When Air Traffic Management Meets Blockchain Technology: a Blockchain-based concept for securing the sharing of Flight Data

Marina Dehez Clementi, Mohamed Ali Kaafar, Nicolas Larrieu, Hassan Asghar, Emmanuel Lochin

When Air Traffic Management Meets Blockchain Technology: a Blockchain-based concept for securing the sharing of Flight Data

Marina DEHEZ CLEMENTI
ISAE-SUPAERO, Université de Toulouse, France
Macquarie University, Australia
Sydney, Australia
marina.dehez-clementi@isae-supaero.fr

Nicolas LARRIEU
ENAC, Université de Toulouse, France
Toulouse, France
nicolas.larrieu@enac.fr

Emmanuel LOCHIN
ISAE-SUPAERO, Université de Toulouse, France
Toulouse, France
emmanuel.lochin@isae-supaero.fr

Mohamed Ali KAAFAR
Macquarie University, Australia
Sydney, Australia
dali.kaafar@mq.edu.au

Hassan ASGHAR
Macquarie University, Australia
Sydney, Australia
hassan.asghar@mq.edu.au

***Abstract*— The Aviation industry has been booming for several decades and is expected to keep growing in the future. Therefore, Air Traffic Management (ATM) tools are likely to be soon overwhelmed by the demand. The Single European Sky ATM Research Program (SESAR) 2020, controlled by EUROCONTROL, intends to revisit the management of aeronautical information along its full lifecycle and across the whole European ATM system. The efficient sharing of information over large scale cyber physical systems is a non-trivial problem that raises several challenges including data lineage, data consistency, access rights management, and many more. Part of the SESAR initiative, System-Wide Information Management (SWIM) project defines standards to enhance the security of aeronautical data shared among stakeholders. Most of its propositions include centralized or partially centralized mechanisms in order to enforce data confidentiality, and privacy. In this paper, we intend to discuss how blockchains can improve the sharing of sensitive data over the ATM system. More specifically, we use the example of flight data and describe a high-level Blockchain-based concept that mimics the decentralized nature of existing ATM system to provide a reliable, distributed storage platform for flight information.**

Keywords—ATM, blockchains, Flight planning, data security

I. INTRODUCTION

The 2019 Deloitte report, on the global Aerospace and Defense Industry, suggests the sector will keep growing during the next decades. Consequently, Air Traffic Management (ATM) systems are likely to experience an increase and diversification of communications.

Anticipating the upcoming obsolescence of the ATM tools, EUROCONTROL have launched the Single European Sky ATM Research Program (SESAR) 2020.The idea behind this project is to offer a complete change in paradigm of how aeronautical information is managed along its full lifecycle and across the whole European ATM system. Improvements include automating and securing the sharing of information between European actors, through the SWIM concept, System Wide Information Management.

However, sharing information can suffer from restrictions and additional security concerns should be examined. Considering a flight plan (formal document containing details on a proposed flight), from its submission to the competent authorities, until its archiving, many stakeholders have access, can update and add data to the document. The integrity and authenticity of the shared data are critical for ATM services in their attempt to reduce air route congestion. Furthermore, the availability and integrity of metadata (e.g. weather and route updates, ongoing operations in the airspace), are essential to pilots during the flight (e.g. to adapt their trajectory and avoid sensitive areas).

Cyber-security threats on ATM technologies used in the sharing of flight data have been recently reported; they include, among others: eavesdropping - hearing sensitive and potentially critical operational information; jamming - preventing two entities (e.g. aircraft and ground station) from talking to each other; flooding the aircraft or ground station with messages to prevent systems from handling them; message deletion and modification.

Consequently, we split our threat model into two levels. The first, "Data Level Threat", defines violations due to entities' actions on the data. It includes genuine unreported route modifications issued from controllers, resulting in data traceability disruption; as well as malicious users' actions, resulting in a breach of data integrity. The second level, "Service Level Threat", defines the disruption of services' availability, either due to unintentional or malicious interferences.

Many of these issues seem naturally linked to the problems solved by blockchains. Indeed, the blockchain technology has gained significant popularity in the last decade. In this work, we describe how blockchains can be used in ATM to improve the security of aeronautical data shared among stakeholders through applications compatible with the SWIM standards. Hence, we base our study on flight planning, as described above. Currently in Europe, the process is centralized, handled by a single central entity from EUROCONTROL, the "Network Manager".

Our goal is to achieve the following security improvements: ensure data integrity, traceability, immutability and non-repudiation by leveraging the main features of blockchains as a

data structure; and ensure availability of data and services during all airspace operational phases by using blockchains as a distributed storage and decisional system.

Therefore, we propose a high-level blockchain-based concept that mimics the decentralized nature of existing ATM systems. On one hand, this solution could cope with some environments with no existing centralized architecture and could ease the deployment of future ATM services in countries (e.g. Africa or South America) without existing ATM architecture. On the other hand, this blockchain-based architecture could also represent a lighter and more efficient alternative to traditional PKI-based architecture which are currently deployed for supporting for instance SWIM capabilities. It envisions a reliable, distributed storage platform for flight plans, leveraging blockchains' main features.

In addition to the thorough description of our concept, this paper provides a review on the intersection of ATM systems and blockchains. We present a background on ATM and EUROCONTROL's projects, introduce blockchains, discuss their applicability to flight planning, and identify open challenges in this direction.

II. An overview of Air Traffic Management (ATM)

The European Air Traffic Management (ATM) system is a large-scale, safety-critical, cyber-physical system (CPS) similarly to the US version. [1] It relies on a ground network composed of weather stations and radar facilities which feeds enable Air Traffic controllers to handle 25,000 (off-peak season) to 35,000 flights daily. [2]

A. Infrastructure

In Europe, the administration in charge of the safe and seamless ATM is known as the European Organization for the Safety of Air Navigation (EUROCONTROL). It handles part of the Single European Sky regulations on behalf on the EU. More specifically, the "Agency" designates its only executive entity and represents the central authority for coordination and planning of air traffic control (ATC) for all Europe.

