PART 4 — CRYPTOGRAPHIC ARCHITECTURE OF THE NOVAK PROTOCOL

This section establishes the **formal cryptographic spine** of NOVAK:

- HVET: Hash-Verified Execution Trace
- EIR key structures (formerly NIPS → Execution Identity Receipt)
- RGAC lineage functions (formerly REVELATION)
- Deterministic safety proofs
- Physical-layer cryptographic considerations (PL-X)
- Psycho-social integrity anchoring (PS-X)
- Hash functions, identity primitives, audit recursion
- Global timestamp integrity
- Non-malleability enforcement via Laws L1–L4
- Recursive verification structures (L7–L15)

NOVAK is a cryptographic *execution environment*, not a blockchain, checksum, or logging system.
This architecture guarantees that execution can never occur without deterministic proof.

I. HASH-VERIFIED EXECUTION TRACE (HVET)

Formal Definition

For action **A**, executed under deterministic rule **R**, with attested input **D**, actor **I**, output **O**, and timestamp **T**, the HVET is:

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

Where:

- **HR** = hash of rule R
- **HD** = hash of input data D
- **HI** = hash of identity I
- **HO** = hash of output O
- **T** = globally ordered timestamp
- **nonce** = SG-generated anti-replay field
- **PLX** = physical-layer hash objects per Addendum PL-X
- **PSX** = psycho-social integrity hash objects per Addendum PS-X

Purpose

HVET is the **canonical, cryptographically sealed description** of what happened *before something happens*.

It enforces:

- **L0 — Anchor Law**
- **L1–L4 — Deterministic Purity + Non-Malleability**
- **L5 — Pre-Execution Hashing Law**
- **L6 — Execution Identity Binding**

II. HASH FUNCTIONS USED IN NOVAK

NOVAK requires two-tier hashing:

Tier 1 — SHA-3 / SHA3-512

For deterministic rule hashing and safety enforcement.

Tier 2 — SHA-256 or SHA3-256

For data, identity, timestamp, and device lineage hashing.

Reasoning:

- SHA-3 provides superior sponge-construction security for rule purity.
- SHA-256 provides high-speed, cross-platform interoperability for D, I, O, T.

NOVAK does **not** rely on:

- proof-of-work
- proof-of-stake
- probabilistic consensus
- blockchains
- Merkle-mining trees

NOVAK uses **deterministic cryptographic commitments** only.

III. EXECUTION IDENTITY RECEIPT (EIR)

(formerly NIPS)

The EIR binds the **actor**, the **environment**, and the **execution** into a single cryptographically sealed object.

Formal Definition

> **EIR = H(HI ∥ HR ∥ HD ∥ HO ∥ T ∥ jurisdiction-hash ∥ device-hash ∥ PLX ∥ PSX)**

Where:

- **HI** = identity hash for the actor
- **jurisdiction-hash** = legal boundary context
- **device-hash** = TPM/PUF hardware root identity
- **PLX** = physical-layer state object
- **PSX** = psycho-social integrity object

EIR enforces:

- **L6 — Execution Identity Law**
- **L11 — Public Verifiability**
- **L14 — Machine Non-Deviation**

No action can proceed without a valid EIR.
This is enforced by the **Safety Gate**.

IV. SAFETY GATE CRYPTOGRAPHIC MECHANISM

(formerly HARMONEE → now Deterministic Safety Layer)

Safety Gate (SG) is the **cryptographic barrier** preventing invalid actions.

Its internal operations include:

1. **Rule-Purity Hash Verification**
    - HR must be a pure function of R
    - R must match its canonical SHA-3 fingerprint
    - No mutable state allowed
    - No side effects permitted
2. **Data Non-Malleability Proof**
    - HD must be stable and attestable
    - No data modification is allowed after attestation
    - Schema-lock enforced per L2–L3
3. **Identity Binding**
    - HI must match authorized identity credentials
    - Device-hash must match hardware root
    - Jurisdiction-hash ensures legal boundaries are respected (L6, PL-X, PS-X)
4. **Output Pre-Computation**
    - HO must be pre-computable deterministically
    - No probabilistic results allowed
    - No stochastic “AI drift” allowed (L14)
5. **Timestamp Ordering**
    - T must be monotonic, globally ordered
    - T violations automatically halt execution (L8)

6. **HVET Construction**
    - SG constructs HVET internally
    - Ensures L0–L7 compliance

If any field fails verification, **action is impossible**.

