Distributed Space Traffic Management Solutions with Emerging New Space Industry

SpaceOps-2021,8,x1629

Distributed Space Traffic Management Solutions with Emerging New Space Industry

Gabriel Maiolini Capez[a], Luisa Buinhas[b]*, Mauricio A. Caceres[c], Srinivas Setty[d]

[a] *Vyoma GmbH, Eckhardtstraße 28, 64289 Darmstadt, Germany*, gabriel.maiolinicapez@vyoma.space
[b] *Vyoma GmbH, Eckhardtstraße 28, 64289 Darmstadt, Germany*, luisa.buinhas@vyoma.space
[c] *Vyoma GmbH, Eckhardtstraße 28, 64289 Darmstadt, Germany*, mauricio.caceres@vyoma.space
[d] *Vyoma GmbH, Eckhardtstraße 28, 64289 Darmstadt, Germany*, srinivas.setty@vyoma.space

* Corresponding Author

Abstract

Day-to-day services, from weather forecast to logistics, rely on space-based infrastructures whose integrity is crucial to stakeholders and end-users worldwide. Current trends point towards congestion of the near-Earth space environment increasing at a rate greater than existing systems support, and thus demand novel cost-efficient approaches to traffic detection, characterization, tracking, and management to ensure space remains a safe, integral part of societies and economies worldwide. Whereas machine-learning (ML) and artificial intelligence (AI) have been extensively proposed to address congestion and alleviate big-data problems of the future, little has been done so far to tackle the need for transnational coordination and conflict-resolution in the context of space traffic management (STM).

In STM, there is an ever-growing need for distributing information and coordinating actions (e.g., avoidance manoeuvres) to reduce the operational costs borne by individual entities and to decrease the latencies of actionable responses taken upon the detection of hazardous conditions by one-to-two orders of magnitude. However, these needs are not exclusive to STM, as evidenced by the widespread adoption of solutions to distributing, coordinating, and automating actions in other industries such as air traffic management (ATM), where a short-range airborne collision avoidance system (ACAS) automatically coordinates evasive manoeuvres whenever a conjunction is detected. Within this context, this paper aims at establishing a roadmap of promising technologies (e.g., blockchain), protocols and processes that could be adapted from different domains (railway, automotive, aerial, and maritime) to build an integrated traffic coordination and communication architecture to simplify and harmonise stakeholders' satellite operations.

This paper is organised into seven sections. First, Section 1 introduces the problem of STM, highlighting its complexity. Following this introduction, Section 2 discusses needs and requirements of various stakeholders such as commercial operators, space situational awareness (SSA) service providers, launch-service providers, satellite and constellation owners, governmental agencies, regulators, and insurance companies. Then, Section 3 addresses existing gaps and challenges in STM, focusing on globally coordinated approaches. Next, Section 4 reviews technologies for distributed, secure, and persistent communications, and proposed solutions to address some of these challenges from non-space sectors. Thereafter, Section 5 briefly covers the history of STM proposals and presents the state-of-the-art solution being proposed for modern STM. Following this review, Section 6 devises a step-by-step plan for exploiting and deploying some of the identified technologies within a five-to-ten-year timeline to close several existing gaps. Finally, Section 7 concludes the paper.

Keywords: blockchain, space traffic management, collision avoidance, communications, distributed architectures.

Acronyms/Abbreviations

ACAS	Airborne Collision Avoidance System
AI	Artificial Intelligence
AOCS	Attitude and Orbit Control Systems
ATM	Air Traffic Management
CCSDS	Consultative Committee for Space Data Systems
CDM	Conjunction Data Message
CEPT	European Union Conference of Postal and Telecommunications Administrations

CREAM	Collision Risk Estimation and Automated Mitigation
CSpOC	US Combined Space Operations Center
DLR	German Aerospace Center
ESA	European Space Agency
EU	European Union
EU SST	European Union Space Surveillance and Tracking
EUROCONTROL	European Organisation for the Safety of Air Navigation
FAA	United States Federal Aviation Administration
FCC	United States Federal Communications Commission
GEO	Geostationary Orbit
GfR	Society for Space Applications
IAA	International Academy of Astronautics
IADC	Interagency Space Debris Coordination Committee
IATA	International Air Transport Association
IBM	International Business Machines Corporation
IEEE	Institute of Electrical and Electronics Engineers
ITU	International Telecommunications Union
LEO	Low Earth Orbit
LTE	Long-Term Evolution
M2M	Machine-to-Machine
MHS	Message Handling System
ML	Machine Learning
MVP	Minimum Viable Product
NASA	US National Aeronautics and Space Administration
O/O	Owners and Operators
P2P	Peer-to-Peer
RSO	Resident Space Object
S/C	Spacecraft
SAE	Society of Automotive Engineering
SANA	Space Assigned Numbers Authority
SAO	Standard Archiving Output
SATCAT	Satellite Catalog
SDA	Space Data Association
SSA	Space Situational Awareness
SST	Space Surveillance and Tracking
STM	Space Traffic Management
UAS	Unmanned Aircraft Systems
UN	United Nations
UNCOPUS	United Nations Committee on the Peaceful Uses of Outer Space
US	United States

1. Introduction

As of April 2021, there are over four thousand operational satellites across all orbital regimes, from low-Earth orbit (LEO) to geostationary orbit (GEO). Although certain routine operations, such as conjunction screenings and spacecraft (S/C) health monitoring, are effectively automated by most satellite operators, manoeuvre planning, in particular for collision avoidance, is not. Currently, there is a conjunction warning (close approaches < 1 km) every 4.5 seconds [1], corresponding to nearly 600,000 conjunctions per month and high operational expenses. Existing operational practices involve accessing Space Situational Awareness (SSA) data spread across several providers (catalogues), such as the Space Data Association (SDA), the European Union Space Surveillance and Tracking (EU SST) network and the United States (US) Combined Space Operations Center (CSpOC), each with their own space objects set, propagation tools, and observation processing methodologies. After post-processing, every warning that materialises into a collision detection demands time-consuming human-in-the-loop meetings, often delaying decision-making and actionable responses by hours or even days. Simultaneously, the greatest cost-drivers in satellite operations

are the human staff, who must be permanently stationed, splitting 24/7 work into shifts of flight dynamics experts and operators [2].

To aggravate the situation, these complexities are bound to increase due to many factors:

- The introduction of mega-constellations, coupled with the democratisation and commonization of space, sets us on course for more than 100,000 operational satellites in orbit by the end of the decade [3], leading to a three-order magnitude increase in conjunction-warning rate, at 6.7 million conjunctions per month. Even if only a fraction of these warnings materialises into potential collisions, undoubtedly there are not enough human and financial resources to plan and coordinate avoidance manoeuvres efficiently.

- Current data providers rely on inadequate information that is sporadically updated and often of unknown quality. Consequently, there are large uncertainties when estimating S/C position and velocities in specific instants of time, resulting in a high conjunction warning rate. Moreover, as satellites start to employ electric propulsion, these uncertainties will worsen due to the lack of accurate trajectory modelling and computational resources for trajectory propagation, fundamental for meaningful orbit predictions.

- Commercial industries are the key drivers of the new space era, whose main motivations to utilise the orbital environment are coupled with short-term financial interests, and thus they have little incentive to protect it in the long term.

- Space exploration is inherently geopolitical; in the recent years, there has been an increase in political polarisation and protectionism. Consequently, the pursuit of transnational and transcontinental objectives through cooperation in the space sector is being substituted for international competition for dominance [4, 5].

When considering all these factors and modern society's reliance on space-based services and the space economy, one quickly concludes there is an urgent need to harmonise space activities.

These same concerns about congestion at the international level drove coordination in the aviation and shipping industries, leading to the implementation of mechanisms [6, 7] to coordinate routes safely and automatically upon the detection of hazards, particularly when the response windows were truly short - within minutes.

To accommodate the massive number of stakeholders with unique commercial and political interests, the solution towards traffic coordination must be a trustable distributed framework for global space traffic management as previous centralised attempts in sectors such as aviation, albeit quite successful, lack capacity and transparency, which is essential for trust in conflict resolution mechanisms [8]. For STM, considerations over sovereignty, security, and the strategic importance of space dominate over all other concerns, something already seen in ATM [9]. Thus, STM frameworks should be capable of enhancing cooperation while preventing the access of sensitive, proprietary, information by unauthorised users, a property called 'customisable transparency'.

The issue of a distributed or decentralised system deeply impacts trust; a distributed system relies on the network's peers sharing and validating the veracity of data, that is, its authenticity and integrity, through a common protocol to ensure that, eventually, there is a consensus of the truth. In this case, at least at a high-level, part of the trust is shifted from traditional institutions towards technology such as software, servers, code developers, build toolchains, and cryptographic proofs, each of which may be corrupted or broken, representing a single point of failure [10]. However, considering STM's scalability and security requirements, where tamper-resistance and auditability are demanded, such distributed systems are likely the best solution [11] [12].

Finally, although certainly a complex and long endeavour, automated space traffic coordination must become the norm to ensure that space remains usable for generations to come [13].