Anticipating the upcoming obsolescence of the ATM tools [3], EUROCONTROL has launched the Single European Sky ATM Research Program (SESAR) 2020. The idea behind this project is to modify the way aeronautical information is managed along its full lifecycle and across the whole European ATM system. The project aims at improving the current ATM system on four aspects: by providing a way to handle the rising traffic in terms of services' availability (in other words improving the system's "capacity"); by reducing the occurrences of accidents and consequently improving "safety"; by preserving the "environment" and diminishing the impact of flights on global warming; and by cutting the gate-to-gate ATM costs, thus improving "cost-effectiveness". The entire European aviation business and its stakeholders, from Airport operators and ANSPs, to civil and military airspace users and the aerospace manufacturing industry, are concerned by the SESAR implementation. The primary focus of the regulations is to enhance the automation and securing of the sharing of information between European actors, through the System Wide Information Management (SWIM) concept.

SWIM is the fundamental keystone for a collaborative sharing of information between stakeholders. Its purpose is the design of an efficient, unified data exchange platform [4]. It consists of a combination of multiple information management projects and aims at enhancing the secure sharing of data between aeronautical stakeholders. It defines standards for real-time, reliable and consistent transmission of data among the different ATM participants [5]: major airlines, ATC departments, airports, etc. Besides implementing mechanisms to improve the ATM system's overall efficiency, SWIM architecture relies on 5 core services [6]; the 5th, called "information assurance", provides security protections compatible with the security needs of the ATM users.

Flight planning is the core mechanism of ATM. It refers to the process of producing a flight plan to describe the route an aircraft will follow. Its production is mandatory. It contains the aircraft identification, the departure and destination aerodromes, a description of the route to be followed, a time of departure and an estimation of the total elapsed time, among others. It can be submitted from up to one year until a few hours before the flight, to the entity in charge of the verification and distribution of flight plans at EUROCONTROL, called the "Network Manager".

B. Current concerns & limitations

Over the past decades, there has been renewed interest in moving towards a more adaptable and flexible airspace and flight operations to improve traffic flow, capacity, efficiency and safety. Despite the effort of researchers and industries, we believe that some critical limitations still remain. Below, we discuss the four main concerns that would, in our opinion, curtail the development of new ATM systems if not considered.

Scalability. The latest (2019) Deloitte report on the Global Aerospace and Defense Industry [7] suggests that the sector will likely keep growing over the next decades. More aircraft means more passengers using them. Whether it be the Airports Council International (ACI) or the International Air Transport Association (IATA), the expected number of passengers in the 2040's will likely be twice times the current levels. Similar growth has been witnessed during the past 20 years, yet human traffic controllers and airspace resources, such as the ground infrastructure have not been upgraded [8]. The scalability of the aeronautical physical infrastructure and resources is a prominent preoccupation.

Resilience. The ATM system will become more vulnerable to malicious attacks that aim to compromise stakeholders and flight data. [9] The two major reasons are: first, because Air Traffic Navigations Service Providers (ANSPs) rely on a growing number of interconnected services, situation that will get worse with the development and use of SESAR [10]. Indeed, the project enhances the sharing of information and promotes the interconnection between aeronautical stakeholders. Because of that, SESAR will likely increase the attack surface of any future malware. Secondly, while the previous ATM systems were relying on specialized and expert knowledge, providing security through isolation and obscurity, a current trend is to use Commercial Off the Shelf (COTS) software [11]. Examples include the integration of the Linux OS, the implementation of

the Internet Protocol (IP) and Voice over IP (VOIP), as well as enhancements to GPS.

Consistency. Therefore, the diversity and heterogeneity of the ATM ecosystem is likely to generate inconsistency in the data shared among stakeholders. Indeed, the geographical distribution of the nodes is the first concern as latency and propagation time are not the same depending on the environmental context (the weather impacts connectivity). Furthermore, the nature of the systems can also be a serious impediment to their processing capabilities (regarding the computational power of their components for instance). Keeping a consistent view of the system and the data transferred through the network is therefore of utmost importance.

Privacy. Sharing information implies the implementation of mechanisms able to restrict the access to the data to the authorized entities only. Indeed, new systems developed and promoted in the context of SESAR, notably the Automatic Dependent Surveillance Broadcast (ADS-B) system, do not incorporate functions to insure a granular-level of privacy, when required (for instance in the case of military flights). [12] ADS-B systems are particularly useful in the positioning of aircraft in geographical zones where the deployment ground-based radars and systems is difficult. However, the technology relies on the broadcast of an aircraft's positions to all its peers within a limited range. Therefore, an adversary close enough to the emitting aircraft can eavesdrop its exact location and eventually predict its future route. The privacy leakage could therefore have a disastrous impact on users' safety (e.g. terrorist attack). Currently, Public Key Infrastructure (PKI) is the cryptographic solution privileged by the Aviation Community to address these privacy concerns. Their idea is to encrypt flight data so to restrict their access to the authorized parties. However, PKI is a heavy process to implement and maintain. Therefore, the confidentiality issue remains an ongoing challenge.

In recent years, since the advent of Bitcoin in 2009 to be exact, its underlying technology has become very popular by itself: also known as the blockchain. In this article, we consider the ATM environment, its flaws and limitations, and try to envision how the blockchain can potentially be used to tackle or at least reduce their impact on the overall system safety (which includes the passengers and stakeholders' safety).

III. Background on Blockchains

A Blockchain is essentially a digitized, distributed and public database, also called "ledger", that records all the transactions or digital events that have been executed and shared among a network. When a peer joins the network, they get a local copy of the current state of its associated ledger. There exist several types of blockchains: according to the degree of anonymity provided to the users or to the amount of trust put into the validators; but also depending on the algorithm chosen to achieve a consensus.

A. Fundamental keystones

Blockchains are built upon basic components which, put together, constitute the technology's strength. These include the use of hash functions and blocks to organize data, and its chained and distributed nature to replicate them. These elements are described in the following paragraphs.

Hash functions. The first and essential mechanism upon which is built any blockchain is the cryptographic hash function chosen for its design. A cryptographic hash function is a function that maps an input of arbitrary length to an output of a fixed length of bits, also called the hash (value). A robust hash function H must satisfy three security requirements that prevent an adversary that knows the input, the output or both to forge another distinct input that would match the same output. In the context of blockchains, the hash of a block refers to its fingerprint. It is a unique and alphanumeric identifier. Therefore, one must take special attention to how strongly respected the requirements are. Indeed, having a weak hash function would result in finding another transaction or block with the same identifier and thus enable an attacker to change the content of one block while keeping the chain intact, in other words: without the other peers noticing it.

