GPR Journals
www.gprjournals.org

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

Blockchain for Aircraft Part Traceability in MRO (Maintenance, Repair, Overhaul)

Saketh Kumar Vishwakarma

Advanced Supplier Management-Manufacturing Agent, Bombardier, Kansas, USA.

Author's Email: sakethkumarvishwakarma@gmail.com

Article's History

Submitted:25th November 2025
Revised:23rd December 2025
Published:25th December 2025

Abstract

Aim: The study aims to examine the application of blockchain technology as a secure, reliable, and tamper-resistant solution for lifecycle record management of aircraft parts within the aviation Maintenance, Repair, and Overhaul (MRO) sector.

Methods: The study adopts a design-oriented and case-based approach to evaluate the integration of blockchain technology with existing MRO systems. A permissioned blockchain architecture is proposed, leveraging smart contracts for automated compliance verification and maintenance scheduling. Real-time aircraft telemetry is ingested using Apache Kafka and processed through Apache Spark to validate and enrich data before being recorded on the blockchain. A proof of concept and case study are used to assess system performance, auditability, and integration challenges with enterprise resource planning (ERP) systems.

Results: The findings demonstrate that blockchain implementation significantly improves auditability, data accuracy, and time efficiency in aircraft parts traceability among original equipment manufacturers (OEMs), MRO providers, and aviation authorities. The proof of concept highlights reduced risks of record tampering, improved regulatory compliance, and enhanced transparency across the aircraft parts lifecycle. However, challenges related to system integration, implementation costs, scalability, and market adoption barriers are also identified.

Conclusion: The study concludes that blockchain technology has strong potential to reshape trust, transparency, and productivity in aircraft parts record-keeping within the MRO environment. By providing a secure digital footprint for serialized parts, blockchain serves as a foundational technology for advancing the digital transformation of the aviation MRO ecosystem.

Recommendations: The study recommends adopting a phased, three-stage blockchain implementation strategy supported by regulatory alignment and cross-stakeholder collaboration among OEMs, MRO organizations, and aviation authorities. Future efforts should focus on cost optimization, ERP integration frameworks, scalability testing, and industry-wide standards to enable sustainable and widespread adoption of blockchain-based MRO solutions.

Keywords: *Blockchain, traceability, aviation, smart contracts, digital ledger, regulatory compliance*

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

1. INTRODUCTION

1.1. Traceability as a Strategic Imperative in MRO

In the aviation industry, MRO plays a vital role in aircraft maintenance, repairs, and upkeep for it to be airworthy for duty and meet operational requirements. It also ensures that the aircraft fully complies with the set regulations for its operation in the industry. The traceability of the aircraft parts is central to MRO, and it has been a particularly troublesome domain in terms of fragmentation, incorrect documentation, and general opaqueness. Due to their life cycle of journeying through OEMs, suppliers, logistics providers, repair stations, and airlines, a documented chain of custody is a logical necessity and a contractual and legal requirement. Lack of detailed part descriptions can lead to inherent safety hazards, fines, and unserviceability of aircraft. Therefore, traceability is no longer just an element of quality control but is now a value driver in MRO ecosystems. The aviation industry worldwide follows rules and regulations laid by organizations like the FAA, EASA, and ICAO, making it imperative to authenticate the history of every component, including its origin, status, and certification. However, even in this regard, the industry continues to maintain siloed databases, manual record-keeping, and paper-based systems. It generates data gaps, adds extra audit overheads, and makes operators vulnerable to fake or unrecognized parts entering the supply chain. These are not just bureaucratic concerns but directly affect flight operational safety and standards, especially when there is increased international use of aircraft.

Through automation, ERP integration, and digital record management, digital transformation in the aviation sector has started solving these challenges. However, most current systems also lack the means to provide end-to-end, fully auditable, verifiable records throughout interactions with other organizations. Compared to traditional databases, conventional digitized databases do not incorporate solutions for transforms for secure logging, decentralized. In a multi-stakeholder system like aerospace MRO, the actors may be based in various jurisdictions, and the sector's technological advancement may not be uniform across the board. These are some quasi-relational problems that reduce the possibility of transparent collaboration. This is where blockchain can help solve these long-standing traceability problems, since it provides for a distributed system that is very difficult to alter once created. By providing a decentralised and encrypted history of an aircraft part from manufacturing, installation, servicing, to dismantling, blockchain fosters accountability, traceability, and reliability within the MRO supply chain. With technologies like Apache Kafka for real-time data ingestion and Apache Spark for analytics, blockchain can automatically be more than a ledger but an intelligence agent. Maintenance events, inspections, or even compliance checks are also possible, which can be logged in real time and instantly validated by smart contracts, which can be made available to the concerned stakeholders worldwide with ease.

Furthermore, the change in the aviation industry transitions the infrastructure technology. Traditional large applications are becoming increasingly split into small components called microservices and event-based systems. This shift offers the possibility to build blockchain functionality into the core of these next-generation systems rather than as an add-on or final solution. By leveraging these tech models through well-defined APIs, cloud-native deployments, and tie-ins with compliance engines, the vision of traceability becomes possible to implement and enforceable at scale. In this regard, the transcendental importance of traceability is not limited to

GPR Journals
www.gprjournals.org
Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

protocol-based compliance. It becomes a cornerstone of operational reliability, supply chain quality, and equipment maintenance. Blockchain for Airlines, MRO providers, and OEMs is not a technology paper. It is a business solution that mitigates risk, cuts paperwork, and creates credibility. This paper investigates the structural and dynamic framework, practical directions, interconnection models, and business effects of blockchain-based peripherals' modernization for aircraft. It also examines subprocesses, including Kafka, Spark, and Artificial Intelligence, and the legal, ethical, and forward-looking perspectives. From this perspective, traceability is viewed not as an overhead but as an enabler of change in the aviation MRO environment.

2. BLOCKCHAIN TECHNOLOGY: FOUNDATIONS AND RELEVANCE TO MRO

Blockchain also encompasses the possibility of being an enabling technology for decentralized and transparent systems in numerous and sophisticated contexts. Blockchain solutions can provide new unalterable entries for recording part history within the MRO space and can be integrated in managing documentation across a company's boundaries. The fundamental characteristics of the blockchain, assessment of preferred platforms for the aviation industry, and how smart contracts work in managing compliance of aircraft parts (Ho *et al.,* 2021).

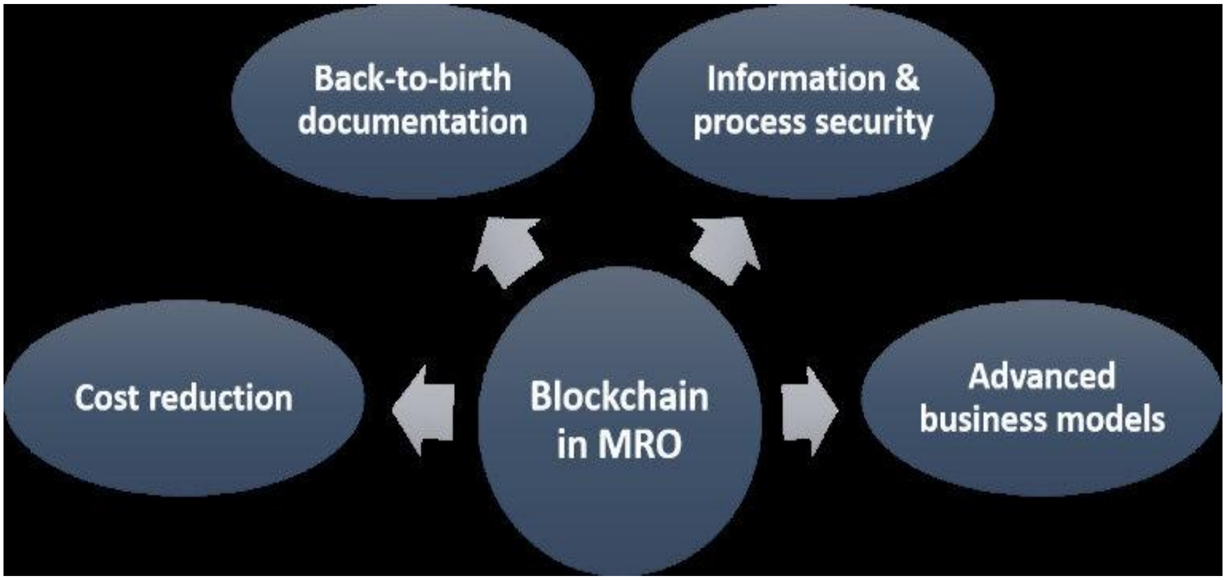

Figure 1: Blockchain in Aircraft MRO

2.1 Distributed Ledgers and Immutable Records

Blockchain is a distributed ledger technology (DLT) that helps multiple participants maintain a record of exchanges without intermediaries. They are electronically signed, and each one is stamped with date and time and linked to the previous transaction, making it tamper-proof. This immutability is especially important in aerospace MRO, as records of aircraft parts may be accessed for auditing purposes and other life cycle certifications (Chavan, 2024). Maintaining change history, installation records, and part transfer information as a blockchain will ensure no party can change or fake information recorded in the system earlier. This level of tamper-resistance eliminates the possibility of counterfeiting and undocumented repair or use of other substandard components. In addition, consensus protocols also help to ensure that only valid transactions are entered into the ledger to build confidence between OEMs, MRO providers, and the aviation

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

industry. These features offer a platform for creating useful traceability systems that can guarantee aviation's necessary safety and compliance.

2.2 Public vs Permissioned Blockchain in Regulated Environments

Public blockchains such as Ethereum are comparatively open to the public. They are better for wide-utility implementations, hence unsuitable for aviation MRO industry requirements such as data privacy and regulatory compliance. However, permissioned blockchain platforms like Hyperledger Fabric and R3 Corda are designed to have specific functionalities required for regulatory compliance (Dhanagari, 2024). These provide maximal privacy, highly tunable access controls, and global scalability, benefiting the aerospace industry. The permissioned blockchain solution, Hyperledger Fabric, can implement modular consensus and smart contract logic or chaincode that ensures compliance with policies specific to part handling or certification. This also provides for data segregation so that only selected actors like OEMs, airlines, or regulators can access specific instances of the transactions. Although R3 Corda does not belong to the Blockchain type of DLT solutions, its operative principle involves shared ledgers between involved parties to exchange transaction info without compromising privacy. Both forms are interoperable with enterprise applications and IT systems, making them suitable for the gradual transformation of the current aviation architecture of a company.

