Blockchain Enabled Space Traffic Awareness (BESTA): Discovery of Anomalous Behavior Supporting Automated Space Traffic Management

Harvey Reed[1]
The MITRE Corporation, 202 Burlington Road, Bedford MA 01730 USA, hreed@mitre.org

Nathaniel Dailey, MPAP, CEA[2]
The MITRE Corporation, 7525 Colshire Drive McLean, VA 22102 USA, and Johns Hopkins University, Paul H. Nitze School of Advanced International Studies (SAIS), 1740 Massachusetts Ave NW, Washington, DC 20036 USA, ndailey@mitre.org and ndailey2@jhu.edu

Robert Carden[3]
The MITRE Corporation, 1155 Academy Park Loop, Colorado Springs, CO 80910 USA, rcarden@mitre.org

Dave Bryson[4]
The MITRE Corporation 201 East Moore Drive Bldg 856, Room 102E, Maxwell AFB-Gunter Annex, Montgomery, AL 36114 USA, dbryson@mitre.org

Today, satellite launches, on-orbit operations, and deorbiting by space faring countries is manual-intensive and safe. However, projected increases in number of space faring nations, and volume of space traffic, will strain Space Traffic Management (STM) processes and operations, requiring increased automation. STM processes and operations require timely space object data for all objects, in the context of clear and unambiguous understanding of the current agreements and intents for maneuvering and operating active space objects.

However, the volume, types, and complexity of space object data is steadily increasing, for example (a) increasing number space objects including from mega constellations; (b) increasing number of types of data beyond TLE such as intent to maneuver and health/status; (c) increasing number of sources of data from commercial and national sources, and; (d) increased need for cross-domain information sharing and integration across space, air space, land, and maritime domains. The increase in number, types, and complexity of space object agreements is driven by a growing number of spacefaring and space interested nations who enter into agreements which describe increasingly complex ranges and constraints of operational behavior. The ability to discover behavioral anomalies by comparing observed

[1] Blockchain Capability Lead
[2] Enterprise Architect
[3] Space BMC2 Systems Lead Engineer
[4] Blockchain Technology Lead

behavior to agreed and intended behavior is the foundation for encouraging good behavior and enforcing compliance.

BESTA Blockchain Enabled Space Traffic Awareness) is a proposed framework for automatically detecting behavioral anomalies, by comparing observations to agreements, then recording the anomalies on the BESTA blockchain as evidence dockets for subsequent adjudication. This is a first step toward automating key activities of STM. BESTA compares space object data to agreements in order to detect anomalies which represent potential non-conforming space object behavior. These anomalies, together with pertinent data and agreements are captured in evidence dockets on the BESTA blockchain, for subsequent adjudication, either human in the loop, or automatic. Comparison of data and agreements requires provably correct provenance of both the space object observation and other data, and the applicable agreement documents. Further, the generated evidence docket must be protected against tampering. BESTA is an open source, permissioned blockchain-enabled capability suitable for international and commercial stakeholders, providing tamper-evident, attributed, resilient, and available data. This paper describes high level modular architecture and needed research to enable prototype implementations.

BESTA internal architecture is modular, enabling continuous evolution and improvement. Types of modules include (a) SDA Input Provenance; (b) SDA Information Sharing; (c) Agreements Provenance; (d) Agreement Information Sharing; (e) SDA and Agreement Comparison; (f) Anomaly Evidence Preparation; (g) Anomaly Adjudication. For each type of module, there may be multiple instances of module, where each instance is dedicated to a type of data, such as TLE, frequency, etc. The instance of module then uses instances of actual data at runtime.

BESTA research topics inform modules such as anomaly discovery in the SDA and Agreement Comparison module, and evidence capture and secure storage in the Anomaly Evidence Preparation module. Discovery research includes automatic ingest of agreements, policies, and regulations into machine readable ontologies for later comparison to behavior observation data streams, as well as reconciliation of multiple and perhaps differing observation data (e.g. multiple catalogs). Evidence capture and secure storage research includes automatic preparation of evidence packages which contain relevant agreements and observations, to be used in subsequent adjudication and mitigation activities. Results of discovery and evidence preparation must be trusted across all stakeholders even in contested or adversarial environments (e.g. space and great power competition). Further, BESTA must be "brownfield", that is able to be used in current context (agreements, data) with minimal disruption.

The vision for BESTA is a platform to enable safe and secure voluntary information sharing and decision making to support international cooperative STM. There are analogs to the envisioned information sharing model, such as the Aviation Safety Information Analysis and Sharing (ASIAS), and International Civil Aviation Organization (ICAO) operating models. BESTA blockchain nodes are owned and operated by participating spacefaring nations ensuring tamper-evident and attributed data with resilience and availability against accident or attack. Use of the International Space Reference Architecture (ISRA, Dailey, Reed IAC 2019) to align policy, behavior, and lexicon can assure common understanding and meaning of discovered anomalies and evidence packages.

Paper closes with a proposed information sharing model for STM that includes: (a) foundational space sensor data (e.g. Space Surveillance Network); (b) economically-driven augmentation of foundational space sensor data with commercial and academic sensor data, and; (c) use of BESTA to reconcile multiple inputs of space object data, compared to prior agreements and statements of intent, automatically detecting anomalies and recording them in evidence dockets as they occur..

I. Keywords, Acronyms,

Space Situational Awareness (SSA), Space Traffic Management (STM), International Space Reference Architecture (ISRA), U.S. Strategic Command (USSTRATCOM), U.S. Space Policy Directive – 3 (SPD-3), Asia-Pacific Ground-Based Optical Space Object Observation System (APOSOS), International Scientific Optical Network (ISON), U.S. Federal Aviation Administration) (FAA), Blockchain Enabled Space Traffic Awareness (BESTA), Sensor Network Autonomous Resilient Extensible (SNARE), Two Line Element set (TLE), Global Value Function (GVF), Local Value Function (LVF), Open Architecture Data Repository (OADR), U.S. Dept. of Commerce (DoC), International Telecommunication Union (ITU)

II. Introduction

Satellite launches, on-orbit operations, and deorbiting is manual-intensive and safe, and requires stakeholder Space Situational Awareness (SSA), coordination, and automation. However, projected increases in both number of space faring nations, and volume of space traffic, will strain these processes and operations, and require increased stakeholder coordination and automation.