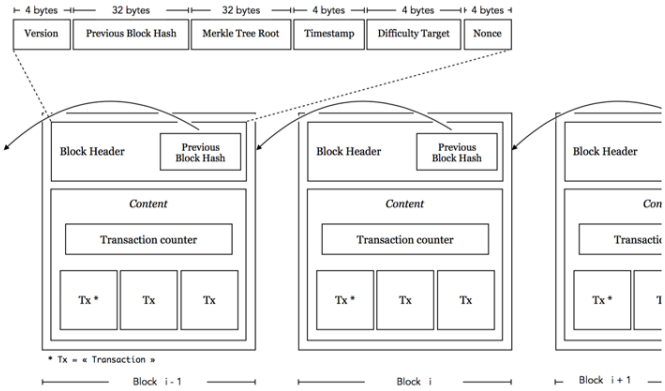


Figure 1 - Simplistic view of a Blockchain's data structure [13]

Block. The second brick in the blockchain technology is the block. A block incorporates a lot of information related to the network, the application and the current state of the ledger; among others, it stores: a number – incremental, starts at 0 for the genesis block; a nonce – an alphanumeric string used to compute the hash value of the block; some data; its hash and the hash of the previous block in the chain.

Chain. Consequently, a blockchain is a chain of approved blocks, linked together by incorporating the hash value of the latest added block into the new one. The consensus used to add a block differs depending of the application considered. In the case of Bitcoin, only "signed" blocks can be added to the blockchain. Signing a block refers to the process of computing the hash value of the block by bruteforcing on the nonce value, i.e. trying several nonce values until finding a value below a certain threshold called the "difficulty". This mechanism is also known as "proof-of-work".

Distribution. In addition to this data structure, blockchains leverage the power of distribution by relying on a peer-to-peer network. Each peer stores a local version of the ledger, updated each time the consensus is reached. Its chained data structure along with its distribution among the peers is what make blockchain a secured database. Indeed, tampering with a block

changes its hash value and comparing this chain to the existing copies of the ledger reveals the ongoing modifications.

B. Taxonomy of Blockchains

There are several studies describing complex and detailed taxonomies of blockchain technologies. The taxonomy of Ballandies et al. [14] details the most comprehensive study, that includes a crowd-sourced evaluation feedback from experts in the blockchain community. They identify cryptocurrency-based blockchains as a set of four components: the distributed ledger (DL), the consensus, the action and the token component. Each component is derived into attributes; in total, they study 19 different attributes (e.g. the read and actor permission attributes related to the action component, the write and validate permission attributes linked to the consensus component).

Unlike common sayings, the Bitcoin blockchain is not anonymous but pseudonymous. Some studies have shown that it was possible to link together the transactions issued by one pseudonym (transaction graph analysis paper); others have proven the possibility of associating the found clusters to the pseudonyms' real-world identities (network-based analysis). However, for some applications, especially in healthcare and financial systems, complete anonymity in transactions over the network is essential. Therefore, an alternative to public blockchains is needed. From Ballandies et al.'s work, we can identify four different clusters of blockchain technologies, that provide four distinct levels of confidentiality.

Public and Permissionless blockchains. Every node, with a network connection and a terminal device, can write on the ledger and become a validator (run the consensus algorithm). Inside the network, authorized actions and permissions are the same for every participant (e.g. Bitcoin [25]).

Public and Permissioned blockchains. There is no restricted access to the network itself, but only certain nodes are granted the validation function; others are only passive owners of the data (e.g. IOTA [26]).

Private and Permissionless blockchains. The access to the network is restricted, but once the participant is authenticated, the read and write permissions are the same the other nodes on the network. It can be compared to a company-wide intranet: the access is granted by a third-party; but every "authenticated" node can perform any actions (e.g. Ripple [27]).

Private and Permissioned blockchains. Only certain participants are granted access and only some of the nodes have permission to add information. It is the most restrictive type of blockchains: the access is granted by a third-party which also manage the permissions (e.g. Ripple).

Therefore, depending on the degree of trust one puts in their peers and the degree of anonymity they want to provide, they will choose between one of the four families.

C. Consensus algorithms

The implementation choice between the different types of blockchains is directly related to the application context. Depending on this choice, one family of consensus algorithm would be privileged. For instance, the use of Proof of Work (Pow) based algorithms is interesting for public blockchains because of their large scale; the use of computational power as the elective resource complicates the compromising of more than 51% of the network's power [28]. However, private networks, because of their limited resources, are more vulnerable.

In blockchain networks, the consensus is the process by which new data are declared worthy of being added to the previous records; it refers to the block validation mechanism. The "validation", also called "verification", consists in signing a block, i.e. finding a nonce n, random parameter, such as the hash h of the block's content c along with the nonce n answers certain conditions Cs. In Bitcoin, a block is signed when the resulting hash h is less than the target hash h_0. For nonce n, alphanumeric string, find hash h such as: $h = f(c|n) \leq h_0$, with f hash function.

The value of the target hash h_0 defines the difficulty of running the consensus. Upon success, the peer will send the hash h, the nonce n and the content c of the block B to its peers. Verifying the validity of the signing is then simple, as all data are known, and consists in computing $f(c|n)$, with f the same hash function, and comparing the result h' obtained to the expected result h.

This agreement on a unique and common view of the blockchain should be achieved, even in the presence of faulty nodes, also called "Byzantine" nodes. These faulty nodes usually have arbitrary behavior including malicious attacks (e.g. Sybil attacks [15], and double spending [16]) nodes mistakes or also connection errors (e.g. leading to forks [17]).

The consensus protocols vary as mentioned above and can be categorized into two big families: they are either collaboratively or competitively computed.

