



The development of an uncrewed traffic management (UTM) system using cross-cutting technologies:

**Distributed ledgers and artificial intelligence**

# Executive summary

**The main goal of an UTM (uncrewed aircraft systems (UAS) traffic management) system, is the automatic, safe and efficient management of UAS operations. This needs to be achieved through the provision of a seamless set of services, products and infrastructure and in collaboration with all stakeholders in this new aviation environment. As a guidance to develop this new ecosystem, the International Civil Aviation Organisation's (ICAO) framework<sup>1</sup> for UTM systems has put together an initial review of essential parameters that should be in place. These include: the safety and efficiency of the UTM system, registration and identification methods, communications compatibility between UTM, traditional air traffic control (ATC) and air traffic management (ATM), detect and avoid (DAA) capabilities, geofencing-like systems, interoperability (with other systems and other States), adaptability of the architecture, infrastructure performance requirements (including reliance on existing infrastructure) and cyber security.**

Within this paper we are concentrating on those issues related to data exchange, interoperability, registration and identification of stakeholders, protected and permissioned data accessibility, immutability of the data, data privacy and cyber security. Within these areas we have focused on the characteristics and the potential of cross-cutting technologies such as distributed ledger technologies (DLTs) and artificial intelligence (AI) that could accelerate UTM solution development and implementation. For example, by addressing information and data exchange using distributed ledgers, we can also address secure registration and identification of users, safety and cyber security and information exchange and interoperability between stakeholders. Furthermore, we explore how the convergence of these two technologies can improve each others capabilities, for example, AI can enhance cyber security measures for DLTs while DLT can address the explainability, traceability of AI models as well as facilitating drone operations using AI federated learning with data collection and processing during operations based on standards.

Another important issue that we address in this paper is the element of trust within the UTM ecosystem. This would differ greatly from traditional trust frameworks currently applied within ATM that rely on the use of regulations, certifications and standards and direct controller-pilot communications. For this, we propose a governance framework that sets a series of rules for those stakeholders participating in a distributing ledger, so that they can provide and receive data and services in a safe and trustworthy environment.

Furthermore, we highlight the need for modernisation of ATM in order to allow for the interoperability between UTM and ATM over areas where both need to interact. ATM and UTM information must be accessible to all relevant stakeholders and the exchange of information may permit coincident ATM and UTM operations. At a minimum, the exchange of essential information at intersection areas must be ensured for safe and efficient operations. We believe the work done through the project Fly2Plan as part of the UK Future of Flight initiative contributes greatly to a vision of how this might happen.

We conclude that there is only one-way forward to achieve this ambitious and necessary advance in technology and solution development. This is, the collaboration between the UTM service providers, UTM digital infrastructure providers, unmanned aerial vehicles (UAVs) operators, physical infrastructure providers, ATM service providers, regulators, local and regional authorities, the general public and all the stakeholders that might have some point of interaction with this new aviation ecosystem. Only by opening up to collaboration, innovation and stakeholder engagement can we create a new and forward-thinking industry with an integrated and common vision.

<sup>1</sup> ICAO UTM - A Common Framework with Core Boundaries for Global Harmonization - Edition 3

# Introduction

**In recent years we have seen the development of new types of entrants into the aviation ecosystem, from uncrewed vehicles of small and medium size to urban air taxi prototypes. These new vehicles are different from traditional aircraft, and they will not be able to use the traditional aviation controller-pilot communications. Currently, in traditional ATM a significant number of functions are still conducted by human operators with already high workload levels. This is aggravated by the fact that these operators are supported by a multitude of separate systems (e.g. meteorological information, situational awareness through radar and communication systems, flight planning, etc), the information of which they have to analyse, understand, and then decide what to do with it. This is clearly not scalable. The industry is therefore looking into increasing the levels of automation and autonomy, in order to make the overall system more efficient to accommodate the increasing trend of air traffic, as well as enabling the introduction and the seamless integration of UAS<sup>2</sup>. Consequently, new ways of information exchange between these new airspace stakeholders are needed. This is acknowledged by ICAO<sup>1</sup>, it is already being explored by NASA and the FAA<sup>3</sup> and SESAR<sup>4</sup> and Eurocontrol<sup>5</sup> have numerous projects researching Concept of Operations (CONoPS), new technologies and use cases, with the goal of fully unlocking the benefits of UAS applications. In the UK, UK Research and Innovation (UKRI) through the Future of Flight Challenge<sup>6</sup> are investing in research, development and demonstrators to advance understanding, safe and seamless deployment of this new ecosystem and open up new markets and applications of new vehicles. So, the need to establish new ways of operating and exchanging meaningful information, based on standards, is obvious to all those involved and crucial for the way ahead.**

The nature of UTM and the diversity of new vehicles in the airspace means that it needs to be built on layers of information sharing and secured data exchange to achieve safe operations. For example, vehicle operators need to identify themselves as trusted entities and share their flight intent with each other. Moreover, being able to trust the exchanged information is fundamental in order to manage the complexity of the future demand while keeping high levels of safety and security. This trusted communication exchange is core to the modernisation of aviation data distribution and has been demonstrated effectively within the UK Future of Flight Challenge and the sponsored project Fly2Plan.

Interoperability is also an essential requirement. There will be a need to share operational information between UTM service providers and between both ATM and UTM providers. ATM and UTM information must be accessible to relevant stakeholders (airspace users, service providers, states, etc.).

At the same time as new aircraft are being introduced into the aviation ecosystem, there are new technologies that are maturing in order to meet the needs for new information exchange systems. Two of these new technologies are distributed ledger technologies (DLTs) and artificial intelligence (AI). The convergence of these two technologies is expected to revolutionise the next digital generation of integrated systems. AI can help build a machine learning system on DLTs for better security, scalability, and more effective personalisation and governance. DLT technologies can open up the way for new AI distributed solutions. Both have a lot of promising benefits that can address challenges of trustworthiness and push forwards the development and implementation of both technologies in the aviation industry, whilst addressing the existing legacy issues of conventional ATM data distribution.

This paper will explore the challenges of this new UTM aviation ecosystem from the technical and industry points of views. Its aim is to shape the thinking and development of solutions using new information exchange methods and propose the way forwards by using the above cutting-edge technologies to address the UTM challenges indicated above.

<sup>2</sup> SESAR sample projects: Metropolis 2, EuroDRONE, Aura

<sup>3</sup> FAA and NASA [www.faa.gov/uas/research\\_development/traffic\\_management/utm\\_pilot\\_program/](http://www.faa.gov/uas/research_development/traffic_management/utm_pilot_program/)

<sup>4</sup> SESAR sample projects: Metropolis 2, EuroDRONE, Aura

<sup>5</sup> Eurocontrol, Concept of Operations for European UTM Systems

<sup>6</sup> [www.ukri.org/our-work/our-main-funds/industrial-strategy-challenge-fund/future-of-mobility/future-flight-challenge/](http://www.ukri.org/our-work/our-main-funds/industrial-strategy-challenge-fund/future-of-mobility/future-flight-challenge/)

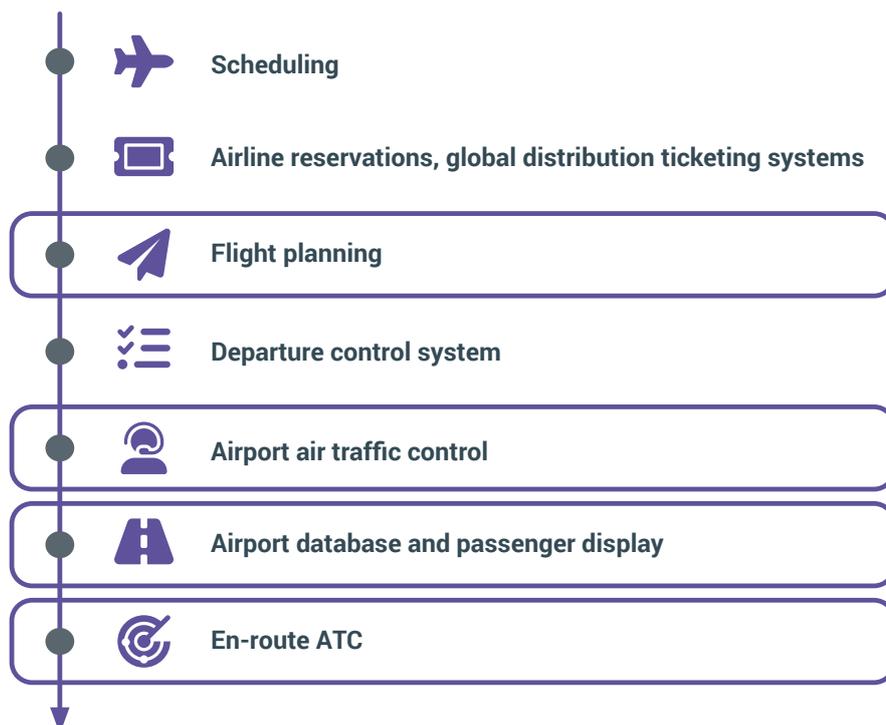
# 1 The current industry context: UTM challenges

According to the PricewaterhouseCoopers (PWC) and UKRI 2021 report<sup>7</sup>, uncrewed and autonomous aviation is predicted to unlock £42 billion to the UK economy by 2030. European demand suggests a valuation in excess of EUR 10 billion annually, in nominal terms, by 2035 and over EUR 15 billion annually by 2050<sup>8</sup>. In terms of operational savings, PWC<sup>7</sup> analysis on a particular case study using drones for inspection tasks, showed that the expected costs of undertaking powerline inspection using beyond visual line of sight (BVLOS) drones was around 34% less than business as usual.

