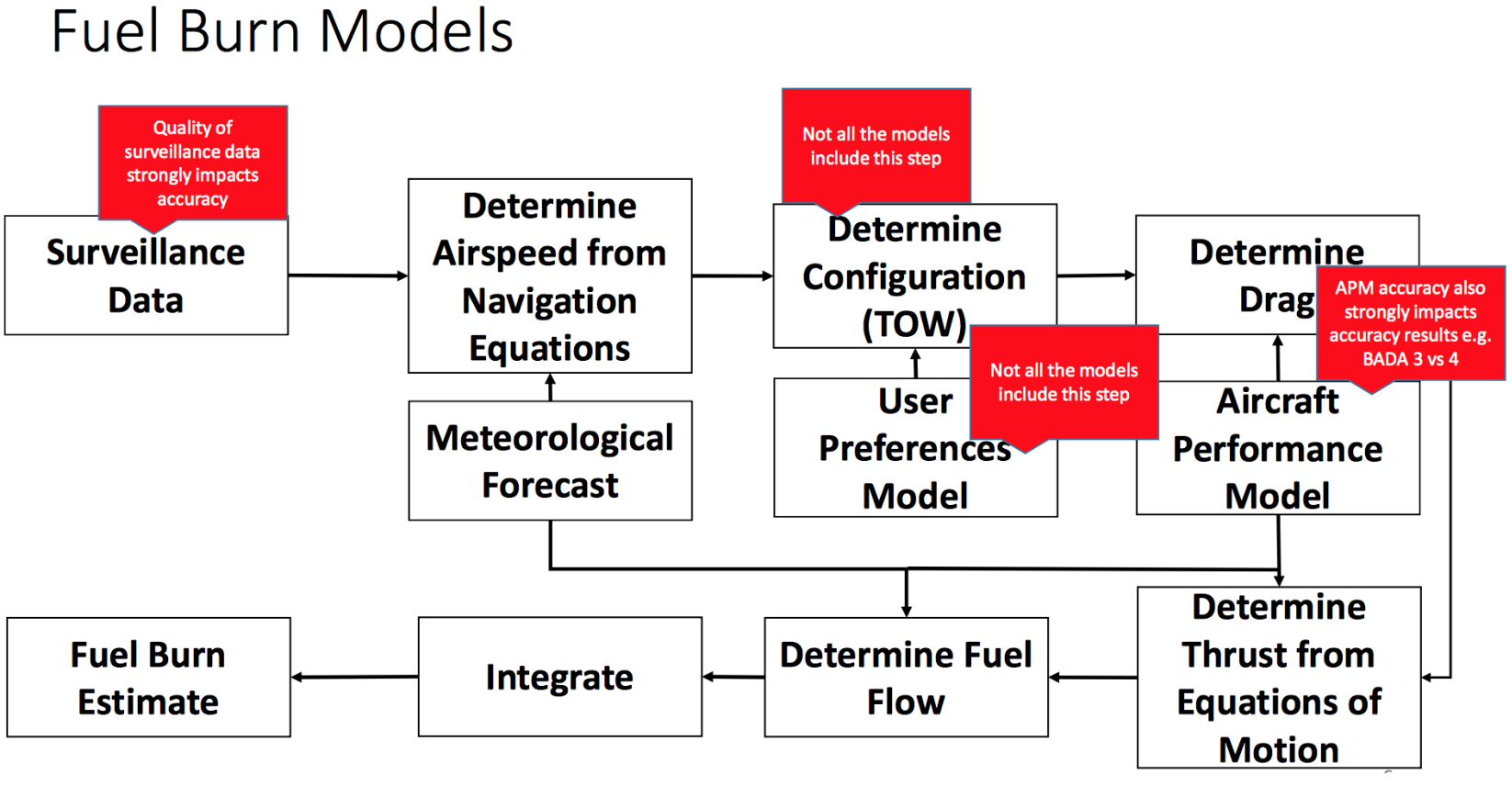
Modeling Aircraft Performance Parameters with Open ADS-B Data
Authors: *Junzi Sun, Joost Ellerbroek, Jacco Hoekstra (Delft University of Technology)*

Predicting Performance of Ground Delay Programs
Authors: *Alexander Estes, Michael Ball, David Lovell (University of Maryland)*

