NOVAK PROTOCOL SERIES

Standard Protocol-2 (SP-2): Cryptographic Standard

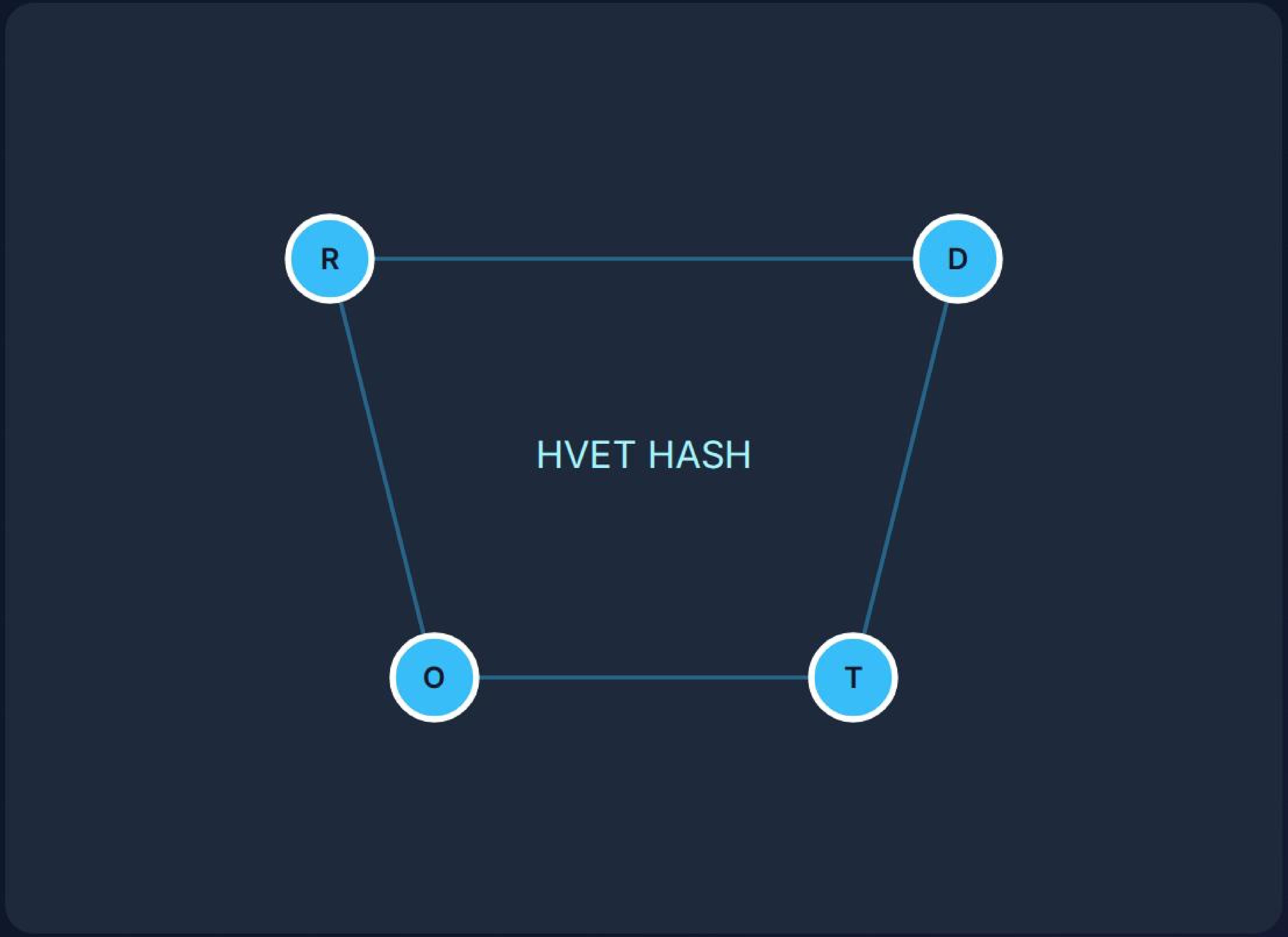
Hash-Verified Execution Traces (HVET) &
Recursive Global Audit Chain (RGAC)

Version 1.0 (Dec 2025)

The Mathematical Backbone

SP-2 defines the core cryptographic truth conditions for the NOVAK Protocol. It is the mathematical foundation that ensures every action in a PBAS (Proof-Before-Action System) is:

- **Deterministic:** Reproducible outputs.
- **Identity-Bound:** Tied to a specific actor.
- **Tamper-Evident:** Impossible to alter history.



