Part 3: Scientific Foundations

Cryptographic, Mathematical, and Physical Basis

Authoritative Edition

The Scientific Pillars

Safety Gate
~~formerly HARMONEE~~

Deterministic Barrier

RGAC
~~formerly REVELATION~~

Global Audit Chain

EIR
~~formerly NIPS~~

Identity Receipt

1. Safety Gate (SG)

The Universal Invariant:

> "An action is not allowed to occur unless the system first proves, with cryptographic certainty, that all inputs, rules, and outputs are deterministic."

The Gate

If proof is incomplete, action is impossible.

Scientific Basis of SG

Pure Functions

No side effects. Same input = Same output.

Automata

Deterministic finite-state transitions.

Crypto Checks

SHA-2/SHA-3 structural integrity enforcement.

Integrated with PL-X (Jitter Correction) and PS-X (Fraud Mitigation).

2. RGAC (Recursive Global Audit Chain)

Infinite-depth audit recursion.

$$RGAC(n) = H(\ HVET(n)\ ||\ RGAC(n-1)\ ||\ T(n)\ )$$

NOT Blockchain

- ✕ No Mining
- ✕ No Forks
- ✕ No Probabilistic Finality

Scientific Guarantee

If a malicious actor alters entry k, all entries $k+1$ through infinity become invalid. The chain creates an infinite regression barrier.

Infinite Regression Barrier

Why it cannot be rebuilt

- 🕐 Timestamps are external/monotonic.

- 👆 Identity proofs cannot be recomputed.

- 🚫 Safety Gate refuses unprovable replays.

Physical Integration (PL-X)

- ▦ Hardware TPM/PUF sealing.

- ⎍ Metastable state rejection.

3. EIR (Execution Identity Receipt)

Cryptographic finality for identity.

```
EIR = H( Identity || Rule || Data || Output || Time || Device )
```

Proven

Unforgeable cryptographic binding.

Bound

Attached to specific hardware/actor.

Public

Verifiable without secret keys.

The NOVAK Execution Ladder

1   **Safety Gate:** Verifies determinism & attestation.

2   **EIR:** Binds identity to the proof.

3   **HVET:** Produced from R, D, I, O, T.

4   **RGAC:** Records event into global lineage.

