



UNIVERSIDAD EUROPEA DE MADRID

ESCUELA DE ARQUITECTURA, INGENIERÍA Y DISEÑO

Máster Universitario en Ingeniería Aeronáutica

TRABAJO FIN DE MASTER

Blockchain en la Industria Aeronáutica: Un Estudio del Caso del Aircraft Technical Log

Pablo Hernández Fish

Curso 2022-2023

Título: Blockchain en la Industria Aeronáutica: Un Estudio del Caso del Aircraft Technical Log

Autor: Pablo Hernández Fish

Tutor: Pablo López Delgado

Titulación: Máster Universitario en Ingeniería Aeronáutica

Curso: Trabajo Fin de Master

RESUMEN

La revolución tecnológica global ha impulsado la digitalización e interconexión de múltiples industrias, incluida la aeroespacial. La tecnología blockchain está emergiendo como un agente transformador en este contexto. El estudio se enfoca en la exploración de su aplicación en la industria aeroespacial, específicamente en el Aircraft Technical Log (ATL), con el objetivo de evolucionar hacia un registro ATL basado en Blockchain.

La blockchain proporciona un marco seguro, descentralizado y transparente, que es esencial en una industria donde la seguridad y la trazabilidad son de vital importancia. Se abordan desafíos como la pérdida de datos y el acceso no autorizado, presentando soluciones innovadoras dentro del contexto blockchain. Se analizan aspectos clave de diseño, como la identificación de usuarios, la integración de sistemas, la escalabilidad y el cumplimiento normativo. Se desarrolla un prototipo funcional del ATL basado en blockchain, demostrando su capacidad para garantizar la seguridad y la trazabilidad de los datos.

El estudio respalda la implementación práctica de un ATL basado en blockchain, haciendo hincapié en la necesidad de perfeccionar, optimizar e integrar tecnologías emergentes. Un marco regulatorio sólido y la participación activa de las partes interesadas se consideran fundamentales para el éxito en la industria aeroespacial. Este trabajo contribuye al debate sobre la digitalización e innovación en la aviación, con el potencial de mejorar significativamente la eficiencia operativa y la seguridad en esta industria crítica.

Palabras clave: Blockchain, Aircraft Technical Log, Seguridad Operacional, Eficiencia, Trazabilidad, Industria Aeronáutica

ABSTRACT

The global technological revolution has driven the digitization and interconnection of multiple industries, including aerospace. Blockchain technology is emerging as a transformative force in this context. The study focuses on exploring its application in the aerospace industry, specifically in the Aircraft Technical Log (ATL), with the aim of evolving towards a blockchain-based ATL record.

Blockchain provides a secure, decentralized, and transparent framework, which is essential in an industry where security and traceability are of vital importance. Challenges such as data loss and unauthorized access are addressed, presenting innovative solutions within the blockchain context. Key design aspects are analyzed, such as user identification, system integration, scalability, and regulatory compliance. A functional prototype of the blockchain-based ATL is developed, demonstrating its ability to ensure data security and traceability.

The study supports the practical implementation of a blockchain-based ATL, emphasizing the need to refine, optimize, and integrate emerging technologies. A robust regulatory framework and active stakeholder participation are considered essential for success in the aerospace industry. This work contributes to the debate on digitization and innovation in aviation, with the potential to significantly enhance operational efficiency and security in this critical industry.

Key words: Blockchain, Aircraft Technical Log, Safety, Efficiency, Traceability, Aerospace Industry

Índice de contenidos

RESUMEN	3
ABSTRACT.....	3
1. Introducción.....	13
1.1 Objetivos del estudio	13
1.2 Justificación y relevancia del estudio.....	14
2. Fundamentos de la tecnología Blockchain	16
2.1 Definición y principios de la tecnología blockchain	16
2.1.1 Definición de Blockchain.....	16
2.1.2 Historia y origen de Blockchain.....	17
2.1.3 Principios fundamentales de Blockchain	19
2.1.4 Tipos de Blockchain.....	20
2.1.5 Estructura de un Bloque	23
2.2 Funcionamiento de blockchain	26
2.2.1 Creación de transacciones	26
2.2.2 Agrupación de transacciones en bloques	27
2.2.3 Proceso de validación	28
2.2.4 Consenso y resolución de conflictos.....	29
2.2.5 Seguridad	31
2.2.6 Interoperabilidad con otros sistemas	32
2.2.7 Smart Contracts	33
2.3 Beneficios y limitaciones de la tecnología blockchain	35
2.3.1 Beneficios de la Blockchain.....	35
2.3.2 Limitaciones de la Blockchain	36
3. Blockchain en la industria aeronáutica	38
3.1 Potenciales beneficios de la implementación de blockchain en la aviación	38
3.1.1 Gestión de identidades de pasajeros (Passenger Identity Management).....	38
3.1.2 Emisión de billetes y pago (Ticketing and Payment)	39
3.1.3 Programas de fidelización (Frequent Flyer programs).....	40
3.1.4 Equipaje y carga	40

3.1.5	Mantenimiento de aeronaves.....	40
3.1.6	Cadena de suministro (Supply chain).....	42
3.1.7	Registros de vuelo.....	43
3.1.8	Gestión de flotas.....	43
3.1.9	Gestión del espacio aéreo y Planificación de vuelos.....	44
3.1.10	Integración de UAS.....	45
3.2	Desafíos y limitaciones de la implementación de blockchain en la aviación.....	46
3.2.1	Desafíos de la implementación Blockchain en la aviación.....	46
3.2.2	Limitaciones de la implementación Blockchain en la aviación.....	48
3.3	Ejemplos de uso y casos de estudio existentes.....	50
4.	Caso de estudio: Aircraft Technical Log basado en blockchain.....	54
4.1	Introducción y relevancia del Aircraft Technical Log en la aviación.....	54
4.1.1	Definición y función.....	54
4.1.2	Marco jurídico y supervisión.....	55
4.1.3	Relevancia en la aviación.....	58
4.2	Problemas y desafíos actuales con el Aircraft Technical Log.....	59
4.3	Aircraft Technical Log utilizando tecnología blockchain.....	60
4.3.1	Análisis sobre el uso de Blockchain en el ATL.....	60
4.3.2	Consideraciones en el diseño y desarrollo de un ATL basado en Blockchain.....	71
5.	Prueba de Concepto: Diseño y Desarrollo.....	92
5.1	Diseño de la aplicación.....	92
5.1.1	Análisis de usuarios y tareas.....	92
5.1.2	Diseño de funcionalidades y flujo de trabajo.....	94
5.1.3	Diseño de la estructura de datos.....	96
5.2	Desarrollo de la aplicación.....	99
5.2.1	Hardware y software utilizado.....	99
5.2.2	Desarrollo de los bloques y estructura de datos.....	100
5.2.3	Desarrollo de la interfaz y funcionalidades.....	106
5.3	Demostración.....	108
5.3.1	Tripulación de Cabina.....	108
5.3.2	Personal de Mantenimiento.....	113
5.3.3	Aerolíneas y Organismos Supervisores.....	119
5.4	Desarrollos Futuros y Expansión de la Aplicación.....	123



6. Conclusiones	126
7. Referencias.....	129

Acrónimos

Acrónimo	Definición
AOC	Air Operator Certificate
API	Application Programming Interface
ATC	Air Traffic Control
ATL	Aircraft Technical Log
CAMO	Continuing Airworthiness Management Organisation
DApps	Aplicaciones descentralizadas
DCA	Digital Certification Authority
DID	Decentralized Identifiers
DPoS	Delegated Proof of Stake
EASA	European Union Aviation Safety Agency
ETL	Electronic Technical Log
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulations
GDPR	Reglamento General de protección de Datos de la UE
IA	Inteligencia Artificial



IATA	International Air Transport Association
IFPS	InterPlanetary File System
IoT	Internet of Things
JSON	JavaScript Object Notation
MRO	Maintenance, Repair, Operations
PoA	Proof of Authority
PoB	Proof of Burn
PoS	Proof of Stake
PoW	Proof of Work
SOA	Software Oriented Architecture
UAS	Unmanned Aerial Systems
UI	User Interface

Figuras

Figura 1. Logo Bitcoin (Wikipedia)	16
Figura 2. Esquema de transacciones Bitcoin (Nakamoto, 2008)	17
Figura 3. Estructura de bloques y Merkle Tree (Liang, 2020)	23
Figura 4. Firma digital (CB, 2023)	27
Figura 5. Smart contract workflow (GG, 2022)	35
Figura 6. IATA Travel Pass basado en tecnología blockchain.....	38
Figura 7. Blockchain de Consorcio para Compartir Datos Seguros de Mantenimiento de Aeronaves: Un Escenario Simplificado (DS.aero, 2019).....	41
Figura 8. Ejemplo Blockchain/UAS caso de estudio (DoT, 2021)	45
Figura 9. Coste de transacción Bitcoin (Bitcoin, 2021)	48
Figura 10. Ejemplo de Aircraft Technical Log.....	54
Figura 11. Logo EASA (izquierda) y FAA (derecha).....	56
Figura 12. Interfaz ETL TrustFlight	61
Figura 13. Ejemplo de árbol de decisión (Chowdhury et al., 2018)	64
Figura 14. Árbol de decisión IATA (Goudarzi et al., 2018)	65
Figura 15. Flujo de trabajo de la tripulación de vuelo	95
Figura 16. Flujo de trabajo del personal de mantenimiento	95
Figura 17. Flujo de trabajo de aerolíneas y organismos supervisores.....	96
Figura 18. Estructura de datos en sistema ATL.....	97
Figura 19. Logo Python (izquierda) y Flask (derecha)	100
Figura 20. Código desarrollado de las funcionalidades Blockchain	101
Figura 21. Código desarrollado de la estructura de un bloque de la red	101
Figura 22. Definición de las clases “Aircraft”, “Flight” y “MaintenanceEntry”	104
Figura 23. Definición de las clases “TechnicalIssue” y “MaintenanceAction”	105

Figura 24. Página de login aplicación de tripulación de cabina	109
Figura 25. Página de selección de aeronave aplicación de tripulación de cabina	109
Figura 26. Historial aeronave A320 aplicación de tripulación de cabina	110
Figura 27. Vuelo MAD-BCN aeronave A320 aplicación de tripulación de cabina	111
Figura 28. Formulario de vuelo “Flight Log” para el vuelo MAD-BCN aplicación de tripulación de cabina	111
Figura 29. Formulario de defectos técnicos en el “Flight Log” para el vuelo MAD-BCN aplicación de tripulación de cabina	112
Figura 30. Historial del A320 con el nuevo vuelo MAD-BCN aplicación de tripulación de cabina	113
Figura 31. Página de login aplicación personal de mantenimiento	114
Figura 32. Página de selección de aeronave aplicación personal de mantenimiento	114
Figura 33. Historial aeronave A320 aplicación personal de mantenimiento (1)	115
Figura 34. Historial aeronave A320 aplicación personal de mantenimiento (2)	115
Figura 35. Formulario de registro de acción de mantenimiento relacionada con un defecto técnico aplicación personal de mantenimiento	116
Figura 36. Acción de mantenimiento en el historial de la aeronave A320 aplicación personal de mantenimiento	117
Figura 37. Formulario actividad de mantenimiento aplicación personal de mantenimiento	118
Figura 38. Historial del A320 con la nueva actividad de mantenimiento aplicación personal de mantenimiento	118
Figura 39. Página de login aplicación aerolíneas/organismo supervisor	119
Figura 40. Página de selección de aeronave aplicación aerolíneas/organismo supervisor	119
Figura 41. Historial aeronave A320 aplicación aerolíneas/organismo supervisor	120
Figura 42. Actividad de mantenimiento aeronave A320 aplicación aerolíneas/organismo supervisor	121
Figura 43. Vuelo MAD-LCG aeronave A320 aplicación aerolíneas/organismo supervisor	121
Figura 44. Filtros adicionales para “Flights” aplicación aerolíneas/organismo supervisor	122
Figura 45. Filtros adicionales para “Maintenance Entries” aplicación aerolíneas/organismo supervisor	122



Figura 46. Ejemplo datos JSON aeronave A320 aplicación aerolíneas/organismo supervisor..... 123

Tablas

Tabla 1. Comparativa de tipos de blockchain	22
Tabla 2. Componentes de un bloque	24
Tabla 3. Matriz comparativa de diferentes modelos de ATL	67
Tabla 4. Análisis comparativo de tipos de blockchain para un sistema ATL.....	76
Tabla 5. Tipos de usuarios, funciones, tareas y permisos necesarios en el sistema ATL propuesto	93

1. Introducción

1.1 Objetivos del estudio

Durante las últimas décadas el mundo ha sufrido una revolución tecnológica que lo ha llevado a ser más interconectado y digitalizado, las tecnologías como la inteligencia artificial (IA) o el Big Data están impulsando oportunidades significativas para mejorar la eficiencia y la seguridad operativa (safety) en diversas industrias. La industria aeronáutica, pese a ser una industria altamente regulada y compleja, también está empezando a beneficiarse en gran medida de la adopción de estas innovaciones. Una de estas tecnologías emergentes es la tecnología blockchain, que ha demostrado su potencial en varios campos, como las finanzas, la logística y la cadena de suministro (Supply chain), entre otros. No obstante, la aplicación de esta tecnología en la industria aeronáutica todavía es tema de debate y se encuentra actualmente en fase de investigación, con el objetivo de comprender sus posibles utilidades, beneficios y riesgos.

El objetivo principal de este estudio consiste en explorar la tecnología blockchain y analizar sus potenciales usos y aplicaciones tanto a nivel global en la industria aeronáutica como en un caso de uso específico. Dicho caso de uso tiene como propósito demostrar la viabilidad de emplear blockchain como tecnología en el desarrollo de un Registro Técnico Digital de Aeronaves o Aircraft Technical Log (ATL), el cual es un componente esencial en las operaciones y el mantenimiento de las aeronaves. Este estudio busca no sólo investigar la teoría detrás de la aplicación de la tecnología blockchain en la industria aeronáutica, sino también proporcionar una visión práctica y tangible de esta aplicación. De estos objetivos globales del estudio se pueden definir además los siguientes objetivos específicos:

1. Analizar los fundamentos y funcionamiento de la tecnología blockchain. Este análisis permitirá comprender mejor los conceptos básicos de blockchain, su funcionamiento, así como las ventajas y limitaciones asociadas con esta tecnología.

2. Explorar las posibles aplicaciones de la tecnología blockchain en la industria aeronáutica. La tecnología blockchain puede tener diversas aplicaciones en la industria aeronáutica, desde la mejora de la eficiencia en las operaciones de mantenimiento hasta la garantía de la trazabilidad y la autenticidad de las piezas de las aeronaves. Este estudio buscará identificar estas posibles aplicaciones y discutir sus beneficios y desafíos asociados.

3. Identificar y analizar ejemplos de uso y casos de estudio existentes de blockchain en la industria aeronáutica. A través de esta revisión y análisis se pretende poder proporcionar una visión más concreta y práctica del potencial de la tecnología blockchain en la aviación.

4. Investigar la relevancia del Aircraft Technical Log en la industria aeronáutica e identificar problemas y desafíos actuales asociados con su uso. Como se ha mencionado el ATL es un elemento esencial de las operaciones de vuelo y mantenimiento de las aeronaves, y su manejo eficiente y seguro es clave para garantizar la seguridad operacional y aeronavegabilidad de las mismas. Este estudio buscará entender mejor su papel, los requisitos y obligaciones por parte de los agentes que utilizan

esta tecnología así como los desafíos y limitaciones actuales en su manejo y cómo la tecnología blockchain puede ayudar a abordar estos desafíos.

5. Establecer una serie de hipótesis de partida para el posible diseño y desarrollo de un Aircraft Technical Log basado en blockchain. En este estudio, se presentarán una serie de consideraciones que se deberán tener en cuenta a la hora de proceder al diseño y desarrollo de un ATL basado en blockchain, incluyendo aspectos como la identificación de usuarios, integración con otros sistemas, la escalabilidad o el cumplimiento normativo.

6. Desarrollar una prueba de concepto de un Aircraft Technical Log basado en blockchain y demostrar su funcionalidad. Para proporcionar una visión más práctica de la propuesta, este estudio incluirá el desarrollo y la demostración de un prototipo básico de ATL basado en blockchain.

7. Evaluar la viabilidad y ofrecer recomendaciones para la implementación del Aircraft Technical Log basado en blockchain en la práctica. Finalmente, este estudio buscará evaluar la viabilidad de la implementación de la propuesta en la práctica y ofrecerá recomendaciones para una futura posible implementación.

1.2 Justificación y relevancia del estudio

La elección de la tecnología blockchain como tema de estudio surge debido al creciente auge y relevancia de esta tecnología en numerosos sectores de la economía global durante la última década. Con sus fundamentos en la seguridad, la descentralización y la transparencia, la tecnología blockchain tiene el potencial de revolucionar la manera en que se realizan las transacciones y se almacenan los datos en muchas industrias. En el sector aeronáutico, donde la seguridad, la precisión y la trazabilidad son elementos críticos, es razonable que la tecnología blockchain presenta un gran potencial para aportar mejoras significativas.

El Aircraft Technical Log, como caso de estudio específico, se ha seleccionado por su importancia en las operaciones diarias de la aviación y por los desafíos que actualmente se enfrentan en su gestión. Los registros técnicos de las aeronaves, que contienen información vital sobre el estado de las aeronaves y sus componentes, son esenciales para garantizar la seguridad operacional y la eficiencia de las operaciones. Sin embargo, su manejo y almacenamiento actual pueden enfrentar desafíos, como la pérdida o alteración de datos, el acceso no autorizado y el manejo ineficiente. La tecnología blockchain, con sus características de seguridad y trazabilidad, ofrece una solución potencial a estos desafíos.

Este estudio tiene una relevancia particular en dos aspectos principales. Primero, desde el punto de vista de la industria aeronáutica, la exploración de nuevas tecnologías que pueden mejorar la eficiencia y la seguridad de las operaciones aeronáuticas es esencial y es algo que ha caracterizado al sector. A medida que la tecnología avanza y los desafíos en la industria aeronáutica se vuelven cada vez más complejos (ej. efecto de emisiones sobre el medio ambiente o la saturación del espacio aéreo y aeropuertos aumentando los retrasos y complejidad de las operaciones), es importante explorar y

adoptar innovaciones que pueden ofrecer soluciones. Segundo, desde el punto de vista de la tecnología blockchain, este estudio busca realizar una contribución a la creciente literatura que explora las aplicaciones de la tecnología blockchain en diversos sectores. Aunque la tecnología blockchain ha sido ampliamente estudiada en sectores como las finanzas, su aplicación en la industria aeronáutica aún está en una fase temprana de investigación y exploración. Existe una brecha notable en la literatura existente sobre la aplicación práctica de la tecnología blockchain en la industria aeronáutica. Aunque hay numerosos estudios teóricos y conceptuales sobre el tema, actualmente carecemos de un corpus amplio de investigaciones que ofrezcan ejemplos prácticos o prototipos que impulsen su aplicación real.

En cuanto al impacto potencial de este estudio, los hallazgos podrían tener diversas implicaciones significativas. Para la industria aeronáutica, los resultados de esta investigación podrían ayudar a mejorar la comprensión sobre la implementación práctica de la tecnología blockchain para mejorar las operaciones aéreas. Asimismo, para los investigadores especializados en tecnología blockchain, este estudio podrá ofrecer un ejemplo de cómo esta tecnología puede ser aplicada en un caso de estudio específico en la aviación. Además, a largo plazo, el estudio realizado puede contribuir a fomentar una mayor adopción de la tecnología blockchain en la industria aeronáutica, a medida que los profesionales de la aviación y los responsables de la toma de decisiones se familiaricen con sus potenciales beneficios y aplicaciones prácticas.

2. Fundamentos de la tecnología Blockchain

2.1 Definición y principios de la tecnología blockchain

2.1.1 Definición de Blockchain

La tecnología blockchain fue presentada por primera vez en 2008 por un individuo (o entidad) conocido como Satoshi Nakamoto, quien la implementó como componente fundamental de la criptomoneda Bitcoin (Nakamoto, 2008). Desde entonces, la tecnología blockchain ha superado su propósito original de aplicación en el ámbito de las criptomonedas para convertirse en una tecnología disruptiva con potencial para transformar diversas industrias.



Figura 1. Logo Bitcoin (Wikipedia)

En su sentido más básico, una blockchain es una estructura de datos distribuida que mantiene una creciente lista de registros, llamados bloques, los cuales están enlazados y asegurados usando criptografía (Narayanan et al., 2016). Cada bloque en una blockchain contiene información sobre transacciones o eventos, y tiene un enlace a su bloque anterior a través de una "huella" criptográfica única, conocida como hash. Este diseño enlazado asegura la inmutabilidad de los datos: una vez que un bloque se ha añadido a la cadena, su contenido no puede ser modificado sin alterar todos los bloques siguientes, lo cual es computacionalmente inviable en una red con un gran número de participantes. Además de su inmutabilidad, otra característica clave de la blockchain es su naturaleza descentralizada. A diferencia de las bases de datos tradicionales, que suelen ser controladas por una única entidad, las blockchains son mantenidas por una red de nodos que participan en la validación y el registro de las transacciones (Tapscott & Tapscott, 2016). Esto significa que ninguna entidad única tiene control total sobre la información registrada en la blockchain. El término "blockchain" en realidad abarca una familia de tecnologías con características y principios similares (Wamba et al., 2020). Aunque la blockchain de Bitcoin es la más conocida, existen otras variantes como las blockchains de consorcio o privadas, que restringen quién puede participar en la red o validar transacciones. Pero, independientemente de su forma, todas las blockchains comparten unos principios fundamentales que se verán en la sección 2.1.3. Para el resto del estudio se usará la palabra "blockchain" con definición genérica de tecnología de registros digitales distribuidos de transacciones firmadas criptográficamente que se agrupan en bloques. Cada bloque está vinculado criptográficamente al anterior, haciéndolo a prueba de manipulaciones, tras ser validado y sometido

a una decisión consensuada. A medida que se añaden nuevos bloques, se hace más difícil modificar los anteriores, creando resistencia a la manipulación. Los nuevos bloques se replican en copias del libro mayor dentro de la red, y cualquier conflicto se resuelve automáticamente mediante reglas establecidas (Yaga et al., 2019).

2.1.2 Historia y origen de Blockchain

La tecnología blockchain tiene su motivación en la búsqueda de una forma de moneda digital descentralizada que comenzó en las últimas décadas del siglo XX. El primer logro significativo en este campo fue la creación de la criptografía de clave pública en la década de 1970, que se convirtió en la base de las firmas digitales y los protocolos de transmisión segura de datos (Diffie & Hellman, 1976). En la década de 1980 y 1990 surgen las primeras investigaciones en el desarrollo de lo que será el blockchain entendiéndolo como una lista de registros o bloques que se enlazan y protegen utilizando criptografía (Haber & Stornetta, 1991). No es hasta 2008 que Satoshi Nakamoto introduce el protocolo de Bitcoin (Nakamoto, 2008), que es un servidor de marcas de tiempo entre pares que se basa en funciones criptográficas de hash en lugar de confianza para registrar y confirmar computacionalmente transacciones electrónicas sin intermediarios. Bitcoin resuelve entre otros el problema del doble gasto, la posibilidad de que una misma moneda digital se gastara más de una vez, al mantener cronológicamente un libro mayor distribuido que verifica que la moneda utilizada en una transacción no se haya utilizado previamente en otra transacción. El libro mayor es mantenido y verificado por una red de nodos en lugar de un tercero de confianza o una autoridad central. Este libro mayor distribuido se conoce como Blockchain, donde cada bloque incluye un conjunto de transacciones que están vinculadas con bloques anteriores a través de hashes criptográficos.

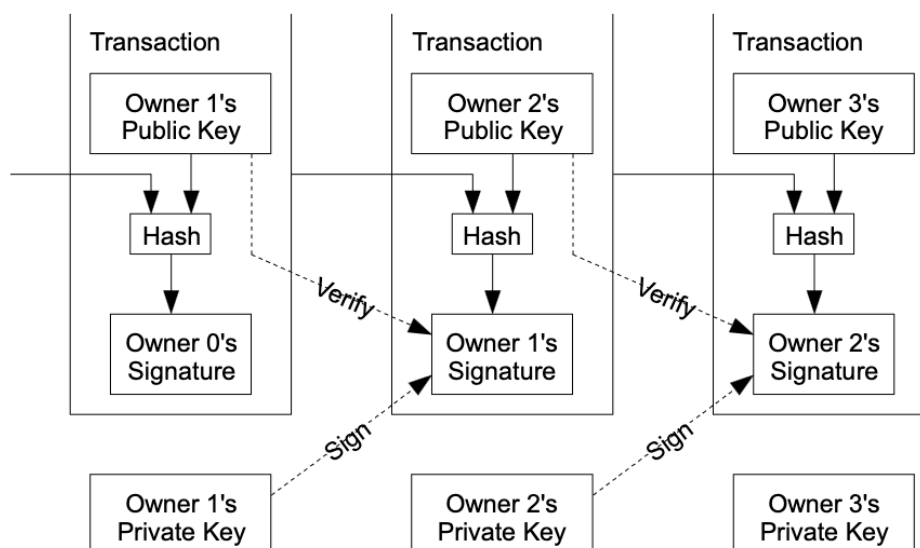


Figura 2. Esquema de transacciones Bitcoin (Nakamoto, 2008)

Tras la aparición de Bitcoin, la tecnología blockchain comenzó a atraer un creciente interés más allá de su uso en las criptomonedas. En la actualidad se puede categorizar la evolución de la tecnología blockchain en 4 etapas:

- **Blockchain 1.0** se refiere a la primera generación de la tecnología blockchain, que giraba principalmente en torno a las criptomonedas. Se inicia con la publicación del famoso libro blanco de Satoshi Nakamoto (Nakamoto, 2008). Esta tecnología ofrecía inmutabilidad, transparencia y transacciones seguras a través de un mecanismo de consenso conocido como prueba de trabajo. Bitcoin rápidamente ganó popularidad y sirvió como una moneda digital y reserva de valor.
- **Blockchain 2.0** la segunda generación de la tecnología blockchain expandió la utilidad de la blockchain más allá de las criptomonedas. Uno de los hitos significativos en esta generación fue la introducción de Ethereum. Ethereum, como se describe en su libro blanco por Vitalik Buterin (Buterin, 2014), permitió la creación de contratos inteligentes y aplicaciones descentralizadas (DApps). Los contratos inteligentes, programados en la cadena de bloques de Ethereum utilizando el lenguaje Solidity, permitieron transacciones automatizadas y autoejecutables. Esta innovación abrió puertas a diversas aplicaciones, incluyendo finanzas descentralizadas (DeFi), tokenización y financiamiento colectivo.
- **Blockchain 3.0** representa la tercera generación de la tecnología blockchain, enfocada principalmente en abordar los desafíos de escalabilidad e interoperabilidad. Proyectos como EOS¹, Cardano² y NEO³ surgieron durante esta era para mejorar la velocidad y capacidad de transacción. Los mecanismos de consenso evolucionaron más allá del intenso consumo de energía de la prueba de trabajo (PoW), incorporando algoritmos de prueba de participación (PoS) y prueba de participación delegada (DPoS). Estos avances tenían como objetivo mejorar la escalabilidad, eficiencia energética y rendimiento de la red. Además, surgieron protocolos de interoperabilidad para facilitar la comunicación entre diferentes redes blockchain, permitiendo la transferencia de datos y la colaboración sin problemas.
- **Blockchain 4.0** representa la última generación de la tecnología blockchain, que enfatiza la integración de la cadena de bloques con tecnologías emergentes. Esta generación busca aprovechar las capacidades de la IA, el Internet de las cosas (IoT), el big data y el aprendizaje automático. Blockchain 4.0 tiene como objetivo mejorar la privacidad, seguridad y eficiencia en diversas industrias. Proyectos como IOTA⁴ y VeChain⁵ exploran las posibles aplicaciones de blockchain en la gestión de la cadena de suministro, logística e integridad de datos. Al

¹ <https://eos.io/>

² <https://cardano.org/>

³ <https://neo.org/>

⁴ <https://www.iota.org/>

⁵ <https://www.vechain.org/>

combinar blockchain con estas tecnologías emergentes, Blockchain 4.0 tiene como objetivo revolucionar procesos, optimizar operaciones y crear nuevos modelos de negocio.

Aunque la tecnología blockchain todavía es relativamente joven, ya ha demostrado ser una herramienta poderosa y disruptiva. Su impacto potencial se extiende mucho más allá del ámbito de las criptomonedas y el financiero, y tiene el potencial de revolucionar una amplia gama de industrias, incluyendo la aeronáutica, como explicaremos en las siguientes secciones de este estudio.

2.1.3 Principios fundamentales de Blockchain

En esta sección, se explorarán los principios fundamentales de la tecnología blockchain con el objetivo de empezar a comprender su relevancia y aplicabilidad en diversas industrias. Los principios incluyen la descentralización, que elimina la necesidad de una autoridad central; la seguridad y la criptografía, que garantizan la inmutabilidad y confiabilidad de los datos; la transparencia y el anonimato, que permiten una visibilidad total de las transacciones manteniendo la identidad de los usuarios protegida; los métodos de consenso, esenciales para mantener la seguridad de la red y prevenir el doble gasto; y los contratos inteligentes, que amplían las posibilidades de la blockchain más allá de las transacciones financieras. Todos estos principios, en su conjunto, forman los fundamentos innovadores de la tecnología blockchain.

1. **Descentralización:** La descentralización es una característica intrínseca y fundamental de la tecnología blockchain. De manera contraria a la mayoría de sistemas actuales de gestión de información y transacciones que son centralizados (Mougayar, 2016), la blockchain se fundamenta en un modelo descentralizado. En lugar de contar con una entidad centralizada que controla y toma decisiones, la blockchain opera en una red de nodos distribuidos. Cada nodo mantiene una copia completa de la blockchain y participa activamente en el proceso de verificación y registro de las transacciones (Nakamoto, 2008). Este sistema de descentralización ofrece diversas ventajas. Entre otras aumenta la resistencia, robustez y seguridad del sistema ya que la información no está almacenada en un único lugar, por lo que la red puede seguir funcionando incluso si algunos nodos fallan o son atacados (Tapscott & Tapscott, 2016).
2. **Seguridad y Criptografía:** La seguridad es un componente principal y crítico de la tecnología blockchain, y se logra mediante el uso de técnicas criptográficas avanzadas en toda la red. Cada bloque en la cadena contiene una serie de transacciones y está vinculado a su bloque anterior a través de un hash criptográfico. Esta propiedad confiere a la blockchain su naturaleza inmutable al asegurar que una vez que un bloque ha sido añadido a la cadena este no puede ser alterado ni eliminado (Narayanan et al., 2016). Este nivel de seguridad puede ser vital en muchos entornos e industrias donde la autenticidad y la precisión de los datos son de gran importancia. Además, el uso de criptografía avanzada no solo ayuda a proteger la integridad de los datos sino que también puede utilizarse para asegurar la confidencialidad y

la privacidad de las transacciones, proporcionando una tecnología óptima para la transferencia segura y fiable de información (Zyskind et al., 2015).

- 3. Transparencia y Anonimato:** La tecnología blockchain aporta un equilibrio único entre transparencia y anonimato que de primeras pueden parecer conceptos opuestos. Por un lado, todas las transacciones son públicas y están disponibles para ser auditadas por todos los participantes de la red. Esto aporta un alto grado de transparencia y permite el rastreo de transacciones (Narayanan et al., 2016). Por otro lado, los usuarios pueden mantener su anonimato ya que las transacciones no están vinculadas a identidades personales, sino a direcciones virtuales (Miers et al., 2013). Estas direcciones en la blockchain son secuencias exclusivas de caracteres que simbolizan la identidad de un usuario. Estas cadenas se crean mediante un procedimiento criptográfico y no se relacionan directamente con la identidad personal de alguien.
- 4. Consenso:** Los mecanismos de consenso son fundamentales para el funcionamiento de la blockchain. Estos mecanismos permiten que los nodos de la red acuerden el estado de la blockchain y validan las transacciones proporcionando la base para tener un sistema de transacciones seguras y confiables (Bonneau et al., 2015). Existen una variedad de métodos de consenso siendo los más comunes el "Proof of Work" (Prueba de Trabajo) y el "Proof of Stake" (Prueba de Participación).
- 5. Contratos Inteligentes:** Los contratos inteligentes son programas que se ejecutan en la blockchain y permiten la automatización de procesos y acuerdos sin necesidad de intermediarios. Estos contratos se ejecutan de manera autónoma y se auto-verifican habilitando la realización de acuerdos y transacciones de forma segura y eficiente (Buterin, 2014). Los contratos inteligentes posibilitan la realización de transacciones y acuerdos de confianza entre diversas partes anónimas, sin requerir la intervención de una entidad central, un sistema jurídico o un mecanismo externo de aplicación.

No existe un conjunto fijo y universal de principios fundamentales establecidos para la tecnología blockchain. En ocasiones, algunos de estos principios se agrupan, mientras que en otras ocasiones se desglosan en principios más específicos. El listado anterior proporciona una selección de definiciones que busca ofrecer una visión general lo más precisa y completa posible de las características de la blockchain. En secciones posteriores se profundizará en más detalle en algunos de estos principios fundamentales.

2.1.4 Tipos de Blockchain

Como se ha visto en las secciones anteriores, aunque la tecnología blockchain tiene su primera implementación funcional con Bitcoin, el desarrollo posterior ha sido diverso dando lugar a la aparición de diversos tipos de blockchain. Estas variantes fueron diseñadas para satisfacer diferentes necesidades y escenarios de uso particulares. Aunque comparten principios fundamentales como la

descentralización o la seguridad basada en criptografía existen diferencias significativas en aspectos como el acceso, los participantes de la red y los métodos de validación de transacciones. En esta sección se realizará una introducción a los diferentes tipos existentes de blockchains describiendo sus características, ventajas y desafíos asociados. En la actualidad existen 4 tipos principales de blockchains:

- 1. Blockchain Pública:** Las blockchains públicas, también a veces denominadas blockchains abiertas, se caracterizan por ser de libre acceso, lo que significa que cualquier usuario puede participar en la red, realizar transacciones, verificar y añadir nuevas transacciones a la cadena, o leer los datos de la cadena. Bitcoin y Ethereum son ejemplos notables de blockchains públicas. Entre sus ventajas destaca su independencia de organizaciones, lo que significa que pueden seguir funcionando incluso si la organización original deja de existir. Además, la transparencia de la red es una ventaja, siempre y cuando los usuarios sigan los protocolos de seguridad. Entre las principales desventajas está que la red puede ser lenta, las empresas no pueden restringir el acceso o el uso y no escalan bien. Además, también tienen un riesgo de que hackers con más del 51% del poder de cómputo de la red puedan modificarla unilateralmente.
- 2. Blockchain Privada:** A diferencia de las públicas, las blockchains privadas o permissionadas se caracterizan por limitar la participación en la red. Solo los usuarios previamente autorizados pueden realizar transacciones y tener acceso a los datos de la cadena. Estas blockchains se usan generalmente en entornos empresariales o gubernamentales donde se necesita un mayor control sobre quién puede interactuar con la blockchain. La ventaja principal de las blockchains privadas es que la organización controladora puede establecer niveles de permisos, seguridad, autorizaciones y accesibilidad. Además, por regla general al ser de un tamaño más limitado pueden ser más rápidas. Algunas de las desventajas es su limitación en la filosofía de la descentralización pudiendo llegar a ser más difícil lograr plena confianza en la información debido a que los nodos centralizados determinan qué es válido. Además, un pequeño número de nodos puede implicar una menor seguridad.
- 3. Blockchain de Consorcio:** Las blockchains de consorcio representan un término medio entre las públicas y las privadas. En este tipo de blockchain, el proceso de verificación de las transacciones está controlado por un grupo preseleccionado de nodos, normalmente conformado por un consorcio de empresas o entidades. R3 Corda⁶ y Hyperledger Fabric⁷ son ejemplos de blockchains de consorcio. Este tipo de blockchains tienden a ser más seguras, escalables y eficientes que las redes de blockchain públicas y al igual que las blockchains privadas e híbridas, también ofrecen controles de acceso. Las desventajas son que son menos transparentes que las blockchains públicas.

⁶ <https://corda.net/>

⁷ <https://www.hyperledger.org/>

- 4. Blockchain Híbrida:** Este tipo de blockchain de manera similar a las de consorcio intenta combinar lo mejor de las blockchains públicas y privadas. Permiten que los propietarios de la red decidan quién puede participar en la red y qué transacciones se hacen públicas. Esto permite que las organizaciones tengan control sobre su propia información, a la vez que se mantiene transparente para el público lo que necesitan ver. Una de las principales ventajas de la blockchain híbrida es que, al trabajar dentro de un ecosistema cerrado, los hackers externos no pueden llevar a cabo un ataque del 51% en la red. También protege la privacidad pero permite la comunicación con terceros y suelen ser más rápidas y con mejor escalabilidad que una red de blockchain pública. La principal desventaja es que este tipo de blockchains no son completamente transparente debido a que la información puede ser protegida.

A continuación la tabla 1 presenta una comparación entre los diferentes tipos de blockchains expuestos.

Tabla 1. Comparativa de tipos de blockchain

Características	Blockchain Pública	Blockchain Privada	Blockchain de Consorcio	Blockchain Híbrida
Acceso	Abierto a todos	Requiere autorización	Limitado a un consorcio	Regulado pero con acceso público a ciertos datos
Control	Descentralizada	Centralizada	Compartido entre el consorcio	Compartido, con algunos aspectos centralizados
Seguridad	Alta (dependiente del consenso)	Alta (dependiente de la entidad que la controla)	Alta (controlada por el consorcio)	Alta (medidas de seguridad personalizables)
Velocidad	Puede ser lenta debido al consenso	Rápida debido a la menor cantidad de nodos	Depende del número de participantes en el consorcio	Variable, depende del diseño de la red
Principales Ventajas	<ul style="list-style-type: none"> ● Independencia ● Transparencia 	<ul style="list-style-type: none"> ● Control de accesos ● Escalabilidad 	<ul style="list-style-type: none"> ● Control de accesos ● Escalabilidad ● Seguridad 	<ul style="list-style-type: none"> ● Control de accesos ● Performance ● Seguridad
Principales	<ul style="list-style-type: none"> ● Performance 	<ul style="list-style-type: none"> ● Confianza 	<ul style="list-style-type: none"> ● Transparencia 	<ul style="list-style-type: none"> ● Transparencia

Desventajas	<ul style="list-style-type: none"> • Escalabilidad • Seguridad 		
-------------	--	--	--

2.1.5 Estructura de un Bloque

En la siguiente sección se explorará en detalle la estructura y el funcionamiento de un bloque, que constituye la entidad fundamental de la blockchain y es la base para el almacenamiento de la información en la red.

Un bloque en la tecnología blockchain va más allá de ser un simple contenedor de transacciones. Es un complejo mecanismo de almacenamiento de información con características únicas que garantizan la seguridad, integridad y transparencia de las transacciones. En su esencia, un bloque almacena una serie de transacciones, pero su estructura y funcionalidad se diseñan meticulosamente para brindar una solidez a la red.

Un bloque se compone de varios elementos clave como son el número de bloque, el hash del bloque anterior, el hash del bloque actual, una marca de tiempo, un nonce y una lista de transacciones. En la figura 3 se puede ver un ejemplo de la estructura interna de los bloques en una red de blockchain.

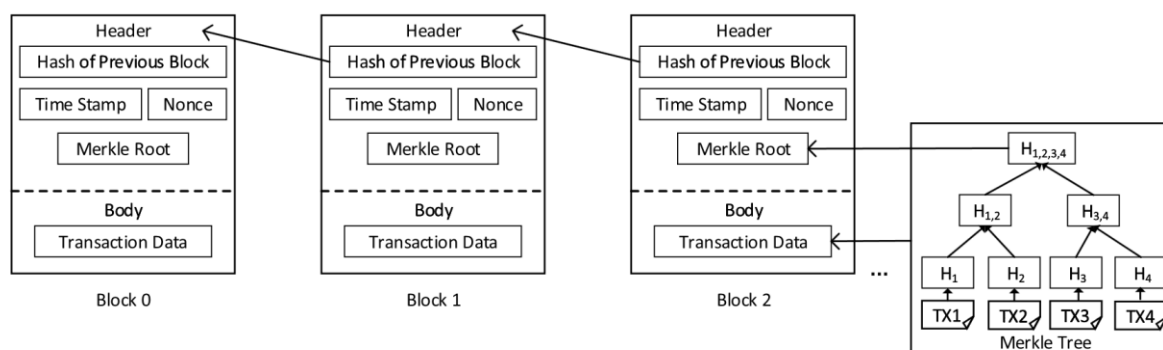


Figura 3. Estructura de bloques y Merkle Tree (Liang, 2020)

A continuación, se presentará una descripción más detallada de los componentes clave que conforman la estructura de un bloque en la tecnología blockchain. La tabla 2 presenta un resumen de los componentes de un bloque y sus funciones:

- **Número de bloque:** Es un identificador único asignado a cada bloque en la cadena de bloques. Este número es esencial para mantener un orden secuencial de los bloques en la cadena, lo que facilita la identificación, búsqueda y verificación de los bloques en la red. Además, el encabezado del bloque incluye tres conjuntos de metadatos específicos del bloque.
- **Hash del bloque anterior y actual:** Son códigos generados por un algoritmo de hash criptográfico. Un hash es una representación compacta de la información contenida en un bloque. Si bien de primeras puede parecer una serie aleatoria de números y letras, cada hash es único para cada bloque y cambia con cualquier modificación en la información del mismo.

Este carácter único y sensible de los hash es crítico para detectar y prevenir cualquier intento de alteración de los bloques. Cabe destacar que el hash del bloque actual no se incluye realmente dentro de la estructura de datos del bloque, como se puede ver en la figura 3, ni cuando se almacena en el almacenamiento persistente de un nodo como parte de la cadena de bloques. En cambio, cada nodo calcula el hash del bloque al recibirlo de la red (Antonopoulos, 2014).

- **Nonce:** Es un número que se utiliza una sola vez en la generación del hash del bloque. Es un elemento clave de la prueba de trabajo en el bloque (PoW). Los mineros ajustan este número repetidamente hasta que encuentran un nonce que, combinado con los datos del bloque, produce un hash que cumple con los criterios de la red.
- **Marca de tiempo:** Es un componente importante que proporciona información sobre cuándo se creó el bloque. Es una cadena de caracteres que identifica unívocamente el documento o evento e indica cuándo se creó. Esto garantiza la trazabilidad y la transparencia de las transacciones.
- **Transacciones:** Son la razón de ser de los bloques. Cada transacción en el bloque contiene información como la dirección del remitente, la dirección del receptor y la cantidad de criptomonedas transferidas (en el caso de las blockchains de criptomonedas). Estas transacciones se almacenan en una estructura de datos conocida como árbol de Merkle.
- **Árbol de Merkle:** Es un árbol binario que almacena los hash de las transacciones. Permite mapear eficientemente grandes cantidades de datos y detectar fácilmente cambios realizados en los datos (Szydlo, 2004). Cada nodo del árbol contiene el hash de los datos de transacción (en el caso de los nodos de las hojas) o el hash de los hash de sus nodos hijos (en el caso de los nodos internos). El nodo raíz del árbol, conocido como la raíz de Merkle, contiene un resumen de todas las transacciones en el bloque. Este diseño permite una verificación eficiente y segura de las transacciones.

Tabla 2. Componentes de un bloque

Componente	Descripción
Número de bloque	Identifica de forma única a cada bloque en la cadena.
Hash del bloque anterior	Enlaza el bloque con el bloque anterior en la cadena.
Hash del bloque actual	Proporciona una firma única para los datos del bloque.
Marca de tiempo	Proporciona un registro del momento en que se creó el bloque.
Nonce	Se utiliza para la minería de bloques y garantiza la integridad de la

	cadena.
Lista de transacciones	Contiene todas las transacciones registradas en el bloque.
Árbol de Merkle	Estructura de datos que agrupa los hash de las transacciones.

Es importante comprender la estructura y función de los bloques en la cadena de bloques para tener un conocimiento completo de esta tecnología. Asimismo, es importante reconocer los distintos tipos de bloques presentes en una cadena de bloques. En concreto, existen tres tipos principales: bloque de génesis, bloques válidos y bloques huérfanos.

- 1. Bloque Génesis:** El bloque de génesis es el primer bloque de cualquier cadena de bloques. Fue ideado por Satoshi Nakamoto al lanzar Bitcoin (Nakamoto, 2008). Actúa como la piedra angular de la cadena, estableciendo el precedente para los bloques posteriores. Dado que no hay un bloque anterior al bloque de génesis, el hash del bloque anterior en este bloque se establece típicamente en cero. Sin el bloque de génesis, sería imposible iniciar una cadena de bloques ya que cada bloque subsiguiente necesita el hash del bloque anterior para su creación.
- 2. Bloques Válidos:** Un bloque válido es un bloque que ha sido añadido a la cadena de bloques principal. Este bloque cumple con todas las reglas y protocolos establecidos por la red. Por ejemplo, todas las transacciones dentro del bloque son válidas y el hash del bloque cumple con el nivel de dificultad establecido por la red (en el caso de que se use la prueba de trabajo). Un bloque válido también incluye un hash que enlaza correctamente con el bloque anterior en la cadena principal. Este enlace crea una cadena inmutable de bloques que se remonta al bloque génesis.
- 3. Bloques Huérfanos:** También conocidos como bloques estancados, son bloques que no se incluyen en la cadena de bloques principal. Estos bloques son válidos en sí mismos ya que cumplen con todas las reglas y protocolos de la red. Sin embargo, no forman parte de la cadena principal porque otro bloque, que también contiene el hash del mismo bloque anterior, se añadió a la cadena principal antes que ellos. Los bloques huérfanos suelen ser el resultado de la competencia entre los mineros para resolver el rompecabezas criptográfico y añadir el próximo bloque a la cadena. La red eventualmente resolverá este conflicto aceptando el bloque que forma parte de la cadena más larga y relegando el otro bloque al estado de huérfano.

2.2 Funcionamiento de blockchain

2.2.1 Creación de transacciones

En el marco de la tecnología blockchain, una transacción denota cualquier operación que causa un cambio de estado en la cadena de bloques. Estos cambios pueden variar desde la transferencia de activos digitales, como las criptomonedas, hasta la ejecución de operaciones establecidas por contratos inteligentes (Gupta & Sadoghi, 2021).