A Comparative Analysis of Models for Predicting Delays in Air Traffic Networks
Authors: *Karthik Gopalakrishnan, Hamsa Balakrishnan (MIT)*

Open source software and crowd sourced data for operational performance analysis
Author: *Rainer Koelle (EUROCONTROL)*

DATA MODELS: EXAMPLE



Taken from: ATM Seminar, 2017 - Gabriele Enea, Ph.D. Engility Corporation, Jesper Bronsvoort, Ph.D.,, Airservices Australia Hartmut Fricke, Ph.D., TU Dresden, Almira Ramadani, Mike Paglione, FAA Christian Seiß, Judith Rosenow, Ph.D., GfL

DATA MODELS: EXAMPLE

"As it is clear from the cross-comparison of various models, with different levels of complexity,

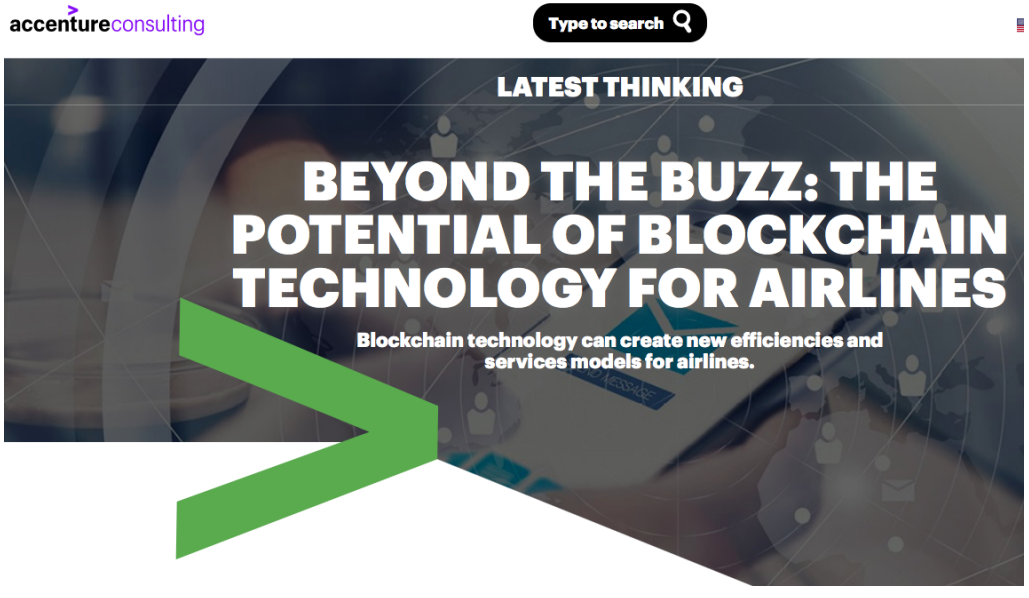
the accuracy of the models is not always adequate to the changes that model users want to observe.

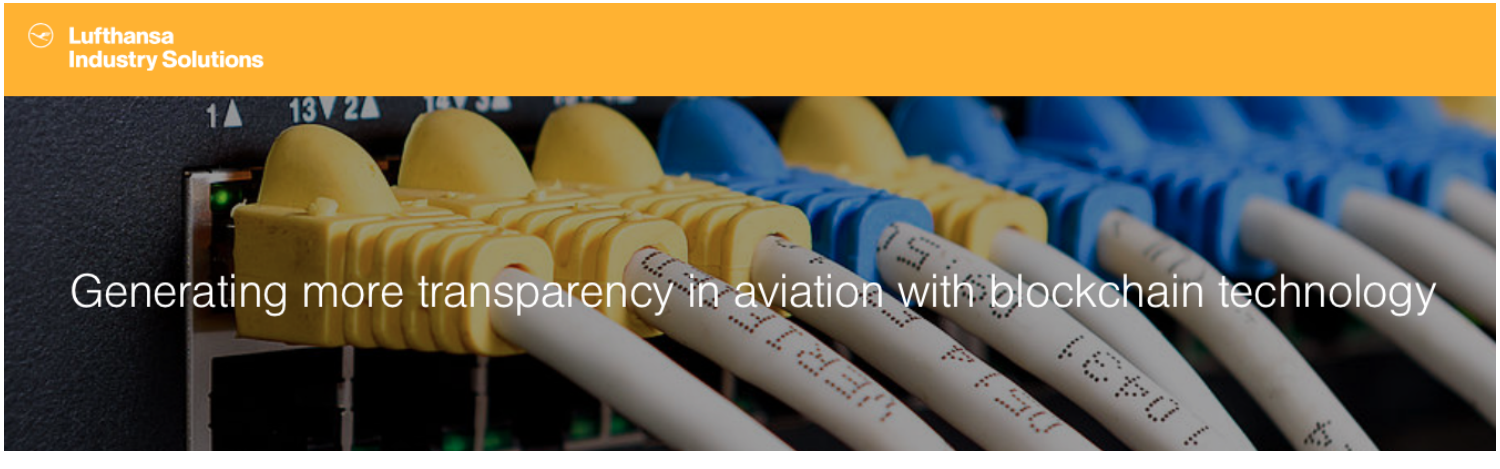
This is not just the limitation of the models itself, but also the accuracy of the input data"