V. TEMPORAL ORDERING AND GLOBAL TIMECHAIN

NOVAK time is not a local clock.
It is a **global monotonic timestamp lineage** secured through:

1. **Trusted Time Attestation Nodes (TTANs)**
2. **Monotonic sequence counters**
3. **Drift-locked correction circuits** *(PL-X)*
4. **Cross-jurisdiction verification**

Formal Time Object

T = H(UTC-time ∥ sequence-counter ∥ device-timing-state ∥ drift-profile)

This satisfies:

- **L8 — Temporal Ordering**
- **L9 — Global Consistency**

VI. RGAC — RECURSIVE GLOBAL AUDIT CHAIN

(formerly REVELATION)

RGAC is a **cryptographically recursive, infinite-depth audit chain**.

Formal Recurrence Relation

$$RGAC_n = H(RGAC_{n-1} \,//\, HVET_n \,//\, EIR_n \,//\, T_n \,//\, PLX_n \,//\, PSX_n)$$

Guarantees:

- **Immutability (L0)**
- **Recursive verifiability (L7)**
- **Global ordering (L8)**
- **Cross-domain interoperability (L10)**
- **Public verifiability (L11)**
- **Minimal trust surface (L12)**
- **Regulatory determinism (L13)**
- **Machine non-deviation (L14)**
- **Universal auditability (L15)**

RGAC is *not* a blockchain.
It is a **deterministic audit recursion** with no forks, no miners, no consensus failures, and no economic incentives.

VII. NON-MALLEABILITY ENFORCEMENT

(L2–L4 in cryptographic detail)

Non-malleability ensures:

- Inputs cannot be covertly altered
- Outputs cannot be reinterpreted
- Rules cannot be substituted
- Identity cannot be swapped
- Timestamps cannot be rewritten
- Devices cannot misreport state
- Actors cannot repudiate actions

The system implements:

- **Schema-locking**
- **Attestation hashing**
- **Value-domain sealing**
- **Deterministic output graphs**
- **Side-channel rejection (PL-X)**
- **Deception-surface bounding (PS-X)**

Every object in NOVAK is **structurally locked** at the cryptographic level.

VIII. IDENTITY BINDING DETAILS

(EIR internal cryptography)

Identity is composed of:

1. **User ID Hash**
2. **Device PUF/TPM Hash**
3. **Jurisdiction Hash**
4. **Behavioral Intent Pattern Hash** *(from PS-X)*
5. **Control-Surface Integrity Hash**
6. **Multi-Factor Credential Hashing**

All are merged into HI, which is used in HVET and EIR.

Identity cannot be forged because:

- PUF signatures are unique
- TPM roots cannot be duplicated
- jurisdiction-hash adds legal invariance
- intent-pattern sensing detects fraud vectors

This satisfies L6, L11–L14.

IX. RECURSIVE AUDIT MATHEMATICS

RGAC enables three forms of recursion:

1. Backward Recursion

Auditors can follow the chain back to the very first event.

2. Forward Recursion

Any tampering at step *k* invalidates *all* forward steps automatically.

3. Cross-Recursion

Multiple independent NOVAK implementations can validate each other's audit chains via deterministic hashing.

This enforces the NOVAK universal rule:

> **Tampering anywhere = tampering everywhere = detected immediately.**

X. PHYSICAL-LAYER CRYPTOGRAPHY (PL-X)

HVET, EIR, and RGAC integrate:

- metastability detection
- hardware jitter correction
- clock-skew modeling
- propagation-delay sealing
- environmental hash fields
- power-profile fingerprinting

This closes hardware attack surfaces.

XI. PSYCHO-SOCIAL CRYPTOGRAPHY (PS-X)

Every NOVAK event includes:

- intent-consistency hashing
- fraud-pattern matching

- behavioral signature models
- user-action lineage indexing
- multi-identity deception detection

This closes human attack surfaces.