Stakeholder coordination requires situational awareness of the current orbit and position of satellites, launch paths through the atmosphere, and deorbit paths at end of life. Today, much of space situational awareness of orbits is expressed in the U.S. Strategic Command (USSTRATCOM) space catalog [1], where objects are screened and potentially updated at least daily. Recently, U.S. Space Policy Directive – 3 (SPD-3) [2] directs the U.S. Dept. of Commerce (DoC) to provide a catalog that incorporates SSA data from not only traditional sources, but also commercial companies (e.g. LEO-Labs, AGI), and data from other nations (e.g. Germany, France, Australia).

SPD-3 directs U.S. Government to:

- Provide basic SSA data and basic Space Traffic Management (STM) services to the public (Sec. 4.d Goals)
- Improve SSA data interoperability and enable greater SSA data sharing (Sec. 4.e Goals)
- Improve SSA coverage and accuracy (Sec. 5.a.i Guidelines)
- Establish an Open Architecture SSA Data Repository (Sec. 5.a.ii Guidelines)

There are additional space situational efforts such as Asia-Pacific Ground-Based Optical Space Object Observation System (APOSOS) organized by China, International Scientific Optical Network (ISON) organized by Russia, as well as commercial and academic sensors. Today, the SSA data above is provided as disparate siloed services with independent access rules.

Maturation of current launch, orbit, and deorbit lifecycle processes and operations into STM requires not only DoC orbital data in the current space catalog, but also orbital data from APOSOS, ISON, commercial launch and payload companies, academic and lab observations, from all space faring nations. Today, this data is provided in siloed services with independent access rules. Beyond orbital data, launch paths through the atmosphere, and deorbit paths must be included.

SSA for STM must be useful for space operations in a tactical timeline, versus a post-mortem autopsy, and must remain current and relevant during expected and unexpected circumstances. STM situational awareness must also be extensible to include new data types and sources, with access for all stakeholders to data once written. This expanded definition of situational awareness tracks assets from ground to space and back is challenged by the need for data collection and sharing among a diverse and increasing number of stakeholders. This paper focuses on timely information sharing among diverse stakeholders to support STM.

The international space faring community will benefit by sharing SSA from the above sources and more. Sharing SSA information among competitive nations and commercial interests requires transparency, identifying which party is contributing what data (identity, and data provenance), and trust in the safe keeping of SSA data (data integrity, availability, resilience to accident and attack). Sharing SSA information among competitive nations and commercial interests requires a mutually beneficial mission (STM and flight/orbit safety) and transparent structure of data protection to incentivize cooperation. The U.S. Federal Aviation Administration (FAA) overcame the competitive concerns among commercial airlines though a clearly defined structure of data protection in the Aviation Safety Information Analysis and Sharing (ASIAS) program [3], and this effort can inform improvements to SSA and STM.

Blockchain Enabled Space Traffic Awareness (BESTA) is proposed as both an extension to the current catalog, and as an alternative to the (multiple) single owner / operator model. Blockchain technology is uniquely suited to enable reading and writing among all STM stakeholders, by increasing the confidence in data that is cryptographically attributed to the originator, where that data cannot be counterfeited, changed, or destroyed. Blockchain provides the opportunity to streamline stakeholder relationships, shortening timelines for capturing data, and provides a secure foundation for increased automation.

III. Diffused and Centralized Mission Information Sharing

Missions are multi-stakeholder endeavors which span enterprise stakeholders and end user persons. These missions deliver benefits for the stakeholders and individual persons and require cooperation and coordination among stakeholders to achieve success.

Examples of multi-stakeholder missions include:

- Cryptocurrencies
- Food safety and other supply chains
- Logistics and shipping
- Sensing
- Financial and banking

Cooperation and coordination are largely achieved by stakeholders exchanging data across their enterprise and organizational boundaries, often in diffused (all-to-all), centralized (all-to-one), or feudal (islands of centralization) information sharing approaches. A government, commercial, or other enterprise typically has their own identity and credential regime, and funds, owns and operates its own computing and data resources. Each stakeholder is responsible to maintain their data inside their own enterprise, including their version of situational awareness of the entire mission, sharing as needed with other mission stakeholders to execute their contribution to mission execution.

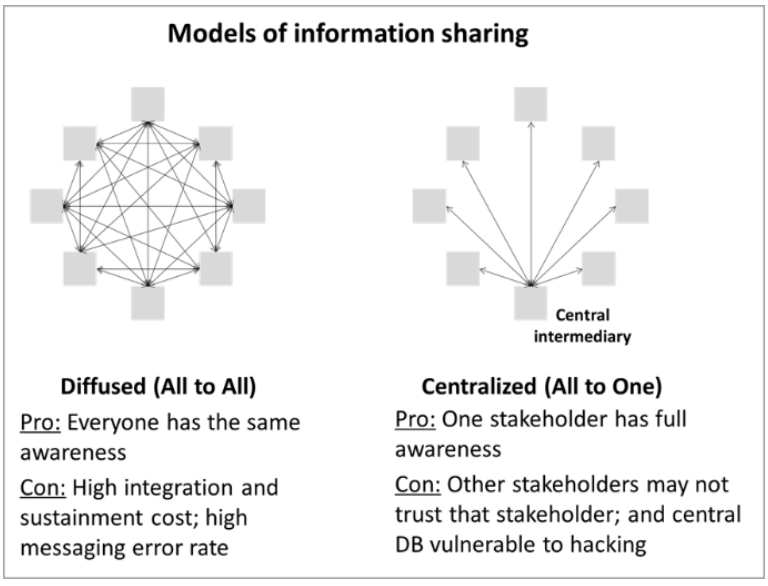

Fig. 1 Information Sharing Models

Two types of mission stakeholder information sharing are diffuse and centralized, see Fig. 1. Each pose significant challenges to free flow of sharing mission information. The diffuse model requires each stakeholder to negotiate with all the other stakeholders to bridge bi-lateral security and data sharing protocols. Each new stakeholder is required to integrate with all other stakeholders and requires existing stakeholders to integrate with the newcomer. This results in significant integration and sustainment cost, as well as numerous points of failure for exchanging information, due to political, technical, accidental, and malicious attack causes.

