NOVAK PROTOCOL SERIES

Part 4: Cryptographic Architecture

Formal Spine: HVET, EIR, RGAC

Authoritative Edition

The Cryptographic Spine

HVET

Execution Trace

EIR

Identity Receipt

RGAC

Recursive Chain

NOT A BLOCKCHAIN. NOT LOGGING.

1. HVET (Hash-Verified Execution Trace)

The canonical, sealed description of the event.

```
HVET(A) = H( HR || HD || HI || HO || T || nonce || PLX || PSX )
```

- **HR:** Rule Hash
- **HD:** Input Hash
- **HI:** Identity Hash
- **HO:** Output Hash
- **T:** Global Timestamp
- **PLX:** Physical Layer
- **PSX:** Psycho-Social
- **Nonce:** Anti-Replay

2. Hashing Standards

Tier 1: Rules

SHA-3 / SHA3-512

Used for deterministic rule hashing. Superior sponge construction for rule purity.

Tier 2: Data

SHA-256

Used for data, identity, and timestamps. High-speed cross-platform interoperability.

No Proof-of-Work. No Merkle Trees.

3. EIR (Execution Identity Receipt)

Formerly "NIPS". Binds the actor to the execution.

```
EIR = H( HI || HR || HD || HO || T || Jurisdiction || Device || PLX || PSX )
```

- **Enforces:** L6 (Execution Identity).
- **Enforces:** L11 (Public Verifiability).
- **Enforces:** L14 (Machine Non-Deviation).

4. Safety Gate Cryptography

The cryptographic barrier preventing invalid actions.

1 **Rule Purity:** R matches canonical SHA-3.

2 **Data Lock:** Schema enforced.

3 **Identity:** Hardware root match.

4 **Output:** Deterministic pre-calc.

🚫

FAIL CLOSED

If any bit fails, action is impossible.

5. Global Timechain

NOVAK time is not a local clock. It is a monotonic lineage.

```
T = H( UTC || Sequence || DeviceState || DriftProfile )
```

Trusted Nodes

Monotonic Counter

Drift-Locked

6. RGAC (Recursive Global Audit Chain)

Infinite-depth audit recursion. Not a blockchain.

```
RGAC(n) = H( RGAC(n-1) || HVET || EIR || T || PLX || PSX )
```

n-1

n

n+1

No forks. No miners. No consensus failure.

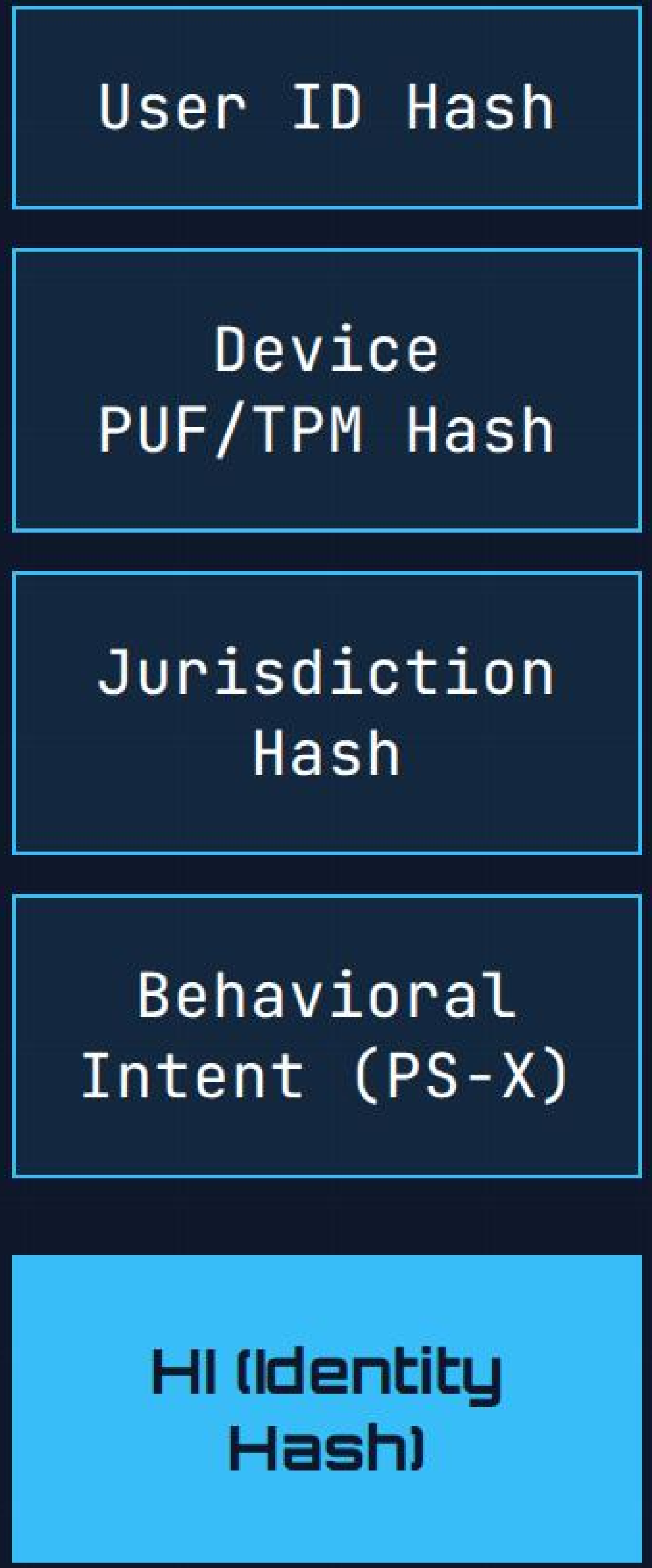
7. Non-Malleability (L2-L4)

Cryptographic structure ensures:

- Inputs cannot be covertly altered.
- Rules cannot be substituted.
- Devices cannot misreport state.
- Actors cannot repudiate actions.

8. Identity Binding (Internal)

Identity (HI) is a composite hash.



User ID Hash

Device PUF/TPM Hash

Jurisdiction Hash

Behavioral Intent (PS-X)

HI (Identity Hash)

9. Recursive Audit Mathematics

Backward

Auditors can trace to genesis.

Forward

Tampering at k invalidates $k+1$.

Cross

Systems validate each other.

"Tampering anywhere = Tampering everywhere."

10. Extended Cryptography

PL-X (Physical)

Hardware Cryptography

- Metastability detection.
- Jitter correction.
- Power-profile fingerprinting.

PS-X (Social)

Behavioral Cryptography

- Intent-consistency hashing.
- Fraud-pattern matching.
- Deception detection.

Questions?

NOVAK Protocol Standards Series

Part 4: Cryptography