Taken from: ATM Seminar, 2017 - Gabriele Enea, Ph.D. Engility Corporation, Jesper Bronsvoort, Ph.D.,, Airservices Australia Hartmut Fricke, Ph.D., TU Dresden, Almira Ramadani, Mike Paglione, FAA Christian Seiß, Judith Rosenow, Ph.D., GfL

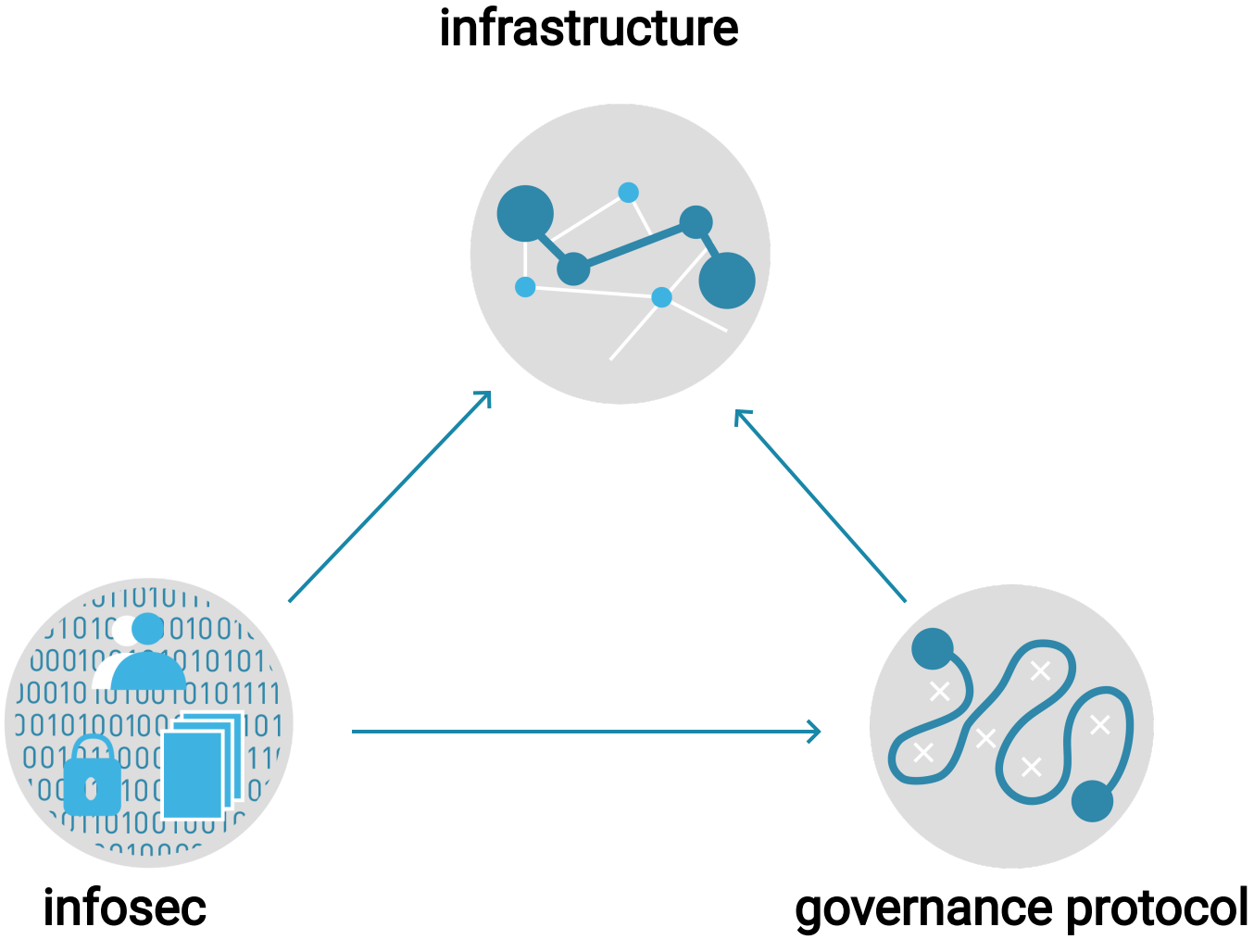
3
CONTEXT:
THE BLOCKCHAIN

BLOCKCHAIN PROTOCOL





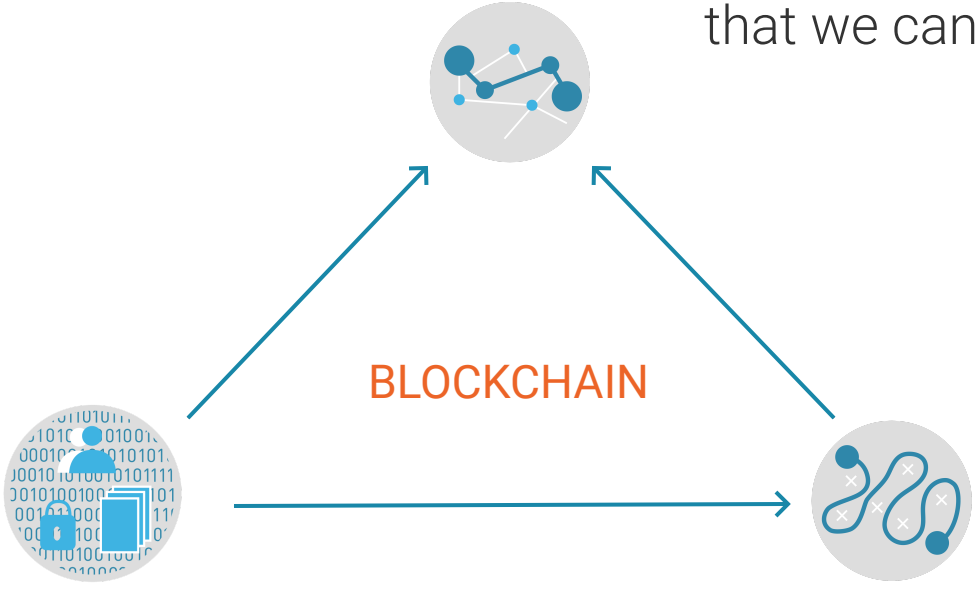
A CRYPTO GOVERNANCE PROTOCOL



THE 2009 NAKAMOTO PROTOCOL

infrastructure

Can we build an infrastructure that we can trust?



infosec

Do we need to protect secrets but still compute?

governance protocol

Do we need to design a system or procedure based on those secrets?

4

INFORMATION SECURITY - DEFINITION & TOOLBOX

INFOSEC: DEFINITION & GOALS

Definition:

is the practice of preventing

unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction

of secret information

Goals:

- Privacy
- Confidentiality of communications
- Message integrity
- Compute any math function over private data
- Reach consensus over the use of common resources through private data, f.i. through blind auctions
- ... ...

TOOLBOX FOR INFOSEC

Strict rule: do not use proprietary crypto primitives or even implementations

- Encryption, to preserve privacy and confidentiality

- Digital signatures, to prove sender identity

- Hashes: consistency of a chain of messages, build merkel data structures,...