Una transacción en la cadena de bloques consta de varios elementos esenciales que posibilitan su procesamiento y posterior validación. Estos elementos son:

- **ID del remitente:** Es la identificación única del individuo o entidad que inicia la transacción. El ID del remitente se genera a partir de una clave pública, la cual se deriva de una clave privada. Aquel que posee la clave privada tiene un control absoluto sobre los activos vinculados a la clave pública correspondiente (Stephen & Alex, 2018).
- **ID del destinatario:** Similar al ID del remitente, es una identificación única que señala al receptor de la transacción.
- **Cantidad o tipo de datos:** Este elemento se refiere a los activos o información que se transfieren en la transacción. En blockchains como Bitcoin, esto suele referirse a una cantidad específica de criptomonedas. Sin embargo, en cadenas de bloques más versátiles como Ethereum, esto puede referirse a una amplia gama de activos digitales o datos (Buterin, 2014).
- **Firma digital:** Es un elemento clave para mantener la seguridad e integridad de la transacción. La firma digital se crea con la clave privada del remitente, certificando que el remitente es realmente el propietario de los activos que se transfieren y que ha autorizado la transacción (Fang et al., 2020).
- **Datos adicionales (opcional):** Este componente se utiliza en blockchains más avanzadas que admiten contratos inteligentes. Los datos adicionales pueden ser instrucciones o información adicional que un contrato inteligente necesita para ejecutar una función específica (Buterin, 2014)

El proceso de creación de una transacción comienza cuando el remitente forma un mensaje que incluye los detalles de la transacción. Este mensaje se firma digitalmente usando la clave privada del remitente, resultando en una firma digital. Esta firma actúa como una prueba criptográfica de que la transacción ha sido aprobada por el remitente y verifica la integridad del mensaje. Además, el remitente no puede negar haber enviado el mensaje, ya que la firma digital se basa en su clave privada, que es única y exclusiva del remitente. El uso de claves privadas y públicas, en combinación con la firma digital, se representa en la figura 4.

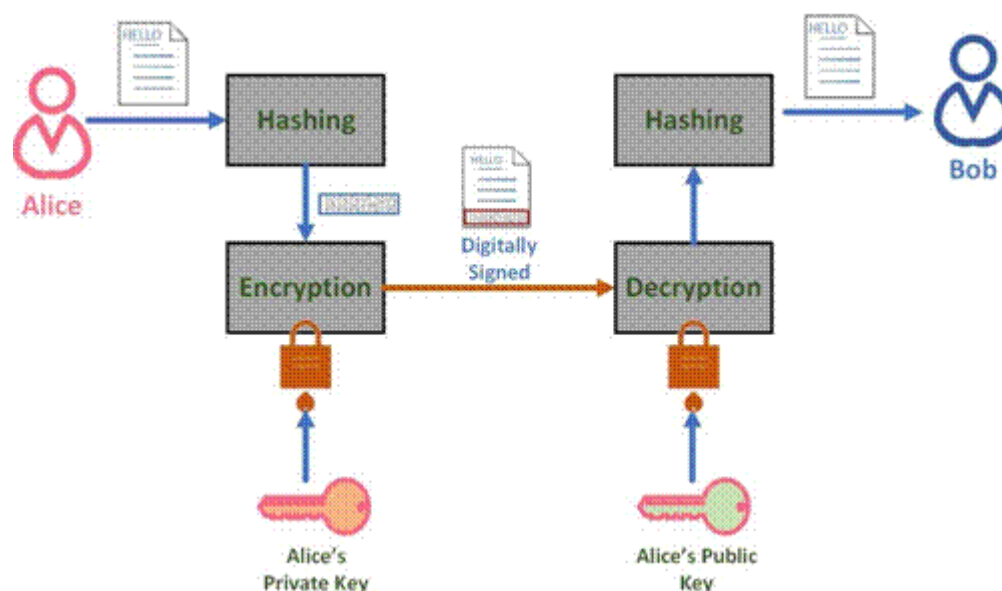


Figura 4. Firma digital (CB, 2023)

Siguiendo el ejemplo de la figura 4, el proceso comienza con la creación de un resumen del mensaje (message digest) del documento usando una función de hash criptográfica. El message digest es una representación numérica de tamaño fijo del contenido de un mensaje, calculada mediante una función hash (IBM, 2023). A continuación, Alice cifra el resumen del mensaje con su clave privada. Luego, añade el resumen del mensaje cifrado al documento original y envía el mensaje combinado. Al recibir el mensaje combinado de Alice, Bob separa el resumen del mensaje cifrado del propio documento. Bob utiliza la clave pública de Alice para descifrar el resumen del mensaje cifrado. Además, Bob calcula el resumen del mensaje del documento recibido y compara el resumen del mensaje resultante con el resumen del mensaje descifrado para ver si coinciden. Si hay coincidencia, Bob puede estar seguro de que el documento proviene de Alice sin ninguna manipulación.

La transacción se transmite a la red blockchain. Normalmente esta transmisión se realiza a través de un nodo al que el remitente está conectado. A partir de este nodo la transacción se propaga a lo largo de la red hasta los demás nodos. Los mineros o validadores de la red recogen la transacción transmitida. Estos actores verifican la validez de la transacción confirmando que la firma digital coincide con la dirección del remitente y que los fondos o datos son válidos y están disponibles. Si la transacción es válida se incluirá en un nuevo bloque en la cadena. Este nuevo bloque se enlaza al bloque anterior en la cadena.

2.2.2 Agrupación de transacciones en bloques

Una vez creada y transmitida, una transacción pasa por un proceso de validación y agrupación en bloques.

Comenzando con la recolección de transacciones. Los mineros o validadores de la red recogen las transacciones transmitidas en la misma. Estos nodos buscan constantemente transacciones validadas en la red, recolectando estas para procesarlas en el siguiente bloque de la cadena. Es importante mencionar que los mineros o validadores pueden tener ciertas reglas para seleccionar qué transacciones incluir. Como dar preferencia a las transacciones que incluyen tarifas más altas en blockchains donde se aplican tarifas por transacción, como en el caso de Bitcoin (Antonopoulos, 2017).

Una vez recolectadas las transacciones, el minero o validador comienza a crear un nuevo bloque. Estos bloques, como ya se ha visto anteriormente, no solo consiste en la transacción, sino que contienen información importante que ayuda a mantener la integridad y seguridad de la cadena de bloques.

Una vez validado, el bloque se propaga a través de la red. Otros nodos en la red verifican la validez del bloque y, si se considera válido, se añade a la cadena de bloques de cada nodo, registrando las transacciones de manera permanente en la red y haciendo que los cambios de estado representados por las transacciones se consideren "confirmados".

2.2.3 Proceso de validación

La validación es un componente crítico en el funcionamiento de la blockchain. Este proceso garantiza que todas las transacciones y bloques cumplen con las reglas de la red, lo que mantiene la integridad y la seguridad de la cadena de bloques.

Cada transacción en una cadena de bloques debe ser validada antes de que pueda ser incluida en un bloque. Esto puede implicar varias comprobaciones:

- **Verificación de la firma digital:** Se comprueba que la firma digital de la transacción se ha creado con la clave privada correspondiente a la dirección del remitente. Esto garantiza que el remitente de la transacción es realmente quien dice ser (Kewell et al., 2017).
- **Verificación de los fondos:** Se verifica que el remitente tiene suficientes fondos (o el activo apropiado) para realizar la transacción. Esta comprobación se realiza consultando el estado actual de la cadena de bloques (Godfrey-Welch et al., 2018).
- **Verificación de doble gasto:** Se comprueba que los fondos que se están gastando no se han gastado ya en otra transacción. Esto se logra revisando las transacciones anteriores en la cadena de bloques (Nakamoto, 2008).

Si una transacción supera todas estas comprobaciones se considera válida y puede ser incluida en el siguiente bloque.

Después de recopilar un conjunto de transacciones en un bloque, el bloque también debe ser validado antes de poder ser añadido a la cadena de bloques. La validación del bloque depende en gran medida del protocolo de consenso utilizado en la red. En el caso de la prueba de trabajo (PoW) que es utilizada por muchas cadenas de bloques, incluyendo Bitcoin, la validación implica resolver un problema

criptográfico. El primer minero que resuelve este problema valida el bloque y se le concede el derecho a añadirlo a la cadena (Nakamoto, 2008).

Una vez que un bloque es validado se propaga a través de la red y cada nodo realiza una serie de comprobaciones para asegurarse de que el bloque es válido antes de añadirlo a su propia copia de la cadena de bloques. Esto incluye verificar que todas las transacciones en el bloque son válidas, que la solución al problema criptográfico es correcta (en el caso de la prueba de trabajo) y que el bloque incluye un hash correcto del bloque anterior, lo que garantiza la continuidad de la cadena.

2.2.4 Consenso y resolución de conflictos

En blockchain, el consenso es un mecanismo esencial que permite a todos los participantes acordar un estado único y coherente de la cadena a pesar de estar descentralizada y distribuida en muchos nodos diferentes. El protocolo de consenso asegura que todas las transacciones sean procesadas en el orden correcto y que los conflictos sean resueltos.

Existen varios tipos de protocolos de consenso en la tecnología blockchain. Cada uno con sus propias ventajas y desventajas. Los más conocidos incluyen (Lashkari & Musilek, 2021):

- **Prueba de trabajo (Proof of Work - PoW):** Este mecanismo se hizo popular gracias a su implementación en Bitcoin. En PoW los mineros compiten entre sí para resolver problemas matemáticos complejos. Estos problemas requieren una gran cantidad de poder de cómputo y los mineros deben demostrar que han realizado un trabajo significativo para encontrar una solución. El primer minero en resolver el problema con éxito tiene el derecho de agregar el siguiente bloque a la cadena de bloques y recibir una recompensa por ello. La dificultad de los problemas se ajusta automáticamente para mantener una tasa constante de generación de bloques. Aunque PoW ha demostrado ser seguro y confiable también es conocido por su alto consumo de energía y la competencia entre los mineros.
- **Prueba de participación (Proof of Stake - PoS):** En PoS los validadores son seleccionados en función de la cantidad de tokens que poseen. Un token es una representación digital de un activo o un conjunto de reglas que se encuentra almacenado en una cadena de bloques. Funciona como un activo virtual que puede tener diferentes usos como ser una criptomoneda como Bitcoin o Ether, o representar derechos de voto o licencias. En lugar de competir por resolver problemas matemáticos los validadores son elegidos de manera determinística y las probabilidades de ser seleccionado aumentan proporcionalmente a la cantidad de tokens apostados. Los validadores seleccionados tienen la responsabilidad de validar transacciones y crear nuevos bloques. Este enfoque reduce drásticamente el consumo de energía en comparación con PoW ya que no se requiere un proceso intensivo de resolución de problemas. Ethereum cambió de PoW a PoS con su actualización llamada Ethereum 2.0 en 2022.

- **Prueba de participación delegada (Delegated Proof of Stake - DPoS):** DPoS es una variante de PoS en la que los titulares de tokens votan y eligen a delegados para validar los bloques en su nombre. En lugar de que todos los titulares de tokens participen directamente en el proceso de validación, se elige a un grupo reducido de delegados. Estos delegados tienen la responsabilidad de mantener la seguridad y la integridad de la red. DPoS es conocido por ser escalable y eficiente en términos de consumo de energía pero también se considera más centralizado ya que los delegados tienen cierto grado de poder y toma de decisiones.
- **Prueba de quemado (Proof of Burn - PoB):** En PoB los usuarios queman una cantidad determinada de tokens al enviarlos a una dirección inaccesible sin claves privadas. La quema de tokens demuestra el compromiso y la dedicación de los usuarios hacia la red. A cambio de quemar sus tokens los usuarios obtienen el derecho de participar en la creación de nuevos bloques y recibir recompensas proporcionales. Este mecanismo tiene como objetivo mejorar la escasez de tokens y aumentar la seguridad de la red ya que los usuarios deben sacrificar sus propios tokens para obtener la capacidad de minar.
- **Prueba de autoridad (Proof of Authority - PoA):** PoA es un mecanismo de consenso centralizado que es adecuado para redes de blockchain privadas como redes empresariales o gubernamentales. En PoA, una entidad central o una autoridad asigna nodos específicos para crear nuevos bloques y validar transacciones. Estos nodos, conocidos como autoridades, son confiables y conocidos por todos los participantes de la red. La ventaja de PoA es su alta eficiencia y velocidad en comparación con otros mecanismos de consenso. Sin embargo, la desventaja es que la red se vuelve menos descentralizada ya que la autoridad central tiene el poder de tomar decisiones y modificar transacciones si así lo decide.

La resolución de conflictos es un elemento integral y esencial en la tecnología de blockchain. A medida que la red se expande y se vuelve cada vez más descentralizada, las probabilidades de conflictos aumentan significativamente. Los conflictos más comunes que surgen en la red blockchain están relacionados con las transacciones y la adición de bloques a la cadena. Para garantizar la fiabilidad y la seguridad de la red, estos conflictos deben resolverse de manera eficiente y justa.

El protocolo de consenso, por su papel esencial en la cadena de bloques, tiene la función crucial de resolver conflictos. Define las reglas que los nodos de la red deben seguir para agregar nuevos bloques a la cadena. Al mismo tiempo, proporciona un mecanismo de resolución de conflictos que permite a la red continuar operando de manera eficiente a pesar de los desacuerdos inevitables que surgen entre los nodos.

Un ejemplo clásico de conflicto en la red blockchain es cuando dos mineros crean un nuevo bloque válido al mismo tiempo. En este escenario diferentes partes de la red pueden recibir información sobre los dos bloques nuevos en un orden diferente, lo que puede llevar a una bifurcación en la cadena. Sin un mecanismo de resolución de conflictos efectivo esto podría llevar a la creación de dos cadenas de bloques paralelas poniendo en peligro la coherencia y la seguridad de la red.

La resolución de este conflicto depende del protocolo de consenso específico que utilice la red blockchain. En la prueba de trabajo (PoW) se resuelve favoreciendo la cadena más larga. La longitud

de la cadena en PoW se mide por la cantidad de trabajo computacional que se ha invertido en ella. Así, cuando ocurre una bifurcación, los mineros tienden a trabajar en la cadena en la que creen, pero eventualmente se unen a la cadena más larga ya que esa cadena tiene una mayor probabilidad de ser aceptada por otros nodos. Esto asegura que cualquier trabajo realizado en la cadena más corta se desperdicia, desincentivando a los mineros de continuar trabajando en cadenas más cortas. Como resultado, la cadena más larga prevalece y la cadena más corta se descarta.

2.2.5 Seguridad

Como se vio en la sección anterior, la seguridad es un pilar fundamental de la tecnología blockchain. En una red blockchain, la seguridad se sostiene sobre una serie de características fundamentales de la red. Entre los principales están:

- **Descentralización:** Una característica clave de la mayoría de las redes blockchain es su naturaleza descentralizada por diseño. Esto significa que, en lugar de estar almacenado en un único servidor central o controlado por una única entidad, el libro de contabilidad de la cadena de bloques está distribuido en muchos nodos diferentes. Como se ha visto, cada uno de estos nodos mantiene una copia de toda la cadena de bloques. Esta configuración garantiza que incluso si un solo nodo o un grupo de nodos fallara o fuera atacado, la información de la cadena de bloques seguiría estando segura e intacta en los demás nodos. Además, como ninguna entidad tiene el control total de la cadena de bloques, resulta extremadamente difícil para cualquier actor malintencionado manipular los datos de la cadena. Para modificar la cadena de bloques, sería necesario controlar al menos el 51% de los nodos (Ye et al., 2018), lo que resulta muy difícil y costoso desde el punto de vista técnico, por lo que proporciona una importante capa de seguridad.
- **Criptografía:** La criptografía es el elemento fundamental de la seguridad de la blockchain. Como también se ha visto, se utilizan dos conceptos criptográficos principales: hashing y firmas digitales. El hashing se utiliza para garantizar la integridad de los datos y las firmas digitales para garantizar la autenticidad y el no repudio.
- **Mecanismos de consenso:** Los mecanismos de consenso garantizan que todos los nodos de la red están de acuerdo sobre el estado de la cadena de bloques compartida. Diseñados para manejar situaciones en las que los nodos pueden tener versiones contradictorias de la cadena de bloques debido a la naturaleza descentralizada de la red.
- **Libro mayor inmutable:** Una de las características fundamentales de la tecnología blockchain es la inmutabilidad de sus datos. Una vez que un bloque se ha añadido a la cadena de bloques es prácticamente imposible alterar o borrar la información que contiene (Politou et al., 2019). Si un atacante quisiera alterar un bloque tendría que cambiar la información de ese bloque y de todos los bloques posteriores, y luego superar la adición de nuevos bloques a la red. Esto requeriría un esfuerzo computacionalmente muy elevado haciéndolo prácticamente inviable, en especial en cadenas de bloques grandes y bien establecidas.

- **Transparencia:** En muchas redes blockchain, todas las transacciones que se producen son visibles para todos los participantes en la red. Esta transparencia permite a todos verificar las transacciones garantizando de esta manera la integridad de la red (Stephen & Alex, 2018). También actúa como elemento disuasorio para las actividades fraudulentas debido a que cualquier acción de este tipo es visible públicamente y puede rastrearse con facilidad. Además, la transparencia también permite un alto grado de auditabilidad ya que todo el historial de transacciones de la cadena de bloques está disponible para su revisión.
- **Pseudo-Anonimato:** La tecnología Blockchain permite a los usuarios realizar transacciones hasta cierto nivel preservando su privacidad. Cada usuario se identifica mediante una dirección (cadena de números y letras) y aunque todas las transacciones asociadas a esa dirección son públicas, la identidad real de la persona detrás de la dirección puede permanecer oculta. Este seudónimo proporciona a los usuarios cierto grado de privacidad, al tiempo que garantiza que la red siga siendo transparente y que todas las transacciones puedan auditarse. Algunas blockchains ofrecen incluso características adicionales para mejorar la privacidad de los usuarios, como los zk-SNARK utilizados por Zcash, que permiten a los usuarios demostrar que poseen cierta información sin revelarla (Petkus, 2019).

2.2.6 Interoperabilidad con otros sistemas

En el contexto de las tecnologías de la información, la interoperabilidad se refiere a la capacidad de diferentes sistemas y tecnologías para trabajar en conjunto, es decir, para intercambiar y hacer uso de la información de manera efectiva (Wegner, 1996). Para la tecnología blockchain la interoperabilidad es un aspecto clave debido a que influye en cómo se puede integrar y usar en conjunción con otros sistemas y/o redes blockchain existentes. Dada la creciente proliferación de diferentes redes blockchain, cada una diseñada con sus propios protocolos y estándares, este aspecto se vuelve cada vez más crucial.

- **Interoperabilidad entre Blockchains:** Con el creciente interés en las tecnologías blockchain existe una creciente necesidad de permitir la interacción y el intercambio de información entre estas. Este tipo de interoperabilidad es esencial para permitir la transferencia de activos y datos entre diferentes blockchains pudiendo maximizar su utilidad y eficiencia. En la actualidad existen varios enfoques para intentar abordar este problema. Por ejemplo, las cadenas de bloques denominadas "puente" funcionan como intermediarios, facilitando la comunicación entre dos blockchains diferentes al poder interpretar y transmitir transacciones de una cadena a otra (Stone, 2021). Otra de las soluciones son los protocolos de interconexión de blockchains, como Polkadot y Cosmos, que permiten que diferentes blockchains operen en un marco unificado, lo que facilita la interoperabilidad. Estos sistemas operan a través de un 'hub' central o cadena de bloques de relevos que puede interactuar con varias cadenas de bloques, permitiendo el intercambio de información y transacciones (Zamyatin et al., 2019).
- **Interoperabilidad con otros sistemas informáticos:** La interoperabilidad no solo se limita a la comunicación entre diferentes blockchains, sino que también se extiende a la integración de

blockchain con otros sistemas informáticos existentes como pueden ser una base de datos tradicional o el sistemas de gestión de suministros de una empresa. Esta capacidad de interacción puede ser crítica para que una organización adopte la tecnología blockchain. Las API (Interfaz de Programación de Aplicaciones) se utilizan comúnmente para lograr esta integración, actuando como un 'puente' entre la red blockchain y el sistema existente. Las API proporcionan un conjunto de reglas y protocolos estandarizados para cómo los diferentes programas de software deben interactuar, permitiendo una integración eficiente entre diferentes sistemas (RedHat, 2022).

A medida que siga evolucionando la tecnología blockchain será crucial que se siga trabajando en mejorar la interoperabilidad tanto entre diferentes redes blockchain como entre blockchain y otros sistemas informáticos. Estos avances permitirán la integración más fluida de la blockchain en diversos sectores y la expansión de sus aplicaciones.

2.2.7 Smart Contracts

Los contratos inteligentes, o smart contracts, son un componente crítico y revolucionario en el ecosistema blockchain. Originalmente propuestos por el criptógrafo Nick Szabo en 1994, previo a la aparición de blockchain, son esencialmente programas de ordenador almacenados en una cadena de bloques que se ejecutan automáticamente cuando se cumplen determinadas condiciones predefinidas (Szabo, 1997).

- **Definición y Características de los Smart Contracts:** Un contrato inteligente es un protocolo autoejecutable que facilita, verifica y aplica la negociación o el cumplimiento de un contrato previamente definido. Está escrito en forma de código de ordenador en vez de un lenguaje legal y sus cláusulas están directamente vinculadas a transacciones en la cadena de bloques. Los contratos inteligentes son importantes porque pueden eliminar la necesidad de intermediarios en una amplia gama de aplicaciones desde transacciones financieras hasta acuerdos de uso compartido de datos.
- **Funcionamiento de los Smart Contracts:** Los contratos inteligentes operan en la lógica "if-then" (si esto, entonces aquello). Por ejemplo, en el caso de un contrato de seguro de vuelo, si este se cancelará (condición "if"), entonces el asegurado recibiría un pago compensatorio (condición "then"). Esta lógica es fundamental para permitir contratos que se auto-ejecutan y se auto-verifiquen, eliminando la necesidad de intermediarios humanos y permitiendo establecer un alto grado de automatización. Además, dentro de un contrato inteligente, puede haber tantas estipulaciones como sea necesario para satisfacer a los interesados de que la tarea se completará satisfactoriamente. En la figura 5 se puede ver el flujo de desarrollo de un contrato inteligente (GG, 2022):
 - a. **Identificación del acuerdo:** Varias partes identifican una oportunidad de cooperación y los resultados deseados.

- b. **Establecimiento de condiciones:** Los contratos inteligentes pueden ser iniciados por las partes involucradas o cuando se cumplen ciertas condiciones externas a la red.
 - c. **Codificación de la lógica:** Se escribe un programa informático que se ejecutará automáticamente cuando se cumplan los parámetros condicionales establecidos y acordados.
 - d. **Encriptación y tecnología blockchain:** El programa se encripta y se introduce en la cadena de bloques proporcionando autenticación segura y transferencia de mensajes entre las partes en relación con los contratos inteligentes.
 - e. **Ejecución y procesamiento:** En la iteración de blockchain, cada vez que se alcanza un consenso entre las partes en lo que respecta a la autenticación y la verificación, el código se ejecuta y los resultados se registran para su cumplimiento y verificación.
 - f. **Actualizaciones de la red:** Una vez que se ejecutan los contratos inteligentes, todos los nodos de la red actualizan su libro mayor para reflejar el nuevo estado. Una vez que el registro se publica y verifica en la red de blockchain, no puede ser modificado.
- **Usos de los Smart Contracts:** Los contratos inteligentes pueden tener aplicaciones en diversas industrias. En el sector financiero, pueden mejorar la eficiencia de las transacciones y los pagos. En la venta de billetes, pueden gestionar el consentimiento para compartir datos o automatizar reclamaciones de seguros. En el ámbito legal, pueden agilizar la ejecución de contratos.
 - **Beneficios de los Smart Contracts:** Los contratos inteligentes brindan una serie de beneficios como la velocidad, eficiencia y precisión, ya que las operaciones se ejecutan automáticamente una vez que se cumplen las condiciones, eliminando papeleo y posibles errores humanos. Al operar sin intermediarios y compartir registros encriptados de transacciones entre participantes, se garantiza confianza y transparencia, sin temor a la alteración de la información. Su naturaleza encriptada y la interconexión de registros en una cadena de bloques hacen que los contratos inteligentes sean muy seguros, prácticamente inmunes a los ataques de hackers. Además, la eliminación de intermediarios reduce significativamente los costos asociados, pudiendo resultar en ahorros de costes.
 - **Desafíos y Limitaciones de los Smart Contracts:** Sin embargo, los contratos inteligentes también presentan ciertos desafíos. Su naturaleza inmutable significa que una vez que se implementa un contrato inteligente, no puede ser modificado, lo que puede ser problemático si hay errores en el código. Los contratos inteligentes también pueden enfrentarse a problemas legales y regulatorios debido a la actual falta de un marco legal claro para su uso.

How does a Smart Contract Work?

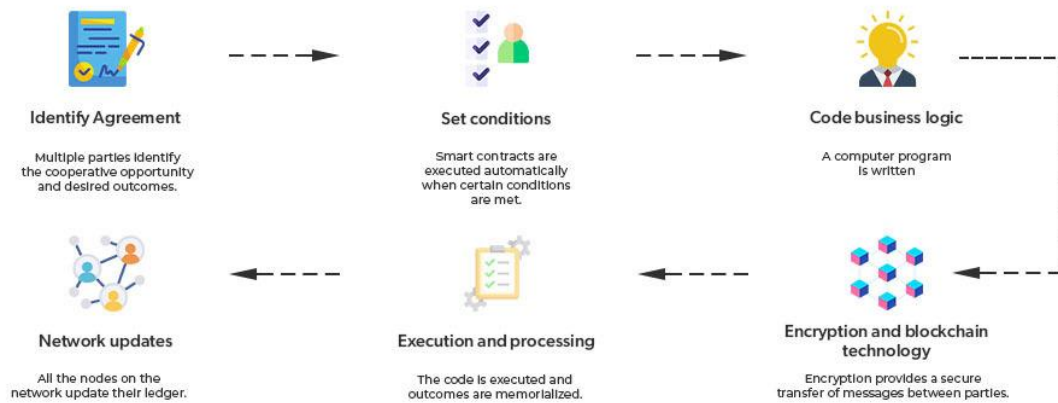


Figura 5. Smart contract workflow (GG, 2022)

2.3 Beneficios y limitaciones de la tecnología blockchain

2.3.1 Beneficios de la Blockchain

La tecnología blockchain está transformando el futuro de diversas industrias con su potencial innovador. Existen numerosos estudios tanto en el ámbito técnico (Atlam et al., 2020; Ali et al., 2021) como en el socioeconómico (Swan, 2017), que han identificado y resaltado algunos de los beneficios que tiene esta tecnología. Estos beneficios se originan en las características fundamentales de la blockchain como la descentralización, inmutabilidad, transparencia y seguridad (Zheng et al., 2018). A continuación, se desarrollará con más detalle los principales beneficios derivados del uso de la tecnología blockchain.

- 1. Seguridad y Privacidad:** La seguridad es un fundamento básico de la tecnología blockchain. Los datos sensibles y/o cruciales son protegidos mediante encriptación de extremo a extremo y almacenados en un registro inmutable, lo cual ayuda a prevenir el fraude y la actividad no autorizada (Zhang et al., 2019). Además, los problemas de privacidad pueden ser abordados en blockchain al anonimizar los datos personales y usar permisos para prevenir el acceso no autorizado.
- 2. Transparencia:** A diferencia de las bases de datos centralizadas, la blockchain emplea un sistema de registro distribuido. Esto implica que las transacciones y datos se duplican y almacenan en varios nodos de la red de manera idéntica (Tapscott & Tapscott, 2016). Esta característica garantiza que todos los participantes autorizados de la red tengan acceso simultáneo a la misma información otorgando una transparencia total al sistema. Este nivel de visibilidad prácticamente imposibilita la posibilidad de fraude ya que los participantes

pueden revisar íntegramente el historial de una transacción, incluyendo sus correspondientes marcas de tiempo.

3. **Trazabilidad e Inmutabilidad:** En la blockchain, cada transacción se registra de manera inmutable en la cadena de bloques, lo que genera un rastro de auditoría claro y verificable. Esta característica no solo facilita el seguimiento del origen y el seguimiento de los productos, sino que también fortalece la confianza en los procesos comerciales al permitir la verificación de autenticidad y aumentar la protección contra la falsificación y/o el fraude (Yaqoob et al., 2021).
4. **Coste:** La tecnología blockchain reduce los costos asociados con el ajuste y mantenimiento de servidores centralizados grandes al utilizar la capacidad de procesamiento de dispositivos de comunicación, a diferencia de las arquitecturas centralizadas que requieren un sistema completo de hardware y software avanzado para construir un servidor centralizado (Christidis & Devetsikiotis, 2016).
5. **Mayor Eficiencia y Velocidad:** La blockchain puede agilizar los procesos tradicionales que dependen en gran medida del papel y que son propensos a errores humanos. Se elimina la necesidad de intermediarios e intercambiar documentos en papel (o incluso digitales) así como la posible necesidad de conciliar bases de datos permitiendo la definición y ejecución de procesos mucho más eficientes.
6. **Automatización y Autonomía:** Las transacciones en la blockchain pueden incluso ser automatizadas mediante "contratos inteligentes", que aumentan aún más la eficiencia y velocidad del proceso (Christidis & Devetsikiotis, 2016). Los contratos inteligentes reducen la intervención humana y la dependencia de terceros para verificar que se han cumplido las condiciones de un contrato.

2.3.2 Limitaciones de la Blockchain

La tecnología blockchain ofrece numerosos beneficios, como se ha destacado en la sección anterior. No obstante, al evaluar su utilización, es esencial tener en cuenta ciertas limitaciones que podrían surgir en su implementación (Hughes et al., 2019). Es necesario comprender estas restricciones para que usuarios y organizaciones evalúen de manera más completa y precisa si esta tecnología es la opción adecuada para sus necesidades específicas. A continuación, se detallarán las principales posibles limitaciones derivadas del uso de la tecnología blockchain.

1. **Escalabilidad:** La blockchain al contrario que servicios más centralizados suele presentar problemas en términos de escalabilidad debido a su diseño descentralizado y a la necesidad de consenso entre los nodos de la red (Chauhan et al., 2018). A medida que aumenta el número de transacciones, la capacidad de procesamiento de la blockchain puede verse limitada, lo que resulta en posibles retrasos y congestión en la red. Aunque cabe destacar que

este problema es mayor en redes públicas debido a su tamaño en comparación con redes privadas, de consorcio o híbridas.

2. **Gobernanza:** La naturaleza distribuida del blockchain ofrece ventajas significativas para casos de uso específicos, pero puede ser una limitación en términos de control y gobernanza para organizaciones basadas en supervisión centralizada (Rikken et al., 2019). Aunque la descentralización brinda transparencia y seguridad, las entidades de supervisión pueden encontrar dificultades para ejercer un control total sobre la red, ya que las decisiones se toman colectivamente por los participantes. La ausencia de una entidad central puede dificultar la implementación de cambios rápidos y la aplicación de regulaciones específicas. Además, la responsabilidad de mantener y actualizar la red recae en los participantes individuales, lo que puede generar inconsistencias en los datos.
3. **Costes:** A medida que una cadena de bloques crece el almacenamiento de datos se puede convertir en un cuello de botella. Por su naturaleza, cada nodo de la red debe almacenar una copia completa de la cadena lo que puede requerir una capacidad de almacenamiento considerable. Esto puede generar costes adicionales, especialmente en el caso de aplicaciones que manejan grandes cantidades de datos (Ismail et al., 2022).
4. **Regulación y cumplimiento normativo:** La tecnología blockchain presenta desafíos en términos de regulación y cumplimiento normativo. La naturaleza descentralizada y la falta de una autoridad centralizada dificultan la aplicación de leyes y regulaciones en ciertos casos, como la protección de datos personales y la prevención de actividades ilícitas (Fabiano, 2017; Hughes et al., 2019).
5. **Interoperabilidad:** La falta de estándares comunes en la tecnología blockchain puede obstaculizar la interoperabilidad entre plataformas y cadenas de bloques (Belchior et al., 2021). Las blockchains se basan en reglas únicas para alcanzar un consenso descentralizado y seguro sobre la precisión de las transacciones. Sin embargo, este consenso sólo es aplicable internamente y no se puede lograr verificación fuera del blockchain o en la comunicación entre diferentes aplicaciones. Como resultado, se limita la capacidad de transferir datos y activos entre distintos ecosistemas blockchain, lo que dificulta la adopción generalizada y la colaboración entre proyectos diversos.
6. **Consumo energético:** Las aplicaciones basadas en blockchain suelen requerir de una gran cantidad de energía. Esto se da generalmente en aquellas redes que utilizan algoritmos de consenso como el de prueba de trabajo (PoW). Estos implican la resolución de complejos problemas matemáticos lo que consume una cantidad significativa de recursos energéticos. Se ha llegado a estimar que Bitcoin consume entre 60 y 125 TWh al año, un consumo similar al de países como Austria o Noruega (Sedlmeir et al., 2020). Esto plantea preocupaciones en términos de sostenibilidad y huella de carbono.

A pesar de estas limitaciones, el potencial disruptivo de la tecnología blockchain continúa impulsando su investigación y desarrollo. A medida que se abordan estas limitaciones y se realizan avances en la tecnología, es probable que la implementación de la tecnología blockchain se extienda y llegue a desempeñar un papel cada vez más importante en la transformación digital de diversas industrias.

3. Blockchain en la industria aeronáutica

3.1 Potenciales beneficios de la implementación de blockchain en la aviación

En las secciones anteriores se ha explorado la historia, beneficios y limitaciones de la tecnología blockchain. Cada avance tecnológico tiene el potencial de revolucionar diferentes industrias mejorando la eficiencia, seguridad y sostenibilidad. La aviación no es una excepción en este contexto. Con su compleja interconectividad y organización de múltiples agentes a nivel internacional, la aviación presenta un escenario propicio para implementar una transformación a través de la tecnología blockchain.

En el análisis exhaustivo que se presenta en este capítulo, se explorarán en detalle las diversas posibles aplicaciones de la tecnología blockchain en el sector de la aviación. Estas aplicaciones abarcan desde la gestión de identidades y emisión de billetes, hasta la gestión del espacio aéreo y la integración de sistemas aéreos no tripulados (UAS).

3.1.1 Gestión de identidades de pasajeros (Passenger Identity Management)

Por lo general, la seguridad de una industria depende de la capacidad para identificar de manera precisa a los principales usuarios y proveedores de servicios que interactúan en su complejo ecosistema. Esta necesidad es aún más relevante en el entorno internacional de la aviación.

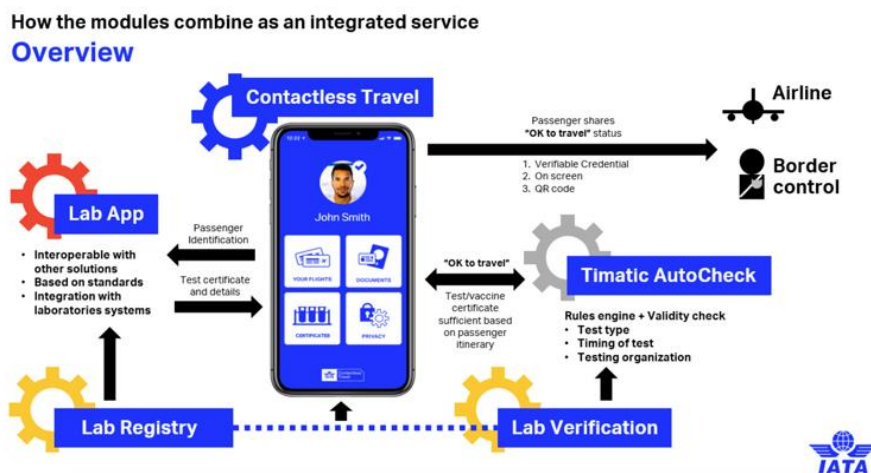


Figura 6. IATA Travel Pass basado en tecnología blockchain

Tradicionalmente, la verificación de la identidad en la aviación implica la comprobación manual de documentos, lo que puede ser costoso en cuanto a tiempo y ser propenso a errores. Además, estos sistemas centralizados son vulnerables a las filtraciones de datos y al posible fraude de identidad. La aplicación de blockchain en la gestión de identidades puede agilizar este proceso permitiendo agilizar los procedimientos de facturación y mejorando la seguridad reduciendo riesgos de fraude o usurpación.

Un sistema de gestión de identidades basado en blockchain puede crear identificadores descentralizados (DID) que proporcionen a los pasajeros identidades digitales verificables (Stockburger et al., 2021). Este sistema puede almacenar información vital como datos biométricos, información del pasaporte y detalles del visado en una blockchain. Los datos en blockchain son inmutables, lo que significa que no pueden manipularse mitigando así el riesgo de fraude de identidad. Además, los pasajeros pueden gestionar de forma segura sus identidades sin depender de un tercero intermediario manteniendo un alto nivel de privacidad y control sobre su información. En la figura 6 se puede ver IATA Travel Pass una propuesta que realizó IATA de pasaporte sanitario digital basado en blockchain.

Por último, además de aplicarse a pasajeros, este enfoque de gestión de identidades también puede extenderse al personal del aeropuerto y las tripulaciones, brindando un mayor control y fortaleciendo la seguridad en el entorno operativo. Al establecer sistemas confiables de identificación y verificación basados en tecnología blockchain, se pueden prevenir suplantaciones de identidad y garantizar un acceso seguro a áreas restringidas, mientras se facilita una supervisión más precisa de las actividades del personal y se mejora la transparencia en la gestión operativa.

3.1.2 Emisión de billetes y pagó (Ticketing and Payment)

La venta de billetes es otro ámbito clave de la aviación que puede beneficiarse de blockchain. Tradicionalmente, en la venta de billetes intervienen múltiples intermediarios, cada uno de los cuales aumenta los precios. Además, el fraude o la posible reventa son problemas recurrentes.

Con blockchain, las aerolíneas pueden emitir billetes digitales que son únicos y no pueden duplicarse debido a la seguridad inherente de blockchain (Ahmad et al., 2021). Información como el precio de los billetes, los compradores o detalles del vuelo se pueden almacenar de forma segura e inmutable en blockchain permitiendo realizar una verificación de la autenticidad y propiedad de los mismos. Esto reduce los riesgos de fraude y de reventa. Los sistemas de pago basados en blockchain pueden permitir transacciones más rápidas, seguras y rentables, eliminando la necesidad de intermediarios y reduciendo las tarifas de transacción.

Además, el almacenamiento de tickets inteligentes en blockchain podría ayudar a mitigar o eliminar los efectos del caos que puede provocar un fallo en la base de datos centralizada de tickets de una aerolínea o de todo un aeropuerto (Lufthansa, 2023). Al tener los tickets almacenados de forma segura y descentralizada en la cadena de bloques, se reduce la dependencia de una única base de datos centralizada, lo que proporciona una mayor resiliencia y evita posibles interrupciones en el servicio

mejorando la experiencia del usuario y evitando posibles pérdidas de ingresos y costes de indemnización (DBJ, 2016).

3.1.3 Programas de fidelización (Frequent Flyer programs)

Los programas de fidelización son esenciales para las estrategias de marketing de las aerolíneas ya que incentivan la lealtad de los clientes mediante puntos de recompensa. Sin embargo, la gestión de estos programas puede ser compleja debido a problemas como la caducidad de los puntos y el canje o su transferencia y utilización entre aerolíneas de la misma alianza.

La blockchain transforma los programas de fidelidad al tokenizar los puntos de fidelidad, mejorando su transparencia, seguridad y eficiencia en distribución y canje. Además, habilita la interoperabilidad de puntos entre distintas plataformas y aerolíneas, brindando a los clientes una experiencia mejorada al poder utilizar sus puntos en una amplia gama de servicios y productos. Esta flexibilidad y utilidad adicional refuerzan la propuesta de valor de los programas de fidelidad fomentando una mayor participación de los clientes y aumentando su atractivo de manera significativa.

3.1.4 Equipaje y carga

La gestión del equipaje y la carga representa un reto constante en la aviación, con casos demasiado frecuentes de pérdida de equipaje y extravío de carga (CNET, 2022). Estos problemas no solo perjudican la experiencia del cliente, sino que también aumentan los costes operativos. El equipaje de los pasajeros y la carga pasa por diversos procesos automatizados y manuales antes de ser entregado, y los datos relacionados con el viaje del equipaje a menudo se almacenan de manera no estandarizada por los distintos agentes involucrados, como el personal de aerolíneas, empresas de transporte, aeropuertos y autoridades locales.

La tecnología Blockchain ofrece una solución al proporcionar visibilidad y trazabilidad de extremo a extremo del equipaje y la carga (Li et al., 2021). Todas las partes interesadas, incluidas las aerolíneas, los servicios de asistencia en tierra y los clientes, pueden acceder en tiempo real a la información de seguimiento, lo que reduce las posibilidades de pérdida de artículos. Además, un sistema basado en blockchain puede gestionar las declaraciones de aduana y los pagos de derechos, simplificando la logística transfronteriza.

3.1.5 Mantenimiento de aeronaves

El mantenimiento de una aeronave supone un coste elevado a las aerolíneas debido a que implica inspecciones periódicas, reparaciones y sustituciones de piezas. Llevar un registro preciso de estas

actividades de mantenimiento es fundamental para garantizar la seguridad y la longevidad de las aeronaves. Sin embargo, los métodos tradicionales de registro suelen ser fragmentarios y propensos a imprecisiones.

El proceso de mantenimiento, reparación y revisión (MRO) en el ámbito de la aviación es altamente complejo, involucrando a diversos actores clave como fabricantes, comerciantes de componentes, aerolíneas, proveedores de servicios y autoridades regulatorias. Cada uno de estos participantes desempeña un papel fundamental en el mantenimiento y funcionamiento seguro de las aeronaves. Sin embargo, esta complejidad se ve agravada por la fragmentación de la información, ya que cada actor almacena datos en bases de datos separadas o registros físicos.

Esta fragmentación de datos representa un desafío significativo, ya que dificulta la obtención de una visión completa y precisa sobre los componentes y el mantenimiento de las aeronaves. La falta de una fuente estandarizada de datos puede llevar a discrepancias y duplicidades, lo que pone en duda la confiabilidad de la información y la seguridad de los componentes.

Además, el sistema actual de registros de mantenimiento de aeronaves presenta deficiencias en términos de seguridad y accesibilidad. Las aerolíneas suelen almacenar los datos en bases de datos centralizadas, lo que las expone a posibles manipulaciones y compromisos de seguridad. Por otro lado, cada parte interesada mantiene su propia base de datos, lo que dificulta la extracción eficiente de información en situaciones críticas como auditorías o investigaciones de accidentes. La limitada accesibilidad a los datos también supone un obstáculo, ya que solo la agencia responsable de los registros tiene acceso a la información, lo que dificulta el intercambio de datos con otras partes involucradas en el proceso de MRO.

Además de estas deficiencias, la utilización de registros en papel añade otro nivel de complejidad y riesgo. Los registros en papel son propensos a pérdidas, daños o alteraciones, lo que compromete la integridad de la información.

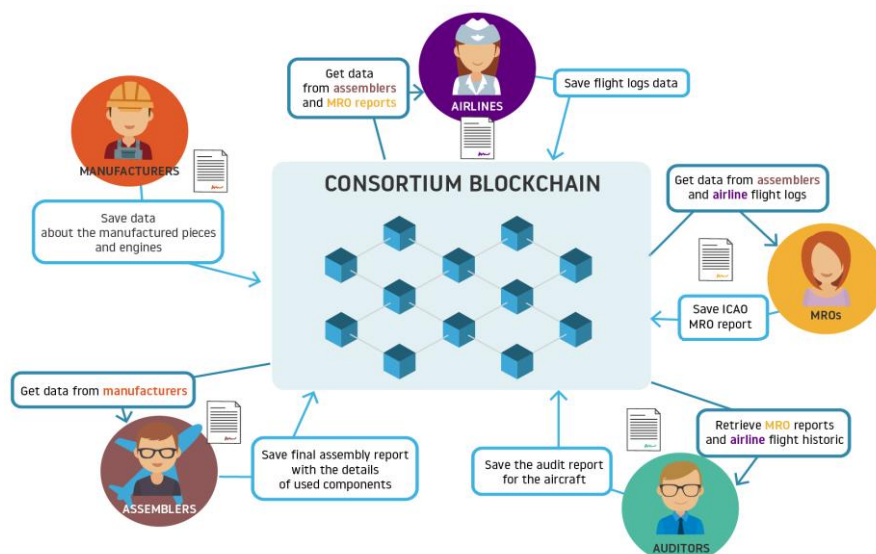


Figura 7. Blockchain de Consorcio para Compartir Datos Seguros de Mantenimiento de Aeronaves: Un Escenario Simplificado (DS.aero, 2019)

La implementación de la tecnología blockchain en el mantenimiento de aeronaves garantiza confianza y transparencia en el intercambio de información. Almacenando registros de mantenimiento en una cadena de bloques privada o pública, permite un acceso fluido mediante contratos inteligentes, promoviendo un enfoque descentralizado que mejora la eficiencia y confianza en el sistema (Efthymiou et al., 2022). Esta tecnología revoluciona el mantenimiento al simplificar el registro de datos, establecer una cadena de suministro transparente y rastreable, generar confianza en piezas de repuesto usadas y facilitar el seguimiento en tiempo real de componentes, aumentando la eficiencia y reduciendo costos. La figura 7 muestra un simplificado ejemplo de red blockchain de consorcio para el mantenimiento de aeronaves.

Además, el uso de blockchain podría permitir a las aerolíneas realizar un mantenimiento más predictivo, al permitir a los técnicos revisar la configuración completa y el historial de los distintos componentes. Esto ayudaría a abordar los problemas de forma preventiva en lugar de actuar después de que se haya producido un problema. De igual manera, los proveedores de MRO también podrían utilizar blockchain para ofrecer estos servicios ahorrando dinero tanto para ellos como para las aerolíneas.

3.1.6 Cadena de suministro (Supply chain)

La gestión de la cadena de suministro es un componente crítico en la industria de la aviación, donde la seguridad y la eficiencia son de suma importancia. Actualmente, el proceso de gestión de la cadena de suministro en la aviación enfrenta desafíos relacionados con la falta de transparencia, la trazabilidad limitada de los componentes y la falta de colaboración entre los diversos actores involucrados, como fabricantes, proveedores de servicios, aerolíneas y reguladores.

La blockchain puede desempeñar un papel transformador en la gestión de la cadena de suministros. Blockchain, como un registro descentralizado e inmutable, puede proporcionar una plataforma segura y transparente para el intercambio de información ofreciendo un seguimiento en tiempo real de piezas y materiales, garantizando su fabricación en condiciones aceptables (Dutta et al., 2020). Mediante el uso de blockchain, cada componente utilizado en la fabricación y el mantenimiento de aeronaves puede ser registrado y rastreado a lo largo de su ciclo de vida. Esto brinda a los actores de la cadena de suministro la capacidad de verificar la procedencia y la calidad de los componentes, lo que a su vez garantiza la seguridad y confiabilidad de las aeronaves. También puede agilizar las adquisiciones mediante contratos inteligentes, que automatizan las transacciones basándose en reglas predefinidas, reduciendo el papeleo manual y mejorando la transparencia.