The demand of drones on all areas of the airspace for different applications highlights the critical nature of creating a new UTM type of system. Drones will create new forms of traffic especially at very low levels of airspace with high demand in densely populated areas where risk levels will be increased. But the system-of-systems that keeps our skies safe for all traditional forms of flight cannot cope with the increasing demands. To make the most of the economic opportunities of future flight – with all kinds of autonomous drones performing different tasks, as well as the traditional aircraft with pilot and crew – we need to use our airspace efficiently and safely. And that means getting on top of huge amounts of data, showing what is flying where. Appropriate new and adapted procedures along with the development of technology related to the management of airspace are a "must-have" for safely unlocking growth.

The difficulty is, today's technology used to coordinate and manage aviation is distinctly last-century. Information systems used by many airports, airlines and air traffic controllers pre-date the Internet, but they are still the basis of the aviation world. New technology is rarely adopted first by the aviation industry, and it has become a technology ecosystem that is "hermetically sealed", insulated from the internet and all its threats. So that is a big challenge to new players in aviation who have embraced the cloud computing offerings of Microsoft or Amazon, and operate their equipment using public 4G/5G connectivity. Outdated and unreliable technology is a drag on the existing aviation industry. A Cranfield study<sup>9</sup> has estimated that 60 percent of flight delays that aren't weather-related are due to failures in handling data. In this day and age, consumer expectation couldn't be higher and IT failures, often causing chaos at busy Airports are inexcusable. For example, a notable disruption suffered by British Airways (BA) at London's Heathrow and Gatwick airports in May 2017 when a power surge knocked out its IT system forcing it to cancel almost two-thirds of all flights, cost the airline £80 million<sup>10</sup> which fell on a busy bank holiday weekend. Another BA IT failure with check-in systems in 2018 cost the airline in the region of £8 million<sup>11</sup>. Heathrow suffered further setbacks in June 2017 after a baggage system failure prevented luggage from being checked in at terminals 3 and 5. Other disruptions at the airport included the failure of e-gates at security three times during 3 months in 2021 and we have seen further numerous disruptions of IT systems of other airlines and airports.

## ATM processes that can benefit from integrated DLT and AI technologies



The processes highlighted were considered in the Fly2Plan project and the benefits of using DLT and AI were demonstrated specifically in these aviation data distribution processes.

<sup>7</sup> PWC UKRI Future of Flight Challenge, Socio-economic study <https://www.reuters.com/article/us-iag-ceo-idUSKBN1961H2>

<sup>8</sup> SESAR, European Drones Outlook study, [www.sesarju.eu/sites/default/files/documents/reports/European\\_Drones\\_Outlook\\_Study\\_2016.pdf](http://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf)

<sup>9</sup> DARTEC, Cranfield University, Addressing the Digital Aviation Challenge, 20

<sup>10</sup> [www.reuters.com/article/us-iag-ceo-idUSKBN1961H2](http://www.reuters.com/article/us-iag-ceo-idUSKBN1961H2)

<sup>11</sup> <https://www.internationalairportreview.com/news/99786/british-airways-it-systems-failure/>

The Fly2Plan project was born from recognising that a transformation is needed. Working with traditional aviation companies such as Heathrow airport, British Airways, and NATS (the UK air traffic services provider), the teams have demonstrated how a new system-of-systems for aviation data, based on standards, could replace the one that has developed bit by bit over decades of human-controlled flight: a reliable, more efficient new system that would be much easier to scale for the autonomous flights of the future. Cloud infrastructure and DLTs can blend to result in airspace being managed more securely for all forms of users: a decentralised system means there's no single, central critical point that can fail, or be attacked. From an environmental point of view by using cloud infrastructure, the need for on-premise, power-hungry data centres can be reduced.

Other challenges remain, regulation still limits the extent to which drones can operate on their own and the ease of which operations can expand across countries using the same drones and certifications. Critical parts of the evolving regulation will be the extent to which drones can be operated BVLOS, in populated areas or/and without a dedicated pilot per each drone. Furthermore, societal worries on privacy and accidents create an additional barrier that must be overcome in order for regulators to allow flights in populated areas. These concerns over safety are magnified by the fact drones are bringing aviation capabilities to a group of new users. The "newness" of aviation to these users increases the number of issues regulators must consider<sup>12</sup>. EASA has released regulatory frameworks for certain types of drones and uses<sup>12</sup> and in February 2022 published the drone guidance extended and updated to support safe drone operations in EASA Member States<sup>12</sup>. Although this is a good start, there is still more detail to be added and it is envisaged that it will be an evolving document. They also recognise that more time is needed to continue the discussions with stakeholders on the amendments to Specific Operations Risk Assessment (SORA) related to the design verification of drones. Also, a distinction is drawn between 'certified' drones and 'specific' drones in anticipating categories being defined as part of EASA's pending framework. 'Specific' drones, representing medium levels of risk, have been defined generally as being below 25 kilograms and flying near or below 150 metres. The 'certified' category is used for drones flying well above 150 metres – i.e., have impact on controlled airspace as well as uncontrolled airspace. This highlights once again the need for collaboration between UTM and ATM systems<sup>13</sup> and the importance of new ways for secured identification and registration of drone operators and vehicles.

Volumes of drones might grow to become 10 times the number of today's flights, operating well below the cruising altitudes of an airliner, and in and out of populated areas to deliver urban air mobility (UAM). On the route to scale-up, pilots will likely fly the first generations of electric vertical take-off and landing (eVTOL) craft in-vehicle, long before remote or even autonomous operations are proven to be safe. A trained and qualified human decision-maker carries the cognitive ability to sense, see and avoid risks, will hold appropriate insurance to cover their liabilities, and importantly, make balanced and intelligent safety choices with full situational awareness. But as demand increases, the "humans in the loop" in the system will gradually shift to managing by exception, supported by advanced tools and becoming more reliant on artificial intelligence (AI).

An (AI) driven ecosystem requires a resilient, trusted digital infrastructure to ensure that the best possible choices are made for safely operating in all weathers, terrains and traffic densities (see CAP2272). Accountable and explainable decisions will be required at all times, and the trust placed on data will require AI to monitor anomalous behaviours, signalling cyber-threats or attacks under way. Solutions using this type of emerging technology lack clear guidelines on acceptable levels of performance for increasingly automated and autonomous systems, particularly for safety-critical operations and the onus is on the operators and solution providers to assess and demonstrate system performance based on tolerable risk for their application.

In Fly2Plan, we've seen two technologies coming together as a virtuous circle, these are DLTs and AI technologies and the benefits of their convergence for solution development. When considering the benefits of DLTs for AI we will explore using distributed ledgers and self-sovereign identity to get the best collaborative version of truth and trust. AI for DLTs will investigate how AI techniques can spot threat and anomalies in a complex decentralised multi-party ecosystem. As we can see, the technology and industry challenges are there but the solutions are also under way.