2. Current and Future Stakeholder Needs

With the democratization of space and as different players gain access to the orbital environment, the number, type, and interests of stakeholders becomes increasingly diverse, as illustrated in Figure 1, which shows the main sectors in the space economy scaled according to their revenues in billions of dollars. In this section, we present a brief survey of some of the participants in the STM domain, their respective activities, requirements, and concerns in interacting with an automated manoeuvre-coordination framework.

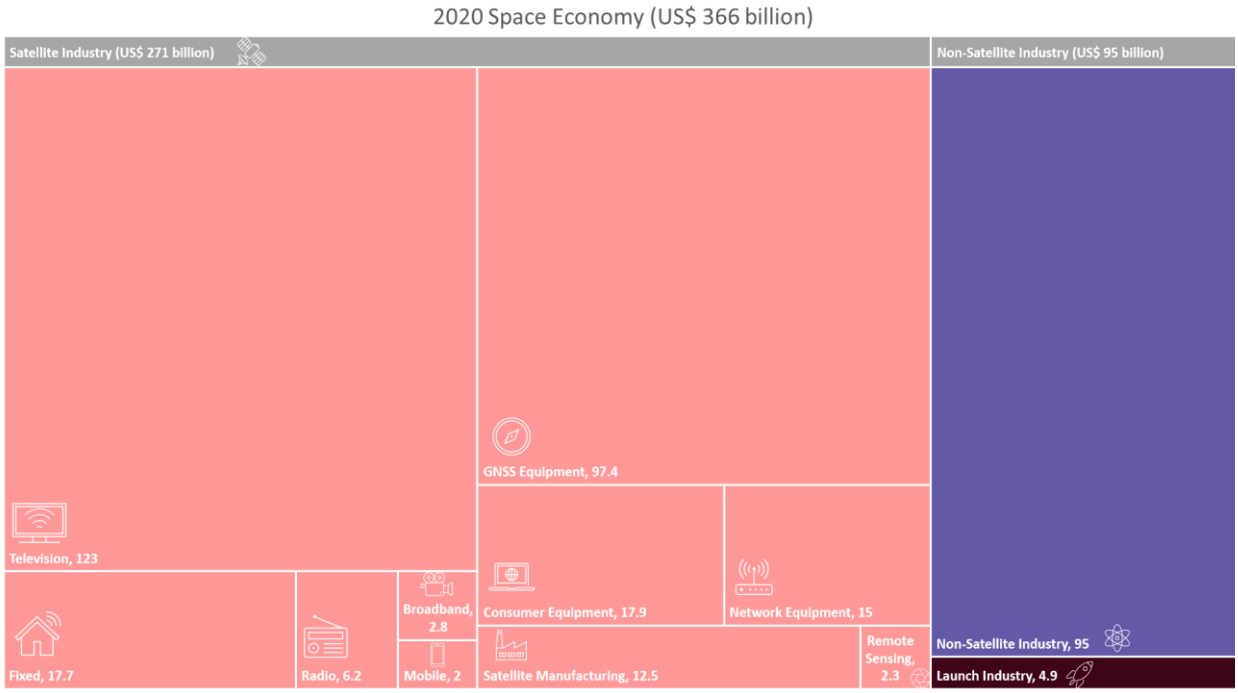

Figure 1 – 2020 Space Economy Main Stakeholders (data source: Bryce Tech, 2020)

2.1 Satellite Owners and Operators

Satellite owners and operators (O/O) are the main stakeholders in the STM industry. They drive and support a multi-billion Euro industry through in-orbit service-providing satellites. Although there is no economic incentive *per se* for satellite owners to invest in the automated coordination of manoeuvre activities in the short-term, with increasing congestion, adaptations must be made to conserve personnel and financial resources.

Primarily, owners and operators of satellites have an understandable interest in safeguarding their own assets at the lowest cost possible. As soon as a conjunction is detected, the state-of-the-art resolution strategy is one that maximises responsiveness and efficacy while minimizing action latencies and costs.

While a coordinated response to impending collisions can indeed provide these benefits, collision avoidance strategies must be negotiated between multiple satellite O/O, implying that information concerning at least one of the parties must be shared so that an agreement can be reached.

This may be a cause of concern for these stakeholders as they might have competing or conflicting interests that makes them wary of disclosing vital information about their satellites, such as orbital positions or manoeuvring capabilities.

As such, baseline requirements must assure transparent processes for negotiating coordination strategies, data exchange and conflict resolution. Equally paramount to foster trust in such systems, data authenticity and security are not only vital to ensure that the data upon which decision-making strategies are built upon is uncorrupted and that the communication mechanisms are unsusceptible to attacks, but also that the data shared within the network is *only* shared with those concerned in the resolution of a given conflict and not necessarily with all users of the network.

2.2 Launch Services Providers and Operators

Companies operating vehicles that transfer satellites from ground to orbit are interested in ensuring that the payload they carry reaches its destination safely. As such, prior to launch, they require an analysis of risks that may threaten the launch and orbit insertion processes. During the launch, these companies must monitor the launch vehicle's environment and, once the launch of the payload is completed, any launch-vehicle parts that either remain in orbit or are de-orbited, namely the upper stages, must not represent a collision hazard to comply with debris-mitigation guidelines.

Launch service providers and operators contribute to existing data catalogues by sharing orbit information and hardware properties (e.g., mass, volume, density of materials, reflectivity parameters, etc.) related to their assets. However, the hardware left behind in orbit is typically not manoeuvrable. If a collision with an active manoeuvrable satellite is detected, the collision avoidance burden falls on the satellite. In this case, since launch-hardware remnants are of little interest to launch service providers once their service obligations have been fulfilled issues surrounding data privacy or transparency of coordination protocols are not of great concern to these stakeholders.

2.3 Data Owners, Aggregators and Service Providers

In the context of manoeuvre coordination, data owners and providers, data can be in the form of satellite orbital information (tracking), of space-weather forecast and atmospheric modelling or, in case of defence and military applications, in the form of satellite behavioural-pattern reporting that plays a role in increasing space situational awareness (SSA).

As stakeholders, data providers are a diverse lot. On the commercial side, data providers leverage data scarcity to upsell accurate tracking information to other stakeholders, such as satellite owners and operators, whilst making freely available orbital information with greater uncertainties. Instead, governmental data providers contribute to catalogue pools, as in the case of the EU SST network, but access to and allocation of physical sensors is negotiated bilaterally between governments. Some entities, like the SDA, fall within this group and could play a major role in shaping the future of STM.

Despite being net contributors of information to the traffic coordination frameworks, data providers have unique interests and constraints in managing access to information. Firstly, commercial actors need to be sure that only those who paid to retrieve detailed information concerning the orbital environment can have it, bringing the issue of identity validation and contractual fulfilment to the forefront as sensitive SSA data must only be shared by those who are authorised to access it. Secondly, they must ensure that the recipient of information receives true and uncorrupted data, thus making data integrity a vital element for data providers and their customers. Thirdly, the issue of security and resilience to malfeasance is central to governmental and institutional data-providers. Overall, data providers are less concerned about how the coordination strategies are managed than with the handling of the data they produce.

2.4 International Authorities, Policy Makers and Regulation Agencies

Authorities, both national and international, policy makers and regulation agencies are institutional players who are typically on the receiving end of the data dissemination. These stakeholders generate guidelines, issue certifications, award licenses and, in some cases, write laws with national and international reach. They rely on accurate information (e.g., congestion status of different orbital regimes from operators, predictions from research institutions) to make important decisions that have an impact socially, economically, and politically. It is thus of paramount importance that these stakeholders have access to authentic, integral, and rigorous data.

Simultaneously, regulatory bodies may play a role in how avoidance manoeuvre strategies between two (or more) satellites are negotiated in a distributed architecture that serves a multitude of stakeholders. For example, if a follow-up collision is detected for one satellite, but not the other, these agencies may mandate that the manoeuvring solution resulting in the least amount of entropy in orbit over a specified amount of time be selected. Thus, the algorithms which are used in the implementation of coordination of traffic directly depend on the output of these regulatory bodies.

Nonetheless, current international conventions alone are insufficient to cope with over-congestion in space. The industry requires stricter definitions of liability and fault, collaborations, and a convergence of legal interpretations among different countries to measurably incentivise proper space traffic management. Another way to stimulate a responsible use of the space environment is by awarding compliance certificates to space-asset owners and audit operational procedures that minimise in-orbit collisions.

While STM has been defined simply as technical and regulatory requirements for safety in space [14], it encompasses much more than that, including political concerns [15]. Consequently, defining clear rules for space traffic regimes such as the S/C launch, in-orbit operation, and re-entry phases demands substantial negotiation between stakeholders with competing interests to manage their perception of loss of freedom when participating in STM frameworks.

Moreover, for a STM system to operate, it must satisfy a variety of legal and regulatory requirements from regional, national, and international bodies. Therefore, it is essential to comprehend the legislative context within which it will be inserted.

Unfortunately, current legal and regulatory frameworks are focused on radiofrequency interference (i.e., European Union Conference of Postal and Telecommunications Administrations (CEPT), United States Federal Communications Commission (FCC), and International Telecommunications Union (ITU) requirements), debris mitigation (Interagency Space Debris Coordination Committee (IADC) guidelines), arms treaties, and launch authorization, detection, and notification, and lack the necessary structure to support STMs.