Blockchain permitiría la colaboración y el intercambio de datos entre los diferentes actores de la cadena de suministro. Al tener un registro compartido y confiable de la información, se pueden eliminar las barreras y los retrasos asociados con la reconciliación de datos entre múltiples sistemas. Esto permite una mayor eficiencia en la gestión de inventarios, la planificación de la producción y la coordinación de los pedidos, lo que se traduce en una mejor gestión de la cadena de suministro en general.

Además, también permitiría aumentar la seguridad de los datos y la protección contra la falsificación de componentes. A través de la criptografía y registros inmutables para garantizar la integridad de los datos. Esto proporciona una capa adicional de seguridad y confianza, lo que permite a los actores de la cadena de suministro verificar la autenticidad de los componentes y protegerse contra productos falsificados o de baja calidad.

3.1.7 Registros de vuelo

Los registradores de datos de vuelo son fundamentales para mantener la seguridad de los vuelos e investigar los accidentes. Sin embargo, las cajas negras tradicionales pueden dañarse o perderse en caso de accidente, lo que dificulta la recuperación de datos. Además, en la actualidad las registradoras de datos de vuelo suelen venir con un engorroso proceso de documentación y mecanismo de almacenamiento que en muchas ocasiones dificulta el poder extraer información por parte de las aerolíneas o empresas de mantenimiento.

Blockchain ofrece una solución eficaz para almacenar datos de vuelo en una red descentralizada, brindando seguridad y accesibilidad. Su naturaleza segura y transparente garantiza la confiabilidad de los datos durante las investigaciones de accidentes, incidentes o simplemente al ser usados por la aerolínea, mejorando así la seguridad en la aviación. Además, el uso de blockchain en los registros de vuelo proporciona garantías de seguridad y precisión, alta disponibilidad de los registros, mantenimiento persistente del historial de vuelo de la aeronave y registros de la tripulación. También permite un seguimiento preciso de los vuelos, verificación de certificados de entrenamiento y ofrece beneficios como inmutabilidad de datos, trazabilidad, transparencia, visibilidad y mayor seguridad (Ahmad et al., 2021). Esto permite diseñar políticas de gestión y evaluación de riesgos más precisas y confiables basadas en la tecnología blockchain, que garantiza la integridad de los datos y promueve la seguridad operacional y confianza de la industria de la aviación.

3.1.8 Gestión de flotas

La gestión de flotas es fundamental en la industria de la aviación, donde el seguimiento y mantenimiento eficiente de las aeronaves son cruciales para garantizar la seguridad y el rendimiento óptimo. Sin embargo, los actuales sistemas de gestión de flotas a menudo se enfrentan a desafíos relacionados con la falta de transparencia, la complejidad de los registros y la coordinación entre múltiples actores.

Blockchain puede ayudar a mejorar los procesos de gestión de flotas y lograr una mayor eficiencia y confiabilidad. Una aplicación clave de blockchain en la gestión de flotas es el mantenimiento de registros digitales inmutables. Mediante el uso de blockchain, se pueden crear registros digitales precisos y verificables de cada aeronave, incluyendo su historial de mantenimiento, reparaciones realizadas, componentes reemplazados y cualquier otra información relevante. Estos registros se

mantienen de forma descentralizada y se actualizan en tiempo real, lo que permite a todas las partes interesadas acceder a la información más reciente de la flota de aeronaves.

Además, la tecnología blockchain en la gestión de flotas puede permitir la optimización de los procesos de mantenimiento y reparación. Al contar con registros precisos y actualizados de cada aeronave, los operadores y proveedores de servicios de mantenimiento pueden planificar y programar las tareas de manera más eficiente. Esto ayuda a reducir los tiempos de inactividad no planificados y los costos asociados, al tiempo que mejora la seguridad y la disponibilidad de las aeronaves.

3.1.9 Gestión del espacio aéreo y Planificación de vuelos

La gestión eficiente del espacio aéreo y la planificación de vuelos son elementos cruciales para garantizar la seguridad en las operaciones de las aeronaves. Sin embargo, estos procesos enfrentan desafíos como la falta de interoperabilidad entre los sistemas de gestión del tráfico aéreo de diferentes países y la necesidad de compartir información en tiempo real de manera precisa y segura. En este sentido, la tecnología blockchain ofrece soluciones innovadoras que podrían transformar la forma en que se gestionan y planifican los vuelos.

Una aplicación potencial de blockchain en la gestión del espacio aéreo y la planificación de vuelos es el almacenamiento y compartición de datos de vuelo en una red descentralizada y segura (Clementi et al., 2019). Mediante la utilización de contratos inteligentes, los registros de vuelo podrían ser almacenados de manera inmutable en la cadena de bloques, lo que garantizaría la integridad y la transparencia de la información. Esto permitiría a las autoridades de tráfico aéreo, aerolíneas y otros actores relevantes acceder a datos precisos y actualizados en tiempo real, facilitando la toma de decisiones y mejorando la eficiencia operativa.

Además, blockchain podría mejorar la interoperabilidad entre los sistemas de gestión del tráfico aéreo de diferentes países. Al utilizar una red descentralizada y consensuada, se eliminarían las barreras existentes para compartir datos entre las distintas autoridades y se garantizaría la confianza y la transparencia en la gestión del espacio aéreo a nivel global. Esto permitiría una mejor coordinación de los vuelos, reduciendo los retrasos y optimizando el uso del espacio aéreo.

Otro beneficio potencial de utilizar blockchain en la gestión del espacio aéreo y la planificación de vuelos es la mejora de la seguridad (Lu et al., 2021). La tecnología blockchain proporciona una capa adicional de protección contra la manipulación y el fraude de datos, ya que los registros almacenados en la cadena de bloques son inmutables y auditables. Esto contribuiría a fortalecer la confianza en los datos de vuelo, lo que resulta crucial en situaciones de investigación de accidentes o incidentes.

3.1.10 Integración de UAS

La integración de los sistemas de aeronaves no tripuladas (UAS) en el espacio aéreo ofrece una gran oportunidad para aprovechar tecnologías innovadoras como blockchain en un ecosistema de espacio aéreo completamente nuevo. Estos nuevos dispositivos tienen el potencial de ser "más inteligentes" que las aeronaves convencionales, ya que aprovechan tecnologías de vanguardia de manera más rápida. La infraestructura de soporte prevista para gestionar estos vuelos se basa en una red de proveedores de servicios de UAS interconectados, que dependen en gran medida de la difusión de información entre una amplia variedad de entidades en red (Alladi et al., 2020). Gran parte del intercambio de datos implica información estatal relevante tanto para las aeronaves como para los entornos de espacio aéreo por los que estas aeronaves transitan.

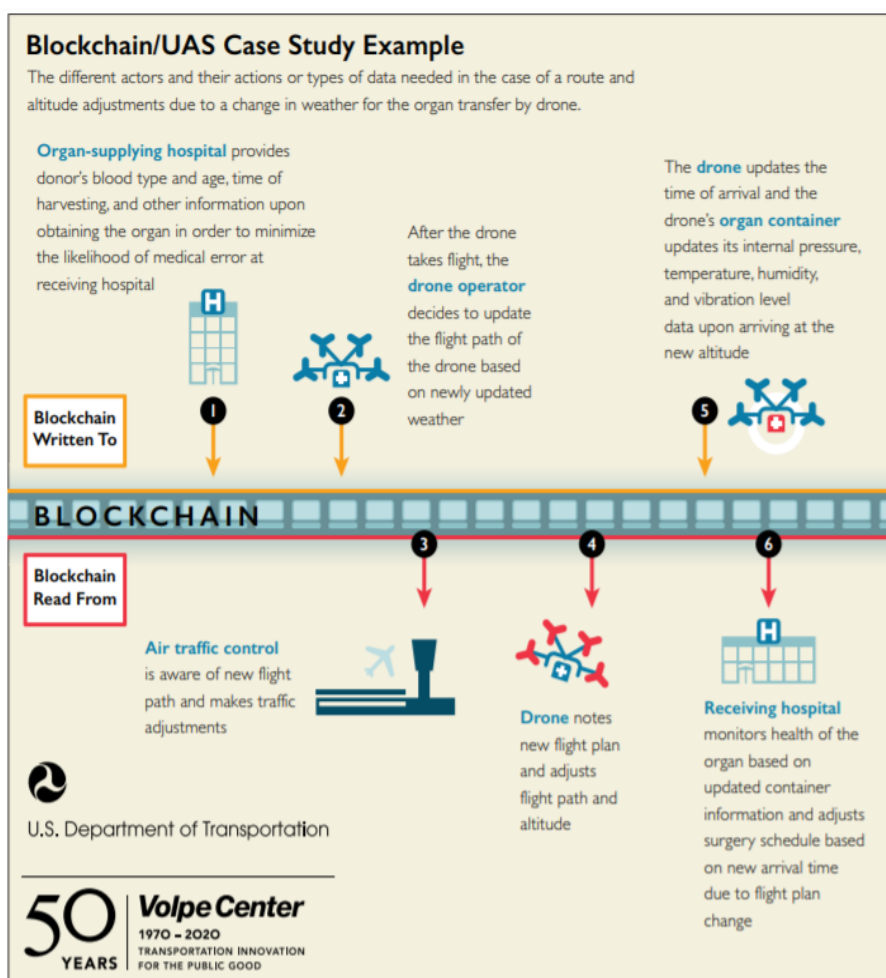


Figura 8. Ejemplo Blockchain/UAS caso de estudio (DoT, 2021)

Una aplicación potencial de blockchain en la integración de UAS es el almacenamiento y la compartición de datos de manera segura y transparente. La tecnología blockchain puede mejorar la integridad y la seguridad de la identificación, registro y seguimiento remoto de UAS. Los protocolos de blockchain permiten la comunicación punto a punto y el intercambio de datos de manera segura, autenticada y cohesionada (Wang et al., 2021). Además, blockchain podría utilizarse en la infraestructura de soporte de gestión de tráfico de UAS (UTM) para designar y comunicar la

accesibilidad del espacio aéreo en diferentes momentos y para diferentes actores (Allouch et al., 2021). A largo plazo, los proveedores de servicios de UTM y otros proveedores de datos podrían beneficiarse de blockchain al proporcionar servicios y productos a través de la cadena de bloques. En la figura 8 se muestra un ejemplo de caso de estudio de operación UAS para transporte de órganos basado en tecnología blockchain

La implementación temprana de blockchain en el marco de UTM permitiría aprovechar los beneficios de un entorno operativo seguro desde el principio. A medida que la funcionalidad de blockchain se vuelve más confiable y confiable, los conceptos de blockchain pueden fusionarse directamente en los entornos de espacio aéreo tripulados, donde el riesgo es inherentemente mayor.

3.2 Desafíos y limitaciones de la implementación de blockchain en la aviación

En esta sección, se explorarán los desafíos y limitaciones asociados con la implementación de la tecnología blockchain en la industria de la aviación. Como se ha mencionado anteriormente, la tecnología blockchain tiene el potencial de revolucionar las operaciones en este sector, ofreciendo ventajas como la emisión de billetes, el seguimiento del equipaje, la trazabilidad de las piezas y la verificación de la identidad de los pasajeros.

Sin embargo, a pesar de su potencial prometedor, la adopción generalizada de blockchain en la aviación está todavía lejos de ser una realidad. En esta sección, examinaremos de cerca los desafíos significativos que surgen durante la implementación de esta tecnología y las limitaciones inherentes que requieren una consideración.

La interoperabilidad, la escalabilidad, la seguridad y el marco legal son algunos de los desafíos clave que deben abordarse para aprovechar al máximo el potencial de blockchain en la aviación. La falta de estándares, la heterogeneidad de los sistemas existentes y la necesidad de garantizar la protección de datos sensibles plantean desafíos significativos para la adopción y el funcionamiento eficiente de la tecnología blockchain en la industria de la aviación.

3.2.1 Desafíos de la implementación Blockchain en la aviación

3.2.1.1 Desafíos Técnicos

Una transición de los sistemas tradicionales actuales a los basados en blockchain en la aviación plantea importantes retos técnicos. El principal de ellos es la interoperabilidad. En la actualidad, la falta de interoperabilidad acaba obstaculizando la adopción de la tecnología en múltiples aplicaciones (Lacity & Khan, 2019). Por un lado, se han desarrollado diferentes soluciones de blockchain que al no existir estandarización causa que estas por lo general no son interoperables entre sí. Por otro lado, los

sistemas de aviación existentes, desarrollados durante años con funcionalidades específicas, no se diseñaron pensando en muchas ocasiones en la integración con otros sistemas mucho menos con blockchain. Es por ello que es de gran importancia no solo buscar la interoperabilidad entre distintas blockchains, sino también entre las blockchains y los sistemas tradicionales (Lacity et al., 2019).

Otro desafío técnico son la escalabilidad, la latencia y el rendimiento de la blockchain. Como ya se mencionó en secciones anteriores, las blockchains más tradicionales, en particular las que dependen de algoritmos de consenso PoW, tienen dificultades para procesar grandes volúmenes de transacciones en tiempo real y el tiempo necesario para validar una transacción puede aumentar a medida que más nodos se unen a la red (Croman et al., 2016). Esto supone un obstáculo importante para las aplicaciones de aviación que necesitan acceso y procesamiento instantáneo de datos, como el seguimiento de vuelos en tiempo real o los sistemas de gestión del espacio aéreo como el control del tráfico aéreo.

3.2.1.2 Desafíos Regulatorios

La aviación es uno de los sectores más regulados del mundo, y el cumplimiento de la normativa es primordial. La implantación de la tecnología blockchain en este entorno plantea varios problemas normativos, principalmente en torno a la privacidad de los datos y la protección de los usuarios (McGhin et al., 2019). Las incertidumbres legales y regulatorias son uno de los desafíos sociales más citados (Swan, 2015), advirtiendo que la regulación podría ser uno de los factores más determinantes del futuro de la tecnología blockchain.

Por ejemplo, las normativas sobre privacidad de datos como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea entran en conflicto con el principio de inmutabilidad intrínseco a la tecnología blockchain. Según el GDPR, las personas tienen el "derecho a ser olvidadas", que obliga a las entidades a borrar los datos personales previa solicitud, un requisito que choca con la naturaleza permanente de los registros de blockchain (Finck, 2018). Además, la falta de regulaciones uniformes a nivel mundial complica el establecimiento de un sistema blockchain de cumplimiento universal en la aviación.

3.2.1.3 Problemas de Seguridad y Privacidad

Aunque la blockchain cuenta con sólidas funciones de seguridad gracias al uso de criptografía, no es totalmente inmune a posibles ciber-amenazas y ataques. Por ejemplo, el llamado "ataque del 51%", por el que una entidad se hace con el control de la mayoría de la potencia de cálculo de la red, puede comprometer la integridad de una cadena de bloques (Golosova & Romanovs, 2018). Por otra parte, según el artículo (McGhin et al., 2019), se destaca que un nodo con recursos limitados puede representar un riesgo, ya que en una estrategia de minería egoísta, los mineros pueden unirse para separar bloques de la cadena principal y hacerlos accesibles sólo a sistemas dentro de su red privada o bajo ciertas condiciones.

También existen problemas de privacidad. Eso se debe por un lado al hecho de que los datos y transacciones son visibles para todos en la red, lo que genera preocupaciones sobre la confidencialidad. Esto provoca que los miembros sean reacios a almacenar información confidencial en ella (Ruoti et al., 2019). Por otro lado, aunque los datos en blockchain son seudónimos, un análisis sofisticado de los datos podría vincular las identidades a las transacciones, lo que plantearía importantes riesgos para la privacidad (Reid & Harrigan, 2013)]. Dada la sensibilidad en la aviación de ciertos datos como información de los pasajeros o información operacional, estos problemas de seguridad no pueden pasarse por alto.

3.2.2 Limitaciones de la implementación Blockchain en la aviación

3.2.2.1 Complejidad y Coste

La implantación de blockchain en la aviación, como en cualquier industria, no es una tarea sencilla debido a que exige conocimientos técnicos y recursos considerables. Esto puede suponer un obstáculo para las entidades más pequeñas o con recursos limitados. Las plataformas descentralizadas como

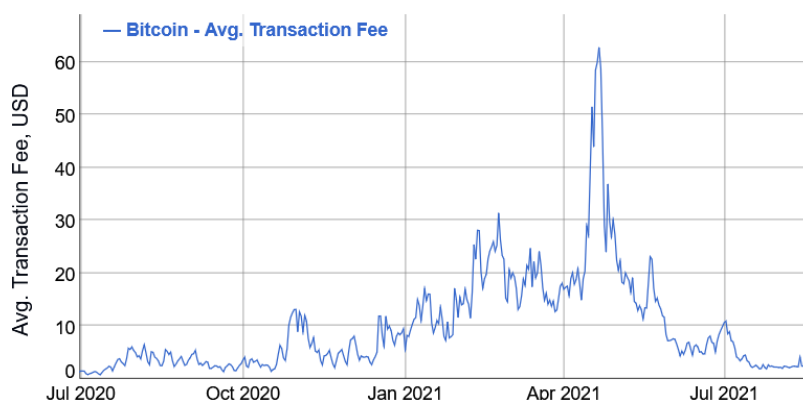


Figura 9. Coste de transacción Bitcoin (Bitcoin, 2021)

Bitcoin y Ethereum pueden tener tarifas de transacción elevadas debido a la competencia por el espacio limitado en los bloques y la alta demanda en períodos de congestión. En abril de 2021 el coste de transacción de Bitcoin llegó a estar por encima de los 60\$, ver figura 9.

Además, las blockchain públicas, en particular, son notorias por su uso intensivo en energía, lo que contribuye a unos costes operativos significativos (O'Dwyer & Malone, 2014). Dada la creciente presión sobre las partes interesadas de la aviación para optimizar la eficiencia operativa y reducir costes, la viabilidad económica de la implementación de blockchain es una consideración crucial.

3.2.2.2 Madurez Tecnológica

Como tecnología emergente, blockchain todavía se encuentra en fase de desarrollo en la industria de la aviación. Aunque se han propuesto numerosas aplicaciones y se están realizando pruebas de concepto, su integración con los sistemas existentes y la gestión de grandes volúmenes de datos generados en la aviación aún plantean desafíos. Además, es necesario abordar la necesidad de procesar datos en tiempo real, lo que requerirá soluciones efectivas para garantizar la eficiencia y la interoperabilidad. La madurez de blockchain en la industria de la aviación aún está en proceso de demostración, y se requiere más investigación y desarrollo para comprender plenamente su potencial y aplicabilidad en este sector (Li et al., 2021).

3.2.2.3 Falta de Estandarización

Como ya se destacó anteriormente, la ausencia de estandarización es un factor determinante que limita la aplicación de blockchain en la aviación. Esta situación se manifiesta de diversas formas y afecta a numerosos aspectos de la incorporación de esta tecnología. En primer lugar, sin protocolos y formatos de datos estandarizados, la integración de sistemas dispares se convierte en una tarea imposible. Los diferentes sistemas y tecnologías de la industria de la aviación han sido desarrollados y evolucionados a lo largo de los años, dando como resultado sistemas heterogéneos con diferentes protocolos y formatos de datos. La integración de estos sistemas dispares con una nueva tecnología como blockchain implicaría un gran trabajo de reconciliación y compatibilidad de datos (Zyskind et al., 2015). Esto puede resultar particularmente desafiante cuando se trata de compartir información entre diferentes organizaciones o incluso entre diferentes departamentos dentro de la misma organización.

En segundo lugar, la falta de normativas estandarizadas también supone una barrera importante. La normativa legal respecto a blockchain aún se encuentra en una fase incipiente en muchas jurisdicciones, y la falta de regulaciones coherentes y estandarizadas puede generar un ambiente de incertidumbre legal. Por ejemplo, el manejo de los datos de los pasajeros y la información de vuelo puede estar sujeto a regulaciones de privacidad y protección de datos muy estrictas en algunas jurisdicciones. La naturaleza inmutable de la blockchain puede chocar con los derechos de los individuos a modificar o eliminar sus datos personales. La ausencia de un marco regulatorio estandarizado para blockchain puede hacer que sea difícil para las aerolíneas y otros actores de la industria de la aviación garantizar el cumplimiento de estas regulaciones.

3.2.2.4 Barreras culturales y organizativas

La introducción de una tecnología emergente y disruptiva como blockchain a menudo se encuentra con resistencias culturales y organizativas. Esto es especialmente cierto en sectores tradicionales y altamente regulados como la aviación. Estos desafíos pueden ser igual o incluso más cruciales que los desafíos técnicos ya que pueden tener un impacto significativo en la velocidad y el éxito de la implementación de blockchain.

Existen diferentes razones por las que podría haber una resistencia inicial a la aplicación de blockchain en la aviación. De primeras se puede percibir como una pérdida de empleos debido a la automatización y la eficiencia que blockchain puede traer, mientras que otros pueden percibir un aumento en la complejidad de su trabajo debido a la adopción de nuevas tecnologías y procedimientos (Marikyan et al., 2022). Además, la falta de conocimientos sobre blockchain puede llevar a una adopción ciega impulsada por la exageración del mercado, sin tener en cuenta los casos de uso adecuados para la tecnología (Casino et al., 2019). También los ejecutivos o responsables de la toma de decisiones necesitan comprender la tecnología, sus capacidades y desafíos, que no son solo técnicos, sino también sociales y organizativos (Lacity, 2018).

Además, la percepción pública de blockchain ha sido afectada por incidentes notorios (Cointelegraph, 2022) que han deteriorado la reputación y la percepción pública de la blockchain. Este tipo de incidentes de alto perfil puede obstaculizar la adopción de sistemas basados en blockchain en la aviación, donde la confianza del público en la seguridad o la privacidad de los datos es crítica.

3.2.2.5 Impacto Medioambiental y Barrera Geográfica

Las blockchains públicas, como Bitcoin, son conocidas por su alto consumo de energía, contribuyendo a significativas emisiones de carbono que se han asociado con la minería de criptomonedas y el mantenimiento de la red blockchain (Stoll et al., 2019). Dado que la industria de la aviación ya está bajo un alto escrutinio por su impacto medioambiental, la adición de una tecnología que consume grandes cantidades de energía podría crear retos significativos en términos de relaciones públicas y sostenibilidad. El nivel de consumo de energía, junto con la huella de carbono que resulta de la generación de esta energía, es un factor crítico que la industria de la aviación debe considerar, dado su compromiso actual con la sostenibilidad y la reducción de las emisiones de gases de efecto invernadero.

Además, la dependencia de la red blockchain de una conexión a Internet estable y de alta velocidad presenta un problema adicional. Las partes del mundo que no tienen una conexión a Internet fiable pueden enfrentarse a desafíos significativos para implementar y mantener un sistema blockchain a nivel equiparable de la industria (McGhin et al., 2019). Este desafío es particularmente relevante para la industria de la aviación, que opera a nivel mundial y en zonas geográficas donde la infraestructura de Internet puede no estar a la altura de los requerimientos de una red blockchain.

3.3 Ejemplos de uso y casos de estudio existentes

En esta sección se realizará una recopilación y análisis de algunos de los proyectos innovadores en la industria de la aviación que aprovechan la tecnología blockchain para optimizar operaciones y servicios. Cabe destacar que esta recopilación no es exhaustiva, sino que simplemente busca destacar

algunas iniciativas principales en desarrollo. Estos proyectos sirven como demostradores de las diversas aplicaciones de blockchain en la industria.

- **IATA:** La asociación internacional de transporte aéreo está trabajando en diversos proyectos donde utilizan tecnología blockchain como IATA Coin o IATA Digital Certification Authority (DCA) (Goudarzi et al., 2018). IATA Coin es un concepto de moneda digital supranacional con el objetivo de utilizar la tecnología blockchain en los sistemas de liquidación de IATA, especialmente en la Cámara de Compensación de IATA. IATA DCA es una plataforma que facilita la gestión de identidades digitales en la aviación comercial. El objetivo es proporcionar acceso en tiempo real a datos confiables y de alta calidad a sus socios para realizar transacciones de manera segura.
- **AERON:** Es un sistema profesional de aviación basado en la cadena de bloques Ethereum que ofrece soluciones en tres casos de uso distintos (AERON, 2020). Para los pilotos, proporciona una aplicación móvil que les permite registrar vuelos, rastrear la ubicación y acceder a registros históricos, así como adquirir servicios en el destino. Para las empresas, la aplicación móvil facilita la gestión de vuelos completados, reservas de aeronaves y tareas de mantenimiento, junto con un sistema de reserva y gestión de clientes. Para los pasajeros, el portal web aerotrips.com ofrece acceso a una base de datos global de ofertas de vuelos, permitiendo la selección de vuelos demo verificados por Aeron, pagos en línea con moneda tradicional o criptomonedas, y una membresía en el club aerotrips.com.
- **FlightChain:** Es un proyecto de investigación blockchain iniciado por SITA Lab en colaboración con Heathrow Airport Holdings Limited (HAL) e International Airlines Group (IAG). El objetivo de FlightChain es establecer una "única fuente de verdad" para los datos de vuelo. Utiliza una blockchain de tipo privada implementada en Ethereum y Hyperledger-Fabric. Almacena información de vuelo en la blockchain y utiliza contratos inteligentes para resolver posibles conflictos de datos (FlightChain, 2017).
- **Loyyal:** Es una startup que busca revolucionar los incentivos y programas de fidelización para clientes utilizando la tecnología blockchain. Ofrece métodos estandarizados para crear, recompensar y gestionar puntos de fidelización reduciendo los costes operativos asociados con la conciliación y el pago. Su plataforma permite la colaboración entre industrias fragmentadas, proporciona información en tiempo real para ofertas personalizadas y garantiza la trazabilidad de los puntos de fidelización. Además, facilita la transferencia transparente de millas entre socios de aerolíneas y permite a los pasajeros acceder en tiempo real a los puntos de fidelización. La solución está construida sobre la plataforma blockchain Hyperledger Fabric.
- **Trustabit⁸:** Es un sistema basado en blockchain que ofrece servicios a aerolíneas para ayudar a los clientes a obtener compensación por vuelos cancelados o retrasados. Utiliza contratos inteligentes en la cadena de bloques y emite automáticamente vales a los pasajeros cuando

⁸ <https://www.hyperledger.org/>

hay una interrupción en el vuelo. Esto elimina la necesidad de procedimientos administrativos prolongados y permite la entrega inmediata de los vales a través del correo electrónico registrado del pasajero.

- **SkyThread for Parts**⁹: surge de una colaboración entre AFI KLM E&M y SkyThread. Mediante el uso de tecnología blockchain se busca facilitar, acelerar y asegurar el seguimiento de los componentes desde su fabricación hasta su desmantelamiento. Basada en una blockchain privada y segura, permite a los usuarios registrar eventos relacionados con el ciclo de vida de los componentes y eliminar errores asociados con la interacción humana.
- **GoDirect**¹⁰: Es una plataforma de comercio en línea de Honeywell que utiliza la tecnología blockchain. A través de su solución llamada Trust Trace, GoDirect proporciona información detallada sobre la procedencia y el historial de las piezas de aeronaves, permitiendo a los consumidores tomar decisiones más informadas. Además, utiliza tecnología de marcaje y autenticación en blockchain para combatir la falsificación y rastrear físicamente las piezas durante su vida útil.
- **DARS (Digital Aviation Record System)**¹¹: Es una plataforma digital de registros de aeronaves desarrollada en colaboración con TrustFlight, Boeing, RaceRocks y la Universidad de British Columbia. El objetivo principal de DARS es mejorar la eficiencia en la industria de la aviación al permitir la transferencia de información precisa de manera fluida y eliminar la necesidad de entrada manual de datos. La plataforma conectará datos en toda la cadena de suministro, mejorando la productividad y eficiencia del mantenimiento de las aerolíneas.
- **TRUengine**¹²: Es una plataforma basada en blockchain para el seguimiento y rastreo de la cadena de suministro desarrollada por GE Aviation en colaboración con Microsoft Azure. La plataforma tiene como objetivo mejorar la eficiencia y transparencia en la industria de la aviación al monitorear y recopilar datos relacionados con la fabricación y ciclo de vida de las partes críticas de los motores de avión. TRUengine proporciona un formato único para los datos estructurados, eliminando la necesidad de ingreso manual de datos y agilizando la evaluación y redistribución de los activos de los motores. La plataforma permite a los propietarios, compradores, arrendadores y tasadores de motores verificar fácilmente la autenticidad al mismo tiempo que reduce costes, aumenta la eficiencia y mejora la seguridad en la industria de motores de avión.
- **Investigación y Desarrollo**: actualmente, se están llevando a cabo diversos proyectos de investigación que exploran la utilidad de la tecnología blockchain en el campo de la aviación.

⁹ <https://www.skythread.aero/>

¹⁰ <https://www.godirecttrade.com/>

¹¹ <https://www.digitalsupercluster.ca/projects/digital-aviation-record-system/>

¹² <https://www.geaerospace.com/services/truengine>

Financiados por la Unión Europea podemos destacar **SlotMachine**¹³ o **AICHAIN**¹⁴. El proyecto SlotMachine busca desarrollar una solución basada en blockchain para automatizar los intercambios de slots entre aerolíneas, con el objetivo de mejorar la eficiencia y reducir costos en la industria. AICHAIN es una solución que utiliza blockchain para permitir la explotación de grandes conjuntos de datos privados de diferentes actores de la industria de la aviación. Mediante el uso de un enfoque de aprendizaje federado y privacidad-preservada, los modelos de aprendizaje automático pueden entrenarse y ejecutarse en las instalaciones de los propietarios de datos sin compartir información sensible. Además, se implementa un mecanismo basado en blockchain que garantiza la confiabilidad de los modelos y proporciona incentivos directos a los participantes. Además, EASA ha financiado el proyecto **VIRTUA**¹⁵ que tiene como objetivo desarrollar soluciones digitales para el transporte aéreo mediante el uso de tecnologías de virtualización y blockchain. El caso de estudio propuesto busca evaluar los beneficios y limitaciones de la implementación de tecnologías blockchain en la gestión de piezas y componentes a lo largo de su ciclo de vida. También se analizarán los cambios necesarios en regulaciones, estándares y procesos de trabajo, así como la preparación de pautas y materiales de apoyo para la evolución regulatoria y la implementación de soluciones blockchain.

¹³ <https://sesarju.eu/projects/SlotMachine>

¹⁴ <https://sesarju.eu/projects/aichain>

¹⁵ <https://www.easa.europa.eu/en/research-projects/virtua-digital-transformation-case-studies-aviation-safety-standards>

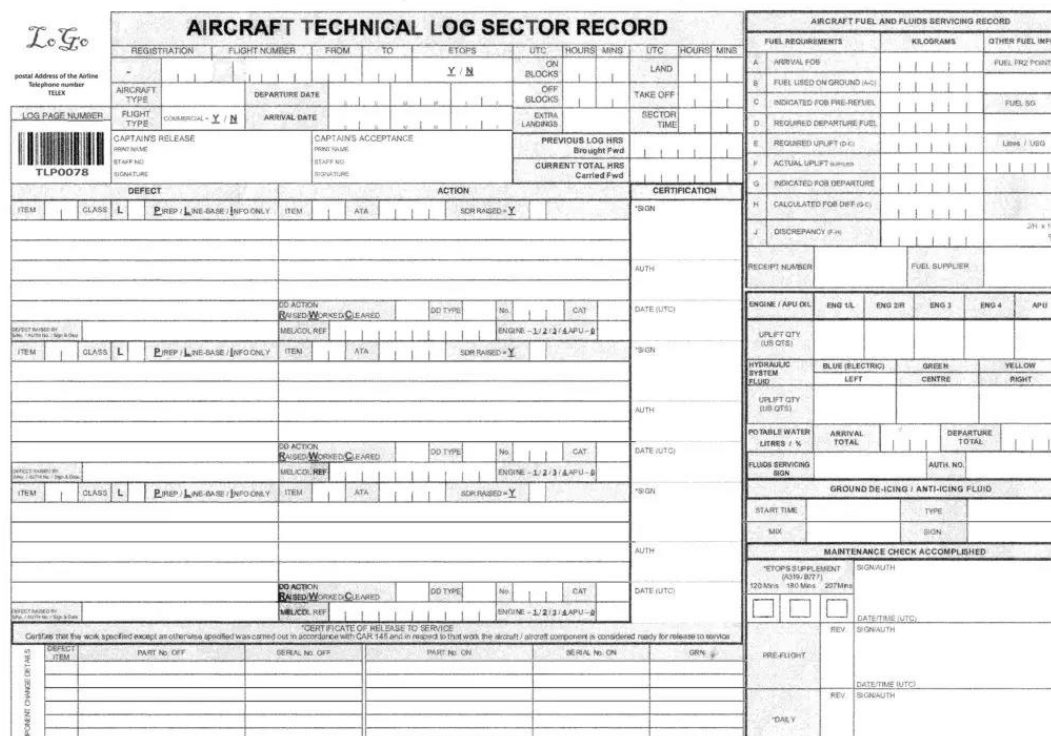
4. Caso de estudio: Aircraft Technical Log basado en blockchain

4.1 Introducción y relevancia del Aircraft Technical Log en la aviación

4.1.1 Definición y función

El Aircraft Technical Log (ATL), también denominado “tech log”, es una parte fundamental de la gestión de la aviación. Representa una documentación completa y en tiempo real del estado mecánico de una aeronave, su estado operativo y un registro del mantenimiento realizado en la misma aeronave. El ATL es una parte indispensable de la supervisión diaria de una aeronave y desempeña un papel crítico en el mantenimiento de la seguridad, eficiencia y regularidad de las operaciones de vuelo. Aunque el contenido y el formato del registro técnico pueden variar de un operador aéreo a otro, su función fundamental es la misma.

El ATL capta información vital sobre el estado de la aeronave antes de cada de vuelo, incluidas las ubicaciones y horas de salida y llegada, la carga y los niveles de combustible, los niveles de aceite y fluidos hidráulicos, el estado de los defectos, la aplicación de descongelante si procede y otras actividades regulares de mantenimiento de línea. En la figura 10 se puede ver un ejemplo de ATL.



The form is titled "AIRCRAFT TECHNICAL LOG SECTOR RECORD" and is divided into several main sections:

- REGISTRATION:** Includes fields for registration number, flight number, from/to, ETOPS, UTC, hours, mins, and land.
- FLIGHT INFORMATION:** Includes aircraft type, departure date, arrival date, and flight type (Commercial - Y/N).
- DEFECTS:** A table with columns for item, class, L, P, REP, LINE-BASE, INFO ONLY, and ATA.
- ACTIONS:** A table with columns for DO ACTION, RAISED, WORKED, CLEARED, DO TYPE, No., and CAT.
- CERTIFICATION:** Includes fields for SIGN, AUTH, and DATE (UTC).
- AIRCRAFT FUEL AND FLUIDS SERVICES RECORD:** Includes fuel requirements, arrival/actual/uplift fuel, and fuel supplier information.
- MAINTENANCE CHECK ACCOMPLISHED:** Includes a table for "EFFECTS SUPPLEMENT" and a section for "GROUND DE-ICING / ANTI-ICING FLUID".

At the bottom, there is a section for "MAINTENANCE CHECK ACCOMPLISHED" with a table for "EFFECTS SUPPLEMENT" and a section for "GROUND DE-ICING / ANTI-ICING FLUID".

Figura 10. Ejemplo de Aircraft Technical Log

El ATL permanece a bordo de la aeronave, accesible para los ingenieros y las tripulaciones de vuelo, independientemente del lugar en el que se incorporen a la aeronave y de su capacidad para comunicarse con otros equipos o sistemas. Esta información permite un acceso inmediato al registro de mantenimiento de la aeronave, facilitando la toma de decisiones informadas y las acciones relativas al estado operativo de la aeronave y sus necesidades de mantenimiento. Antes de cada vuelo, se deja en tierra una copia del registro ATL. Esta copia sirve como registro del estado de la aeronave antes del vuelo, contribuyendo al seguimiento exhaustivo del historial operativo de la misma.

El capitán del vuelo desempeña un papel crucial en el proceso ATL, ya que es responsable de firmar cada registro ATL. Al hacerlo, el capitán acepta el estado de la aeronave como apta para el vuelo. Al mismo tiempo, los ingenieros de línea son responsables de aprobar cada actividad de mantenimiento registrada en el ATL. Esta aprobación es una afirmación de que la actividad relacionada se ha completado según el estándar correcto y, por lo tanto, la aeronave se libera para el servicio. Una regla fundamental en las operaciones de aviación es que una aeronave no puede despegar con defectos abiertos. Por lo tanto, todos los defectos deben rectificarse o aplazarse, siguiendo procesos estrictamente supervisados, antes de que la aeronave pueda despegar. Este proceso garantiza la aeronavegabilidad de la aeronave y su preparación para el vuelo previsto.

El proceso típico en una aerolínea para trabajar con el ATL es utilizar un bloc autocopiativo de varias hojas, que registra múltiples copias en hojas de diferentes colores para documentar una notificación. Estos blocs se imprimen a medida para reflejar el diseño ATL específico de la aerolínea y cuentan con un número único impreso en cada página" para garantizar que no haya vacíos en los registros ATL.

Al finalizar un vuelo, el personal de tierra se queda con la copia correspondiente del registro del mismo, mientras se inicia una nueva página en la ATL para el siguiente. A continuación, el personal de tierra lleva la copia del registro a la oficina local. Al final del día, estas se suelen escanear y enviar a la aerolínea. Los datos del registro del vuelo son escaneados o se introducen, normalmente manualmente, en el sistema de mantenimiento de la aerolínea, normalmente con un retraso de al menos un día. En el caso de flotas más grandes con múltiples bases de ingeniería, todos los ATL originales deben devolverse también a la oficina central para su archivo.

La aerolínea es responsable de garantizar que el ATL se registra de acuerdo con unos procedimientos aprobados. Aunque el formato del formulario ATL es importante, las autoridades reguladoras hacen hincapié en el procedimiento. Este procedimiento está certificado por la Autoridad de Aviación local, y cualquier cambio en el mismo suele requerir aprobación previa.

4.1.2 Marco jurídico y supervisión

La legislación aeronáutica determina y regula la aplicación, estructura, contenido y uso del ATL. Estas directrices legales son cruciales para la normalización y la seguridad de las operaciones aéreas. Dependiendo de la jurisdicción, la autoridad supervisora puede variar. El siguiente análisis se centrará exclusivamente en Europa donde la agencia supervisora principal es EASA aunque también en Estados Unidos, donde la agencia supervisora es la Administración Federal de Aviación (FAA) .



Figura 11. Logo EASA (izquierda) y FAA (derecha)

Comenzando con EASA. La EASA proporciona un marco exhaustivo para el ATL, el cual denominan “Aircraft technical log system”, en virtud del Reglamento de la UE 1321/2014 Anexo 1 (Parte-M), sección A requisitos técnicos. Este reglamento es uno de los varios que EASA utiliza para gestionar la seguridad de la aviación y en particular para cubrir los requisitos para el mantenimiento de las aeronaves. La Parte-M describe las normas y procedimientos para la gestión del mantenimiento de la aeronavegabilidad de las aeronaves, incluido el mantenimiento, las inspecciones y el proceso de revisión de la aeronavegabilidad. En virtud de esta directiva, la EASA dicta, “M.A.306 Aircraft technical log system,” que toda aeronave que participe en el transporte aéreo comercial debe mantener un ATL. Además, también se destaca como un elemento necesario en los registros de mantenimiento de la aeronavegabilidad continuada “M.A.305 The aircraft continuing airworthiness records shall consist of”.

El ATL, según las directrices de la EASA, tiene como función registrar los defectos y averías durante la operación de la aeronave y para registrar los detalles de todo el mantenimiento realizado en una aeronave entre las visitas programadas de mantenimiento en la base. Además, se utiliza para registrar la información de seguridad de vuelo y mantenimiento que la tripulación operativa necesita conocer incluido defectos y fallos de funcionamiento de la cabina o de la cocina que afecten a la seguridad de la explotación de la aeronave o a la seguridad de sus ocupantes. EASA no establece directamente como debe ser el ATL pudiendo variar desde un simple documento de una sola sección hasta un complejo sistema que contenga muchas secciones. El sistema ATL de la aeronave puede ser un sistema en papel o informático o cualquier combinación de ambos métodos aceptables para la autoridad competente. Lo único que sí que se especifica es que debe contener información de al menos las siguientes secciones:

1. **Información de vuelo:** El ATL debe incluir información detallada sobre cada vuelo, garantizando la seguridad continuada de la operación. Puede incluir datos específicos del vuelo, como las horas de salida y llegada, la duración del vuelo, información sobre la ruta, el consumo de combustible y cualquier incidencia digna de mención durante el vuelo.
2. **Certificado de aptitud para el servicio de la aeronave:** El ATL debe contener el certificado de aptitud para el servicio de la aeronave. Este certificado confirma que la aeronave se ha sometido al mantenimiento y las inspecciones necesarias, garantizando su aeronavegabilidad

y el cumplimiento de los requisitos reglamentarios. Sirve como autorización formal para que la aeronave pueda operar.

3. **Declaración de mantenimiento:** El ATL debe incluir la declaración de mantenimiento actual, que proporciona una visión general del estado de mantenimiento de la aeronave. Esta declaración resume las tareas de mantenimiento programadas y destaca cualquier requisito de mantenimiento fuera de fase. Sin embargo, la autoridad competente puede permitir que la declaración de mantenimiento se almacene en un lugar separado, previo acuerdo.
4. **Defectos diferidos pendientes:** El ATL debe documentar cualquier defecto diferido pendiente que aún no se haya rectificado pero que pueda afectar al funcionamiento de la aeronave. Estos defectos requieren atención y resolución, y su inclusión en el registro técnico garantiza que no se pasen por alto y que puedan tomarse las medidas adecuadas para solucionarlos.
5. **Orientación de apoyo al mantenimiento:** El ATL debe contener todas las instrucciones de orientación necesarias en relación con los acuerdos de apoyo al mantenimiento. Puede incluir información sobre proveedores de mantenimiento autorizados, datos de contacto, procedimientos para obtener apoyo de mantenimiento o cualquier otra instrucción que se considere crucial para garantizar la disponibilidad de servicios de mantenimiento cuando sea necesario.

Además, se establece que si una organización de gestión del mantenimiento de la aeronavegabilidad (CAMO) es contratada por operadores que forman parte de un grupo empresarial de transporte aéreo único y tienen la intención de transferir regularmente aeronaves de un titular de certificado de operador aéreo (AOC) a otro dentro del grupo se espera que la CAMO garantice al menos:

- Que exista un sistema interoperable de registro técnico de aeronaves para todos los operadores asociados.
- Que se definan unos formatos de datos comunes e intercambio de los mismos.

Siguiendo con la FAA. La FAA proporciona un marco completo para el ATL, denominado "Aircraft maintenance records", bajo las regulaciones federales de aviación (FAR) 91.417, 121.701-709, y 135.439-447. Estas regulaciones constituyen parte de los múltiples mandatos que la FAA emplea para supervisar la seguridad de la aviación y cubrir los requisitos para el mantenimiento de las aeronaves. Las FAR describen las normas y procedimientos para la gestión del mantenimiento de la aeronavegabilidad de las aeronaves, incluido el mantenimiento, las inspecciones y el proceso de revisión de la aeronavegabilidad. Bajo este conjunto de directivas, la FAA estipula que toda aeronave que participe en el transporte aéreo comercial, privado y otros tipos de aeronaves deben mantener un ATL. Además, también se enfatiza como un elemento necesario en los "Aircraft Continuing Airworthiness Records".

El ATL, bajo las directrices de la FAA, tiene como función registrar los defectos y averías durante la operación de la aeronave y para registrar los detalles de todo el mantenimiento realizado en una aeronave. Además, se utiliza para registrar la información de seguridad de vuelo y mantenimiento que la tripulación operativa necesita conocer, incluido defectos y fallos de funcionamiento que afecten a

la seguridad de la explotación de la aeronave o a la seguridad de sus ocupantes. La FAA establece la siguiente información como necesaria:

- **Mantenimiento, modificaciones y alteraciones:** Debe documentarse un registro de todas las actividades de mantenimiento, modificaciones y alteraciones realizadas en la aeronave.
- **Tiempo total y aterrizajes/ciclos:** El ATL debe incluir el tiempo total en servicio de la aeronave y los motores, así como el número de aterrizajes o ciclos.
- **Componentes de vida limitada y calendario general:** Debe registrarse el estado actual de los componentes que tienen limitaciones de tiempo o calendario. Esto incluye información sobre cuánto tiempo queda antes de que estos componentes requieran sustitución.
- **Estado de la inspección:** El ATL a debe indicar el estado actual de inspección de la aeronave, incluyendo el cumplimiento de las inspecciones requeridas especificadas por el fabricante o el programa de mantenimiento.
- **ADs (Directivas de Aeronavegabilidad):** Debe incluirse una lista completa de todas las directivas de aeronavegabilidad aplicables a la aeronave, junto con los registros de cumplimiento de dichas directivas.
- **Formulario 337:** El ATL debe incluir una lista de todas las reparaciones o alteraciones importantes realizadas en la aeronave, con referencias al formulario 337 asociado. Estos formularios documentan los detalles de estas reparaciones o alteraciones.

4.1.3 Relevancia en la aviación

El ATL desempeña un papel importante en varios aspectos de la aviación, sobre todo en la seguridad operacional, el mantenimiento, el cumplimiento de las normas y la toma de decisiones.

- **Seguridad Operacional:** Al proporcionar un registro detallado del historial de una aeronave y de su estado técnico actual, el ATL contribuye a garantizar que las aeronaves se mantengan en condiciones que garanticen su funcionamiento seguro. Los pilotos deben consultar el ATL antes de cada vuelo para conocer el estado de la aeronave. Además, tras la finalización de cada vuelo estos deben registrar en el ATL información del mismo así como cualquier defecto o problema encontrado para informar a los equipos de mantenimiento y dejar constancia para la siguiente tripulación.
- **Mantenimiento:** El ATL es una herramienta fundamental para las organizaciones de mantenimiento. Permite a los ingenieros de mantenimiento hacer un seguimiento de los defectos notificados y subsanarlos, planificar el mantenimiento preventivo y documentar el trabajo realizado. Además, constituye un registro de cuándo deben realizarse las inspecciones y comprobaciones rutinarias, lo que garantiza que el mantenimiento de la aeronave se realiza según lo previsto.