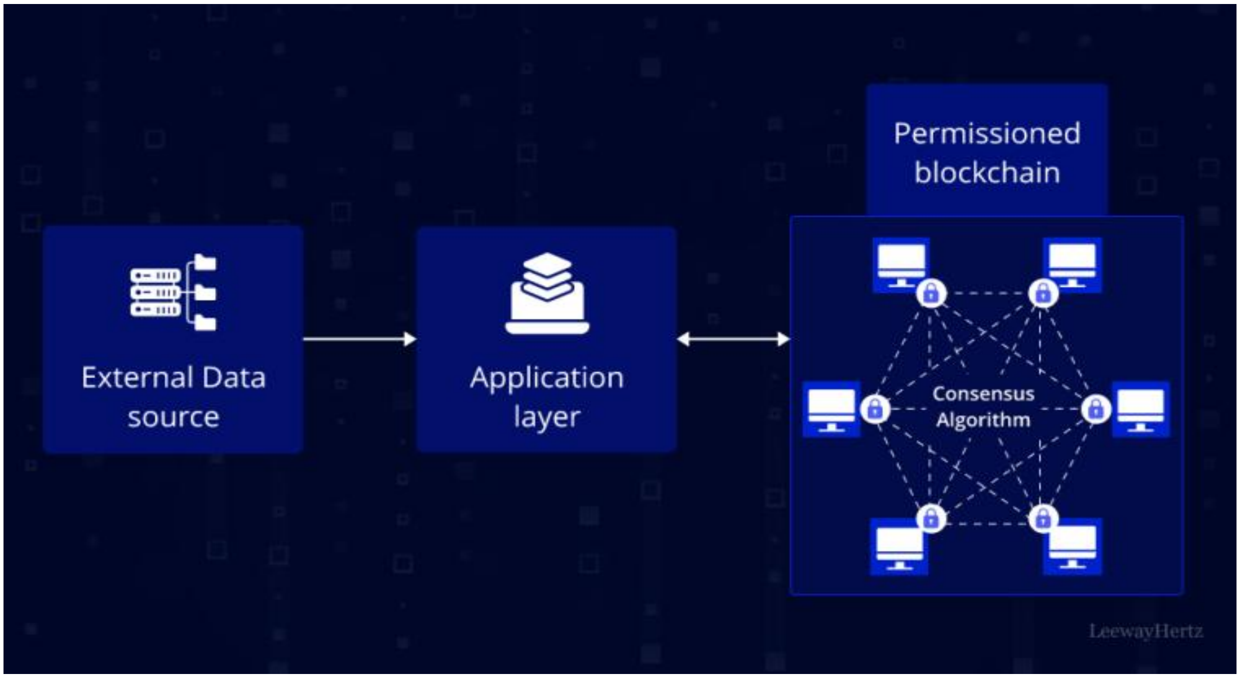

Figure 2: Creating a Permissioned Blockchain

2.3 Blockchain Interactions via Smart Contracts in MRO

Smart contracts refer to automated forms of contractual relations implemented on blockchain technology that automatically execute some operations upon the occurrence of certain conditions. In aerospace MRO, they provide an effective method to manage and audit compliance and enforce business rules with few interventions (Vieira *et al.,* 2016). For example, a smart contract may contain provisions regarding the warranty of an engine part that will deny warranty in case such

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

operations are recorded or if the limit of usage cycles is met. Likewise, custody transfer contracts can institutionalise rules for using part handoffs between suppliers, logistics service providers, and repair centres. Dispositions mention that asset transfer is only possible once a chain of custody requirement has been electronically confirmed. Maintenance parameters like compulsory inspection time or usage limits may also be included in smart contracts so that notifications or banning the usage of the object can be made, or work orders can be set. Smart contracts bring the rules into the Ledgers themselves, eliminating paperwork, mistakes, and variation in the procedure throughout the functional lifecycle of MRO.

The distributed nature of trust, the immutability of records within a chain, and the embedded automated process logic of the blockchain make it a very useful tool in providing traceability in the MRO industry. Properly chosen permissioned platforms and logical implementation of smart contracts will allow showing compliance in real-time, maintaining maintenance records, and proving the origins of the parts. Subsequently, the subsequent parts will describe how blockchain works with a high velocity data processing platform using Apache Kafka and Spark to ensure that batches of part characteristics and operational events are synchronised with the immutably stored part records on the blockchain.

3. INTEGRATING BLOCKCHAIN WITH REAL-TIME DATA STREAMS

For the identified applications of blockchain-based traceability in aviation MRO, a closed loop of real-time operational data must exist. Aviation continuously produces a high-speed data flow of telemetry data, sensor data, and maintenance events that need to be captured, processed, analyzed, and secured beyond editing in real time. Apache Kafka and Apache Spark work for real-time ingestions and analytics, and their structures blend into the blockchain system, a write-once-only immutable ledger.

3.1 Streaming Aircraft Part Data via Apache Kafka

Apache Kafka is a distributed event streaming platform for handling a high volume of event streams from aircraft systems and MRO processes in real-time (Chavan, 2021). Various data sources are integrated into the Kafka system in the context of maintaining aviation, including the engine sensors, avionics modules, the maintenance logs, and even tagged parts and repair shop interfaces. Such a point is emitted as an event, encoded in formats like Avro or Protobuf, and published to Kafka topics. Kafka is an asynchronous high-throughput messaging system that can decouple the producers and consumers of maintenance data so that messages, in this case, can flow through without any data loss during periods of heavy loads. Kafka Connect will enable airlines or their MRO providers to connect to third-party data sources like aircraft health monitoring systems (AHMS) and ground support tools for data integration to enterprise applications (Chang *et al.,* 2019). Kafka maintains the ordering of messages and supports replay to allow an exact replication of the sequence of events leading to the part's use, inspection, or failure.

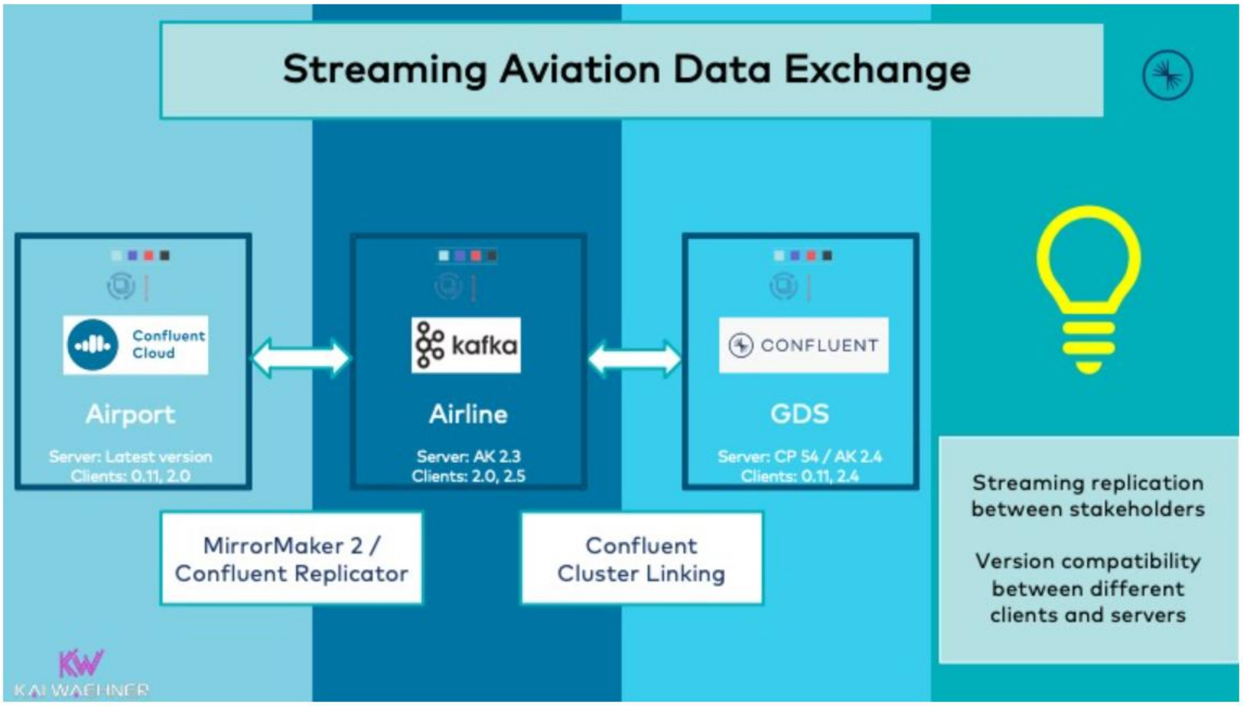

Figure 3: Apache Kafka in the Aircraft, Airline and Aerospace Industry

3.2 Real-Time Analytics and Validation Using Apache Spark

Apache Spark Streaming works hand in hand with Kafka as it processes and validates the ingested aircraft data in real time before it gets committed to blockchains (Du, 2018). When a Kafka stream is set, Spark jobs take these events as micro-batches or, through structured streaming filters, check that only clean and authenticated data is processed further. For instance, Spark can eliminate duplicate entries in maintenance logs, compare the data from sensors to the expected maintenance schedule, and ensure metadata validity before any entry is written into the blockchain. Additional validation in Spark may involve matching the part numbers with the past maintenance records, checking on the identity of the technicians, and checking on the formatting of data based on the type of part. These operations are needed because once a transaction happens in the blockchain, it cannot be undone. Thus, Spark is an intermediary that filters events and checks their validity before entering the blockchain. Moreover, based on the obtained data, using Spark MLlib, it is possible to apply machine learning models to identify anomaly levels or predict part degradation, thereby adding value-added information to the blockchain record (Krupa, 2023).

3.3 Harmonizing Data Velocity with Blockchain Immutability

Principal difficulties in Kafka+Spark+Blockchain implementations are increasing the write speed while maintaining blockchain immutability and ensuring compatibility with high-speed data pipelines. Public blockchains or distributed ledgers built on permissionless platforms, for example, Bitcoin or Ethereum, also have built-in latency commensurate with the consensus mechanism and extensive cryptographic computations (Gamage *et al.,* 2020). Writing to the ledger for each incoming event is undesirable for performance and consumes an unmanageable amount of storage. To overcome this, the following techniques include data summarization, event batching, and asynchronous ledger writing. For instance, Spark may be used to group similar events, for example, recurrent sensor readings, into easily consumable packets of information, like an hourly usage report or a breach of a threshold warning. These aggregated records are then written on the blockchain at certain specified intervals or when certain conditions are fulfilled, thus minimizing the number of transactions while keeping the records secure. Besides, Kafka and Spark pipelines can store a copy of records in the data lakes to create a blockchain for housing only the compliance-laden snapshots (Sardana, 2022).

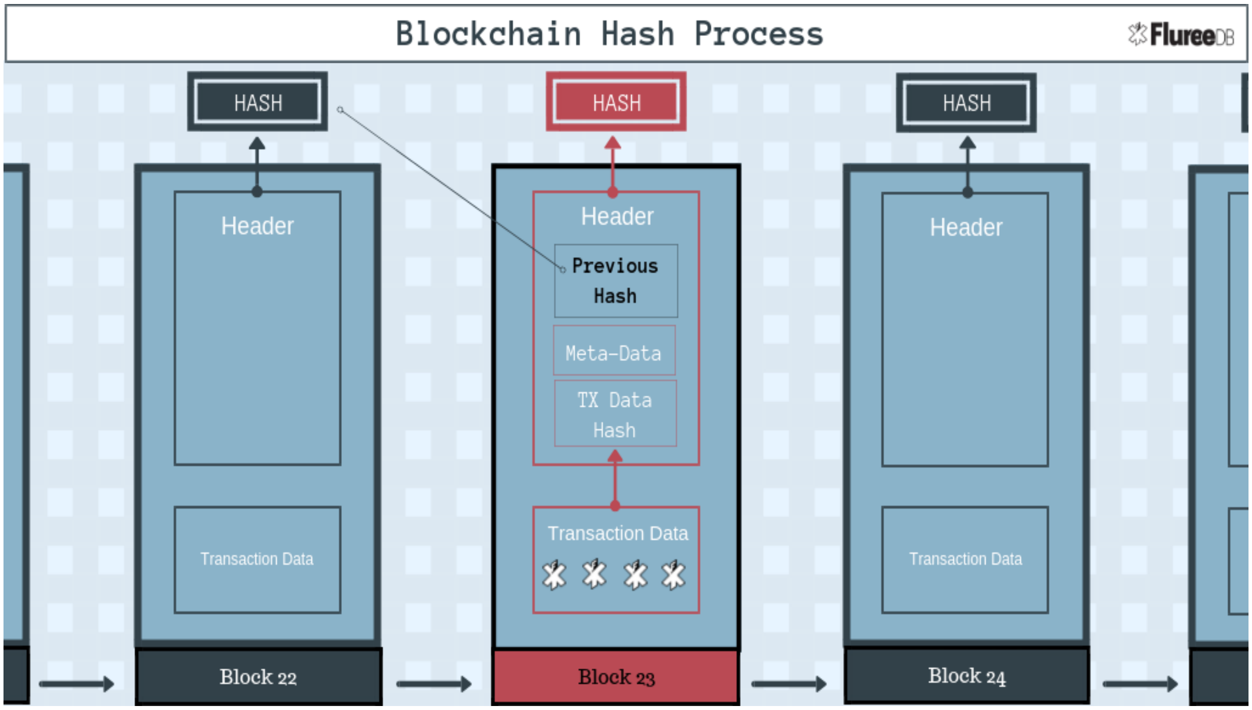

Figure 4: Why Does Blockchain Immutability Matter?

