

NOVAK PROTOCOL SPECIFICATION

Laws L0-L15: Core Protocol

Authoritative Cryptographic Governance Framework

Version 1.0 (Final Draft)

The Paradigm Shift

Legacy Model

Execute → Then → Audit

Allows silent corruption and errors before detection.

NOVAK Model

Prove → Then → Act

No cryptographic proof = No execution.

L0

The Zeroth Law (L0)

"No system may act unless cryptographic proof confirms the input, rules, and output have not changed."

All other laws are subordinate to L0.

L1: Deterministic Rule Execution

Every computation must produce the **same output** for the same inputs, rules, and environment.

- ⊘ No Randomness.
- ⊘ No Race Conditions.
- ⊘ No Hidden Variables.



L2-L4: The Cryptographic Trinity



L2: Rule Hash

Code is frozen.

`HR = Hash(Rule)`



L3: Data Hash

Input is attested.

`HD = Hash(Data)`



L4: Output Hash

Result is bound.

`H0 = Hash(Output)`

L5 & L6: Binding & Precedence

L5: Execution Binding (HVET)

NOVAK binds the trinity into a single immutable identity.

```
HVET = Hash(HR || HD || H0)
```

L6: Precedence Rule

No action can occur unless:

Provided HVET = Expected HVET

Mismatch → Execution Halts.




L8: Recursive Global Audit Chain

Every approved HVET becomes the next link in the chain.


$$\text{Receipt}(n) = \text{Hash}(\text{Receipt}(n-1) \parallel \text{HVET}(n))$$

L10: Zero Trust Execution Model

The system must assume:

-  Data can lie.
-  Rules can drift.
-  Memory can be manipulated.

Trust Source

Cryptography Only.

L12: Deterministic Safety Gate



This is the enforcement layer that blocks execution until HVET validation succeeds.

- ✓ **Deterministic:** No ambiguity.
- ✓ **Non-Bypassable:** Hard stop.
- ✓ **Visible:** Audit logs generated.

L14: Identity Receipt (EIR)

```
// L14 Structure
```

```
EIR = {  
    rule_hash: HR,  
    data_hash: HD,  
    output_hash: HO,  
    hvet: HVET,  
    timestamp: ISO_8601,  
    actor: Identity_Key  
}
```

Authoritative Proof of State.

System Invariants

L7: Frozen Snapshot

Decisions must reference a frozen snapshot of inputs. Live streams are untrusted until hashed.

L9: Forward-Only

Prohibits rewriting history, erasing links, or selective rollback. Every drift is visible.

L11: No Hidden States

All inputs, rules, and outputs must be explicitly included in hashes. No undocumented variables.

L13 & L15: Audit Transparency

L13: Global Verifier

All verification logic must be publicly documentable and independently re-runnable.

If it can't be re-run, it's not trusted.

L15: Full Disclosure

System must disclose all hashing mechanisms, failure modes, and chain linkages.

No Black Boxes.

Summary

15

Immutable
Laws

Universal Governance

These laws define the NOVAK model. Any system—governmental, financial, medical, robotic, or AI—can adopt these laws to guarantee the highest level of integrity.

Questions?

NOVAK Protocol Standards Series

Category: Laws L0-L15