- **Conformidad:** El ATL constituye una parte crucial del proceso de conformidad. Los organismos reguladores, como la EASA y la FAA, imponen requisitos específicos para mantener y conservar los registros del ATL, que pueden ser inspeccionados durante las auditorías para garantizar el cumplimiento de la normativa. El ATL proporciona las pruebas necesarias de que la aeronave se ha mantenido de acuerdo con las leyes y reglamentos aplicables.
- **Toma de decisiones:** El ATL también es una valiosa fuente de información para la toma de decisiones. Mediante el análisis de los datos del ATL, los operadores pueden identificar tendencias en defectos, fiabilidad y actividades de mantenimiento, lo que les ayuda en la toma de decisiones relativas a los programas de mantenimiento, la adquisición de piezas y la gestión general de sus aeronaves mejorando por un lado la seguridad de las operaciones así como la disponibilidad de la flota.

4.2 Problemas y desafíos actuales con el Aircraft Technical Log

Como se ha visto el ATL desempeña un papel fundamental en el mantenimiento y la certificación de la aeronavegabilidad de las aeronaves. Registra cronológicamente todos los detalles del vuelo de la aeronave y las actividades de mantenimiento, permitiendo la transmisión fluida de información vital entre la tripulación de vuelo y el personal de mantenimiento en tierra. Sin embargo, los procesos actuales de ATL plantean varios problemas. Estos problemas se refieren principalmente a la gestión de datos en papel, la integridad de los datos, el intercambio de datos, auditorías y la disponibilidad de la información en tiempo real.

El primer problema surge de la naturaleza tradicionalmente en papel del ATL. En su forma más convencional, el ATL es un documento en papel, cumplimentado por pilotos e ingenieros, que permanece con la aeronave en todo momento. Las entradas manuales hacen que el proceso sea susceptible de errores humanos, escritura ilegible, omisión de información, daño o pérdida del ATL. Todo lo cual podría tener graves consecuencias en el mantenimiento y la seguridad de las aeronaves (Latorella & Prabhu, 2000).

Otro problema reside en la falta de transparencia, integridad de los datos y la trazabilidad de los registros. Con los sistemas actuales, ya sean en papel o centralizados, pueden producirse alteraciones o pérdidas de datos, ya sean accidentales o deliberadas. Esto podría dar lugar a casos de fraude, desinformación o interpretación errónea, poniendo en peligro la seguridad y la eficacia operativa de las aeronaves.

El tercer problema se refiere al intercambio eficaz de información. La práctica actual de ATL provoca a menudo retrasos en el intercambio de datos entre las distintas partes interesadas, incluidos pilotos, ingenieros de mantenimiento de aeronaves, gestores de operaciones y organismos reguladores. Esto podría obstaculizar la prontitud de las acciones de mantenimiento, alterar los horarios de vuelo y crear cargas económicas adicionales para las aerolíneas.

Además, la falta de disponibilidad de datos en tiempo real es uno de los principales inconvenientes de las prácticas ATL actuales. El acceso instantáneo a la información ATL no sólo es crucial para mantener unas operaciones de vuelo óptimas, sino también para garantizar respuestas rápidas a emergencias en vuelo o necesidades de mantenimiento imprevistas. El sistema actual no satisface plenamente las necesidades de datos en tiempo real de las operaciones aéreas modernas.

Por último, el ATL actual requiere un proceso de auditoría manual y exhaustivo para verificar la precisión de los registros. Esto puede ser lento, costoso y propenso a errores humanos. Además, el cumplimiento de los requisitos reglamentarios puede ser complicado debido a la dificultad de verificar la autenticidad e integridad de los registros.

4.3 Aircraft Technical Log utilizando tecnología blockchain

4.3.1 Análisis sobre el uso de Blockchain en el ATL

4.3.1.1 *Electronic Aircraft Technical Log*

Hasta el momento, en ocasiones, se ha estado haciendo referencia al uso de la tecnología blockchain como una solución en sí misma. Sin embargo, es importante destacar que blockchain por sí solo no es una solución completa para el ATL. En este trabajo estudiamos la blockchain como una tecnología de alto interés que se puede aplicar para modernizar el ATL. Por lo tanto, es necesario utilizarla en combinación con otras soluciones e innovaciones. En el caso del ATL, estamos hablando del Electronic Technical Log (ETL).

El ETL es una iteración del ATL en la cual se busca digitalizar el proceso de registro de eventos y mantenimiento de una aeronave. En esencia, ETL es un sustituto digital del proceso convencional en papel del ATL. Utiliza ordenadores, como portátiles, tabletas o dispositivos integrados en la cabina, para registrar y almacenar información que tradicionalmente se registraba en los formularios de papel. De este modo, se crea un registro digital completo de los datos técnicos de la aeronave.

Un ETL debe cumplir los mismos criterios que su homóloga en papel, ya que tiene ambos cumple la misma finalidad. Por ejemplo, debe permitir la creación de una copia de los registros del sector en tierra antes del despegue. Sin embargo, es importante entender que el ETL es meramente un sustituto del propio registro técnico físico en papel y no un sustituto de todo el proceso. Debe incluir funciones que permitan firmar y registrar correctamente los números de aprobación. Existen en la actualidad empresas como TrustFlight o NVABLE que ofrecen estas soluciones software para la aviación. Todas estas suelen tener las mismas funcionalidades mínimas:

- Registrar los datos del ATL en formato digital.
- Transmitir los datos del ordenador a un servidor.

- Pasar esos datos a la compañía aérea.
- Proporcionar accesibilidad y visibilidad directa a los datos.

El uso de estos registros electrónicos ETL puede aportar importantes ventajas ya que soluciona algunos de los problemas del ATL físico y puede ayudar a mejorar la eficacia operativa y la precisión de los datos. A continuación se presentan algunas de las principales ventajas:

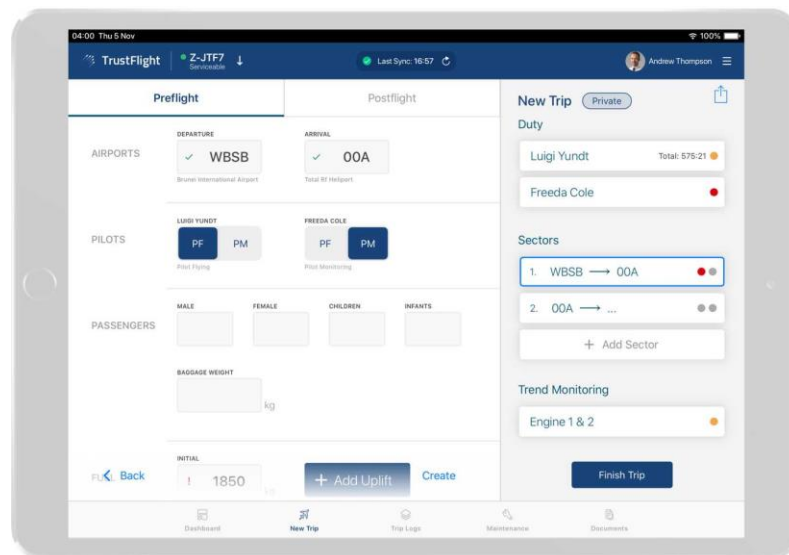


Figura 12. Interfaz ETL TrustFlight

- **Visibilidad en tiempo real:** ETL proporciona visibilidad al minuto del estado de la flota, lo que ayuda a simplificar el control de las tareas de mantenimiento y la planificación de la flota.
- **Reducción de errores:** ETL reduce los errores pudiendo automatizar cálculos, aplicando reglas de validación e integrando los flujos de datos. Esto mejora la precisión de los datos, eliminando los errores introducidos mediante procesos manuales.
- **Ahorro de tiempo:** ETL simplifica la revisión, transcripción y actualización de los registros técnicos, ahorrando tiempo en comparación con los procesos basados en papel.
- **Simplificación del Mantenimiento de Línea:** El ETL proporciona un acceso fácil a los datos sobre defectos, acciones correctivas y tareas fuera de fase, simplificando el control y la planificación del mantenimiento en la línea.
- **Alertas y mantenimiento predictivo:** ETL permite obtener alertas en tiempo real basadas en condiciones o umbrales específicos, facilitando la planificación proactiva del mantenimiento y las prácticas de mantenimiento predictivo.
- **Eficiencia y reducción de costes:** ETL elimina la introducción manual de datos, ahorrando tiempo y reduciendo las interrupciones para los pilotos, ingenieros y planificadores.

Sin embargo, también cabe mencionar algunos problemas y desafíos que el uso de ETL puede presentar.

- **Mantenimiento adicional:** El uso de ETL requiere un soporte operativo adicional que debe ser considerado. A menos que el dispositivo utilizado (como una computadora portátil o una tablet) esté permanentemente acoplado en la cabina de la aeronave y se cargue automáticamente, se deben realizar tareas adicionales para asegurar su funcionamiento adecuado. Esto puede incluir cargar regularmente la batería del dispositivo o realizar cambios físicos de batería. Dependiendo del hardware utilizado y las políticas de la aerolínea, también puede ser necesario intercambiar dispositivos de almacenamiento, como tarjetas SD, de acuerdo con las necesidades y procedimientos establecidos.
- **Nuevos modos de fallo:** A diferencia de los procesos en papel, la utilización de dispositivos electrónicos y la infraestructura para enviar y recibir datos introduce nuevos desafíos y posibles fallos como fallo del hardware, fallo del software o problemas en la transmisión de datos. Se deben establecer protocolos para mitigar estos nuevos posibles modos de fallo.
- **Manejo de los datos:** Durante la operación normal, los datos recopilados mediante el ETL generalmente se envían a la aerolínea. El método específico puede variar según la implementación del ETL, pero el resultado final es que la aerolínea recibirá regularmente un flujo de datos. Esto puede implicar la apertura de cortafuegos, la configuración de sitios FTP y la gestión de la entrada de datos, ya sea de forma manual o automática.
- **Formación:** Otro desafío importante asociado con el uso de ETL es la formación del personal. La formación del personal en el uso adecuado del ETL es crucial para garantizar una implementación exitosa y maximizar los beneficios del sistema, siendo necesario adaptar la formación a las necesidades y políticas específicas de cada aerolínea.

Los problemas y desafíos previamente expuestos serían también potencialmente extrapolables a una solución de ETL basada sobre tecnología blockchain. Además, también podemos identificar algunos problemas y desafíos específicos al utilizar esta tecnología en base a los problemas y desafíos previamente expuestos en las secciones anteriores.

- **Interoperabilidad:** Uno de los desafíos clave con el uso de un ETL basado en blockchain sería la interoperabilidad con otros sistemas. Como se ha visto anteriormente dado que blockchain es un conjunto relativamente nuevo de tecnologías, puede haber problemas de compatibilidad con sistemas existentes en la aerolínea, desde bases de datos operativas hasta sistemas de gestión de mantenimiento de aeronaves. Esto puede requerir una integración cuidadosa y posiblemente costosa para garantizar que los datos del ETL basado en blockchain se pueden usar de manera efectiva.
- **Seguridad y privacidad de los datos:** A pesar de que blockchain es conocido por su seguridad, la adopción de un ETL basado en blockchain puede plantear importantes consideraciones en términos de seguridad y privacidad de los datos. Dado que la blockchain mantiene un registro distribuido permanente de todas las transacciones, existe la posibilidad de que los datos sensibles se expongan si no se manejan adecuadamente. Además, las regulaciones de

privacidad y protección de datos, como el GDPR en la Unión Europea, también pueden presentar desafíos en términos de cumplimiento.

- **Adopción y resistencia al cambio:** Como con cualquier tecnología emergente, puede haber resistencia al cambio por parte de los usuarios finales. Esta resistencia puede surgir debido a la falta de comprensión de la tecnología blockchain, a las preocupaciones sobre la seguridad de los datos, o simplemente al temor al cambio. Para abordar esto, las aerolíneas tendrán que emprender iniciativas de cambio de gestión para educar a los empleados sobre los beneficios del ETL basado en blockchain y mitigar cualquier posible preocupación.
- **Escalabilidad:** A medida que el tamaño del blockchain crece, también lo hace la cantidad de datos que deben almacenarse y procesarse. En situaciones donde se recogen grandes volúmenes de datos esto puede convertirse en un problema. Los problemas de escalabilidad pueden hacer que la red se ralentice y que las transacciones tarden más tiempo en procesarse perdiendo efectividad.

4.3.1.2 ¿Deberíamos considerar blockchain?

A medida que la aplicabilidad de la tecnología blockchain se extiende a diversos sectores, incluida la aviación, se puede caer fácilmente en las tendencias del momento a la hora de aplicar una tecnología innovadora pudiendo ser innecesaria. Es por ello importante evaluar la idoneidad de dicha solución antes de su aplicación. Blockchain, con sus atributos inherentes de descentralización, inmutabilidad y transparencia, no es de aplicación universal, y puede que no siempre proporcione la solución óptima para determinadas aplicaciones. Por ello, se han desarrollado varios modelos de decisión para ayudar a las partes interesadas a comprender cuándo es mejor considerar la tecnología blockchain.

- **Árbol de decisiones:** Es un modelo de decisión que ofrece una forma directa de evaluar la necesidad y la eficacia potencial de una solución blockchain a través de una serie de preguntas. Siguiendo el árbol con cada una de las respuestas se llegará a una recomendación final sobre el uso de blockchain como tecnología en la solución planteada. En la figura 13 se puede ver un ejemplo de árbol de decisión para el uso de blockchain. El árbol de decisiones de blockchain ofrece un buen punto de partida para evaluar la necesidad de la tecnología blockchain, pero no en ocasiones no considera las complejidades que podrían surgir de los escenarios del mundo real, como las restricciones legales, los requisitos de infraestructura técnica o las consideraciones detalladas sobre la privacidad de los datos.
- **Lienzo de decisiones:** Este modelo amplía el alcance de la evaluación más allá del enfoque simplificado del árbol de decisiones. Profundiza en el escenario, explorando aspectos como los intereses de las partes interesadas, los riesgos potenciales que conlleva la implantación de la tecnología blockchain, valor añadido o la integridad de datos y procesos (Klein & Prinz, 2018). Este modelo de decisión reconoce la interconexión de los diversos factores que intervienen en la implantación de una cadena de bloques en el mundo real y hace hincapié en la importancia de considerar las implicaciones más amplias de la adopción de la tecnología blockchain. Sin embargo, aplicar el lienzo de decisiones a un caso de uso requiere un esfuerzo

considerable, así como un profundo conocimiento y experiencia tanto del caso de uso específico como de la propia tecnología blockchain.

- **Marcos de Idoneidad:** Estos modelos presentan el enfoque más detallado y exhaustivo. Consideran factores adicionales como la eficiencia del mecanismo de consenso, el tamaño de la red y los requisitos únicos de privacidad de los datos, entre otros (Almeshal & Alhogail, 2021). Estos modelos también tienen en cuenta las posibles limitaciones de la tecnología blockchain, como los problemas de escalabilidad, los costes energéticos de los mecanismos de prueba de trabajo o la complejidad de la programación de contratos inteligentes. Estos marcos proporcionan un análisis exhaustivo pudiendo resultar excesivos para escenarios más sencillos y requerir incluso más conocimientos y recursos que el lienzo de decisiones.

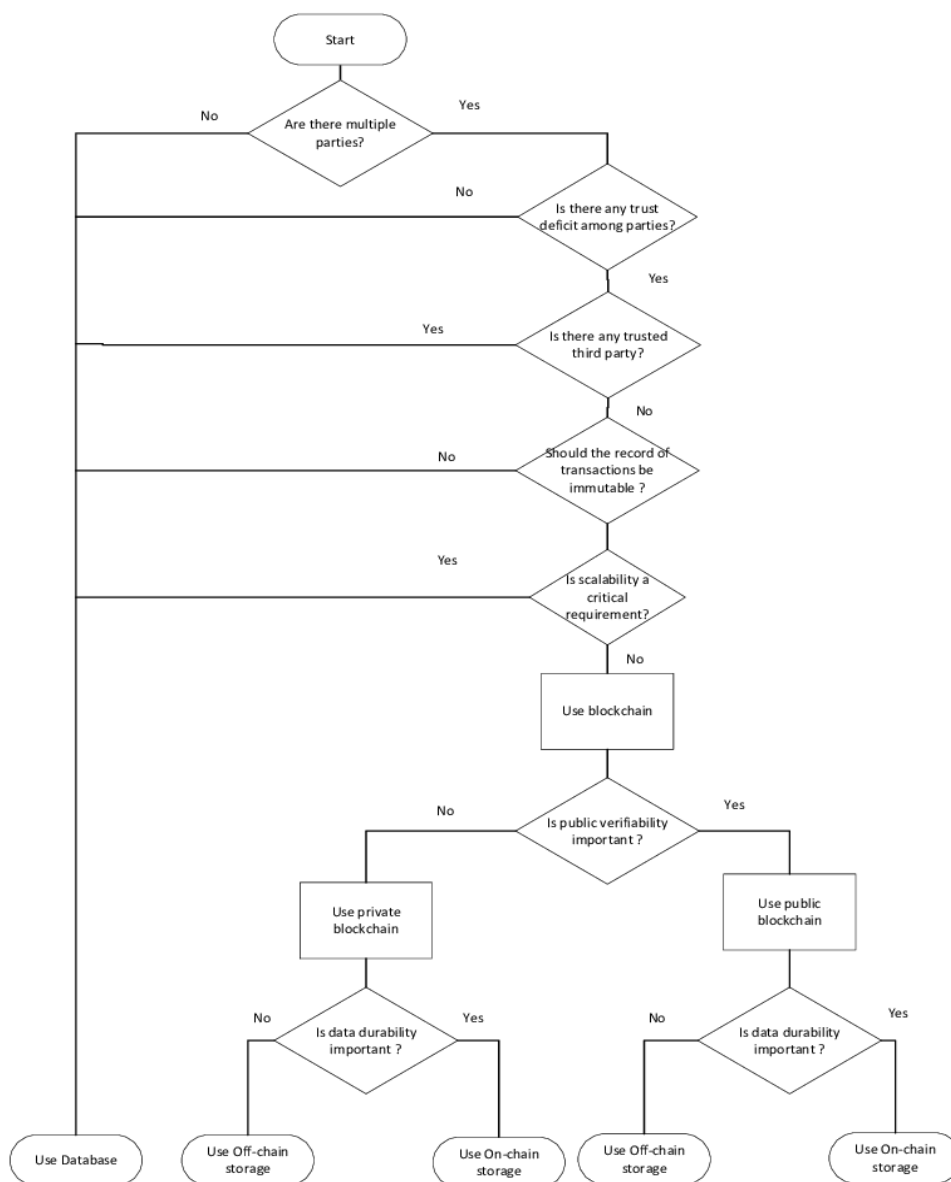


Figura 13. Ejemplo de árbol de decisión (Chowdhury et al., 2018)

Para el caso de uso de blockchain como tecnología combinada con un ETL se decidió utilizar un modelo de árbol de decisión para evaluar la idoneidad de la tecnología. Esto se debe a que aun conociendo sus limitaciones los árboles de decisión son sencillos y visualmente intuitivos, lo que facilita su comprensión e interpretación. Guían el proceso de toma de decisiones a través de una serie clara de opciones binarias (sí/no), lo que reduce la complejidad de la evaluación. Además, en 2018 IATA desarrolló un árbol de decisión para evaluar la idoneidad de utilizar tecnología blockchain en una solución, ver figura 14. Los nodos de decisión se han numerado para facilitar el seguimiento del modelo de decisión. La numeración azul indica bloque de pregunta y los verdes bloque de decisión. Para evaluar la posible aplicación de la tecnología blockchain en el contexto del ETL, aplicamos el modelo de árbol de decisiones IATA como marco estructurado para este análisis.

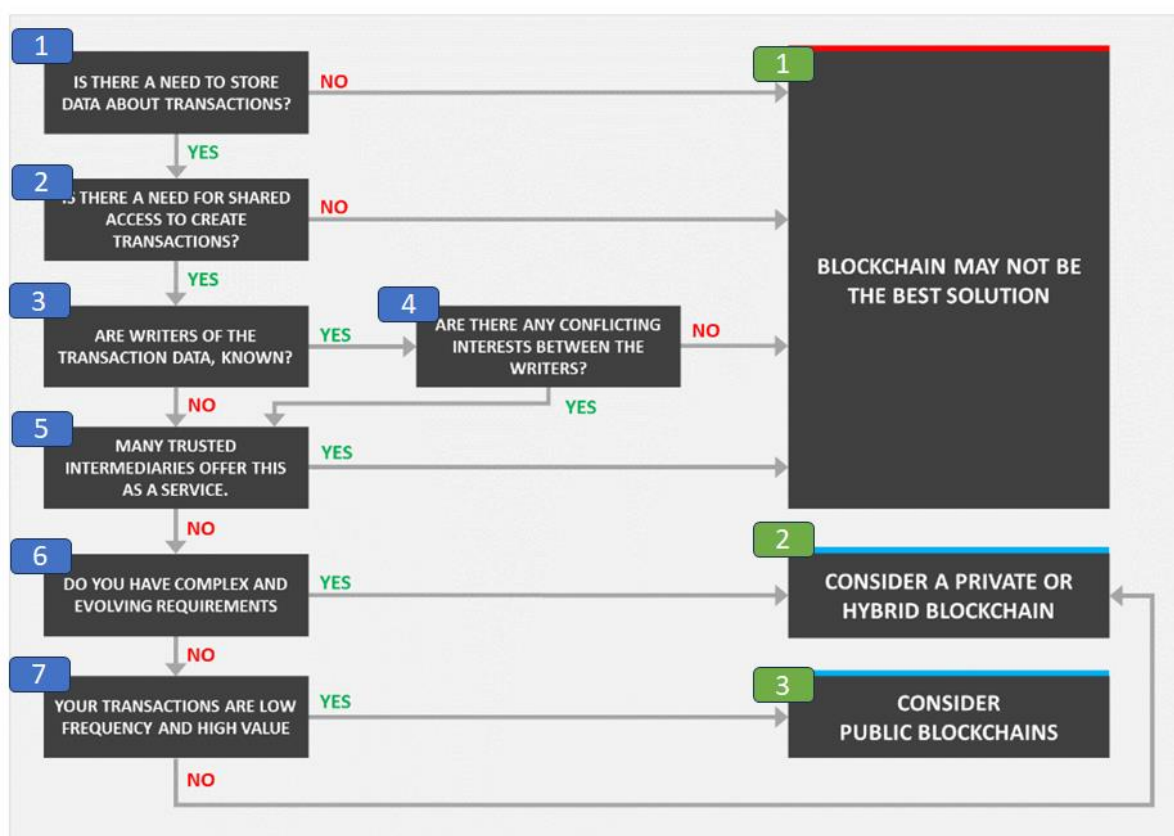


Figura 14. Árbol de decisión IATA (Goudarzi et al., 2018)

- **Pregunta 1:** En este primer bloque se debe evaluar si el caso de uso requiere almacenar datos sobre transacciones. El registro ETL implica intrínsecamente la documentación de una gran cantidad de datos transaccionales, como información sobre operaciones de vuelo, actividades de mantenimiento, consumo de combustible y otros detalles importantes relacionados con el funcionamiento y el rendimiento de la aeronave. Estos conjuntos de datos constituyen un componente crítico del cumplimiento de la normativa, la seguridad operativa y la eficiencia. Por lo tanto, la necesidad de almacenamiento de datos transaccionales es un atributo inherente de ETL. La respuesta sería "Sí" por lo que se iría ahora al segundo bloque de pregunta.

- **Pregunta 2:** El segundo bloque consiste en evaluar la necesidad de un acceso compartido para crear transacciones. En el contexto de ETL, el acceso compartido es un requisito crucial. Múltiples partes interesadas participan en la creación, modificación y revisión de los datos. Entre ellos se encuentran los pilotos, el personal de mantenimiento y el personal administrativo tanto de la aerolínea como de los organismos reguladores. La necesidad de atender a esta multitud de usuarios que se autentifican e interactúan con el sistema justifica la necesidad del acceso compartido. La respuesta por tanto sería "Sí", y se iría al tercer bloque de pregunta.
- **Pregunta 3:** En el tercer bloque se evalúa si los redactores de los datos de la transacción son entidades conocidas. En el contexto de la ETL, los redactores o entidades que aportan datos son identificables y conocidos, incluido el personal identificable de la aerolínea, como pilotos, personal de mantenimiento y otro personal administrativo. Por lo que la respuesta sería "Sí", y se iría al cuarto bloque de pregunta.
- **Pregunta 4:** En el cuarto bloque se analiza la posible presencia de intereses contrapuestos entre los redactores de datos. En el caso del ETL, hay distintas partes interesadas que pueden tener prioridades diferentes. Por ejemplo, el personal de mantenimiento puede dar prioridad a minimizar el tiempo de inactividad y, por tanto, preferir menos tareas de mantenimiento, mientras que los pilotos o los responsables de seguridad de las aerolíneas se inclinarían por comprobaciones y mantenimiento exhaustivos para garantizar la seguridad y el cumplimiento de las normas. Por lo que se puede considerar que existen conflictos de intereses. Por lo que la respuesta sería "Sí", y se iría al quinto bloque de pregunta.
- **Pregunta 5:** El quinto bloque evalúa la existencia de intermediarios de confianza que ofrecen este tipo de servicio. En la actualidad, hay muy pocos intermediarios, si es que hay alguno, que ofrezcan servicios integrales basados en blockchain para ETL. Dada esta falta de proveedores de servicios intermediarios de confianza en este campo específico, la respuesta a este bloque sería "No", y se pasaría al sexto bloque.
- **Pregunta 6:** El sexto bloque evalúa la complejidad y el carácter dinámico de los requisitos del sistema. El campo de la aviación está en continua evolución. Los avances tecnológicos, los cambios en los procedimientos operativos, las modificaciones en las normas de seguridad y la evolución de los requisitos reglamentarios contribuyen a crear un entorno muy dinámico con requisitos complejos. Por lo tanto, para este bloque de decisión la respuesta sería "Sí".
- **Decisión 2:** La decisión final del árbol, basada en las anteriores respuestas, sería la del uso de una red blockchain de tipo privada o híbrida para el caso de uso del ETL. Los sistemas blockchain privados o híbridos pueden proporcionar la flexibilidad, solidez y seguridad necesarias para adaptarse a los requisitos complejos, evolutivos y multilaterales de las ETL en la aviación.

En resumen, el análisis efectuado a través del árbol de decisión de la IATA sugiere que una blockchain privada o híbrida puede ser una alternativa viable para la implementación en un sistema ETL. En la sección 4.3.2, se examinarán las consideraciones principales para el desarrollo de una solución ETL basada en blockchain, proporcionando así una guía inicial para su desarrollo.

4.3.1.3 Análisis comparativo de posibles soluciones de ATL

En esta sección se realizará un análisis comparativo de las diferentes soluciones propuestas hasta ahora para el Aircraft Technical Log:

1. **PTL:** Registro tradicional en formato físico (papel) que recopila la información relacionada con el mantenimiento y las operaciones.
2. **ETL:** Registro electrónico en una base de datos convencional que almacena la información relacionada con el mantenimiento y las operaciones.
3. **BTL:** Registro electrónico utilizando tecnología blockchain para almacenar la información relacionada con el mantenimiento y las operaciones.

En la tabla 3 se presenta el análisis comparativo en diferentes áreas de las mencionadas soluciones ATL.

Tabla 3. Matriz comparativa de diferentes modelos de ATL

	PTL	ETL	BTL
Acceso a los datos	Limitado: Debido a que los registros físicos no pueden proporcionar acceso en tiempo real a los datos.	Mejorado: Se puede acceder a los datos en tiempo real siempre que se cuente con una conexión a internet.	Mejorado: Similar al ETL proporcionando acceso a los datos en tiempo real a todas las partes autorizadas de la red.
Seguridad	Baja: Es vulnerable a la pérdida o daño físico. Además, es susceptible a posibles alteraciones sin control de versión o edición..	Media: Es vulnerable a ciberataques causando pérdida o manipulación de los datos. Depende del grado de ciberseguridad del sistema.	Alta: Proporciona un elevado nivel de seguridad gracias principalmente a la encriptación y descentralización. Además, cada transacción es inmutable y verificable, lo que reduce el riesgo de manipulación.
Trazabilidad	Baja: En el registro físico puede ser difícil establecer un historial de modificaciones o accesos.	Moderada: Los sistemas electrónicos pueden mantener un historial de cambios, pero rastrear el acceso no autorizado o las alteraciones aún	Muy alta: La blockchain registra todas las transacciones, lo que proporciona un historial completo e inmutable de cambios.

		puede ser un desafío	
Transparencia	Baja: Difícil compartir información a través de los diferentes interesados. Requiere transporte físico de los registros.	Moderada: Los registros electrónicos permiten un mejor intercambio de información. Sin embargo, los problemas de acceso a los datos pueden persistir.	Muy alta: Por lo general todos los participantes en la blockchain tienen acceso a la misma información. Esto aporta transparencia y confianza a la solución.
Integridad de los datos	Moderada: Las firmas físicas se utilizan para garantizar la integridad y conformidad con la información pero pueden ser fácilmente falsificadas.	Alta: Los registros electrónicos pueden utilizar firmas digitales para verificar la autenticidad de los datos. Sin embargo, estos sistemas dependen de la seguridad del proceso de creación y verificación de firmas.	Muy alta: La blockchain utiliza firmas criptográficas digitales para garantizar la autenticidad de los datos. Una vez que los datos están registrados, el original permanece inalterado, garantizando su integridad y autenticidad.
Redundancia	Baja: Una vez perdidos o dañados, los registros físicos no pueden ser recuperados.	Alta: Los registros electrónicos suelen tener protocolos de respaldo “back-up” para prevenir la pérdida total de los datos.	Alta: Cada participante en la red de blockchain mantiene una copia del registro completo, asegurando la redundancia de los datos.
Eficiencia	Baja: La entrada manual de datos, la transferencia física de registros y la búsqueda manual son procesos inherentemente lentos y propensos a errores.	Alta: Los registros electrónicos permiten una entrada, transferencia y búsqueda de datos más rápidas y precisas, mejorando la eficiencia del proceso.	Muy alta: Los sistemas basados en blockchain permiten la transferencia automática y segura de datos entre partes. El uso de contratos inteligentes puede ayudar a automatizar procesos, haciendo el proceso altamente eficiente.
Escalabilidad	Baja: La escalabilidad de los registros	Alta: Los registros electrónicos son	Moderada a alta: Los sistemas de blockchain

	basados en papel tiene una escalabilidad costosa y compleja.	generalmente fácilmente escalables aunque el aumento del volumen de datos puede requerir más almacenamiento y capacidad de procesamiento.	pueden ser escalables, pero la complejidad de la red y la necesidad de almacenamiento y capacidad de procesamiento pueden aumentar con el número de participantes y/o transacciones.
Auditabilidad	Baja: La auditoría de registros basados en papel puede ser un proceso lento y propenso a errores debido al manejo manual de los datos.	Alta: Los sistemas electrónicos simplifican el proceso de auditoría. Los datos digitales pueden ser fácilmente buscados, ordenados y analizados.	Muy alta: En blockchain, cada transacción queda completamente registrada, simplificando las auditorías.
Interoperabilidad	Baja: Los registros en papel son difíciles de integrar con otros sistemas o procesos digitales. Esto puede limitar la interoperabilidad.	Moderada a alta: Los registros electrónicos pueden diseñarse para integrarse con otros sistemas. Sin embargo, esto puede variar dependiendo del diseño del sistema y pudiendo surgir problemas de compatibilidad.	Moderada a alta: La blockchain puede diseñarse con APIs y contratos inteligentes para facilitar la integración con diversos sistemas y procesos.
Riesgo de Error Humano	Alto: La entrada manual de datos es propensa a errores humanos, lo que puede resultar en errores en la información.	Bajo: La entrada de datos electrónicos puede reducir la posibilidad de errores.	Bajo: Los sistemas de blockchain pueden automatizar muchos procesos, lo que reduce el riesgo de error humano.
Coste	Moderado: Los costes de impresión, almacenamiento, entrada manual de datos y transferencia pueden ser elevados y acumularse con el	Variable: La inversión inicial en registros electrónicos (software, hardware y capacitación) puede ser significativa. Sin embargo, con el tiempo, las ganancias	Variable: Los costes iniciales de implementación de la blockchain también pueden ser altos. Sin embargo, estos costes pueden verse compensados con el

	tiempo.	de eficiencia pueden superar estos costes iniciales.	tiempo debido a la eficiencia operativa mejorada y la reducción de los costes de auditoría.
Facilidad de Implementación	Alta: Los registros en papel son fáciles de implementar ya que no requieren ninguna infraestructura técnica especializada.	Moderada: Los registros electrónicos requieren de una infraestructura técnica y conocimientos para su implementación.	Baja: La implementación de la blockchain requiere una comprensión técnica significativa y la migración desde los sistemas existentes puede ser compleja. Además, es necesario garantizar la adopción y aceptación por parte de todos los participantes en la red.
Madurez de la Tecnología	Alta: La tecnología de registro en papel está muy asentada en la actualidad.	Moderada a alta: Aunque la industria de la aviación a veces es muy reacia al cambio, los registros electrónicos se están empezando a adoptar ampliamente y su tecnología está bien establecida y demostrada.	Moderada: La blockchain es una tecnología relativamente nueva y todavía está evolucionando. Aunque ha sido adoptada en varias industrias, todavía hay áreas de su aplicación que están siendo exploradas y desarrolladas.

Del análisis comparativo de soluciones recogido en la tabla 3, se puede concluir que el uso de la tecnología blockchain en los registros técnicos de aeronaves (BTL) tiene el potencial de superar las limitaciones presentes tanto en los registros en papel (PTL) como en los electrónicos (ETL). La BTL ofrece una mayor transparencia, trazabilidad, seguridad, eficiencia e integridad de los datos, y proporciona una solución más robusta para la auditoría y la resiliencia a fallos técnicos. Sin embargo, también es importante tener en cuenta que la implementación de la blockchain puede ser más compleja y costosa inicialmente, y la madurez de la tecnología todavía está en desarrollo. A pesar de estos desafíos, las ventajas potenciales que la blockchain puede ofrecer, como la mejora de la gestión de datos y la reducción de errores y disputas, la posicionan como una solución prometedora para mejorar la gestión de los registros técnicos de aeronaves.

4.3.2 Consideraciones en el diseño y desarrollo de un ATL basado en Blockchain

En esta sección se abordan las consideraciones de diseño para un ATL basado en tecnología Blockchain. El objetivo es ofrecer un conjunto de pautas que habría que considerar al planificar el diseño y desarrollo de este sistema de ATL. Es importante destacar que estas consideraciones no constituyen un plan exhaustivo para el proceso de diseño y desarrollo, sino que pretenden actuar más a modo de guía para resaltar aspectos clave que requieren una comprensión exhaustiva y una deliberación cuidadosa. Los principales aspectos a considerar abarcan:

- Identificación de las partes interesadas y los usuarios
- Elección del tipo de blockchain
- Estructura de datos
- Diseño de la interfaz de usuario
- Integración del sistema
- Utilización de contratos inteligentes
- Seguridad
- Escalabilidad
- Rendimiento
- Cumplimiento normativo
- Costes

Cada uno de estos factores desempeñan un papel fundamental en el diseño y desarrollo de una solución exitosa, eficiente y segura de ATL basada en blockchain. A través de este enfoque exploratorio y holístico, se busca poder ayudar a futuros desarrolladores e investigadores a crear un sistema bien diseñado y completo que aproveche el poder de la tecnología blockchain, al tiempo que se mitiguen los posibles obstáculos y desafíos.

4.3.2.1 *Identificación de partes interesadas y usuarios*

Al desarrollar cualquier sistema nuevo, resulta fundamental identificar con precisión a las partes interesadas y a los usuarios que interactuarán con dicho sistema o que se verán afectados por él. Este paso es de vital importancia, ya que permite comprender sus necesidades, preocupaciones y expectativas, lo que a su vez proporciona información valiosa para moldear el proceso de diseño, desarrollo e implementación. Al tener claridad sobre quiénes son los actores involucrados y cuáles son sus requisitos, se puede garantizar que el sistema se ajuste de manera óptima a sus demandas y logre los objetivos previstos. Además, al involucrar a las partes interesadas desde las etapas iniciales, se fomenta la colaboración y se obtiene una visión más completa de los diferentes aspectos que deben tenerse en cuenta. Para ello se debe identificar quienes son las partes directamente interesadas y las partes indirectamente afectadas por el nuevo sistema, quienes son los usuarios y sus requisitos así como definir una estrategia de colaboración con las partes interesadas y los usuarios durante el desarrollo del sistema.

Empezando por la identificación de las partes directamente interesadas, estas son aquellas que interactúan directamente con el ATL como parte de sus funciones. Cada parte interesada puede tener necesidades y requisitos específicos que deben tenerse en cuenta a la hora del diseño y desarrollo de un ATL basado en blockchain. Se pueden identificar las siguientes partes directamente interesadas:

- **Operador Aéreo:** Principalmente compañías aéreas que explotan las aeronaves. Estas dependen directamente de los datos del ATL para una gestión eficaz y segura de su flota. Les proporciona información esencial sobre el estado de las aeronaves, la eficiencia del combustible, las necesidades de mantenimiento y otros aspectos operativos críticos. Un sistema ATL basado en blockchain tiene el potencial de ofrecer los datos fiables en tiempo real que puedan mejorar su eficiencia operativa, reducir el tiempo de inactividad y optimizar la programación.
- **Personal de Mantenimiento:** Este grupo incluye a técnicos, ingenieros y demás personal responsable de realizar las comprobaciones y el mantenimiento periódicos de las aeronaves. El ATL es una herramienta esencial para ellos, ya que contiene información detallada sobre el historial de la aeronave, incluidos los trabajos de mantenimiento previamente realizados, fallos identificados y las correcciones necesarias. La solución ATL blockchain permitirá realizar registros rápidos y sin errores y proporcionar historiales de mantenimiento actualizados y fácilmente accesibles.
- **Tripulación de Vuelo:** Esto incluye a los pilotos así como al resto de la tripulación de abordo. Es crucial para ellos contar con un registro con una interfaz sencilla, con actualizaciones fiables en tiempo real sobre cualquier problema o notificación de mantenimiento. Con él ATL se realizan las comprobaciones previas al vuelo necesarias para asegurarse de que la aeronave es segura para la operación. Un sistema blockchain puede ofrecer una presentación clara, concisa, actualizada y fiable de los datos relevantes para la tripulación de vuelo, ayudándoles a comprender rápidamente cualquier posible problema potencial.
- **Autoridad Reguladora/Supervisora:** Entidades como EASA o la FAA necesitan acceder a los datos ATL para garantizar el cumplimiento de la normativa y las normas de seguridad, y para llevar a cabo investigaciones cuando sea necesario. Necesitan un amplio acceso a los datos, sólidas capacidades de búsqueda y garantías de integridad de los datos. Un ATL basado en blockchain podría proporcionar un registro transparente e inmutable, facilitando su función de supervisión y auditoría.
- **Desarrolladores Blockchain:** En este grupo estará el personal encargado de diseñar, implantar y mantener el sistema ATL basado en blockchain. Necesitan directrices y requisitos claros, así como información constante de las otras partes directamente interesadas, para garantizar que el sistema cumple los objetivos y necesidades previstas. Es su responsabilidad abordar cualquier desafío técnico, implementar actualizaciones y garantizar el buen funcionamiento de todo sistema.

También es importante identificar a aquellas partes interesadas indirectamente, que no interactúan directamente con la ATL, pero cuyas funciones y/u operaciones se ven influidas. Estas partes interesadas indirectas suelen necesitar datos fiables y puntuales así como la garantía de su exactitud. Posibles partes interesadas indirectas son:

- **Control del tráfico aéreo (ATC):** Los controladores aéreos deben garantizar el movimiento seguro y ordenado de las aeronaves tanto en tierra como en el aire. Aunque no interactúan directamente con el ATL, dependen de la actualización precisa y puntual del estado de las aeronaves. Un sistema ATL ineficaz podría dar lugar a la circulación de información incorrecta, lo que podría afectar indirectamente a sus operaciones. Un sistema ATL basado en blockchain, con su promesa de actualizaciones verificables en tiempo real, podría proporcionar una capa adicional de fiabilidad y seguridad en los datos que utilizan para tomar decisiones.
- **Gestión aeroportuaria:** Los gestores de aeropuertos son responsables del buen funcionamiento de numerosas tareas interrelacionadas en el ámbito de un aeropuerto. Unos datos ATL fiables pueden ayudar a garantizar el mantenimiento a tiempo, reducir los posibles retrasos y optimizar la programación de los recursos aeroportuarios. Por ejemplo, si un avión requiere mantenimiento, se puede planificar en consecuencia para liberar espacio en las puertas de embarque o reorganizar los horarios, reduciendo las interrupciones generales. Con la tecnología blockchain se podría proporcionar a la gestión aeroportuaria una mayor visibilidad y previsibilidad en sus operaciones.
- **Pasajeros:** Aunque los pasajeros tampoco interactúan directamente con el ATL, su seguridad, comodidad y experiencia de vuelo están significativamente influenciadas por la información contenida en él. Los datos precisos y puntuales de la ATL pueden reducir los retrasos y las cancelaciones de vuelos, y mejorar la seguridad general de las operaciones de vuelo. Todo esto conduce a una mayor satisfacción de los pasajeros. Por ello, una ATL basada en blockchain puede contribuir indirectamente a mejorar la experiencia de los pasajeros.

Continuando con la identificación de usuarios y sus requisitos, la identificación de los usuarios finales del sistema ATL basado en blockchain desempeña un papel integral en el diseño y funcionalidad del sistema final. Los usuarios serán las personas que interactúen directamente con el sistema y dependerán de él para una parte significativa de su trabajo. Identificar a estos usuarios, comprender sus funciones y especificar sus requisitos es crucial para crear un sistema que sea eficiente, intuitivo y capaz de satisfacer plenamente sus necesidades. Las tres acciones clave son las siguientes:

1. **Identificación de las funciones de los usuarios:** Las funciones de los usuarios suelen coincidir con aquellas de las partes directamente interesadas, ya que son las personas que interactúan directamente con el ATL. Sin embargo, dentro de estos puede haber distintos roles de usuario basados en funciones laborales específicas que desempeñen. Por ejemplo, entre el propio personal de mantenimiento puede haber roles distintos. Por un lado aquellos encargados de introducir los datos en el sistema y, por otro, aquellos que analizan la información suministrada para la toma de decisiones acorde. Cada función tendrá unos requisitos específicos que deben definirse claramente para que el sistema pueda satisfacerlos eficazmente.

2. **Definición de los requisitos de los usuarios:** Debido a que habrá usuarios con diferentes roles esto significa que cada uno podrá tener unos requisitos específicos para el sistema ATL. Por ejemplo, el personal de mantenimiento necesitará una interfaz que les permita registrar con precisión los trabajos de mantenimiento realizados. Esto puede requerir campos personalizables, sellado automático de tiempo y una manera fácil de revisar registros anteriores. Por otro lado, las autoridades reguladoras pueden requerir un amplio acceso a los datos así como capacidades de búsqueda avanzadas para poder revisar eficazmente los historiales de las aeronaves y garantizar el cumplimiento de la normativa. Definir estos requisitos en una fase temprana del proceso de diseño puede ayudar a garantizar que el sistema satisface las necesidades de todos los usuarios.
3. **Interacción del usuario con el sistema:** La frecuencia y naturaleza de las transacciones que cada usuario tendrá con el sistema es otra consideración clave. Algunos usuarios pueden interactuar con el sistema ATL varias veces al día, mientras que otros pueden hacerlo con menos frecuencia. Algunos tendrán que introducir datos, mientras que otros se dedicarán exclusivamente a recuperarlos y analizarlos. Comprender estas interacciones diferentes puede informar el diseño de la interfaz de usuario y las funcionalidades del sistema, así como a la gestión de permisos y roles.

Por último, es fundamental mantener una colaboración y comunicación constante con las partes interesadas y los usuarios a lo largo de todo el proceso de diseño, desarrollo e implementación para garantizar el éxito del sistema. Esto garantizará que el sistema se construya teniendo en cuenta todas las necesidades e intereses de los usuarios, así como facilitará su adopción. Para construir y mantener esta colaboración y comunicación se debe realizar lo siguiente:

- **Compromiso Temprano:** Obtener el compromiso temprano de las partes interesadas y los usuarios puede ayudar a dar forma en gran medida al diseño inicial y la funcionalidad del sistema ATL. Al involucrar a los usuarios y las partes interesadas desde el principio, los desarrolladores del sistema pueden alinear el diseño del sistema con las necesidades de sus usuarios finales, mitigando el riesgo de cambios significativos más adelante en el proceso.
- **Comunicación Regular:** La comunicación constante a lo largo del proceso de desarrollo es crucial. Actualizaciones regulares e informes de progreso pueden asegurar que todas las partes estén al tanto del estado del desarrollo del sistema y de cualquier problema o retraso potencial. También ofrece la oportunidad a las partes interesadas y los usuarios de ofrecer comentarios o expresar inquietudes durante la fase de desarrollo.
- **Bucles de Retroalimentación:** Establecer mecanismos de retroalimentación continua de los usuarios y partes interesadas es esencial. Estos bucles de retroalimentación pueden ser tanto formales (revisiones programadas) como informales (comentarios y sugerencias espontáneas). La retroalimentación será especialmente valiosa durante las pruebas iniciales permitiendo solventar cualquier problema antes de su despliegue en operaciones reales.
- **Formación y Soporte:** Para una implementación y adopción exitosas, las partes interesadas y los usuarios deben sentirse seguros de su capacidad para utilizar y mantener el nuevo sistema. Establecer programas de formación y mecanismos de soporte continuo pueden facilitar esto.

- **Revisión Post-Implementación:** Tras una implantación de sistema sería importante mantener el compromiso de las partes interesadas y los usuarios. Las revisiones posteriores a la implementación pueden ofrecer ideas sobre desafíos o beneficios inesperados, informar sobre actualizaciones o ajustes, y ayudar a evaluar la satisfacción general con el sistema.

La identificación de las partes interesadas y los usuarios, comprender sus requisitos y mantener un compromiso constante con ellos es un pilar fundamental para diseñar con éxito un sistema ATL basado en blockchain. Este enfoque garantiza que el sistema satisfaga sus necesidades, sea fácil de usar y maximice los beneficios de la tecnología blockchain. Establece el escenario para los siguientes pasos de consideraciones de diseño en el desarrollo de una solución robusta, confiable y efectiva que mejore la seguridad, eficiencia y transparencia.

4.3.2.2 Elección de tipo de Blockchain

Como ya se ha comentado en la sección 2.1.4., la tecnología blockchain se presenta en diversas variantes, cada una con sus características distintivas.