The ability to integrate Apache Kafka and Spark with blockchain to provide real-time and scalable traceability for the MRO frameworks makes this architecture complementary. Kafka facilitates the guaranteed data ingestion from multiple sources, while Spark validates and enriches the data before it submits it to the blockchain. Through the blockchain's high data velocity and well-defined immutability, this layered architecture allows the aviation industry actors to put into place effective but operationally agile and legally sound traceability solutions.

4. METHODOLOGY: ARCHITECTURE AND IMPLEMENTATION OF A BLOCKCHAIN-BASED MRO SYSTEM

Maintenance, Repair, and Overhaul (MRO) Traceability using blockchain can be technically effective if it adopts a structured approach in system scoping, modernization of its architecture, and intelligent exception management (Mohamed, 2021). This is a clear roadmap of how an efficient and effective blockchain-based MRO system can be created pragmatically regarding prioritized use cases, cryptographic data models, interfaces to connected monoliths, and AI leveraged self-auditing. It is therefore imperative to design a flexible, scalable, and secure security architecture to meet the needs of aviation regulation and operation.

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

4.1 Defining System Scope and Use Cases

In the initial stage, defining the boundaries to target the elements with the highest risk, value, or regulation is crucial. Some of the first areas to adopt blockchain will include avionics modules, jet engines, auxiliary power units (APUs), and life-limited parts. They require frequent service, have extensive airworthiness record documentation, are often sold or leased between operators, and are ideal for creating an immutable record of their history. It entails developing comprehensive use cases of each part, including OEM manufacturing and certification, installation, use, inspection, and aftermarket overhaul or sale. It aims to determine process points where one needs to provide evidence of compliance, mention the chain of custody, or use point-check automation. Each use case is then mapped to smart contract logic and data ingestion event from the existing aircraft system. For instance, a smart contract can execute under certain conditions, such as when an avionics module has not been updated on its software for a specified number of months or when the vibration level of an engine has surpassed the permitted limit. This is an ideal time for data modeling and new interface work to be planned and guided by these use cases.

4.2 Data Model Design and Cryptographic Identity of Parts

This requires that for each aircraft part identifier, a unique cryptographic ID has to be generated for accountability in case of tampering. This is often done by mapping part attributes like serial number, batch code, the manufacturer identification number, and the certification metadata into a unique digital signature imprinted on the blockchain. SHA-256 or BLAKE2 cryptographic hash function is used in practice to generate a repeatable and collision-free identifier for each part (Konneru, 2021). Besides hashes, the entries in the blockchain might include links to digital certificates, signed maintenance logs, and written-down sensor metadata, depending on which ledger model is used. It can be tied to smart contract states that will include information about the state of the part, for instance, Installed, In Service, Removed for Inspection, or Decommissioned. PKI adds a second layer of authenticity to the transactions, proving that OEMs, MRO shops, and regulators were part of the transaction. This makes it possible for every event in the lifecycle to be concrete, auditable, and linked back to a cryptographic ID to remove confusion or forgery of parts of documents across jurisdictions and organizations.

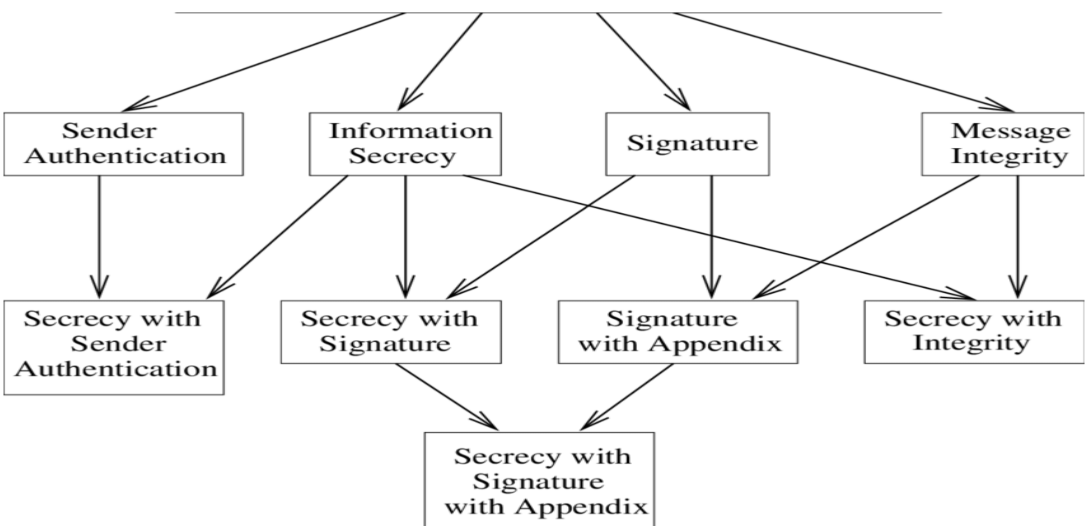

Figure 5: Cryptographic Design Patterns

www.gprjournals.org
Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

4.3 Retrofitting Monolithic MRO Systems with Microservices

Typical prior MRO systems are based on standalone modules with tightly coupled inventory functionalities, scheduling, and compliance functionalities (Choo, 2004). Unfortunately, all these systems do not have native support for the decentralized infrastructure. To prepare such monoliths for blockchain integration, the microservices-based architecture has to be employed, where all the functionality has to be exposed through APIs. Each of the microservices deals with a specific domain of the overall solution, for example, the serialization of a part, the submission of a maintenance log, or compliance verification. An API gateway is an additional layer between the monolith and the blockchain network, which provides a safe and asynchronous interface for interacting with the distributed ledgers. For instance, when a maintenance event is recorded in a legacy system, middleware services map it into blockchain using predefined templates and submit it through a smart contract. Microservices are also essential for identity management, querying the ledger history, and synchronizing the data between the on-ledger and off-ledger. This supports the concept of blockchain and the additional transition, size, and flexibility of the MRO system for AI integration, scalability, and regulation.

4.4 Leveraging Compliance-Driven AI for Exception Handling

After the architecture of a blockchain is established, artificial intelligence is used to identify possible nonconformities and set off the proper procedure. Compliance embedded AI consumes data from streaming systems such as Kafka, ledger events, by the appearance of departure of the Expected Part behaviours, or service gaps (Alam *et al.,* 2020). These computer-based models trained with maintenance history, failure modes, and operational limits help identify variance in real time (Karwa, 2024). For instance, where a hydraulic pump requires a check after every 500 flight hours, while the ledger shows that it has been 600 flight hours since the last check, an AI model can send a smart contract alert for the breach. Likewise, using predictive models, one can recognize the abovementioned regularities of unauthorized repairs, unregistered activity of technicians, or signs of part fatigue as shown by certain sensors. This, in turn, can lock the said smart contacts for further usage, alert regulatory systems, or trigger secondary audits. This AI layer perpetually checks for compliance and implements continuous monitoring to minimize manual inspection, which can only pick up safety concerns at a given time, throughout the lifecycle of the aircraft part.

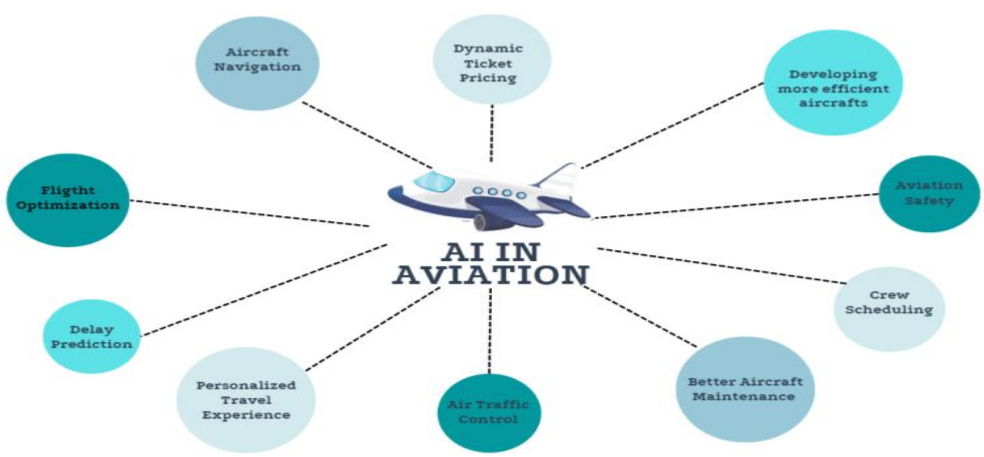

Figure 6: Uses of Artificial Intelligence in Aviation

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

The steps for a blockchain-based MRO system involve using cryptographic identity models, a solid software structure, and incorporating artificial intelligence in handling any exceptions in the handling of the parts (Perboli *et al.,* 2018). The key is considering the scope of high-impact areas and gradually introducing microservice architecture for MRO by refactoring the existing aviation infrastructure. Implementing the aforementioned architecture is already gaining attention and being prototyped, with the Aerospace and aviation industry leading the way on using blockchain for regulatory and various operational benefits.

5. BLOCKCHAIN DESIGN PATTERNS FOR TRACEABILITY IN AEROSPACE

Applying the concept of blockchain in aerospace Maintenance, Repair, and Overhaul (MRO) requires application architecture patterns that are strong and flexible simultaneously. The best practices that guarantee traceability, transparency, and compliance in large, complex, and multi-player environments are categorized below into design patterns. These patterns enhance data coherence, audibility, and the capabilities of the data storage system, as well as conform to domain requirements of custody tracking, event integrity, and data partitioning. This overview presents the three fundamental patterns of blockchain traceability application for aerospace, namely event sourcing, provenance chains, and CQRS (Ahmad *et al.,* 2021).

Table 1: Blockchain Design Patterns for Aerospace MRO Traceability

Pattern	Purpose	Key Features
Event Sourcing	Immutable maintenance history	Blockchain ledger, time-stamped events, smart contract automation
Provenance Chains	Custody and certification tracking	Digital part identity, smart contracts, tamper-proof hand-offs
CQRS Architecture	Efficient read/write separation	Kafka pipelines, blockchain for writes, data lakes for reads
Real-Time Triggers (Kafka)	Immediate event processing	IoT/Kafka integration, smart alerts, operational visibility
Compliance Anchoring	Multi-actor regulatory conformity	Cross-border validation, automated audits, and cryptographic proof of compliance

5.1 Event Sourcing and Replay for Maintenance Logs

In blockchain-based MRO systems, any user action must be recorded as an event that cannot be altered or deleted. Event sourcing is based on recording changes in part status, such as installation, inspection, or removal, and maintains historical data. These events are written into the blockchain and can be replayed to give an end-to-end history of a part, which is very useful during audits, warranty claims, and incidents. It provides end-to-end auditability and future-proof analytics pipeline architecture so that decision-making is reliably anchored on sequential data history (Kumar, 2019). It also provides excellent failure diagnosis, allows for debugging of previous maintenance activities through time-travel, and provides automation of compliance to deterministic event flows legally enforceable by smart contracts.

5.1.1 Immutable Event Ledger for Lifecycle Tracking

Every maintenance event is identified as a unique and timestamped block in a blockchain. For instance, when a technician has inspected the turbine blade, information that describes the blade is created in a digitized format. Technician identification number, time of inspection, the unique identification number from the aircraft, the specific number on the part, and the inspection result. This record is encrypted with a private key and put on the permissioned blockchain node. This will use event sourcing, where auditors and system agents can query and replay the actual use and the compliance of all the aspects of a part up to service intervals (Akuku, 2011). Analyzing root causes of component failures in different maintenance networks is essential to guarantee reliability. Blockchain technology can record specific events permanently, making it easy for the software to check for tampering and avoid central databases while providing legal proof. With the off-chain storage of significant artifacts, for example, PDF documents with inspection reports, this pattern provides a high enough resolution and data integrity while maintaining a high speed. Moreover, event versioning can also support schema evolution to aggregate systems and change without affecting historical coherency and compatibility. It helps with forensic investigations, eases the reconstruction process at the review level needed for audits, and creates replayable scenarios for app or component quality assurance and recertification.