Core Components

HVET

Hash-Verified Execution Trace
The atomic unit of proof. A cryptographic binding of Rules, Data, and Output.

EIR

Execution Identity Receipt
The authoritative pre-execution proof. Binds the HVET to a specific identity and time.

RGAC

Recursive Global Audit Chain
An append-only, local hash chain that orders execution events sequentially.

Concept 1: Canonical Serialization

To ensure **deterministic hashing**, all data must be serialized using the NOVAK-CANONICAL-1 format before hashing. Even a single whitespace difference changes the hash.

- **UTF-8 Only:** Universal encoding standard.
- **Lexicographical Sort:** All fields sorted by key.
- **String Numbers:** No floating-point errors.
- **No Whitespace:** Zero normalization allowed.

Concept 2: HVET Structure

The Ingredients

HR	Hash of Ruleset
HD	Hash of Input Data
HO	Hash of Output
T	Timestamp (ISO8601)

The Formula

The final HVET is a SHA-256 hash of the concatenated components.

```
HVET = SHA256(
  HR ||
  HD ||
  HO ||
  Timestamp
)
```

How HVET Works (Simple Analogy)

Think of creating an HVET like baking a cake where the receipt must prove *exactly* what ingredients were used.

STEP 1: CANONICAL HASHING

The Ingredients

We weigh the flour and sugar exactly. In the computer, we standardize the Rules, Data, and Output. If you change a single grain (or number), the weight (Hash) completely changes.

STEP 2: CONCATENATION

The Mix

We pour the ingredients into the bowl in a strict order, adding the exact time we started. We join all these digital pieces together into one long sequence.

STEP 3: SHA-256 HASHING

The Final Seal

We bake and stamp the cake. This creates the HVET—a unique digital fingerprint. If anyone tampered with the recipe in the past, this final fingerprint wouldn't match.

Concept 3: Execution Identity Receipt (EIR)

The "Signed Check"

An HVET proves *what* happened. An EIR proves *who* did it and *when*.

It acts as a digital container that wraps the HVET with:

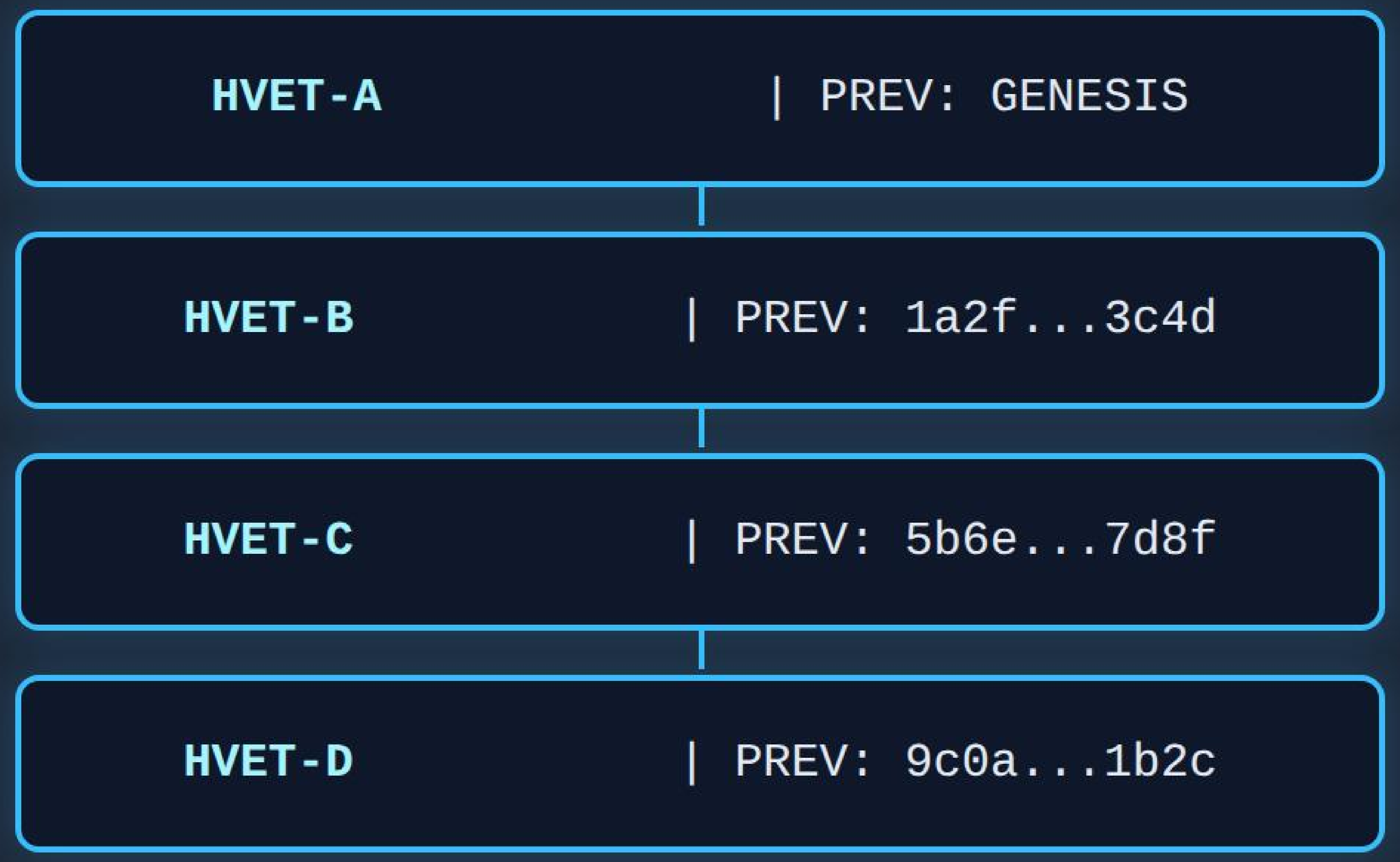
- Unique UUID (eir_id)
- Executor Identity (Public Key)
- Digital Signature (ECDSA/Ed25519)
- Rule Versioning

Concept 4: RGAC

Recursive Global Audit Chain

A tamper-evident, append-only hash chain. While it looks like a blockchain, it is fundamentally different:

- ✗ No Miners
- ✗ No Consensus Mechanism
- ✓ Local & Deterministic
- ✓ Ultra-fast Audit Speed



HVET-A | PREV: GENESIS

HVET-B | PREV: 1a2f...3c4d

HVET-C | PREV: 5b6e...7d8f

HVET-D | PREV: 9c0a...1b2c

RGAC Append Logic

Each new entry is cryptographically linked to the previous one, creating an unbroken chain of custody.

Step 1

Fetch Previous Hash

(Or "GENESIS")

Step 2

New EIR Arrives

(Verified Proof)

Step 3

Calculate Link

SHA256(Prev || New)

Step 4

Append Entry

Push to Chain

Security Guarantees

SP-2 protects against specific failure modes by relying on cryptographic collision resistance and digital signatures.

- **Input Modification:** Detected by HD mismatch.
- **History Rewrites:** Breaks the RGAC chain.
- **Identity Spoofing:** Fails Signature verification.
- **Replay Attacks:** Blocked by unique UUIDs.

NOVAK-compliant systems must support at least **CL-3**.

Level	Definition	Feature Set
CL-1	Basic HVET Generation	Hash logic only. No identity.
CL-2	Full EIR Binding	Identity + Timestamps added.
CL-3	Full RGAC Chain	Historical audit chain (Mandatory).
CL-4	Signature Support	Cryptographic signatures enabled.

Protocol Summary

3

Core Primitives

(HVET, EIR, RGAC)

A Deterministic Future

SP-2 provides the mathematical certainty required for high-stakes automated decision making. It moves audit from a "post-event" activity to a "pre-action" requirement.

Status: Effective Dec 2025

Questions?

NOVAK Protocol Standards Series

Category: PBAS-02 (Proof-Before-Action Systems)