- **Blockchain Públicas:** Están abiertas a cualquier persona para participar. Las transacciones son transparentes e inmutables, proporcionando un alto grado de descentralización.
- **Blockchain Privadas:** Restringidas a miembros u organizaciones específicas, ofrecen un mayor grado de control sobre los datos. La privacidad se mejora ya que el acceso está limitado, lo que las hace potencialmente adecuadas para industrias que manejan información confidencial.
- **Blockchain de Consorcio:** Estas son administradas de manera colaborativa por un grupo de organizaciones, equilibrando entre la descentralización de las blockchains públicas y el control de las privadas. Pueden ofrecer privacidad y control al tiempo que mantienen cierto nivel de confianza entre los participantes.
- **Blockchain Híbridas:** Su objetivo es aprovechar lo mejor de ambos mundos al ofrecer la transparencia y seguridad de una blockchain pública mientras se conserva la privacidad y el control de una blockchain privada. El equilibrio entre estas características depende del diseño específico de la blockchain híbrida.

Las características de cada uno de estos tipos de blockchain distintos se tendrá que tener en cuenta para el diseño del sistema. Los requisitos específicos del sistema ATL tendrán un papel significativo en determinar qué tipo de blockchain sería más adecuada. Algunos de los aspectos clave a considerar en relación con la selección de blockchain incluyen:

- **Privacidad de los datos:** El ATL contiene a menudo información sensible sobre las aeronaves y sus registros de mantenimiento. Esto requiere un sistema que garantice la privacidad de los datos, lo que podría favorecer las cadenas de bloques privadas, de consorcio o híbridas frente a las públicas.

- **Control de acceso:** La naturaleza de los participantes que accederán al sistema ATL y el nivel de control necesario sobre sus derechos de acceso es otro factor. Esto podría influir en si es más adecuado un blockchain privado, de consorcio o híbrido.
- **Nivel de confianza:** Si el sistema ATL está destinado a ser utilizado entre entidades con distintos niveles de confianza, esto podría favorecer a los blockchains de consorcio o híbridos. Estos tipos de blockchain pueden ofrecer un equilibrio entre transparencia y control.
- **Cumplimiento normativo:** La industria de la aviación está sujeta a estrictas regulaciones. Estas normativas, en particular las relativas a la privacidad de los datos y la auditabilidad, desempeñarán un papel importante a la hora de decidir el tipo de blockchain.
- **Escalabilidad:** El volumen de datos y la velocidad a la que deben procesarse las transacciones en el sistema ATL también pueden afectar a la elección de blockchain. Mientras que las cadenas de bloques públicas pueden gestionar grandes volúmenes, las cadenas de bloques privadas, de consorcio o híbridas pueden ofrecer una mayor velocidad de transacción.

A continuación, en la tabla 4, se presenta un breve análisis comparativo de las características de los diferentes tipos de blockchain en el caso de estudio de un sistema ATL.

Tabla 4. Análisis comparativo de tipos de blockchain para un sistema ATL

Características	Blockchain Pública	Blockchain Privada	Blockchain de Consorcio	Blockchain Híbrida
Privacidad de los datos	Baja	Alta	Media	Customizable
Control de acceso	Bajo	Alto	Medio	Customizable
Nivel de confianza	Alto	Bajo	Medio	Customizable
Cumplimiento normativo	Varia	Alto	Alto	Customizable
Escalabilidad	Baja	Alta	Media	Customizable
Coste por transacción	Alto	Bajo	Medio	Customizable
Performance	Bajo	Alto	Medio-Alto	Customizable
Interoperabilidad	Alta	Baja-Media	Media	Customizable

El análisis realizado en la tabla 4 no es un análisis exhaustivo, simplemente pretende proporcionar una visión general comparativa. Se necesitaría llevar a cabo un análisis más preciso y detallado donde se tendría que tener en cuenta las necesidades de las diferentes redes así como tener definidos los requisitos normativos, las expectativas de las partes interesadas, la integración necesaria con otros sistemas, consideraciones de costes y las necesidades futuras de escalabilidad.

Una vez completado este análisis más exhaustivo de los distintos tipos de blockchain en relación con las necesidades del sistema ATL se podría realizar la selección final. No se trata simplemente del tipo de cadena de bloques que obtenga la puntuación más alta en la tabla, sino del que más se ajuste a los requisitos, limitaciones y prioridades específicos del sistema ATL. La justificación de la elección final debe exponerse claramente y estar respaldada por el análisis comparativo. Esta explicación debe incluir las razones por las que se aceptan o descartan ciertos rasgos, la alineación de la blockchain elegida con los requisitos del sistema ATL y cómo el tipo de blockchain seleccionado da cabida al equilibrio necesario entre control, privacidad, transparencia y eficiencia.

Por último, es importante tener en cuenta que la tecnología blockchain no es estática y está en constante evolución. Pueden surgir nuevas soluciones, y las existentes pueden evolucionar para satisfacer mejor las demandas del caso de uso específico. Por lo tanto, y cuando sea posible, la elección final del tipo de red debe ser adaptable y estar abierta a futuros avances tecnológicos y modificaciones.

4.3.2.3 Estructura de datos

En el diseño y desarrollo de un ATL basado en blockchain, uno de los aspectos importantes a tener en cuenta es el diseño de la estructura de datos. Por un lado, la singularidad de los datos ATL y por otro las capacidades y limitaciones inherentes a la tecnología blockchain, hacen que se requiera una planificación y un diseño cuidadosos. Esta sección tiene como objetivo proporcionar una visión general de las consideraciones críticas y directrices para el diseño de una estructura de datos eficaz para un sistema ATL basado en blockchain.

Es crucial comprender la naturaleza y los requisitos de los datos ATL para poder diseñar una estructura de datos adecuada de un sistema ATL basado en blockchain. Normalmente, como ya se ha visto en la sección 4.1, los datos ATL incluyen información sobre operaciones de vuelo, mantenimiento de aeronaves, fallos técnicos, rectificaciones y otros detalles relevantes para la aeronavegabilidad. Cada categoría de datos tiene su propia importancia. Por ejemplo, los datos de vuelo son cruciales para supervisar el uso de la aeronave y planificar los programas de mantenimiento. Los datos de mantenimiento constituyen la columna vertebral del historial de servicio de la aeronave y contribuyen a garantizar la seguridad y el cumplimiento de la normativa. Los datos de averías y rectificaciones son vitales para solucionar problemas y mejorar la fiabilidad de la aeronave. Además, es importante tener en cuenta que los datos ATL suelen ser secuenciales y con fecha y hora, lo que los hace especialmente adecuados para la estructura inherente de una blockchain. Una comprensión clara de estas características de los datos ATL será clave para adaptar la estructura de datos de la blockchain para acomodar y gestionar de forma óptima esta información.

Antes de diseñar la estructura de datos para un sistema ATL, es importante revisar cómo se organizan normalmente los datos en blockchain. Una blockchain es una cadena de bloques, donde cada bloque contiene una lista de transacciones que pueden ser cualquier tipo de intercambio de datos. Los bloques están conectados entre sí mediante enlaces criptográficos, creando una cadena de datos rastreable e inmutable.

Sin embargo, debido a los diversos y únicos requisitos de los datos ATL, la estructura de datos de la cadena de bloques debe personalizarse en consecuencia. Esta personalización garantizará que el sistema pueda manejar de manera efectiva y segura los diferentes tipos de datos, manteniendo la integridad y trazabilidad que ofrece blockchain.

Teniendo en cuenta los requisitos únicos de los datos ATL y la estructura básica de una cadena de bloques, queda claro que un sistema ATL basado en blockchain requerirá una estructura de datos cuidadosamente adaptada. Aunque la estructura tradicional basada en transacciones sigue siendo relevante, debe ajustarse para gestionar la naturaleza diversa y compleja de los datos ATL.

Por ejemplo, los registros de mantenimiento de una aeronave requerirán una estructura que pueda capturar, almacenar y recuperar de manera eficiente información compleja anidada, como detalles de piezas sustituidas, resultados de inspecciones, nombres y credenciales del personal autorizado, entradas con fecha y hora, entre otros. Además, algunos elementos de los datos ATL deben ser fácilmente localizables y analizables, lo que implica que la estructura de datos debe admitir funcionalidades potentes de indexación y análisis.

Otro aspecto clave en el diseño de la estructura de datos es encontrar el equilibrio entre redundancia de datos y eficiencia de almacenamiento. Aunque la naturaleza de blockchain implica la replicación de datos en la red, es importante considerar la eficiencia de almacenamiento debido al gran volumen de datos generados. Por lo tanto, se pueden considerar mecanismos como la poda de datos, el almacenamiento fuera de la cadena o el uso de IPFS (InterPlanetary File System) (Kumar & Tripathi, 2020).

Por último, la inmutabilidad es una característica fundamental de las cadenas de bloques. Esto añade complejidad al diseño de la estructura de datos. Una vez que se realiza una entrada esta no se puede modificar ni eliminar. Por lo tanto, los mecanismos de rectificación o enmienda deben ser diseñados cuidadosamente, especialmente cuando se trata de corregir errores o actualizar entradas en el ATL.

4.3.2.4 *Diseño de la interfaz de usuario*

El diseño de una interfaz de usuario, o UI (User Interface), para un nuevo sistema de ATL basado en blockchain requerirá de un estudio y análisis de las necesidades del usuario, un fuerte compromiso con la usabilidad así como en la accesibilidad y la compatibilidad entre plataformas. También requiere un enfoque de diseño basado en la experiencia de uso que acepte la retroalimentación y la iteración y tenga en cuenta los requisitos únicos de la visualización de datos blockchain. Por ello las principales

actividades y acciones a tener en cuenta durante el diseño, desarrollo e implementación del nuevo sistema en materia del diseño de interfaz de usuario serían:

- **Comprender las necesidades del usuario:** Como se ha visto este es un elemento clave en varias áreas del diseño del sistema. Un enfoque centrado en el usuario (Human-centered design) es fundamental en el diseño de la interfaz de usuario (Harte et al., 2017). Esto implica identificar la diversa gama de usuarios y comprender sus necesidades únicas, flujos de trabajo e interacciones con el sistema ATL. Al estudiar y analizar a los diversos posibles usuarios, los diseñadores pueden desarrollar interfaces intuitivas que reduzcan la carga cognitiva y se alineen con los flujos de trabajo existentes, garantizando así una integración fluida del sistema en las operaciones diarias de estos.
- **Diseño para la usabilidad:** La usabilidad es un aspecto clave en el diseño de la interfaz de usuario. El sistema debe diseñarse de tal manera que todos los usuarios, independientemente de su experiencia técnica, lo encuentren fácil de usar. Conceptos como el diseño amigable para el usuario, la navegación intuitiva, la etiquetación clara, la jerarquía visual y la simplicidad deben impulsar el proceso de diseño. El objetivo final siempre será crear una interfaz que permita a los usuarios realizar sus tareas de manera eficiente y efectiva.
- **Accesibilidad:** Puede requerirse que el nuevo sistema debe ser accesible para todos los usuarios, incluidos aquellos con discapacidades. Esto implica considerar factores como el tamaño y contraste del texto para usuarios con discapacidades visuales, funciones de comandos de voz para aquellos que no pueden usar un mouse o teclado, y un lenguaje fácil de entender para aquellos para quienes el inglés no es su primer idioma. Garantizar la accesibilidad no solo amplía la base de usuarios del sistema, sino que también se alinea con los principios de inclusión.
- **Compatibilidad móvil y multiplataforma:** Dada la naturaleza móvil del trabajo en aviación, la interfaz del sistema puede deber ser compatible con diversos dispositivos, como teléfonos inteligentes, tabletas y computadoras de escritorio. Además, puede diseñarse para funcionar de manera efectiva con diferentes sistemas operativos como Android, iOS, Windows o Linux. La compatibilidad multiplataforma garantiza que los usuarios puedan acceder e interactuar con el sistema cuando y donde lo necesiten, aumentando la utilidad y la satisfacción.
- **Bucles de retroalimentación con el usuario:** La retroalimentación del usuario es un recurso clave para los diseñadores de la interfaz de usuario. Les permite comprender de manera ágil qué funciona, qué necesita mejorar y cómo interactúan los usuarios con el sistema en escenarios del mundo real. Esta retroalimentación se puede recopilar a través de sesiones de prueba de usuarios, encuestas y/o herramientas de análisis. Este enfoque iterativo conduce a una mejora continua y a un sistema que satisfaga las necesidades reales del usuario.
- **Visualización de datos de blockchain:** Dada la naturaleza de los datos de blockchain, es importante considerar cómo se pueden visualizar de manera efectiva en la interfaz de usuario. Los datos deben presentarse de manera significativa y fácil de entender, adecuada para el rol y las necesidades del usuario específico. Por ejemplo, se pueden utilizar representaciones

visuales o paneles de control para proporcionar una visión general a nivel ejecutivo, mientras que las vistas de datos detalladas pueden ser críticas para el personal técnico.

- **Formación y soporte:** La formación puede ser esencial para garantizar que los usuarios entiendan el sistema nuevo y puedan interactuar de manera efectiva con él. Proporcionar materiales de formación, tutoriales y soporte continuo puede ayudar a los usuarios a familiarizarse rápidamente y de manera eficiente.

El diseño de la interfaz de usuario para un sistema ATL basado en blockchain debe ser un proceso minucioso que sitúe las necesidades del usuario y la usabilidad como pilar central. Será necesaria una combinación de comprensión de las necesidades de los usuarios, atención a la usabilidad, garantía de accesibilidad e integración de los comentarios de los usuarios. Esto permitirá que el nuevo sistema cuente con una interfaz optimizada para que los usuarios puedan realizar sus funciones de manera eficaz y eficiente.

4.3.2.5 Integración con otros sistemas

Durante el diseño y desarrollo del nuevo sistema ATL basado en blockchain, debe prestarse especial atención a la necesidad e interés de integración con otros sistemas existentes en el ecosistema de la aviación. Un sistema altamente integrado puede ayudar a mejorar la eficiencia en diferentes ámbitos, permitir el intercambio de datos en tiempo real y reducir la posibilidad de errores o discrepancias en estos.

Antes de que pueda comenzar cualquier forma de integración de sistemas, es crucial comprender primero las necesidades específicas de integración de la solución ATL propuesta. Esta fase de definición puede dividirse en varios componentes:

- **Interdependencias:** Es importante siempre tener en cuenta que el sistema ATL no existe en un entorno tecnológicamente aislado. El sistema ATL interactúa e intercambia datos con muchos otros sistemas, como el software de mantenimiento, reparación y revisión (MRO), los sistemas de operaciones de vuelo y los sistemas de gestión de inventario, entre otros. Comprender estas interdependencias es clave para definir qué datos deben compartirse y cuándo.
- **Identificar los flujos de datos:** Comprender el flujo de datos es un aspecto crítico de la integración de sistemas. Se deberá dar respuesta a cuestiones como ¿Qué datos deben transferirse entre sistemas? ¿En qué dirección fluyen los datos (bidireccional o unidireccional)? para determinar la estrategia de integración.
- **Formatos de datos y normas:** Los distintos sistemas pueden utilizar formatos de datos y normas diferentes. Identificarlos al principio de la fase de planificación permitirá planificar las transformaciones de datos o los esfuerzos de estandarización requeridos.

- **Procesamiento en Tiempo Real vs. Batch processing:** En función de los requisitos del sistema ATL y de los sistemas con los que interactúa, puede ser necesario intercambiar datos en tiempo-real (i.e. disponibilidad y bajo retardo) o por el contrario pueden recopilarse, procesarse y enviarse por lotes (Batch processing). Esta diferencia debe considerarse especialmente en el diseño de recursos del sistema.

Además, se debe también evaluar la compatibilidad previa a la integración de sistemas. Este proceso es necesario para garantizar que los distintos sistemas, incluido el nuevo sistema ATL, puedan comunicarse y funcionar eficazmente entre sí. La evaluación de la compatibilidad puede dividirse en varias áreas:

- **Compatibilidad técnica:** Se debe comprobar si los sistemas utilizan tecnologías compatibles con los utilizados en el nuevo sistema ATL basado en Blockchain.
- **Compatibilidad funcional:** Este aspecto evalúa si las funciones realizadas por los diferentes sistemas pueden operar en tándem sin causar posibles conflictos o redundancias.
- **Compatibilidad de datos:** Garantizar que los datos utilizados y producidos por los sistemas están en formatos que pueden ser entendidos y procesados por todos los sistemas integrados o se requiere de un procesamiento adicional para transformación y adecuación de estos.
- **Compatibilidad de seguridad:** Las medidas de seguridad utilizadas por los distintos sistemas deben ser compatibles, garantizando que la integración no introduzca vulnerabilidades.
- **Compatibilidad con el usuario:** Garantizar que el sistema completo integrado sea fácil de usar y no cree una experiencia inconexa o difícil para el usuario final.

Una vez establecidas las necesidades de integración, así como realizado el análisis de compatibilidad, se debe decidir los métodos de integración del sistema. Existen diferentes estrategias de integración, cada una con sus ventajas y desventajas, y la elección final dependerá de los requisitos específicos y las limitaciones del sistema ATL. Entre los métodos más comunes se encuentran:

- **Integración Directa:** Los sistemas se conectan directamente entre sí con los datos fluyendo de un sistema a otro sin intermediarios. Este tipo de integración puede ser rápida y eficiente aunque puede provocar un acoplamiento entre sistemas dificultando posibles cambios y actualizaciones en el futuro.
- **Integración mediante Middleware:** El software de middleware actúa como un puente entre los sistemas, permitiéndoles comunicarse sin estar conectados directamente. Este método reduce la interdependencia del sistema facilitando la actualización o reemplazo de los sistemas. Sin embargo, agrega otra capa de complejidad y puede requerir recursos adicionales.
- **Arquitectura Orientada a Servicios (SOA):** En SOA, los sistemas se comunican a través de servicios, que se definen mediante una interfaz estándar. Estos servicios pueden ser utilizados por diferentes sistemas, promoviendo la reutilización y reduciendo la redundancia. SOA es un enfoque flexible y escalable, pero puede ser complejo de diseñar e implementar.

- **Integración basada en API:** Con este método, los sistemas exponen APIs a las que otros sistemas pueden llamar para acceder a datos o funcionalidades. Este método es flexible y puede proporcionar un alto nivel de control sobre el acceso a datos, pero requiere que los sistemas admitan el uso de estas APIs.
- **Arquitectura de Microservicios:** El sistema se divide en servicios pequeños e independientes que se comunican a través de APIs. Este enfoque permite una gran flexibilidad y escalabilidad, pero puede ser complejo de gestionar y coordinar.

Otro aspecto clave para la integración, y relacionado con la estructura de datos sección 4.3.2.3., es el intercambio de datos y la consistencia de los mismos. Para una integración exitosa con otros posibles sistemas, el nuevo sistema ATL debe garantizar que los datos se intercambien de manera confiable entre los sistemas y se mantengan consistentes en todo momento. Para ello se debe definir y diseñar lo siguiente:

- **Protocolos de intercambio de datos:** Esto se refiere a las reglas que deben existir para la transmisión de datos entre los sistemas. Incluye la definición de formatos de datos, protocolos de comunicación y métodos de transferencia. Los sistemas deben acordar estos protocolos para garantizar un intercambio de datos sin problemas.
- **Consistencia de datos:** Mantener la consistencia de los datos es fundamental en un entorno de sistemas integrados. Esto implica garantizar que un cambio en un sistema se refleje con precisión en todos los demás sistemas integrados. Se pueden utilizar técnicas como transacciones atómicas (Lampson, 1981), en las que los cambios se aplican por completo en todos los sistemas o no se aplican en absoluto, para mantener la consistencia.

Por último, para conseguir una integración exitosa entre múltiples sistemas se deberán realizar diversas iteraciones de pruebas y validaciones exhaustivas con el objetivo de asegurar la funcionalidad y cumplimiento de las necesidades de los usuarios. Esto puede incluir desde pruebas de unidades a nivel de componentes hasta pruebas de integración de sistemas completos. El enfoque de integración también debe ser proactivo durante el diseño y desarrollo teniendo en cuenta siempre las posibles necesidades futuras. A medida que las tecnologías de aviación cambian y evolucionan puede que el nuevo sistema ATL debe diseñarse para una fácil escalabilidad e integración con nuevas tecnologías emergentes como el Big Data o la inteligencia artificial.

4.3.2.6 Diseño de Smart Contracts

Como ya se ha visto en la sección 2.2.7., los smart contracts son contratos auto-ejecutables en los que los términos del acuerdo se escriben directamente en líneas de código. En el contexto de un sistema ATL basado en blockchain, los smart contracts ofrecen potencial para automatizar muchos procesos, mejorando la eficiencia, reduciendo los errores humanos y aumentando la transparencia.

Dentro del nuevo sistema ATL los smart contracts podrían utilizarse para realizar un registro automático de los datos de vuelo. Por ejemplo, se podría definir un smart contract para registrar

automáticamente una serie de parámetros esenciales de vuelo, como horarios de salida y llegada, duración del vuelo o consumo de combustible. Estos smart contracts incluso podrían interactuar con varios sensores o sistemas de la aeronave para obtener estos datos directamente registrándolos de manera inmutable en el blockchain. Además, los smart contracts también podrían proporcionar un monitoreo automatizado de los datos del ATL a lo largo del tiempo. Por ejemplo, permitiendo revisar los datos acumulados de vuelo y programar tareas regulares de mantenimiento basadas en el uso de la aeronave.

El diseño de los smart contracts va más allá de la codificación de las reglas comerciales. Para garantizar su eficiencia, seguridad, mantenibilidad y adaptabilidad a posibles necesidades futuras, es importante considerar los siguientes factores durante el diseño y desarrollo.

- **Lógica del contrato:** La implementación de la lógica dentro del smart contract debe ser precisa y tener en cuenta todos los escenarios posibles y casos extremos. La naturaleza autoejecutable de los smart contracts significa que operan y se ejecutan exactamente como están escritos. Por ejemplo, un smart contract encargado de programar el mantenimiento después de cierto número de horas de vuelo necesitaría realizar un seguimiento preciso de cada vuelo independientemente de posibles cambios de estado del mismo (e.g. completado, retrasado, cancelado u otros). Además, el contrato podría necesitar tener en cuenta diferentes tipos de vuelos, como vuelos de corta distancia versus vuelos de larga distancia, o diferentes condiciones operativas.
- **Coste de ejecución:** Los costes de ejecución, especialmente en ciertos tipos de blockchain como Ethereum, son una consideración clave. Cálculos complejos o altas necesidades de almacenamiento de datos pueden generar costes elevados. Es necesario por tanto utilizar técnicas de optimización, como reducir los pasos computacionales, optimizar el almacenamiento de datos y eliminar redundancias, para crear contratos eficientes y rentables. Además, la elección de la plataforma blockchain en sí misma puede verse influenciada por el coste de ejecución del contrato.
- **Actualizaciones y flexibilidad:** La naturaleza cambiante de las regulaciones y la tecnología de la aviación requiere un enfoque de diseño que incorpore flexibilidad por defecto. Si bien los smart contracts son inmutables una vez implementados en el blockchain, técnicas como la capacidad de actualización del contrato, patrones de proxy o el uso de contratos de almacenamiento de datos externos pueden permitir cambios en la funcionalidad con el tiempo, sin necesidad de crear contratos completamente nuevos (Bui et al., 2021).
- **Interoperabilidad:** La interoperabilidad se refiere a la capacidad de los smart contracts para interactuar con otros contratos, sistemas externos y usuarios. Por ejemplo, un contrato de programación de mantenimiento podría necesitar interactuar con otros contratos que registran datos de vuelo, con sistemas externos que gestionan el inventario de partes y con usuarios humanos que confirman tareas de mantenimiento. Una planificación cuidadosa de estas interacciones es crucial para garantizar un funcionamiento sin problemas y la integridad de los datos en todo el sistema.

- **Simplicidad y legibilidad:** Un código complejo tiene más probabilidades de contener errores y vulnerabilidades de seguridad. Aunque los smart contracts pueden ser capaces de realizar operaciones complejas es importante que su diseño debe priorizar la simplicidad y la legibilidad. Esto ayuda a asegurar que puedan ser auditados y mantenidos de manera precisa, y reduce la probabilidad de comportamientos inesperados.
- **Escalabilidad:** Se debe tener en cuenta la escalabilidad de los smart contracts, especialmente a medida que el sistema ATL pueda crecer con el tiempo. Por ejemplo, esto puede implicar planificar un mayor almacenamiento de datos o la creación de nuevos contratos a medida que se agreguen más aeronaves al sistema.

Además, otro de los aspectos clave a la hora de diseñar los smart contracts, en especial cuando interactúan con datos sensibles, es la seguridad. Para garantizar al máximo la seguridad de estos contratos, se deben entender y abordar las posibles vulnerabilidades en las etapas de diseño y prueba. Entre las principales vulnerabilidades de los smart contracts encontramos:

- **Ataques de Reentrancia:** Estos ataques se dan cuando un smart contract llama a otro contrato en su código y, cuando finaliza la nueva llamada, continúa con la ejecución. Los atacantes roban estas llamadas externas y hacen una llamada recursiva de vuelta al contrato con la ayuda de la función callback. Mediante esta acción pueden crear un contrato en una dirección externa utilizando código malicioso. Para prevenir estos ataques se suele utilizar el patrón de Checks-Effects-Interactions (CEI), donde primero se verifican todas las condiciones, luego se realizan los cambios y finalmente se interactúa con otros contratos (Tikhomirov et al., 2018).
- **Desbordamiento y Subdesbordamiento de Enteros:** Estos ataques explotan las capacidades de almacenamiento limitadas de los enteros. Un desbordamiento ocurre cuando una operación da como resultado un número mayor al valor máximo que un entero puede contener, y un subdesbordamiento cuando se calcula un número menor al valor más pequeño posible. Por ejemplo, Solidity, el lenguaje de programación utilizado para los smart contracts de Ethereum, no genera un error cuando ocurren estos eventos, por lo que el contrato continuará ejecutándose con valores incorrectos (Lai & Luo, 2020). Estos problemas se pueden mitigar utilizando bibliotecas como SafeMath de OpenZeppelin que incluyen verificaciones de seguridad.
- **Límite de Gas y Bucles:** Cada bloque en el blockchain tiene un límite de cuántas operaciones computacionales puede incluir conocido como el 'gas limit'. Los bucles en los smart contracts, especialmente aquellos que operan sobre longitudes de matrices dinámicas, podrían consumir gas que exceda este límite provocando el fallo del contrato. Esto se puede evitar limitando el uso de bucles o utilizando técnicas para procesar datos en fragmentos más pequeños.
- **Dependencia de la Marca de Tiempo:** Los smart contracts que utilizan la variable 'block.timestamp' para funcionalidades críticas pueden ser manipulados en cierta medida por los mineros, ya que tienen la capacidad de ajustar ligeramente la marca de tiempo. Se recomienda no depender de 'block.timestamp' para la funcionalidad crítica del contrato.

- **Funciones Expuestas:** Las funciones en los smart contracts que no se especifican como 'privadas' pueden ser llamadas por direcciones externas, lo que puede llevar a un comportamiento no deseado del contrato. Siempre se debe establecer la visibilidad de funciones adecuadas para garantizar que solo las direcciones autorizadas puedan ejecutar funciones.
- **Ataque de Dirección Corta:** Este ataque ocurre cuando un contrato interactúa con una dirección enviada por un usuario. Si la dirección es más corta de lo esperado y el contrato no valida la longitud de la dirección, el contrato podría interpretar la parte restante como valor de transacción. Esto se puede prevenir validando las longitudes de entrada.
- **Asegurar que los Smart Contracts sean Pausables:** Es esencial garantizar que los smart contracts se puedan pausar o detener por direcciones autorizadas en caso de detectar una anomalía o ataque. Esto ayuda a prevenir daños adicionales.

Los smart contracts deben someterse a pruebas de seguridad y auditorías rigurosas para descubrir y resolver cualquier vulnerabilidad y asegurar la robustez. Dada la inmutabilidad del blockchain, cualquier defecto en un contrato desplegado es permanente y puede ser explotado por actores maliciosos. El uso de herramientas automatizadas y servicios de auditoría de terceros puede proporcionar un nivel adicional de garantía, aunque no reemplaza la necesidad de un diseño cuidadoso y pruebas internas. Las pruebas rigurosas y las auditorías son etapas integrales en el proceso de desarrollo de smart contracts. Algunas de las pruebas que se pueden realizar para asegurar la robustez y seguridad del sistema ATL basado en blockchain son:

- **Pruebas Unitarias:** Estas pruebas permiten a los desarrolladores verificar la corrección de las funciones individuales dentro del contrato. Para cada función, se deben considerar diversos escenarios y casos límite.
- **Pruebas de Integración:** Una vez que las funciones individuales han sido probadas se debe probar también la integración de las mismas entre sí y asegurar que funcionen conjuntamente como se espera. Esto implica probar el contrato en su conjunto y observar la interacción entre las funciones, especialmente en cuanto al flujo de datos y los cambios de estado.
- **Pruebas de Estrés:** Las pruebas de estrés someten a los smart contracts a condiciones extremas para evaluar su rendimiento. Por ejemplo, en el caso del sistema ATL, una prueba de estrés podría simular un número extremadamente alto de vuelos en un corto período de tiempo o entradas consecutivas rápidas a la función de programación de mantenimiento..
- **Auditoría de Seguridad:** Puede ser necesario auditar los smart contracts en busca de posibles vulnerabilidades de seguridad. Este proceso implica una revisión exhaustiva del código del contrato, evaluando su solidez frente a vectores de ataque conocidos.
- **Verificación Formal:** Este es un enfoque matemático para asegurar que el código de un contrato implemente correctamente sus especificaciones. Si bien la verificación formal puede brindar un alto nivel de confianza en la corrección de un contrato, es un proceso complejo que requiere una experiencia significativa y no es adecuado para todos los contratos.

El diseño, desarrollo e implementación de los smart contracts para un futuro sistema ATL basado en blockchain es una tarea que requiere una cuidadosa consideración de diversos factores que van desde los requisitos funcionales de los contratos hasta las posibles vulnerabilidades de seguridad. Estos contratos actúan como columna vertebral del sistema, facilitando las transacciones, manteniendo la integridad de los datos y aplicando automáticamente la compleja lógica inherente a las operaciones y el mantenimiento de las aeronaves. El uso de las mejores prácticas en el diseño, la consideración cuidadosa de las vulnerabilidades de seguridad, las pruebas rigurosas y los procesos de auditoría exhaustivos pueden ayudar a garantizar que los contratos inteligentes cumplan su propósito de manera eficaz y segura. También hay que tener en cuenta que a medida que el campo de la tecnología blockchain siga evolucionando, también lo harán las metodologías y herramientas utilizadas para crear, probar y proteger los contratos inteligentes, lo que subraya la importancia del aprendizaje y la adaptación continuos.

4.3.2.7 Seguridad y Privacidad

Si bien la tecnología blockchain ofrece altas garantías inherentes de seguridad y privacidad no es completamente inmune a vulnerabilidades y posibles ataques. Estas vulnerabilidades pueden ser explotadas comprometiendo la integridad y seguridad de la red. Es por ello que es importante tomar medidas durante las fases de diseño y desarrollo para mitigar al máximo estas vulnerabilidades. Algunas de las medidas de seguridad que se pueden implementar son:

- **Elección del algoritmo de consenso:** Los diferentes algoritmos de consenso existentes ofrecen diferentes niveles de seguridad y resistencia a diferentes tipos de ataques. Por ejemplo, los algoritmos PoS y DPoS tienen mecanismos para disuadir manipulaciones maliciosas haciéndolos más resistentes a ataques como el del 51%. Además, algoritmos más nuevos como PoA pueden proporcionar seguridad adicional en blockchains permissionadas donde los validadores son entidades conocidas y de confianza.
- **Protocolos de seguridad en capas:** Implementar múltiples capas de protocolos de seguridad puede proporcionar una defensa contra ataques más robusta. Esto incluye protecciones a nivel de red como firewalls o sistemas de detección de intrusiones. Además, protecciones a nivel de sistema como controles de acceso y autenticación de múltiples factores pueden ayudar a prevenir contra accesos no autorizados y amenazas internas.
- **Monitoreo regular de la red:** El monitoreo regular de la red es fundamental para detectar y responder de manera rápida a posibles amenazas de seguridad. Las herramientas de monitoreo pueden rastrear la actividad de la red y detectar anomalías que indiquen posibles ataques, como picos en el tráfico de red o patrones de transacciones inusuales.
- **Auditoría y actualizaciones de smart contracts:** La auditoría regular de smart contracts es fundamental para identificar y solucionar vulnerabilidades existentes.

De entre las medidas a aplicar para mejorar y asegurar la privacidad de los datos en la red blockchain se pueden encontrar las siguientes:

- **Tipo de blockchain:** Como se ha visto previamente, en las blockchain privadas o de consorcio el acceso está restringido a un grupo específico de participantes, lo que mejora la privacidad. En el contexto de un sistema ATL, una blockchain de consorcio podría ser especialmente adecuada, donde solo se permite la participación de entidades específicas como aerolíneas, organizaciones de mantenimiento y organismos reguladores de aviación.
- **Tecnologías de preservación de la privacidad:** La implementación de tecnologías que mejoran la privacidad también puede fortalecerla en un sistema blockchain. Por ejemplo, las “zero-knowledge proofs” permiten la validación de transacciones sin revelar los datos reales de la transacción pudiendo así preservar la privacidad de los datos sensibles. Por otro lado, la computación multiparte segura permite la realización de cálculos en datos encriptados, manteniendo la privacidad de los datos de entrada incluso para aquellos que realizan el cálculo (Zhou et al., 2021).
- **Prácticas de manejo de datos:** La implementación de prácticas sólidas de manejo implica considerar cuidadosamente qué datos se almacenan en la blockchain. Idealmente deberían ser mínimos para evitar una exposición innecesaria de datos sensibles. La mayoría de los datos deben almacenarse fuera de la blockchain, y se pueden utilizar técnicas criptográficas como el hashing de datos para garantizar la integridad de los datos fuera de la cadena.

Al adoptar estas medidas de seguridad y privacidad, un sistema ATL basado en blockchain puede mitigar eficazmente las posibles amenazas, asegurando que el sistema sea seguro, privado y cumpla con las regulaciones y necesidades de los usuarios.

4.3.2.8 Escalabilidad y Rendimiento

El diseño adecuado de la escalabilidad y el rendimiento son esenciales para cualquier sistema y en especial en el contexto de la tecnología blockchain. Se entiende por escalabilidad a la capacidad del sistema para manejar una creciente cantidad de trabajo o su potencial para expandirse y adaptarse, y el rendimiento como la medida de la eficiencia del sistema al procesar transacciones. En el caso de un sistema ATL basado en blockchain, se debe desarrollar una plataforma capaz de soportar un gran volumen de transacciones de datos sin comprometer la velocidad o la estabilidad del sistema. El sistema debe ser capaz de procesar rápidamente actualizaciones, como nuevas entradas de datos de vuelo, registros de mantenimiento y verificaciones de seguridad, sin causar retrasos que puedan obstaculizar las operaciones de las aerolíneas.

Como se ha visto en anteriores secciones, la elección del tipo de blockchain puede tener un impacto significativo en la escalabilidad de la red. De entre las principales consideraciones de escalabilidad a la hora de diseñar están el tamaño del bloque y el tiempo de generación del bloque. Los bloques más grandes pueden contener más transacciones, pero a su vez pueden tardar más tiempo en procesarse y requerir más recursos computacionales. Por otro lado, los bloques más pequeños pueden procesarse más rápido, pero pueden limitar el número de transacciones que la red puede manejar simultáneamente. El tiempo de generación del bloque también contribuye a la velocidad de procesamiento de transacciones del sistema.

También, el diseño de los smart contracts también puede afectar la escalabilidad. Smart contracts escritos de manera ineficiente que realizan cálculos complejos o requieren grandes cantidades de almacenamiento de datos pueden ralentizar la red y aumentar los costos de transacción. En un sistema ATL, los smart contracts pueden llegar a manejar tareas complejas como verificar los datos de vuelo según los protocolos de mantenimiento, emitir alertas para los controles requeridos y actualizar las entradas del ATL para cada avión. Por lo que es importante que estos contratos deben diseñarse para ser eficientes. Esto puede incluir optimizar las operaciones computacionales, minimizar el almacenamiento de datos en la cadena y gestionar adecuadamente los costes de gas.

Además de la escalabilidad de los smart contracts, las consideraciones de almacenamiento de datos son esenciales en sistemas donde se pueden generar grandes volúmenes de datos con el tiempo. Almacenar todos los datos directamente en el blockchain puede causar problemas significativos de escalabilidad debido a las limitaciones de almacenamiento y al aumento de costes a medida que el blockchain crece. Como solución, se puede decidir solo almacenar en la red la información esencial, mientras que la mayoría de los datos se pueden almacenar fuera de la cadena en bases de datos tradicionales o sistemas de archivos distribuidos. Se pueden utilizar técnicas como el hashing de datos para verificar la integridad de los mismos fuera de la cadena, lo que permitiría una gestión eficiente y segura de los datos sin sobrecargarla red. Además, como ya se ha mencionado, existen soluciones como los sistemas de almacenamiento IPFS que se pueden integrar con el blockchain y ofrecen almacenamiento descentralizado con funciones de hash criptográficas que garantizan la integridad de los datos. Este enfoque combinaría los beneficios de la inmutabilidad y la descentralización del blockchain con la escalabilidad de los sistemas de almacenamiento de datos tradicionales.

Si bien el diseño cuidadoso de la red y los smart contracts puede ayudar a optimizar tanto la escalabilidad como el rendimiento, existen estrategias y avances en la tecnología blockchain que pueden mejorar significativamente el rendimiento del sistema. Por ejemplo, las soluciones “Layer 2” permiten que las transacciones se procesen fuera de la cadena y luego se agrupen antes de ser agregadas al blockchain principal. Este enfoque puede aumentar drásticamente el rendimiento de las transacciones y reducir los costes de transacción (Sguanci et al., 2021).

El fragmentado es otro método en el que el blockchain se divide en partes más pequeñas, cada una capaz de procesar sus propias transacciones y smart contracts. Esto puede aumentar considerablemente la capacidad de la red, ya que la carga de trabajo se distribuye entre los diferentes fragmentos. Los nuevos algoritmos de consenso, como PoS, DPoS y PoA (ver sección 2.2.4), también ofrecen un rendimiento mejorado en comparación con los sistemas tradicionales PoW. Estas alternativas ofrecen tiempos de creación de bloques más rápidos y requisitos computacionales más bajos, lo que las hace más escalables y eficientes.

Dado el rápido desarrollo en la tecnología blockchain es importante considerar durante el diseño y desarrollo cómo el sistema ATL se podría adaptar a los cambios futuros en tecnología, regulación y requisitos comerciales. Para ello se puede diseñar el sistema con modularidad en mente. Al desarrollar componentes (como smart contracts) que se pueden reemplazar o actualizar fácilmente, el sistema es suficientemente flexible y puede evolucionar con el tiempo sin requerir renovaciones extensas.

Por último, para asegurar que el sistema funcione a su capacidad óptima, las pruebas regulares de rendimiento y el monitoreo son esenciales. Pueden ayudar a identificar cuellos de botella, medir la respuesta del sistema a cargas de trabajo crecientes y evaluar el efecto de cualquier cambio o actualización en el sistema. Para ello se pueden utilizar tanto herramientas de pruebas de rendimiento pueden simular cargas altas o condiciones de estrés como herramientas de monitoreo que pueden proporcionar información en tiempo real sobre el rendimiento del sistema, alertando sobre posibles problemas. Este análisis continuo puede ayudar a mantener el alto rendimiento y la escalabilidad del sistema.

4.3.2.9 Cumplimiento normativo

El cumplimiento normativo es un factor crítico que debe tenerse en cuenta a la hora de diseñar, desarrollar, implantar y operar cualquier sistema dentro del sector de la aviación, incluido un nuevo sistema ATL basado en blockchain. Dado que la tecnología blockchain a menudo presenta características únicas debido a su naturaleza descentralizada e inmutable, es importante conocer y comprender estas plenamente para planificar el completo cumplimiento normativo.

La industria de la aviación opera bajo numerosas regulaciones específicas que rigen la operación y mantenimiento de aeronaves. Como se ha visto en la sección 4.1.2, en Europa, marcado por EASA, y en Estados Unidos, marcado por la FAA, existe un marco jurídico específico que cubre los requisitos y características que debe tener un ATL. En ambas se destacan la necesidad de realizar un seguimiento y registro meticuloso de acciones de mantenimiento específicas, ciclos de vuelo y horas voladas. Ciertos tipos de datos deben ser registrados y mantenidos por períodos especificados, y estar disponibles para inspecciones o auditorías regulatorias. Como se ha venido viendo un futuro sistema ATL basado en tecnología blockchain puede ofrecer ventajas únicas para cumplir con estos requisitos regulatorios. Tanto la EASA como la FAA no establecen un requisito específico para el formato del sistema ATL, permitiendo que pueda ser en papel o en formato digital. Sin embargo, sí establecen la necesidad de que el sistema sea aprobado por la autoridad competente (en el caso de Europa). Además, estas regulaciones establecen requisitos sobre la información mínima que debe incluir el sistema ATL, así como los casos en los que se debe garantizar la interoperabilidad y estandarización de los datos.

Con el avance creciente de la digitalización en la aviación, es importante considerar otras regulaciones, especialmente aquellas relacionadas con la protección de datos y la privacidad. Un ejemplo destacado de estas regulaciones, mencionado previamente, es el GDPR en Europa. Estas leyes establecen requisitos estrictos sobre la recopilación, procesamiento, almacenamiento y compartición de datos personales. Esto se puede traducir en que a la hora del diseño y desarrollo del nuevo sistema ATL basado en blockchain se deba proporcionar a las personas el control sobre sus datos personales, como por ejemplo la información de los miembros de la tripulación, así como cómo implementar procesos necesarios de anonimización de datos y establecer medidas estrictas de control de acceso. Además, puede ser necesario emplear técnicas de preservación de la privacidad, o establecer mecanismos en contra de naturaleza inmutable de la blockchain para respetar el "derecho al olvido" en el GDPR.

El proceso de verificación del cumplimiento de todas las normativas pertinentes es continuo y debe ser parte fundamental del uso operacional del sistema ATL. Esta verificación puede ser en forma de auditorías periódicas, certificaciones u otros medios de verificación del cumplimiento de las normas exigidas. También se debe tener en cuenta la rápida evolución de la tecnología blockchain y la posible normativa aplicable. Esta adaptabilidad debe ser una característica central del diseño del nuevo sistema ATL. Las leyes y normativas que rodean a esta tecnología pueden cambiar rápidamente, sobre todo a medida que los reguladores de todo el mundo siguen lidiando con las implicaciones de la tecnología inmutable y distribuida. Estos cambios pueden tener implicaciones importantes a futuro para el sistema ATL, requiriendo potencialmente alteraciones o adaptaciones en la forma en que opera el sistema. Por lo tanto, construir el sistema con la capacidad de adaptarse a los cambios en el panorama normativo es clave para garantizar su viabilidad y cumplimiento a largo plazo.

4.3.2.10 Costes

Realizar un análisis de costes en profundidad es una parte clave del desarrollo e implementación de cualquier sistema nuevo como el sistema ATL basado en blockchain. Es importante comprender no sólo los costes inmediatos asociados a la puesta en marcha de un sistema de este tipo, sino también los posibles costes a largo plazo derivados del funcionamiento, mantenimiento y posible ampliación.

- **Costes de instalación:** El coste de instalación inicial de un sistema ATL basado en blockchain puede ser significativo una de las principales barreras para su aplicación. Esto incluye principalmente el coste de la infraestructura como servidores y equipos de red necesarios para soportar el sistema. También incluye los costes de desarrollo de software para diseñar y construir el sistema como la propia red blockchain y los contratos inteligentes. Además, también deben tenerse en cuenta los costes de integración del sistema incluyendo el esfuerzo necesario para conectar el nuevo sistema con los sistemas existentes, así como los costes iniciales de prueba y validación.
- **Costes operativos:** Una vez implementado el sistema hay que tener en cuenta los costes operativos continuos. Entre ellos están los costes de alojamiento y de red. También hay costes de mantenimiento regular del sistema que incluyen posibles actualizaciones de software y reparaciones o sustituciones de hardware. La gestión y actualización de los contratos inteligentes también puede implicar costes sustanciales a lo largo del tiempo.
- **Costes de ampliación:** A medida que crece el uso o las necesidades del sistema ATL puede surgir la necesidad de escalar el sistema para gestionar más usuarios, transacciones o datos. Esto puede implicar la actualización de la infraestructura, la ampliación de la capacidad de almacenamiento o la optimización de los contratos inteligentes para una ejecución más eficiente.
- **Costes de cumplimiento:** Garantizar el cumplimiento de todas las leyes, reglamentos y normas pertinentes es un requisito que también puede añadirse al coste total del sistema. Esto podría implicar auditorías periódicas, certificaciones o posibles ajustes del sistema para cumplir requisitos nuevos o modificaciones.

- **Costes de seguridad:** Implantar medidas de seguridad sólidas puede suponer un coste considerable, aunque esencial para proteger la integridad del sistema y los datos que contiene. Esto incluye el coste de las auditorías de seguridad periódicas, la aplicación y actualización de los protocolos de seguridad y los posibles costes asociados a la resolución de cualquier incidente de seguridad que pueda producirse.
- **Análisis coste-beneficio:** Es esencial evaluar estos costes frente a los beneficios que proporciona el nuevo sistema ATL basado en blockchain. Estos beneficios podrían incluir una mayor eficiencia gracias a la automatización de las tareas manuales, una mayor integridad de los datos gracias a la inmutabilidad de blockchain, una mejora del cumplimiento gracias a procesos transparentes y auditables, y un posible ahorro de costes gracias a la reducción de errores o a un uso más eficiente de los recursos.

Un análisis exhaustivo de los costes es crucial para evaluar la viabilidad del nuevo sistema ATL basado en blockchain. Es también importante destacar que aunque un sistema de este tipo conlleva costes iniciales y continuos que pueden ser elevados, también proporciona beneficios significativos que pueden justificar estos costes. Sin embargo, cada situación es única, y debe prestarse especial atención al contexto y los requisitos específicos de cada escenario de aplicación.