Examples of *competitive consensus algorithms* are:

- **Proof of work (PoW).** This is the most popular scheme, used in Bitcoin. A node earns the right to add a new block to the chain if it can demonstrate having spent a certain amount of computational power. To do so, it has to solve a computationally difficult cryptographic puzzle as presented above (hash computation).
- **Proof of Stake (PoS).** Implementation partially in Ethereum, and entirely in BlackCoin [20] and Peercoin [21], the proof of stake assumes that entities having a large stake in the blockchain have more interest in guaranteeing its integrity. IN this case, the probability a node has to mine the next block is linked to the proportion of its stakes.

The *collaborative consensus algorithms* stand out since there is no puzzle to solve before the others. Instead, nodes are granted the authority to validate blocks because they have been approved by a trusted third party in the case of the Proof of Authority (PoA) [22-23], or because of their honest history in the network like with the Proof of Reputation (PoR) [24]. These alternative algorithms have been developed to address the main and major flaw of the PoW-based consensus algorithms, that is the high energy required to compute the puzzle.

IV. Related Work

Few articles have been presenting blockchain-based solutions for improving the security of the next generation aeronautical and ATM systems.

In [18], the authors propose a new blockchain-based algorithmic approach to achieve secure communications between aircraft and ground stations (GSs). The scheme relies on three algorithms, each one defining the interactions between aircraft and ground stations for a specific context. The first algorithm defines the registration procedure and the storage of registration details in the distributed ledger. The second describes the first authentication negotiation between both entities. And finally, the third one determines how entities communicate after this first exchange, i.e. once authenticated. While the solution ensures private communication for registered parties (if the registration details, including the public and private keys, are not stored in the ledger, there is no chance to encrypt the data transferred between parties), there are some limitations. The first one concerns the storing of the private keys inside the ground stations which could cause severe privacy leakages in case of compromising. Then, the ledger that records the identification data is indeed distributed (among the ground station nodes) but there is no mention to any consensus algorithm used to add the data to the chain, nor to a choice of a technology (e.g. « bitcoin-like blockchains », « consortium blockchain », etc).

In [12], the author stresses once again the security and privacy issues related to the adoption of ADS-B systems, and the defiance from the military aviation community. His paper is a contribution to the cryptographically « secure broadcast authorization » by presenting a novel blockchain-based PKI implementation. To do so, he presents a « Aviation Blockchain Infrastructure » that leverages the Hyperledger Fabric (HLF) software, as it is argued to be the more suitable to meet enterprise-like requirements. Indeed, the prototype described defines different types of « organizations » according to the nodes that compose the aeronautical network (e.g. military, corporate and civilian aircraft are simulated as well as airline companies and Air Traffic Management Services, ATMS). For each organization, a ledger is generated with associated access rights (e.g. military-type ledgers are only accessible by the aircraft at stake and ATMS; airline companies create one ledger for each of their aircraft in-flight). While this paper presents an exhaustive description of the roles and ledgers composing the prototype and propose to use a well-known private blockchain like HLF, it lacks of performance evaluations as well as security analysis.

SWIM Registry is a key element of next generation aeronautical systems that enhances interoperability by referencing the sources of the services available for SWIM applications. It consists in three entities: service providers, behind the design of services; service consumers, that implement the applications; and the regulatory authority, for the communication and monitoring of services and applications via registry. The idea in [19] is to associate each service with its own blockchain. Access to the blocks is restricted in writing and reading permissions to authorized parties only. A case of application is flight planning data. Each stored transaction is a flight plan, of which the access requires the knowledge of the hash generated during the registration process. The authors use, once again, the chained structure of the blockchain as well as its distributed nature as the two main features for their contribution. However, there is no clear explanation on how the data are validated, and how the access to the data is monitored by a trusted third party (i.e. the service system).

V. Preliminaries

A. Problem statement

There are two major drawbacks related to the current flight planning process and the new technologies developed to improve it.

1) **Inconsistency in flight planning.** The larger the network becomes, the more difficult it is to maintain a consistent view of a specific flight plan among it. Therefore, we need to implement a mechanism that enables fast and secure updates and their recording within a peer-to-peer network.

2) **Privacy leakage due to new systems.** As exposed in the related work section, new developed components (e.g. ADS-B) do not necessarily incorporate privacy-preserving and security functions. Indeed, flight data are currently not considered as confidential data. However, they are highly sensitive and, in some case, critical to the safety of operations and operators. Therefore, they are becoming more valuable to malicious adversaries, easier to target and lead to dramatic safety breaches. Consequently, as part of the safety-for-security process, we need to define and apply an additional security layer to protect the aeronautical data and secure their sharing through existing communication protocols.

B. Nodes

The ATM system is composed of different types of stakeholders, all sharing information to enhance the safety and security of the past, future and ongoing flights. The list of aeronautical stakeholders is provided in Table 1 along with their respective group id and the information they share.

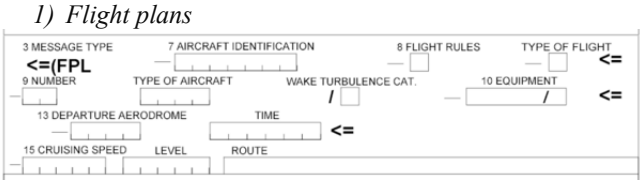
Table 1 - Nodes' description

Set	Name	Composition	Information
U	Users	Pilots/Aircraft	Flight plan; location
E	External sources	Sensors, Meteorological Services; Airline/ Airport/ Military operations centers	SO6 traffic flow; weather forecasts; flight cancellation, merging; ground operations (runway upgrades, incidents); …
A	Approvers	ANSPs	Flight plan approval; route changes; traffic information

C. Flight Data

Flight data are of two types: there are flight plans, initially filled by the end-user and modify as required all along the flight by ANSPs. And there are the SO6 files which are aeronautical information automatically generated by the radars.

1) Flight plans



2) SO6 files

```
EDDF_$GHFY,EDDF,EDDH,A319,121700,121716,4,10,0,DLH6PH,131212,131212,3002,514.233333,3001.65,513.616667,17287411
$GHFY_$GHFZ,EDDF,EDDH,A319,121716,121847,10,50,0,DLH6PH,131212,131212,3001.65,513.616667,2998.816667,508.666667
$GHFZ_ROXAP,EDDF,EDDH,A319,121847,122007,50,93,0,DLH6PH,131212,131212,2998.816667,508.666667,2994.916667,501.8
ROXAP_$GHFb,EDDF,EDDH,A319,122007,122043,93,110,0,DLH6PH,131212,131212,2994.916667,501.85,2997.883333,499.9,172
```

D. Storyline

We consider a scenario where an operator (pilot of an aircraft or airline company on behalf of the pilot) uses the Air Traffic Control and Management services provided by EUROCONTROL's ANSP (Air Navigation Service Provider) network to fly from an airport (departure) to another (arrival). We assume that the ANSPs are responsible for the collection of events (including military operations, ground operations, weather forecast, etc.), their processing and integration into the flight plan for to be addressed in almost real-time to the operator (in the form of recommendations: changing route, alternative arrival airport, on hold, etc).