One approach for information sharing within a mission is to create a new centralized repository, owned and operated by a single stakeholder who functions as a centralized intermediary, and whose data is collected from all or a subset of stakeholders, and later used by all mission stakeholders. One example of a centralized intermediary is the USSTRATCOM publication of the www.space-track.org space object catalog [4]. The data is centrally collected from sensors (e.g. government and commercial) and published as a centralized resource.

The obvious benefit of the centralized information sharing model is a simplified data exchange where each stakeholder accesses one space catalog. However, as the criticality and number of data types and stakeholders increase, so does distrust of the single owner and operator among the stakeholder community.

Stakeholder distrust of shared information can arise in each of the diffused, centralized, or feudal information sharing models. The diffused sharing model can drop messages (e.g. accident or attack) and prevent each stakeholder's internal mission worldview from accurately reflecting reality. When stakeholder's internal worldviews are not in sync with reality, distrust increases (e.g. am I missing critical data?) and cooperation is slowed or inhibited. The centralized sharing model attempts to correct the synchronization problem (e.g. one source of data) but in turn introduces distrust due to one stakeholder holding all the data (e.g. possibility of agenda driven data), since there may be no assurance of integrity and availability (e.g. lack of cryptographic proof). The feudal sharing model combines aspects of both centralized and diffuse and inherits the data sharing problems of both.

An alternative is to decentralize the mission using blockchain technology [5].

IV. Decentralized Mission Information Sharing

Missions can improve the sharing of information and mission outcomes, by requiring stakeholders to post information sharing transactions to a shared mission blockchain. The mission blockchain is conceptually external to all stakeholders, while being shared by all stakeholders. This is a disruptive change from legacy information sharing models, whether diffuse, centralized, or feudal. These legacy information sharing models require each stakeholder to generate and maintain their own internal copy of needed mission data in their enterprise. Independent copies of mission data introduce risk of data misalignment among stakeholders.

In contrast, a decentralized information sharing model externalizes mission data to the blockchain, which is comprised of independent nodes, each of which contain a redundant copy of all the data posted to the blockchain, see Fig. 2. Stakeholders operate blockchain nodes in their enterprise environments in accordance with mission governance decisions. Ideally, blockchain nodes will operate in sufficiently diverse operating environments to provide resiliency to attack. Regardless of node allocation to operating environments, nodes must maintain P2P (Peer-to-Peer) network connection with each other to validate transactions and perform consensus on blocks of transactions.

Using blockchain, all stakeholders write and read transactions, simplifying information exchange and maximizing data transparency. The blockchain uses multiple nodes for redundancy, where posted transactions are replicated across blockchain nodes, and data consistency is assured by the consensus algorithm. Each stakeholder reads each other's blockchain transactions, improving situational awareness, self-synchronization, and outcomes. Each stakeholder bears the responsibility to update their own enterprise data capabilities to incorporate blockchain as the mission authoritative source for shared information.

Stakeholders individually have confidence in the blockchain data, even if they would not necessarily trust each other bilaterally without the blockchain. Some blockchain descriptions use the term "trustless" although this is confusing. A better description is that stakeholders who may not otherwise trust each other, can trust the blockchain and share specific agreed types of mission data for the mutual benefit of stakeholders engaged in a common mission.

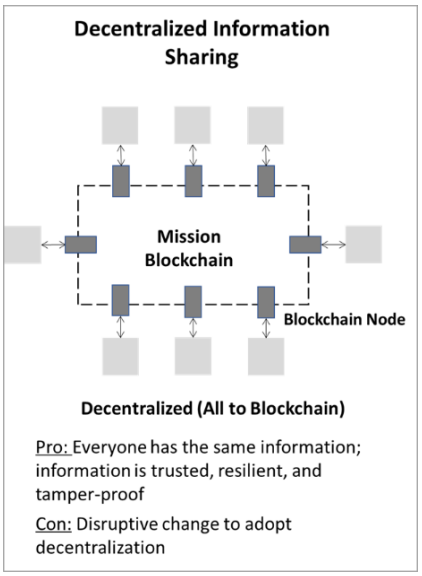

Fig. 2 Decentralized Information Sharing

Blockchain was first used to implement cryptocurrency such as Bitcoin [6], which records amounts of digital value (BTC) assigned to users via their public Bitcoin addresses. Blockchain later evolved to support commercial activities, such as the Walmart food safety blockchain network, where the blockchain records food supply chain events (e.g. harvest, process, retail sale) as blockchain transactions. Both cases can be described as missions with many users or stakeholders, where effective information sharing can improve mission outcomes (e.g. indisputable ledger of Bitcoin ownership, rapid response to tainted food).

Cryptocurrencies are implemented with public blockchains, frequently with thousands of nodes, operated by crypto mining companies and individuals alike. Public blockchains use a consensus mechanism that is competitive, energy intensive, and can survive sizeable attacks up to nearly half of the nodes being malicious. Commercial and government missions frequently use permissioned blockchains, with a hundred or less nodes, controlling which nodes are permitted to join, participate, and leave. Permissioned blockchains which use the voting-based byzantine fault tolerant consensus mechanism, are significantly faster and less energy intensive, and can survive attacks up to almost a third of the nodes being malicious.

V. BESTA Architecture

BESTA is proposed as an open source, internationally funded, built, governed, and operated permissioned blockchain to record SSA of space objects, and other critical data to enable international cooperation in the STM mission.

BESTA captures the catalog of SSA space objects position data, recorded from independent sensors, curated feeds (e.g. DoC, Russia, China), commercial, and academic sources, see Fig. 3. BESTA is also proposed to record SSA data such as intents to maneuver, as well as critical international governance shared agreements that support STM such as architecture, policy and regulation documents. Blockchain technology provides trust in SSA data and shared agreement documents by using cryptographically hashed documents, added to blockchain transactions which are signed by the originator (proof of origin), and cannot be counterfeited, changed, or destroyed (proof of integrity). BESTA is owned and operated by international stakeholders providing diversity of operating and geopolitical environments, ensuring that BESTA will continue to operate in the event of accidents or attacks. Blockchain technology enables use of increased automation (e.g. smart contracts) to process data as it is recorded as a transaction.