5. Prueba de Concepto: Diseño y Desarrollo

5.1 Diseño de la aplicación

Esta sección se enfoca en la aplicación práctica del estudio realizado en este trabajo mediante el diseño y desarrollo de una prueba de concepto básica para el ATL basado en blockchain. El objetivo de este ejercicio es demostrar los beneficios y funcionalidades de dicho nuevo sistema, así como posibles desafíos de la implementación. Se desea resaltar que esta prueba de concepto es puramente ilustrativa y tiene como objetivo proporcionar una representación tangible de los conceptos teóricos y principios de diseño y desarrollo previamente discutidos. Como tal, no sigue un ciclo de desarrollo completo ni incluye todas las funcionalidades o capacidades que tendría un sistema ATL completamente operativo. La intención es poner de relieve el potencial de un sistema de este tipo y fomentar nuevas investigaciones, desarrollos y despliegues de la tecnología blockchain en los sistemas de mantenimiento y seguridad de la aviación.

5.1.1 Análisis de usuarios y tareas

En este apartado, se aborda la fase inicial del análisis de usuarios y tareas, la cual, como se ha visto, resulta fundamental para el desarrollo de cualquier sistema. Se realizará una descripción general de los tipos de usuarios que interactuarán con el nuevo sistema ATL basado en blockchain. En el caso de la prueba de concepto diseñada y desarrollada, los usuarios principales pueden ser categorizados en tres grupos, cada uno con roles y requisitos distintos.

1. **Tripulación de cabina:** Este grupo de usuarios incluye a los pilotos responsables de operar la aeronave, y en especial al piloto al mando (Pilot in Command) el cual es el responsable último de la seguridad de la aeronave. Sus principales tareas dentro del sistema ATL serán:
 - a. Registrar información de vuelo: Esto implica ingresar datos clave, como tiempos de vuelo, condiciones de vuelo, consumo de combustible y cualquier otro parámetro relevante.
 - b. Registrar problemas técnicos: Los miembros de la tripulación deben poder registrar cualquier anomalía técnica o falla que observen durante las operaciones de vuelo.
 - c. Revisar el historial de la aeronave: Los miembros de la tripulación pueden necesitar acceder al historial técnico completo de la aeronave que están operando. Por lo tanto, el sistema debe proporcionar una forma sencilla de recuperar y navegar por los registros de vuelo y mantenimiento anteriores.
2. **Personal de mantenimiento:** Este grupo es responsable del mantenimiento de la aeronave. Dentro del sistema ATL, deben poder:

- a. Revisar el historial de la aeronave: Al igual que la tripulación de la aeronave, el personal de mantenimiento también necesita acceder al historial completo de la aeronave para identificar posibles necesidades de mantenimiento.
 - b. Registrar trabajos de mantenimiento: Cualquier actividad de mantenimiento realizada, especialmente aquellas relacionadas con problemas técnicos reportados, debe registrarse de manera precisa en el sistema.
 - c. Registrar otras acciones de mantenimiento: El sistema también debe permitir el registro de acciones de mantenimiento rutinarias o preventivas, asegurando un historial de mantenimiento completo.
3. **Aerolíneas y Autoridad supervisora:** Este grupo necesita acceder al ATL para garantizar el cumplimiento de los estándares de seguridad y regulaciones. Su principal tarea es:
- a. Revisar el historial completo de acciones e información relacionada con una aeronave: Esto incluye registros de vuelo, problemas técnicos reportados y registros de mantenimiento. El sistema debe proporcionar a estos usuarios una vista clara y cronológica del historial de una aeronave permitiendo realizar auditorías, monitorear el cumplimiento normativo y comprender el estado general de la flota.

Diseñar el sistema para las funciones y tareas específicas de cada usuario es esencial. La tabla 5 proporciona una visión clara y resumida del análisis de usuarios y tareas, destacando los tipos de usuarios, sus respectivas funciones, tareas y los permisos necesarios que requieren para llevar a cabo eficazmente estas tareas dentro del sistema. Esta visión general estructurada sirve como punto de referencia a medida que se avance en el diseño y desarrollo del sistema.

Tabla 5. Tipos de usuarios, funciones, tareas y permisos necesarios en el sistema ATL propuesto

Usuario	Funciones	Tareas	Permisos Blockchain
Tripulación de la aeronave	Operación	Registrar información de vuelo	Escritura
		Registro de problemas técnicos	Escritura
		Revisar el historial de la aeronave	Lectura

Personal de mantenimiento	Mantenimiento	Revisar el historial de la aeronave	Lectura
		Registrar los trabajos de mantenimiento relacionados con los problemas técnicos	Escritura
		Registrar otras acciones de mantenimiento	Escritura
Aerolínea y Autoridad supervisora	Auditoría/Regulación	Revisar el historial de acciones e información relacionadas con la aeronave	Lectura

5.1.2 Diseño de funcionalidades y flujo de trabajo

Una vez establecidos y definidos los usuarios, así como sus tareas a realizar, se puede pasar a diseñar las funcionalidades y los flujos de trabajo del nuevo sistema ATL basado en blockchain. Las funcionalidades básicas necesarias requeridas por el sistema se basan en las tareas identificadas en el análisis previo de usuarios, el cual refleja las necesidades de la tripulación de cabina, el personal de mantenimiento y los organismos reguladores y de las aerolíneas. Las funcionalidades básicas son:

1. **Registro de información:** El sistema debe proporcionar una interfaz sencilla e intuitiva que permita a la tripulación de cabina así como al personal de mantenimiento registrar nueva información. Esto incluye detalles del vuelo, problemas técnicos y actividades de mantenimiento. El sistema puede también implementar mecanismos de validación de datos para garantizar su exactitud e integridad.
2. **Revisión del historial:** Todos los tipos de usuarios deben poder acceder y navegar fácilmente por el historial completo de la aeronave. Esta característica requiere un diseño cuidadoso para garantizar una rápida recuperación de la información de la cadena de bloques, manteniendo al mismo tiempo la seguridad y la privacidad.
3. **Auditoría y verificación:** Para las aerolíneas y los organismos supervisores, el sistema debe tener sólidas capacidades de auditoría. Esto incluye la capacidad de rastrear cambios, ver quién hizo cada entrada y verificar la integridad de los datos. Dada la inmutabilidad de los registros de blockchain, estos usuarios pueden estar seguros de la autenticidad de la información.

El diseño del flujo de trabajo del sistema ATL debe reflejar el flujo operativo de los usuarios garantizando una integración perfecta del sistema en los procesos de trabajo existentes. Los flujos de trabajo definidos para la prueba de concepto son:

1. **Flujo de trabajo de la tripulación de cabina:** Previo a un vuelo la tripulación debe revisar el estado técnico de la aeronave e identificar posibles problemas técnicos que hayan sido registrados pero no se hayan tomado las medidas correctoras necesarias. Después de un vuelo, la tripulación registra los detalles del vuelo y cualquier problema técnico observado. El sistema deberá guiarlos a través de este proceso, garantizando que se capte toda la información necesaria. Una vez registradas, estas entradas estarán disponibles inmediatamente para su revisión por la misma tripulación o por la del siguiente vuelo, así como el resto de usuarios. En la figura 15 se puede ver el flujo de trabajo de manera esquemática.

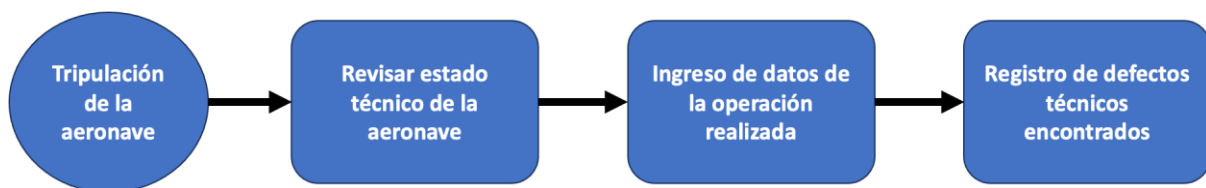


Figura 15. Flujo de trabajo de la tripulación de vuelo

2. **Flujo de trabajo del personal de mantenimiento:** El personal de mantenimiento debe poder revisar los problemas marcados, realizar las tareas necesarias y, a continuación, registrar sus acciones de mantenimiento. Además, también deben poder registrar otras actividades de mantenimiento no relacionadas con deficiencias técnicas identificadas por la tripulación. El flujo de trabajo debe resaltar los problemas pendientes de la aeronave y guiar el proceso de mantenimiento. Una vez finalizado el trabajo de mantenimiento, el estado actualizado de la aeronave debe reflejarse en el sistema. En la figura 16 se puede ver el flujo de trabajo de manera esquemática.



Figura 16. Flujo de trabajo del personal de mantenimiento

3. **Flujo de trabajo de aerolíneas y autoridad supervisora:** Estos usuarios necesitan principalmente revisar el historial de la aeronave, incluidos los diarios de vuelo y los registros de mantenimiento. El flujo de trabajo debe permitir a estos usuarios navegar fácilmente por los registros, con funciones adicionales para auditorías detalladas y comprobaciones de conformidad. En la figura 17 se puede ver el flujo de trabajo de manera esquemática.

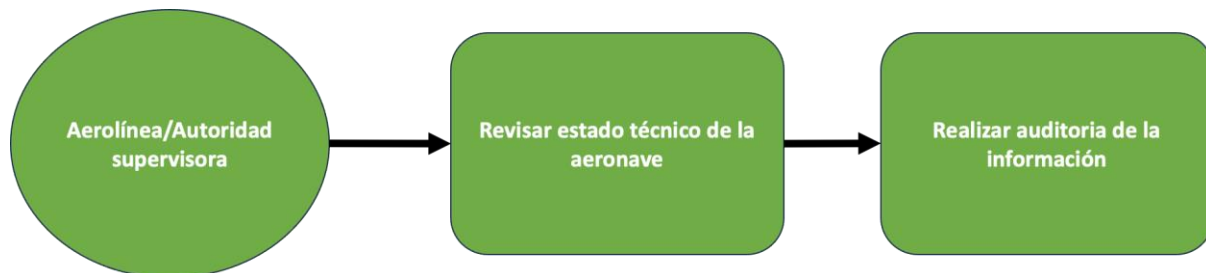


Figura 17. Flujo de trabajo de aerolíneas y organismos supervisores

Se deberá asegurar hasta donde sea posible que la funcionalidad y el diseño del flujo de trabajo del sistema ATL basado en blockchain propuesto satisfaga las necesidades específicas de los grupos de usuarios identificados, al tiempo que mejoran la eficiencia y la precisión de las operaciones. La naturaleza transparente, segura e inmutable de la tecnología blockchain puede apoyar en gran medida estas funcionalidades, dando lugar a una mayor fiabilidad y credibilidad de los registros de aeronaves. En la siguiente fase de diseño de los bloques y la estructura de datos, estos requisitos funcionales guiarán las decisiones arquitectónicas subyacentes de la red blockchain.

5.1.3 Diseño de la estructura de datos

En esta sección, se llevará a cabo el diseño preliminar de la estructura de datos para la implementación de la aplicación blockchain en el contexto del ATL. Este proceso abarca la identificación de las diversas actividades esenciales que deben ser registradas, su interconexión efectiva dentro de la plataforma y la determinación y definición de la información relevante que deberá ser capturada para cada una de dichas actividades.

En el marco de la aplicación blockchain para el ATL, se identifican varias actividades fundamentales que deben ser registradas y relacionadas para garantizar el correcto mantenimiento y operatividad de las aeronaves. Estas actividades clave son:

- **Aeronave:** Representa el componente central de la plataforma y respecto al cual, de una u otra manera, se referencian todo el resto de datos.
- **Vuelos:** Cada vez que una aeronave inicie y concluya un vuelo, se generará un registro en la aplicación blockchain.
- **Actividades de Mantenimiento:** Se registrarán todas las actividades de mantenimiento realizadas en cada aeronave, ya sea de rutina o en respuesta a eventos específicos.

- **Defectos Técnicos:** En caso de que se detecte algún defecto técnico durante el vuelo, se generará un registro específico para este evento.
- **Acciones de Mantenimiento Relacionadas con Defectos Técnicos:** Para abordar los defectos técnicos registrados, se documentarán las acciones de mantenimiento llevadas a cabo para su corrección.

La relación entre estas actividades será establecida mediante la estructura de datos final y el uso de la tecnología blockchain, permitiendo una trazabilidad inmutable y transparente en todo el proceso. La aplicación asegurará que cada actividad esté vinculada a la aeronave correspondiente, y que las acciones de mantenimiento estén relacionadas con los defectos técnicos detectados. Asimismo, los vuelos efectuados por una aeronave específica estarán enlazados con los registros de actividades de mantenimiento y defectos técnicos asociados a ese vuelo en particular. Esta interconexión de datos garantizará una visión integral y confiable del historial técnico de cada aeronave, facilitando la toma de decisiones informadas y la optimización de la seguridad operativa en la industria de la aviación. En la figura 18 se puede ver el esquema de datos para una aeronave.

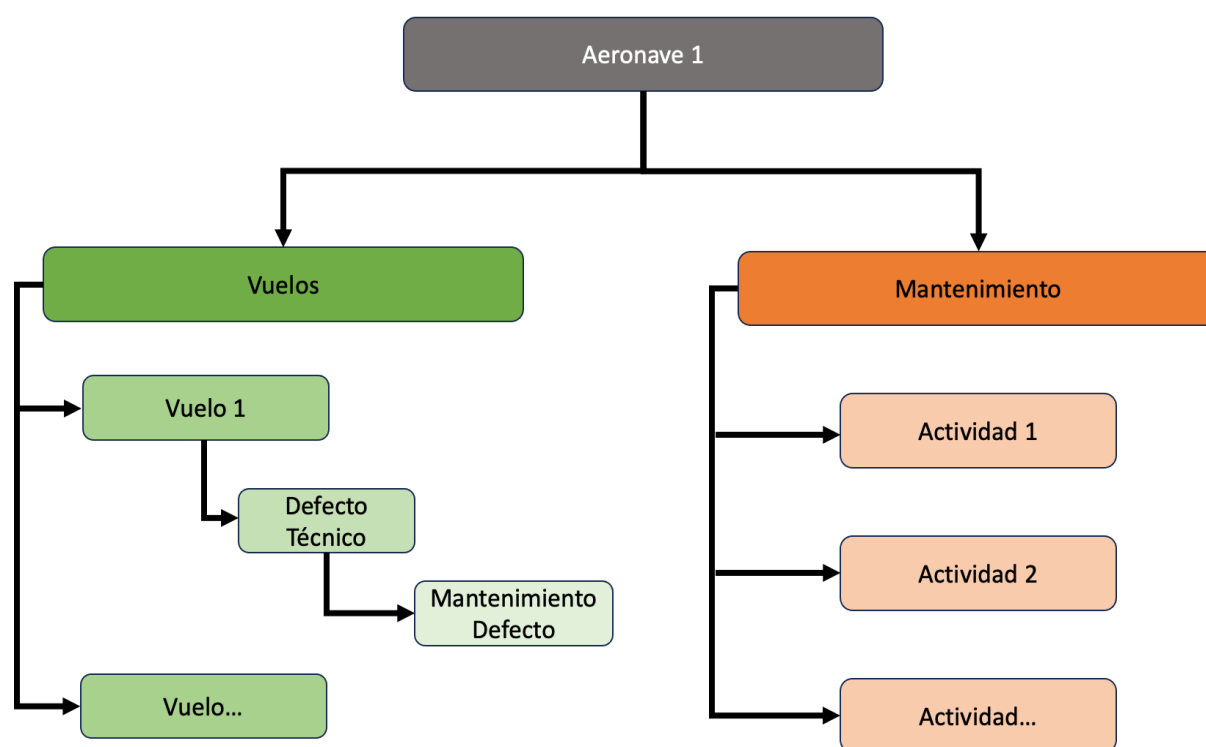


Figura 18. Estructura de datos en sistema ATL

Tras establecer la estructura de actividades y su interrelación en la aplicación ATL, se deben definir los datos mínimos necesarios que se recopilarán de cada una de ellas. Estos datos esenciales deberán ser suficientes para capturar toda la información necesaria y permitir a los usuarios realizar su trabajo de forma eficaz y eficiente. A continuación, se detallan los datos que se recogerán para cada actividad:

1. Aeronave:

- a. Número de registro: Matrícula identificativa de la aeronave.
- b. Fabricante: Nombre del fabricante de la aeronave.
- c. Modelo: Modelo específico de la aeronave.
- d. Número de serie: Número único de serie de la aeronave del fabricante.

2. Vuelos:

- a. Identificador de la aeronave: Número de registro de la aeronave que realizó el vuelo.
- b. Identificador de vuelo: Identificación de la aeronave durante el vuelo.
- c. Piloto al mando: Nombre del piloto responsable durante el vuelo.
- d. Aeropuerto de salida: Código del aeropuerto de salida.
- e. Aeropuerto de llegada: Código del aeropuerto de llegada.
- f. Fecha de salida: Fecha en la que se inició el vuelo.
- g. Hora de salida: Hora en la que se inició el vuelo.
- h. Duración del vuelo: Tiempo total de duración de vuelo.
- i. Consumo de combustible: Cantidad de combustible consumida durante el vuelo.
- j. Defectos técnicos: Lista de problemas técnicos registrados durante el vuelo.

3. Actividad de Mantenimiento:

- a. Tipo de mantenimiento: Indicación de si el mantenimiento es programado o no programado.
- b. Ubicación del mantenimiento: Lugar donde se realizó el mantenimiento.
- c. Responsable del mantenimiento: Nombre del responsable que llevó a cabo el mantenimiento.
- d. Fecha de inicio del mantenimiento: Fecha en la que comenzó el mantenimiento.
- e. Hora de inicio del mantenimiento: Hora en la que comenzó el mantenimiento.
- f. Horas totales de trabajo: Horas totales empleadas en el mantenimiento.
- g. Descripción de acciones: Detalles de las acciones específicas realizadas durante el mantenimiento.

- h. Sistemas afectados: Lista de sistemas afectados durante las acciones de mantenimiento.

4. Defectos Técnicos:

- a. Resumen del defecto: Descripción breve del defecto identificado.
- b. Descripción del defecto: Descripción detallada del defecto técnico.
- c. Sistemas afectados: Lista de sistemas afectados debido al defecto identificado.

5. Acciones de Mantenimiento Relacionados con Defectos Técnicos:

- a. Estado de reparación: Indicación de si la reparación está completa o incompleta.
- b. Responsable del mantenimiento: Nombre del responsable que llevó a cabo el mantenimiento.
- c. Descripción de acciones: Descripción detallada de las acciones realizadas durante el mantenimiento.
- d. Sistemas afectados: Lista de sistemas afectados durante las acciones de mantenimiento.

5.2 Desarrollo de la aplicación

5.2.1 Hardware y software utilizado

En esta sección se ofrece una visión general del hardware y el software utilizados en el desarrollo de la aplicación como prueba de concepto para el ATL basado en una solución blockchain básica.

El hardware principal utilizado para el desarrollo de la aplicación es ordenador portátil personal equipado con las siguientes especificaciones:

- **Procesador:** El entorno de desarrollo utilizó una CPU Intel(R) Core(TM) i7-10710U a 1,10 GHz, con una frecuencia Turbo Boost máxima de 4,70 GHz.
- **Memoria:** 16 GB de RAM.
- **Almacenamiento:** El ordenador estaba equipado con una unidad de estado sólido (SSD) de alta velocidad.

Las diferentes herramientas y tecnologías de software utilizadas en el desarrollo de la aplicación son las siguientes:

- **Lenguaje de programación:** Se eligió Python como lenguaje de programación principal por su versatilidad, sus amplias bibliotecas y su facilidad de uso. Esto lo hizo idóneo para implementar tanto la solución de cadena de bloques personalizada como los componentes basados en web de la aplicación.
- **Marco web:** La aplicación web se creó utilizando Flask, un marco web ligero y flexible para Python. Flask permite el manejo de peticiones y respuestas HTTP, permitiendo la rápida creación de prototipos.
- **HTML y CSS:** Para crear una interfaz fácil de usar para interactuar con el sistema ATL basado en blockchain, se diseñaron diferentes plantillas HTML. HTML proporcionó un diseño estructurado, mientras que CSS se utilizó para estilizar y mejorar la experiencia del usuario.



Figura 19. Logo Python (izquierda) y Flask (derecha)

5.2.2 Desarrollo de los bloques y estructura de datos

En la siguiente sección se verá el desarrollo tanto de la red blockchain utilizada en la aplicación, como de la estructura de datos de está basada en las consideraciones de diseño establecidas en las secciones anteriores.

Para la prueba de concepto se decidió implementar una blockchain creada manualmente. Aunque este diseño de blockchain es bastante simple en comparación con soluciones blockchain más sofisticadas y completas disponibles en el mercado, se consideró más que suficiente para demostrar la factibilidad y las ventajas de utilizar la tecnología blockchain en el contexto de ATL. Esta blockchain simple y manual permite una comprensión clara de cómo se manejan y protegen los datos, proporcionando una base sólida para la prueba de concepto y demostrando el potencial para futuras implementaciones más complejas y robustas. En las figuras 20 y 21 se puede ver el código desarrollado en Python para la definición de la estructura “Block” y funcionalidades “Blockchain” de la red.

```
class Blockchain:

    def __init__(self):
        self.chain = []
        try:
            self.load_chain()
        except (FileNotFoundError, EOFError):
            self.create_genesis_block()

    def create_genesis_block(self):
        genesis_block = Block(0, datetime.now(), [], "0")
        self.chain.append(genesis_block)

    def add_block(self, block):
        block.hash = block.calculate_hash(self.chain[-1].hash)
        self.chain.append(block)

    def get_latest_block(self):
        return self.chain[-1]

    def get_aircraft_list(self):
        aircraft_list = []
        for block in self.chain:
            for data in block.data:
                if isinstance(data, Flight) and data.aircraft not in aircraft_list:
                    aircraft_list.append(data.aircraft)
        return aircraft_list

    def save_chain(self):
        with open('blockchain.p', 'wb') as f:
            pickle.dump(self.chain, f)

    def load_chain(self):
        with open('blockchain.p', 'rb') as f:
            self.chain = pickle.load(f)
```

Figura 20. Código desarrollado de las funcionalidades Blockchain

```
class Block:

    def __init__(self, index, timestamp, data, previous_hash):
        self.index = index
        self.timestamp = timestamp
        self.data = data
        self.previous_hash = previous_hash
        self.hash = None

    def calculate_hash(self, previous_hash):
        hash_string = str(self.index) + str(self.timestamp) + str(self.data) + str(previous_hash)
        hash_bytes = hash_string.encode('utf-8')
        return hashlib.sha256(hash_bytes).hexdigest()
```

Figura 21. Código desarrollado de la estructura de un bloque de la red

Como se ha visto en secciones anteriores la pieza fundamental de toda red blockchain es el bloque en sí. En la figura 21 se puede ver la definición de la clase “Block” diseñada en la aplicación ATL. Esta tiene varios atributos clave que permiten mantener la integridad y funcionalidad de la blockchain:

1. **“index”**: Este entero sirve como identificador para cada bloque, proporcionándonos una forma fácil de referenciar bloques individuales y asegurando la naturaleza ordenada de la blockchain.
2. **“timestamp”**: Este objeto datetime registra el momento exacto en que se creó el bloque. Proporciona un registro cronológico de cuándo se añadió la información a la blockchain.
3. **“data”**: Esta es una lista que puede contener varios tipos de datos. En el caso de la aplicación ATL los datos estarán relacionados con un vuelo o una entrada de mantenimiento.
4. **“previous_hash”**: Esta cadena es el enlace criptográfico al bloque anterior de la cadena. Es una parte fundamental de la seguridad ya que cualquier cambio en un bloque resultaría en un cambio en su hash, rompiendo la cadena y alertando de posibles actividades fraudulentas.
5. **“hash”**: Esta cadena contiene el propio hash único del bloque que se calcula en base a los datos propios del bloque y al hash del bloque anterior. Este atributo permite preservar la integridad y la seguridad de la blockchain.

La clase “Block” también incorpora un método adicional llamado “calculate_hash”. Esta función genera el hash criptográfico para un bloque. Toma el “previous_hash” como parámetro y forma una cadena concatenando el “index” del bloque, el “timestamp”, “data” y el hash anterior “previous_hash”. Esta cadena se transforma entonces en bytes y se hashea utilizando el algoritmo SHA256, resultando en una cadena que representa el hash propio del bloque.

Después de la creación de la clase “Block”, se desarrolla la clase “Blockchain”, ver figura 20, que sirve como la estructura colectiva que alberga todos los bloques. La clase “Blockchain” presenta un atributo “chain”, que es una lista que contiene todos los bloques de la blockchain. El método de iniciación de esta red está diseñado para primero comprobar si hay una blockchain previamente almacenada en un archivo. Si existe, la blockchain se carga desde el archivo y si no se genera un bloque génesis.

La clase “Blockchain” además cuenta con otros métodos para asegurar un funcionamiento adecuado:

1. **“create_genesis_block”**: Esta función genera el bloque génesis con un índice de 0, el timestamp actual, una lista de datos vacía y un hash anterior de "0". Una vez creado, este bloque se añade inmediatamente a la red.
2. **“add_block”**: Esta función acepta un bloque como parámetro, calcula el hash del bloque y añade el bloque a la blockchain.
3. **“get_latest_block”**: Esta función recupera el bloque más reciente en la blockchain, necesario para añadir nuevos bloques y verificar la integridad de la cadena.
4. **“get_aircraft_list”**: Esta función escanea toda la blockchain y devuelve una lista de todas las aeronaves únicas incluidas en los bloques. Este método es útil para obtener una rápida visión general de todas las aeronaves registradas en el sistema.

5. **“save_chain”** y **“load_chain”**: Estos métodos son responsables de mantener el estado de la blockchain a través de las sesiones. El método **“save_chain”** guarda el estado actual de la blockchain en un archivo, mientras que el método **“load_chain”** recupera una blockchain previamente guardada desde un archivo.

La estructura de bloques desarrollada para la aplicación ATL aunque simple permite proporcionar un seguridad, inmutabilidad y trazabilidad. A continuación se profundizará en la estructura de datos específica y cómo encapsulamos los datos de vuelo y mantenimiento dentro de cada bloque.

La estructura de datos se debe desarrollar siguiendo también el diseño inicial para capturar información relacionada con las aeronaves, los vuelos, los problemas técnicos y las acciones de mantenimiento. Proporcionando de esta manera un registro exhaustivo de las actividades relacionadas con las aeronaves de una aerolínea. En la figura 22 se puede ver la definición en Python de las clases relativas a la aeronave **“Aircraft”**, vuelos **“Flight”** y actividades de mantenimiento **“MaintenanceEntry”**.

1. **“Aircraft”**: Esta clase es la columna vertebral de la estructura de datos ya que representa una aeronave específica. Encapsula en ella cuatro atributos clave:
 - a. **“registration_number”**: Número de registro.
 - b. **“manufacturer”**: Fabricante.
 - c. **“model”**: Modelo..
 - d. **“serial_number”**: Número de serie.
2. **“Flight”**: Esta clase es un registro detallado de cada vuelo realizado. Los atributos de esta clase son:
 - a. **“aircraft”**: Una referencia a un objeto Aircraft, asociando el vuelo a una aeronave específica.
 - b. **“callsign”**: Identificador de vuelo.
 - c. **“pilot_in_command”**: Piloto al mando.
 - d. **“departure_airport”** y **“arrival_airport”**: Códigos de los aeropuertos de salida y llegada.
 - e. **“departure_date”** y **“departure_time”**: La fecha y hora de salida del vuelo.
 - f. **“flight_duration”**: Duración del vuelo (horas y minutos).
 - g. **“fuel_consumed”**: Combustible consumido durante el vuelo.
 - h. **“technical_issues”**: Una lista de objetos TechnicalIssue que se registraron durante el vuelo. Si no existiera ninguna, este atributo se genera con una lista vacía.

3. **“MaintenanceEntry”**: Esta clase es un registro de las actividades de mantenimiento realizadas a una aeronave. Los atributos de esta clase son:
 - a. **“aircraft”**: Este atributo hace referencia a un objeto Aircraft, asociando la entrada de mantenimiento con una aeronave específica.
 - b. **“maintenance_type”**: Tipo de mantenimiento, si el mantenimiento fue programado (“Scheduled”) o no programado (“Unscheduled”). Además se incluye una comprobación para asegurar que solo pueda ser uno de estos dos estados.
 - c. **“maintenance_location”**: Ubicación del mantenimiento.
 - d. **“start_date”** y **“start_time”**: Fecha y hora del inicio del mantenimiento.
 - e. **“total_hours”**: Horas totales de trabajo.
 - f. **“actions_description”**: Descripción de acciones de mantenimiento.
 - g. **“affected_systems”**: Lista de los sistemas de la aeronave que fueron afectados o atendidos durante el mantenimiento. Esta lista se valida contra una lista predefinida de sistemas válidos para garantizar la coherencia y la precisión de los datos.
 - h. **“maintenanceresponsible”**: Responsable del mantenimiento.

```
class Aircraft:
    def __init__(self, registration_number, manufacturer, model, serial_number):
        self.registration_number = registration_number
        self.manufacturer = manufacturer
        self.model = model
        self.serial_number = serial_number

class Flight:
    def __init__(self, aircraft, callsign, pilot_in_command, departure_airport, arrival_airport, departure_date, departure_time, flight_duration, fuel_consumed, technical_issues=None):
        self.aircraft = aircraft
        self.callsign = callsign
        self.pilot_in_command = pilot_in_command
        self.departure_airport = departure_airport
        self.arrival_airport = arrival_airport
        self.departure_date = departure_date
        self.departure_time = departure_time
        self.flight_duration = flight_duration
        self.fuel_consumed = fuel_consumed

        # Initialize technical_issues as an empty list if it's None
        if technical_issues is None:
            self.technical_issues = []
        else:
            self.technical_issues = technical_issues

class MaintenanceEntry:
    def __init__(self, aircraft, maintenance_type, maintenance_location, start_date, start_time, total_hours, actions_description, affected_systems, maintenanceresponsible):
        self.aircraft = aircraft

        # Validate maintenance_type
        valid_types = ["Scheduled", "Unscheduled"]
        if maintenance_type not in valid_types:
            raise ValueError("Invalid maintenance_type. It should be 'Scheduled' or 'Unscheduled'.")
        self.maintenance_type = maintenance_type

        self.maintenance_location = maintenance_location
        self.start_date = start_date
        self.start_time = start_time
        self.total_hours = total_hours
        self.actions_description = actions_description

        # Validate affected_systems (as a list)
        for system in affected_systems:
            if system not in VALID_AFFECTED_SYSTEMS:
                raise ValueError("Invalid affected_system '{}'. It should be one of the following: {}".format(system, VALID_AFFECTED_SYSTEMS))
        self.affected_systems = affected_systems

        self.maintenanceresponsible = maintenanceresponsible
```

Figura 22. Definición de las clases “Aircraft”, “Flight” y “MaintenanceEntry”

En la figura 23 se puede ver la definición en Python de las clases relativas a los defectos técnicos “TechnicalIssue” y acciones de mantenimiento relacionadas con defectos técnicos “MaintenanceAction”.

```
class TechnicalIssue:
    def __init__(self, summary, description, affected_systems):
        self.id = uuid.uuid4()
        self.summary = summary
        self.description = description

        # Validate affected_systems (as a list)
        for system in affected_systems:
            if system not in VALID_AFFECTED_SYSTEMS:
                raise ValueError("Invalid affected_system '{}'. It should be one of the following: {}".format(system, VALID_AFFECTED_SYSTEMS))
        self.affected_systems = affected_systems

class MaintenanceAction:
    def __init__(self, repair_status, maintenance_datetime, description, affected_systems, associated_issue_id, maintenanceresponsible):
        self.repair_status = repair_status

        # Validate repair_status
        valid_types = ["Complete", "Incomplete"]
        if repair_status not in valid_types:
            raise ValueError("Invalid maintenance_type. It should be 'Scheduled' or 'Unscheduled'.")
        self.repair_status = repair_status

        self.maintenance_datetime = maintenance_datetime
        self.description = description

        # Validate affected_systems (as a list)
        for system in affected_systems:
            if system not in VALID_AFFECTED_SYSTEMS:
                raise ValueError("Invalid affected_system '{}'. It should be one of the following: {}".format(system, VALID_AFFECTED_SYSTEMS))
        self.affected_systems = affected_systems

        self.associated_issue_id = associated_issue_id
        self.maintenanceresponsible = maintenanceresponsible
```

Figura 23. Definición de las clases “TechnicalIssue” y “MaintenanceAction”

1. **“TechnicalIssue”**: Esta clase encapsula detalles sobre los problemas técnicos que pueden ocurrir durante un vuelo. Incluye:
 - a. “id”: Un identificador único generado utilizando el algoritmo UUID4, asegurando que cada problema puede ser rastreado individualmente. Esto es necesario para poder relacionar las “MaintenanceAction” con las “TechnicalIssue”
 - b. “summary”: Resumen del defecto.
 - c. “description”: Descripción del defecto.
 - d. “affected_systems”: Lista de los sistemas afectados por el problema. Estos sistemas se validan contra una lista predefinida de sistemas válidos, asegurando que sólo se registren sistemas reconocidos.
2. **“MaintenanceAction”**: Esta clase es un registro de las acciones tomadas para rectificar problemas técnicos identificados. Incluye:
 - a. “repair_status”: El estado de la reparación, que puede ser "Completo" o "Incompleto".
 - b. “maintenance_datetime”: La fecha y hora en que se realizó el mantenimiento.
 - c. “description”: Descripción de las acciones de mantenimiento.

- d. “affected_systems”: Lista de sistemas afectados por la acción de mantenimiento, validados de manera similar a la clase “TechnicalIssue”.
- e. “associated_issue_id”: Una referencia al ID del “TechnicalIssue” asociado, proporcionando un enlace directo entre el problema y la acción tomada para resolverlo.
- f. “maintenanceresponsible”: Responsable del mantenimiento.

La estructura de datos definida para la aplicación ATL proporciona una primera aproximación a un marco robusto, completo y consistente para almacenar y recuperar datos de vuelo y mantenimiento dentro de cada bloque en la blockchain. A continuación, la siguiente sección profundizará en el desarrollo de las funcionalidades e interfaz de la aplicación a ser usadas por los usuarios de la aplicación.

5.2.3 Desarrollo de la interfaz y funcionalidades

Para atender eficazmente a los diferentes roles y requisitos de los usuarios previamente identificados se han desarrollado tres aplicaciones distintas como parte de la solución ATL basada en blockchain. Estas aplicaciones están diseñadas para los tres grupos principales de usuarios definidos: miembros de la tripulación de cabina, personal de mantenimiento, aerolíneas y organismos supervisores. Cada aplicación proporciona una interfaz de usuario y funcionalidades personalizadas que satisfacen las necesidades únicas de cada grupo de usuarios, asegurando una interacción eficiente con el sistema de blockchain ATL.

Comenzando con la aplicación para la tripulación de cabina mencionar que el se ha puesto un gran énfasis en crear una interfaz de usuario que fuera limpia y fácil de usar permitiendo a la tripulación de cabina interactuar de manera efectiva con el sistema. El usuario puede iniciar sesión en la aplicación a través de la función de login, donde los datos de usuario y contraseña se verifican contra una lista de usuarios registrados. Una vez autenticado, el usuario puede seleccionar una aeronave específica de la lista de aeronaves disponibles en la blockchain.

Una vez seleccionada la aeronave, se puede acceder al historial de la aeronave. En este se muestra una lista de vuelos y entradas de mantenimiento para la aeronave seleccionada ordenadas cronológicamente. Adicionalmente, para cada vuelo se muestran los problemas técnicos asociados y las acciones de mantenimiento realizadas para resolver dichos problemas. Todos estos datos se recopilan a partir de la información almacenada previamente en la blockchain.

La aplicación también permite a los miembros de la tripulación de cabina registrar nuevos vuelos. Durante el registro de un nuevo vuelo deben introducir todos los datos básicos como el número de vuelo, los aeropuertos de salida y llegada o la fecha y hora de salida entre otros. También pueden registrar cualquier problema técnico que se haya producido durante el vuelo, incluyendo el resumen del problema, una descripción detallada y los sistemas de la aeronave que se vieron afectados. Todos estos datos se encapsulan en un objeto “Flight”, que luego se utiliza para crear un nuevo bloque. El

bloque se añade a la blockchain, proporcionando un registro seguro e inmutable del vuelo y de cualquier problema técnico que haya surgido.

Continuando ahora con la aplicación para el personal de mantenimiento. Al igual que la aplicación para la tripulación de cabina, el usuario puede iniciar sesión en la aplicación mediante la función de login, verificando los datos de usuario y contraseña contra una lista de usuarios registrados. Una vez autenticado, el usuario puede seleccionar una aeronave específica de la lista de aeronaves disponibles en la blockchain.

En el historial de la aeronave, el usuario puede ver una lista de vuelos y entradas de mantenimiento, ordenadas cronológicamente, para la aeronave seleccionada. Para cada vuelo, se muestran los problemas técnicos asociados y las acciones de mantenimiento realizadas para resolver dichos problemas.

Además, la aplicación permite al personal de mantenimiento registrar nuevas acciones de mantenimiento y entradas de mantenimiento. Durante el registro de una nueva acción de mantenimiento, se pueden introducir datos como el estado de la reparación, la fecha y hora del mantenimiento, la descripción de las acciones realizadas, y los sistemas de la aeronave que se vieron afectados. Todos estos datos se encapsulan en un objeto "MaintenanceAction", que luego se utiliza para crear un nuevo bloque. El bloque se añade a la blockchain.

La aplicación también permite al personal de mantenimiento registrar nuevas entradas de mantenimiento, lo que incluye la introducción de datos como el tipo de mantenimiento, la ubicación del mantenimiento, la fecha y hora de inicio, el total de horas, la descripción de las acciones y los sistemas de la aeronave afectados. Estos datos se encapsulan en un objeto "MaintenanceEntry", que luego se utiliza para crear un nuevo bloque añadiendo se esté a la blockchain.

Por último, la aplicación para aerolíneas y organismos supervisores permite, como las anteriores, a los usuarios iniciar sesión mediante la función de login. Los datos del usuario y la contraseña se verifican contra una lista de usuarios registrados. Una vez autenticado, el usuario puede seleccionar una aeronave específica de la lista de aeronaves disponibles en la blockchain.

En el historial de la aeronave, el usuario puede ver una lista de vuelos y entradas de mantenimiento, ordenadas cronológicamente, para la aeronave seleccionada. Para cada vuelo, se muestran los problemas técnicos asociados y las acciones de mantenimiento realizadas para resolver dichos problemas. Además de visualizar los datos, la aplicación también se ha desarrollado permitiendo a los usuarios descargar los datos en formato JSON. El archivo JSON descargado contiene los mismos datos que se muestran en el historial de la aeronave, lo que permite a los usuarios conservar un registro local de los datos de la aeronave para su posterior análisis.

La aplicación también proporciona un conjunto avanzado de filtros para que los usuarios puedan buscar datos específicos dentro del conjunto de datos de la aeronave. Los usuarios pueden filtrar los datos por tipo de entrada (vuelo o mantenimiento), rango de fechas, aeropuerto de salida, aeropuerto de llegada, sistemas afectados en el vuelo, tipo de mantenimiento, ubicación del mantenimiento y sistemas afectados en el mantenimiento.

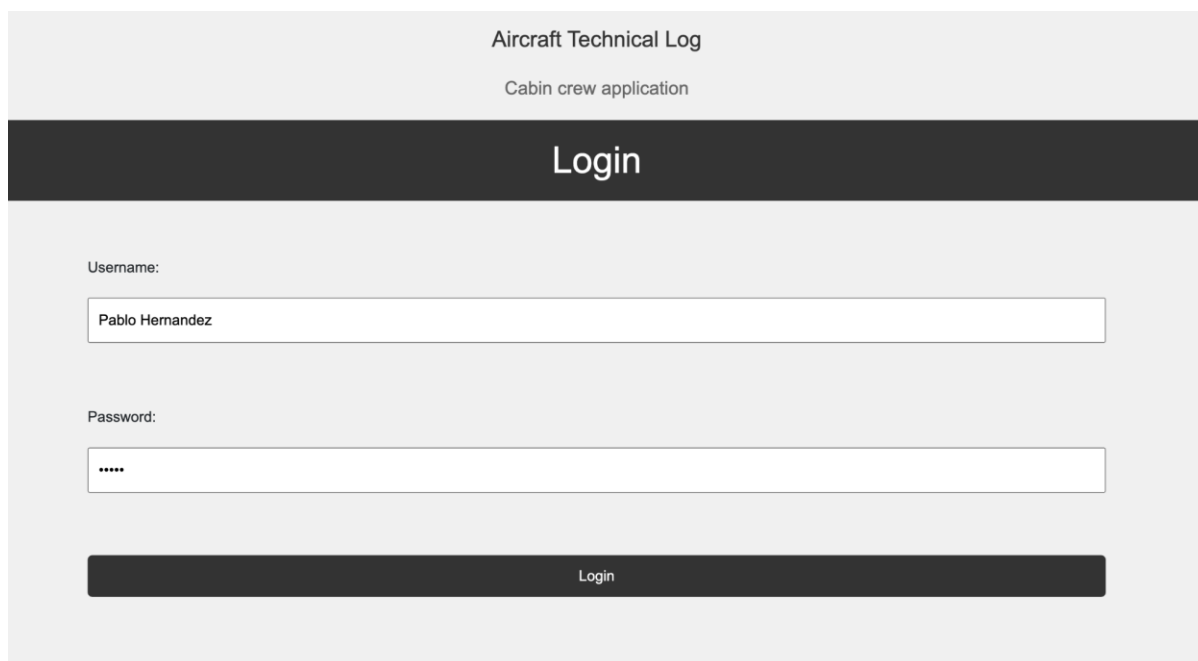
En conclusión, para el nuevo sistema ATL basado en blockchain se han desarrollado tres aplicaciones web distintas para adecuarse a los requisitos y funcionalidades necesarias de los usuarios. Todas las aplicaciones se implementan utilizando el framework Flask de Python y utilizan plantillas HTML para la interfaz de usuario.

5.3 Demostración

En la siguiente sección, se realizará una demostración detallada de las tres aplicaciones web desarrolladas: la aplicación de la tripulación de cabina, la aplicación de mantenimiento y la aplicación de la aerolínea y organismo supervisor. Esta demostración servirá como un "walkthrough", mostrando el flujo de trabajo de cada aplicación y destacando sus características y funcionalidades clave. Para hacer esta demostración más ilustrativa, se han generado datos de ejemplo para poblar la blockchain y permitir una experiencia de usuario realista. Sin embargo, es importante destacar que todos los datos mostrados en esta demostración son ficticios y no hacen referencia a ninguna aeronave real. La demostración tiene como objetivo mostrar cómo estas aplicaciones podrían ser utilizadas en la práctica y no pretende representar ninguna operación de vuelo o mantenimiento real.

5.3.1 Tripulación de Cabina

Para demostrar el funcionamiento de esta aplicación, se propondrá un escenario ficticio en el que una tripulación tiene previsto realizar un vuelo desde Madrid a A Coruña el 27 de julio de 2023. Conforme al uso de un Aircraft Technical Log (ATL), la tripulación deberá llevar a cabo una revisión previa a cada vuelo para garantizar el estado óptimo de la aeronave y detectar cualquier posible problema o requerimiento de mantenimiento antes de su utilización. Como se menciona en la sección 5.2.3, antes de acceder a la aplicación, la tripulación deberá autenticarse mediante un usuario y contraseña. Esta autenticación no solo permitirá el acceso, sino que también se utilizará para identificar la suscripción de un nuevo bloque en la cadena, tal como se verá posteriormente. En la figura 24 se muestra la página de inicio de la aplicación.



Aircraft Technical Log
Cabin crew application

Login

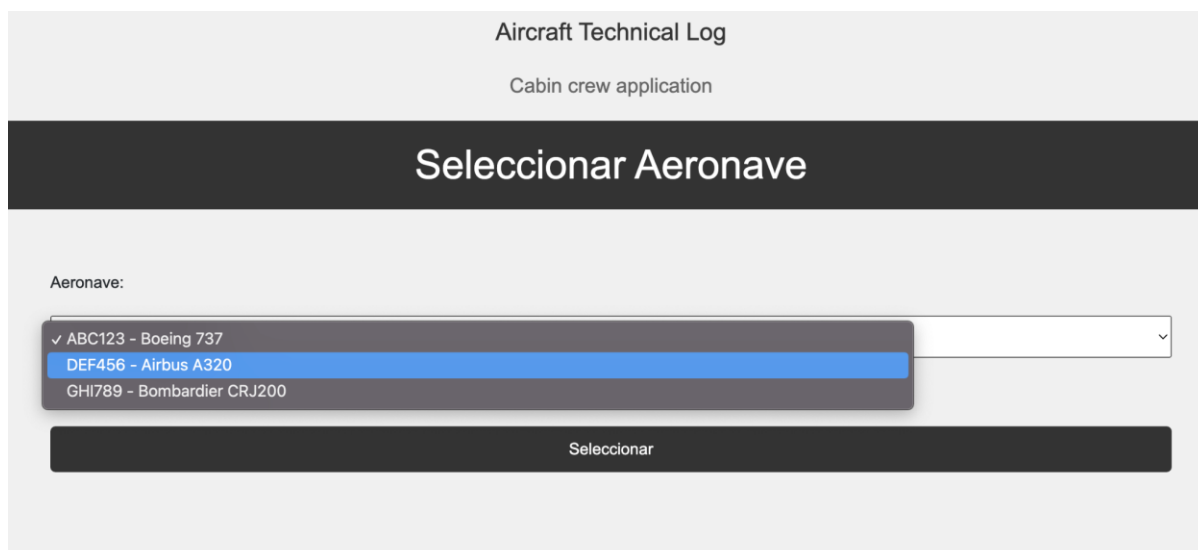
Username:
Pablo Hernandez

Password:
.....

Login

Figura 24. Página de login aplicación de tripulación de cabina

Una vez dentro de la aplicación, el primer paso para la tripulación será seleccionar la aeronave que van a operar. Para este escenario en particular, se supondrá que utilizarán un A320. Esta selección se hace mediante un desplegable, ver figura 25.