- Secure multi-party computation

- Erasure codes

- Timelock crypto

- Homomorphic encryption / obfuscation

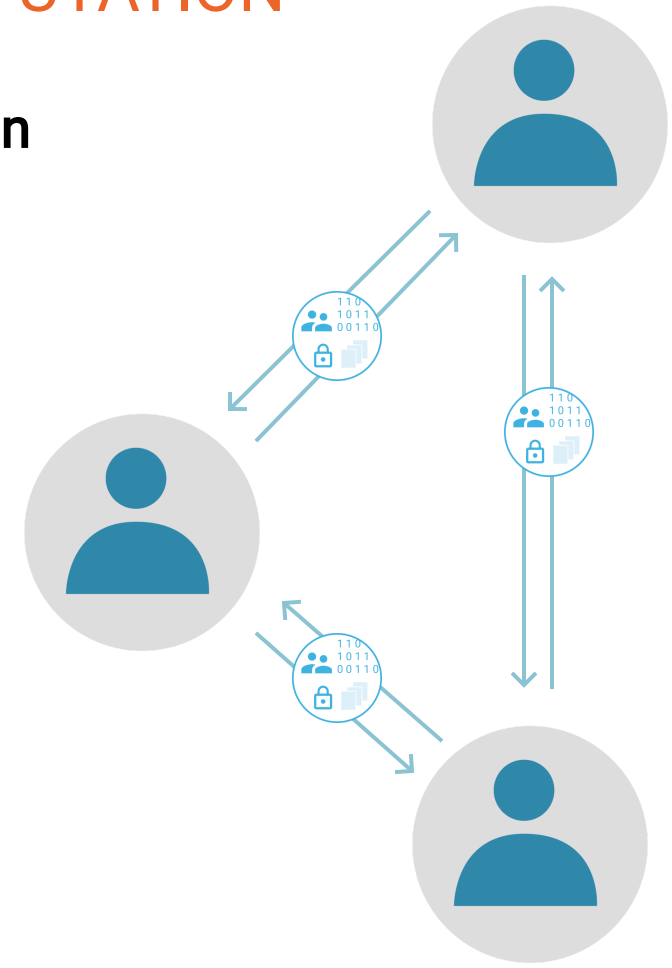
- ZKPs: prove arbitrary computable predicates on messages