For example, the international treaties negotiated through the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUS), establishes the governing principles of activities in the exploration and use of outer space, laying out obligations for states and commercial entities that launch with the consent and supervision of a member state's national authority. However, there is no international regulatory body with sole authority over space as member states maintain jurisdiction over when and what they launch, and more importantly, over trajectories and orbits.

However, in the US, the recently signed Space Policy Directive 3 places civil SSA and STM responsibilities in the United States Department of Commerce, a civilian entity, and provides relevant guidance to the development of a STM architecture. Specifically, it affirms the importance of a STM ecosystem that offers free, government provided, basic SSA and STM services in a manner consistent with "supporting new opportunities for U.S. commercial and non-profit SSA data and STM services."

Therefore, we have identified a few recommendations for regulatory entities. It is necessary to define data exchange and provisioning rules and adequate stakeholder notification of pre-launch activities, active and operational lifetimes, orbital manoeuvres, and active de-orbiting.

For the European Space Agency (ESA) and EUSST, we recommend that they work towards developing standards and protocols for the creation of an open architecture data repository to improve SSA data interoperability, enabling universal sharing of SSA data.

2.5 Insurers

Satellite insurance providers are made up of a small number of companies backed by large capital resources. Insurance coverage typically revolve around pre-launch, launch and in-orbit risks.

In a fast-evolving ecosystem whereby new, untried, and unproven technologies are put to the test in an orbital environment that is becoming increasingly congested, insurance companies have had to navigate an increasingly complex market and revise conventional insurance policies and associated premiums, and thus could benefit from a clean orbital environment and a string of successful missions, minimizing their compensation costs.

To accurately assess satellite operation risks, insurance companies rely on technical expertise and decades-long practices in space. To keep up with the pace of change and be able to generate revenue with more business certainty and confidence, these insurers would benefit from accessing data directly from providers and operators and in shorter time intervals. More specifically, this would allow them to calculate their premiums based on the auditable collision-avoidance operations.

2.6 Research Institutions

Academic and research bodies play a significant role in STM as several of the technological innovations and the study of their consequences are driven by dedicated experts and investigation groups with no commercial affiliations. They help policymakers make informed decisions and shape the conversation around the dangers of debris which equally serves to bring awareness to the public in general.

Typically characterised by creative and ingenious minds applying rigorous methods to their work, these institutions lay out actionable, technical solutions towards the problem of congestion in the orbital environment and may including drive the design and adoption of a pan-stakeholder traffic-management architecture that is agnostic to participants' interests (political, financial, etc.).

2.7 STM Infrastructure and Core Service Providers

A final group of entities that needs to be considered within the collaboration framework are STM Infrastructure and Service Providers, which would take the role of maintaining the STM infrastructure, implementing fixes and new features, and providing the core services that enable its usage, like registration, authentication, and authorisation. While ideally such roles should be distributed among different agencies and/or regulatory entities, an international public private partnership (PPP) body might be formed to oversee the platform, host some of its core services, and steer its further development in an impartial manner.

3. Current Gaps and Challenges in Space Traffic Management Systems

Space traffic management has been traditionally done ad-hoc on a per-collision basis, where involved stakeholders act independently or with limited coordination upon collision detection, leading to suboptimal manoeuvres, disagreements, and potential litigation for conflict resolution [16]. Although spaceflight safety agreements have been reached between few stakeholders as recent as March 18th, 2021 [17], they are clearly insufficient to deal with the complexity of managing hundreds of thousands of objects owned and operated by thousands of stakeholders, as illustrated by the April 9th, 2021 emergency collision avoidance manoeuvres of SpaceX and OneWeb, following warnings by the United States Space Force [18]. Moreover, STM faces unique challenges that have yet to be properly addressed in traditional terrestrial, maritime, and aerial domains, whose centralised architectures do not provide the scalability, security, resilience, and redundancy required.

Primarily, STM must contend with the legal and political realities of space; it is not segmented into regions controlled by single national authorities and thus any sort of hierarchy, regulatory authority, and enforcement bodies must be derived from the consensus of STM users, who must navigate complex space jurisdictional issues for conflict resolution. Achieving this consensus in the presence of uncooperative, unwilling, or malicious stakeholders is key, especially given the lack of an International Air Transport Association (IATA)-like regulator for the space sector to enforce their use; stakeholders' commitments to collaboration might be limited, either by their own interests or by national policies that restrict the use of foreign infrastructure.

Also, economic considerations indicate funding, maintaining, and scaling STM in such a diverse environment can be challenging because as the number of users and assets grows, greater financial resources and coordination are required to deal with its complexity. Hence, stakeholders should be incentivised to sustain these costs by highlighting STM benefits, in terms of greater autonomy and risk and cost reductions. If this is not possible, then they should be rewarded directly through service payments.

Absent widespread stakeholder participation, a regulatory authority to enforce compliance, and standardised positional information, it is impossible for a hierarchical command and control system to work for STM. Thus, it is critical that STM accommodates a mix of commercial and public entities without relying on a single command authority capable of compelling manoeuvres or assuming unified and comprehensive situational awareness.

To do so, STM must harmonise systems at various levels (global, national, institutional, and corporate) and support stakeholders' many use cases and interests, ensuring compatibility and interoperability not only between data and protocols, but also with regards to actions. At the very least, if not standardised, it is fundamental that STM provide action guidelines and recommendations for acting under a set of operational and technical constraints, particularly when planning and negotiating collision avoidance manoeuvres, where it is important to assign stakeholder liability. For example, by requiring avoidance manoeuvres be notified at least to involved stakeholders so they are aware of planned trajectories and follow-on collision probabilities so that they cannot claim to lack information or liability for

their subsequent actions. In this case, one could consider no-action notifications or at least an acknowledgement of the reception and processing of Conjunction Data Messages (CDM) and manoeuvre announcements, as those might become key evidence for forensic and insurance purposes.

From an operational perspective, there is a need for autonomous STM and manoeuvre coordination processes to scale with the growth of space assets in congested regimes in LEO; decrease operational latencies producing cost savings to operators, planners, and S/C owners and designers; and improving the overall quality of service (QoS) with reduced mission downtimes. These processes must support several types of operations and manoeuvres and allow the efficient exchange of risk events, S/C trajectories, and manoeuvre decisions between stakeholders for prompt, effective and, eventually, automatic coordination of risk mitigation actions.

Thus, a vital STM requirement is a unified communication infrastructure for fault-tolerant, secure, and seamless communications between heterogenous stakeholders that ensures the authenticity of communication and data records for traceability and auditability purposes, where there is clear need for a data chain of custody made of auditable, authenticated, and immutable data. Therefore, it should store information efficiently and reliably so that it can scale with the number of users. Consequently, this infrastructure must have a remarkably high capacity to support transferring a multitude of raw and processed data formats at Terabit-scale with relative low latencies between terrestrial and space users, and to allow quick information sharing, negotiation, and collaboration between stakeholders, which are critical for conflict resolution.

To share this vast amount of data in a plethora of formats, identity management is crucial; within the space traffic management economy, stakeholders, and assets in space (RSOs) and on-ground (e.g., tracking stations) require users and operators be uniquely identified. However, a single identity management provider may not be feasible or receive reluctance from some stakeholders, and thus identities should be federated and assignable by multiple authorities, such as regional and national space agencies, using unique identifiers and distributed digital identity registries. In this way, data ownership, that is, control over which users are licensed to access and share raw and processed data, can be guaranteed, enabling new ways of providing space-based services. For instance, it would be possible to publicly disseminate conjunction detections of high public interest events, while offering S/C owners and operators private conjunction screenings from the SSA services they are subscribed to, and to request on-demand screening, for example, when preparing a manoeuvre campaign.

Because of this need to maintain data confidentiality and integrity, securing this infrastructure against internal and external attacks is critical and it should include hotfix management and security monitoring functionalities in addition to auditing capabilities and routine security assessments.

However, securing communications is not enough; user and data privacy must be guaranteed. STM operations would include the participation of public (i.e., space agencies and regulators), commercial (i.e., space asset operators and ground sensor owners), and military agencies, all of which could be reluctant to participate in STM due to the classified nature of their missions. Therefore, proper data access control policies as well as end-to-end encryption is necessary and only authorised users should be capable of accessing their data, considering a threat model where not only an external attacker trying to gain access to the system, but also users trying to spoof or tamper with data or exceed their authorisation. Consequently, STM systems should offer means of privately exchange of data and provide secure channels where strict need-to-know principles are enforced to preserve data classification and encryption requirements.

Additionally, current standards are lacking when it comes to supporting STM operations, machine-to-machine (M2M) communications, and a STM economy; for instance, there are no standards to support contracts, transaction requests, and monetisation strategies, and data exchange formats have no standardisation for communicating space operators' decisions, verifying data authenticity and integrity, preserving data ownership, and satisfying accountability and traceability requirements. Even traditional Consultative Committee for Space Data Systems (CCSDS) standards are insufficient and do not provide a standardised way to include space weather and the nature of S/C manoeuvres (planned, commanded, performed) and its associated parameters (Attitude and Orbit Control Systems (AOCS) configuration, measured performance, etc). Therefore, they must be adapted or created from scratch, focusing on dedicated risk analysis processes and software for monetised data sharing, both for terrestrial and space users.