5.1.2 Real-Time Event Triggers via Kafka Integration

For real-time reaction, the blockchain event sourcing is coupled with Apache Kafka to directly ingest operational events from aircraft systems, IoT sensors, or MRO databases. For example, a flight control unit producing high vibration data will raise a Kafka event, followed by Apache Spark validation of that data to check if certain limits are crossed, and the result is recorded in the blockchain. This action may also start a subsequent process, for example, scheduling an inspection on all the equipment or pulling down an aircraft. Re-posting events from Kafka topics gives users information on what happened, when, and how. As a topic-based architecture, Kafka enables a time-ordered stream of events to be processed asynchronously to various systems like analytics platforms, digital twins, and compliance systems (Nyati, 2018). Finally, Kafka's real-time streaming complements blockchain's immutability, always keeping event sourcing operationally up to date while capturing a complete history. It also allows integration with alerting tools, such as Prometheus or Grafana, and closes the loop between detection and action. Thus, it enables just-in-time interventions, improves analytical isolation of faults, and ensures that operational insight data is in sync with predictive maintenance with the aid of telemetry events.

www.gprjournals.org
Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

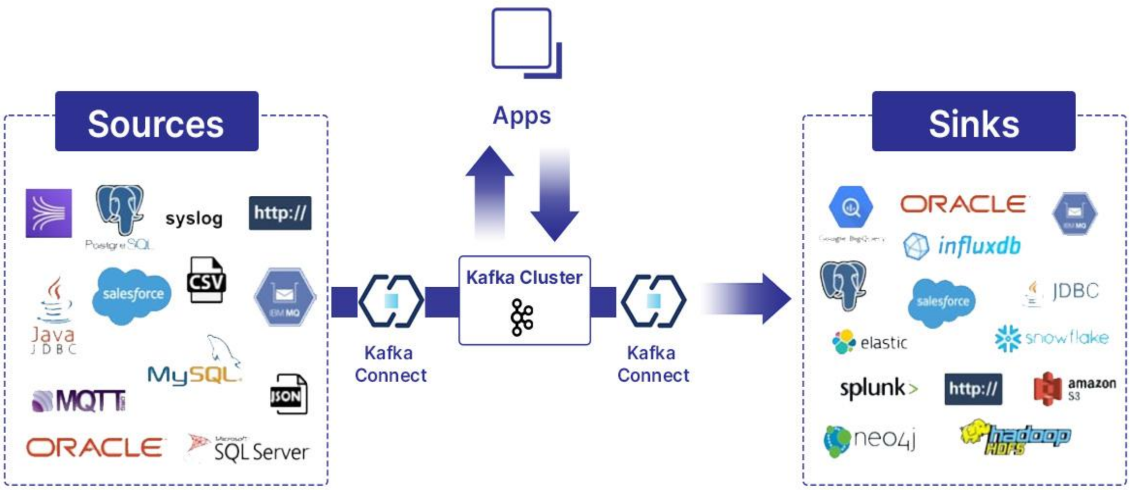

Figure 7: Advantages of Kafka in Real-Time Business Insights

5.2 Provenance and Custody Chain Patterns

A practical and trustworthy custody chain is imperative to keep counterfeits at bay and, more importantly, ensure that parts stay certified through different organizations. Provenance patterns are established through blockchain, and each transfer and certification of a part's entire lifecycle is recorded, creating trust between OEMs, repair stations, and airlines. These patterns comprise the digital logistics chains established in such transitions, where each transition is deeply encrypted and linked to an unalterable record, minimizing conflict and the need for verification (Goel *et al.,* 2024). This cuts down on reconciliation processing time for multinational transactions and offers jurisdictional neutrality, granting auditable consensus at every point of custody.

5.2.1 Cryptographic Part Hand-Off Protocols

This digital identity is created based on the object's serial number, batch code, and manufacturer-signed certificates, hashed into a unique number. When a part has changed custody, from an OEM to a logistics provider, the blockchain record digitally signed and timestamped transaction consists of two important parts (Palamara, 2016). These are custody data, like the chain-of-temperature records, or seal integrity data. Smart contracts ensure that a custody transfer can occur only when every condition precedent that accompanies the transition of the document has been met, including checks and regulatory documents. This protocol acts as a barrier to entry of fake or substandard components or products into supply chains. On one hand, through observer nodes, regulatory authorities can ensure that any custody trail of a part is valid and meets the jurisdiction's requirements. Adding tamper-proof IoT seals or RFID tags to this solution further ties the asset's chain of custody to the blockchain. It facilitates zero-trust supply chain systems in which any participant has no dependence on others to verify identity or status. It guarantees transactional integrity at each handoff point, addresses the threat of forged documentation, and provides near-real-time regulators' visibility of cross-border supply chain occurrences.

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

5.2.2 Compliance Anchoring Across Multi-Actor WorkflowsCustody chain validation is also broadened to multi-actor-based workflows, such as joint inspection or part transfer based on international logistics. Before a part is refurbished at an overseas repair shop, it is important to ensure that a blockchain captures the refurbishment data and any checks and certifications done after repair. Smart contracts also ensure that the technician's certification passes a verification check and conforms to the appropriate certification standards, and only pre-approved facilities sign off on the work critical to safety (Singh, 2022). After entering domestic operations, authorities can check the existence of the chain of custody without interaction with the foreign repair station. This pattern ensures compliance at both the organization and the jurisdiction level while trying to minimize the cost of reconciliation and rely less on manual verification. The ledger becomes a compliance anchor, whereby each transfer of physical custody is self-attested and can be proven perpetually in the event of a dispute. Accounting for changes in version-controlled schemas also prevents the degradation of the historical custody chain integrity due to other standards that may be developed. It does not require cross-border system access for auditability, automatically expires validity checks, and supports resolution of disputes using cryptographic proof.

5.3 Command Query Responsibility Segregation (CQRS)

Blockchain and Kafka systems assume a predominant right-side, mostly write-oriented, and a predominant pattern. However, traceability systems will require high ingestion, search, analytics, and reporting. The CQRS pattern logically partitions reads and writes into separate business systems, ensuring high efficiency, availability, and data integrity in aerospace-grade MRO platforms. This way, real-time ingestion and the analytic pipelines can run in parallel without interference for complex analytical queries or data remediation activity. It isolates ingestion from the mission-critical knowledge discovery processes, reduces locking contention in multiple-accessed tables, and ensures SLA compliance across different analytical operations (Kansara *et al.,* 2022).

5.3.1 Write-Optimized Blockchain and Kafka Pipelines

In the CQRS architecture, all inputs, that is, the messages from the sensors, logs from the inspections, or records from installments, are implemented through Kafka and recorded on the blockchain. These systems are highly suitable for capturing large volumes of data that are unlikely to change. However, they are inefficient with complex queries because their data model is first-order and occurs in sequences locked in consensus (Wang *et al.,* 2023). This way of isolating writes guarantees that no read operation can be slowed or prevented from executing while the logger device works. For instance, when an engine's maintenance cycle is complete, a serialized and signed log is created and then sent to Kafka, which pushes the log to a smart contract that checks the latter's format before archiving it to a blockchain. This approach allows for linear scalability in ingestion pipelines. It establishes unbroken traceability, even during increased operational activity, such as large-scale inspection campaigns or urgent repairs due to airworthiness directives. Kafka Streams and Flink can be used to create states for intermediate transformations, which are stored in a cache for downstream simplification of computation during writing processes (Raju, 2017). It minimizes write-contended operations, scales separately from analytics engines, and handles multi-tenant ingestion modes without a ledger synchronization pause.

GPR Journals
www.gprjournals.org
Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

5.3.2 Read-Optimized Data Lakes and Compliance Dashboards

For analytics and compliance purposes for traceability, blockchain and Kafka streams are copied to read-optimal data lakes/OLAP stores. Spark or Flink jobs transfer, transform, and load relevant blockchain events into relational or graph-based databases to conduct complex evaluation queries, such as finding all parts with manufacturing defects or components installed by a suspect technician. CQRS read models are highly normalized for performance and indexed by part ID, flight number, or certificate type. Those stores provide the basis for dashboards used for visualization, to identify anomalies, and to meet the requirements of regulations. This architectural layering also enhances the system's security as direct access to the blockchain layer is kept to the bare minimum to avoid write requests unless they have passed through validation. All write requests are validated before being ledgered. Meanwhile, the entire system supports analysis to all manner of degrees without necessarily risking the integrity of the ledger layer. Specific data formats, such as the Parquet format and indexing, also enhance the response of compliance queries and enable real-time analysis of part histories on the fly. It also allows the execution of multiple concurrent regulatory queries, which makes data lineage transparency easy to achieve, and offers real-time lineage context for anomaly detection frameworks (Singh, 2024).

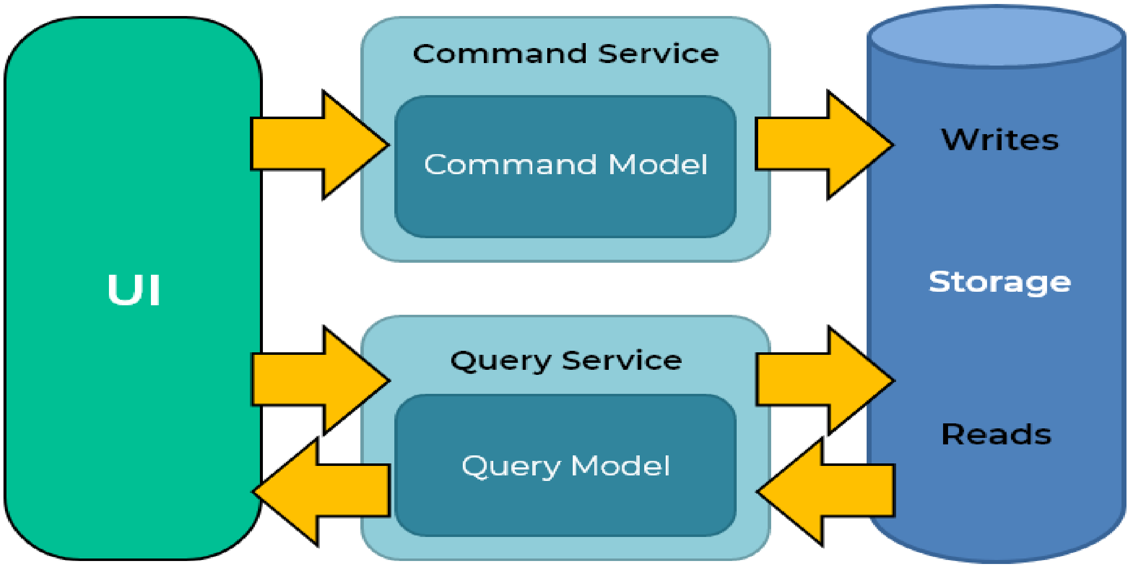

Figure 8: Command Query Responsibility Segregation (CQRS)

Event sourcing, custody chain tracking, and CQRS are generally implemented patterns within aerospace MRO for implementing a system's traceability. At a practical level, they outline how to guarantee the block's content's immunity to change, its parts' uniqueness, and the high availability and concurrency of processes across multiple actors. While these patterns establish the usability of blockchain for today's targets and obligations of operational and regulatory, they also set the stage for predictive maintenance and integration of artificial intelligence and cross-border traceability. In this evolving aerospace system, these established patterns provide a roadmap for safer, smarter, and trustworthy part lifecycle management. They must be implemented strictly, the stakeholders must be in harmony, and even the continually developing standards must be followed strictly in aviation engineering.

6. CASE STUDY: LUFTHANSA TECHNIK'S BLOCKCHAIN MRO PLATFORM

Lufthansa Technik, an overall aircraft service provider owned by Lufthansa Group, implemented blockchain in aircraft maintenance, repair, and overhaul (MRO) to improve aircraft part traceability, compliance, and real-time operational performance. This analyzes the strategic goals, technological application, and quantifiable advantages of Lufthansa Technik's blockchain for the MRO digital platform (Riechmann, 2020). Using this approach, the organization solved some of the most significant industry problems related to part legitimacy, paper-based records, and auditing issues, thus setting up the process for change that is sustainable in applicability for aviation maintenance systems.