E. Desired properties

In the traditional ATM system, military flights can be granted with a certain level of anonymity to prevent the release of critical, sensitive operational data. With the recent projects in Aviation (SESAR20 in Europe and NextGen in the US), automation in the data collection (ADS-B systems for positioning), as well as the increased collaborative decision-making leads to the leakage of information to parties that may not be authorized to access them. While considering/hearing the requests from the community, in terms of data and users' privacy, EUROCONTROL still advocates for the non-provision of ATC and ATM services to anonymous aircraft. Therefore, there is an urgent need to find a mechanism for a tradeoff between user privacy and data traceability.

Traceability. EUROCONTROL's Network Manager is the entity responsible for the reception, analysis and distribution of flight data. It is also the authority that charges aeronautical stakeholders that benefit from the use of ATC and ATM services. Due to the heterogeneity in the Aviation network and their wide spread spatial expansion, flight planning suffers from data inconsistency. The lack of traceability n impacts the relationship between airline companies and EUROCONTROL, with recurring disagreements on the charges imposed for using their services, due to the lack of traceability.

Privacy. Some airspace users expect their activities to be kept private (military operations, medical emergencies, diplomatic travels, etc). We argue that current airspace communications (e.g. when an aircraft broadcasts its position to its closest peers; or when it receives commands from the ATM controller) can't be changed to enable private communication (i.e. we won't implement mechanisms to ensure directional/isolated communications). Communications can be eavesdropped. Therefore, privacy should be taken into consideration along with the data itself (e.g. encryption).

Performance. The ATM system is operating in a real-time fashion and nodes have limited capabilities in terms of storage space, computational power, etc. (especially aircraft and sensors). This introduces the following constraints:

- *Real-time processing:* the mechanisms implemented to enhance privacy and ensure traceability should not introduce additional delays in communications above a certain conceded threshold (to be defined in line with the application).

- *Minimal processing:* the mechanisms should be defined in compliance with the smallest (in terms of resources) nodes (probably the sensors). For instance, if encryption is retained for privacy-preserving mechanisms, it should be lightweight enough to be handled by a sensor node.

F. Limitations and scope

Infrastructure. The ATC and ATM physical infrastructure cannot be changed. We are working with standards defined as in the SESAR 2020 project, with physical facilities that represent the ground foundation of the ATM network. Therefore, our initiative here does not aim at proposing a new architecture for the whole physical system, but rather a protocol of communication that would allow for the recording of aeronautical data in an inconspicuous fashion while guaranteeing the safety and security of the system and its participants.

Authentication process. An adversary may compromise a node. However, we argue that, while it can lead to catastrophic incidents, it can also be done in the traditional systems. Our concerns are about ensuring the traceability of the data (data lineage) along its lifecycle and providing required levels of confidentiality. The solution itself does not provide means to authenticated users prior to their entrance in the network, but rather mechanisms to detect abnormal behaviors of authenticated participants. The first authenticity checks are offload to a trusted third party (e.g. EUROCONTROL, governments, etc.).

Real-time. The ATM system is a cyber physical system (CPS). It implies relationships between digital systems and the real-world activities (quote). Moreover, it is a Critical Infrastructure (CI), i.e. a system where safety and security are in tandem. As the real, physical world is timed, any digital operation leading to a decision making with direct impacts on physical systems should be processed in real-time. Real-time is not achievable, therefore, we aim at designing this solution such as it releases commands in quasi-real-time.

VI. Our Approach

In the following section, we introduce a layered overview of the ATM application and incorporate a description of the blockchain model we envisioned. We decided to narrow down the protection of aeronautical data to the management (submission, validation and recording) of flight plans. We detail a mathematical characterization of the acting nodes and present a basic Flight Planning management workflow relying on blockchain-based interactions.

A. Node characterization

Let time t be a real number such as *t in [0, T]*. Let *(x(t), y(t), z(t)) in [-180;180]x[-180;180]x[-370;+∞[* (-370 m under sea level is the airport of Bar Yehuda, Israel) be the 3D coordinates of the aeronautical object for each time *t*. *x(t)* and *y(t)* are respectively the latitude and longitude of the object in degree, and *z(t)* its altitude in meters. Because of the aeronautical context, we may change this metric in the future, to the profit of Flight Levels (FLs).

A **node** *n(t)* indiscriminately refers to a user, an approver or an external node (see Table 1). Each node is identified by the following tuple: *(ID, x(t), y(t), z(t))*, where ID is a unique constant alphanumerical identifier for the node, and *(x(t), y(t), z(t))* its 3D coordinates in space as defined above. As a tradeoff between the continuous nature of the airspace activities and the discrete representation of data, we introduce a simplified, discrete representation for the nodes as follows: $n_i = (ID, x_i, y_i, z_i)$; the set $\{n_i\}_{i=0..N}$ where *N* is bounded (and refers to the number of locations crossed to reach the arrival from the departure airport) represents the effectively followed route.

User node. Let **U** denote the set of users, that is, n_u *in* ***U*** indiscriminately designates the pilot and their aircraft. Note: these are the only moving nodes. The user node positions $(\{n^i_u\})_{i=0..N}$ are identified via the tuples $\{(ID, x^i_u, y^i_u, z^i_u)\}_{i=0..N}$. User nodes can be categorized into two categories: *ordinary user nodes* and *special user nodes*. The special nodes require a specific treatment due to the critical and sensitive activities they perform (e.g. military operations). A special node will be declared with an additional label that would specify the level of confidentiality it needs.