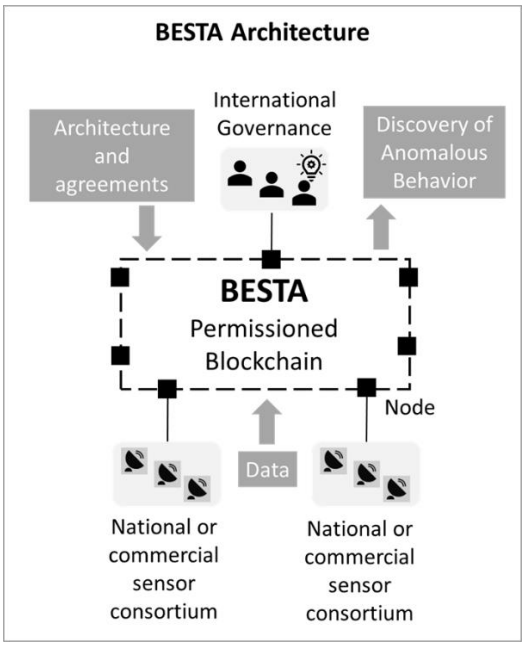

Fig 3. BESTA Architecture

BESTA assumes a technical and architectural context managed by the BESTA international governing body, to prioritize activities to develop and operate the blockchain, record SSA data, and record shared agreements including smart contracts (e.g. support conjunction alerts). Once agreements are reached, the document hashes and shared agreements are recorded in the blockchain, and the files stored in appropriate repositories. The corpus of recorded agreements informs the larger architecture and cycles of innovation. BESTA concepts are an extension of ongoing MITRE research SNARE (Sensor Network Autonomous Resilient Extensible) which uses permissioned blockchain to record orbital element sets from space sensors, discussed next.

SNARE

Sensor Network Autonomous Resilient Extensible (SNARE) is a MITRE architectural and operational concept (in prototype) that uses permissioned blockchain for a space-based sensor network which is sensor agnostic, extensible, and enables the use of traditional and non-traditional sensor data to achieve greater observational capacity and information gain. SNARE enables a new collection approach which provides a candidate replacement for the legacy centralized daily collection regimen (SP TASKER) with a new regimen that continually collects data from sensors. Each sensor schedules its own collection, coordinating with other sensors by recording collects on a shared blockchain network. Blockchain technology provides resiliency to attack and accident for tamper-evident and highly available records. The sensors and CSpOC exchange information, including collects and priorities, on the blockchain network. Scheduling observations on SSN for the legacy RSO space catalog, is a resource-constrained daily whole-of-SSN optimization problem. Bound by observation and revisit requirements, known scheduling violations can be minimized under the resource constraint using a selective decision process. The initial SNARE approach is to move away from a daily whole-of-SSN optimization problem, and toward a continuously updated relative economic value prioritization problem for each RSO and sensor pair. The economic value for SNARE is the value of the importance of the collect based on priority, last revisit time, how many successful tracks in the last 24 hours, and present ability to collect, but not the monetary value of the RSO. The economic value prioritization can include additional factors over time, though this paper constrains discussion to this initial approach.

The economic value of collection for each RSO then drives sensor tasks over time. This decision process utilizes properties of individual RSOs within a catalog, combined with properties of the global system such as sensor work-load distribution and sensor-RSO visibility. Each sensor-RSO pair receives a relative economic value of collect which can be easily compared against other sensor-RSO pairings and priorities to determine and execute an economically driven collection scheme for each sensor. This paper provides the mathematical basis for the SNARE collection regimen.

SNARE is also an architectural concept which integrates sensors into a decentralized, agnostic, sensor network which enables the use of additional trusted and non-trusted, non-SSN sensor data to achieve greater observational capacity and information gain. Sensors, including non-traditional, plug into the SNARE architecture via SNARE blockchain nodes, with the intention of enabling autonomous self-directed observational collection behavior.

SNARE seeks to maximize information gain and achieve emergent tip-and-cue behavior to achieve persistence and discovery of RSOs, while minimizing resource loading to the individual sensors. SNARE provides near real time change detection and sensor follow up for confirmation of events. Data replication and consensus algorithms in the SNARE blockchain provides resiliency which ensures the data flowing through the system is valid, and that all SNARE nodes use the same information for local economic prioritization. The data replication function of blockchain enables immediate recovery of a node and provides a functional equivalent of highly redundant continuity of operations (COOP) for SNARE nodes.

SNARE is envisioned to enable sensors and their SNARE nodes to independently collect positional data, cooperatively share positional data with each other, behaving in an emergent manner, providing greater information gain than a centrally directed network of sensors. The SNARE network provides resiliency through blockchain data replication and redundant, decentralized computing. The emergent collection behavior, paired with resilient computing and resilient data, contributes to improving mission outcomes, such as improved space object custody.

VI. BESTA Data

BESTA provides increased confidence in the data written and read by international stakeholders including space position data, intent to maneuver, smart contracts, shared agreements, and more, see Fig. 4. Each data transaction is cryptographically attributed to the sender and recorded as a tamper-evident transaction on the BESTA blockchain. Attribution combined with data integrity creates an internationally trusted set of data [7].

Space object position data is recorded from independent sensors, as well as curated data from sensor consortiums operated by nations, commercial, and academic interests. Space object position data is used by international governance, nations, commercial, academic, and independent interests, for building their space situational awareness. Attribution is transparent and enables stakeholders to build their situational awareness according to their data quality and provenance criteria. Transparency also enables national operators to alert sensors and sensor consortiums if their data appears to be missing or in error. Space object intent to move is also shared, enabling advanced planning by stakeholders to conduct their own subsequent defensive maneuvers.

Smart contracts are modules of code, deployed to each blockchain node, which execute on behalf of select transactions. Smart contracts enable portions of a mission business process to be executed and can be complemented with off-chain mission processes.

