SNE Labs — SNE Vault Protocol

Sovereign Physical Infrastructure: A Dual-Kernel Architecture for Truth & Custody

Renan Melo
sneradar@gmail.com
https://snelabs.space/

Resumo

SNE Labs é um laboratório de pesquisa e engenharia focado em infraestrutura física para soberania digital. Unimos criptografia avançada, hardware dedicado e execução determinística na borda (edge computing) para transformar conceitos como *self-custody*, *trust minimization* e resistência à censura em propriedades técnicas verificáveis. O **SNE Vault** combina execução confiável em hardware físico, processamento determinístico local, provas on-chain de existência física (Proof of Uptime) e segregação rígida entre leitura de mercado e custódia. Este documento descreve a arquitetura do ecossistema, os fluxos de comunicação, a topologia de implantação e o modelo de governança e auditoria.

Sumário

1. VISÃO E PROPÓSITO

SNE Labs acredita que soberania operacional é, antes de tudo, física. Mobilizamos engenharia de hardware, primitives criptográficas e desenho de protocolo para que operadores individuais possuam e controlem a infraestrutura que lê o mercado e assina transações. Ao deslocar computação crítica para hardware controlado pelo operador, removemos pontos centrais de confiança e transformamos auditoria em prova técnica.

2. RESUMO EXECUTIVO DO SNE VAULT

O SNE Vault é uma arquitetura dual-kernel composta por:

- **SNE Radar (Intelligence Layer)** — execução read-only do motor determinístico de leitura de mercado (NTE) em memória volátil;
- **SNE Pass (Custody Layer)** — Secure Element (TPM/TEE) isolado responsável por chave raiz, assinaturas e políticas de acesso;
- **BitAxe / ASIC** — módulo físico que gera Proof of Uptime (PoU) por hashing contínuo;
- **Scroll L2 Registry** — registro on-chain para licenças, publicação de provas agregadas (Merkle roots) e governança SNIPs.

Pontos-chave: execução em **RAM volátil**, zero persistência de pesos/chaves legíveis em disco; tamper-resistance física com Zeroization; ingestão de dados por canais diretos (WebSockets/satélite) e prova on-chain da corporalidade do nó.

3. ARQUITETURA DO ECOSSISTEMA

3.1 Componentes e responsabilidades

Edge Node Unidade física composta por controlador (ARM/x86), SE (SNE Pass), BitAxe e chassi tamper-resistant. Executa ingestão, NTE e participa do PoU.

SNE Radar Pipeline de leitura de mercado que constrói $\mathbf{V}_t$ e executa o NTE em RAM — sem persistir pesos θ em armazenamento não-volátil.

SNE Pass Secure Element que guarda EK/SNE Physical Key, executa HKDF/Sign/monotonic counters e impõe políticas de ativação via handshake on-chain.

BitAxe (ASIC) Motor de resiliência que gera o heartbeat criptográfico usado no PoU.

Relayers & Aggregators Infraestrutura off-chain que coleta proofs dos nós, agrega em Merkle trees e publica roots na Scroll L2.

Scroll L2 (Registry) Autoridade on-chain para licenças, checkAccess (nodeID), publicação de proofs e coordenação de SNIPs (governança).

3.2 Topologia

A rede é uma malha descentralizada: cada Edge Node consome feeds diretamente, verifica licenças on-chain e participa do ecossistema sem depender de servidores centrais. Relayers são utilizados apenas para agregação e publicação de proofs.