As a final consideration, implementation of STM may be limited by technological maturity considerations regarding safety or scalability, especially for a distributed system whose overall complexity may be extremely high. For example, current proposals, studied in Section 4, are not yet ready to offer the level of automation and the transaction and communication capacity required for universal STM and distributed collision avoidance, whose challenges are discussed in detail in [19].

4. Proposed Blockchain-enabled Solutions for Industry

To fulfil the traffic management gaps of Section 3, many solutions have been proposed over the years across all industry domains using a specific type of distributed ledger denominated blockchains. Blockchains are distributed data structures that manage transactions transparently, chronologically, and immutably in a computer network. Thus, they replace the core concept of databases with centralised transaction management in terms of atomicity, consistency, integrity, and durability with distributedly maintained data [20].

Using blockchains, these systems implement and automate cooperation logics through Smart Contracts [21], which can be understood as applications that execute functions once a set of conditions is met; for example, they can automatically act upon receiving external information as input, following the rules defined in the contract. For this purpose, the contract details are stored in a specific blockchain address. Then, if the specified external event occurs, a transaction is sent to the address triggering the execution of the contract, effectively automatising interactions between systems, agents, and their environment; contracts can be executed, enforced, verified, and inhibited by algorithms without intervention or control by intermediaries.

Within their extremely broad range of applications [22], they allow authenticated, auditable and immutable data to be shared and used in smart contracts to efficiently provide services to a massive number of users and stakeholders, especially for trust management, secure data sharing and storage, and traffic management – the focus of the this section.

4.1 Automotive

For road traffic management, several proposals of blockchain-enabled solutions for trust management, data sharing and storage, vehicle announcement, and intelligent traffic management systems have been proposed [23, 24, 25, 26, 27, 28].

They all rely on privacy-maintaining secure, tamper-proof, broadcasting/sharing of information through distributed ledgers to incentivise users and service providers to cooperate, increasing quality of service. Service providers, public or private, receive verified user data, including not only vehicle's current position, but also its intended trajectory and information regarding road and vehicle conditions. In turn, users receive optimised routes, reducing the time it takes for them to reach their destination. Consequently, overall traffic congestion is reduced. To validate data, users rely on consensus-based approaches, where nearby users or authorities verify the data being broadcast with information they have at hand.

While some systems are based on a permissioned approach, that is, where there are trusted authorities to validate and control the information being input into the system; for example, by verifying that the data the user is providing is compatible with road conditions (i.e., icy roads in extremely hot days), others allow vehicles and service providers to coordinate without intermediation.

4.2 Railway

As with other industry sectors, rail transport is seeing its fair share of blockchain-enabled proposals, ranging from overlays over existing railway traffic management (RTM) systems [29] to innovative intelligent traffic management and route optimization using federated learning [30], but also for train-to-train economy and addressing train condition-based monitoring and maintenance [31].

These systems all rely on a blockchain to share the data they need to make the traffic decisions they are responsible for, and on smart contracts to manage the services they provide. All these systems are predicated on a decentralised approach for privacy and security, while still remaining conflict free and safe.

When building upon the existing RTM system, the data shared through the blockchain is mainly used for forecasting and data distribution, so that operators have access to accurate up-to-date information in significantly greater amounts

than traditional systems. Then, if desired, operators can use smart contracts to negotiate traffic management strategies between them.

Instead, for innovative decentralised or federated RTM systems, smart contracts are responsible for managing all operations. For operators that agree to share data among themselves, federated learning can be used to optimise their traffic while preserving data privacy and security. When pushed to their limits, these systems can allow train-to-train services and autonomous train decisions, coordination, and conflict resolution.

4.3 Maritime

The issue of real-time data sharing across the shipment supply chain has led International Business Machines Corporation (IBM) and Maersk to create a blockchain technology company which supports smart contracts [32]. This initiative has been similarly replicated in Asia to support cargo movement tracking [33, 34] and augment port management activities using blockchain technology [35, 36]. Indeed, blockchains have been consistently proposed for deployment within the shipping industry in recent years [37, 38, 39] to address logistical inefficiencies (e.g., container handling), shipping traceability issues and paperwork overhead.

4.4 Airborne

For aerial traffic management of the massive number of unmanned low-altitude aircraft currently in use and to share flight data between manned and autonomous aircraft, blockchain-enabled solutions were proposed using distributed ledgers, peer-to-peer (P2P) networks, and open data sharing platforms to overcome the limitations of traditional solutions, among which three stand out: Flight Chain [40], Distributed Sky [41], and Sky Grid [42].

They enable monitoring and managing airspace, synchronizing aircraft, performing complex route planning and adaptation, and providing topographical and supplemental data while tracking liabilities in a detailed auditable trail that can be inspected by the relevant authorities.

All information is kept in a distributed ledger to ensure their accessibility, authenticity, and immutability. Moreover, by using the blockchain, users and service providers can transfer goods and services more easily in an auditable way. To do so, they define a smart contract with the terms of payment and service, including data ownership and access permissions.

When a user requests a service such as route planning or data provisioning, a smart contract that includes the transfer of liability is created inside the blockchain. If the smart contract is accepted by the user, who provides the necessary input for its execution, then the service is provided to the user, concluding the contract.

5. Space Traffic Management

5.1 Previous Efforts

In a precursor European STM concept [43] and, later, a White Paper [44] by German Aerospace Centre's Society for Space Applications (DLR GfR) and its partners presented key results of their evaluation study on behalf of ESA. The study's primary objective was to produce a roadmap for implementing a European STM system within the next two decades, that is, by 2035, as an evolution of the Air Traffic Management (ATM) system.

Moreover, to demonstrate that space debris collision risks do not preclude suborbital space flights, they introduced a proof of concept to demonstrate they are feasible [45], if significant advances in heat and collision shielding technologies are made.

In response to European STM needs, technical, conceptual, and organisational setups were envisioned [46], focussing on technology and infrastructure development, Space Debris, Space Surveillance & Tracking, Space Weather Monitoring and ATM and STM integration.

Then, for the European STM system to be operational in the 2030 – 2035 timeframe, [47] presents an initial roadmap and the main STM issues that must be tackled while ESA's Collision Risk Estimation and Automated Mitigation (CREAM) activities [48] attempt to tackle the automation of collision avoidance manoeuvres and space traffic management.

In the US, NASA is currently working on a civilian STM research initiative inspired in the United States Federal Aviation Administration (FAA) proposal for Unmanned Aircraft Systems (UAS) Traffic Management [49], exploiting many synergies between UAS and satellite operations and aiming at enabling efficient data sharing and coordination between participants, to facilitate safe spaceflight operations.

The proposed architecture [50] foresees a civilian governmental entity hosting a **centralised**, open-access software platform for STM where stakeholders like Owner/Operators, STM service suppliers, SSA suppliers, conjunction assessment suppliers, supplemental data suppliers can participate in the network through a STM gateway, which manages data registration, authentication and auditing, and is in general open to other external users. The modularity of the concept allows for an evolutionary path to implement proposed STM architecture. At a high-level, it is divided into two parts: the core STM architecture and the STM network itself. The former is composed of national and international authorities that interact among themselves and interface with the network through a spaceflight information management system to verify or provide information for safety and regulatory purposes. Instead, the network links various stakeholders so they can perform sensor tasking, share SSA data, conjunctions assessments, observation, and other sorts of information. Lastly, STM Service Suppliers deconflict spacecraft and function as an interface between spacecraft owners and operators and the remainder of the system.

To support collision avoidance operations, Cabrera et al. (2019) [51] explores different approaches for conflict resolution, including rule-based, dual manoeuvre implicit cost split, auction based, resource based or last-minute action.

Nag et al. (2019) [52] discusses how their concept would automatise STM, where efficient and standardised machine to machine communication methods is critical to achieve highly autonomous coordination and decision making that minimises the need for human decision making or review.

5.2 Proposed Blockchain-enabled Solutions

As blockchain technology evolved, the space industry became ever more interested in applying it to Space Traffic Management, leading to the invention of a patent-pending trust-based framework for decentralised STM and SDA by L3Harris, and the achievement of a minimum viable product (MVP) in 2020. Zaidi et al. (2020) [53] presents this product, which is built upon blockchain principles and consists of:

- A data curation system to determine astrometric veracity (i.e., accuracy) and transaction handling volume;
- A method to establish trustworthy datasets using independent validation;
- A message handling system (MHS) that allows stakeholders to openly communicate imminent conjunctions, flight paths, force model assumptions.

Moreover, the authors discuss data validation, organization and security, and stakeholder incentives, identifying key performance indices and using them to evaluate proposed use cases.

Of particular importance, they identify the main challenge in distributed blockchain-based STM systems as establishing trust between the different network nodes, that is, the SDA data providers, which can be done by a variety of consensus processes.

Additionally, security is crucial, and a regulatory role is foreseen for entities such as UNCOPUOS to provide certifications for the exchange and curation of data, making the proposed STM framework a “permissioned” blockchain environment. This exchange is double blind, that is, the identities of providers, curators and users are hidden from each other during transactions; only the regulatory authority knows them.

Also, as a by-product of using distributed ledger technologies, it is simple to identify bad actors providing untrustworthy data, tampering with the STM system, or disrupting other space users.

Finally, the proposed framework enables customers to purchase trustworthy data from commercial SDA providers.