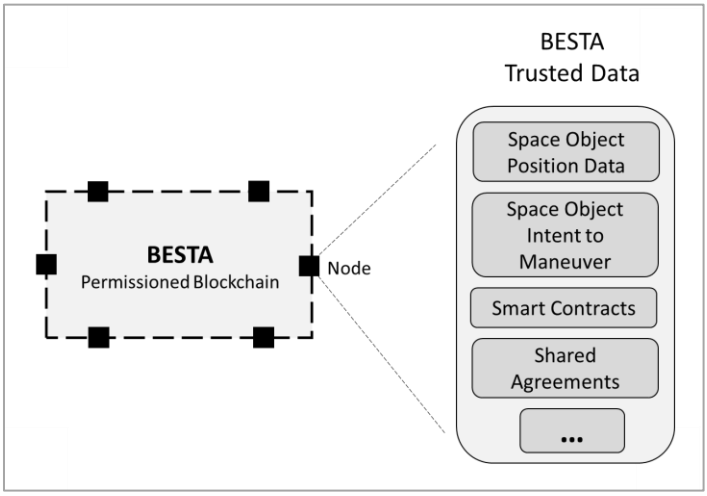

Fig. 4 BESTA Trusted Data

Shared agreements between stakeholders are implemented as versions of documents, enforced by operations and governance. Documents can be a variety of formats and stored in repositories as appropriate. A cryptographic link to the document can be established by storing a hash of the document in a blockchain transaction, which can be subsequently used when needed to verify the authenticity of the document. The corpus of recorded shared agreements informs the mission architecture and cycles of innovation.

VII. BESTA Governance

Development, operation, and sustainment of BESTA as part of international SSA and STM requires an international governance body to enforce the agreed direction and tempo. The decisions of the governing body should be informed by an architecture that enables technical interoperability of all technology required for international space cooperation, including but not limited to BESTA, see Fig. 5. The goal of governance and BESTA is to build a layer of trusted and transparent data which informs SSA and ultimately improves the performance of STM. All data recorded in BESTA can be seen by any stakeholder and verified as authentic, which enhances international trust in the data in the blockchain.

MITRE is proposing International Space Reference Architecture (ISRA) [8] as a starting point for such an architecture (separate paper). Intent of ISRA is to support international common terms, approaches, and interoperability. Each spacefaring nation can contribute and cooperate in this architecture, which also drives the development and operation of BESTA.

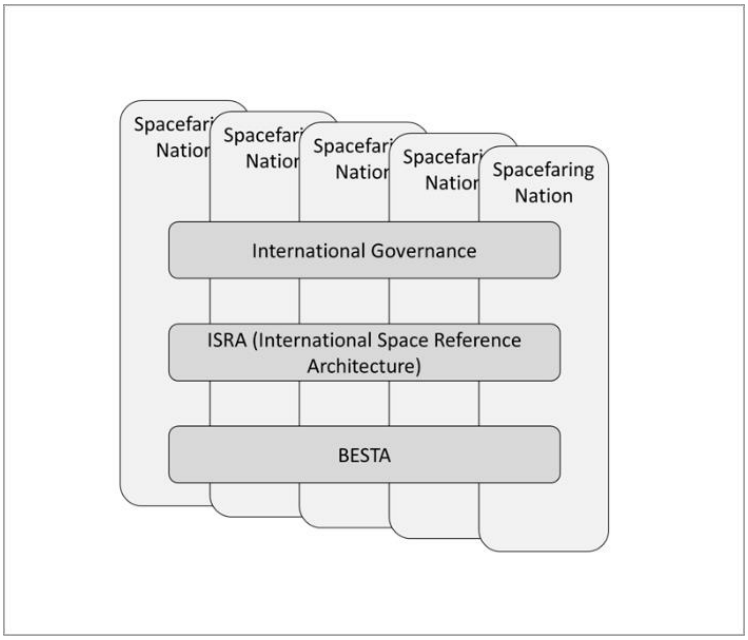

Fig. 5 BESTA Governance

ISRA is an open architecture that serves as a foundation for generating shared agreements which support and enable space flight safety, SSA, STM, and other related space activities. ISRA is an internationally governed and interdisciplinary concept that sets the foundation for standards and conventions that multilaterally span technical, engineering, operational, and policy domains.

ISRA intends to solve unique challenges of an international space mission, supporting decentralized stakeholder relationships. The theme is to forge international agreements on language, policy, and technical points as needed, generate shared agreements and record them as hashed versions in BESTA and full versions in file repositories. Open decentralized file repositories assure everyone has equal access to the shared agreements as needed, with ability to verify authenticity in BESTA by comparing hashes to pertinent blockchain transactions. In addition to formal shared agreements – best practices, behavioral norms, and TTPs (Tactics, Techniques, and Procedures) can be recorded in BESTA as well.

The result is a foundation on which rules of engagement can be generated, persisted, and used to enable safe international space travel in an era of rapidly increased use of space. Rules of engagement can include operational aspects such as proximity definitions, and governance such as transparency, accountability, and forensic approaches. Further, governance must listen to international community feedback and prioritize development needs, which drives iterative improvement of BESTA and ISRA as continuous cycles of innovation. Feedback can also drive risk analysis which further informs governance.

VIII. BESTA Operations

BESTA operation creates two flows of internationally trusted data: (1) Reconciled SSA, and; (2) Reconciled agreements, both of which inform and enable STM automation, see Fig. 6.