Approver node. Let **A** be the set of approvers. Approver nodes are identified by the tuples (ID, x_a, y_a, z_a), which do not depend on the variable t, because these nodes are fixed. They refer to the ANSPs, Air Navigation Service Providers. Validator nodes have been approved by the CA and granted the authority to validate the flight plans, propose modifications, etc.

External node. Let **E** be the set of external sources to the ATM network. These are typically the nodes that provide useful information for the ATC and ATM services in a one-way fashion. They cannot read the information stored in the blockchain, but still can submit transaction (information feeds) to be added to the blockchain for traceability purposes and incorporated in the ATM decision making process. **E** regroups the sensors (automated radar network) as well as the meteorological services, airport, airline and military operations centers. We assume that the two latter may need an additional level of privacy. For now, we just make the following simplified assumption: the confidentiality required applies on the nature of the operation not the location nor the time when it is performed. External nodes are identified via tuples similar to (ID, x_s, y_s, z_s), which do not depend on the variable t, because these nodes are static.

B. A layered overview

On Figure 2, we give a layered overview of our envisioned Blockchain-based Flight Planning Architecture for Reliable Data Traceability and Confidentiality.

The top layer corresponds to the physical world and represents the three phases of a flight: the pre-flight phase, when the pilot formulates the flight plan and interacts with the ANSPs to modify it if necessary; the in-flight phase, during which the aircraft is in the air and receives eventually updates from the ANSPs; and finally, the post-flight phase which corresponds to the archiving of the flight plan.

The second layer, called "Infrastructure layer", geographically positions the blockchain's nodes on the map.

The network layer represents the digital peer-to-peer network and is composed by user nodes (black), external sources (blue) and approver node (orange). The approver nodes receive, broadcast the flight plan to their peer and run the verification protocol.

Finally, the bottom layer corresponds to the blockchain data structure. Each modification (pre-flight phase and in-flight) triggers the recording of the modified flight plan (for traceability purpose).

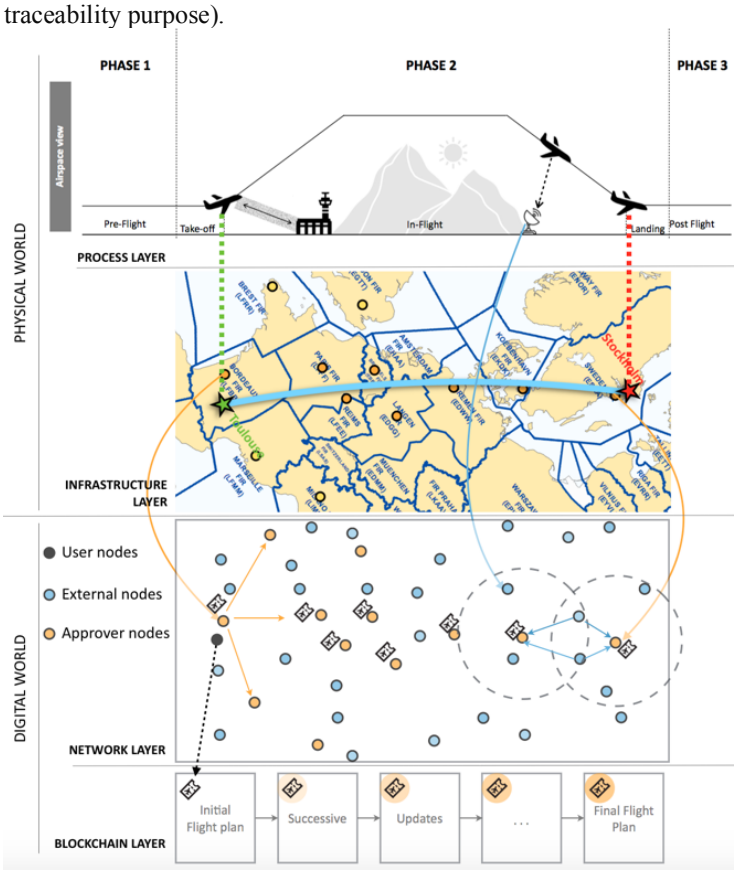


Figure 2 - A Blockchain -based Flight Planning Architecture for Reliable Data Traceability and Confidentiality

C. Proposed workflow

Nominal behavior. Here below, and as illustrated on Figure 3, we describe the normal interactions that should be observed within the network if all parties are honest.

Before the flight:

1) Initialize: A user $\mathbf{U_0}$ submits the initial flight plan ***FP*** to one of the approvers $\mathbf{A_0}$.

2) Collect: In the meantime, $\mathbf{A_0}$ collects information ***I*** from the external sources (*Upload*).

3) Synthetize: Based on the flight plan ***FP*** and the information ***I***, $\mathbf{A_0}$ approves/modifies the flight plan and sends it back to user $\mathbf{U_0}$.

4) Process: User $\mathbf{U_0}$ analyses the suggestions of $\mathbf{A_0}$ and either agrees (step 5) or proposes alternative modifications (go back to 3).

5) Accept: 3 and 4 are repeated until $\mathbf{U_0}$ and $\mathbf{A_0}$ agree on a common version of the flight plan $\boldsymbol{FP_0}$, the approved plan. At that point, the approver $\mathbf{A_0}$ will *6) Store* the flight plan and make it available (only) for U_0 to see it at any time.

During the flight:

7) Update: During the flight, $\mathbf{A_0}$ receives updated information from its sources **E**. These data are likely to influence the route of the flight for safety reasons (weather, ground/air operations, etc.)

After the flight:

8) Record: At the end of the flight, $\mathbf{A_0}$ makes sure to report any change I nthe route of the flight compared to the initial flight plan approverd by both parties $\boldsymbol{FP_0}$ and to correlate these modifications to the information provided by the set **E**.