<sup>12</sup> EASA Civil drones regulations [www.easa.europa.eu/domains/civil-drones](http://www.easa.europa.eu/domains/civil-drones)

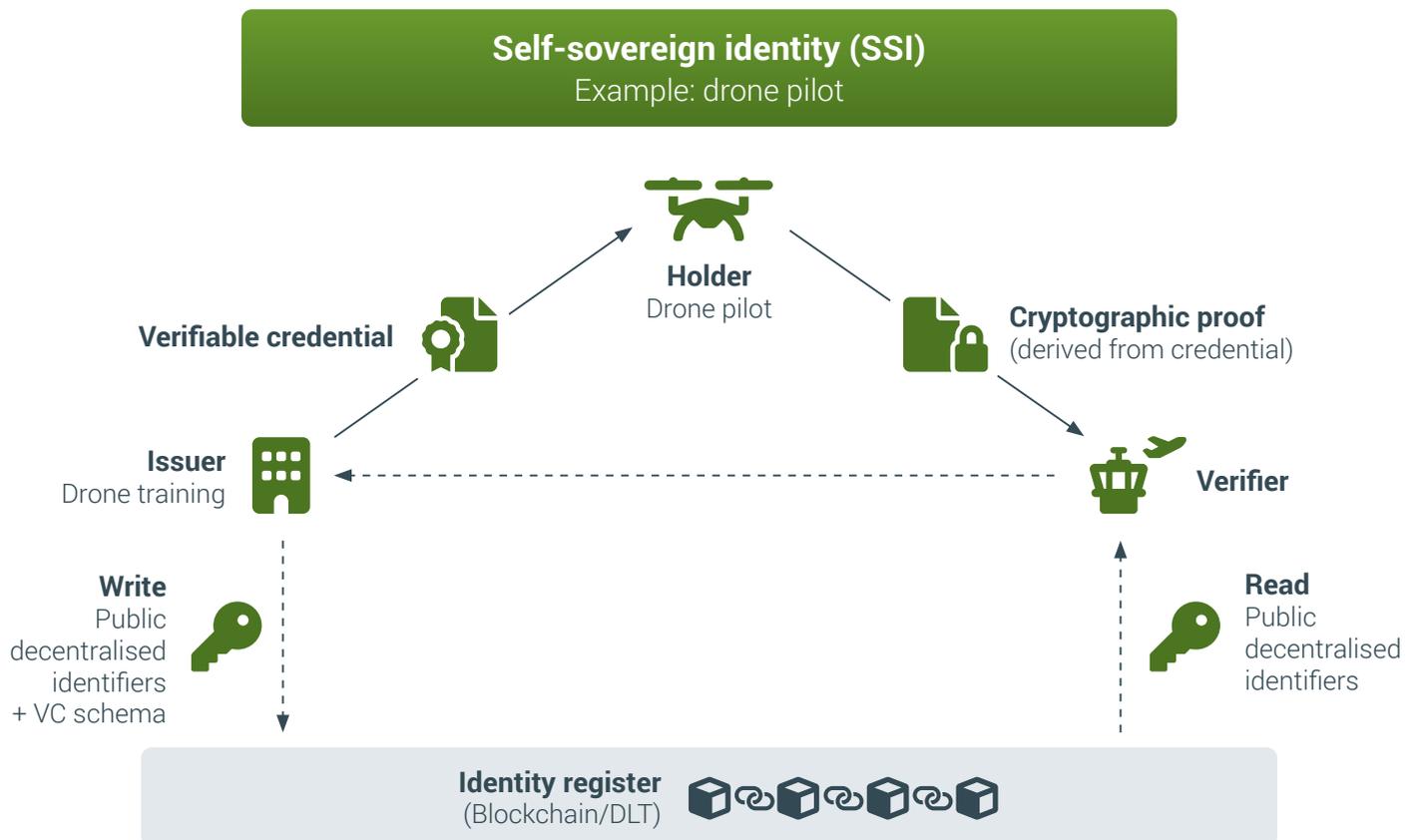
<sup>13</sup> EASA, Drone guidance extended and updated to support safe drone operations in EASA Member States [www.easa.europa.eu/newsroom-and-events/news/drone-guidance-extended-and-updated-support-safe-drone-operations-easa](http://www.easa.europa.eu/newsroom-and-events/news/drone-guidance-extended-and-updated-support-safe-drone-operations-easa)

## 2.1 DLT technology for UTM

Distributed systems describe those formed from a multitude of independent stakeholders and computers coming together to achieve common goals. The existing ATM infrastructure is a form of distributed system, ensuring interoperability through global standards. However, many of the messaging formats and protocols come from an era of fixed lines and teletype machines and any homogenisation to a single entity to build a unified infrastructure that meets the global needs of safety and efficiency is unlikely to occur. A vast amount of technological evolution in innovation has occurred since, which aviation IT has failed to exploit, much to its own detriment.

Regarding modern distributed systems, the explosion of interest in blockchain technology has brought forth a software toolkit that is exceptionally well suited to rebuilding UTM (and ATM) as a system-of-interoperable-systems that replaces old protocols, human-level trust, obscurity and lockout with computational verification of actors, assertions, and processes.

Take for example the potential for DLT to enable thousands of independent computers to achieve uniformity of history and view over stateful data<sup>14</sup>, a process known as consensus. These systems also embed cryptographically-enforced controls over user actions, and can allow for the embedding of parameterised process controls (so-called 'smart contracts'). Such systems can be paired with other distributed technologies such as direct peer-to-peer data transfers for exchanging large stateless data objects (e.g. radar data) and Verifiable Credentials and Self-Sovereign Identity (SSI) technology for encapsulating the permissions of independent actors. This second example is illustrated in the figure below which shows the 'trust triangle' formed between issuer, holder, and verifier of a drone pilot's credentials.



<sup>14</sup> McKinsey, Notes From the AI Frontier: Modeling the Impact of AI on the World Economy. Accessed: Mar. 4, 2020. Available: [www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economySeptember-2018.ashx](http://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economySeptember-2018.ashx)

With simple architectural definitions, open source code and open APIs, this base infrastructure can be used to underpin the future filing of flight plans, the capture and exchange of live routing data, and ensure the right data is made available to the right stakeholders at the right time, with embedded access controls for visibility of and interactions with said data. This data availability, verifiability, and traceable liability can only enhance situational awareness and the development of tactical decisions by humans or future AI systems.

With the appropriate will, these approaches could also enhance the existing ATM communication infrastructure, or be made interoperable with it through suitable interpreters and interfaces. National digital UTM/ATM infrastructures could be underpinned by core stakeholders such as large airports or air traffic control centres, and bridged to other national infrastructures for the verifiable and safe point-to-point routing of flight or other critical data. These could be cryptographically wrapped to control legibility, further enhanced with read receipts, made machine readable and processable for risk analysis, and co-interpretation with live radar or weather data.

The critical point to this is that truly distributed approaches are now available, to make the underlying digital infrastructure of our UTM and ATM systems reflect the real-world interactions of its users and stakeholders rather than enforcing a one-size-fits-all approach.

Some of the challenges that lie in the way of achieving this vision of a modular yet interoperable distributed system topology for future UTM (and potentially ATM) include scalability, sustainability, technological instability and cyber security.

Scalability and sustainability go hand-in-hand with these technologies, and derive from the computer science fundamentals that underlie them. Following their initial invention in the late 1980s, multiple methods and algorithms have since been developed that aim to bring disparate independent computers to consensus (a singular view over stateful data). Without getting too far into the details, there is a trade-off between the number of consensus participant computers within a network, the maximum message density or finalisation rate, message size, and physical distribution of participants.

The class of consensus algorithms that underpin public blockchains (e.g. Bitcoin) enable tens of thousands of consensus participants, but have low message finalisation rates and consume a lot of energy to achieve this. Other consensus algorithms (including the original versions invented) can be run on ordinary laptops without any real processing power, with far higher messaging rates, but only tolerate 1-2 orders of magnitude fewer consensus participants than public blockchains.

However, these trade-offs can be made to balance out if the network topology is appropriately designed. A selection of participants drawn from recognised aviation organisations (e.g. airports, major operators) could form the core consensus group for securing the ledger of record. Many tens of thousands of external organisations or users could then be variously able to hold clones of the ledger or submit transactions to it, but not be able to take part in its consensus. Across aerospace borders, there could be bridging solutions built between private national ecosystems with shared consensus.

This leads into the challenge of technological instability. Blockchain was invented just over a decade ago, and already there have been at least 10 unique approaches (and thousands of clones of these) to implement a distributed ledger. Prematurely selecting the consensus algorithm and other elements from the 'distributed ledger toolkit', including programmability or 'smart contracting' may lead to significant technical debt should better solutions arrive in due course. However, this must be balanced against the cost of technological inertia in taking no action today.