6. Roadmap

In this section, we present a roadmap for the design and implementation of a STM system within a five-to-ten-year timeline, highlighting key activities and their timeframe, and discussing their main technical risks and challenges.

6.1. Activities

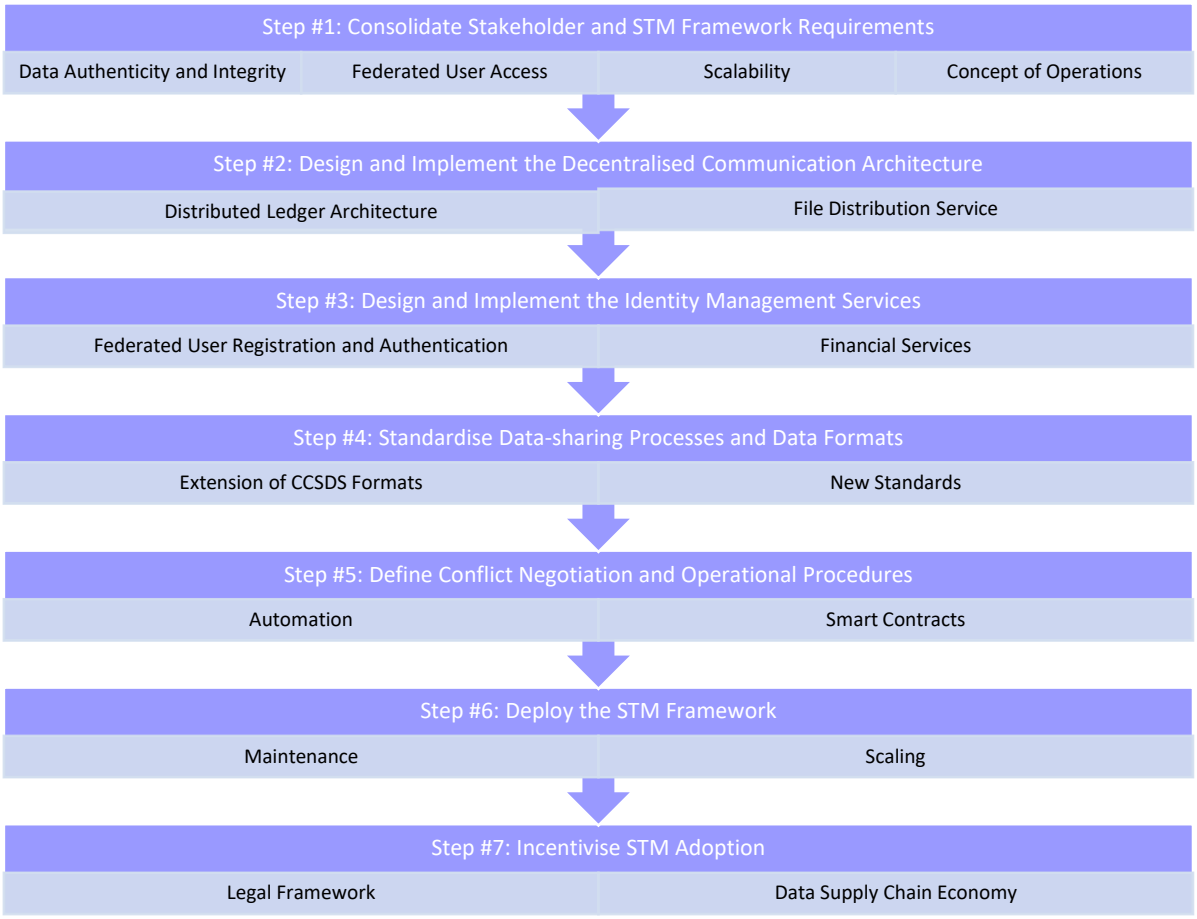

Figure 2 – Unified STM Framework Roadmap.

As discussed in Section 3, Space Traffic Management demands a communication infrastructure for sharing collected and processed data (e.g., position and ranging measurements and conjunction and collision warnings) and negotiating and coordinating actions, taking into consideration applicable standards and regulations as well as environmental and operational constraints.

The first step towards unified STM operations at a global scale is surveying, deriving, and consolidating stakeholder and STM framework requirements, balancing the enormous number of competing use cases and needs by defining key performance indices and performing trade-off analysis. As part of this step, a study on existing distributed traffic management should be performed focusing on STM needs of coordination, data authenticity and integrity, federated user access, and scalability. Once this has been accomplished, a concept of operations for the STM framework can be derived.

The next step is building the decentralised communication architecture, based on a peer-to-peer blockchain infrastructure and a distributed file distribution service, expanding the work done so far in [52] [53] so that stakeholders can share data publicly or privately and provide services to one another through smart contracts. Within this step, one must evaluate blockchain protocols, data sharing formats, and their technological maturity level, safety and security, and transaction throughput rates. Also, their applicability to ground and space segments should be assessed because the latter is highly constrained in cost and complexity.

Then, it is necessary to design and implement the identity management services, defining how identity and access management is enforced, that is, how users are registered, authenticated, or blocked and banned, and how to perform

access control to information. To do so, identity federation, that is, the division of users into identity providers, responsible for authenticating users, and service providers, responsible for controlling accesses to resources, will be necessary. This may also be considered when designing the distributed ledgers, which may be permissioned – where only certain users can perform validation. Considering that STM requires worldwide adoption to work satisfactorily, identity management will require significant effort to achieve consensus about what a valid identity is made of and how these distributed identity services interact. For example, stakeholders must choose whether users must be validated by national space agencies, commercial or public institutions and what unique identifiers to use.

Following the development of the communication and identity management infrastructures, one must develop and standardise novel interfaces, processes, and protocols for data sharing, establishing precisely how to transmit spacecraft trajectories, manoeuvring capabilities, ephemeris, conjunction and collision warnings and space weather data. These processes and protocols should be designed with native support for monetisation through smart contracts so that users can programmatically request and pay for services, allowing a STM economy to flourish. Inspiration may be drawn from existing, obsolete, or proposed CCSDS standards such as Spacecraft Manoeuvre Messages [54], Spacecraft Perturbation Messages [55], Navigation Hardware Messages [56], Conjunction Data Messages [57], which may potentially be adapted for STM. Instead, message transmission could be based upon traditional CCSDS space data transfer and file-delivery protocols [58], or terrestrial file-based transfer protocols, potentially relying on web applications. However, unique platform constraints must be accounted for; spacecrafts have limited communication and computational capabilities compared to terrestrial systems.

At this point, one must define the processes for conflict negotiation, manoeuvre planning, and risk management, covering collision avoidance, data exchange, and data-provenance verification use cases. These processes should be heavily automated, especially for conflict resolution and collision avoidance manoeuvres, because it is the only way for STM to scale without being bottlenecked by intensive human labour requirements.

After assessing the STM framework implemented satisfies design requirements, it should be deployed for widespread use. At this point, infrastructure and core service providers should take over maintenance and scaling activities and become responsible for the implementation of new features, patching, and user support. Moreover, considering the constantly evolving security landscape, they should regularly perform security assessments and auditing, and respond to security incidents.

The last step is incentivising stakeholder adoption. First, by highlighting the financial benefits of using the unified STM architecture to reduce operational latencies and workforce requirements and increase safety, aiming at fully funding the framework's maintenance and scaling. Second, by developing a legal framework to establish stakeholder contractual abilities, liabilities, and responsibilities across different regions, considering the difficulties of enforcing contracts internationally and the trust-based nature of STM, building the foundation of the STM data supply chain economy, in which stakeholders can freely negotiate, pay for, and provide services.