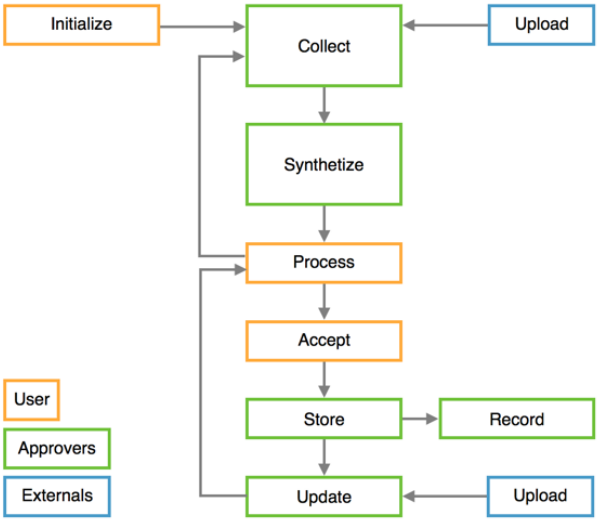


Figure 3 - Nominal behavior, workflow execution chart

D. Peers' possible actions

In this environment, the nodes are allowed to perform some actions to fuel the data flow according to the needs of the ATM application and related to the use of blockchains. These actions are described below.

Submission. In the best-case scenario, an owner $\mathbf{O_1}$ inserts their filled flight plan in a transaction and sends it to the blockchain network. This document includes the departure and arrival aerodrome, a list L of en-route points. An en-route point belongs to a Flight Information Region (FIR) itself administrated by an Area Control Center (ACC). It determines the altitude and time at which the aircraft will cross a specific location. The election of the validators is based on this list L. Let's note that the FIRs' surface is different in the upper airspace and the lower airspace. Therefore, the set of validators is chosen as the union of both sets of ACCs of the crossed FIRs from the upper airspace and the lower airspace; they are denoted ACC Type_1 on the map. ACCs of Type_2 are the validators that are not concerned by the flight.

Verification. The validators concerned by the flight will individually run the verification process. They will check: the identity of the owner $\mathbf{O_1}$, the authenticity of the data transferred, the validity of the flight plan, its conformity with air traffic regulations. And finally, they check their own availability for the time of crossing. If approved, the validator sends back a signed approval message.

Modification. Sometimes, adjustments are required. For instance, one controller can handle only 20 aircrafts at the same time. Therefore, it can happen that the available capacity in one area of control may slightly change between the preparation of the flight plan and its submission. In that case, the validator will send a "modification request". This request will include the reason invoked, a list of the closest en-route point alternatives with their current capacity for the time of crossing. The modification request is sent to owner $\mathbf{O_1}$ but also to the ACCs in charge of the proposed en-route point alternatives. $\mathbf{O_1}$ will then either chose one alternative and re-start the negotiation process or cancel the flight.

In-flight updates. Due to meteorological events or fortuitous in-air or ground operations, the controller may need to change the route of an aircraft. (e.g. a weather forecast reporting a big storm). The controller decides to send an "update request" to inform the aircraft affected by the storm and propose an alternative route. The forecast has been received by everyone, including all the set of validators from the previous update. A new set of validators is immediately elected: it comprises the latest update's set of validators plus the newest validators affected by the proposed alternative route. All check the proposition and upon agreement, the pilot is authorized to change its course.

Archiving. The archiving process is simplified by the chained nature of the blockchain. Indeed, the final flight plan, that will be used by Eurocontrol to compute the amount of fees to tax, can be obtained by tracking all the transactions related to the flight.

E. Performance Evaluation

While lot of studies have tried to evaluate the performance of blockchain technologies, comparing them to one another, and despite of the recent design of benchmarking frameworks [20], the performance evaluation remains one of the main challenges when designing a blockchain-based system. Moreover, to the best of our knowledge, no evaluation study has been done yet regarding the use of blockchains applied to Aeronautical context. As part of our future work, we aim to provide such analysis. To do so, we are planning to:

1) Expand our mathematical representation of the ATM application by incoporating a technical description of the data, peers and communication links between them;

2) Based on this description, we will qualitatively compare several blockchain options, evaluate them according to the

observed throughput and latency introduced by their consensus algorithm, the memory footprint generated by the production and storage of flight plan, as well as the energy consumption in terms of computational power.

3) We will consequently choose the best option and implement it. Through simulations, we will evaluate the system designed in terms of performance and security.

F. Main challenges,

Consequently, as of now, we identify the main challenges to overcome before being able to formulate a strong and relevant performance analysis and benefit from the use of blockchains in this context. We will have to clarify two major concepts: the first one is the data representation; and the second, the decision-making process.

Data representation. Blockchains are first and foremost distributed databases. It implies that the data and the recording techniques should comply not only with the application context (i.e. that the recorded data are of interest and relevant in regards with the application considered) but also with the peers that compose the network (which have limited resources in terms of storage space and computational power). Consequently, one will have to take special precautions regarding the data selection and their representation. In MPF-BC for instance, authors develop functions that reduce the memory footprint of their blockchain.

Decision making. The addition of new transactions to the blockchain's ledger is the result of an agreement between node. This agreement can be reached either cooperatively or competitively. In the case of Bitcoin and any PoW-based blockchain, the election of the node that will be able to add new data to the chain is performed via the computation of a highly difficult mathematical puzzle. The first node to find a solution is the one elected. On the other hand, in PoA-based blockchain, the agreement is reached via cooperation between "authorized" nodes. Choosing the consensus algorithm compatible with the application and environment is critical for the viability of the blockchain solution. It depends on the type of blockchain considered. Indeed, public blockchains rely on a fully untrustworthy P2P network, as anyone can join and quit the network, i.e. there is little or no monitoring of identities (pseudonymous network). Therefore, collaboration is excluded; in that case, competitive consensus algorithms will be preferred (PoW, PoS). On the other hand, for private blockchains, the access to the network is monitored by competent and trusted authorities. In this case, nodes are no longer anonymous, we know their identity - or at least, if identities are kept private, there is proof of authenticity provided by the agreement given by the certifying authority (which is the only to know the node's true identity).

VII. Conclusion and Future Work

In this paper, we introduced a high-level blockchain based concept for improving flight planning efficiency and security. We believe that decentralization is the key for better performance and improved security as no central authority can hijack the whole system nor be targeted as the high-value asset it represents. Also, by distributing the data storage and computations, we remove all risks related to the single point of failure, such as the unavailability of services and data, the alteration of flight plans, the compromising/leakage of recorded information. However, we still have some challenges to overcome before being able to propose a fully functioning prototype. These are summarized as follows:

Refine. In our future work, we want to refine this high-level presentation of the system, in terms of technical functions. We will develop our mathematical model of the system, provide a threat model as well and detail the parameters and functions that we need in order to enable the introduced actions.