Finally, cyber security is an ever-present challenge to computer systems, and is no different in a distributed system. Fortunately, Byzantine Fault Tolerant consensus algorithms (a sub-class of consensus algorithms) do allow the ledger to tolerate a proportion of malicious actors within the system and still achieve faithful data availability and replication. Furthermore, gross collusion or corruption of consensus actors only allows for the censorship of new transactions, and not the editing of submitted transactions, and the theft of cryptographic signing keys only allows the manipulation of new and not historic ledger entries. These features intrinsic to (certain) distributed ledgers can overcome many of the fears of system intrusion and corruption.

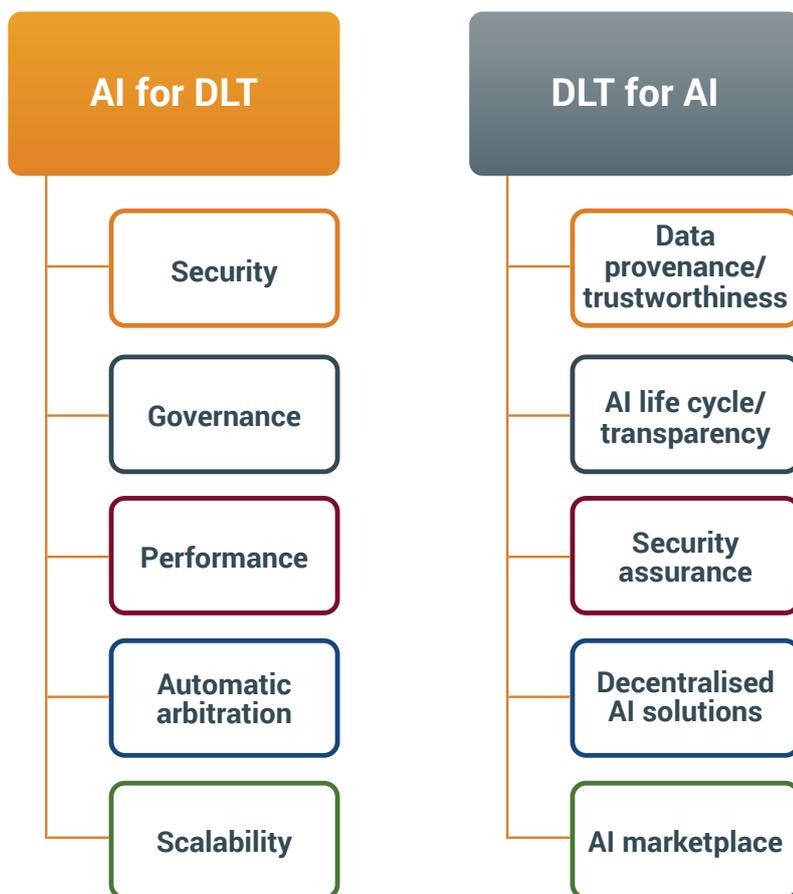
In terms of 'smart contracting' or user-programmable functionality, there are cyber security challenges with Turing Complete virtual machines which must be carefully managed in terms of who is allowed to submit code to be executed, and how strictly it is reviewed prior to acceptance. Domain-specific programmability, to restrict the permitted behaviours, may be more desirable in mission-critical situations, such as aviation.

Perhaps the greatest cyber security risk is the permanence of records in a distributed ledger. No matter the cryptographic methods selected, they could be susceptible to decryption and intrusion at some point in the distant future. The choice of cryptography, and the contents of messages must therefore be carefully considered in the overall design of a DLT-based UTM (or ATM) solution.

## 2.2 The convergence of AI and DLT for UTM

Artificial intelligence (AI) and distributed ledger technology (DLT) are among today's most exciting developments in information technology. McKinsey Global Institute 2018 report estimated that the application of AI in various industries could deliver an additional global economic output of around USD 13 trillion by 2030<sup>14</sup>. Regarding DLTs, a study by the World Economic Forum<sup>15</sup> predicts that by 2025, up to 10% of the world's GDP may be stored on a blockchain, which is the most commonly used concept of DLT today. Furthermore, the integration of AI and DLT yields great potential to advance the capabilities of both technologies. As a result, we are increasingly seeing the emergence of potential applications using both in combination. Much of the work is still in a nascent stage with practical applications being still tested and results assessed. The market and industry evolution into new products combining the two technologies has still to materialise.

### Benefits of integrating AI and DLT



Taking the above into account, within the context of UTM aviation ecosystem we can foresee scenarios where combination of both technologies would be extremely beneficial. Within the following sections we will explore some of the advantages of using AI to enhance DLTs and DLTs applications for AI. For example, AI can support DLT systems by increasing their security and scalability, by acting as an automated referee and governance mechanism, and for privacy-preserving personalized systems<sup>16</sup> whereas AI can benefit from DLTs immutability for trustworthiness and for applications such as Federated Learning.

<sup>15</sup> World Economic Forum. Building Block(chain)s for a Better Planet. Accessed: Mar. 4, 2020. Available: [www3.weforum.org/docs/WEF\\_Building-Blockchains.pdf](http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf)

<sup>16</sup> T.N. Dinh and M.T. Thai, "AI and blockchain: A disruptive integration," Computer, vol. 51, no. 9, pp. 48–53, Sep. 2018.

## 2.2.1 AI for DLT

### 2.2.1.1 AI for DLT Security in UTM

**AI can be used to improve the detection of anomalous and malicious behaviour in many digital systems; this includes DLT-based systems. Anomaly-detection algorithms are required for the detection of anomalous UTM message content. They are also required more broadly for the detection of anomalous behaviour of participants in the DLT. This requires detailed threat modelling to understand what behaviours of actors may signal attempts to attack or game the system. Attacks on a DLT-based system could include, for example, attempts by an actor to gain a certain level of control (e.g., by taking control of a high enough proportion of network nodes in a Practical Byzantine Fault Tolerance (PBFT) based system, or gaining control of a high enough level of computing power in a proof-of-work-based system).**

AI (or advanced machine learning) algorithms can, as in other anomaly-detection systems, be trained on historical data to recognise “expected” UTM message content and the “expected” behaviours of parties, and to thus detect deviations that may signal misbehaviour on a DLT system. This can help to increase the reliability of the data shared over the DLT: suspected malign messages can be removed or marked-up. It can also help to identify malign actors on the system, such that they can be dealt with. This could mean removing them from the system, for example, or it could mean that individual actors develop an understanding that the data these parties post may not be trustworthy.

### 2.2.1.2 AI for DLT operational efficiency

**The characteristics of AI technology mean that it could support DLTs by increasing their scalability, by acting as an automated governance mechanism, and for privacy-preserving personalised systems. For example, when there is a spike in the number of transactions, the AI might be smart enough to increase the block creation rate, which would increase the throughput at the cost of longer confirmation times.**

Also, protocol governance could be an adjusted proof-of-work-based consensus mechanism. The DLT protocol could use AI to regularly update system governance parameters, such as the ideal number of validators and the rate of block creation. In the case of human-in-the-loop-based AI smart contract governance, an AI may assist a human decision maker which can intervene at any time in case an AI-based system faces and detects an irregular situation.

Another potential application relates to the proof of work mechanism. The proof-of-work mechanism consumes large amounts of energy for protocols. Some authors therefore propose a proof of useful work mechanism, in which miners train an AI model instead of finding a number for a certain block hash. The block which contains an AI model with the least test error is then accepted as the new block by the other nodes<sup>17</sup>.

<sup>17</sup> K.D. Pandl et al.: On the Convergence of AI and DLT: Scoping Review and Future Research Agenda, IEEE Explore, 2020.

## 2.2.2 DLT for AI

### 2.2.2.1 DLT for AI trustworthiness

**Interpreting and explaining AI algorithms is one of the main barriers that AI is facing nowadays with regards to its practical implementation. The inability to fully understand the reasons why AI algorithms perform as they do, is a real problem for practical implementation and trust, particularly in highly safety-critical environments. There is a gap between the research community and business sectors that has been impeding the full penetration of the newest AI models in sectors that have traditionally lagged behind in the digital transformation of their processes<sup>18</sup>.**

One of the elements of trust on AI is the provenance and data quality, and consistency across sources used to train and test the AI algorithms. These data, which provides the foundation for creating trusted AI, can be stored in many different ways. The advantage of a distributed system is that it could store provenance information without requiring a trusted central entity. In this sense, DLTs provide a good solution to provenance data that can be validated and cross-checked by a diverse set of entities. The goal is to provide an immutable record of the origin of data (provided by participants or organizations) used to train the models. This in turn leads to a more verifiable and, therefore, more trusted AI solution.