6.1 Project Overview and Strategic Objectives

Lufthansa Technik started its blockchain MRO to centralize and digitalize information on aircraft component history. The project's key goals were to increase the accuracy and availability of such part traceability data, decrease paperwork and documentation for compliance, and increase real-time information sharing with suppliers, regulators, and internal engineering teams. Before blockchain implementation, parts of the history were sparsely distributed and documented either manually or in a semi-automated manner, resulting in time-consuming verifications and a high risk of data duplication and inconsistent formats of audits. Lufthansa Technik adopted the idea of having a permanent record of part lifecycle events to centralize information and keep track of maintenance actions such as inspections, removals, and installations (Pohya *et al.,* 2021). Another key component was the improvement of regulatory transparency through providing read access to authorized parties, including the national aviation authorities. It also aimed at enhancing the effectiveness of tracking inventories and reducing misplaced assets in the facility by employing IoT integration and the smart contract impact of asset identification.

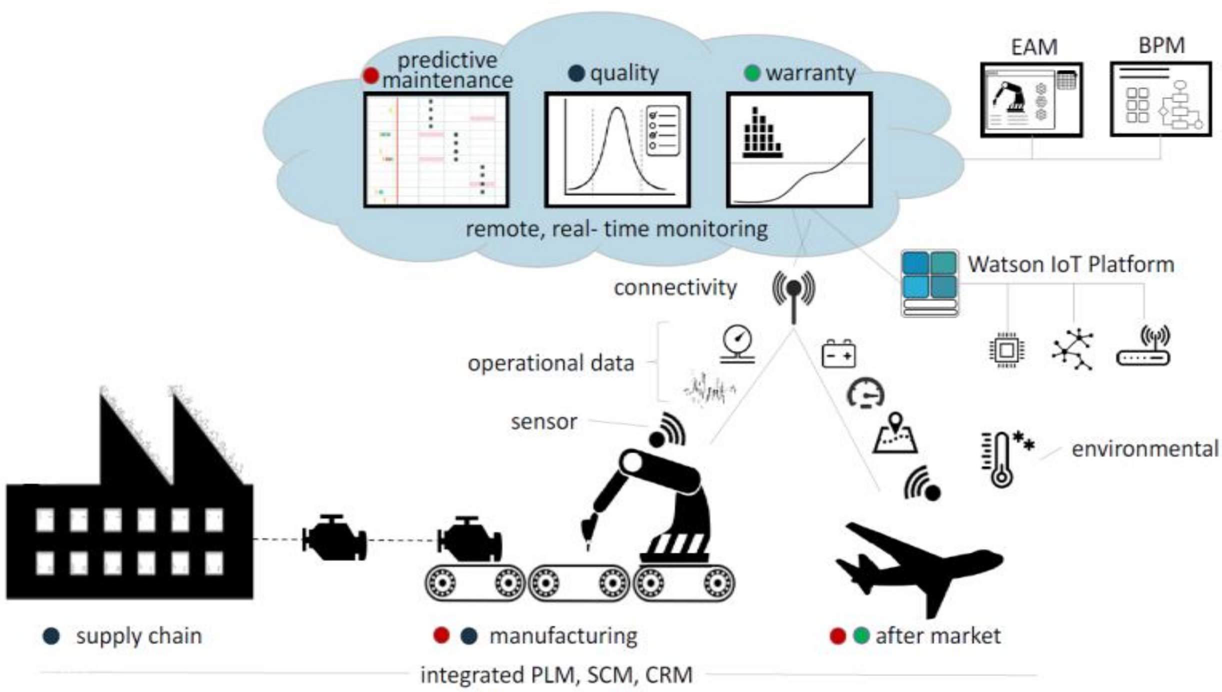

Figure 9: Blockchain in Aviation

GPR Journals
www.gprjournals.org
Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

6.2 Implementation Architecture: Kafka, Hyperledger, and Legacy ERP Integration

Lufthansa Technik's blockchain-based MRO platform architecture is based on Apache Kafka for messaging, Hyperledger Fabric for the blockchain framework, and an integration layer for the existing ERP system. Kafka is at the center of ingesting event streams from relevant operational sources like the maintenance terminals, IoT sensors, RFID readers, and digital inspection tools (Chonata, 2019). Kafka Connect directly communicates with aircraft systems and shop-floor applications, encoding Avro's structural data events to ensure standardization and examination. These events are fed into Apache Spark jobs, where the correctness of the data received is checked against the predefined schema, the signatures of the transactions are validated, and data integrity is confirmed before this data is introduced into the Hyperledger ledger. They used Hyperledger Fabric due to its permissioned design, chain code protocols, and the fact that it is easy to establish specific approvals for certain data blocks. Every part in an aircraft has an equivalent hashed value linked with particular smart contract states describing its lifecycle status. To integrate with the SAP-based ERP system of Lufthansa Technik, the Web APIs on different RESTful standards were used to connect blockchain data as its asset and compliance module. This bidirectional gateway allows applications created before this system to send maintenance events into the blockchain and receive formal histories back out for auditing purposes or other needs, without the end user ever being exposed to the blockchain interface.

6.3 Measured Results and ROI

Implementing the blockchain MRO platform yielded several operational and regulatory benefits in the Lufthansa Technik maintenance environment. Verification time also benefited from reducing about 50% through on-demand, cryptographically authenticated component histories. Maintenance technicians could therefore view all the records and details of the services through the work desk and organizational dashboards without going through various systems or referring to physical logs. Some subassemblies were lost or misplaced in the past due to a lack of adequate inventory management. However, with the integration of RFID tracking with blockchain events, they became rare occurrences. The reduced number of unverified or untraceable elements also enhanced audit preparedness at Lufthansa Technik, already causing more than a 40% reduction in the audit preparation. Similarly, the administrative staff claimed there was reduced redundancy of documentation processes since smart contracts automatically validate service intervals, technician approvals, and warranties. The project's financial aspect yielded a positive ROI within the first 18 months, given the differences in labor hours, inventory accuracy, and downtime (Giel *et al.,* 2013). However, the other major stakeholders of Lufthansa Technik have gained more confidence from leasing companies and the regulatory auditors since the system was opened. Once recorded, it is difficult to tamper with.

GPR Journals
www.gprjournals.org
Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

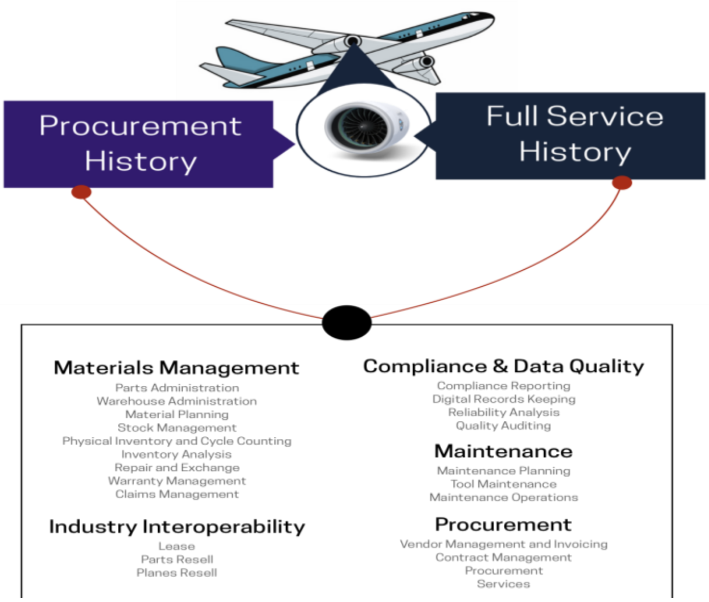

Figure 10: Using Blockchain in MRO Tracking

Lufthansa Technik's blockchain example showcases how a technically solid, standardized, and integrated architecture can transform the aerospace MRO industry. Hirsch, using real-time data ingestion or the DLT's immutability and integration points with the existing legacy systems, was able to drive improvements in traceability, compliance, and operations. This case proves that blockchain is not just an academic solution still in its proof-of-concept phase, but a reliable technology suitable for high-risk contexts such as aviation. It becomes an example of reference for all aerospace companies that want to operationalize the notion of traceability.

7. LEGAL, ETHICAL, AND REGULATORY CONSIDERATIONS

The use of blockchain for traceability in aerospace MRO has legal, ethical, and regulatory implications (Goritiyal *et al.,* 2021). Identification of the jurisdiction of data control, accountability issues, and changes in the international aviation authorities' tasks arise from various parts crossing borders and smart contracts that automate compliance. The legal implications of decentralised record keeping define the regulatory approaches needed to achieve lawful and ethical use of blockchain within the global aviation domain.

7.1 Data Sovereignty and Jurisdictional Compliance

As with any blockchain-based solution, adhering to international data residency regulations becomes key. Many components may be transported between countries for repair or inspection purposes, so their files must be easily retrievable without violating the laws of various countries. While blockchain's immutability can help prevent tampering with records, it can increase GDPR Article 17 issues concerning cross-border data management and compliance between aviation authorities and blockchain operators.

www.gprjournals.org
Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

Figure 11: Simplified Data Sovereignty Strategy

7.1.1 Blockchain Partitioning for Regional Data Residency

Leading companies such as Lufthansa Technik and others have started investigating geolocation blockchain nodes and separated storage to maintain compliance with data sovereignty. In this approach, the profile of nodes across the concurrently interconnected blockchain networks corresponds to the jurisdictions, which means that nodes will be established based on the requirements of the GDPR in Europe, CCPA in the United States, or the PDPA in Singapore. Payload is not recorded in the global ledger, and only metadata or even a cryptographic hash of the event is stored. All the sensitive data is stored locally within conformity restraints. Different access permissions are set by smart contracts, which check jurisdiction-skew before allowing data sharing across borders. Furthermore, more complex off-chain solutions, such as InterPlanetary File System (IPFS) with regional pinning rules, enable restricted geographical access to the data. This designed architecture integrates the capability of global traceability into an environment while respecting the lawful limitations of such a facility at the local level (Bhatt *et al.,* 2016). Regional portfolios also include compliance logs and related audit trails to allow authorities to view a record of transactions while not violating foreign data regulations. Thus, enhancing operational openness sans excessive regulation.

7.1.2 Legal Interoperability Across Multinational MRO Workflows

Organizational MRO environments in the multinational environment require LCM system interaction, first of all in the technical aspect and legal context. For instance, a part made in Germany, repaired in Singapore, and installed in an aircraft registered in the United States must meet each country's export control requirements, airworthiness directives, and data requirements. To support this, legal frameworks must accept blockchain-based certifications and even digital signatures across multiple borders. This is due to modern standards such as UNCITRAL's Model Law on Electronic Transferable Records (MLETR) and the EU's eIDAS regulation that legally recognize electronic records and identity management systems. In practice, smart contracts can enforce jurisdiction rules so that any part transfer in any transaction follows all the right export or import laws. Cross-border part transactions are time-stamped cryptographically to prove that the legal compliance check was performed at every stage. Legal gateways, or services that work as mediators and connectors between national compliant portals and the blockchain, also translate and verify documentation by the applicable national legislation, thus establishing a world where legal compliance becomes an intrinsic part of the transactions.

7.2 Ethics of Automation in Regulatory Processes

In MRO systems, smart contracts assume several essential critical tasks related to compliance, such as technician verification and inspection frequency. While this leads to increased operational efficiency and standardization, it raises questions about responsibility, fairness, and the human role in the decision process. Code-based regulation repositions authoritative decision-making in aviation in a way that disempowers individuals. Therefore, participants in the relevant activities must guarantee that automation enhances, instead of diminishing, responsibility and fairness.

7.2.1 Smart Contract Accountability and Oversight

Smart contracts in MRO platforms automate the execution of contracts based on predefined rules (Schyga *et al.,* 2019). Therefore, conflict is created when contract rules are poorly devised or unclear, and the surrounding environment is unknown. For instance, a contract may fail on a part installation due to a non-critical metadata mismatch while it is in operation. To eliminate such risks, Lufthansa Technik and other operators first adopt supervisory control, which means that there is manual override authority provided that certain conditions prevail. These overrides are logged and are not amendable to allow for auditable functionality without compromising the protocol. Governance frameworks provide provisions on when a given override can be executed, who has permission to do so, and whether the process should be documented. In addition, third-party auditing of smart contract logics is often done in search of logical errors and discussion bias, particularly in compliance decisions. Specifically, it guarantees that the contract operates within the legal mandates while at the same time being open to flexibility in execution. Ethical design means that one needs to let robots act according to rules and guidelines, but there must be a place for limited judgment where robots can make exceptions.