Choose. With a more technical view of the nodes, the data exchanged, and the protocols used to manipulate and share the data, we will be able to choose which type of blockchains is the most suitable to our application's context.

Analyze. We plan on deepen the mathematical model by providing an adversarial model, and perform a qualitative threat analysis on this system.

Implement. The final goal of this project is to implement the solution and test it on real-world data, that would be provided by EUROCONTROL. In addition, we would perform on evaluation of the model in terms of performance and security.

Once these challenges are addressed, our goal will be to evaluate the proposed solution and to compare it to traditional PKI-based architecture, currently deployed in the ATM environment, which are efficient but very expensive solutions. The comparison would determine the limitations and plus-value of one solution in regards with the other both in terms of performance and security.

Acknowledgment

This work was partly supported by the French government through the Toulouse graduate School of Aerospace Engineering (TSAE). Contract ANR-17-EURE-0005. We would also like to thank our colleagues from DSNA-DTI and EUROCONTROL who provided insight and expertise that greatly assisted the research.

References

[1] W. Zhang, M. Kamgarpour, D. Sun, and C. J. Tomlin, "A hierarchical flight planning framework for air traffic management," (IEEE, 2012), pp.179–194.

[2] N. Manager, "Overview - february 2019," (EUROCONTROL, 2019).

[3] P. Bonnefoy and R. Hansman, "Scalability and evolutionary dynamics of air transportation networks in the united states," in 7th AIAA ATIO Conf, 2nd CEIAT Int'l Conf on Innov and Integr in Aero Sciences, 17th LTA Systems Tech Conf; followed by 2nd TEOS Forum,(2007), p. 7773.

[4] Q. Ming and L. Songtao, "Overview of system wide information management and security analysis," in Autonomous Decentralized System (ISADS), 2017 IEEE 13th International Symposium on, (IEEE, 2017), pp. 191–194.

[5] J. S. Meserole and J. W. Moore, "What is system wide informationmanagement (swim)?" in 25th Digital Avionics Systems Conference, 2006 IEEE/AIAA, (IEEE, 2006), pp. 1–8.

[6] B. Stephens, “System-wide information management (swim) demonstration security architecture,” in 25th Digital Avionics Systems Conference, 2006 IEEE/AIAA, (IEEE, 2006), pp. 1–12.

[7] D. R. Team, “2019 global aerospace and defense industry outlook,”(2019).

[8] M. Burns, A. Sentance, B. Chow, C. Smith, E. Lee, A. Copeland, H. Morphet, C. Bottini, P.-E. Pichot, R. Scott, E. Clayton, B. Saraswati, R. Radia, R. Behan, and C. Franzeskides, “Issues and challenges forairport investment,” (PricewaterhouseCoopers, 2017).

[9] C. W. Johnson, “Preparing for cyber-attacks on air traffic managementinfrastructures: cyber-safety scenario generation,” (IET, 2012).

[10] C. W. Johnson, “Cyber security and the future of safety-critical air traffic management: identifying the challenges under nextgen and sesar,” (IET, 2015).

[11] B. Stephens, “Security architecture for system wide information management,” in Digital Avionics Systems Conference, 2005. DASC 2005. The 24th, vol. 2 (IEEE, 2005), pp. 10–pp.

[12] R. J. Reisman, “Air traffic management blockchain infrastructure forsecurity, authentication, and privacy,” (2019).

[13] N. Tinu, “A survey on blockchain technology-taxonomy, consensusalgorithms and applications,” (2018).

[14] M. C. Ballandies, M. M. Dapp, and E. Pournaras, “Decrypting distributed ledger design-taxonomy, classification and blockchain community evaluation,” (2018).

[15] J. R. Douceur, “The sybil attack,” inInternational workshop on peer-to-peer systems, (Springer, 2002), pp. 251–260

[16] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, “A survey on security and privacy issues of bitcoin,” (IEEE, 2018), pp. 3416–3452.

[17] 17. V. Buterin, “Bitcoin network shaken by blockchain fork,” (2013).

[18] A. Arora and S. K. Yadav, “Batman: Blockchain-based aircraft transmission mobile ad hoc network,” in Proceedings of 2nd International Conference on Communication, Computing and Networking, C. R. Krishna, M. Dutta, and R. Kumar, eds. (Springer Singapore, Singapore, 2019), pp. 233–240.

[19] I. S. Bonomo, I. R. Barbosa, L. Monteiro, C. Bassetto, A. de Barros Barreto, V. R. Borges, and L. Weigang, “Development of swim registry for air traffic management with the blockchain support,” in 2018 21st International Conference on Intelligent Transportation Systems (ITSC), (IEEE, 2018), pp. 3544–3549.

[20] Dinh, Tien Tuan Anh, Ji Wang, Gang Chen, Rui Liu, Beng Chin Ooi, and Kian-Lee Tan. "Blockbench: A framework for analyzing private blockchains." In *Proceedings of the 2017 ACM International Conference on Management of Data*, pp. 1085-1100. ACM, 2017.

[21] Vasin, Pavel. "Blackcoin’s proof-of-stake protocol v2." URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf71 (2014).

[22] Aura. https://github.com/paritytech/parity/wiki/Aura.

[23] Clique. https://github.com/ethereum/EIPs/issues/225.

[24] Gai, Fangyu, Baosheng Wang, Wenping Deng, and Wei Peng. "Proof of reputation: a reputation-based consensus protocol for peer-to-peer network." In *International Conference on Database Systems for Advanced Applications*, pp. 666-681. Springer, Cham, 2018.

[25] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[26] IOTA Developer Hub [Internet]. [cited 2018 Jan 25]. Available from: https://dev.iota.org/

[27] Schwartz, D., Youngs, N., and Britto, A. The Ripple Protocol Consensus Algorithm. White Paper. Ripple Labs Inc., San Francisco, CA, 2014; http://www.theblockchain.com/docs/Ripple%20Consensus%20Whitepaper.pdf

[28] Yli-Huumo, Jesse, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. "Where is current research on blockchain technology?—a systematic review." *PloS one* 11, no. 10 (2016): e0163477.