Apart from data provenance, another important element in AI in order to increase trust, is to have the ability to track the development of the data flow and complex behaviours of AI-based systems. DLTs can do exactly that, recording a log of significant events in the data processing and decision-making chain. Through tracking these recordings, we can assess behaviours of AI-based systems across different data input and application scenarios and gain more understanding of, and confidence in, the decisions made by those systems. A clear trail to trace back the machine decision process provides insights to balance performance and prediction accuracy with the explainability of the system<sup>16</sup>.

<sup>18</sup> A. Barredo Arrieta et al. 2020, Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI, Information Fusion, vol. 58, pp. 82–115.

## 2.2.2.2 DLT for AI federated learning

**Traditionally, AI models are developed and deployed in a centralised way. However, when implementing these models in operations this centralisation can cause many issues. For example, when using drones for surveillance and maintenance applications, transferring the collected data to the central station for processing can involve a large computational effort that can lead to operational inefficiencies and various privacy and security threats. DLTs can serve to organise the federated (i.e., decentralised) training and learning of AI models<sup>16</sup>. In such a federated learning (FL) scenario, no input training data is directly shared. Instead, partial AI models are being trained by nodes participating in the FL network (i.e. drones), while training data, provenance and the integrity of the partial AI models are preserved using a distributed ledger. This is particularly important when designing drone operations at scale. Therefore, moving towards decentralised learning represents an efficient solution for drone applications that require autonomous monitoring and real-time decision making.**

Another important issue for drone operations is trajectory planning. The trajectory of drones may impact their energy efficiency and the signal strength between smart devices in smart environments. FL can enable drone edge intelligence to identify suitable trajectories based on predicting the energy consumption for each trajectory<sup>19</sup>. Also, DLT and AI technology can be used to optimise operations. For example, if the battery of one drone is almost depleted, an AI can identify the nearest one that may replace it and carry on with the task while the other one is sent to a nearby charging point. Furthermore, if one sensor's data is not received due to the presence of a malicious device, the drone can borrow the missing data from the nearest drone using the DLT.

In terms of fleet management, FL techniques can play a vital role in data transmission and routing models (based on speed, direction, energy etc.) among multi-drone edge intelligence. AI can be implemented to predict the routine performance regarding optimal routing path for each drone. The local model is aggregated to generate a global model to control multi-drone fleet with the help of a decentralised ledger. This also addresses the risk of single point failure<sup>20</sup>.

There still remain several challenges related to drone operations DLT and AI technologies that need to be explored in real-world cases, but the convergence of both technologies promises to offer great opportunities for deploying drone applications. Linking these two technologies could also help address some of the challenges highlighted by the International Civil Aviation Organisation's (ICAO) framework<sup>1</sup> for UTM systems. For example, in this section we have discussed the benefits that convergence could offer for the safety and efficiency of the UTM system using DLTs and AI for planning operations and federated learning for capture and processing of data, how AI can address and enhance cyber security issues of DLTs so they are trusted in an operating environment.

<sup>19</sup> S.Hamood et al. Predictive estimation of optimal signal strength from drones over iot frameworks in smart cities. IEEE Transactions on Mobile Computing, 2021.

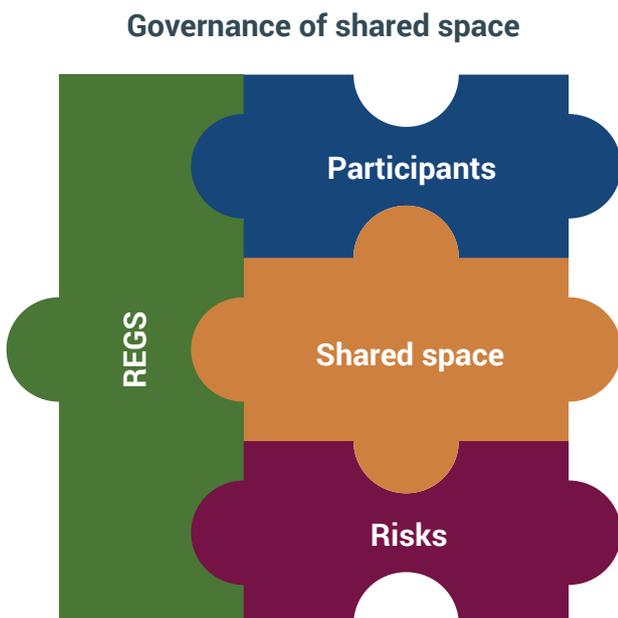
<sup>20</sup> Hankz Hankui Zhuo, Wenfeng Feng, Qian Xu, Qiang Yang, and Yufeng Lin. Federated reinforcement learning. arXiv preprint arXiv:1901.08277, 2019.

## 2.3 Implementing new technology for data interchange within UTM: Governance based on an operational code of participation

Within the air transport industry, there are many participants and interdisciplinary business flows such as manufacturing, carrier services, air traffic management and real-time air-ground communication, where security and safety established procedures ensure trust for the whole operation. Normally, in traditional aviation this trust between stakeholders is provided by certification, standards and regulations. However, these do not exist yet for all of the new UTM ecosystem. Therefore, within Fly2Plan we designed a governance framework for a UTM ecosystem in order to set up rules of participation and define responsibilities especially within the setting of new technologies such as DLTs.

We propose a peer to peer data sharing for certain data classes to support stakeholder business processes and open adjacent subscriptions for supply chain, retail and drone services by a trust framework of digitally governed operating rules, based on robust data models and standards. The aims of the governance framework are to:

- identify, monitor and mitigate risks pro-actively to enable commercial service operation backed by 'group insurance',
- support risk management by auditable reports on stakeholder engagement in relevant business processes by a 'smart contract',
- enable innovation and goal congruence for each 'smart contract' by transparency and adaptability by open source methodologies.



- **Structure**
  - Trust framework
  - Participants and roles
  - Risk and insurance
- **Process and data governance**
  - Process definitions based on existing ISO and other standards
  - Permissions and rules of operation in shared space
  - Privacy and security in shared space and assurance assumptions in enterprise space
  - Service level agreements (SLAs) to operate to plans submitted
  - Demand signals and fulfilment signals as per rules
- **Proposed commercial model options in shared space**

At the governance level, data sharing is underpinned by 'algorithmic governance' to provide a trust framework, or, 'highway code' enabling auditable interactions of data consumption and data publication amongst stakeholders. The 'highway code' consists of core rules which can be adapted to the requirements for each 'smart contract'.

## The Operating Rules

The participants for drone and traditional airspace users each perform a role as described below (in the context of the UK).

Participants	Description
Flight Operators	Airlines or drone operators
Hub Operators	Airports, drone ports and pop ups
Regulators	CAA and ICAO
Airspace Managers/Network Operators	Airports, NATS, drone ports
Pilots	Drone pilots and plane pilots

Table 1: Participants in a UTM governance framework

The participants of a UTM system governance framework interact with each other in a shared space to ensure safe operations for societal benefits and ensure conflicts of interest are addressed. New actors will be required to carry out certification, or assurance, which will be required by industry, for example insurance, or regulators.

Beneficiaries/ Societal impact	PAX	Consumer	Environment	Local airport communities		Operations in Shared Space based on:
Operations participants	Airlines	Airport	Drone operators	ANSP		
Technology and IoT solutions	Blockchain operators	Plane MFG	Drone MFG	Software and IoT solutions	Data service brokers	
Regulators and security	ICAO	CAA	Government	EASA/SWIM		
Risk and certification	Aviation insurers	Drone insurers	Universities	Private certification bodies	Industry assurance	

The core rules of governance are detailed below and are the minimum necessary to put the governance framework into operation.

<b>Rule 1</b>	Role-based participants based on domestic registration and predicted volumes.
<b>Rule 2</b>	Credential used to confirm registration requirements of participants.
<b>Rule 3</b>	Reversal of transactions for off chain activity e.g., fraud or human error.
<b>Rule 4</b>	Use case data management on chain or off chain with hashed off chain data storage. Data off block will adapt based on events. Determination of what data should be on-chain or off-chain.
<b>Rule 5</b>	Data quality index and notification and rejection. Determination of who can access and validate each transaction.
<b>Rule 6</b>	Defined set of shared data for operational use for each use case, based on data standards. Ability to store some historic data off chain.
<b>Rule 7</b>	Changes in technology, security and relevant funding. Published planned changes and process for unplanned changes.