SECURE MULTI-PARTY COMPUTATION

- Computation of "any" math function

- No "exchanges" of secrets

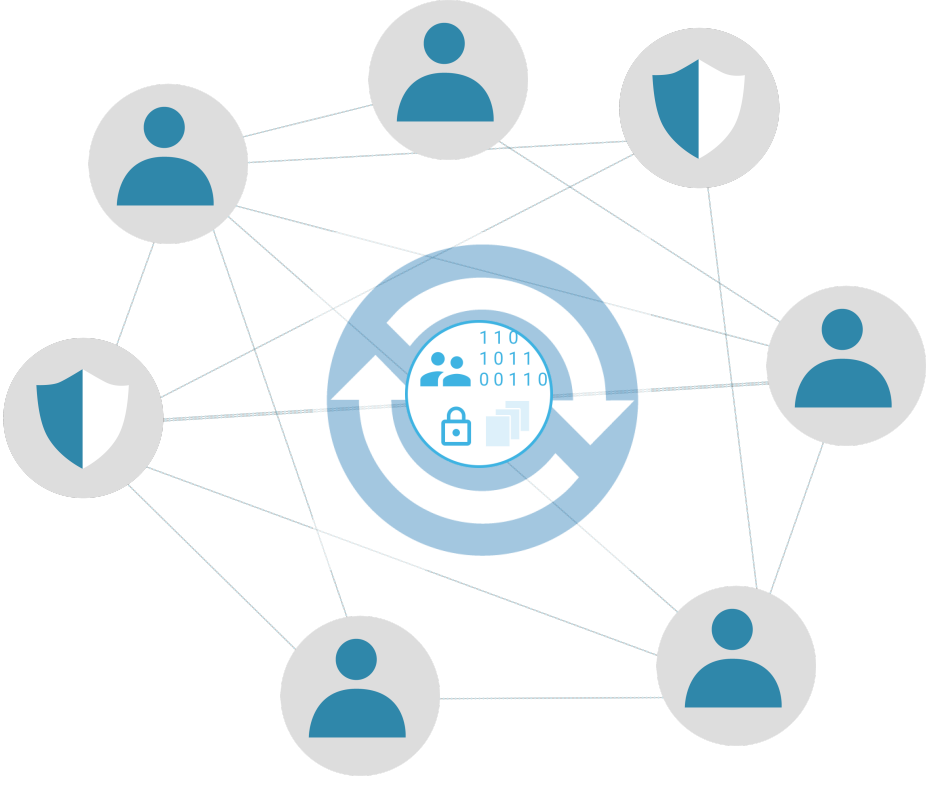
- No "trust" needed



			D1	D2	D3
D1	**7**		1	1	5
D2	**10**	→	2	6	2
D3	**12**		-5	1	16
	29?	→	**-2**	**8**	**23**

Ref: https://en.wikipedia.org/wiki/Secure_multi-party_computation

SECURE MULTI-PARTY COMPUTATION



5

GOVERNANCE PROTOCOLS

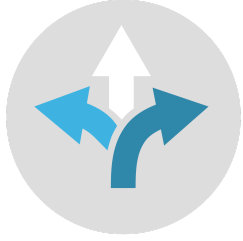
CRYPTO-ECONOMICS

Compute properties of the **past**

to ensure properties of the **future**

accessibility

equity



adaptability

cost effect.

pay for performance

Ref: goo.gl/gUL1e6

CRYPTO-ECONOMICS TOOLBOX

The crypto-economic protocols define:

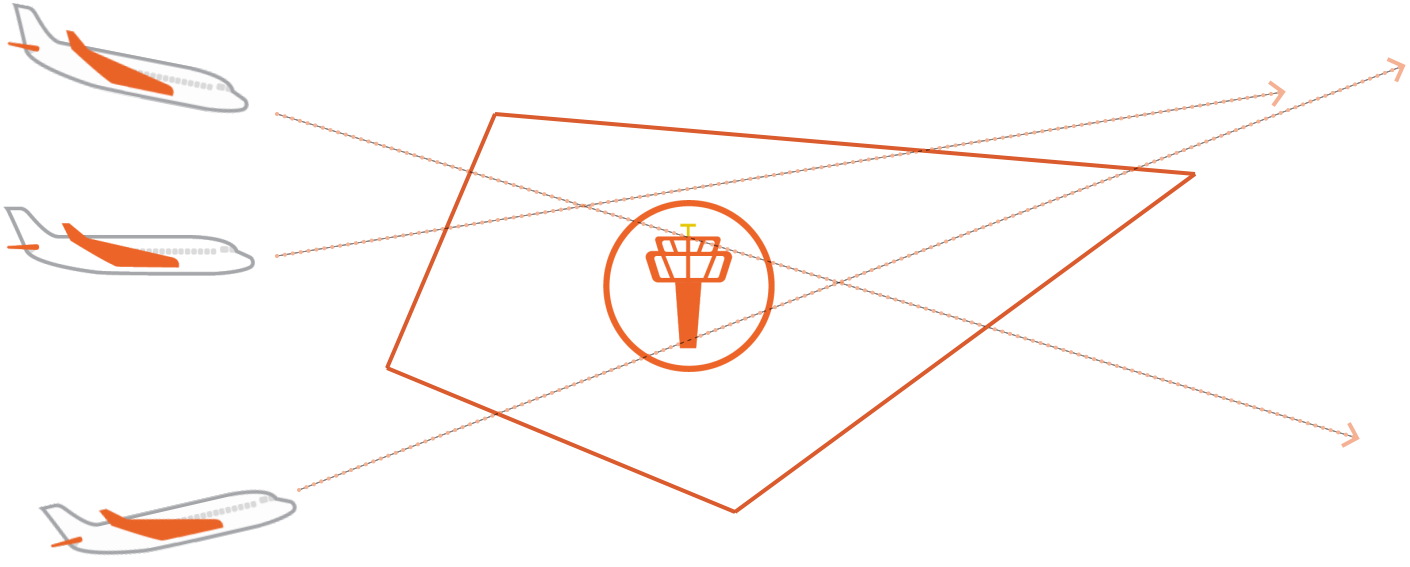
- Tokens: incentivise actors with units of a protocol crypto-currency
- Privileges: incentivise actors by giving them decision rights