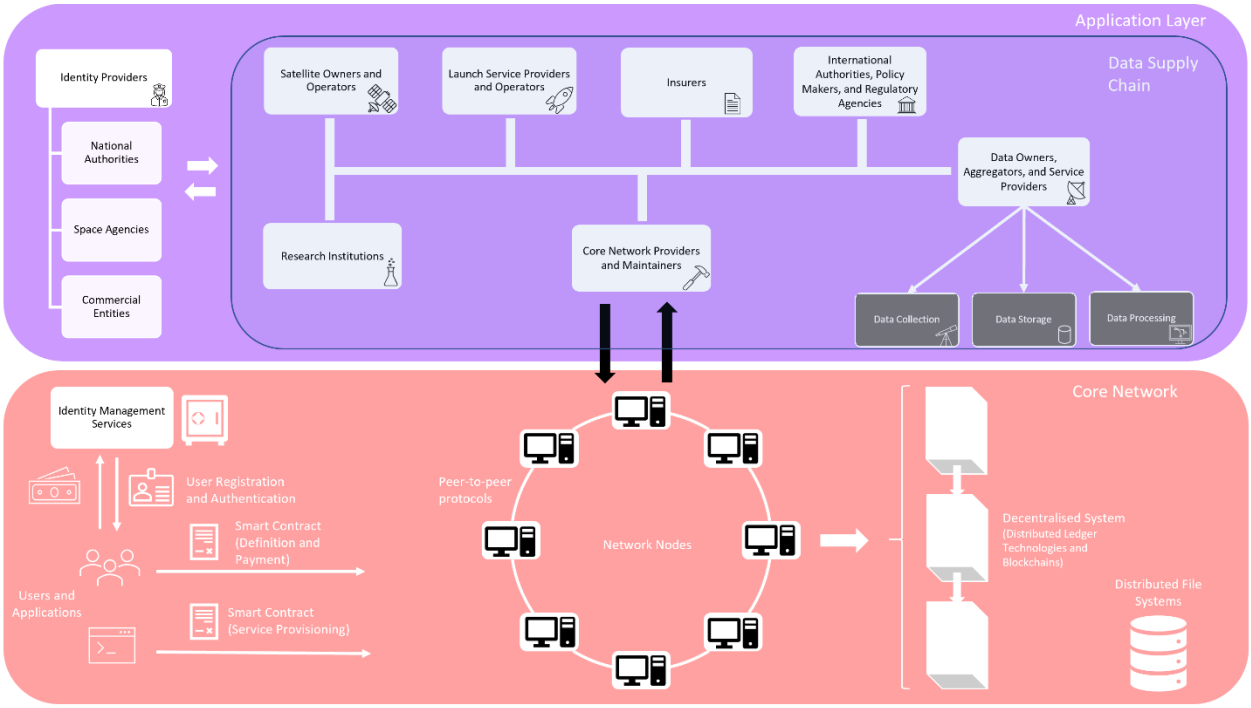

Figure 3 - Space Traffic Management Framework

Figure 3 illustrates the proposed space traffic management framework, which is composed of two blocks: the application layer and the core network. The latter has three components: identity management services, operated by identity providers and responsible for registering and authenticating applications, service providers, and users; smart contracts, for on-demand automated service request and provisioning; and a peer-to-peer network, which validates the authenticity and integrity of the smart contracts and associated data through consensus. Its nodes are part of a distributed ledger or blockchain which contains authenticated and immutable data such as smart contracts and cryptographic hashes of datasets stored across distributed file systems. While it would be possible to directly include all types of data in the blockchain, this would unnecessarily increase its size, and thus, it is better to separate mass data storage and authentication by only inserting key-value pairs that map smart contracts to storage locations. Also, considering that users may be terrestrial, maritime, aerial, or space platforms, it is important for the framework to be sufficiently modular and lightweight so that latency, data-rate, mass storage and on-board computing constraints are satisfied.

At the application layer, identity providers such as national authorities, space agencies, and commercial entities perform identity management for a data supply chain, where stakeholders interface and share data at will. Thus, identity management is split across the two layers, allowing that multiple identity providers share the same identity management service. For example, multiple national authorities and space agencies could perform their duties using a single commercial entity's identity management services.

In the data supply chain, there are seven categories of users and service providers that can be identified: satellite owners and operators and launch service providers and operators, which coordinate manoeuvres and consume data products for collision avoidance; research institutions, which consume all types of data products for research purposes; institutional authorities, responsible for producing certifications, guidelines, and formulating laws and regulations; core network providers and maintainers, which administer the core network; and, finally, data owners, aggregators, and service providers, responsible for collecting, generating, processing, storing, and providing risk assessments, manoeuvring solutions, conjunction warnings, situational awareness and space weather reports, and other types of data to stakeholders.

6.2. Timeline / Schedule

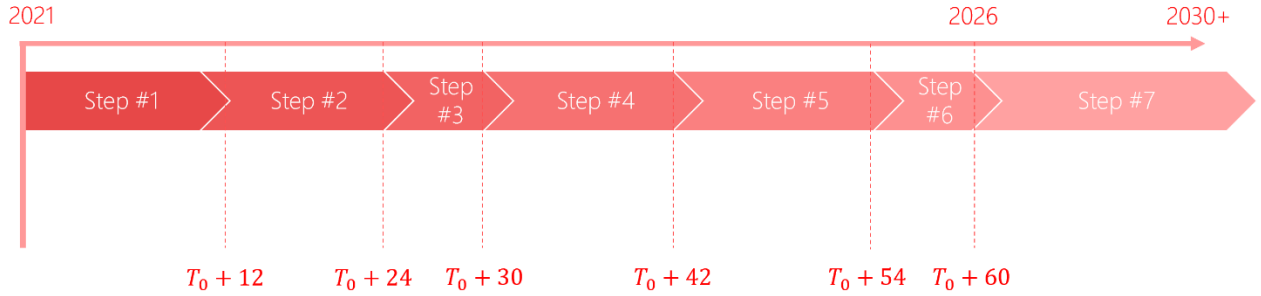

Figure 4 - Possible STM Framework Timeline

Considering the quickly increasing congestion of the space environment, and thus of collision probabilities, highlighted in Section 1, deploying a space traffic management framework before most mega-constellations achieve operational capacity, that is, before 2025 [59], would be ideal but unrealistic because its technical complexity and political obstacles are too great to be overcome in such a compressed timeline. More realistically, an optimistic activity schedule assuming stakeholders were willing to cooperate and invest in its development, is in a five-to-ten-year range, presented in Figure 4.

The first step, deriving and consolidating stakeholder requirements, is likely to last up to twelve months as there are many stakeholders and use cases involved. Thus, there will be a lengthy documentation and negotiation effort before any agreement can be achieved. Afterwards, the technical aspects will dominate; designing and implementing the communication architecture will probably require another twelve months to reach operational capabilities since it is an innovative system that will have to satisfy hundreds to thousands of requirements. Fortunately, if there is a decision to build the STM framework, then during the requirement phase many of the underlying technologies will be rapidly improved due to increased commercial interest, especially with regards to tooling to develop and verify distributed ledger systems. Also, designing and implementing the federated identity management services should be faster, taking up to six months, as these are already well-established in cloud services [60] [61].

Because stakeholders must collaborate and negotiate to standardise and harmonise their wide variety of processes, data formats, and conflict negotiation and operational procedures, steps 4 and 5 could potentially last 24 months if we take as reference international standardisation efforts, which typically take three years from proposal to final publication [62]. Here, the problem is to define few formats and processes capable of matching stakeholder expectations while still not being overly complex to lead to custom ad-hoc uses. For example, simply building a jumbo format would make the entire system dependent on stakeholders' software implementations, negating any advantages of standardisation. Once these procedures and formats are standardised, automating them at the smart contract level is not particularly hard and, at that point, the tooling to implement them should be sufficiently mature to ensure their security.

With enough interest and financial resources, the framework could be deployed and become operational worldwide within six months because there would be no special infrastructure requirements and users and service providers would only require common-off-the-shelf equipment to participate. As part of this step, defining who are the core network maintainers and service providers could easily take a few months given the importance of the framework. Nevertheless, as with any technology, adoption will likely be phased over the years and, as more users switch over to the STM network, the greater will be the incentive for others to participate in it.

Finally, incentivising user adoption, establishing legal frameworks and incorporating users into the data-supply economy are multi-year to multi-decade processes, but should be a natural consequence of building the STM framework and could happen in parallel with its design.

6.3. Challenges

The design and implementation of a unified STM framework combining traffic management, peer-to-peer communication, machine-to-machine (M2M) service infrastructures, and blockchain/distributed ledger technologies,

is extremely challenging not only politically and organisationally, as one must negotiate and manage competing stakeholder needs and interests, but also technically. Each of these systems have different capabilities, interfaces, limitations, and technology readiness levels, and making them interoperable is hard. Two vital issues stand out:

First, insufficient technological maturity, limited throughput, and cybersecurity issues may limit the applicability of distributed-ledger technologies to mission-critical real-time manoeuvre coordination such as evasive manoeuvres where, if the confidentiality, authenticity, latency, and integrity of data cannot be guaranteed, there can be catastrophic consequents with loss of hardware integrity. As novels fields of research, blockchains, distributed ledgers, and smart contracts are still evolving, as are their security and throughput. Over the years, there have been several security incidents and attacks [63, 11] that may make stakeholders reluctant to use them and, considering that a successful cyber-attack on a large, shared network may have higher impact and widespread political and strategic implications than equivalent attacks on current compartmented centralised infrastructures, security considerations may limit stakeholder collaboration and participation.

Second, there is a lack of historical data to validate coordination algorithms and operational processes. Export restrictions notwithstanding, stakeholders shy away from sharing data regarding their assets and processes as they deem it sensitive and business-critical for competitiveness and financial reasons. Also, historically, there were very few owners and operators of space assets managing a total of a few hundred assets. Instead, in the near-future, space congestion will involve thousands of assets flying close to each other and require coordination between tens of stakeholders with severely competing interests. Thus, it may be impossible to realistically model and simulate their behaviour when designing the STM framework, which means that its operational performance may be worse than expected.

Finally, the human aspect can also be a barrier for the adoption of a highly automated STM system because of a lack of trust in automated algorithms and distributed information management systems in such a risk-averse space sector. For the same reason, in the aerial sector, despite human errors being the leading cause of aircraft accidents [64], pilot control is demanded during take-offs and landings and pilots have the ultimate authority to override the aircraft's on-board computer. As a relatively novel and upcoming field of research, distributed ledgers and blockchain are viewed with scepticism, and thus it is expected and natural that experienced operations personnel, who spent decades mastering the profession, feel uneasy about the prospect of leaving complex activities, such as space operations, at the mercy of 'opaque' algorithms.