## Implementation of the operating rules examples

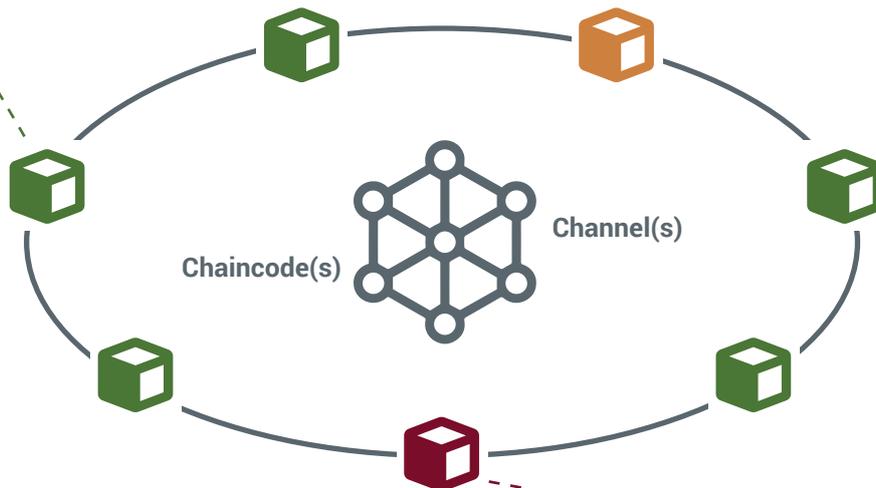
### Rule 1: Role-based participants based on domestic registration and predicted volumes

#### Participating member node

- Can be involved in the consensus of a DLT between members of the network.
- Can create a consortium (channel and/or chaincode) and invite other members to join.
- Can approve or disapprove new member joining a channel or chaincode.
- Can initiate and sign its transactions with its own key(s).
- Can receive private/restricted data.

#### Non-participating member node

- **Cannot** be involved in the consensus.
- Can join consortium by invitation.
- Can initiate and sign its transactions with its own key(s).
- Can receive private/restricted data.



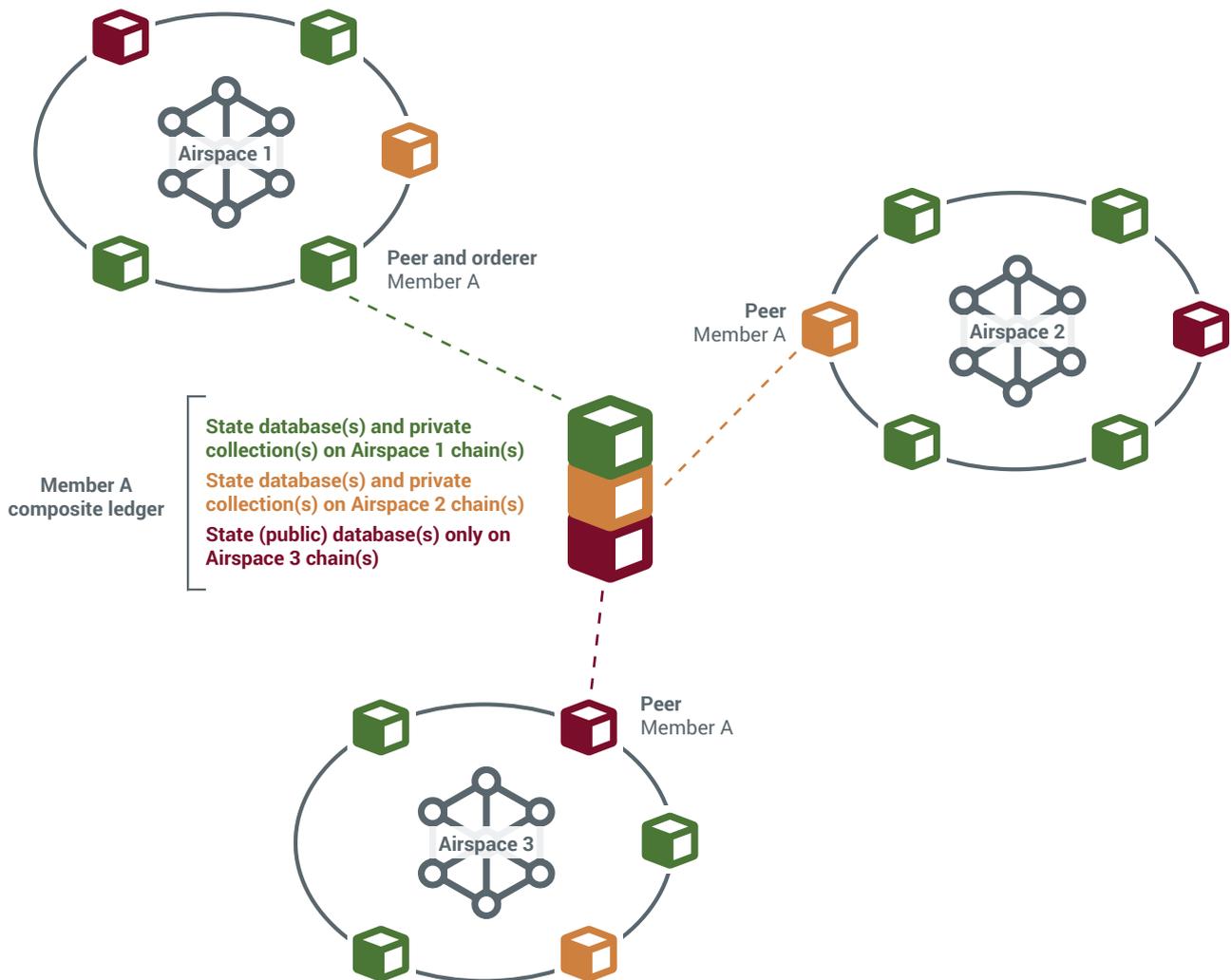
#### Non-participating member node

- Can join consortium by invitation.
- **Cannot** be involved in the consensus.
- **Cannot** submit a transaction.
- **Cannot** receive private data.

For example, according to Rule 1, only domestic registered corporations who are Flight Operators, Hub Operators and Network Operators are permitted to operate a participating member node of the DLT. Participating member nodes are the only ones involved in the consensus. This means only participating member nodes can amend a transaction and deny a transaction (here meaning a data exchange). Non-participating member nodes are not involved in consensus and can send transactions and read transactions only if they have been assigned a read only permission.

The operating rules also act to ensure data of a certain quality is shared in line with preferences set by both participating member node entities and non-participating member node entities and data accessibility is permitted and kept in privacy according to access rules. So, for example, in Rule 4 the data visible to Hub Operators will be different to data visible to Flight Operators.

**Rule 4: Use case data management. Composite ledger from different memberships on different channels.**



The proposed governance model focuses principally on security, transparency, risk mitigation and collaboration amongst participants in a UTM ecosystem using a DLT model, utilising the correct digital representation of the value chain regarding these interactions and processes. As a result, the governance proposed assumes a decentralised mode of operation as a better means to harness new technology safely in an emergent landscape. In this way we can provide digital 'assurances' on entities, data sharing and adherence to operating rules so that risks are managed and mitigated to enable innovation with newer technologies such as DLTs (and AI) and secure societal benefits.

# 3 The way ahead: the UK Future of Flight roadmap

## 3.1 The UK Future of Flight roadmap and the importance of new technologies and standards for data interchange in UTM

The Future Flight Challenge jointly funded by the UK government and industry, has brought together stakeholders from businesses, government bodies, research and technology organisations, academia, professional institutions, local authorities, social scientists and consumers. The main goal is to facilitate a new aviation ecosystem with new entrants such as drones and new passenger vehicles for local and regional mobility and pave the way for innovative solutions and economic growth.

In order to achieve this goal, the design of the Future Flight roadmap involved the assessment of products, systems, services, capabilities and enablers to determine the highest priority areas. These were categorised into three main themes for the Future Flight roadmap:

- Infrastructure (physical, digital, energy and airspace).
- Air vehicle capabilities.
- Regulatory/knowledge-based infrastructure (regulation, standards, insurance, social licence, skills, training, intellectual property).

As per the focus of this paper, in terms of the digital infrastructure roadmap, the table below highlights some of the necessary developments that need to happen at different stages of the roadmap.