The crypto-economic protocols assign, based on actors behaviours:

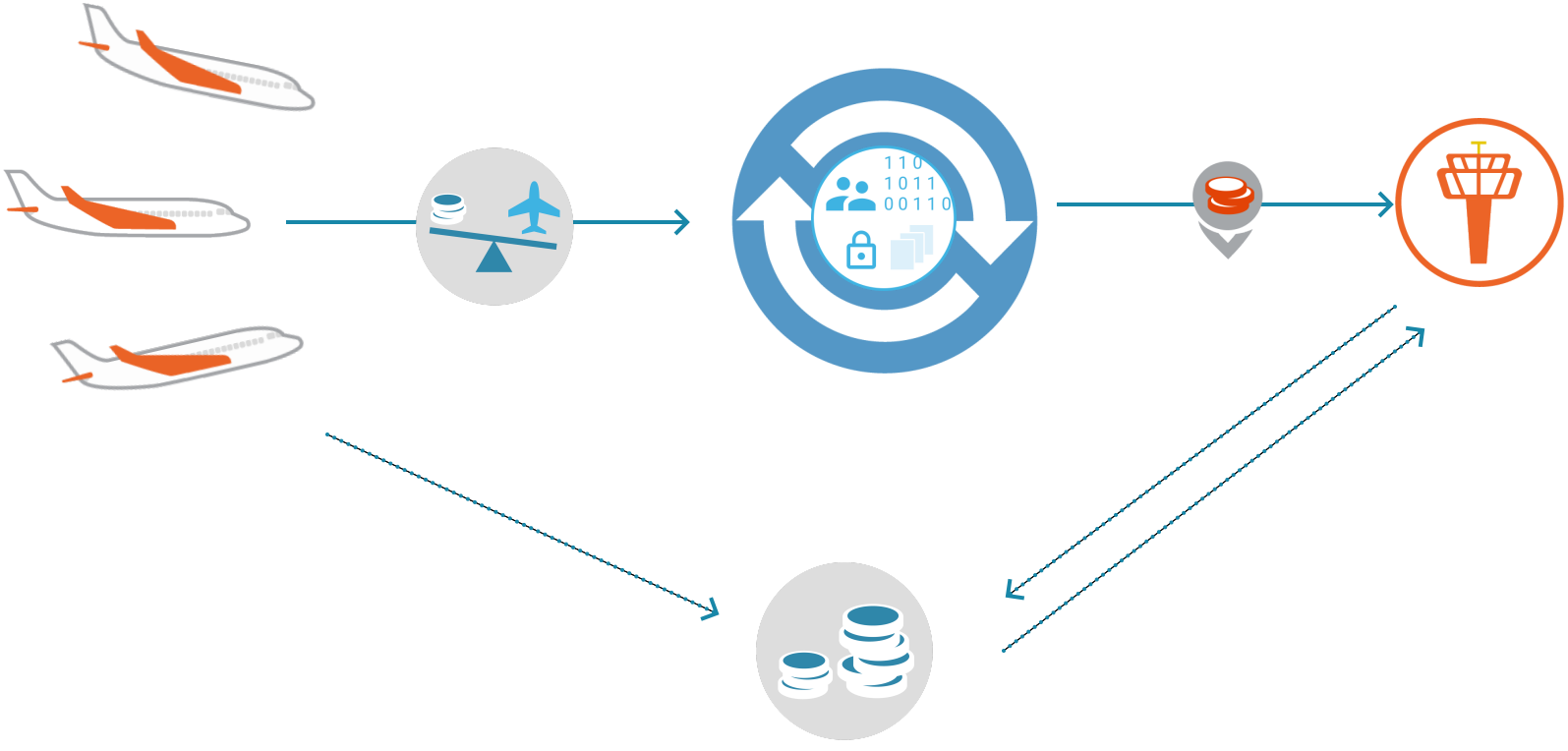
- Rewards: increasee token balances or give privileges
- Penalties: reduce balance or take away privileges

