NOVAK PROTOCOL LEARNING SERIES

CRYPTOGRAPHY 101

From Basic Principles to Authoritative Execution

PART 1: THE TRUST PARADOX

THE PROBLEM WITH TRUST

Historically, digital systems rely on trust: trust in the operator, the hardware, and the database administrator.

This introduces critical vulnerabilities: **Insider Fraud**, **Data Tampering**, and **System Ambiguity**.

> TRUST IS A VULNERABILITY.

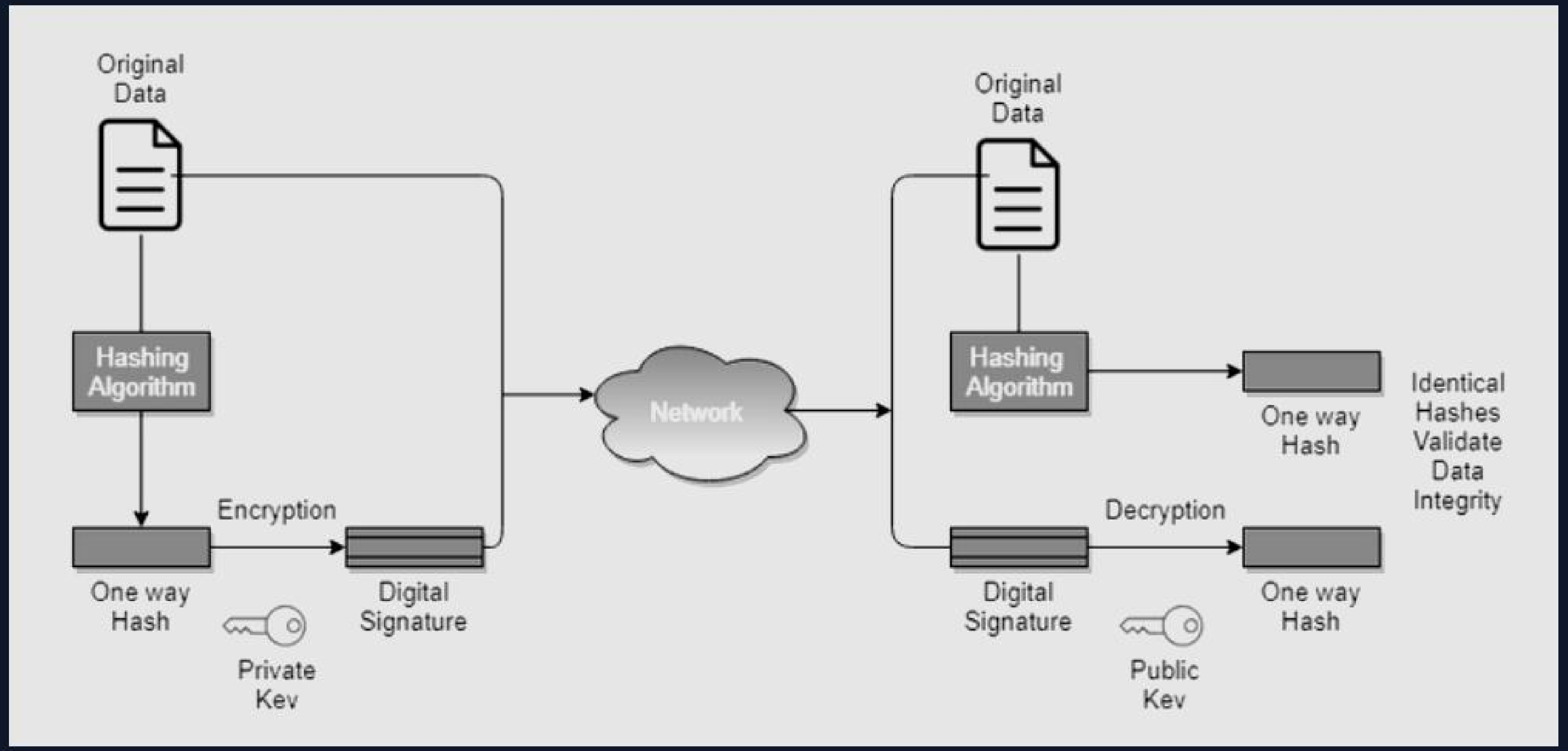
PART 2: HASHING & INTEGRITY

THE FOUNDATION

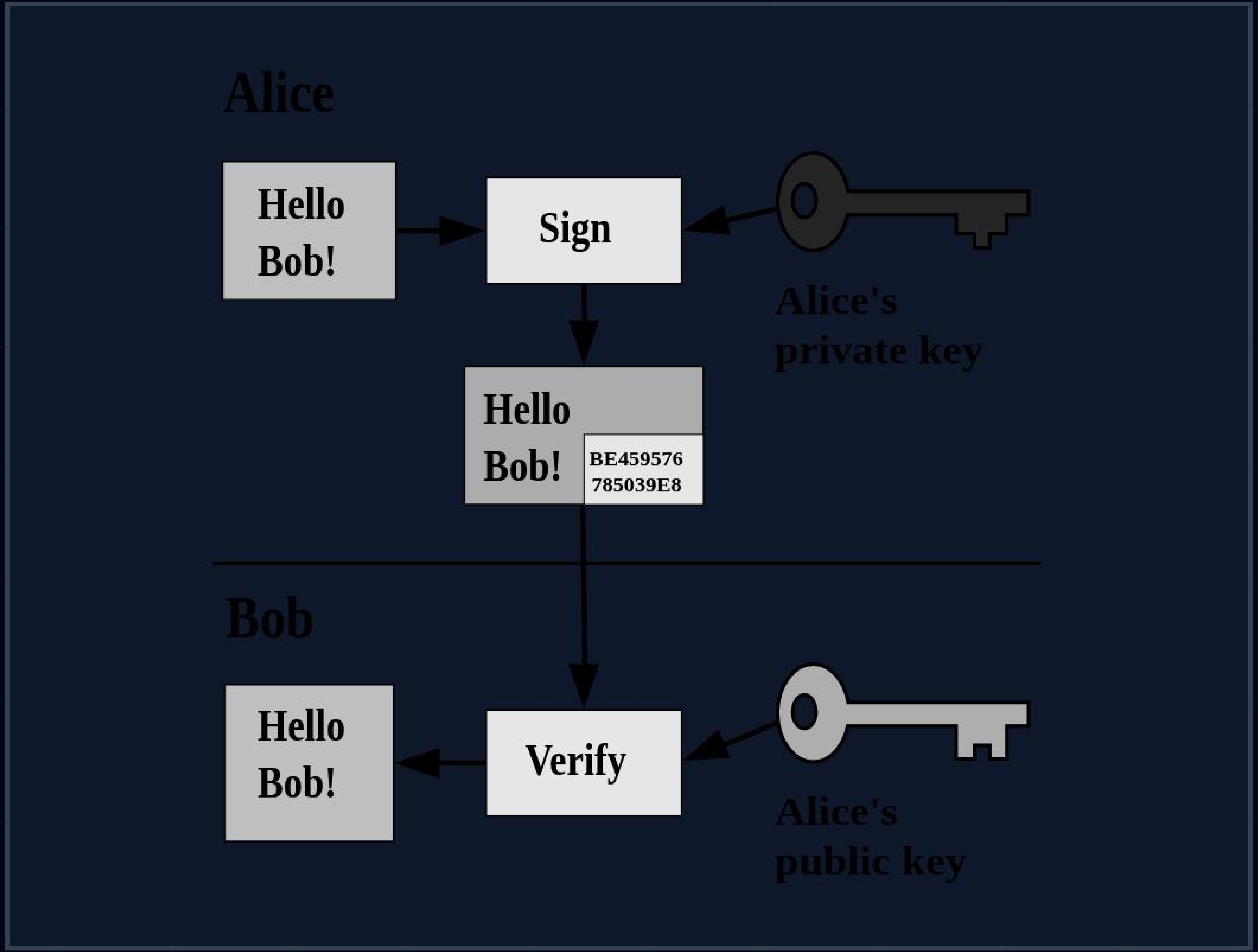
A hash function is a **one-way**, **deterministic** mathematical process that converts any input into a fixed-size string.

Integrity: Changing one bit of input changes the entire hash.

NOVAK Use: Data Attestation (L2-L3).



PART 3: PROOF OF IDENTITY (EIR)



ASYMMETRIC CRYPTOGRAPHY

Digital signatures use a pair of mathematically linked keys to prove identity without revealing the secret.

Private Key: Signs the data (Secret).

Public Key: Verifies the signature (Open).

> NOVAK: ELIMINATES ANONYMOUS ACTION.

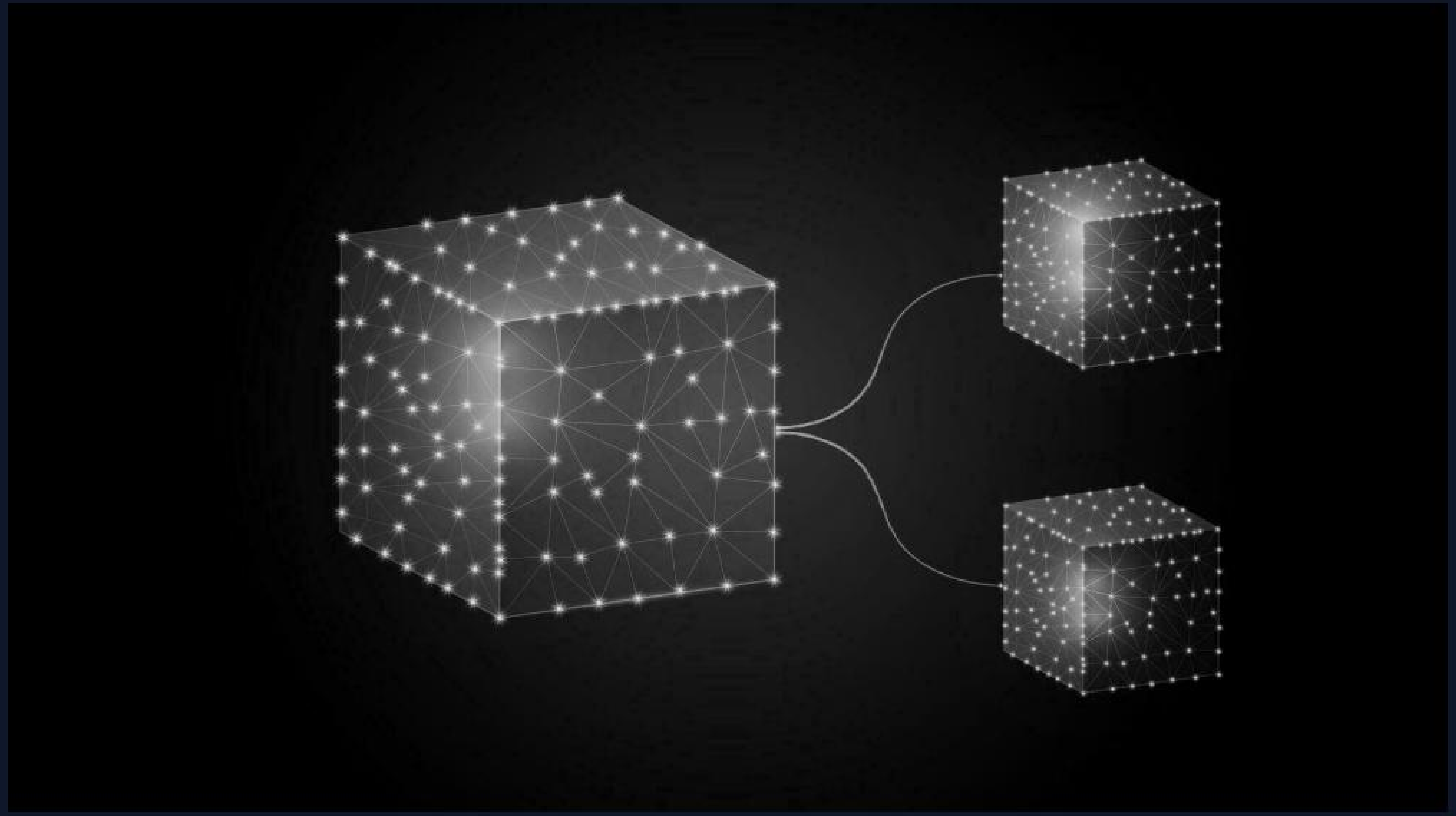
PART 4: ENCRYPTION & SECRECY

SECURING THE DATA

While hashing proves integrity, **encryption** ensures confidentiality. It scrambles data so that only authorized parties can read it.

NOVAK uses standard primitives (like **SHA-3** and **Ed25519**) as dictated by Law L15 to ensure that sensitive data remains secure while its *integrity* is publicly verified.

PART 5: THE CHAIN (RGAC)



IMMUTABLE LINEAGE

The core principle of a blockchain is linking each new record to the hash of the previous one.

NOVAK's RGAC (Recursive Global Audit Chain) uses this to create a forward-only, irreversible history. Tampering with a past record breaks the mathematical chain, making fraud instantly detectable.

PART 6: LAW L0

> "No action can occur until proofs for the rule, data, identity, and timestamp are cryptographically validated."

— THE ZEROTH LAW: PROOF-BEFORE-ACTION

This shifts security from reactive logging to **proactive prevention**.

PART 7: THE HVET

THE CRYPTOGRAPHIC FINGERPRINT

The **Hash-Verified Execution Trace** is the binding proof. It combines the Rule, Data, and Output into a single hash.

This formula is the mathematical "ticket" required to pass the Safety Gate.

$$HVET = HHR + HD + HO$$

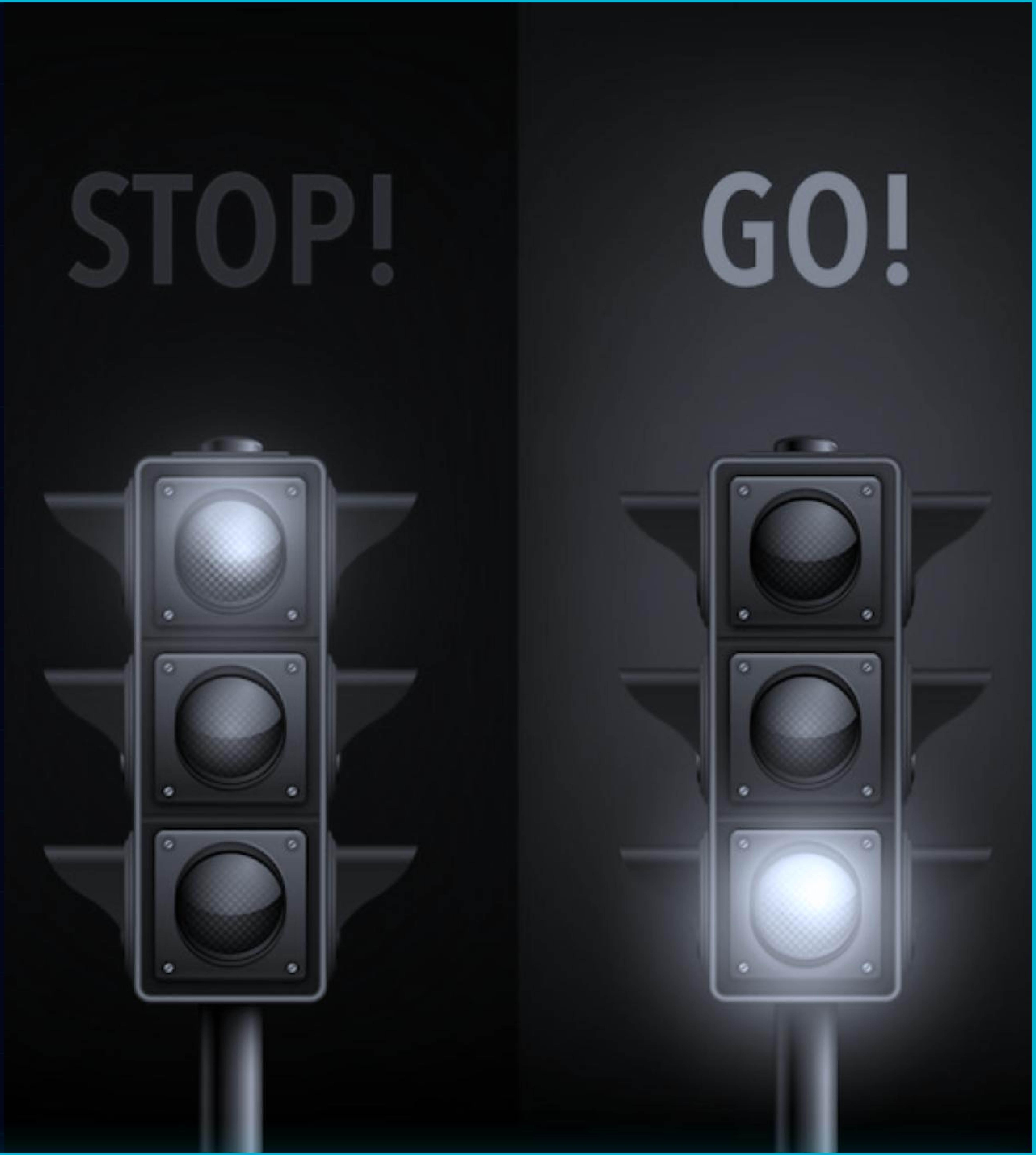
> IF PROOF FAILS, ACTION HALTS.

PART 8: THE SAFETY GATE

The Safety Gate is the **hardware-level enforcement** of Law L0. It protects against two types of failure:

PL-X (Physics-Level): Hardware corruption or sensor drift.

PS-X (Protocol-Subversion): Human fraud or coercion.



PART 9: THE COMPLETE SYSTEM

How NOVAK layers cryptographic principles into an active framework:

PRINCIPLE	NOVAK COMPONENT	FUNCTION
Hashing	HD, HR, HO	Ensures integrity of inputs/outputs.
Signatures	EIR (L6)	Binds identity to every action.
Chain Linking	RGAC (L7)	Ensures immutable history.
Pre-Action Proof	HVET	The "Key" to the Safety Gate.

PART 10: CONCLUSION

100%

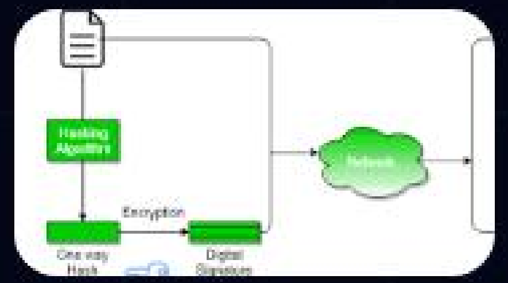
We move from **Trust-based** systems to **Proof-based** systems.

NO PROOF. NO ACTION.

IMAGE SOURCES

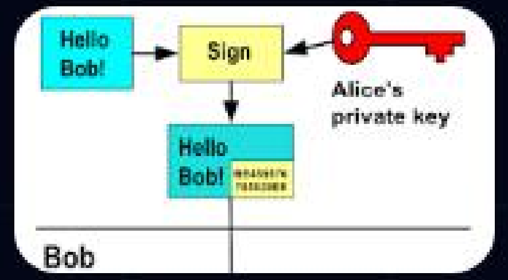
https://img.freepik.com/premium-photo/symbolizing-compromised-security-data-breach-vulnerability-digital-image-broken-padlock-concept-cybersecurity-breach-data-security-weakness-broken-padlock-compromised-protection_918839-95455.jpg

Source: www.freepik.com



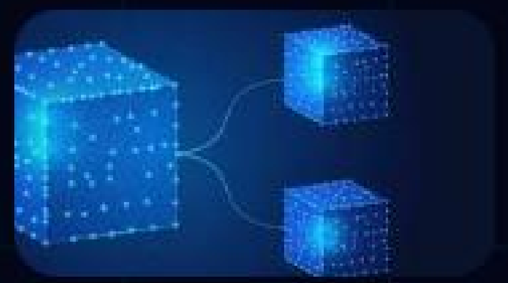
https://www.innokrea.pl/wp-content/uploads/2023/11/2-1.png

Source: www.innokrea.com



https://upload.wikimedia.org/wikipedia/commons/7/78/Private_key_signing.svg

Source: en.wikipedia.org



https://static.vecteezy.com/system/resources/previews/026/831/511/non_2x/polygon-of-blue-glowing-blockchain-cube-enhancing-security-and-efficiency-technology-network-concept-with-connected-digital-cubes-blocks-vector.jpg

Source: www.vecteezy.com

https://img.freepik.com/premium-vector/vector-3d-realistic-detailed-road-traffic-lights-icon-set-isolated-safety-rules-concept-design-template-stoplight-turned-traffic-lights-with-red-yellow-light-traffic-light-concept-banner_153563-6109.jpg

Source: cosmos-seguros.com.br