Aircraft Technical Log
Cabin crew application

Seleccionar Aeronave

Aeronave:

- ✓ ABC123 - Boeing 737
- DEF456 - Airbus A320
- GHI789 - Bombardier CRJ200

Seleccionar

Figura 25. Página de selección de aeronave aplicación de tripulación de cabina

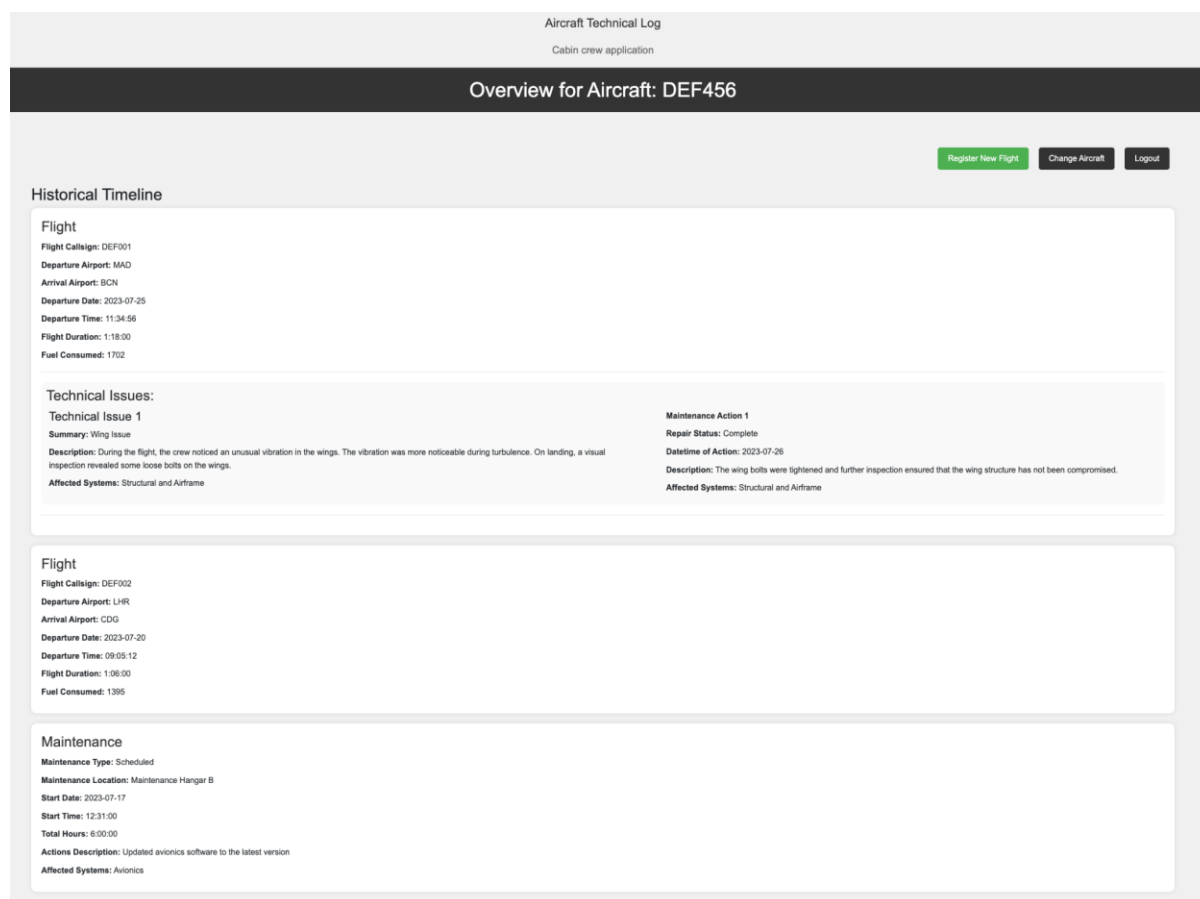
Una vez que la aeronave deseada ha sido seleccionada, el usuario será redirigido a una página donde podrá visualizar el historial completo de dicha aeronave, que incluirá tanto los vuelos realizados como las acciones de mantenimiento llevadas a cabo, todo ordenado cronológicamente. Esta información se puede ver en la figura 26.

En esta vista, se puede verificar que ha habido dos vuelos previos: uno desde Madrid a Barcelona el día 25 y otro desde Londres a París el día 20. Además, se muestra una actividad de mantenimiento programada el día 17. En cuanto al vuelo Madrid-Barcelona, se identificó un problema técnico relacionado con el ala de la aeronave, el cual fue solucionado al día siguiente, el día 26. Se puede ver esta información en la figura 27, donde se presenta una información del historial ampliada.

Una vez que se ha verificado la información y el piloto está de acuerdo con ella, se puede proceder a realizar el vuelo Madrid-A Coruña. Una vez concluido el vuelo, el piloto podrá introducir toda la información necesaria en el ATL a través de la misma aplicación.

En la vista anterior, donde se muestra el historial de la aeronave A320 (figura 26), en la parte superior derecha se encuentran tres botones. Los dos botones de la derecha permiten al usuario regresar a la página de selección de aeronave (Change Aircraft) o desconectarse (Logout) de la aplicación. El botón de la izquierda, resaltado en color verde (Register New Flight), al ser pulsado, redirige al usuario a una página específica para ingresar toda la información relevante del vuelo.

En esta nueva página aparece un formulario “Flight Log” donde ingresar la información esencial del vuelo: número de vuelo, aeropuerto de salida, aeropuerto de llegada, fecha y hora de salida, tiempo total de vuelo en horas y combustible consumido en kilogramos. En la figura 28 se puede ver este formulario.



The screenshot displays the 'Aircraft Technical Log' application interface. At the top, it identifies the application as 'Cabin crew application' and shows the 'Overview for Aircraft: DEF456'. Three buttons are visible in the top right: 'Register New Flight' (highlighted in green), 'Change Aircraft', and 'Logout'. The main content is organized into a 'Historical Timeline' with three sections:

- Flight 1:** Flight Callsign: DEF001, Departure Airport: MAD, Arrival Airport: BCN, Departure Date: 2023-07-25, Departure Time: 11:34:56, Flight Duration: 1:18:00, Fuel Consumed: 1702.
- Technical Issues:** Technical Issue 1. Summary: Wing Issue. Description: During the flight, the crew noticed an unusual vibration in the wings. The vibration was more noticeable during turbulence. On landing, a visual inspection revealed some loose bolts on the wings. Affected Systems: Structural and Airframe. Maintenance Action 1. Repair Status: Complete. Datetime of Action: 2023-07-26. Description: The wing bolts were tightened and further inspection ensured that the wing structure has not been compromised. Affected Systems: Structural and Airframe.
- Flight 2:** Flight Callsign: DEF002, Departure Airport: LHR, Arrival Airport: CDG, Departure Date: 2023-07-20, Departure Time: 09:05:12, Flight Duration: 1:06:00, Fuel Consumed: 1395.
- Maintenance:** Maintenance Type: Scheduled, Maintenance Location: Maintenance Hangar B, Start Date: 2023-07-17, Start Time: 12:31:00, Total Hours: 6:00:00, Actions Description: Updated avionics software to the latest version, Affected Systems: Avionics.

Figura 26. Historial aeronave A320 aplicación de tripulación de cabina

Historical Timeline

Flight

Flight Callsign: DEF001
Departure Airport: MAD
Arrival Airport: BCN
Departure Date: 2023-07-25
Departure Time: 11:34:56
Flight Duration: 1:18:00
Fuel Consumed: 1702

Technical Issues:

Technical Issue 1	Maintenance Action 1
Summary: Wing Issue	Repair Status: Complete
Description: During the flight, the crew noticed an unusual vibration in the wings. The vibration was more noticeable during turbulence. On landing, a visual inspection revealed some loose bolts on the wings.	Datetime of Action: 2023-07-26
Affected Systems: Structural and Airframe	Description: The wing bolts were tightened and further inspection ensured that the wing structure has not been compromised.
	Affected Systems: Structural and Airframe

Figura 27. Vuelo MAD-BCN aeronave A320 aplicación de tripulación de cabina

Aircraft Technical Log
Cabin crew application

Flight Log

[Back to timeline](#)

Flight Number: DEF003

Departure Airport: MAD

Arrival Airport: LCG

Departure Date: 27/07/2023 Departure Time: 14:30

Total Flight Duration (Hours): 1.17

Total Fuel Consumed (KG): 1620

Figura 28. Formulario de vuelo “Flight Log” para el vuelo MAD-BCN aplicación de tripulación de cabina

El formulario presentado en la figura 28 ha sido completado con los datos correspondientes al vuelo Madrid-A Coruña. En la sección final del formulario, como se muestra en la figura 29, se brinda la opción de agregar cualquier defecto técnico que haya ocurrido durante el vuelo. Para ello, se debe proporcionar un resumen de la incidencia, una descripción detallada y seleccionar de una lista los sistemas afectados por dicha incidencia. En este caso, se ha descrito un problema en el tren de aterrizaje del ala izquierda durante la fase final de aproximación. Dado que no se tiene claridad si el problema proviene del tren de aterrizaje o del sistema de alerta, se han marcado como sistemas afectados "Structural and Airframe" e "Instrumentation and Warning".

Una vez que toda la información ha sido introducida, el usuario presiona el botón "Submit". Si no se detecta ningún problema, el nuevo bloque de datos se subirá a la red y el usuario será redirigido a la página del historial de la aeronave, donde podrá verificar que la información se ha subido correctamente, ver figura 30.

Si el piloto tiene otro vuelo, puede volver a utilizar la aplicación para repetir el proceso. De igual manera, el personal de mantenimiento y la siguiente tripulación podrán verificar el estado actual de la aeronave mediante sus respectivas aplicaciones después de este vuelo.

Este ciclo de registro, actualización y verificación en la aplicación proporciona una gestión fluida y confiable de la información relacionada con la aeronave, asegurando una comunicación eficiente entre todos los actores involucrados y mejorando la seguridad y eficiencia en las operaciones aéreas.

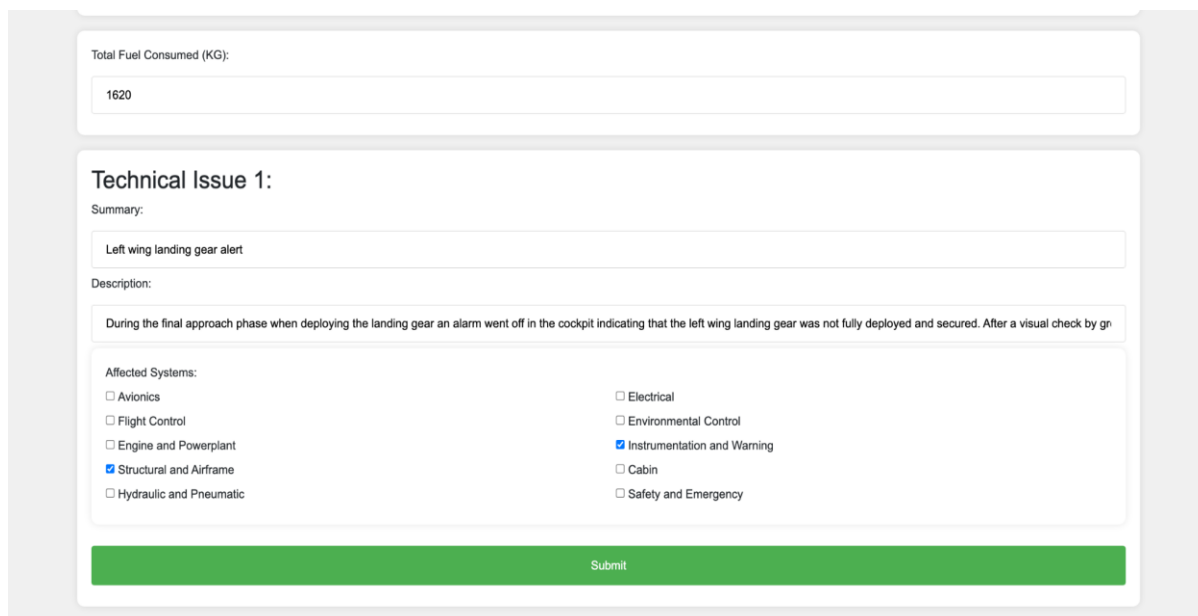


Figura 29. Formulario de defectos técnicos en el "Flight Log" para el vuelo MAD-BCN aplicación de tripulación de cabina

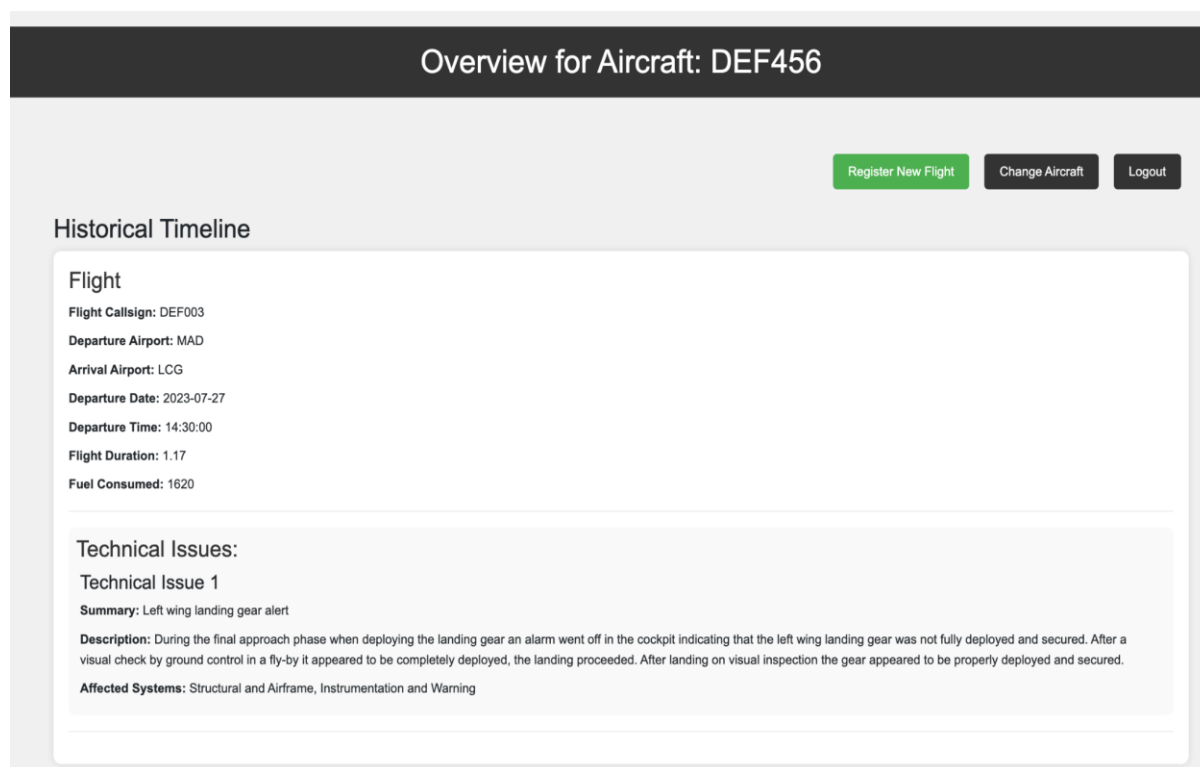


Figura 30. Historial del A320 con el nuevo vuelo MAD-BCN aplicación de tripulación de cabina

5.3.2 Personal de Mantenimiento

Para continuar con la demostración ahora con la aplicación para el personal de mantenimiento, se utilizará el mismo escenario ficticio en el que se realizó un vuelo desde Madrid a A Coruña el 27 de julio de 2023. Esta vez, desde la perspectiva de un miembro del equipo de mantenimiento que utiliza la aplicación de mantenimiento para monitorear cualquier problema con la aeronave utilizada en el vuelo. A través de la aplicación de mantenimiento, el personal puede revisar el estado técnico de la aeronave después de cada vuelo y programar cualquier mantenimiento necesario. Al igual que con la aplicación de la tripulación, antes de acceder a la aplicación además de seleccionar la aeronave que quien visualizar o con la que quieren trabajar. Ver figuras 31 y 32.

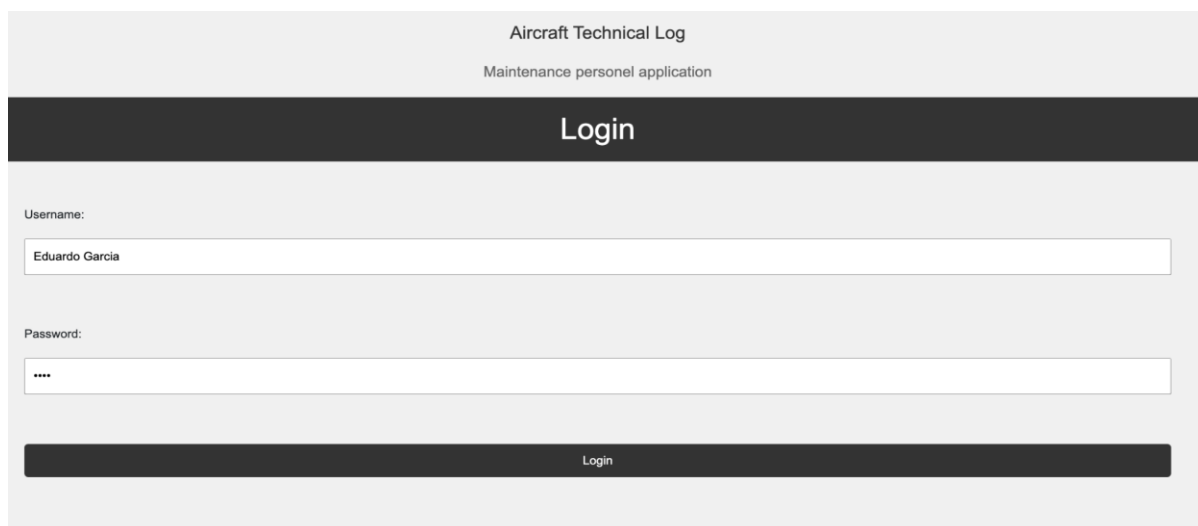


Figura 31. Página de login aplicación personal de mantenimiento

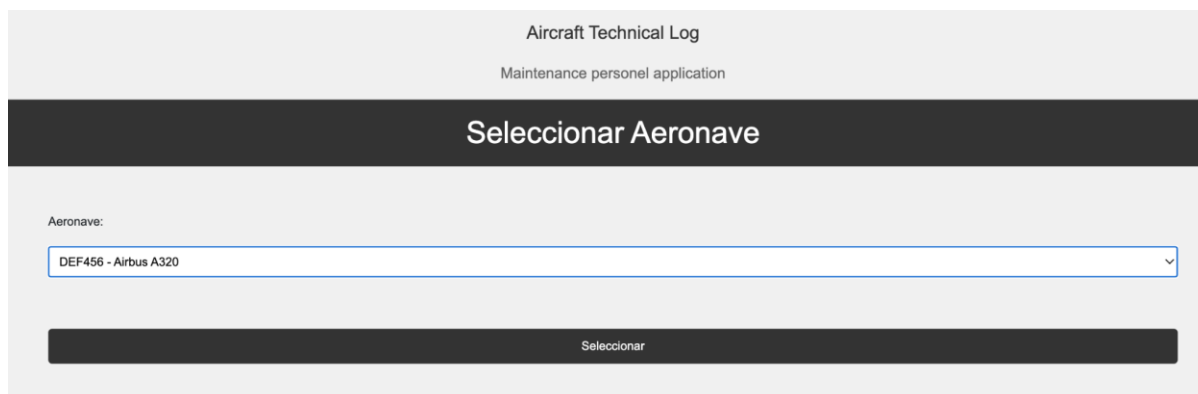


Figura 32. Página de selección de aeronave aplicación personal de mantenimiento

Al acceder a la página del historial de la aeronave A320, se presentan de manera ordenada y cronológica las diversas actividades de vuelos y mantenimientos de dicha aeronave. En este caso, lo primero que se muestra es el vuelo previamente introducido Madrid-A Coruña, junto con el defecto técnico identificado. Una diferencia importante con la aplicación de la tripulación de cabina es que ahora, en aquellos vuelos donde se hayan identificado defectos técnicos, aparecerá un botón que permitirá al usuario agregar una acción de mantenimiento para abordar el problema identificado, tal como se observa en las figuras 33 y 34. Además, el botón verde que anteriormente permitía a los usuarios de la aplicación de tripulación de cabina registrar un nuevo vuelo, en esta ocasión, permite el registro de una actividad de mantenimiento bajo la opción "Register Maintenance Work", ver figura 33.

Aircraft Technical Log
Maintenance personnel application

Overview for Aircraft: DEF456

[Register Maintenance Work](#) [Change Aircraft](#) [Logout](#)

Historical Timeline

Flight

Flight Callsign: DEF003
Departure Airport: MAD
Arrival Airport: LCG
Departure Date: 2023-07-27
Departure Time: 14:30:00
Flight Duration: 1:10:12
Fuel Consumed: 1620

Technical Issues:

Technical Issue 1

Summary: Left wing landing gear alert

Description: During the final approach phase when deploying the landing gear an alarm went off in the cockpit indicating that the left wing landing gear was not fully deployed and secured. After a visual check by ground control in a fly-by it appeared to be completely deployed, the landing proceeded. After landing on visual inspection the gear appeared to be properly deployed and secured.

Affected Systems: Structural and Airframe, Instrumentation and Warning

[Add Maintenance Action](#)

Figura 33. Historial aeronave A320 aplicación personal de mantenimiento (1)

Flight

Flight Callsign: DEF001
Departure Airport: MAD
Arrival Airport: BCN
Departure Date: 2023-07-25
Departure Time: 11:34:56
Flight Duration: 1:18:00
Fuel Consumed: 1702

Technical Issues:

Technical Issue 1

Summary: Wing Issue

Description: During the flight, the crew noticed an unusual vibration in the wings. The vibration was more noticeable during turbulence. On landing, a visual inspection revealed some loose bolts on the wings.

Affected Systems: Structural and Airframe

[Add Maintenance Action](#)

Maintenance Action 1

Repair Status: Complete
Datetime of Action: 2023-07-26

Description: The wing bolts were tightened and further inspection ensured that the wing structure has not been compromised.

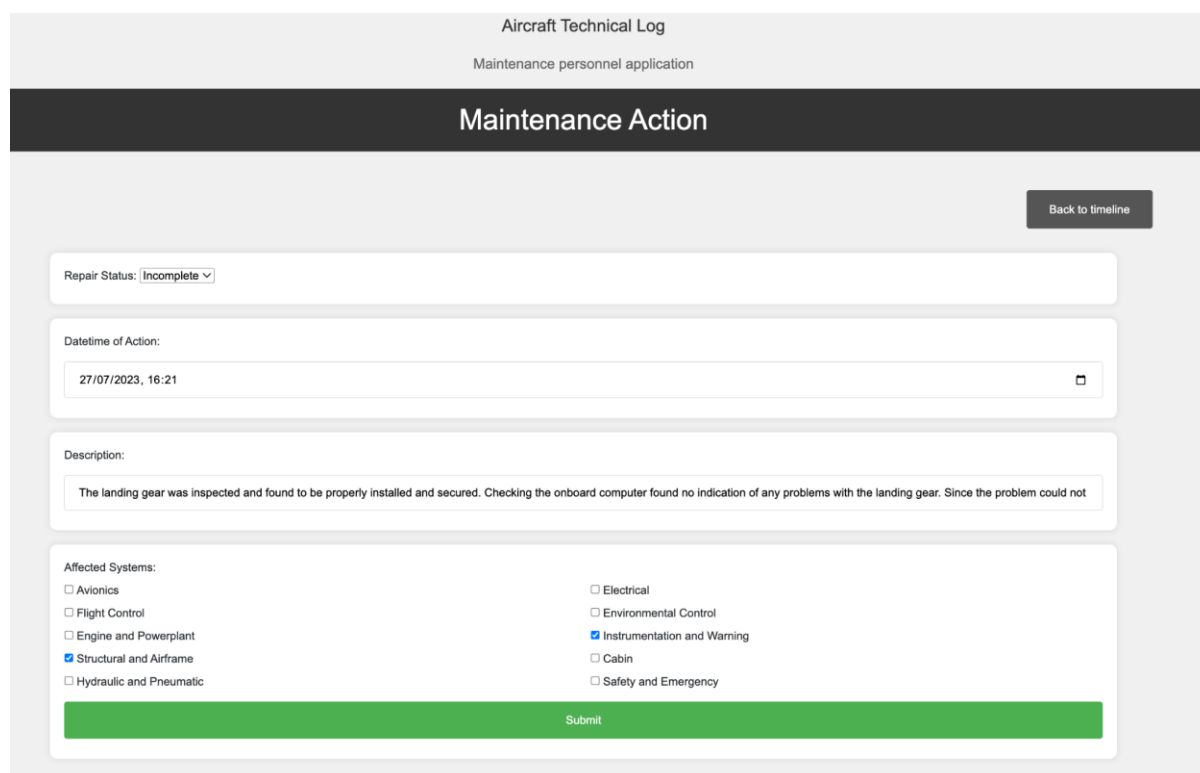
Affected Systems: Structural and Airframe

Figura 34. Historial aeronave A320 aplicación personal de mantenimiento (2)

Para explorar todas las funcionalidades de la aplicación, se imagina que después del vuelo Madrid-A Coruña, el personal de mantenimiento revisa el ATL y decide llevar a cabo una acción de mantenimiento para abordar el defecto técnico identificado. Utilizando la aplicación, presionan el botón "Add Maintenance Action" asociado al defecto técnico, lo que los redirige a un cuestionario específico.

En este cuestionario, se les solicita establecer el estado de la reparación, la fecha y hora de la reparación, una descripción detallada de las acciones llevadas a cabo y los sistemas afectados. Para fines de demostración, se supone que en esta reparación no logran solucionar el problema debido a que no pueden replicarlo, por lo tanto, marcan la acción de mantenimiento como "Incomplete".

La figura 35 muestra el formulario con la información requerida cumplimentada, y la figura 36 muestra cómo queda registrado en el historial una vez que se crea este nuevo bloque en la blockchain. De esta manera, la acción de mantenimiento queda vinculada al vuelo y al defecto técnico específico, asegurando una trazabilidad completa de todas las operaciones y mantenimientos realizados en la aeronave.



Aircraft Technical Log
Maintenance personnel application

Maintenance Action

Back to timeline

Repair Status: **Incomplete** ▾

Datetime of Action:
27/07/2023, 16:21

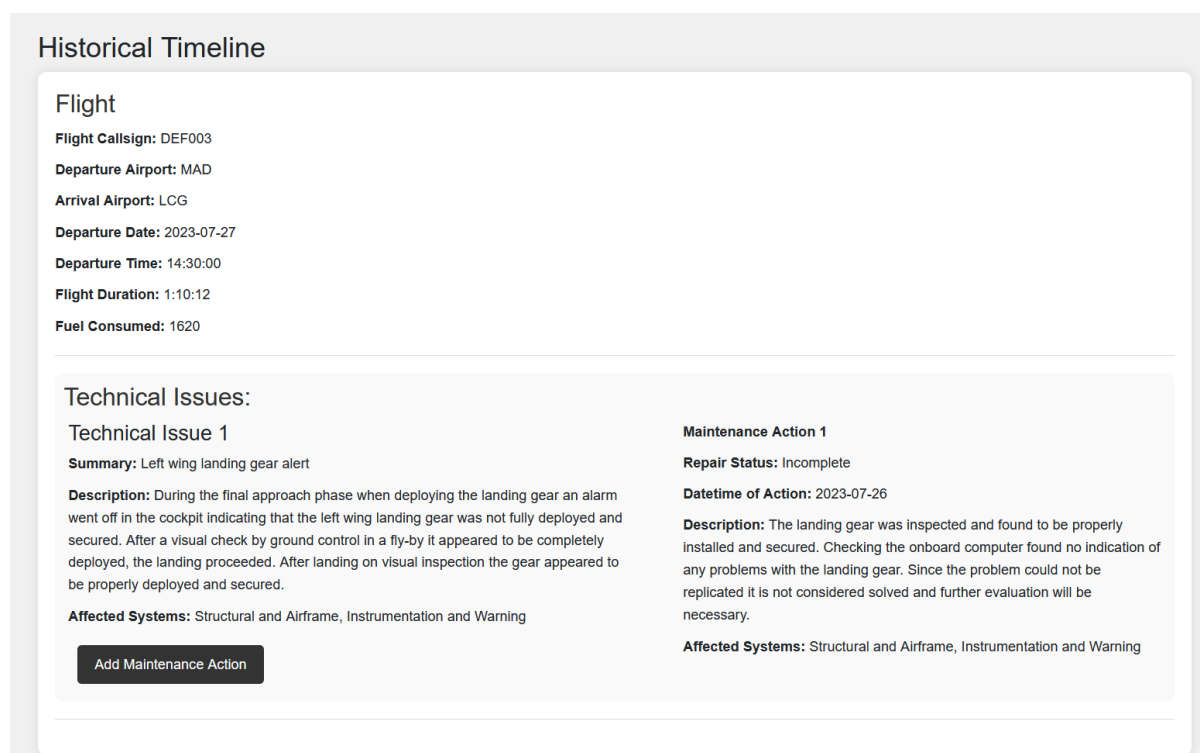
Description:
The landing gear was inspected and found to be properly installed and secured. Checking the onboard computer found no indication of any problems with the landing gear. Since the problem could not

Affected Systems:

- Avionics
- Flight Control
- Engine and Powerplant
- Structural and Airframe
- Hydraulic and Pneumatic
- Electrical
- Environmental Control
- Instrumentation and Warning
- Cabin
- Safety and Emergency

Submit

Figura 35. Formulario de registro de acción de mantenimiento relacionada con un defecto técnico aplicación personal de mantenimiento



The screenshot displays a 'Historical Timeline' section. Under the 'Flight' header, the following details are listed: Flight Callsign: DEF003, Departure Airport: MAD, Arrival Airport: LCG, Departure Date: 2023-07-27, Departure Time: 14:30:00, Flight Duration: 1:10:12, and Fuel Consumed: 1620. Below this, a 'Technical Issues' section is shown. It contains a 'Technical Issue 1' with a summary: 'Left wing landing gear alert'. The description states: 'During the final approach phase when deploying the landing gear an alarm went off in the cockpit indicating that the left wing landing gear was not fully deployed and secured. After a visual check by ground control in a fly-by it appeared to be completely deployed, the landing proceeded. After landing on visual inspection the gear appeared to be properly deployed and secured.' The affected systems are listed as 'Structural and Airframe, Instrumentation and Warning'. A button labeled 'Add Maintenance Action' is visible. To the right, a 'Maintenance Action 1' is detailed with a repair status of 'Incomplete', a datetime of '2023-07-26', and a description: 'The landing gear was inspected and found to be properly installed and secured. Checking the onboard computer found no indication of any problems with the landing gear. Since the problem could not be replicated it is not considered solved and further evaluation will be necessary.' The affected systems for this action are also 'Structural and Airframe, Instrumentation and Warning'.

Figura 36. Acción de mantenimiento en el historial de la aeronave A320 aplicación personal de mantenimiento

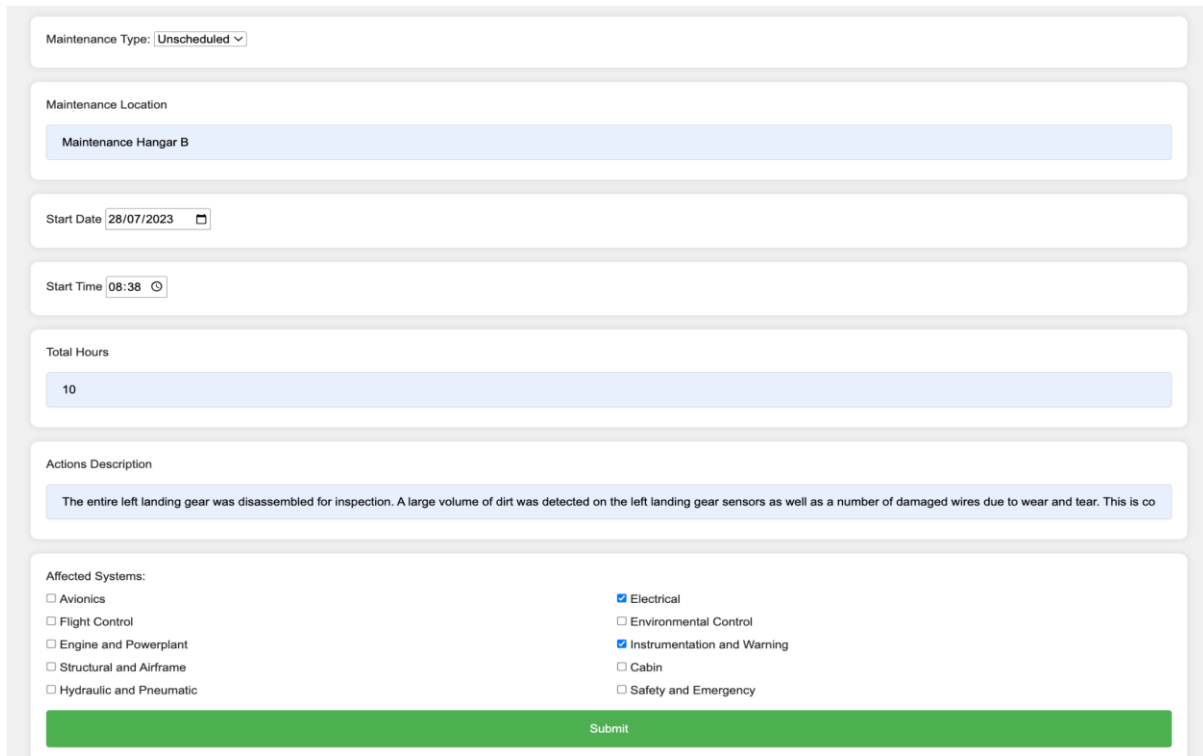
Debido a la imposibilidad de solucionar el problema identificado y considerando su impacto potencial en la seguridad de la aeronave, se toma la decisión de llevar a cabo una actividad de mantenimiento más exhaustiva para abordar el defecto técnico. En esta acción de mantenimiento, se realiza un desmontaje completo del tren de aterrizaje izquierdo y se lleva a cabo una revisión detallada. Durante la inspección, se descubren problemas relacionados con los sensores debido a la presencia de suciedad y se identifican algunos cables dañados. Se considera que esto fue la causa del problema, por lo que se procede a limpiar los sensores y a reemplazar los cables dañados.

Para registrar esta actividad de mantenimiento, el usuario simplemente debe dirigirse a la página del historial de la aeronave y presionar el botón "Register Maintenance Work". Al hacerlo, será redirigido a un cuestionario donde se le solicitará indicar el tipo de mantenimiento, la ubicación, la fecha y hora de inicio, el total de horas de trabajo, una descripción detallada de las acciones realizadas y los sistemas afectados. En la figura 37 se puede apreciar este cuestionario completado con el supuesto planteado.

Una vez que toda la información ha sido introducida, el usuario presiona el botón "Submit". Si no se detecta ningún problema, el nuevo bloque de datos se subirá a la red y el usuario será redirigido a la página del historial de la aeronave, donde podrá verificar que la información se ha subido correctamente, ver figura 38.

Si el personal de mantenimiento detecta algún otro problema durante su inspección o necesita realizar una entrada de mantenimiento adicional, puede volver a utilizar la aplicación para repetir el proceso.

De igual manera, la siguiente tripulación y el personal de mantenimiento podrán verificar el estado actual de la aeronave mediante sus respectivas aplicaciones después de este mantenimiento.



Maintenance Type: **Unscheduled**

Maintenance Location
Maintenance Hangar B

Start Date **28/07/2023**

Start Time **08:38**

Total Hours
10

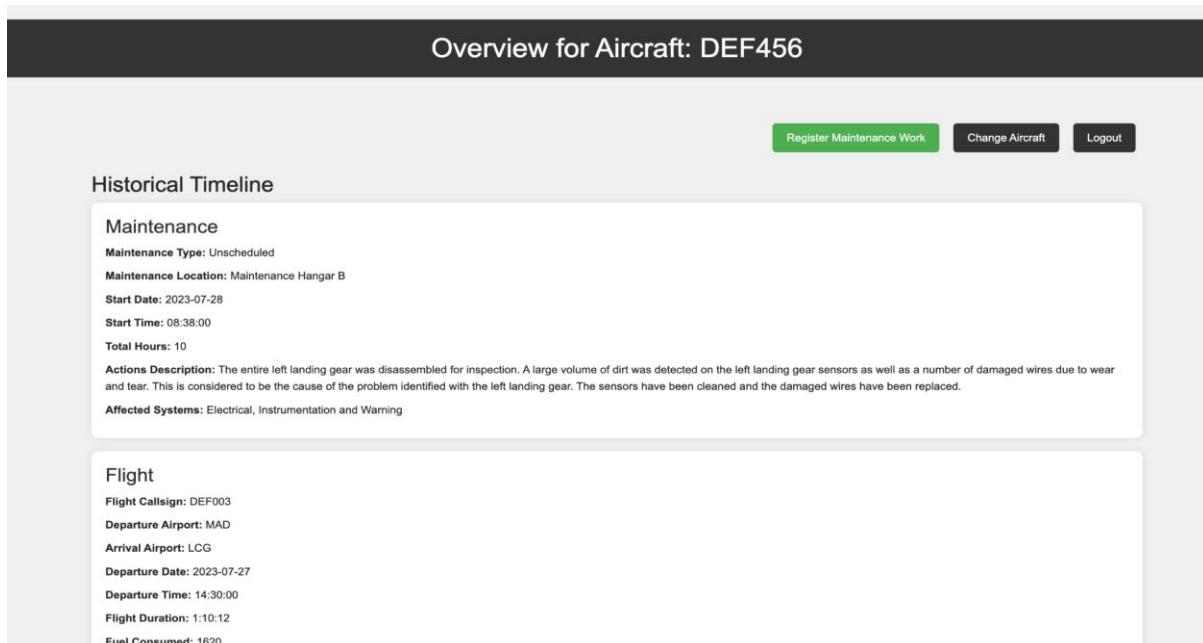
Actions Description
The entire left landing gear was disassembled for inspection. A large volume of dirt was detected on the left landing gear sensors as well as a number of damaged wires due to wear and tear. This is co

Affected Systems:

- Avionics
- Flight Control
- Engine and Powerplant
- Structural and Airframe
- Hydraulic and Pneumatic
- Electrical
- Environmental Control
- Instrumentation and Warning
- Cabin
- Safety and Emergency

Submit

Figura 37. Formulario actividad de mantenimiento aplicación personal de mantenimiento



Overview for Aircraft: DEF456

Register Maintenance Work **Change Aircraft** **Logout**

Historical Timeline

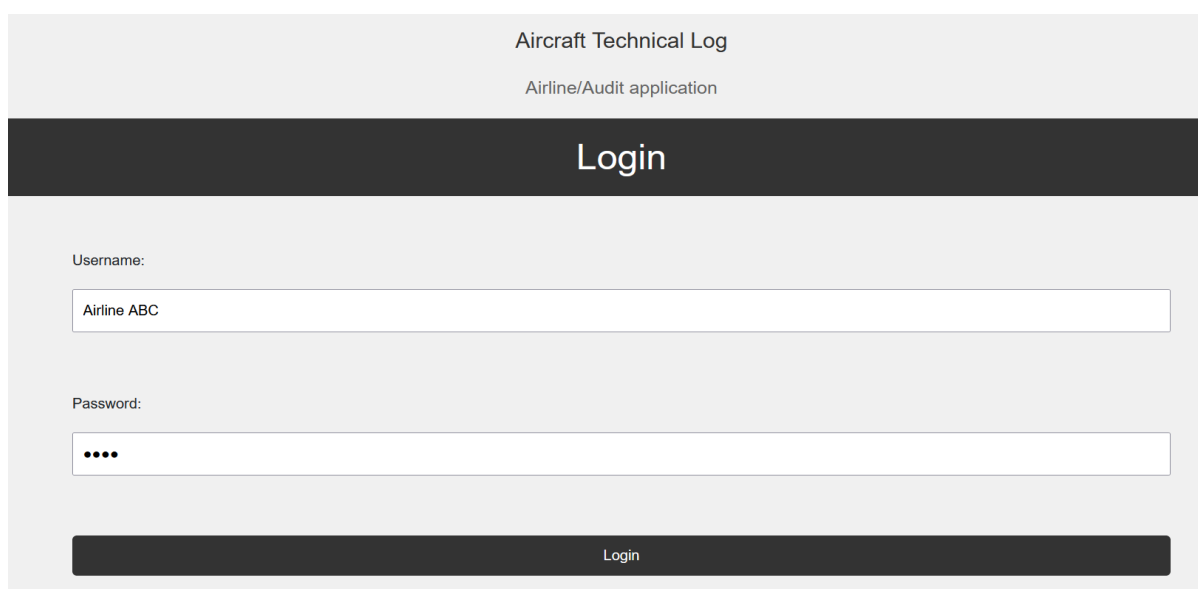
Maintenance
Maintenance Type: **Unscheduled**
Maintenance Location: **Maintenance Hangar B**
Start Date: **2023-07-28**
Start Time: **08:38:00**
Total Hours: **10**
Actions Description: **The entire left landing gear was disassembled for inspection. A large volume of dirt was detected on the left landing gear sensors as well as a number of damaged wires due to wear and tear. This is considered to be the cause of the problem identified with the left landing gear. The sensors have been cleaned and the damaged wires have been replaced.**
Affected Systems: **Electrical, Instrumentation and Warning**

Flight
Flight Callsign: **DEF003**
Departure Airport: **MAD**
Arrival Airport: **LCG**
Departure Date: **2023-07-27**
Departure Time: **14:30:00**
Flight Duration: **1:10:12**
Fuel Consumed: **1620**

Figura 38. Historial del A320 con la nueva actividad de mantenimiento aplicación personal de mantenimiento

5.3.3 Aerolíneas y Organismos Supervisores

Para finalizar con la demostración ahora se verá la aplicación destinada a las aerolíneas y/o organismos supervisores. Se seguirá utilizando el mismo escenario ficticio para un vuelo de Madrid-A Coruña el 27 de julio de 2023 y las acciones de mantenimiento posteriores. Ahora, se examinará el caso desde la perspectiva de un representante de la aerolínea o un organismo supervisor que utiliza la aplicación para revisar la información técnica y de mantenimiento de la aeronave utilizada en el vuelo. A través de esta aplicación, las aerolíneas y los organismos supervisores pueden revisar el estado técnico de la aeronave después de cada vuelo, revisar las entradas de mantenimiento, y tener una visión general de la actividad de la aeronave. Al igual que con las otras aplicaciones, antes de acceder a la aplicación, deben autenticarse y seleccionar la aeronave que desean visualizar o con la que desean trabajar. Ver figuras 39 y 40.



Aircraft Technical Log
Airline/Audit application

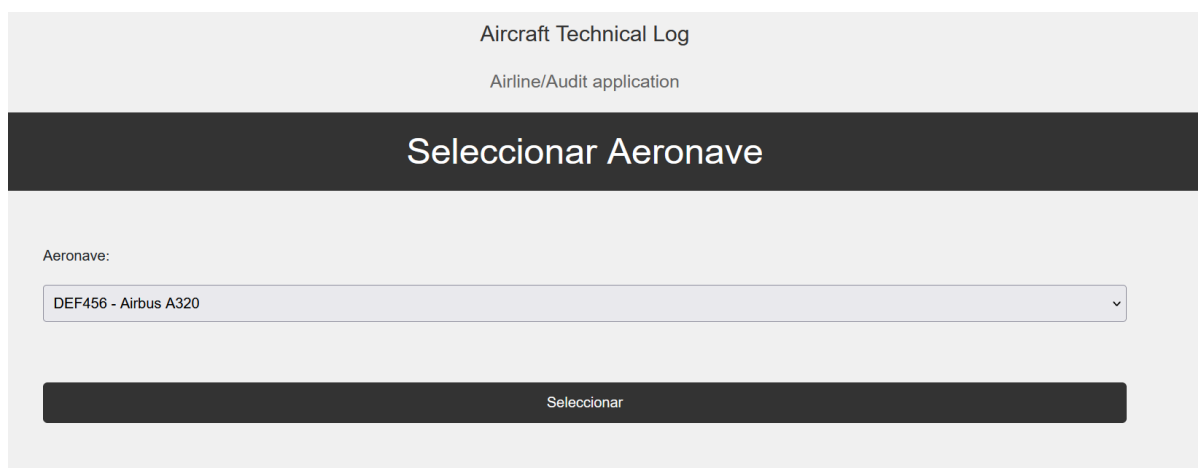
Login

Username:
Airline ABC

Password:
.....

Login

Figura 39. Página de login aplicación aerolíneas/organismo supervisor



Aircraft Technical Log
Airline/Audit application

Seleccionar Aeronave

Aeronave:
DEF456 - Airbus A320

Seleccionar

Figura 40. Página de selección de aeronave aplicación aerolíneas/organismo supervisor

Al acceder a la página del historial de la aeronave A320, se presentan de manera similar a las otras dos aplicaciones, las diversas actividades de vuelos y mantenimientos de dicha aeronave, ordenadas cronológicamente. En este caso, lo primero que se muestra es la actividad de mantenimiento realizada al tren de aterrizaje, que fue introducida en la sección anterior.

La diferencia principal con las aplicaciones de la tripulación de cabina y del personal de mantenimiento es que ahora se ha incorporado una barra de filtros, que permite al usuario modificar los datos visualizados según diversas combinaciones. Esta funcionalidad brinda mayor flexibilidad y permite al usuario obtener información más específica y relevante según sus necesidades. Además, el botón verde que anteriormente permitía registrar un nuevo vuelo o una nueva actividad de mantenimiento, ahora ofrece la opción de descargar los datos visualizados. Esta característica permite que los datos puedan ser utilizados posteriormente en otras aplicaciones o para realizar análisis más detallados. Todo esto se puede ver en la figura 41.