EXPLORATORY EXAMPLE #1 :
PRIORITISATION

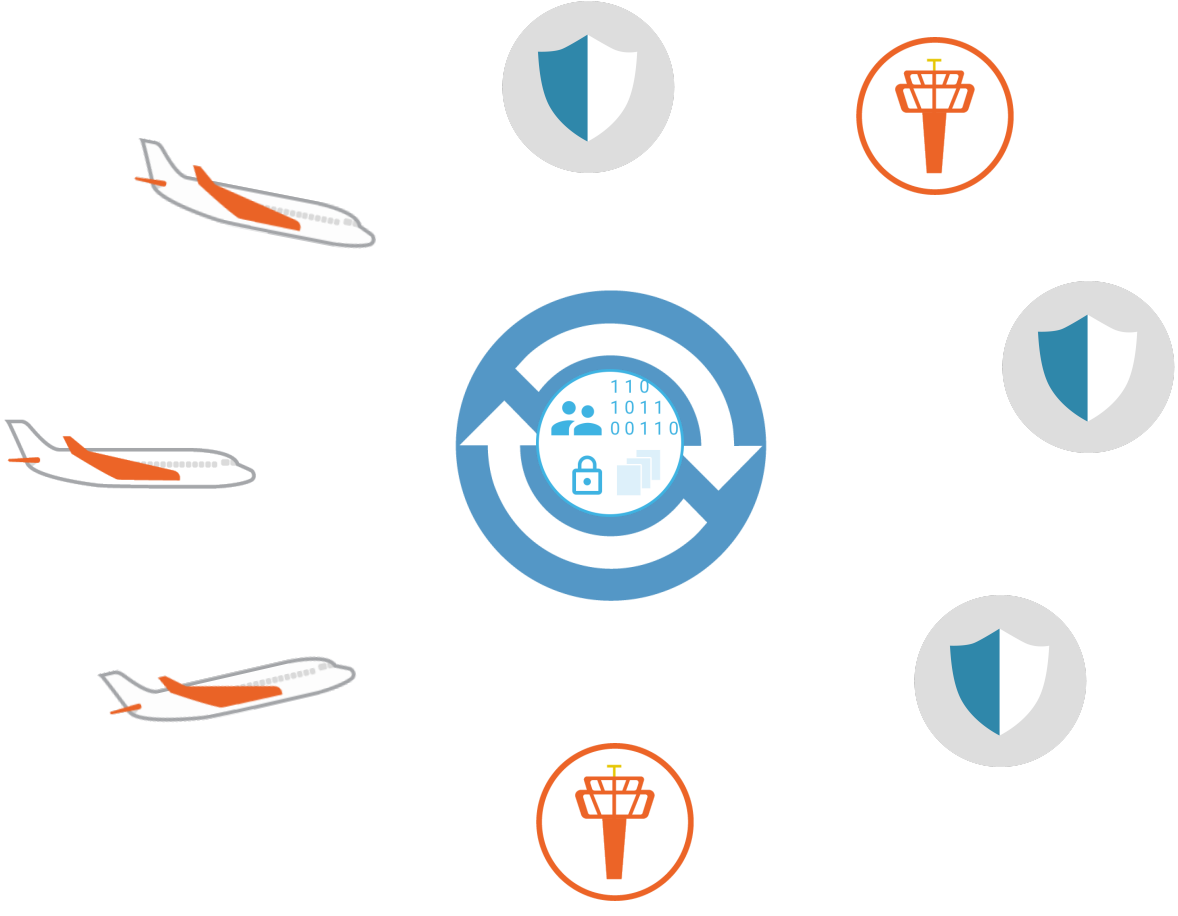
EXPLORATORY EXAMPLE #2:
ROUTE OR ATM EFFICIENCY



EXPLORATORY EXAMPLE #2:
ROUTE OR ATM SAFETY OR EFFICIENCY



EXPLORATORY EXAMPLE #3:
POLICIES ON TRAINING VS SAFETY



CONCLUSIONS

- Several **barriers exist** to share data: trust and software
- Some data **should not be shared**
- Data modelling for system/procedure design is **not always doable**
- **Crypto-economics** leverages crypto to provide governance protocols

- Do we need to choose between **trust** or **fancy math**?

+

- What about the (distributed) **infrastructure** to support these concepts?

TADOREA

KNOWLEDGE DISCOVERY FOR AVIATION

THANK YOU!

dp@tadorea.com