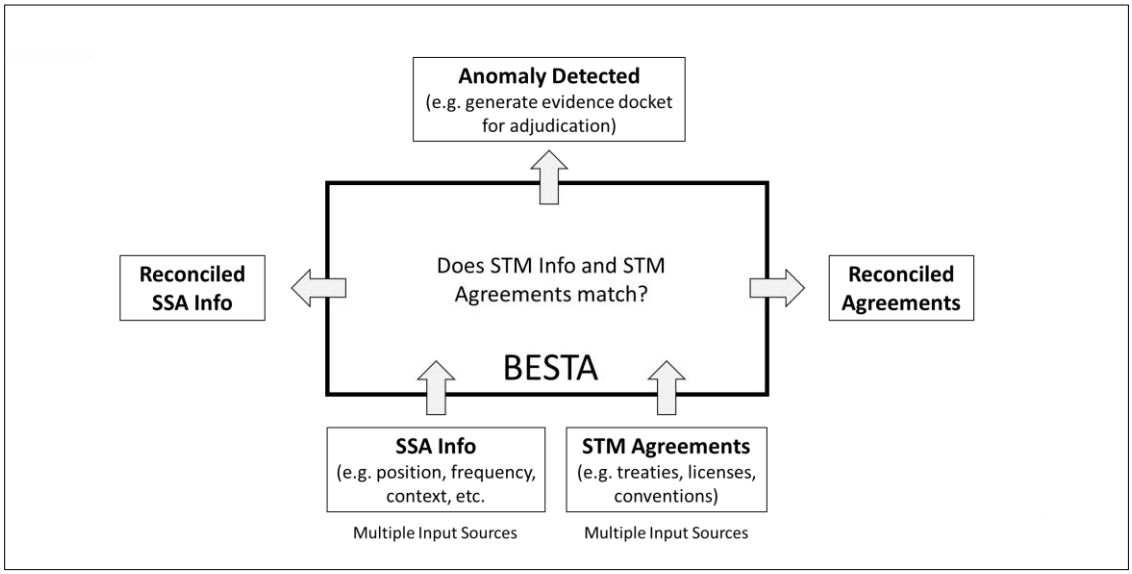

Fig. 6 BESTA Operational Data

Reconciled SSA consists of cumulative sensor data published as catalogs, intents to maneuver, and other data recorded as blockchain transactions submitted, validated, and recorded in BESTA. Space object position data is recorded from independently reporting sensors, as well as curated data from sensor consortiums operated by nations, commercial, and academic interests. Reconciled SSA can be copied from BESTA, into national and international data lakes and space operations centers and build their situational awareness according to their data quality criteria. Provenence of original SSA and reconciled SSA can be captured in blockchain transactions to assure data integrity.
International alignment to reconciled SSA benefits STM in two ways: (a) Stakeholders over time build a similar understanding of SSA, and; (b) Stakeholders are incentivized to continuously innovate to assure that input sources improve, and the reconciled SSA drives global space safety.

Reconciled Agreements consists of cumulative versions of agreed documents between stakeholders. Documents can be a variety of formats and a cryptographic link to the document can be established by storing a hash of the document in a blockchain transaction. The hash can be subsequently used when needed to verify the authenticity of the document. Reconciled agreements help establish norms of behaviour and rules of engagement within ISRA. Reconciled SSA informs STM (e.g. conjunction alerts). Other domains can interface and integrate with BESTA, such as national air space controllers who are responsible for relevant air space to support launches. The cryptographically secure historical record within BESTA can support forensic investigations after incidents to improve practices and evolve shared agreement documents.

IX. BESTA Internals

BESTA internal architecture is modular, enabling continuous evolution and improvement. There are seven types of modules, where each type has a generic function, with potentially multiple concrete instances of modules, one for each data type. For example, SSA Ingest Provenance module type can have concrete instances for TLEs, frequency assignments, etc. The instance of type of module then uses actual data at runtime.

Types of modules include (a) SSA Ingest Provenance; (b) SSA Information Sharing; (c) Agreements Ingest Provenance; (d) Agreement Information Sharing; (e) SSA and Agreement Comparison; (f) Anomaly Evidence Preparation; (g) Anomaly Adjudication, illustrated below.

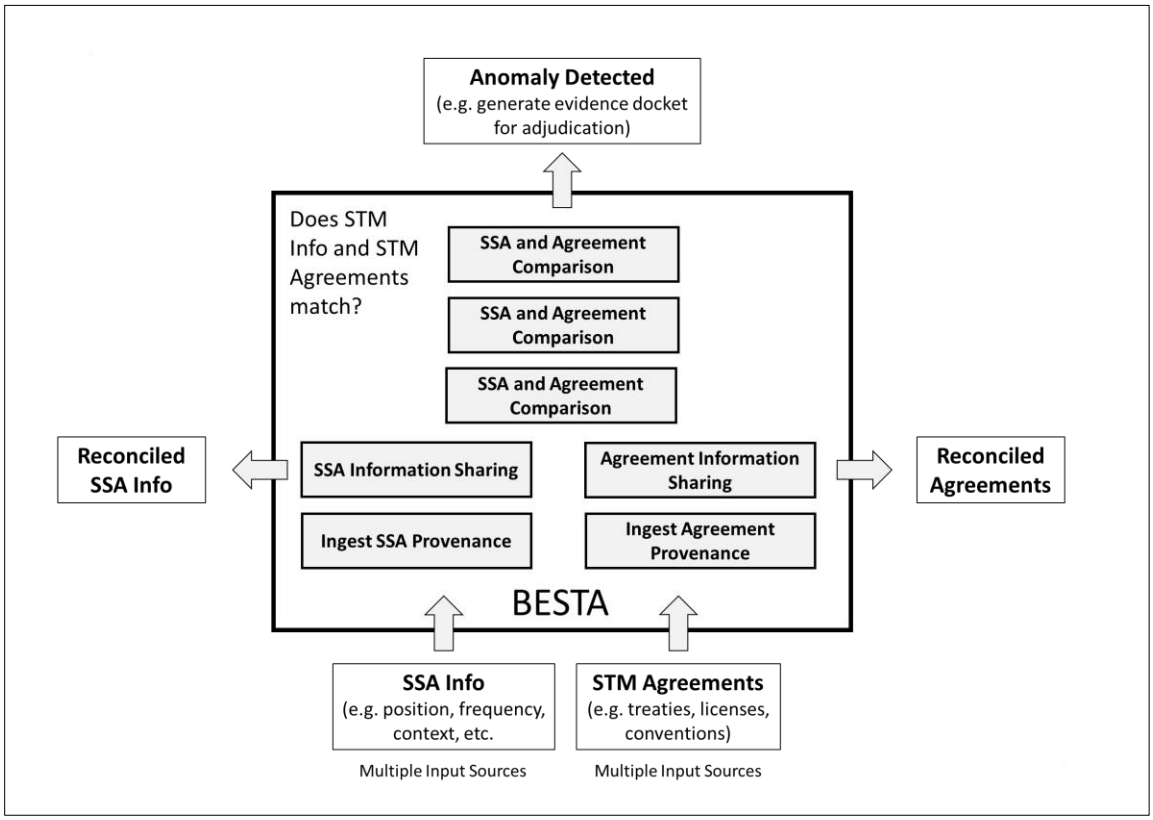

Fig. 7 BESTA Internals

The volume, types, and complexity of space object data is steadily increasing, driven by increasing number space objects including from mega constellations, by increasing number of types of data beyond TLE such as intent to maneuver and health/status, by increasing number of sources of data from commercial and national sources, and by increased need for cross-domain information sharing and integration across space, air space, land, and maritime domains. The increase in number, types, and complexity of space object agreements is driven by a growing number of spacefaring and space interested nations who enter into agreements which describe increasingly complex ranges and constraints of operational behavior. Catalogs are one type of space data, and critically important for STM. There are multiple catalogs, generated from national and commercial sources. For example, U.S. government presently has one catalog (space-track.org, Dept of Defense) and plans to add a second catalog by 2023 (Dept. of Commerce). Further, other countries have their own sensors and catalogs (e.g. Germany, Australia, Russia, China), and private commercial interests have their sensors and catalogs (e.g. SDA [AGI], LEO Labs).