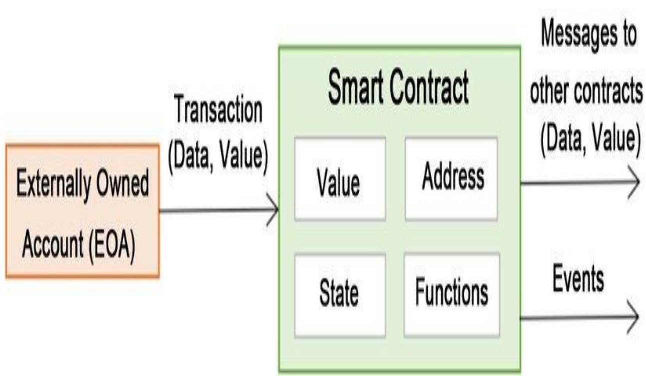

Figure 12: Structure of a Smart Contract

7.2.2 Algorithmic Fairness in Regulatory Enforcement

Incorporating machine learning and smart contracts in blockchain-based systems means that decisions about compliance with the law are made automatically. For example, AI mainly automatically raises maintenance signals by analyzing previous data obtained from sensors to

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

make smart contracts to ensure a given component remains grounded or inform the necessary authorities. This creates machine learning or algorithmic bias issues, especially if the models are trained on data that portrays past system or operational problem areas. In order to overcome this, modern aviation organizations are developing model transparency standards and algorithmic fairness audits. To justify decisions, the use of Explanatory AI approaches is applied to all inference activities, along with smart contract activation, and the result is entirely logged for the compliance path (Nassar *et al.,* 2020). Ethics panels or digital ethics boards appear to reconsider the AI-governed processes and identify potential risks and harms. These concepts are important in organizations such as aerospace industries since small details can cause issues with safety or the availability of flights in the following sessions. The ethical objective is to make the automated decision-making process controllable, transparent, reversible, and sanitary, where humans are held responsible for each layer of the decision-making process.

7.3 Standardization: The Role of ICAO, FAA, and IATA

A standardized strategy cannot assimilate legal and acceptable blockchain traceability globally and economically. Today's central regulators, like ICAO, FAA, and IATA, are partnering with industry groups to set standards that will validate blockchain technology as a reliable, transparent system for managing information and documents like aircraft airworthiness records, certificates, and parts history.

7.3.1 ICAO Blockchain Task Groups and Regulatory Models

The International Civil Aviation Organization (ICAO) has formed subcommittees under its task force on Aviation Blockchain to set technical and policy norms for applying distributed ledger technology in the aviation sector (Abeyratne *et al.,* 2020). These activities are geared toward developing blockchains for tracking the airworthiness, identification, and multiple certifications. For instance, ICAO concepts show how lifecycle events, such as manufacturing, installation, and inspection, align with global data schemata and smart contracts. This makes it easy for the regulators worldwide to understand and verify the blockchain events without making modifications. ICAO also backs the establishment of compliance oracles, pre-authenticated connected APIs that input new regulations into contract services, to keep smart contracts compliant with ever-changing rules. ICAO states that by implementing a governance structure and a trust layer between the aviation stakeholders, it will be possible to guarantee that blockchains implemented in various jurisdictions will be interoperable. This coordination is essential for building cross-border trust within the ecosystem, considering that components may circulate between operators and regulators of various nations using aircraft.

7.3.2 FAA and IATA Standards for Digital Certification

In the United States of America, the Federal Aviation Administration (FAA) has slowly started realizing the advantages of using blockchain to certify aircraft parts and maintenance activities. Pilot implementations have been made by substituting a current PDF-based form 8130-3 airworthiness certification with smart contracts and digital identity solutions. IATA enhances this counterpart through its MRO SmartHub, which aims to fill the aircraft MRO supply chain gaps through data standardization, part verification, and traceability through blockchain. IATA's guidance suggests that new developments, such as blockchain, should be based on open standards such as the ATA Spec 2000 for standardizing blockchain integration with aircraft part records across vendors and with regulation. FAA and IATA are in the process of familiarizing themselves with the fact that certificates issued on blockchain networks are compliant with traditional paper-based records in terms of evidence and audit. The long-term plan is the direct cross-validation of digital certificates and automatically triggered compliance notifications for regulators, suppliers, or operators, as well as decentralized access to the registry to ease the transition of parts and validation of maintenance records internationally.

The use of blockchain technology in aerospace MRO is a legal and ethical issue with active regulation that changes constantly due to the contradiction between innovation and legal responsibility. Privacy, big data, algorithmic bias, and global regulation are core aspects of the responsibility elements of traceability systems (Kroll, 2021). With the directions given by liberal international institutions such as ICAO, FAA, and IATA, and the right design of smart contracts and data governance, blockchain can be a legal, legitimate technology. Industry participants must step up efforts to ensure that the legal foundations follow the potential and development of technology.

Table 2: Summary of Legal, Ethical, and Regulatory Dimensions in Aviation Blockchain

Key Area	Summary
Data Sovereignty	Regional blockchain nodes and off-chain storage (e.g., IPFS) uphold GDPR, CCPA, and PDPA compliance.
Legal Interoperability	Smart contracts enforce export/import laws using UNCITRAL and eIDAS frameworks.
Ethical Automation	Governance models support manual override, auditability, and fairness in AI-driven decisions.
Regulatory Standardization	ICAO, FAA, and IATA promote interoperable blockchain standards for MRO certifications and traceability.

8. SCALING BLOCKCHAIN SYSTEMS IN THE AVIATION SUPPLY CHAIN

While blockchain has been used in initial experimentation to address various solutions in the aviation supply chain, scalability has remained a crucial factor with blockchain implementation shifting to infrastructure (Baharmand *et al.,* 2021). That is why airlines, OEMs, and MRO providers all have to break the digital silos to maintain performance, compliance and data protection. These phases explain the span or breadth, type of organization, including enterprise and national level, and the architectural approach and governance measures needed to ensure secure and scalable blockchain-based traceability.

8.1 Interoperability Across Airlines, MROs, and OEMs

The integration of blockchain systems must span all aspects of the aviation supply chain, from airlines, OEMs, MRO providers, leasing companies, and regulatory agencies. Where there is no centralized data model, cross-organizational traceability fails, component histories become dispersed and fragmented, affecting the trust amongst the partners. To counter this, many aviation industry players are standardizing on data schema and interfaces as articulated by IATA Digital MRP and ATA Spec 2000 (Vinod, 2021). Interoperable blockchain networks also need more than APIs, which address how transactions are semantically and cryptographically verified, given the

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

different models by different organisational members or entities. For instance, when a component is a component of an Airbus provider but later becomes an independent MRO in Singapore. All component records must be coherent, understandable, and comprehensible for audit purposes, given different stacks and data storage formats. Cross-chain messaging protocols and interledger frameworks are being developed to support this. These allow events on one permissioned blockchain, such as Hyperledger Fabric, to be certified or even linked to another blockchain network, such as Corda or Quorum.

8.2 Hybrid Cloud Strategies for Blockchain and AI Workloads

The need for scalability and following the rules of different jurisdictions causes organizations that build aviation blockchains to use hybrid cloud infrastructures. The concept of distributed nodes, where part of the blockchain and AI workloads can be run on-premise, part can be run on public cloud, and part can be run on private clouds, solves latency, computing, and sovereignty issues. For instance, Lufthansa may set up the first level of blockchain validator nodes in a local data centre in Germany because of compliance issues. In contrast, more complex tasks such as AI model training and sensor data analysis may occur in AWS or Azure GPU clusters. According to what is supported by Kubernetes and OpenShift, operators can containerize all blockchain peers, Kafka brokers, and AI inference engines in a manner that is portable and policy-embracing. Smart workload routing, therefore, ensures that latency-sensitive compliance processes are carried out near the data source. At the same time, other larger but less time-sensitive analytic tasks are performed in the more flexible and cheaper elastic compute zones (Gomes *et al.,* 2021). Some Azure support features are geo-fencing and policy-aware storage layers for enforcing data residency, encrypting at rest, and managing keys. These deployments are further protected with service meshes (Istio) and the zero-trust security paradigm that ensures secure multi and cross-cloud communications between the MRO facilities, OEMs, and the airline nodes in a decentralized yet highly synchronized network.

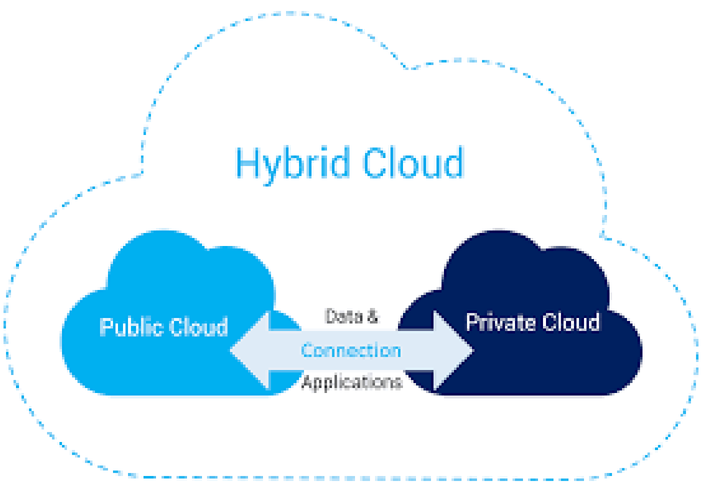

Figure 13: Hybrid Cloud Database Services

8.3 Governance, Key Management, and Role-Based Access

Using blockchain across the aerospace and supply chain industry involves cryptographic keys, identity, and permission management. In a permissioned blockchain like Hyperledger Fabric, each

www.gprjournals.org
Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

player, namely airline, original equipment manufacturer, or regulator, is allocated a unique digital certificate, issued by the certificate authority (CA). These are utilized to affirm and authenticate the various activities carried out in an organization while linking responsibility to identity. These are some of the general policies that relate to private keys, including how keys are created, changed, and cancelled. For example, LSG uses HSMs to store validator keys and identify multi-signature approval for dangerous goods, such as issuers ' compliance with overrides. Redundancy is achieved with threshold cryptographic systems to avoid single points of failure for the key recovery mechanisms. At the same time, the entities are granted permission to perform specific actions only, like changing the status of the part, executing contracts, or reviewing compliance reports through RBAC (Cruz *et al.,* 2018). Policies are expressed in the blockchain ACLs and are effective at the smart contract level, as well as at the method level. To this technical governance stack, there are the consortium governance models in which steering committees that involve selected airlines, MROs, and OEMs regulate changes in the protocol and rules and address conflict-solution mechanisms, contributing to both technical and institutional trust at the scale.