Result: Public Verifiability.
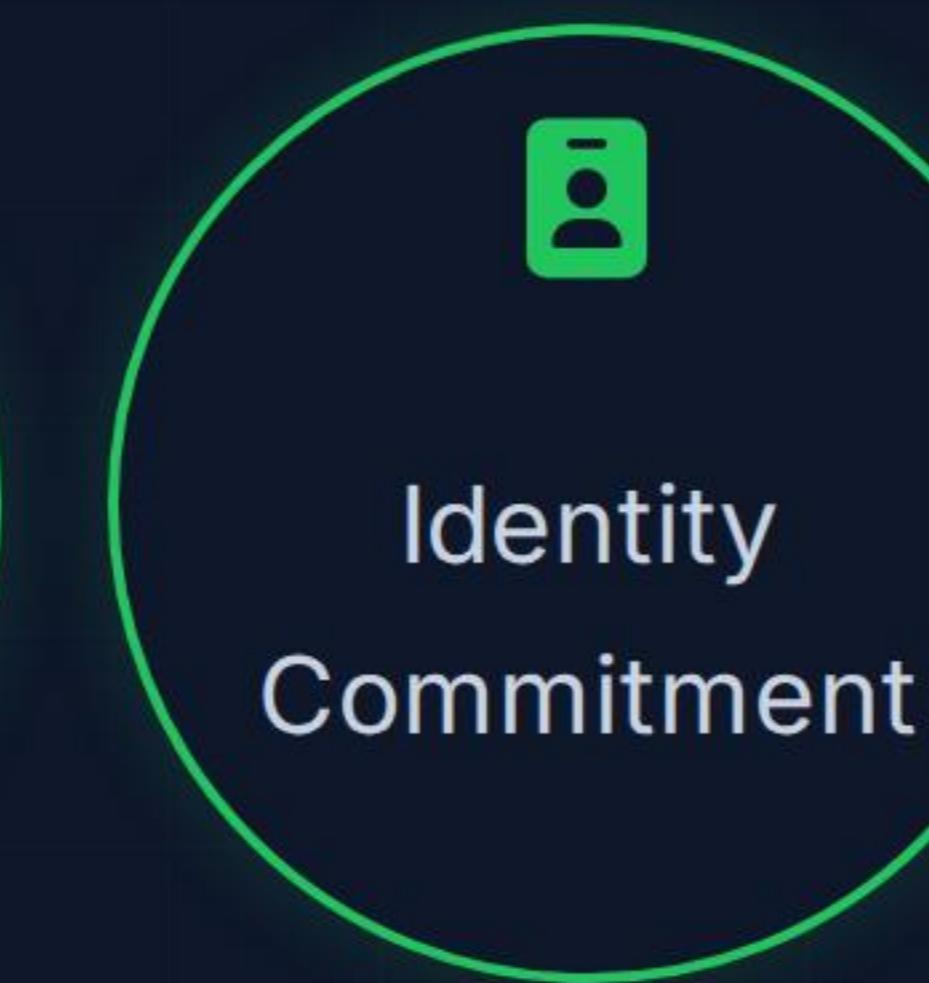
5 Unbreakable Primitives
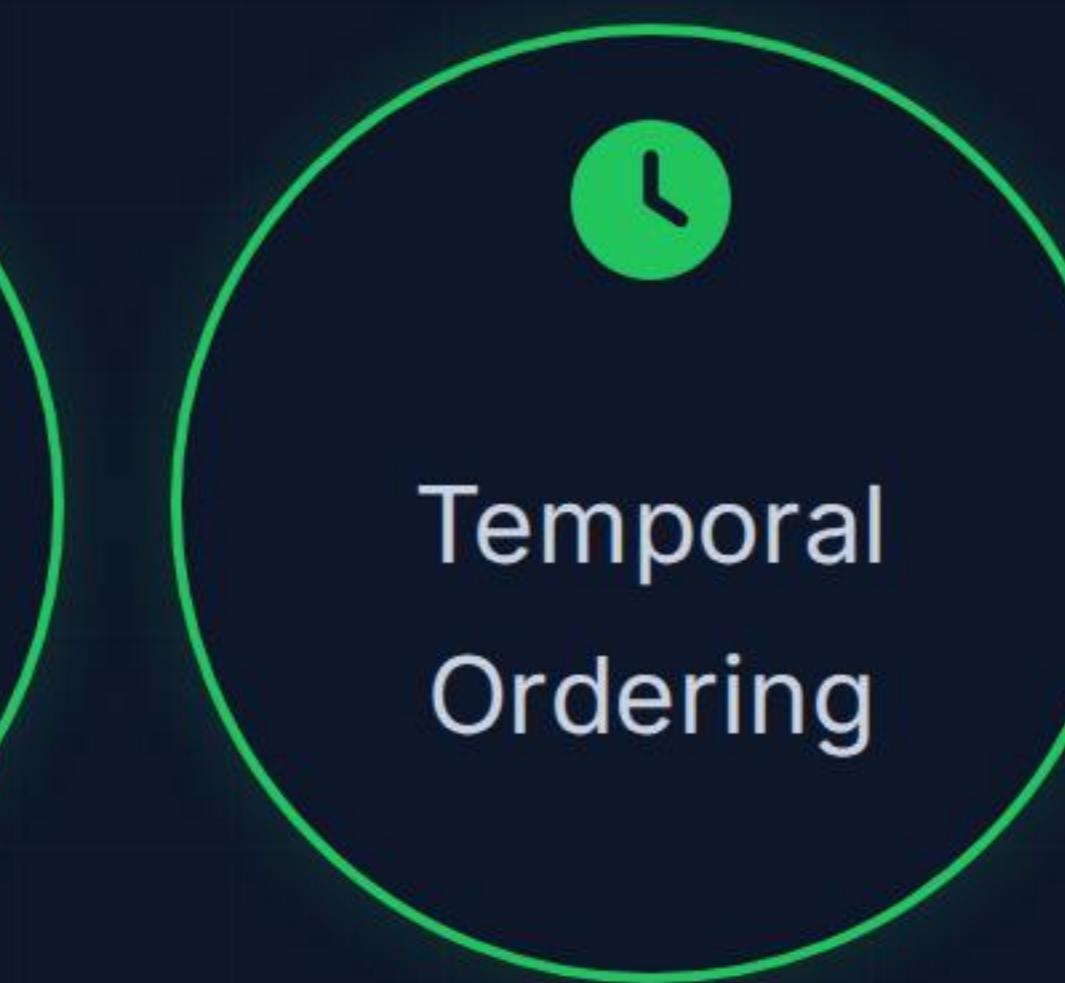
Determinism

Hashing

Identity Commitment

Temporal Ordering

Recursive Auditability

Questions?

NOVAK Protocol Standards Series

Part 3: Scientific Foundations