BESTA (Blockchain Enabled Space Traffic Awareness) supports increased STM automation by comparing space object data to agreements in order to detect anomalies which represent potential non-conforming space object behavior. Will need new processes to generate a single reconciled source of space data for each type of data (e.g. inter-catalog reconciliation) and generate a single reconciled source of agreement for each data type (e.g. planned/agreed

orbit). Further, will be useful to add new data into existing catalogs (e.g. intra-catalog reconciliation). With reconciled sources of space data and agreements, comparisons can be automated. For example, a reconciled catalog can be compared against planned/agreed orbits to determine is the present orbit is non-conforming. A detected anomaly occurs when the agreed behavior differs from the observed behavior (e.g. orbit has unexpectedly changed). These anomalies, together with pertinent data and agreements are captured in evidence dockets using the blockchain for subsequent adjudication, either human in the loop, or automatic. Comparison of data and agreements requires provably correct provenance of both the space object observation and other data, and the applicable agreement documents, with the generated evidence docket also protected against tampering.

The SSA Ingest Provenance type of module reads from national and commercial sources of information (e.g. space-track.org, ITU data), and records receipt and provenance of data in blockchain for data integrity, availability, and resilience. After ingesting, SSA data is passed to SSA Information Sharing type of module where the input streams are reconciled for sharing with all stakeholders. The Agreements Ingest Provenance type of module reads from international, national and commercial sources of agreements (e.g. treaties, ITU), and records receipt and provenance of data in blockchain for data integrity, availability, and resilience. After ingesting, Agreements are passed to the Agreement Information Sharing type of module where the input streams are reconciled for sharing with all stakeholders. The SSA and Agreement Comparison type of module compares the reconciled SSA with the reconciled agreements to automatically detect anomalies. The detected anomalies are passed to the Anomaly Evidence Preparation type of module to capture the current state of reconciled SSA input, reconciled agreement input, and current context in a blockchain transaction for subsequent adjudication by the Anomaly Adjudication type of module.

Trust requires transparency and requires known data and known code algorithms for each step. Each of the ingest provenance, sharing, comparison, evidence, and adjudication types of code modules need to implement stakeholder agreed algorithms and open source code review for each function. Further, the module instance code provenance also needs to be recorded on the blockchain to prevent code hacking from producing erroneous results. The blockchain resilience guards against both attack and accident.

X. STM Information Sharing Stack

BESTA is intended to consume STM national feeds and STM agreements as described above. The STM feeds notionally form an information sharing stack as illustrated in Fig. 7 below. The U.S. STM feed will be provided by the Office of Space Commerce in Dept. of Commerce, as recently reaffirmed by the National Academy of Public Administration (NAPA) in August 2020. The U.S. STM feed is created by the OADR (Open Architecture Data Repository) as directed in Space Policy Directive – 3 (SPD-3). OADR will create the national feed from national sensor feeds, augmented with commercial sensor feeds. SNARE (or presently SP TASKER in CSpOC) collects observations with national sensors. The distinction is that SP TASKER is a roughly daily cycle of collection, where SNARE is intended to decentralize the collection of observations from the SSN national sensors, yielding close to continuous collection.

The combination of SNARE, OADR, and BESTA forms an STM information sharing stack, where observations are fed up the stack. In any national sensor scenario, there are a fixed number of dedicated sensors, and depending on sensor location, each sensor observes distinct parts of orbits. As described above, the OADR can read the national sensor observations, then request additional commercial observations to augment the observations from the national sensors.

Since the needs for augmenting the national feeds can be specified (the under-observed portions of orbits), the requests for commercial observations can be specific and avoid duplication with already observed parts of orbits. Further, prioritization can be applied to seek augmentation starting with high priority objects. Since SNARE is anticipated to be a continuous and automated collection, the augmented feed in OADR should also be automated. Blockchain could be used to manage the auction bid-offer process to automatically select the commercial entity to use for a particular observation, as well as record receipt of the observation, and delivery of payment. Selection could be based on a combination of factors including price, reliability, and past performance.

