NOVAK PROTOCOL LAWS

Law L4:
Output Hash (HO)

Output Non-Malleability & Deterministic Binding

Authoritative Edition

L4 Definition

"The output of the computation must be hashed (HO). It must match the expected digest **before** the output is allowed to be used."

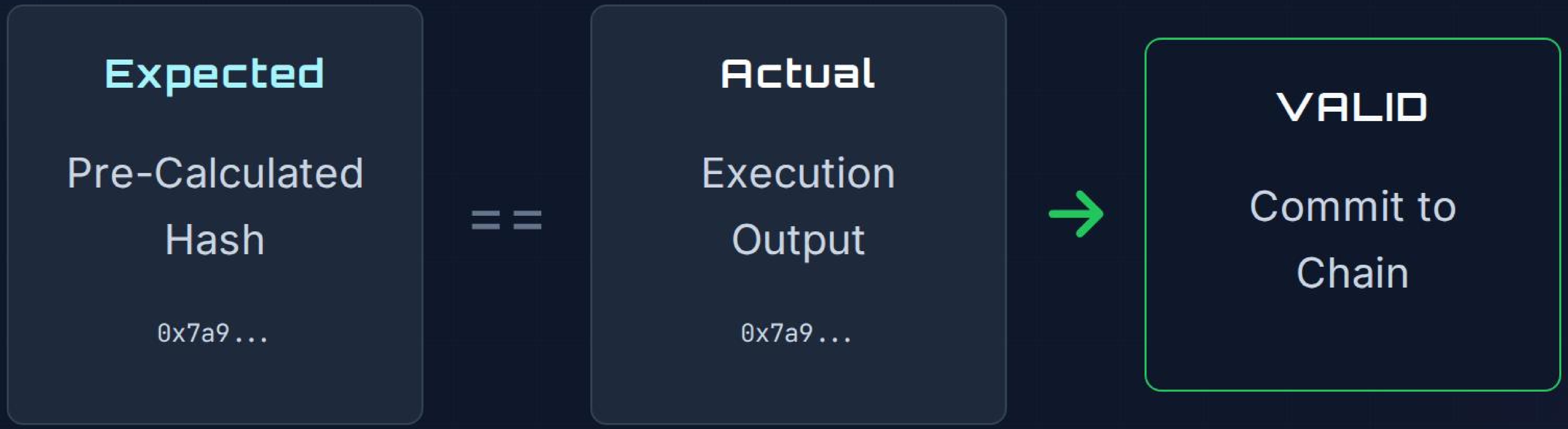
The Commitment Equation

Output is not random. It is the result of Rule applied to Data.

```
HO = SHA256( Rule(Data) )
```

We calculate what *should* happen, then verify it *did* happen.

Pre-Computation & Verification



Expected

Pre-Calculated Hash

`0x7a9...`

==

Actual

Execution Output

`0x7a9...`

→

VALID

Commit to Chain

If hashes differ: **Execution Blocked.**

Output Non-Malleability

Once an output is generated, it cannot be changed.

- **Locked:** The value is frozen.
- **No Edits:** Database admins cannot "fix" a number.
- **No Interception:** Network attackers cannot swap the payload.

The "Check Amount" Analogy

L3 (Input)

Prevents someone from changing the amount you **write** on the check.

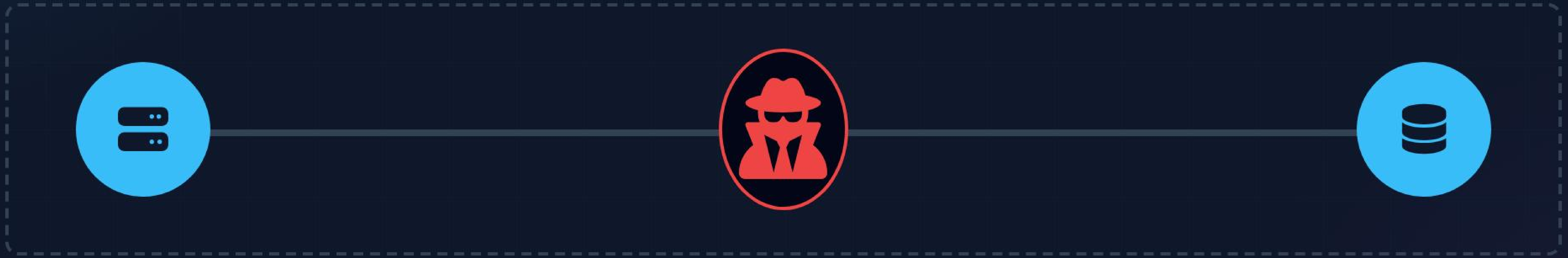
L4 (Output)

Prevents the bank from changing the amount **deposited** after you hand it over.

L4 protects the result **after** calculation but **before** storage.

Defeating Man-in-the-Middle

Attackers often try to swap the output packet.



Without L4, the attacker succeeds.

With L4, the hash mismatch blocks the write.

L4 vs. AI Hallucination

AI models often drift or hallucinate outcomes that contradict their inputs.

- 🤖 **Drift:** Model changes answer next time.
- ⚠ **Hallucination:** Output implies input that didn't exist.

L4 Enforcement

If HO doesn't match the deterministic projection, the hallucination is discarded.

Summary

L4

Output Integrity

The Final Seal

L4 ensures that the result of the work is as immutable as the instruction to do the work. It creates a closed loop of integrity.

Questions?

NOVAK Protocol Standards Series

Law L4: Output Hash (HO)