Present day Development	2024 Demonstration	2026 Industrialisation	2028 Scaling	2030 Service-based
Development of secure digital infrastructure driven by new and disruptive technology.	Consistent and centralised drone registrations. Approved/permitted operations through UTM provider.	Higher volume of UTM traffic safely enabled through strategic deconfliction and efficiency planning.	New airspace categories in place enabling large scale UTM operations.	Fully integrated ATM and UTM service of autonomous systems with global interoperability for high volume use of different/multiple classes of air vehicles.
Development of data exchange services.	Certified and interoperable UTM services available.	Secure and reliable communication and surveillance systems, leveraging existing national infrastructure.	Increasing number of existing airports modernised to support digital mobility-as-a-service operations.	Increased digitisation of air operations.
Emergence of UTM capabilities building upon an existing and established ATM system.	Increasing integration of UTM with evolving ATM systems. Future airspace changes agreed to support higher volume, widespread UTM operations.	Integration of advanced air mobility (AAM) and drone operations with airport systems (e.g. CDM – Collaborative Decision Making) and airport ATC system.	Increasing number of existing airfields modernised and vertiports deployed supporting a highly distributed aviation network.	Mobile/on-demand booking solutions available for AAM vehicles.

Table 2: Future of Flight roadmap elements for UTM digital solutions<sup>23</sup>

<sup>23</sup> IUK Future of Flight Vision and Roadmap, 2021 <https://www.ukri.org/publications/future-flight-vision-and-roadmap/>

The project Fly2Plan was one of the projects funded during Phase 2 to concentrate on digital infrastructure research and development. The project concentrated on three 'use cases' focusing on the development of a secure digital infrastructure driven by new and disruptive technology as applying DLT and AI as well as developing data exchange services and exploring the interaction with ATM systems.

We have taken SITA (the airline's global networks provider) and IBS Software (Heathrow's airport database provider) on a journey of product development to make FlightChain<sup>21</sup> suitable for deployment in the ecosystem – we've shown how Hyperledger, with some changes to its default consensus algorithm, a new identity and access management concept, and containerisation can deploy a global-scale data ecosystem for the soon-to-come exponential increase in users taking to the air. Together with a governance workstream looking at all matters related to insurance, liabilities and alignment of interests, we've built a model that bridges the generational divide of aviation companies born before and after the internet.

Cyber security and AI researchers in Oxford and Cranfield Universities have shown how modernising can assure autonomy with accountable and traceable decisions. And experts in modern aviation data exchange standards, Rockport Software and Cirium have shown how the technology complements the global System Wide Information Management (SWIM) concept<sup>22</sup>. The Civil Aviation Authority had this to say:

"Fly2Plan have collaborated extremely well with the CAA throughout FFC (Future Flight Challenge) Phase 2, especially around the cyber security aspects of their innovation. Collaborating with the Fly2Plan project is helping to mature the CAA's regulatory readiness to tackle cyber-threats that future, unique innovation may bring. We look forward to the outcomes of the research and development phase of Fly2Plan."

Ultimately, the Fly2Plan project is about making the most of a rare opportunity. What we're trying to bring about is not just a periodic asset refresh which leaves the underlying ways of working unchanged. This is a once-in-a-generation chance to improve things fundamentally, and why Innovate UK funding was essential – this is beyond any individual organisation acting alone, and through determination and collaboration, the team have shown how technology can preserve sovereignty and privacy, increase reliability and accessibility to the ecosystem, at a far lower operating cost – all of which are vital attributes for new, autonomous forms of flight as well as airlines.

For 2024 objectives, as per the Future of Flight roadmap<sup>23</sup>, one of the elements that has been explored during Fly2Plan is the use of self sovereign identity (SSI) methods for UAS identification in order to achieve the goal of drone registrations and approved operations through the UTM provider. DLTs can be leveraged to achieve a self sovereign identity management system, providing the technical foundation upon which the concept of self-sovereign identity can be realised (see section 2.1). Beyond individual or industry based SSI solutions, the European electronic Identification, Authentication and Trust Services (eIDAS) regulation has been designed to ensure the cross-border mutual recognition of Electronic Identification (eID) mechanisms among the European Member States<sup>24</sup>.

The industrialisation of these new digital solutions towards 2026 will be determined by the capacity to make these new technologies scalable and robust enough to support the volume of traffic that UTM needs to handle. And on the roadmap towards 2028 and 2030 the priority would be to fully integrate these UTM solutions with current ATM systems in those areas where they need to interact. During the Fly2Plan project, this work has already started in order to test integration of an UTM service provider with an ATC service at an airport tower. We detail more in our case studies in Section 4 of this paper.

We firmly believe that cross-cutting new technologies such as the ones described in this paper, offer the key to opening the roadmap towards a fully operational UTM system by 2030 as per the goals of the Future Flight roadmap and the needs of the international aviation community.

<sup>21</sup> SITA Flightchain Whitepaper <https://www.sita.aero/resources/White-papers/flightchain-shared-control-of-data/>

<sup>22</sup> SWIM Eurocontrol <https://www.eurocontrol.int/concept/system-wide-information-management>

<sup>23</sup> IUK Future of Flight Vision and Roadmap, 2021 <https://www.ukri.org/publications/future-flight-vision-and-roadmap/>

<sup>24</sup> Marco, L. et al. User-Adapted Web Services by Extending the eIDAS Specification with Functional Attributes. Int. J. Environ. Res. Public Health 2021, 18, 3980. <https://doi.org/10.3390/ijerph18083980>

## 3.2 DLT and AI key developments and challenges for a new UTM solution

**Core properties of distributed ledgers are highly desirable for future UTM data interchange, namely strong consistency guarantees, system liveness and system safety. Coupled with cryptographic methods for permission messaging and data legibility, and (in many ledger systems today) programmable logic to control data flows and system behaviours, these would seem to meet the needs of a robust, safe, trustworthy, multi-actor messaging bus to underpin future flight operations.**

However, as alluded to in Section 2.1, there are challenges to the adoption and implementation of solutions based upon DLTs. First and foremost is that they come with trade-offs in system topology, participation, and data encapsulation. While ledgers can strongly enforce their internal data formats etc., data ingestion from outside systems must be converted into the internal format of the ledger. While ledgers ensure all participants have identical data replicas, exactly who is allowed to do what must first be agreed at a human-level (see Section 2.3 for discussion about rules). Finally, certain DLT implementations face issues when attempting to upgrade either embedded 'smart contract' functionality, or the underlying ledger itself.

Each of these challenges are well understood by the community of developers behind the rise in distributed systems technologies and so-called Web3.0. As a result, there has been a flourishing of ledger solutions, technological approaches to system governance, and additional tooling to check the safety of 'smart contracts' and network stability. Each of these has direct positive benefits for the adoption of DLT for future UTM.

In terms of AI, the interface between DLT and machine learning from DLT-secured data has only recently begun to emerge. A small number of start-ups are building tooling to leverage the guarantees of DLTs in their AI solutions, and others are exploiting models of FL and other ways to source data from a distributed user base. These approaches will only continue to grow, and ultimately benefit early adopters of these technologies in the aviation ecosystem.

## 3.2.1 AI and DLT convergence challenges and development needs

Regarding the potential of the convergence of DLT and AI there are still a few challenges to be addressed.

The area of research and development that seems more advanced and could have the first real solutions implemented is the use of AI to enhance DLT security. For example, to detect security vulnerabilities in smart contracts by supervised learning, AI-based methods have outperformed classical, formal verification-based methods<sup>25</sup>. Future research and deployment of solutions could expand this work by aiming at not only detecting security vulnerabilities in a smart contract, but also at localising this vulnerability.

Another area well developed in research and in an advanced stage for concept development and implementation is the use of DLT for AI explainability. For example, a DLT can be used for verifying for AI model ownership, data provenance and data flow tracking, the traceability of the AI model development, deployment and version controls.

However, other areas such as AI-based automated referee and governance for DLT protocols, still require substantial progress in robustness and secure AI before transferring scientific knowledge into practice and the establishing of real-world system. Furthermore, adopting DLT and AI integrated with drone technology places additional constraints on computation, necessitating optimising drone resources based on efficient task allocation, scheduling, and various other mechanisms to reduce energy consumption and extend operation lifetime<sup>25</sup>.

