

# A part outlives the **cryptography** that signs it.

A technical brief on keeping airworthiness records verifiable across the service life of an airframe, including after the quantum transition.

BLOCKCHAIN.AERO  
TECHNICAL BRIEF · 2026

2026 · SEA LEVEL

## Summary

Aviation is committing its airworthiness and parts records to permanent digital ledgers. The cryptographic signatures protecting those records are not built to last the thirty-year service life of the aircraft. Vexidus is an integrity layer that keeps a record's signature verifiable and non-repudiable for decades, including after a quantum computer breaks today's classical cryptography. It anchors to the traceability systems the industry is already deploying rather than replacing them.

## The mismatch

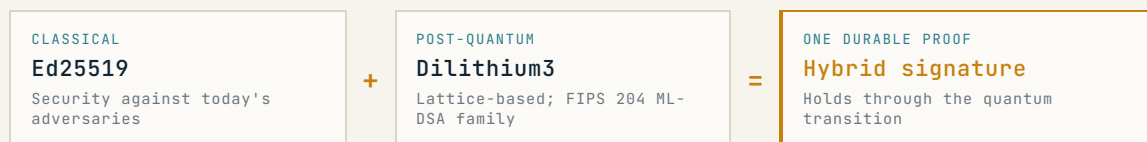
An airworthiness record must remain provable across the full life of the airframe, commonly thirty years or more. The industry is moving that recordkeeping onto digital, permanent infrastructure, pushed by a records-falsification scandal, published coalition recommendations for uniform digital traceability, and supply-chain digitization legislation advancing through 2025.

The platforms carrying that shift sign their records with classical cryptography of the RSA and elliptic-curve family. A cryptographically relevant quantum computer breaks those schemes. The record's data survives, but the signature's guarantee does not: proof of who signed it, and that it was never altered, fails. Non-repudiation of decades of historical records collapses retroactively. This is the harvest-now, forge-later exposure, and for records that must outlive the hardware they were signed on, it is structural rather than hypothetical.

RECORD LIFESPAN **30+ YEARS** // CLASSICAL SIGNATURE TRUST HORIZON **< 30 YEARS**

## What Vexidus is

A public Layer-1 blockchain, written in Rust, currently live on testnet. Every record committed to the chain is protected by a **hybrid signature**: a classical Ed25519 signature and a lattice-based signature at the Dilithium3 parameter level, drawn from the NIST FIPS 204 (ML-DSA) family finalized in August 2024. A verifier accepts a record only if both signatures hold.



If either scheme is later weakened, the other still protects the record during the transition window. A record signed on Vexidus is verifiable now and stays verifiable once classical signatures can be forged.

## How it fits what you already run

Vexidus does not ask aviation to replace the ledgers and MRO systems it is building. It sits beneath them as an anchoring layer. You keep your system of record. For each record you commit a cryptographic hash, together with its signature, to the Vexidus chain. That produces an independent, post-quantum-protected proof that a given record existed in a given state at a given time.

No migration and no rip-and-replace. Only hashes are anchored, so no proprietary data leaves your environment. Even if your internal ledger's classical signatures become forgeable later, the anchored proof on Vexidus still establishes the record's integrity and timestamp, verifiable past the quantum transition. You gain a durable backstop without changing the system your teams already use.

## Platform

ARCHITECTURE	Rust Layer-1, HyperSync consensus
BLOCK TIME	2.2 s
THROUGHPUT CEILING	~500,000 TPS
NETWORK	5 validators across 4 continents
CHAIN HEIGHT	1,800,000+ blocks (testnet)
WIRE PROTOCOL	Borsh
SIGNATURES	Ed25519 + Dilithium3 hybrid (FIPS 204 ML-DSA family)
EXECUTION IP	IntentVM, U.S. Patent Application 19/571,463

## Standards posture

The signature design tracks NIST FIPS 204 (ML-DSA), the federal post-quantum digital-signature standard finalized in August 2024, and pairs it with Ed25519 for classical assurance during the transition. The approach is built to complement, not compete with, the industry's move toward uniform digital traceability standards.

2056 · KÁRMÁN LINE

## Engagement

The first step is a scoped technical conversation. A pilot anchors a defined set of part or maintenance records and measures verification, integration fit, and overhead against your existing stack. Built for MROs, OEMs, Tier-1 suppliers, parts authorities, and the teams building traceability platforms who need a foundation that holds past the quantum transition.

START A CONVERSATION // [blockchain.aero](https://blockchain.aero)

Quantitative figures describe Vexidus testnet performance and architecture. This brief is a technical positioning document and does not assert any aviation deployment, partnership, or regulatory certification. References to industry programs and regulatory activity describe the market context and do not imply endorsement of Vexidus.

VEXIDUS CORPORATION  
DELAWARE C-CORP

blockchain.aero  
POST-QUANTUM INTEGRITY FOR AVIATION RECORDS