7. Summary and Conclusions

The diversity and number of actors in space, the polarization of geopolitics, and the increasing collision threats between space assets and debris demand a cooperative approach to STM where there is a coordination of actions. To tackle this challenge, first and foremost, one must deeply understand drivers, interests and prime stakeholder needs. For instance, balancing short-term financial interests of the satellite industry with the security and trust concerns of data-sharing between data providers and policy-makers regulators are paramount to developing a credible solution capable of accommodating such a diverse ecosystem.

Recent conjunction events have highlighted the gaps and complexities of current STM systems, whereby the issue of liability in the international stage remains unaddressed. The adoption of common STM solutions requires nonetheless that stakeholders agree on strategies, e.g., for collision avoidance, that will form the basis of authoritative coordination decisions. Technically, this entails a standardisation and interoperability of protocols and data. From an economic perspective, the perceived benefit from adopting common solutions must come from significant risk and cost reductions. Furthermore, if a dedicated STM framework is to be developed, establishing data-access control policies and encryption mechanisms will help drive adoption, particularly by institutional and military agents who may be wary of sharing classified information on this bespoke STM network.

With this mindset, distributed technologies such as blockchains have been extensively proposed to overcome these issues. Blockchains facilitate the exchange of data (particularly for communicating imminent conjunctions openly) and the negotiation of avoidance strategies among stakeholders both within and outside of the space sector and support immutable transactions (financial and services) between stakeholders. Ultimately, decisions can be made autonomously and conflict resolution can be automated if stakeholders become adopters and trustees of a blockchain. With the shortening of response windows due to increased congestion, such mechanisms have the benefit of decreasing latencies, increasing operational efficiencies and de-risking of conflicts in the orbital environment.

To unify stakeholder requirements and future trends of the space economy, a stepwise roadmap for exploiting and deploying blockchain technologies within a five-to-ten-year timeline was devised. This roadmap foresees the

implementation of decentralised communications architectures that rely on identity federation and associated identity access management and validation to ensure only authenticated users have access to data and services they are subscribed to. Similarly, automated processes for conflict negotiation, manoeuvre planning, and risk management, including data-provenance verification, must be defined and agreed upon prior to deployment. The last step involves developing a legal framework to establish stakeholder liabilities and contractual responsibilities that can be enforced transnationally, laying the ground for a trustworthy and (user-centred) transparent services and data marketplace.

Finally, a potential future STM solution is composed of a layered architecture that comprises a core network and application layers, whereby the core of the network handles service requests, identity verification of users and the validation of contracts and data exchanged on the network itself via nodal consensus. The application layer consists of national and commercial entities validating the identity of stakeholders that freely transact data in a common data-supply marketplace.

Addressing the space sustainability challenge by putting in place blockchain-led STM solutions is certainly not an easy task. On the one hand, technological immaturity to cope with an increasingly multi-faceted ecosystem may not allow solutions to evolve at the required pace. On the other hand, automating conflict-resolution means to an extent delegating decision-making authority to algorithms. The lack of trust between humans and machines and among stakeholders may dampen collective efforts, particularly in the face of a risk-averse industry. It must be highlighted nonetheless that the higher the adoption of distributed STM solutions, the bigger the incentive for external stakeholders to part-take and contribute to the framework. The window of opportunity for saving the space environment is narrowing and the time to act is now in order to keep up with the rising volume of traffic in orbit.

References

[1] V. Eder, "#spacewatchgl Opinion: Lock Down on all Space Launches.," SpaceWatch.Global, ThorGroup GmbH., 2021. [Online]. Available: https://spacewatch.global/2021/02/spacewatchgl-opinion-lock-down-on-all-space-launches. [Accessed 01 March 2021].

[2] P. Righetti, F. Sancho, D. Lazaro and A. Damiano, "Handling of conjunction warnings in EUMETSAT flight dynamics," *Journal of Aerospace Engineering, Sciences and Applications,* vol. 3, pp. 39-53, 2011.

[3] A. Venkatesan, J. Lowenthal, P. Prem and M. Vidaurri, "The Impact of Satellite Constellations on Space as an Ancestral Global Commons," *Nature Astronomy,* 2020.

[4] S. M. Patrick, "A New Space Age Demands International Cooperation, Not Competition or 'Dominance'," 2019. [Online]. Available: https://www.worldpoliticsreview.com/articles/27869/a-new-space-age-demands-international-cooperation-not-competition-or-dominance. [Accessed 03 March 2021].

[5] D. Fiott, "The European space sector as an enabler of EU strategic autonomy.," European Union Institute for Security Studies (EUISS), Policy Department for External Relations Directorate General for External Policies of the Union PE 653.620, 2020.

[6] EUROCONTROL, "Specification for SWIM Technical Infrastructure (TI) Yellow Profile, Edition: 1.1," EUROCONTROL-SPEC 170, 2020.

[7] S. Velásquez Correa, M. Castells Sanabra and U. Svedberg, "MONALISA 2.0 and the sea traffic management - a concept creating the need for new maritime information standards and software solutions," Technical Report, 2015.

[8] Florence School of Regulation, "Disruptive technologies in air traffic management," 2016. [Online]. Available: https://fsr.eui.eu/disruptive-technologies-atm/. [Accessed 31 03 2021].

[9] International Civil Aviation Organization, "Civil/Military Cooperation in Air Traffic Management (CIR 330 AN/189)," 2012.

[10] B. Scheiner, "Blockchain and Trust," 12 02 2019. [Online]. Available: https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html. [Accessed 31 03 2021].

[11] T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," *IEEE Communications Surveys & Tutorials (Volume: 21, Issue: 1, Firstquarter 2019),* pp. 858-880, 2019.

[12] J. H. Lee, "Systematic approach to analyzing security and vulnerabilities of blockchain systems," Massachusetts Institute of Technology, 2019.

[13] D. J. Kessler, N. L. Johnson, J. C. Liou and M. Matney, "The Kessler syndrome: implications to future space operations.," *Advances in the Astronautical Sciences,* vol. 137, no. 8, 2010.

[14] C. Contant-Jorgenson, P. Lála and K.-U. Schrogl, "The IAA Cosmic Study on space traffic management," *Space Policy,* vol. 22, no. 4, 2006.

[15] F. G. von der Dunk, "Space Traffic Management: A Challenge of Cosmic Proportions," *Proceedings of the International Institute of Space Law 2015,* vol. 58, no. 2016, pp. 385--396, 2016.

[16] M. Wall, "European Satellite Dodges Potential Collision with SpaceX Starlink Craft," Space, 05 September 2019. [Online]. Available: https://www.space.com/spacex-starlink-esa-satellite-collision-avoidance.html. [Accessed 31 03 2021].

[17] National Aeronautics and Space Administration, "NASA, SpaceX Sign Joint Spaceflight Safety Agreement," 18 03 2021. [Online]. Available: https://www.nasa.gov/press-release/nasa-spacex-sign-joint-spaceflight-safety-agreement. [Accessed 31 03 2021].

[18] J. Roulette, "OneWeb, SpaceX satellites dodged a potential collision in orbit," The Verge, 09 04 2012. [Online]. Available: https://www.theverge.com/2021/4/9/22374262/oneweb-spacex-satellites-dodged-potential-collision-orbit-space-force. [Accessed 09 04 2021].

[19] M. K. Ben-Larbi, K. Flores Pozo, T. Haylok, M. Choi, B. Grzesik, A. Haas, D. Krupke, H. Konstanski, V. Schaus, S. P. Fekete, C. Schurig and E. Stoll, "Towards the automated operations of large distributed satellite systems. Part 1: Review and paradigm shifts," *Advances in Space Research,* 2020.

[20] M. Öszu and P. Valduriez, "Distributed and Parallel Database Systems," *ACM Computer Survey,* vol. 28, pp. 125-128, 1996.

[21] N. Szabo, "Formalizing and Securing Relationships on Public Networks," *First Monday,* vol. 2, no. 9, 1997.

[22] S. Klein, W. Prinz and W. Gräther, "A use case identification framework and use case canvas for identifying and exploring relevant blockchain opportunities," in *European Society for Socially Embedded Technologies,* 2018.

[23] C. Kerrache, C. T. Calafate, J. Cano and N. a. M. P. Lagraa, "Trust Management for Vehicular Networks: An Adversary-Oriented Overview," *IEEE Access,* vol. 4, pp. 9293-9307, 2016.

[24] L. Li, J. Liu, L. Cheng, S. Qiu and W. Wang, "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles," *IEEE Transactions on Intelligent Transportation Systems,* vol. 19, no. 7, 2018.

[25] X. Zhang and X. Chen, "ata Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network," *IEEE Access,* vol. 7, pp. 58241-58254, 2019.

[26] A. Fujihara, "Proposing a System for Collaborative Traffic Information Gathering and Sharing Incentivized by Blockchain Technology," *Advances in Intelligent Networking and Collaborative Systems,* vol. 23, p. Lecture Notes on Data Engineering and Communications Technologies, 2019.

[27] D. Prashar, N. Jha, S. Jha, G. Joshi and C. Seo, "Integrating IoT and Blockchain for Ensuring Road Safety: An Unconventional Approach," *Sensors,* vol. 20, no. 11, p. 3296, 2020.

[28] V. Astarita, V. P. Giofrè, G. Mirabelli and V. and Solina, "A Review of Blockchain-Based Systems in Transportation," *2020,* vol. 11, no. 1, p. 21.