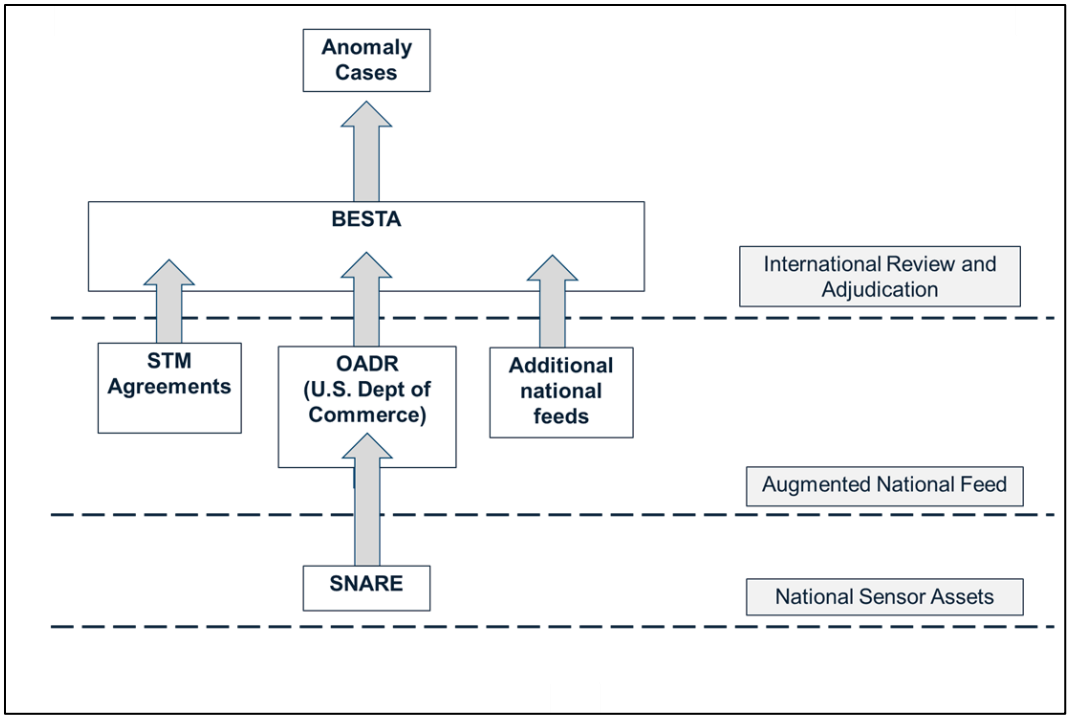

Fig. 8 STM Information Sharing Stack

Each are candidates for using blockchain:

1. SNARE – decentralize SSN observations, collecting on a continuous basis
2. OADR – disintermediate a highly automated commercial observation auction process
3. BESTA – automated detection of anomalies, coupled with evidence handling for adjudication

These are independent opportunities for using blockchain, with no overlap, and no possibilities for using the same blockchain for more than one purpose. The reason for exclusive blockchain use is that each blockchain used in SNARE, OADR, or BESTA:

- Operates on a distinct network
- Has distinct and non-overlapping stakeholders
- Is funded from distinct appropriations
- Has a distinct purpose

XI. BESTA Research Topics

Identification and enumeration of BESTA research topics is in progress and will inform modules such as anomaly discovery in the SSA and Agreement Comparison module, and evidence capture and secure storage in the Anomaly Evidence Preparation module. Discovery research includes automatic ingest of agreements, policies, and regulations into machine readable ontologies for later comparison to behavior observation data streams. Evidence capture and secure storage research includes automatic preparation of evidence packages which contain relevant agreements and observations, to be used in subsequent adjudication and mitigation activities. Results of discovery and evidence preparation must be trusted across all stakeholders even in contested or adversarial environments (e.g. space and great power competition). Further, BESTA must be brownfield, that is able to be used in current context (agreements, data) with minimal disruption.

XII. Discussion

Presently, Starlink is launching hundreds of broadband satellites [9] with a goal to launch thousands. Amazon is planning its own constellation with over three thousand satellites [10]. And the race for commercializing and exploring

space is just beginning. The international space mission is too complex for any single owner of SSA data, and BESTA is proposed to support decentralizing the space mission. BESTA and decentralization is intended to enhance information sharing by creating a highly available, secure, trusted data layer of SSA and agreement data which every nation and every person on the globe can access and use to make space safer, even while more congested.

XIII. Conclusion

BESTA is a decentralized, open source, internationally funded, built, governed, and operated catalog of SSA space objects position data, recorded from independent sensors, curated feeds (e.g. U.S., Russia, China), commercial, and academic sources. BESTA provides data for international stakeholders including space position data, smart contracts, shared agreements, and more. Data is cryptographically attributed to the sender and recorded as a transaction in the BESTA blockchain. In addition, BESTA blockchain cryptographically prevents tampering and node redundancy prevents loss of data. Attribution combined with data integrity creates an internationally trusted set of data. Development, operation, and sustainment of BESTA requires an international governance body to enforce the agreed direction and tempo. The decisions of the governing body should be informed by an architecture such as ISRA, that enables technical interoperability of all technology required for international space cooperation, including but not limited to BESTA. BESTA operation creates two flows of internationally trusted data: space situational awareness and documented shared agreements, both of which inform and enable STM.

XIV. References

[1] USSTRATCOM, "SPACE-TRACK.org," Joint Force Space Component Commander/J3, [Online]. Available: https://www.space-track.org. [Accessed 17 08 2019].

[2] U. W. House, "Space Policy Directive-3, National Space Traffic Management Policy," U.S. Government, 18 06 2018. [Online]. Available: https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/ . [Accessed 17 08 2019].

[3] A. S. I. A. a. S. (ASIAS), "ASIAS Welcome," ASIAS, [Online]. Available: https://portal.asias.aero/web/guest/overview. [Accessed 17 08 2019].

[4] U. S. S. C. P. Affairs, "USSTRATCOM expands SSA data on Space-Track.org," USSTRATCOM, 05 10 2018. [Online]. Available: https://www.stratcom.mil/Media/News/News-Article-View/Article/1655735/usstratcom-expands-ssa-data-on-space-trackorg/. [Accessed 17 08 2019].

[5] D. Bryson, D. Penny, D. Goldenberg and G. Serrao, "Blockchain Technology for Government (report, PDF)," The MITRE Corporation, 04 2018. [Online]. Available: https://www.mitre.org/publications/technical-papers/blockchain-technology-for-government. [Accessed 17 08 2019].

[6] Bitcoin.org, "Bitcoin is an innovative payment network and a new kind of money.," [Online]. Available: https://bitcoin.org. [Accessed 17 08 2019].

[7] M. Norman, Y. Karavas and H. Reed, "The Emergence of Trust and Value in Public Blockchain," in *IX International Conference on Complex Systems*, Cambridge, MA, 2018.

[8] N. Dailey and H. Reed, "International Space Reference Architecture (IAC-19-E3.4.10x50471)," in *70TH International Astronautical Congress*, Washington, D.C., 2019.

[9] D. Mosher, "Elon Musk just revealed new details about Starlink, a plan to surround Earth with 12,000 high-speed internet satellites. Here's how it might work.," Business Insider, 16 05 2019. [Online]. Available: https://www.businessinsider.com/spacex-starlink-satellite-internet-how-it-works-2019-5. [Accessed 17 08 2019].

[10] C. Henry, "Amazon lays out constellation service goals, deployment and deorbit plans to FCC," Space News, 08 07 2019. [Online]. Available: https://spacenews.com/amazon-lays-out-constellation-service-goals-deployment-and-deorbit-plans-to-fcc/ . [Accessed 17 08 2019].