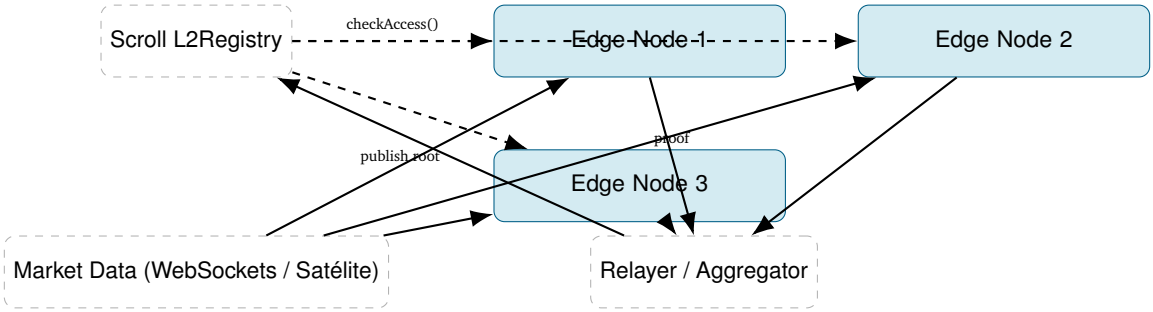

Figura 1: Topologia: Edge Nodes, Feeds, Relayers e Registry on-chain.

4. MOTOR DE INFERÊNCIA DETERMINÍSTICO (NTE)

4.1 Objetivo e desenho

O NTE converte sinais analíticos de múltiplos domínios em uma decisão normalizada. É determinístico, auditável e otimizado para execução vetorial (AVX-512 quando disponível).

4.2 Composição do estado

$$\mathbf{V}_t = [\mathbf{O}_t, \mathbf{T}_t, \mathbf{U}_t, \mathbf{B}_t, \mathbf{P}_t, \mathbf{D}_t]$$

Componentes: osciladores, indicadores de tendência, volume, bandas de volatilidade, heurísticas de padrão e fluxo DOM.

4.3 Função de Confluência

$$y_t = \text{Softmax}\left(\sum_{i \in Layers} w_i \cdot \text{Score}_i(\mathbf{V}_t) \right)$$

Pesos canônicos priorizam microestrutura e liquidez: exemplo $w_{MTF} = 3.0, w_{DOM} = 2.5, \ldots$

4.4 Segurança operacional

Pesos θ residem cifrados em storage (AES-256-GCM). Apenas após handshake válido (verificação on-chain e assinatura do operador) θ é decriptado em RAM e utilizado. Não há logs de decisão persistidos por padrão — quando necessário, commitments (hashes) podem ser publicados on-chain.

5. PROVA DE UPTIME (POU) E GOVERNANÇA

5.1 PoU — definição

BitAxe gera continuamente provas:

$$Proof_{uptime} = H(nonce, ID_{node}, timestamp)$$

Relayers agregam proofs em Merkle trees; a raiz é publicada na Scroll L2. Janela de contestação permite verificação e eventuais slashing.

5.2 Governança (SNIPs) e Poder de Voto

Poder de voto P_{voto} é proporcional ao histórico de PoU:

$$P_{voto} \propto \int_{t_0}^{t_{atual}} Proof_{uptime}(t)\, dt$$

SNIPs definem propostas de evolução do protocolo; a execução on-chain utiliza padrões Proxy para upgrades atômicos sem interromper nós ativos.

6. HANDSHAKES, CHAVES E ZEROIZATION

6.1 Handshake de ativação

1. Nó gera desafio/nonce n.
2. Operador assina: $\sigma = \text{Sign}(n, pk_{user})$.
3. Nó chama `checkAccess(nodeID)` no contrato SNELicenseRegistry.
4. Se válido, SNE Pass deriva K_{enc} (HKDF) e decripta blob θ (AES-256-GCM) em RAM.
   Formalmente:

$$Access_{True} \iff Verify(\sigma, pk_{user}, n) \ \wedge \ checkAccess(nodeID) = Valid$$

6.2 Zeroization e Tamper-Resistance

Chassi contém Tamper-Detection Line; violação interrompe alimentação do SE e purga RAM. Estado de chave:

$$StateKey = \begin{cases} \text{Active}, & \text{se TamperLine = Intact} \\ \varnothing, & \text{se TamperLine = Violated} \end{cases}$$

7. DISTRIBUIÇÃO, PROVISIONAMENTO E OPERAÇÃO

7.1 Tiers de produto

- **Tier 1 — Pro Node:** data-center-grade, AVX-512, para clientes institucionais.
- **Tier 2 — Edge Node:** dispositivos ARM/x86 para operadores menores.
- **Tier 3 — SNE Box:** hardware dedicado com SE, isolamento galvânico e módulo satélite opcional.

7.2 Cadeia de suprimento e provisionamento

Fabricante provisiona SE com Endorsement Key (EK) única; EK_pub, hash de firmware e metadados são registrados em repositório de atestacão (on-chain ou público). O reprovisionamento requer SNE Physical Key e atestado on-chain.

7.3 Atualizações e segurança de firmware

Measured boot, imagens assinadas (HW_sign & SW_sign) e possibilidade de rollback protegido. Atualizações críticas passam por SNIPs e janelas de teste; execução via Proxy Patterns.

8. MODELAGEM DE AMEAÇA E MITIGAÇÕES

8.1 Ameaças principais

Acesso físico (decapsulation, micro-probing), side-channels (DPA/SPA), remanência de DRAM, ataques de supply-chain, censura de feeds e ataques Sybil.

8.2 Mitigações

- Zeroization robusta e kill-switch galvânico.
- SE/TPM discrete com masked/threshold signatures quando aplicável.
- Filtragem e ofuscação de tráfego; múltiplos feeds autenticados (N_feeds ≥ 3).
- Testes QA: DPA/SPA, cold-boot experiments, decapsulation sampling.
- JTAG/UART desabilitados fisicamente; M-of-N para manutenção.

9. AUDITORIA, MÉTRICAS E CRITÉRIOS DE PRODUÇÃO

9.1 Métricas operacionais

Latência E2E (ingestão $\rightarrow$ V_t $\rightarrow$ inferência $\rightarrow$ assinatura) p50/p95/p99; latência de handshake; overhead de zeroization.

9.2 Critérios de aprovação

Sistema apto para produção apenas se:

- Contratos on-chain auditados formalmente;
- Nenhuma reutilização de nonces detectada;
- Testes físicos mostrarem resistência a extração sem destruição;
- RNG de hardware validado e entropia suficiente.

10. CONCLUSÃO E CHAMADO À AÇÃO

SNE Labs propõe um novo paradigma: soberania física como fundamento técnico para leitura de mercado e self-custody. O SNE Vault integra hardware tamper-resistant, execução determinística em memória volátil e provas on-chain para criar infraestrutura auditável, resistente e escalável. Convidamos pesquisadores, operadores e auditores a colaborar em pilotos e auditorias para tornar essa visão operacional.

A. APPENDIX A: RESUMO EXECUTIVO (PARA STAKEHOLDERS)

O que é SNE Labs? Laboratório que constrói infraestrutura física para soberania digital.
O que é SNE Vault? Um cofre-executor de leitura de mercado em hardware, com prova on-chain de existência física.
Por que importa? Remove dependência de nuvem/intermediários e transforma confiança em provas técnicas.

B. APPENDIX B: PSEUDOCÓDIGO HANDSHAKE DE ATIVAÇÃO

```
nonce = random(256)
send_to_operator(nonce)
sigma = operator_sign(nonce)
if verify(pk_user, nonce, sigma) and checkAccess(nodeID) == True:
    Kenc = HKDF(Kroot, info || nodeID || nonce)
    theta = AES256GCM_decrypt(blob_theta, Kenc)
    load_theta_into_RAM(theta)
else:
    deny_access()
```

C. REFERÊNCIAS SELECIONADAS

1. Melo, R. (2025). *SNE Vault: Infrastructure for Physical Digital Sovereignty*. SNE Labs Whitepaper.
2. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
3. Intel Corporation (2023). *Intel® AVX-512 Technical Documentation*.
4. Scroll.io (2024). *Scroll L2: The Community-First zkEVM Documentation*.
5. Haber, S., & Stornetta, W. S. (1991). *How to time-stamp a digital document*.