[29] G. Muniandi, "Blockchain-enabled virtual coupling of automatic train operation fitted mainline trains for railway traffic conflict control," *IET Intelligent Transport Systems,* 2020.

[30] G. Hua, L. Zhu, J. Wu, C. Sehn, L. Zhou and Q. Lin, "Blockchain-Based Federated Learning for Intelligent Control in Heavy Haul Railway," *IEEE Access 8,* pp. 176830-176839, 2020.

[31] M. Kuperberg, D. Kindler and S. Jeschke, "Are smart contracts and blockchains suitable for decentralized railway control?," *arXiv preprint arXiv:1901.06236.,* 2019.

[32] R. Hackett, "IBM and Maersk are creating a new blockchain company.," 2018. [Online]. Available: http://fortune. com/2018/01/16/ibm-blockchain-maersk-company. [Accessed 01 March 2021].

[33] Marine Insight News Network, "PIL, PSA and IBM conclude a successful testing of blockchain technology," 23 February 2018. [Online]. Available: https://www.marineinsight.com/shipping-news/pil-psa-ibm-conclude-successful-testing-blockchain-technology/. [Accessed 01 March 2021].

[34] Medium, "A day to remember: The first ever blockchain-based CargoX Smart B/L™ has successfully completed its historic mission during a trial shipment from China to Europe," 2018. [Online]. Available: https://medium.com/cargoxio/a-day-to-remember-the-first-ever-blockchain-based-cargox-smart-b-l-has-successfully-completed-its-491657fecf71. Accessed 01/03/2021.. [Accessed 01 March 2021].

[35] Marine Insight News Network, "Port of Antwerp confirms pioneering role in the field of innovation with blockchain based document workflow.," 21 June 2018. [Online]. Available: https://www.marineinsight.com/shipping-news/port-of-antwerp-confirms-pioneering-role-in-the-field-of-innovation-with-blockchain-based-document-workflow. . [Accessed 01 March 2021].

[36] Marine Insight News Network, "Abu Dhabi Ports launches blockchain technology for trade community," 4 June 2018. [Online]. Available: https://www.marineinsight.com/shipping-news/abu-dhabi-ports-launches-blockchain-technology-for-trade-community.. [Accessed 01 March 2018].

[37] L. Li and H. Zhou, " A survey of blockchain with applications in maritime and shipping industry.," *Information Systems and e-Business Management,* pp. 1-19, 2020.

[38] M. Jović, E. Tijan, D. Žgaljić and S. Aksentijević, "Improving Maritime Transport Sustainability Using Blockchain-Based Information Exchange.," *Sustainability 12,* vol. 21, no. 2020, p. 8866, 2020.

[39] G. Bavassano, C. Ferrari and A. Tei, "Blockchain: How shipping industry is dealing with the ultimate technological leap," Research in Transportation Business andManagement, 34, 100428., 2020.

[40] FlightChain, "Research into The Usability and Practicalities of Blockchain Technology for the Air Transport Industry Whitepaper," SITA, https://www.sita.aero/globalassets/docs/white-papers/flightchain-whitepaper.pdf, 2017.

[41] Distributed Sky, "Blockchain Framework for UAS Traffic Management," Decentralized Technology, Inc, 2018.

[42] Sky Grid, "Next-Gen Airspace Management for Drones," SkyGrid , 2020.

[43] R. Tüllmann, C. Arbinger, S. Baskcomb, J. Berdermann, H. Fiedler, E. Klock and T. Schildknecht, "Air Meets Space: Shaping the Future of Commercial Space Traffic: I. Study Introduction and Initial Results," in *67th International Astronautical Congress,* 2016.

[44] R. Tüllmann, C. Arbinger, S. Baskcomb, J. Berdermann, H. Fiedler, E. Klock and T. Schildknecht, "On the Implementation of a European Space Traffic Management System -I. A white Paper," 2017.

[45] R. Tüllmann, C. Arbinger, S. Baskcomb, J. Berdermann, H. Fiedler, E. Klock and T. Schildknecht, "On the Implementation of a European Space Traffic Management System -II. The Safety and Reliability Strategy," 2017.

[46] R. Tüllmann, C. Arbinger, S. Baskcomb, J. Berdermann, H. Fiedler, E. Klock and T. Schildknecht, "On the Implementation of a European Space Traffic Management System -III. Technical Requirements," 2017.

[47] R. Tüllmann, C. Arbinger, S. Baskcomb, J. Berdermann, H. Fiedler, E. Klock and T. Schildknecht, "Towards a European Space Traffic Management System," *Proceedings of the 9 th IAASS Conference "Know Safety, No Pain", vol. 9,* pp. 257-263, 2018.

[48] B. Bastida Virgili, T. Flohrer, H. Krag, K. Merz and S. Lemmens, "CREAM—ESA's Proposal for Collision Risk Estimation and Automated Mitigation.," *LPI Contributions 2109,* p. 6031, 2019.

[49] S. Nag, D. Murakami, M. Lifson and P. Kopardekar, "System Autonomy for space traffic management, IEEE," *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC),* pp. 1-10, 2018.

[50] D. D. Murakami, S. Nag, M. Lifson and P. H. Kopardekar, "Space Traffic Management with a NASA UAS Traffic Management (UTM) Inspired Architecture," in *AIAA Scitech Forum,* 2019.

[51] J. V. Cabrera, S. Nag and D. D. Murakami, "An Initial Analysis of Automating Conjunction Assessment and Collision Avoidance Planning in Space Traffic Management," NASA, 2019. [Online]. Available: https://ntrs.nasa.gov/api/citations/20190001614/downloads/20190001614.pdf. [Accessed 01 March 2021].

[52] S. Nag, D. D. Murakami, N. A. Marker, M. T. Lifson and P. H. Kopardekar, "Prototyping Operational Autonomy for Space Traffic Management," *Acta Astronautica,* p. 180, 2019.

[53] W. Zaidi, W. Faber, T. Kelecy., N. Altaf and S. Janakiraman, "Enabling Worldwide and Transparent STM through Decentralized and Trustworthy Space Domain Awareness," in *71st International Astronautical Congress,* 2020.

[54] CCSDS, "Spacecraft Manoeuvre Messages, Proposed Recommendation for Space Data System Standards (CCSDS 511.0-W-4)," 2014. [Online]. Available: https://cwe.ccsds.org/moims/docs/MOIMS-NAV/Draft%20Documents/XX%20-%20Spacecraft%20Maneuver%20Message%20(SMM)%20-%20Obsolete/SMM%20Archive/CCSDS_511.0-W-4.0_Spacecraft_Maneuver_Messages.pdf. [Accessed 31 03 2021].

[55] CCSDS, "Spacecraft Perturbation Messages, Proposed Recommendation for Space Data System Standards (CCSDS 507.0-W-1.2)," 2010. [Online]. Available: https://cwe.ccsds.org/moims/docs/MOIMS-NAV/Draft%20Documents/XX%20-%20Spacecraft%20Perturbations%20Message%20(SPM)%20-%20Obsolete/SPM%20Archive/507x0w1.2-changestracked.pdf. [Accessed 31 03 2021].

[56] CCSDS, "Navigation Hardware Messages, Proposed Recommendation for Space Data System Standards (CCSDS 510.0-W-915)," 2015. [Online]. Available: https://cwe.ccsds.org/moims/docs/MOIMS-NAV/Draft%20Documents/XX%20-%20Navigation%20Hardware%20Message%20(NHM)%20-%20Obsolete/NHM%20Archive/NavigationHardwareMessageV015ChangesAccepted.pdf. [Accessed 31 03 2021].

[57] CCSDS, "Conjunction Data Messages, Recommendation for Space Data System Standards (CCSDS 508.0-B-1)," 2010. [Online]. Available: https://public.ccsds.org/Pubs/508x0b1e2c1.pdf. [Accessed 31 03 2021].

[58] CCSDS, "CCSDS File Delivery Protocol, Recommendation for Space Data System Standards (CCSDS 727.0-B-5)," 2020. [Online]. Available: https://public.ccsds.org/Pubs/727x0b5.pdf. [Accessed 31 03 2021].

[59] KPMG, "30 Voices on 2030 - The Future of Space: Communal, commercial, contest," 05 2020. [Online]. Available: https://assets.kpmg/content/dam/kpmg/au/pdf/2020/30-voices-on-2030-future-of-space.pdf. [Accessed 31 03 2021].

[60] Amazon AWS, "Identity federation in AWS," [Online]. Available: https://aws.amazon.com/identity/federation/. [Accessed 31 03 2021].

[61] Microsoft, "What is federation with Azure AD?," 28 11 2018. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed. [Accessed 31 03 2021].

[62] International Organization for Standardization, "Developing Standards," [Online]. Available: https://www.iso.org/developing-standards.html. [Accessed 31 03 2021].

[63] N. Atzei, M. Bartoletti and T. Cimoli, "As a novel field of research, distributed ledger and blockchain security," in *Proceedings of the 6th International Conference on Principles of Security and Trust - Volume 10204*, 2017.

[64] E. G. Tetteh, "Human factors analysis of commercial aircraft accidents in the United States: 1960-2000.," in *In IIE Annual Conference. Proceedings (p. 1), Institute of Industrial and Systems Engineers (IISE)*, 2006.