Some milestones and interdependencies that need to be resolved in order to make a UTM using DLT and AI a reality include<sup>26</sup>:

- **5G and B5G.** 5th generation (and beyond) of mobile Internet connectivity that is offering super-fast download and upload speeds as well as more stable connections could solve UAVs navigation issues in urban environments. However, 5G is not available everywhere yet.
- **Trade-off between communication delays, computation, and learning accuracy.** There are also particular issues related to drone edge intelligence networks such as heterogeneous resource capacity, which includes data size, computing, energy, channels etc. Therefore, there is a need for more work focusing on efficient FL techniques that consider connectivity maintenance together with ensuring high accuracy learning.
- **Energy efficient operations.** The combination of FL and DLT could aid the design of an efficient framework for energy efficiency analysis. Energy efficient protocols are needed for improving drone operations, maintaining quality of service and enhancing tasks computation. More development is needed in this area in order to be able to scale up operational efficiency of large drone operations.
- Other challenges regarding operational efficiency are those related to **organisation and standardization of services**. For example, battery charging or swapping is not difficult and it can be aided by AI and DLT integration detecting which drone needs charging and closest point of charge. However, there are no standards which enable universal autonomous charging of UAVs made by different manufacturers. Agreement on issues like these will be needed in order to implement solutions.

<sup>25</sup> K. D. Pandl et al.: On the Convergence of AI and DLT: Scoping Review and Future Research Agenda, IEEE Explore, 2020

<sup>26</sup> S. H. Alsamhi et al., "Drones' Edge Intelligence Over Smart Environments in B5G: Blockchain and Federated Learning Synergy," in IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, pp. 295-312, March 2022

## 4 Case studies

### ▶ Altitude Angel

GuardianUTM Enterprise is a cost-effective solution for providing comprehensive oversight of airspace and managing access for drones around airports, critical infrastructure, land and managed properties. Through an intuitive cloud-based interface, airports, landowners, and facility managers can engage directly with airspace user requesters, enabling drone operations to be conducted safely and transparently whilst unlocking innovative new services and opportunities.

By integrating with Fly2Plan's Digital Identity technology, Altitude Angel can cut the time it takes to review, assess and validate a pilot's licence and insurance credentials allowing faster access to flight-restricted areas around airports and other regulated facilities. Our seamless integrations with commonly deployed counter-drone systems ensures that all stakeholders are digitally connected and assured of safe operations.

It's Altitude Angel's view that the technology is supporting the unification of piloted and automated operations, allowing traditional aviation to adopt and adapt to the technology that drone operators have been enjoying for many years. In turn, this will enable the 10x increase in flight volumes predicted by 2030<sup>7</sup>. The Fly2Plan project has shown what we can achieve by working together.

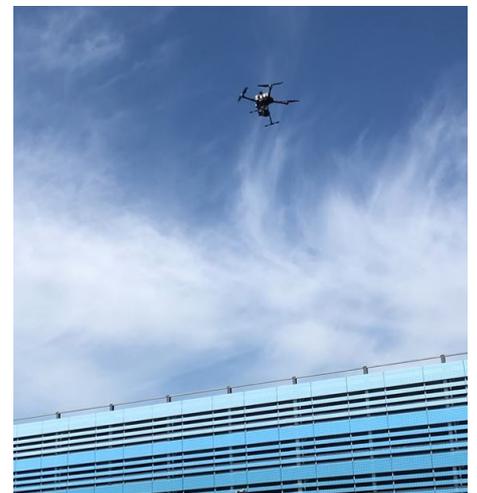
### ▶ Heathrow

At Heathrow, we recognise the benefits that drones can bring to surveying infrastructure, capturing accurate digital twins of taxiways, air-bridges and apron areas. This helps us to monitor asset health and plan maintenance, avoiding expensive short-notice repairs. But operating drones at a busy international airport requires careful coordination across multiple stakeholders, such as air traffic control, police, drone defence and airport operations teams. Even a small area being surveyed may require multiple sorties, and every power-up, take off and power-down needs stakeholders kept informed by phone calls.

Meticulous planning occurs even before flying the mission. Plans must be submitted 28 days ahead of time, safety risks understood and signed off, and proof of operator licence and insurance cover shown. If you're not a regular flyer at Heathrow, the process can quickly add to everyone's workload.

Fly2Plan brings a digital efficiency revolution – a digital drone pilot's licence and digital proof of insurance cover, together with every mission submitted to a collaborative shared record will cut the red-tape burden and allow authorised drones to get flying safely within the Flight Restricted Zone (FRZ). Proof of authorization, and missions flown to plan on an immutable digital record gives pilots a trustworthy log-book. This evidence of competence and compliance helps assure safety and make drone flights as routine any airliner flying in and out of the airport.

Fly2Plan has been designed with an end in mind that converges traditional, remotely piloted and eventually autonomous systems into the same digital infrastructure. We see the cost saving and reliability gains that digitalisation can achieve, and we look forward to seeing our technology partners continue to build on the great research done to modernise aviation data exchange.



# 5 Conclusions and way forward

Throughout this paper we have been exploring the development and application of new technological solutions in order to advance UTM systems development and implementation and facilitate the interaction and exchange of information between different stakeholders. We consider that the following are key elements in order to make this new aviation ecosystem a reality:

## UTM development

There is a rapid advancement of technology with a variety of possible technological solutions that may support a framework for communications systems. As described in this paper, DLTs and the interaction of DLTs with AI systems offer a novel and innovative solution so that UAS communications service providers and suppliers can evolve and work together. Such entities may play a key role in assisting with strategic deconfliction, situational awareness, flight planning and authorisation of UAS operations in the respective airspaces. More work on implementation and more cooperation between stakeholders are essential to scale up and commercialise solutions. Fly2Plan is a clear example of what can be achieved when cooperation happens.

## Interoperability - interaction of systems at intersections

Interoperability refers to ability of exchange information between UTM systems and between ATM and UTM stakeholders. It is envisaged that the interaction of ATM with UTM systems would be the most challenging as ATM needs to modernise and automate their systems and processes in order to be able to interact with UTM at interacting airspaces. Solutions are needed to enable UTM and ATM information exchange capabilities for operations planning purposes and to enable situational awareness. Also, capabilities to meet performance requirements are needed to achieve interoperability and collaboration between UAS operators and traditional flight information management systems (FIMS).

## Industry working together

As mentioned before, the development of solutions using innovative technologies towards the realisation of UTM systems, will require a great degree of collaboration between different stakeholders working in different aspects of development. Following ICAO's recommendations<sup>1</sup>, these are the main areas where working together will be a real necessity going forwards:

- Safety assurance for crewed aviation, UAS and people and property on the ground. This will require a partnership between regulators, service provider(s) and UAS operators, as well as stakeholders new to the aviation domain, such as city authorities, law enforcement agencies, telecommunications providers and suppliers of non-aviation data.
- Flexibility in the systems architecture and UTM service definition to enable UTM systems to react to developments in technology and business applications. This flexibility can be provided by incorporating new technologies such as DLTs and AI to evolve UTM systems as described in this paper.
- Increase in efficiency in UTM service provision, especially as numbers of UAS increase, and this will be dependent on a significant increase in automation. As described earlier, the use of AI federated learning for drone operations in conjunction with DLTs could support the increase expected in UTM and UAVs operations. This needs to be facilitated by digital infrastructure and physical infrastructure as described in this paper. Such developments could also benefit the wider aviation community and ATM operations.
- There is a need for the development of ongoing harmonisation of standards and regulations that support various implementation options as well as governance frameworks such as the one developed during Fly2Plan.
- Automatic and continuous validation of UTM systems. This may require the development of new mechanisms for performing such validation. As such it may be necessary to learn from non-aviation domains, and to determine if alternative mechanisms are suitable for aviation purposes.

To conclude, we firmly believe that as an industry that is growing and diversifying, we need to work together towards achieving all the areas described above, working in a harmonised way and with one common vision. This without doubt will open up new opportunities for growth and develop a new ecosystem of stakeholders that is still being defined. This is an exciting time for the aviation industry, a time where there is the opportunity of setting a direction, to challenge the past and current systems and influence the way forwards to achieve a new and exciting future.

**CATAPULT**  
Digital

DEPARTMENT OF  
**COMPUTER  
SCIENCE**



**SITA**



-  @cranfielduni
-  @cranfielduni
-  /cranfielduni
-  Cranfield University
-  CranfieldUni
-  cranfielduni

Cranfield University  
Cranfield  
MK43 0AL, UK  
T: +44 (0)1234 758540  
E: [study@cranfield.ac.uk](mailto:study@cranfield.ac.uk)



THE QUEEN'S  
ANNIVERSARY PRIZES  
FOR HIGHER AND FURTHER EDUCATION  
2019