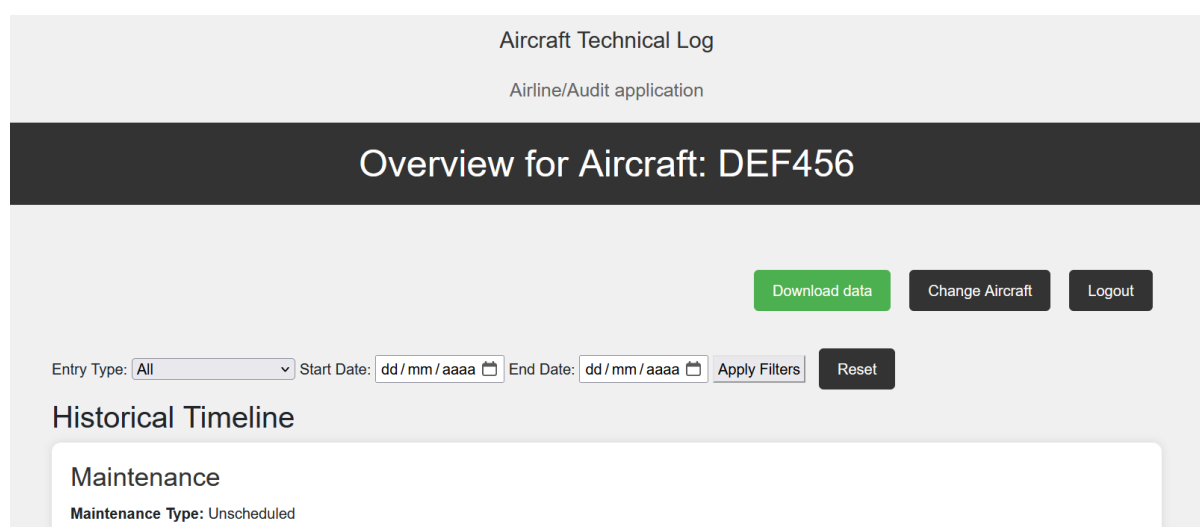
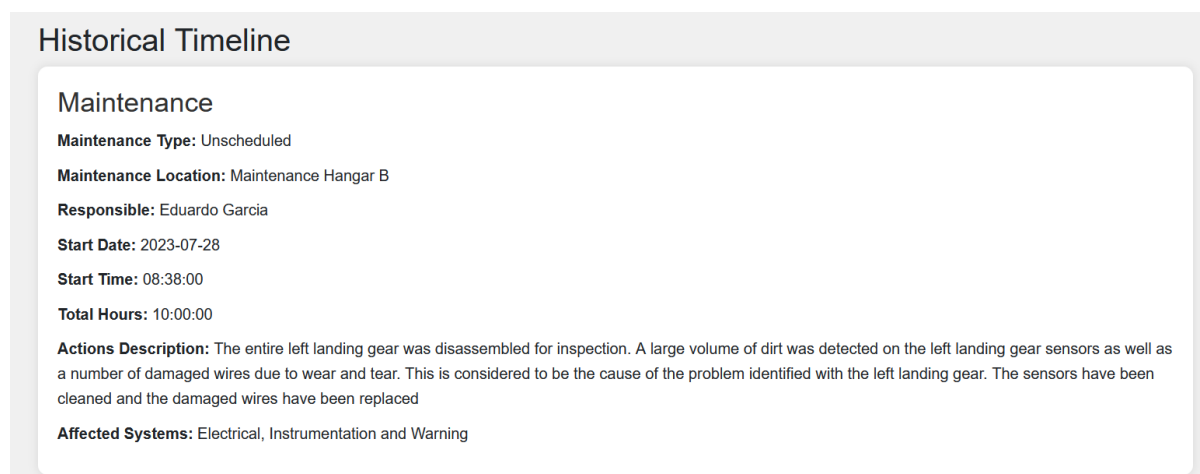


Figura 41. Historial aeronave A320 aplicación aerolíneas/organismo supervisor

Una de las diferencias principales en la información mostrada en esta aplicación, en comparación con las otras, es que aquí se incluyen los nombres del piloto al mando de las operaciones de vuelo, así como el nombre del responsable de las actividades de mantenimiento. Estos datos, que habían sido omitidos en las primeras aplicaciones por motivos de privacidad, ahora son visibles para los usuarios en esta versión.

El objetivo de mostrar esta información es proporcionar la mayor transparencia y trazabilidad posible en todas las operaciones y actividades relacionadas con la aeronave. Al mostrar los nombres de los pilotos y los responsables de mantenimiento, se brinda a los usuarios una visión más completa de cada evento registrado en el historial de la aeronave proporcionando un mayor nivel de detalle y trazabilidad en la gestión de la aeronave, lo que contribuye a mejorar la seguridad, el mantenimiento y la eficiencia en las operaciones aéreas.

En las figuras 42 y 43 se pueden apreciar cómo han quedado correctamente recogidos los nombres del piloto al mando y del responsable de mantenimiento para las actividades introducidas en las sesiones anteriores.



Historical Timeline

Maintenance

Maintenance Type: Unscheduled

Maintenance Location: Maintenance Hangar B

Responsible: Eduardo Garcia

Start Date: 2023-07-28

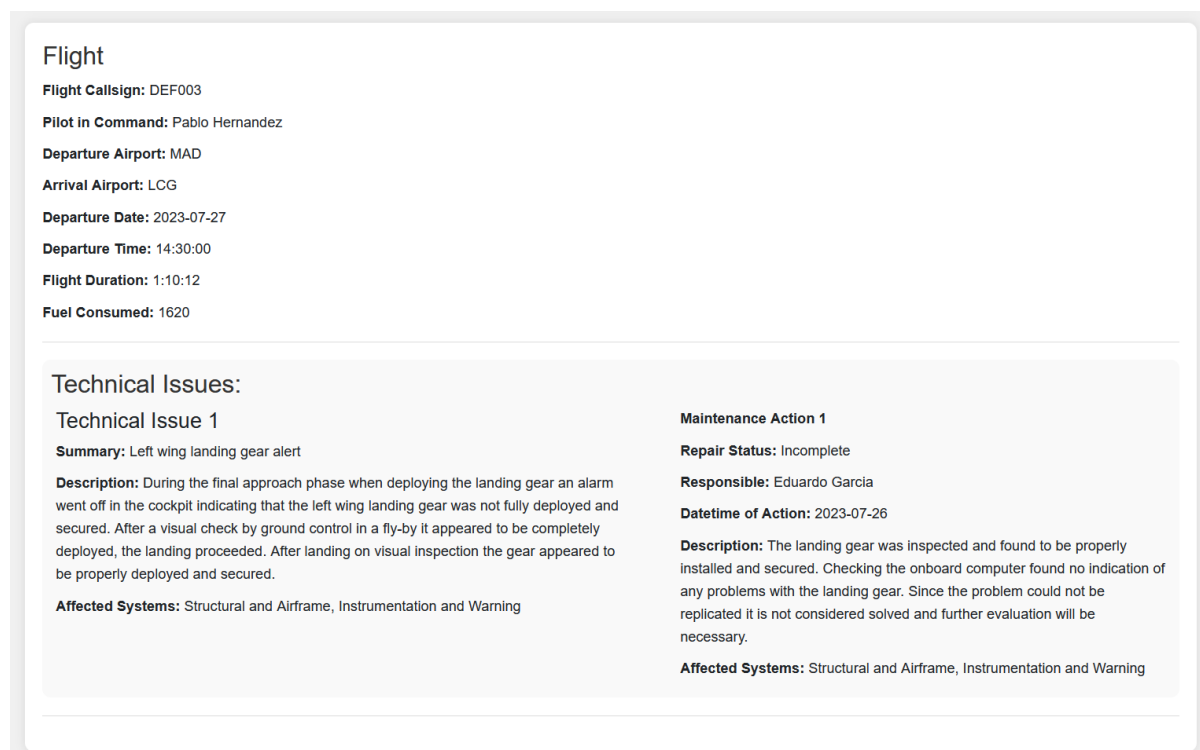
Start Time: 08:38:00

Total Hours: 10:00:00

Actions Description: The entire left landing gear was disassembled for inspection. A large volume of dirt was detected on the left landing gear sensors as well as a number of damaged wires due to wear and tear. This is considered to be the cause of the problem identified with the left landing gear. The sensors have been cleaned and the damaged wires have been replaced

Affected Systems: Electrical, Instrumentation and Warning

Figura 42. Actividad de mantenimiento aeronave A320 aplicación aerolíneas/organismo supervisor



Flight

Flight Callsign: DEF003

Pilot in Command: Pablo Hernandez

Departure Airport: MAD

Arrival Airport: LCG

Departure Date: 2023-07-27

Departure Time: 14:30:00

Flight Duration: 1:10:12

Fuel Consumed: 1620

Technical Issues:

Technical Issue 1

Summary: Left wing landing gear alert

Description: During the final approach phase when deploying the landing gear an alarm went off in the cockpit indicating that the left wing landing gear was not fully deployed and secured. After a visual check by ground control in a fly-by it appeared to be completely deployed, the landing proceeded. After landing on visual inspection the gear appeared to be properly deployed and secured.

Affected Systems: Structural and Airframe, Instrumentation and Warning

Maintenance Action 1

Repair Status: Incomplete

Responsible: Eduardo Garcia

Datetime of Action: 2023-07-26

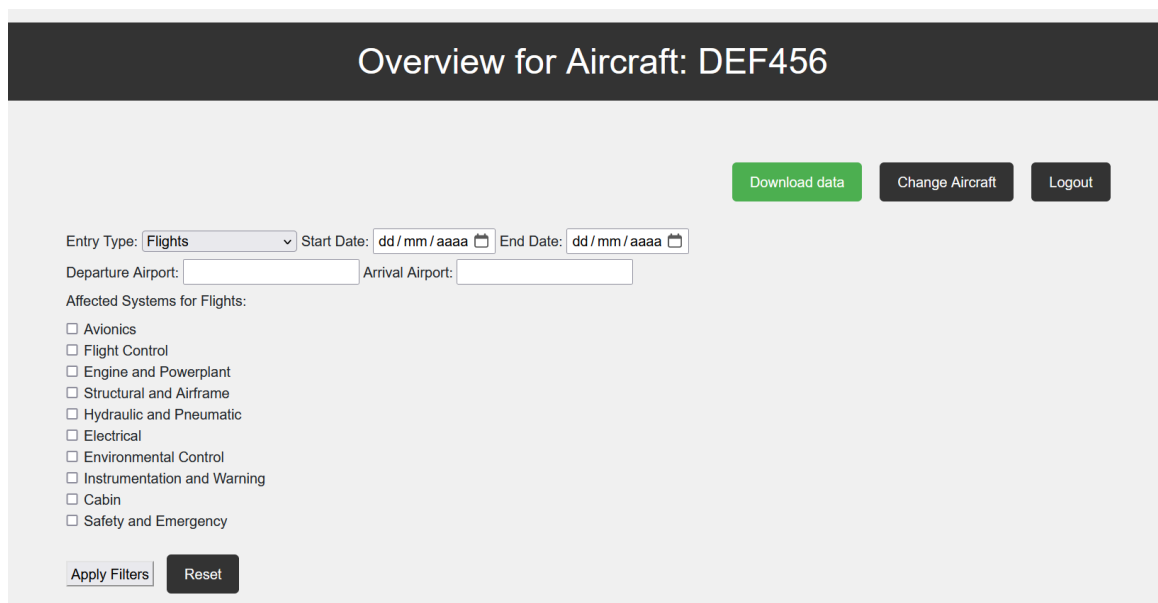
Description: The landing gear was inspected and found to be properly installed and secured. Checking the onboard computer found no indication of any problems with the landing gear. Since the problem could not be replicated it is not considered solved and further evaluation will be necessary.

Affected Systems: Structural and Airframe, Instrumentation and Warning

Figura 43. Vuelo MAD-LCG aeronave A320 aplicación aerolíneas/organismo supervisor

La figura 41 muestra la barra principal de filtros de la aplicación. En esta barra, el usuario tiene la opción de elegir entre ver todos los tipos de entradas o solo aquellos relacionados con vuelos o actividades de mantenimiento (que no incluyen los relacionados con defectos técnicos, ya que estos están asociados a un vuelo). Además, el usuario puede filtrar los registros por un rango de fechas.

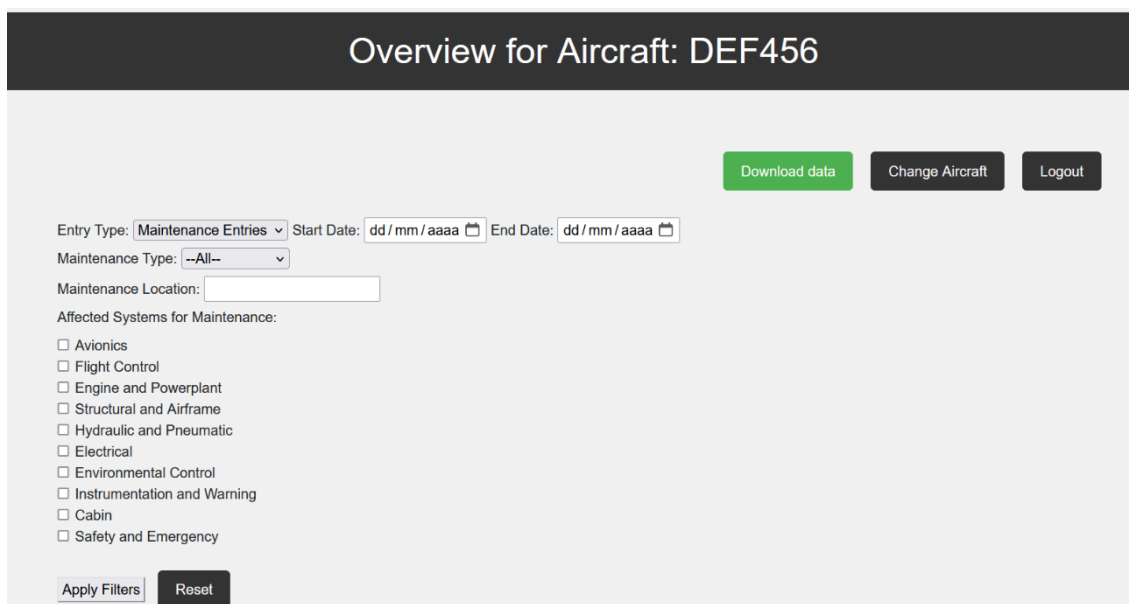
Dependiendo del tipo de entrada seleccionada, se desplegarán filtros adicionales. Si se elige la opción "Flights" (Vuelos), aparecerán tres filtros adicionales. El usuario puede especificar el aeropuerto de salida y el de llegada a través de su código, así como seleccionar los sistemas afectados, ver figura 44. Esto permitirá que solo se muestren los vuelos que tienen defectos técnicos reportados relacionados con el sistema afectado.



The screenshot shows a web interface titled "Overview for Aircraft: DEF456". At the top right, there are three buttons: "Download data" (green), "Change Aircraft", and "Logout". Below these, there are input fields for "Entry Type" (set to "Flights"), "Start Date" (dd/mm/yyyy), and "End Date" (dd/mm/yyyy). There are also input fields for "Departure Airport" and "Arrival Airport". A section titled "Affected Systems for Flights:" contains a list of checkboxes for various systems: Avionics, Flight Control, Engine and Powerplant, Structural and Airframe, Hydraulic and Pneumatic, Electrical, Environmental Control, Instrumentation and Warning, Cabin, and Safety and Emergency. At the bottom left, there are "Apply Filters" and "Reset" buttons.

Figura 44. Filtros adicionales para "Flights" aplicación aerolíneas/organismo supervisor

Por otro lado, si el usuario selecciona la opción de "Maintenance Entries" (Actividades de Mantenimiento), también aparecerán tres filtros adicionales que le permiten especificar el tipo de mantenimiento, la ubicación del mantenimiento y los sistemas afectados en el mantenimiento. En la figura 45 se puede apreciar esta barra de filtros.



The screenshot shows the same web interface as Figure 44, but with the "Entry Type" set to "Maintenance Entries". The "Maintenance Type" dropdown is set to "--All--". There is an input field for "Maintenance Location". The "Affected Systems for Maintenance:" section contains the same list of checkboxes as in Figure 44. The "Apply Filters" and "Reset" buttons are still present at the bottom left.

Figura 45. Filtros adicionales para "Maintenance Entries" aplicación aerolíneas/organismo supervisor

Estos filtros proporcionan una funcionalidad para que el usuario pueda explorar y analizar de manera más precisa y detallada el historial de la aeronave. La aplicación permite una experiencia personalizada al permitir al usuario filtrar y visualizar la información relevante según sus necesidades específicas, lo que contribuye a una mejor comprensión y gestión de la aeronave y sus operaciones.

Finalmente, el botón previamente mencionado "Download data" ofrece a los usuarios la posibilidad de descargar la información de la aeronave seleccionada en formato JSON. El formato JSON (JavaScript Object Notation) es una estructura de datos ligera y de fácil lectura que se utiliza comúnmente para el intercambio de información entre aplicaciones y sistemas.

El formato JSON permite una representación estructurada de los datos, organizados en pares clave-valor. Esta estructura facilita la comprensión y el análisis en profundidad de los datos, ya que la información se presenta de manera clara y concisa. Al descargar la información en formato JSON, los usuarios pueden llevar a cabo análisis detallados y realizar comparaciones más exhaustivas. Además, el formato JSON es altamente compatible y ampliamente utilizado en aplicaciones y sistemas de distintos tipos. Esto significa que los datos descargados pueden ser fácilmente compartidos e interconectados con otras plataformas, lo que fomenta una integración fluida con otros sistemas y aplicaciones relacionados.

Gracias a la opción de descargar los datos en formato JSON, los usuarios tienen la flexibilidad de aprovechar al máximo la información recopilada en la aplicación ATL. Pueden realizar análisis avanzados, compartir datos con otros equipos y sistemas, e incluso utilizarlos en otras aplicaciones para mejorar la toma de decisiones y optimizar la gestión de la aeronave. En la figura 46 se puede ver los datos hasta ahora visualizados en la aplicación en formato JSON.

```
{
  "entry": {
    "_type": "MaintenanceEntry",
    "maintenance_type": "Unscheduled",
    "maintenance_location": "Maintenance Hangar B",
    "maintenanceresponsible": "Eduardo Garcia",
    "start_date": "2023-07-28",
    "start_time": "08:38:00",
    "total_hours": "10:00:00",
    "actions_description": "The entire left landing gear was disassembled for ins",
    "affected_systems": ["Electrical", "Instrumentation and Warning"]}
},
{
  "entry": {
    "_type": "Flight",
    "callsign": "DEF003",
    "pilot_in_command": "Pablo Hernandez",
    "departure_airport": "MAD",
    "arrival_airport": "LCG",
    "departure_date": "2023-07-27",
    "departure_time": "14:30:00",
    "flight_duration": "1:10:12",
    "fuel_consumed": 1620,
    "technical_issues": [
      {
        "_type": "TechnicalIssue",
        "summary": "Left wing landing gear alert",
        "description": "During the final approach phase when deploying the landing gear an alarm went off in the cockpit indicating that the left wing landing"
      }
    ],
    "maintenance_actions": {}
  }
},
{
  "entry": {
    "_type": "Flight",
    "callsign": "DEF001",
    "pilot_in_command": "Ignacio Lopez",
    "departure_airport": "MAD",
    "arrival_airport": "BCN",
    "departure_date": "2023-07-25",
    "departure_time": "11:34:56",
    "flight_duration": "1:18:00",
    "fuel_consumed": 1702,
    "technical_issues": [
      {
        "_type": "TechnicalIssue",
        "summary": "Wing Issue",
        "description": "During the flight, the crew noticed an unusual vibration in the wings. The vibration was more noticeable during turbulence. On lan",
        "affected_systems": ["Structural and Airframe"]}
    ],
    "maintenance_actions": {
      "b8629734-4dcc-463e-8007-4b653c2eb70": [
        {
          "_type": "MaintenanceAction",
          "repair_status": "complete",
          "maintenanceresponsible": "Eduardo Garcia"
        }
      ]
    }
  }
},
{
  "entry": {
    "_type": "Flight",
    "callsign": "DEF002",
    "pilot_in_command": "Lucia Cortes",
    "departure_airport": "LHR",
    "arrival_airport": "CDG",
    "departure_date": "2023-07-20",
    "departure_time": "09:05:12",
    "flight_duration": "1:06:00",
    "fuel_consumed": 1395,
    "technical_issues": [],
    "maintenance_actions": {}
  }
},
{
  "entry": {
    "_type": "MaintenanceEntry",
    "maintenance_type": "Scheduled",
    "maintenance_location": "Maintenance Hangar B",
    "maintenanceresponsible": "Eduardo Garcia",
    "start_date": "2023-07-17",
    "start_time": "12:31:00",
    "total_hours": "6:00:00",
    "actions_description": "Updated avionics software to the latest version",
    "affected_systems": ["Avionics"]}
}
```

Figura 46. Ejemplo datos JSON aeronave A320 aplicación aerolíneas/organismo supervisor

5.4 Desarrollos Futuros y Expansión de la Aplicación

La aplicación ATL basada en blockchain se ha desarrollado con éxito demostrando su potencial como solución innovadora para mejorar la gestión del mantenimiento y registro técnico de las aeronaves.

Sin embargo, esto es solo un primer paso y diversas acciones se podrían tomar desde esta prueba de concepto para el crecimiento y la optimización de la aplicación hasta conseguir un estado operacional. En esta sección se pretende detallar una serie de posibles mejoras futuras y expansiones que se pueden implementar en iteraciones futuras de la aplicación ATL.

1. **Robustez y Seguridad en la Implementación de la Blockchain:** El primer paso sería el de asegurar que la implementación de la red es robusta y segura. Esto significa adherirse a las mejores prácticas y estándares establecidos en el mundo de blockchain. Especial atención se debería dar a la resistencia frente a ataques maliciosos y en garantizar la integridad de los datos almacenados en la cadena. Para ello entre otras acciones se debería implementar el uso de protocolos de consenso como el PoW o el PoS.
2. **Seguridad y Autenticación:** La seguridad debe ser una consideración primordial. Se recomienda la implementación de un sistema de autenticación robusto, como el uso de criptografía de clave pública y privada. Este sistema permitiría a los usuarios firmar transacciones y verificar su identidad de forma segura. Además, es necesario aplicar medidas de protección más robustas para prevenir el acceso no autorizado a la aplicación como el uso del doble factor de autenticación, garantizando que sólo los usuarios autorizados puedan acceder a la aplicación.
3. **Registro Inmutable y Gestión de Permisos:** La naturaleza inmutable de la blockchain es vital para la integridad de los datos. Debe asegurarse que, una vez los registros técnicos se añaden a la cadena, no se puedan alterar o eliminar sin dejar rastro. Sin embargo, puede ser importante considerar la necesidad de editar ciertos datos en circunstancias especiales. Para ello, se podría implementar un sistema de gestión de permisos, donde sólo los usuarios con roles específicos y autorizados puedan realizar cambios, dejando siempre un registro claro de las modificaciones realizadas.
4. **Interfaz de Usuario Intuitiva y Funcional:** La interfaz actual es básica pero funcional. Para mejorar la usabilidad de la aplicación, se recomienda desarrollar una interfaz de usuario intuitiva y amigable. Esta interfaz debe ser fácil de navegar, permitiendo a los usuarios crear, ver y gestionar vuelos, entradas de mantenimiento, problemas técnicos y acciones de mantenimiento de forma sencilla. Además, se pueden incorporar en la aplicación de tripulación de cabina y de personal de mantenimiento filtros y opciones de búsqueda para facilitar la recuperación de información específica.
5. **Notificaciones y Alertas:** La aplicación podría integrar un sistema de notificaciones y alertas para informar a los usuarios sobre eventos importantes a tener en cuenta. Por ejemplo, se podrían enviar notificaciones sobre próximas fechas de mantenimiento, problemas técnicos críticos o cambios en el estado de la aeronave. Esto permitiría a los usuarios estar mejor informados y tomar medidas rápidas y oportunas para garantizar la seguridad y el cumplimiento de las regulaciones.
6. **Registro y Seguimiento Detallado de Auditoría:** Para aumentar la transparencia y la responsabilidad, es importante implementar un registro detallado de auditoría que registre todas las acciones realizadas por los usuarios en la plataforma. Esto incluiría cambios en

registros, modificaciones de datos técnicos, autorizaciones y cualquier otra operación relevante. El registro de auditoría también sería útil para cumplir con los requisitos regulatorios y normativos.

7. **Integración con Sistemas de Terceros:** Con el objetivo de mejorar la utilidad de la aplicación ATL, sería beneficioso explorar la integración con otros sistemas utilizados en la industria de la aviación actualmente. Esto podría incluir la sincronización con sistemas de gestión de flotas, programas de mantenimiento predictivo y bases de datos de entidades reguladoras para agilizar los procesos y mejorar la precisión de la información.
8. **Pruebas Exhaustivas y Optimizaciones de Rendimiento:** A medida que la aplicación crece y aumenta el número de usuarios y registros, es vital realizar pruebas exhaustivas y optimizaciones de rendimiento. Esto garantizaría que la plataforma pueda manejar una carga de trabajo más pesada sin comprometer la velocidad y la eficiencia en el procesamiento de datos.
9. **Implementación de Smart Contracts para la Automatización:** Los smart contracts podrían integrarse en la aplicación ATL. Esto podría revolucionar la gestión del mantenimiento de las aeronaves. Por ejemplo, se podrían crear Smart Contracts para automatizar las notificaciones de mantenimiento programados, enviando automáticamente notificaciones a los responsables de mantenimiento cuando se acerque la fecha de mantenimiento programado para una aeronave en particular, o también para la validación de registros tanto de vuelos como de acciones de mantenimiento, verificando automáticamente la precisión de los registros y confirmando si los datos técnicos cumplen con los estándares establecidos.
10. **Aplicación de Tecnologías Emergentes:** El uso de tecnologías como La IA o el aprendizaje automático pueden aportar un valor significativo a la aplicación ATL. Estas permitirán realizar análisis avanzados y mejoras en la toma de decisiones. Por ejemplo, el uso de la IA permitiría realizar un mantenimiento predictivo en base a los datos del ATL y otra fuentes de datos o la detección de anomalías pudiendo prevenir incidentes y mejorar la seguridad.

6. Conclusiones

Este trabajo de investigación ha indagado profundamente en la tecnología blockchain, con énfasis en sus posibles aplicaciones en la industria aeronáutica. Se han explorado tanto las implicaciones generales de su uso en este sector, como su implementación en un caso específico: el Aircraft Technical Log (ATL).

El estudio ha proporcionado una visión detallada de los fundamentos y operaciones de la blockchain, con la intención de clarificar conceptos básicos y destacar tanto sus ventajas como limitaciones de uso. Además, se han identificado un amplio espectro de posibles usos para la blockchain en la industria aeronáutica, desde su potencial para mejorar la eficiencia de las operaciones de mantenimiento, su capacidad para asegurar la trazabilidad y autenticidad de las piezas de las aeronaves hasta su uso en los programas de fidelización de clientes.

La tecnología blockchain, en su esencia, ofrece seguridad, descentralización y transparencia, lo que tiene el potencial de revolucionar la forma en que se realizan transacciones y se almacenan datos en muchas industrias. En la industria aeronáutica, donde la seguridad, precisión y trazabilidad son elementos críticos, esta tecnología podría aportar mejoras significativas. Aunque su adopción plantea ciertos desafíos, como la necesidad de un marco regulador claro y el potencial de resistencia al cambio en una industria altamente regulada, la blockchain puede ofrecer soluciones innovadoras a problemas existentes.

En la actualidad el ATL juega un papel crucial en las operaciones diarias de la industria aeronáutica. Este registro contiene información esencial sobre el estado de las aeronaves y sus componentes, siendo un elemento clave para garantizar la seguridad operacional y la eficiencia de las operaciones. En su gestión actual, sin embargo, se enfrentan varios desafíos. Estos problemas incluyen la pérdida o alteración de datos críticos, el acceso no autorizado a la información y la gestión ineficiente de los datos. Todos estos problemas pueden tener consecuencias graves para la seguridad y la eficiencia de las operaciones aéreas.

La tecnología blockchain ofrece una solución potencial a estos desafíos. Al asegurar la inmutabilidad y la trazabilidad de los datos, la blockchain puede evitar la pérdida o alteración de los datos. Además, la descentralización de la blockchain puede prevenir el acceso no autorizado a la información, garantizando que sólo las partes autorizadas puedan acceder a los datos del ATL.

En el estudio se han establecido para el diseño y desarrollo de un ATL basado en blockchain, una serie de consideraciones a tener en cuenta. Estas incluyen entre otras la identificación de los usuarios que tendrán acceso al registro, la integración de la blockchain con otros sistemas de la industria aeronáutica, la escalabilidad de la solución y la conformidad con las normativas existentes. Estas consideraciones son esenciales para asegurar que un ATL basado en blockchain sea viable, seguro y eficiente en su implementación.

Además, a lo largo del estudio, se desarrolló una prueba de concepto del ATL incorporando tecnología blockchain con el objetivo de demostrar cómo esta tecnología puede utilizarse para mejorar la gestión

de los registros técnicos de las aeronaves, garantizando la seguridad, la trazabilidad y la eficiencia de los datos.

Las funcionalidades desarrolladas e implementadas en las diferentes aplicaciones que componen la prueba de concepto ATL blockchain, permiten:

- A los miembros de la tripulación de cabina por un lado revisar el historial completo de la aeronave previo a una operación pudiendo garantizar la seguridad de la misma. Asimismo, la tripulación puede registrar todos los datos de su operación y cualquier problema técnico acaecido.
- Al personal de mantenimiento se les proporciona una aplicación con la que realizar el seguimiento de la información de mantenimiento y facilitar el registro de todas las actividades de mantenimiento llevadas a cabo en una aeronave.
- A las aerolíneas y los organismos supervisores se les proporciona una aplicación con la que poder revisar y supervisar de manera eficiente el cumplimiento de las normativas y regulaciones en cuanto a mantenimiento y operatividad de las aeronaves.

La investigación realizada en este estudio sugiere que la implementación del ATL basado en blockchain es viable en la práctica. Sin embargo, se recomienda seguir ciertos pasos para asegurar una futura implementación exitosa. Se recomienda lo siguiente:

1. **Evolución y ampliación del diseño actual:** Desarrollar una arquitectura escalable que pueda manejar un crecimiento de datos exponencial. Incluir redundancias para manejar picos de demanda y asegurar una respuesta rápida.
2. **Estrategias de optimización y eficiencia:** Desarrollar métodos de optimización para gestionar un gran volumen de datos de forma eficaz. Esto puede implicar la utilización de algoritmos de aprendizaje automático para el análisis y la interpretación de los datos.
3. **Incorporación de tecnologías emergentes:** Considerar el uso de contratos inteligentes para facilitar las transacciones y operaciones, así como la aplicación de big data e inteligencia artificial para el análisis de datos y toma de decisiones.
4. **Implementación de medidas de seguridad avanzadas:** Garantizar la seguridad de los datos con la implementación de técnicas criptográficas avanzadas, medidas de autenticación de dos factores y auditorías de seguridad regulares.
5. **Pruebas y validación extensivas:** Llevar a cabo pruebas rigurosas y frecuentes, y utilizar los comentarios de los usuarios finales para mejorar y perfeccionar el sistema.
6. **Elaboración de un marco regulatorio robusto:** Colaborar con las autoridades regulatorias para desarrollar un marco legal que permita la adopción segura de la tecnología blockchain en la industria aeronáutica.
7. **Implicar a todos los actores relevantes:** Crear un consorcio de todas las partes interesadas, que incluya a fabricantes de aeronaves, aerolíneas, organismos de control, personal de

mantenimiento y tripulación de cabina. Este consorcio podría tomar decisiones sobre el desarrollo y la implementación de la blockchain.

8. **Integración y migración cuidadosas:** Diseñar un plan detallado para la integración del sistema blockchain con los sistemas existentes, y ofrecer formación a los empleados para su uso efectivo.
9. **Sensibilización y formación:** Organizar talleres y seminarios para educar a todos los interesados sobre los beneficios y los posibles desafíos de la tecnología blockchain.

En resumen, este estudio se plantea como un catalizador en la investigación de tecnologías de digitalización emergentes en el contexto de la industria aeronáutica. La incursión de la tecnología blockchain en el escenario aeronáutico se presenta como impulsora de transformación radical para el futuro. Las posibilidades de investigación se multiplican: desde la exploración de nuevas aplicaciones de blockchain en la aviación, hasta el establecimiento de marcos regulatorios adaptados a su integración en el sector, pasando por exhaustivos análisis de viabilidad para su implementación en distintas facetas de la industria aeronáutica.

En el trabajo realizado, se ha buscado destacar los aspectos principales que permitan impulsar la exploración de innovaciones basadas en blockchain, que albergan un enorme potencial para optimizar la eficiencia y mejorar la seguridad operativa en este sector crítico. A través de una metodología que combina aspectos teóricos y prácticos, se espera que este trabajo enriquezca el cuerpo de literatura existente sobre la implementación de la blockchain en diversos sectores, y así contribuir de manera valiosa al debate sobre la digitalización y la innovación en la industria aeronáutica.

7. Referencias

(AERON, 2020) AERON Blockchain for Aviation Safety (White paper); 2020

(Ahmad et al., 2021) Ahmad, R. W., Salah, K., Jayaraman, R., Hasan, H. R., Yaqoob, I., & Omar, M. (2021). The role of blockchain technology in aviation industry. *IEEE Aerospace and Electronic Systems Magazine*, 36(3), 4-1

(Ali et al., 2021) Ali, O., Jaradat, A., Kulakli, A., & Abuhalmeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *Ieee Access*, 9, 12730-12749.

(Alladi et al., 2020) Alladi, T., Chamola, V., Sahu, N., & Guizani, M. (2020). Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications*, 23, 100249.

(Allouch et al., 2021) Allouch, A., Cheikhrouhou, O., Koubâa, A., Toumi, K., Khalgui, M., & Nguyen Gia, T. (2021). Utm-chain: blockchain-based secure unmanned traffic management for internet of drones. *Sensors*, 21(9), 3049.

(Almeshal & Alhogail, 2021) Almeshal, T. A., & Alhogail, A. A. (2021). Blockchain for businesses: a scoping review of suitability evaluations frameworks. *IEEE Access*, 9, 155425-155442.

(Antonopoulos, 2014) Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc."

(Atlam et al., 2020) Atlam, H. F., Azad, M. A., Alzahrani, A. G., & Wills, G. (2020). A Review of Blockchain in Internet of Things and AI. *Big Data and Cognitive Computing*, 4(4), 28.

(Belchior et al., 2021) Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR)*, 54(8), 1-41

(Bitcoin, 2021) Bitcoin average transaction fee; URL: <https://bitinfocharts.com/comparison/bitcoin-transactionfees.html>; 2021

(Bonneau et al., 2015) Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. 2015 IEEE Symposium on Security and Privacy.

(Bui et al., 2021) Bui, V. C., Wen, S., Yu, J., Xia, X., Haghghi, M. S., & Xiang, Y. (2021, December). Evaluating upgradable smart contract. In *2021 IEEE International Conference on Blockchain (Blockchain)* (pp. 252-256). IEEE.

(Buterin, 2014) Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." *white paper* 3, no. 37 (2014): 2-1.

(Casino et al., 2019) Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, 36, 55-81.

(CB, 2023) Coding Bootcamps - How Digital Signature Works In Blockchain; URL: <https://www.coding-bootcamps.com/blog/how-digital-signature-works-in-blockchain.html>; 2023

(Chauhan et al., 2018) Chauhan, A., Malviya, O. P., Verma, M., & Mor, T. S. (2018, July). Blockchain and scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 122-128). IEEE

(Chowdhury et al., 2018) Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarda, P. (2018, August). Blockchain versus database: A critical analysis. In *2018 17th IEEE International conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)* (pp. 1348-1353). IEEE.

(Christidis & Devetsikiotis, 2016) Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, 4, 2292-2303

(Clementi et al., 2019) Clementi, M. D., Larrieu, N., Lochin, E., Kaafar, M. A., & Asghar, H. (2019, September). When air traffic management meets blockchain technology: a blockchain-based concept for securing the sharing of flight data. In *2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)* (pp. 1-10). Ieee.

(CNET, 2022) CNET; URL: <https://www.cnet.com/culture/airline-most-likely-to-lose-your-luggage/>; 2022

(Cointelegraph, 2022) Cointelegraph; The 10 largest crypto hacks and exploits in 2022 saw \$2.1B stolen; URL: <https://cointelegraph.com/news/the-10-largest-crypto-hacks-and-exploits-in-2022-saw-2-1b-stolen>; 2022

(Croman et al., 2016) Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Wattenhofer, R. (2016, February). On Scaling Decentralized Blockchains: (A Position Paper). In *International conference on financial cryptography and data security* (pp. 106-125). Berlin, Heidelberg: Springer Berlin Heidelberg.

(DBJ, 2016) Dallas Business Journal; URL: <https://www.bizjournals.com/dallas/news/2016/08/11/southwest-airlinescomputer-outage-costs-could.html>; 2016

(Diffie & Hellman, 1976) Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6), 644-654

(DoT, 2021) Blockchain and Unmanned Aircraft Systems (UAS) - U.S. Department of Transportation; URL: <https://www.volpe.dot.gov/our-work/blockchain-and-unmanned-aircraft-systems-uas>; 2021

(DS.aero, 2019) Datascience.aero; URL: <https://datascience.aero/blockchain-enhance-aircraft-maintenance/>; 2019

(Dutta et al., 2020) Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation research part e: Logistics and transportation review*, 142, 102067

(Efthymiou et al., 2022) Efthymiou, M., McCarthy, K., Markou, C., & O'Connell, J. F. (2022). An exploratory research on blockchain in aviation: the case of maintenance, repair and overhaul (MRO) organizations. *Sustainability*, 14(5), 2643.

(Fabiano, 2017) Fabiano, N. (2017, June). Internet of Things and blockchain: Legal issues and privacy. The challenge for a privacy standard. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 727-734). IEEE

(Fang et al., 2020) Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *EURASIP Journal on Wireless Communications and Networking*, 2020(1), 1-15.

(Finck, 2018) Finck, M. (2018). Blockchains and data protection in the European Union. *Eur. Data Prot. L. Rev.*, 4, 17.

(FlightChain, 2017) FlightChain - Research into the usability and practicalities of blockchain technology for the air transport industry (White paper); 2017

(GG, 2022) Geeks for Geeks - Smart contracts in Blockchain; URL: <https://www.geeksforgeeks.org/smart-contracts-in-blockchain/>; 2022

(Godfrey-Welch et al., 2018) Godfrey-Welch, D., Lagrois, R., Law, J., Anderwald, R. S., & Engels, D. W. (2018). Blockchain in payment card systems. *SMU Data Science Review*, 1(1), 3.

(Golosova & Romanovs, 2018) Golosova, J., & Romanovs, A. (2018, November). The advantages and disadvantages of the blockchain technology. In *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)* (pp. 1-6). IEEE.

(Goudarzi et al., 2018) Goudarzi, H., Martin, J. I., & Meydanli, A. (2018). Blockchain in Aviation Exploring the Fundamentals, Use Cases, and Industry Initiatives. *IATA White Paper*.

(Gupta & Sadoghi, 2021) Gupta, S., & Sadoghi, M. (2021). Blockchain transaction processing. *arXiv preprint arXiv:2107.11592*.

(Haber & Stornetta, 1991) Haber, S., & Stornetta, W. S. (1991). *How to time-stamp a digital document* (pp. 437-455). Springer Berlin Heidelberg.

(Harte et al., 2017) Harte, R., Glynn, L., Rodríguez-Molinero, A., Baker, P. M., Scharf, T., Quinlan, L. R., & ÓLaighin, G. (2017). A human-centered design methodology to enhance the usability, human

factors, and user experience of connected health systems: a three-phase methodology. *JMIR human factors*, 4(1), e5443.

(Hughes et al., 2019) Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, 49, 114-129

(IBM, 2023) IBM - Message digests and digital signatures; URL: <https://www.ibm.com/docs/en/ibm-mq/7.5?topic=concepts-message-digests>; 2023

(Ismail et al., 2022) Ismail, A., Toohey, M., Lee, Y. C., Dong, Z., & Zomaya, A. Y. (2022, August). Cost and Performance Analysis on Decentralized File Systems for Blockchain-Based Applications: State-of-the-Art Report. In *2022 IEEE International Conference on Blockchain (Blockchain)* (pp. 230-237). IEEE

(Kewell et al., 2017) Kewell, B., Adams, R., & Parry, G. (2017). Blockchain for good?. *Strategic change*, 26(5), 429-437.

(Klein & Prinz, 2018) Klein, S., & Prinz, W. (2018). A use case identification framework and use case canvas for identifying and exploring relevant blockchain opportunities.

(Kumar & Tripathi, 2020) Kumar, R., & Tripathi, R. (2020). Blockchain-based framework for data storage in peer-to-peer scheme using interplanetary file system. In *Handbook of research on blockchain technology* (pp. 35-59). Academic Press.

(Lacity & Khan, 2019) Lacity, M., & Khan, S. (2019). Exploring preliminary challenges and emerging best practices in the use of enterprise blockchains applications.

(Lacity et al., 2019) Lacity, M., Steelman, Z., & Cronan, P. (2019). Towards blockchain 3.0 interoperability: Business and technical considerations. *BC CoE*, 1, 2019.

(Lacity, 2018) Lacity, M. C. (2018). Enterprise blockchains: Eight sources of business value and the obstacles in their way. *Arkansas, US* (available at <https://walton.uark.edu/enterprise/downloads/blockchain/LacityBlockchainsExplained.pdf>).

(Lai & Luo, 2020) Lai, E., & Luo, W. (2020, January). Static analysis of integer overflow of smart contracts in ethereum. In *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy* (pp. 110-115).

(Lampson, 1981) Lampson, B. W. (1981). Chapter 11. atomic transactions. In *Distributed Systems—Architecture and Implementation: an Advanced Course* (pp. 246-265). Springer Berlin Heidelberg.

(Lashkari & Musilek, 2021) Lashkari, B., & Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. *IEEE Access*, 9, 43620-43652.

(Latorella & Prabhu, 2000) Latorella, K. A., & Prabhu, P. V. (2000). A review of human error in aviation maintenance and inspection. *International Journal of industrial ergonomics*, 26(2), 133-161.

(Li et al., 2021) Li, X., Lai, P. L., Yang, C. C., & Yuen, K. F. (2021). Determinants of blockchain adoption in the aviation industry: Empirical evidence from Korea. *Journal of Air Transport Management*, 97, 102139.

(Liang, 2020) Liang, Y. C., & Liang, Y. C. (2020). Blockchain for dynamic spectrum management. *Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence*, 121-146

(Lu et al., 2021) Lu, X., Wu, Z., Wu, Y., Wang, Q., & Yin, Y. (2021, October). Atmchain: Blockchain-based solution to security problems in air traffic management. In *2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)* (pp. 1-8). IEEE.

(Lufthansa, 2023) Lufthansa: IT failure causes cancellations and delays for thousands of passengers ; URL: <https://www.euronews.com/travel/2023/02/15/lufthansa-it-failure-causes-cancellations-and-delays-for-thousands-of-passengers>; 2023

(Marikyan et al., 2022) Marikyan, D., Papagiannidis, S., Rana, O. F., & Ranjan, R. (2022). Blockchain adoption: A study of cognitive factors underpinning decision making. *Computers in Human Behavior*, 131, 107207.

(McGhin et al., 2019) McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of network and computer applications*, 135, 62-75.

(Miers et al., 2013) Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. 2013 IEEE Symposium on Security and Privacy.

(Mougayar, 2016) Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley

(Nakamoto, 2008) Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>

(Narayanan et al., 2016) Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press

(Narayanan et al., 2016) Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

(O'Dwyer & Malone, 2014) O'Dwyer, K. J., & Malone, D. (2014). Bitcoin mining and its energy footprint.

(Petkus, 2019) Petkus, M. (2019). Why and how zk-snark works. *arXiv preprint arXiv:1906.07221*.

(Politou et al., 2019) Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, 9(4), 1972-1986.

(RedHat, 2022) RedHat - What is an API?; URL: <https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces>; 2022

(Reid & Harrigan, 2013) Reid, F., & Harrigan, M. (2013). *An analysis of anonymity in the bitcoin system* (pp. 197-223). Springer New York.

(Rikken et al., 2019) Rikken, O., Janssen, M., & Kwee, Z. (2019). Governance challenges of blockchain and decentralized autonomous organizations. *Information Polity*, 24(4), 397-417

(Ruoti et al., 2019) Ruoti, S., Kaiser, B., Yerukhimovich, A., Clark, J., & Cunningham, R. (2019). Blockchain technology: what is it good for?. *Communications of the ACM*, 63(1), 46-53

(Sedlmeir et al., 2020) Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering*, 62(6), 599-608

(Sguanci et al., 2021) Sguanci, C., Spatafora, R., & Vergani, A. M. (2021). Layer 2 blockchain scaling: A survey. *arXiv preprint arXiv:2107.10881*.

(Stephen & Alex, 2018) Stephen, R., & Alex, A. (2018, August). A review on blockchain security. In *IOP conference series: materials science and engineering* (Vol. 396, No. 1, p. 012030). IOP Publishing.

(Stockburger et al., 2021) Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications*, 2(2), 100014

(Stoll et al., 2019) Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The carbon footprint of bitcoin. *Joule*, 3(7), 1647-1661.

(Stone, 2021) Stone, D. (2021). Trustless, privacy-preserving blockchain bridges. *arXiv preprint arXiv:2102.04660*.

(Swan, 2015) Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc."

(Swan, 2017) Swan, M. (2017). Anticipating the economic benefits of blockchain. *Technology innovation management review*, 7(10), 6-13

(Szabo, 1997) Szabo, N. (1997). The idea of smart contracts. *Nick Szabo's papers and concise tutorials*, 6(1), 199.

(Szydlo, 2004) Szydlo, M. (2004). Merkle tree traversal in log space and time. In *Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23* (pp. 541-554). Springer Berlin Heidelberg.

(Tapscott & Tapscott, 2016) Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin.

(Tapscott & Tapscott, 2016) Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin

(Tikhomirov et al., 2018) Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., Takhaviev, R., Marchenko, E., & Alexandrov, Y. (2018, May). Smartcheck: Static analysis of ethereum smart contracts. In *Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain* (pp. 9-16).

(Wamba et al., 2020) Wamba, F. S., Kamdjoug, K. J. R., Bawack, E.R., & Keogh, J. G. (2020). Bitcoin, Blockchain and Fintech:

a systematic review and case studies in the supply chain. *Production Planning and Control*, 31(2–3), 115–142. <https://doi.org/10.1080/09537287.2019.1631460>

(Wang et al., 2021) Wang, J., Liu, Y., Niu, S., Song, H., Jing, W., & Yuan, J. (2021). Blockchain enabled verification for cellular-connected unmanned aircraft system networking. *Future Generation Computer Systems*, 123, 233-244.

(Wegner, 1996) Wegner, P. (1996). Interoperability. *ACM Computing Surveys (CSUR)*, 28(1), 285-287.

(Yaga et al., 2019) Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019)

(Yaqoob et al., 2021) Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2021). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 1-16.

(Ye et al., 2018) Ye, C., Li, G., Cai, H., Gu, Y., & Fukuda, A. (2018, September). Analysis of security in blockchain: Case study in 51%-attack detecting. In *2018 5th International conference on dependable systems and their applications (DSA)* (pp. 15-24). IEEE.

(Zamyatin et al., 2019) Zamyatin, A., Harz, D., Lind, J., Panayiotou, P., Gervais, A., & Knottenbelt, W. (2019, May). Xclaim: Trustless, interoperable, cryptocurrency-backed assets. In *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 193-210). IEEE.

(Zhang et al., 2019) Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, 52(3), 1-34

(Zheng et al., 2018) Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, 14(4), 352-375.

(Zhou et al., 2021) Zhou, J., Feng, Y., Wang, Z., & Guo, D. (2021). Using secure multi-party computation to protect privacy on a permissioned blockchain. *Sensors*, 21(4), 1540.

(Zyskind et al., 2015) Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshop