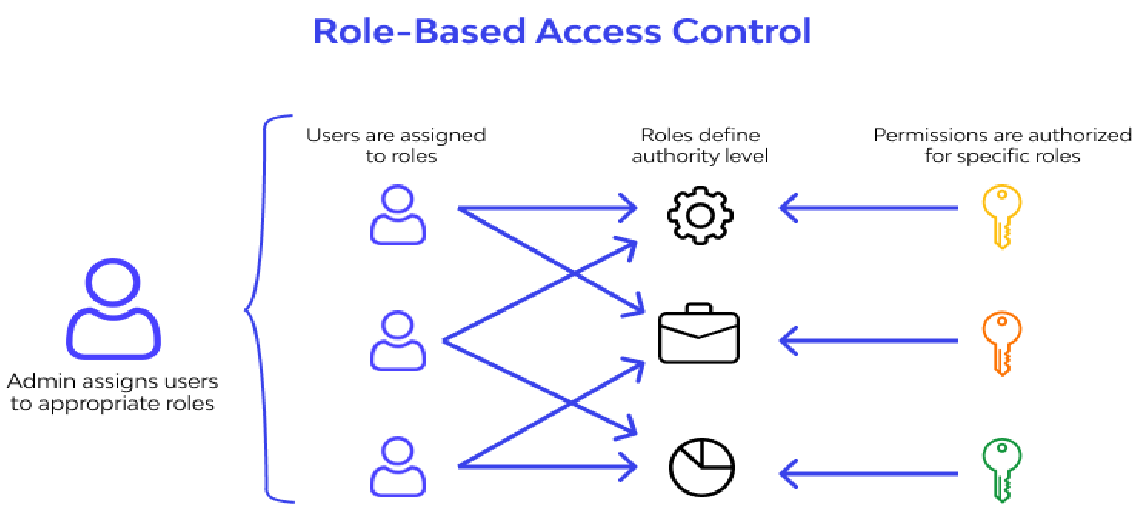

Figure 14: Understanding RBAC

Blockchain is a versatile tool with countless applications. However, to build the foundational elements necessary for its scalability in aviation, the focus needs to shift from adding more and more layers of infrastructure to shared coordinated protocols, distributed intelligence, and durable governance. Interoperability through common schemas, the utilization of hybrid cloud in terms of its performance-concerning compliance, as well as the implementation of class-based security providing role-awareness across stakeholders, holds the key to transitioning blockchains from proof-of-concept into production backbones in the industry. Together, these capabilities ensure that traceability systems remain engaging, sovereign-compliant, and trustworthy for all parts of the aviation industry.

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

9. FUTURE TRENDS: AI-AUGMENTED BLOCKCHAIN AND QUANTUM-READY AVIATION SYSTEMS

As the application of blockchain systems continues to evolve within the aviation industry, two particularly interesting areas are the adoption of artificial intelligence and the possibility of the emergence of new threats. As such, the MRO architectures of the future will incorporate AI to support predictive maintenance and decision-making and protect blockchain infrastructure against quantum attacks. These outline AI, digital twins, and post-quantum cryptography's roles in defining and redesigning traceability and compliance in the Aerospace Supply Chain.

9.1 AI for Predictive Traceability and Maintenance

Integrating artificial intelligence and blockchain technology is expected to revolutionize the aviation industry's predictive maintenance concept. By integrating data accumulated through a blockchain and past histories together with sensor information for the equipment and operational context fed into machine learning platforms, MRO platforms can predict their failure modes before they happen (Karwa, 2023). These models use KPI data of aircraft systems retrieved through Kafka stream, which is immutably timestamped on a blockchain platform, to analyze for anomalies and track the probable degradation of other subsystems like engines, hydraulic systems, and avionics modules. For instance, as the intervals are raised, the vibration record of a turbine blade, exposure to hot temperature, and previous inspection periods help determine the RUL. Consequently, once a specific risk level reaches or crosses a threshold limit, smart contracts can set up maintenance alerts, order replacements in advance, or schedule an inspection. Managing assets also involves reliability-centered maintenance (RCM), whereby AI gathers data on cross-fleet component behavior and recommends new service schedules. These decisions are recorded permanently in the blockchain, making them auditable and legally tenable. Integrating Artificial intelligence and blockchain enhances functionality and security throughout the fledgling global aviation business, transforming maintenance from recovery to prevention.

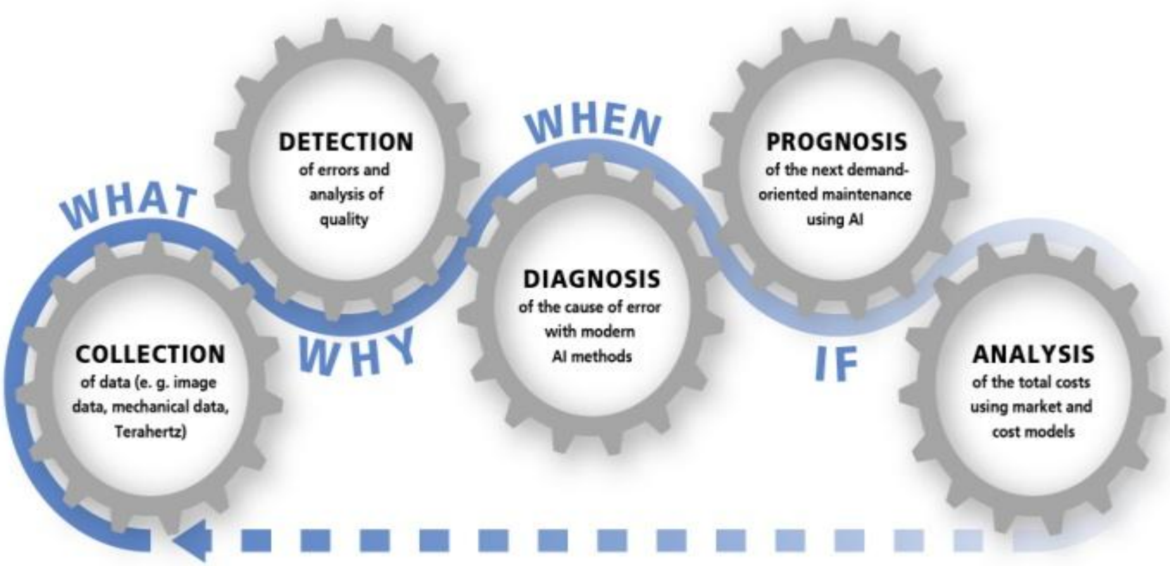

Figure 15: Predictive Maintenance and Condition Monitoring

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

9.2 Blockchain-Enabled Digital Twins for Aircraft Parts

Digital twins, or digital clones of physical objects, are now widely used in lifecycle and performance monitoring in aviation. In conjunction with blockchain records, digital twins also receive the capacity to display not just the physical condition of a part but also its compliance and maintenance records that are built into the system. This integration leads to real-time coordination between all the changes, events, or abnormalities occurring in a part's life cycle, the digital model, and the distributed ledger (Asante *et al.,* 2021). In practice, every part of the aircraft is entered into the blockchain with a unique traceability code associated with a twin virtual model. Here, IoT sensors provide the twin operational data in pressure, temperature, and vibration, whereas blockchain only records events like removal, inspection, and reinstallation. It is a good way to keep that digital representation current and up-to-date with the original record of the physical part, known as the certified audit trail. MRO teams, OEMs, and regulators can use the visualization dashboards that allow access to live data updated with blockchain-provenance records and service logs. This paradigm improves root cause analysis, supports CBM processes, and will shortly create a framework for fully automated MRO processes.

9.3 Post-Quantum Cryptography in Aerospace Ledgers

As quantum computing capabilities improve, classical cryptographic schemes like RSA and ECC grow more vulnerable to being compromised by quantum attacks. With the long lifespan of aerospace components and systems possibly up to decades, blockchain-based MRO platforms need to ready themselves today for tomorrow's cryptographic environment. Post-quantum cryptography (PQC) introduces algorithms resistant to classical and quantum computer attacks, ensuring that ledger integrity, signatures, and encryption will remain secure well into the future. Aerospace blockchain implementations are beginning to transition to quantum-resistant algorithms, such as lattice-based schemes, such as CRYSTALS-Kyber for key exchange and CRYSTALS-Dilithium for digital signatures, hash-based signatures, and code-based encryption. These are being tested on test blockchain environments where hybrid cryptography combines legacy and PQC methods for backward compatibility (Jacob *et al.,* 2021). Key rotation protocols and two-key, multi-signature smart contracts are also being tested to facilitate painless infrastructure upgrading to quantum-resistant hardware without compromising data or trust. Standards organizations such as NIST and ETSI are releasing guidelines for implementing PQC. For MRO blockchain networks, adding PQC is not just a technical upgrade but a necessary evolution to pre-empt aerospace security and compliance environments.

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

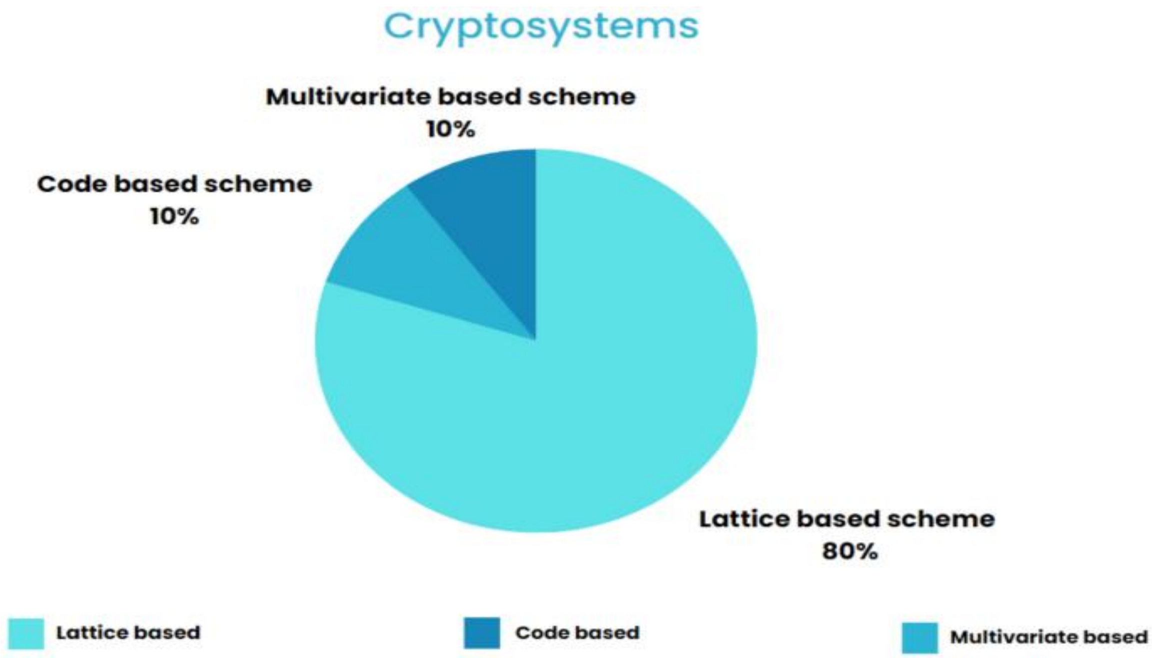

Figure 16: What is Post-Quantum Distributed Ledger Technology?

The future of blockchain in aviation is inextricably linked with advancements in AI, digital twin infrastructure, and quantum-resistant cryptography. By infusing intelligence into ledger-backed maintenance systems and quantum-hardening them, the aerospace sector is getting ready for a new era of predictive, secure, and autonomous operations. Such future-proofed technologies will enhance the accuracy and resilience of MRO systems and revolutionize how safety, compliance, and innovation coexist in the digital aviation ecosystem.

10. CONCLUSION AND ROADMAP FOR ADOPTION

Blockchain has emerged as a game-changing enabler of traceability for the Maintenance, Repair, and Overhaul (MRO) sector, addressing systemic inefficiencies in part tracking, compliance management, and data integrity. Traditional MRO systems hampered by siloed databases, paper record-keeping, and opaque chain-of-custody processes have long failed to meet international aviation's growing regulatory and operational requirements. By contrast, blockchain offers a decentralized, tamper-evident ledger design that allows all stakeholders, airlines, OEMs, MRO shops, lessors, and regulators, a shared, verifiable record of part life cycle events. This design provides cryptographic assurance that every transaction, from installation to inspection and removal, is secure, traceable, and jurisdictionally correct.

Smart contracts extend automation in MRO processes further by allowing rule-based enforcement of service intervals, technician qualification, and warranty conditions. These programmatic contracts reduce administrative overhead and deliver consistency and auditability across heterogeneous systems. Integrating real-time data ingestion platforms like Apache Kafka and streaming analytics with Apache Spark enables near-synchronous validation and blockchain commitment of operational events, bridging the physical part behavior to the digital traceability gap. Cost savings come from various sources, such as less downtime due to proactive maintenance, reduced fines for non-compliance, and reduced labor costs for manual verification and reporting.

Blockchain also enhances safety and risk management by restricting the application of certified, verifiable components to aircraft, reducing the entry of counterfeit or non-compliant parts into critical systems. On a larger scale, blockchain turns traceability from a requirement to fulfillment into a competitive advantage for aerospace supply chain resiliency and MRO optimization.

For Chief Information Officers (CIOs) and MRO executives interested in implementing blockchain solutions, a phased adoption is necessary to minimize risk while achieving maximum value. The first step is to select high-value use cases, which, in most cases, are high-risk items such as engines, auxiliary power units (APUs), avionics modules, and life-limited parts. These items provide the highest return on traceability since they have complex maintenance histories and are essential to flight safety. The initial pilot would integrate blockchain into current ERP and MRO systems through API-based microservices supporting bidirectional synchronization of maintenance events. Pilot technical teams must implement permissioned blockchain platforms such as Hyperledger Fabric or R3 Corda using smart contracts to model component lifecycles, service rules, and compliance logic.

Kafka must be utilized as the event streaming foundation to facilitate real-time consumption from IoT sensors, digital inspection tools, and maintenance terminals. AI models, which have been trained on the history of part behavior, can be introduced here to provide predictive insights correlated to blockchain-stored histories. Upon value being proved by the pilot, the solution needs to scale across multiple aircraft platforms and reach external partners, OEMs, lessors, and regulators via common governance frameworks. Cloud deployment patterns, hybrid, help with scalability concerning data sovereignty, and identity management must be made secure using PKI infrastructure. Access control and audit routines on smart contracts must be embedded in the starting point to introduce access policies and prevent logic mistakes. CIOs must also include compliance and legal experts at the earliest stage to address evolving rules governing digital documents, data storage under different jurisdictions, and smart contract enforceability. Complete integration also requires dashboarding for real-time tracking, automated regulatory reporting, and digital twin interfaces to enable transparency of operations.

Scaling blockchain traceability in aerospace MRO is a technical challenge and requires coordinated cooperation across the industry. Airlines, OEMs, MRO shops, regulators, leasing companies, and digital platform vendors must work together to establish interoperability standards, legal constructs, and shared data governance practices. Blockchain value will be confined to isolated implementations rather than systemic transformation without this coordination. Cross-functional task teams established under industry partnerships such as IATA, ICAO, and SAE can provide the basis for resolving open schemas, API standards, and smart contract templates. Membership within these teams should include IT managers, maintenance engineers, legal counsel, compliance officers, and procurement specialists. Regulator inclusion is vital to blockchain-stored certifications, inspection reports, and digital identities being accepted as legally admissible records across borders. Such collaboration could also effectively synchronize global shipments of components and reduce document duplication when authenticating documents across borders. Lastly, blockchain can elevate traceability from a back-office process to a cross-enterprise capability that improves safety, accelerates innovation, and unleashes operational agility in today's aviation.

GPR Journals
www.gprjournals.org
Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

REFERENCES

Abeyratne, R., & Abeyratne, R. (2020). Blockchain and aviation. *Aviation in the Digital Age: Legal and Regulatory Aspects*, 109-120.

Ahmad, R. W., Hasan, H., Yaqoob, I., Salah, K., Jayaraman, R., & Omar, M. (2021). Blockchain for aerospace and defense: Opportunities and open research challenges. *Computers & Industrial Engineering*, *151*, 106982.

Akuku, B. (2011). *Agent-based system for real-time database audit monitoring* (Doctoral dissertation, University of Nairobi).

Alam, A., Ullah, I., & Lee, Y. K. (2020). Video big data analytics in the cloud: A reference architecture, survey, opportunities, and open research issues. *IEEE Access*, *8*, 152377-152422.

Asante, M., Epiphaniou, G., Maple, C., Al-Khateeb, H., Bottarelli, M., & Ghafoor, K. Z. (2021). Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Transactions on Engineering Management*, *70*(2), 713-739.

Baharmand, H., Maghsoudi, A., & Coppi, G. (2021). Exploring the application of blockchain to humanitarian supply chains: insights from Humanitarian Supply Blockchain pilot project. *International Journal of Operations & Production Management*, *41*(9), 1522-1543.

Bhatt, T., Cusack, C., Dent, B., Gooch, M., Jones, D., Newsome, R., ... & Zhang, J. (2016). Project to develop an interoperable seafood traceability technology architecture: issues brief. *Comprehensive Reviews in Food Science and Food Safety*, *15*(2), 392-429.

Chang, S., Wang, Z., Wang, Y., Tang, J., & Jiang, X. (2019, August). Enabling technologies and platforms to aid the digitalization of commercial aviation support, maintenance and health management. In *2019 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE)* (pp. 926-932). IEEE.

Chavan, A. (2021). Exploring event-driven architecture in microservices: Patterns, pitfalls, and best practices.International Journal of Software and Research Analysis. Analysis.https://ijsra.net/content/exploring-event-driven-architecture-microservices-patterns-pitfalls-and-best-practices

Chavan, A. (2024). Fault-tolerant event-driven systems: Techniques and best practices. Journal of Engineering and Applied Sciences Technology, 6, E167.http://doi.org/10.47363/JEAST/2024(6)E167

Chonata Villamarín, J. F. (2019). *End-to-End IoT System Integration for Real Time Apps using MQTT and KAFKA for collecting and streaming data from Fog to Cloud* (Doctoral dissertation, ETSIS_Telecomunicacion).

Choo, B. S. (2004). *Best practices in aircraft engine MRO: A study of commercial and military systems* (Doctoral dissertation, Massachusetts Institute of Technology).

Cruz, J. P., Kaji, Y., & Yanai, N. (2018). RBAC-SC: Role-based access control using a smart contract. *IEEE Access*, *6*, 12240-12251.

Dhanagari, M. R. (2024). Scaling with MongoDB: Solutions for handling big data in real-time. *Journal of Computer Science and Technology Studies, 6*(5), 246-264. https://doi.org/10.32996/jcsts.2024.6.5.20

Du, D. (2018). *Apache Hive Essentials: Essential techniques to help you process and get unique insights from big data*. Packt Publishing Ltd.

Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J. (2020). A survey on blockchain technology concepts, applications, and issues. *SN Computer Science*, *1*(2), 114.

Giel, B. K., & Issa, R. R. (2013). Return on investment analysis of using building information modeling in construction. *Journal of computing in civil engineering*, *27*(5), 511-521.

Goel, G., &Bhramhabhatt, R. (2024).Dual sourcing strategies.*International Journal of Science and Research Archive*, 13(2), 2155.https://doi.org/10.30574/ijsra.2024.13.2.2155

Gomes, E., Costa, F., De Rolt, C., Plentz, P., & Dantas, M. (2021, December). A survey of real-time to near real-time applications in fog computing environments. In *Telecom* (Vol. 2, No. 4, pp. 489-517). MDPI.

Goritiyal, C., Bairolu, A., & Goritiyal, L. (2021). Application of emerging technologies in the aviation MRO sector to optimize cost utilization: the Indian case. *Intelligent Sustainable Systems: Selected Papers of WorldS4 2021, Volume 2*, 161-176.

Ho, G. T., Tang, Y. M., Tsang, K. Y., Tang, V., & Chau, K. Y. (2021). A blockchain-based system to enhance aircraft parts traceability and trackability for inventory management. *Expert Systems with Applications*, *179*, 115101.

Jacob, I., Lawson, R., & Smith, R. (2021). Future-Proofing AI and Cloud Systems: The Intersection of Quantum and Cybersecurity.

Kansara, M. A. H. E. S. H. B. H. A. I. (2022). A structured lifecycle approach to large-scale cloud database migration: Challenges and strategies for an optimal transition. *Applied Research in Artificial Intelligence and Cloud Computing*, *5*(1), 237-261.

Karwa, K. (2023). AI-powered career coaching: Evaluating feedback tools for design students. Indian Journal of Economics & Business. https://www.ashwinanokha.com/ijeb-v22-4-2023.php

Karwa, K. (2024). The future of work for industrial and product designers: Preparing students for AI and automation trends. Identifying the skills and knowledge that will be critical for future-proofing design careers.*International Journal of Advanced Research in Engineering and Technology*, *15*(5).https://iaeme.com/MasterAdmin/Journal_uploads/IJARET/VOLUME_15_ISSUE_5/IJARET_15_05_011.pdf

Konneru, N. M. K. (2021). Integrating security into CI/CD pipelines: A DevSecOps approach with SAST, DAST, and SCA tools. *International Journal of Science and Research Archive*. Retrieved from https://ijsra.net/content/role-notification-scheduling-improving-patient

Kroll, J. A. (2021, March). Outlining traceability: A principle for operationalizing accountability in computing systems. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 758-771).

Krupa Goel. (2023). How Data Analytics Techniques Can Optimize Sales Territory Planning. Journal of Computer Science and Technology Studies, 5(4), 248-264. https://doi.org/10.32996/jcsts.2023.5.4.26

Kumar, A. (2019). The convergence of predictive analytics in driving business intelligence and enhancing DevOps efficiency. International Journal of Computational Engineering and Management, 6(6), 118-142. Retrieved from https://ijcem.in/wp-content/uploads/THE-CONVERGENCE-OF-PREDICTIVE-ANALYTICS-IN-DRIVING-BUSINESS-INTELLIGENCE-AND-ENHANCING-DEVOPS-EFFICIENCY.pdf

Mohamed, N. (2021). From paper to blockchain: a proof of concept for storing aviation maintenance documents.

Nassar, M., Salah, K., Ur Rehman, M. H., & Svetinovic, D. (2020). Blockchain for explainable and trustworthy artificial intelligence. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *10*(1), e1340.

Nyati, S. (2018).Transforming telematics in fleet management: Innovations in asset tracking, efficiency, and communication. International Journal of Science and Research (IJSR), 7(10), 1804-1810. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203184230

Palamara, P. (2016). Tracing and tracking with the blockchain.

Perboli, G., Rosano, D. M., & Colonna, S. (2018). *Blockchain opportunities in the automotive market-spare parts case study* (Doctoral dissertation, MS Thesis. POLITECNICO DI TORINO. webthesis. biblio. polito. it).

Pohya, A. A., Wehrspohn, J., Meissner, R., & Wicke, K. (2021). A modular framework for the life cycle-based evaluation of aircraft technologies, maintenance strategies, and operational decision making using discrete event simulation. *Aerospace*, *8*(7), 187.

Raju, R. K. (2017). Dynamic memory inference network for natural language inference. International Journal of Science and Research (IJSR), 6(2). https://www.ijsr.net/archive/v6i2/SR24926091431.pdf

Riechmann, J. M. (2020). *Blockchain takes to the skies: an assessment of blockchain applications in the airline industry* (Master's thesis, Universidade Catolica Portuguesa (Portugal)).

Sardana, J. (2022). The role of notification scheduling in improving patient outcomes.*International Journal of Science and Research Archive*. Retrieved from https://ijsra.net/content/role-notification-scheduling-improving-patient

Schyga, J., Hinckeldeyn, J., & Kreutzfeldt, J. (2019, September). Prototype for a permissioned blockchain in aircraft MRO. In *Hamburg International Conference of Logistics (HICL) 2019* (pp. 469-505). epubli GmbH.

Journal of Procurement and Supply Chain Management
ISSN 2958 - 4078 (Online)
Vol.4, Issue 3, pp 14 – 31, 2025

Singh, V. (2022). Explainable AI in healthcare diagnostics: Making AI models more transparent to gain trust in medical decision-making processes. International Journal of Research in Information Technology and Computing, 4(2). https://romanpub.com/ijaetv4-2-2022.php

Singh, V. (2024). Real-time object detection and tracking in traffic surveillance: Implementing algorithms that can process video streams for immediate traffic monitoring. *STM Journals*. https://journals.stmjournals.com/ijadar/article=2025/view=201529/

Vieira, D. R., & Loures, P. L. (2016). Maintenance, repair and overhaul (MRO) fundamentals and strategies: An aeronautical industry overview. *International Journal of Computer Applications*, *135*(12), 21-29.

Vinod, B. (2021). *Evolution of Yield Management in the Airline Industry*. Berlin/Heidelberg, Germany: Springer International Publishing.

Wang, Q., Yu, J., Chen, S., & Xiang, Y. (2023). Sok: Dag-based blockchain systems. *ACM Computing Surveys*, *55*(12), 1-38.