Law L3:
Data Hash (HD)

Input Attestation & Non-Malleability

Authoritative Edition

L3 Definition

"All decision-making data must be hashed before use. Tampered, incomplete, or altered data immediately invalidates execution."

The Attestation Equation

Data is not trusted until it is mathematically sealed.

$$HD = SHA256(\ Input\_Data\ )$$

HD acts as the "Digital Seal" for the input.

What Constitutes "Data"?

L3 applies to ANY input used to make a decision.

JSON / XML

API payloads & structures.

DB Rows

SQL/NoSQL record sets.

Sensor Data

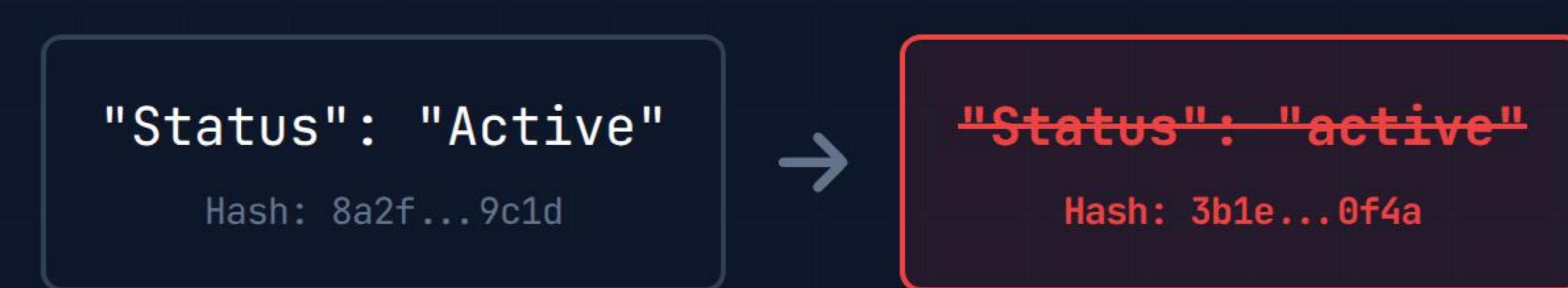Robotic & IoT streams.

Documents

PDFs & Evidence files.

The Attestation Process

Raw Input → Canonicalize (Sort/Trim) → Hash (SHA-256) → HD Generated

This process converts "Information" into "Evidence".

The Principle of Non-Malleability

If you change **one bit**, the seal breaks.

"Status": "Active"

Hash: 8a2f...9c1d

→

"Status": "active"

Hash: 3b1e...0f4a

MISMATCH = EXECUTION BLOCKED.

The Frozen Snapshot

Live data is volatile. You cannot verify a stream that keeps changing.

L3 requires that data be **Snapshotted** (Frozen) before the hash is calculated.

HD: 7f2a...

Immutable State.

Why L3 Matters

Preventing TOCTOU

Time-of-Check to Time-of-Use attacks. Hashing prevents data from changing between verification and execution.

Preventing Silent Corruption

Bit-rot, database errors, or malicious SQL injection attempts immediately invalidate the hash.

Summary

L3
Data Integrity

Attestation

Data is not just input; it is attested evidence. L3 guarantees that the system executes on exactly what was approved—nothing more, nothing less.

Questions?

NOVAK Protocol Standards Series

Law L3: Data Hash (HD)