

# SNE Vault Protocol: Sovereign Physical Infrastructure

A Dual-Kernel Architecture for Truth & Custody

Renan Melo

sneradar@gmail.com

<https://snelabs.space/>

## Resumo

Propomos uma infraestrutura para processamento de sinais de mercado que elimina a dependência de provedores de nuvem centralizados. O sistema utiliza uma rede de nós de borda (edge nodes) para executar um motor de inferência determinístico em memória volátil, condicionado a um registro de licenças em uma rede de segunda camada (Scroll L2). A segurança da propriedade intelectual e das chaves privadas é garantida por uma arquitetura de segregação física e um mecanismo de autodestruição lógica (Zeroization) disparado por sensores de integridade do chassis. A prova de disponibilidade do sistema é mantida por um protocolo de Proof of Uptime (PoU) baseado em carga de trabalho computacional contínua em hardware dedicado.

## 1. INTRODUÇÃO

O comércio de ativos digitais depende fundamentalmente da segurança do material criptográfico. O armazenamento de chaves privadas em ambientes conectados à rede introduz vulnerabilidades intrínsecas, enquanto servidores centralizados representam pontos únicos de falha e impõem latência na propagação de dados de mercado. Embora soluções de hardware (cold wallets) mitiguem o risco de exfiltração de chaves, elas sacrificam a utilidade operacional e a capacidade de resposta automatizada em tempo real. Torna-se necessário um sistema que combine o isolamento de um ambiente de custódia física com a capacidade computacional de um nó de rede de alta performance. Neste artigo, propomos uma solução baseada em nós de borda (Edge Nodes) que utilizam instruções vetoriais ( $AVX - 512$ ) para processamento de sinais e conectividade direta para redução de latência. A arquitetura desacopla a verificação de acesso — registrada de forma imutável na rede *Scroll L2* — da execução da lógica analítica, que ocorre exclusivamente em memória volátil. Este design elimina a dependência em provedores de nuvem e garante a integridade soberana da execução.

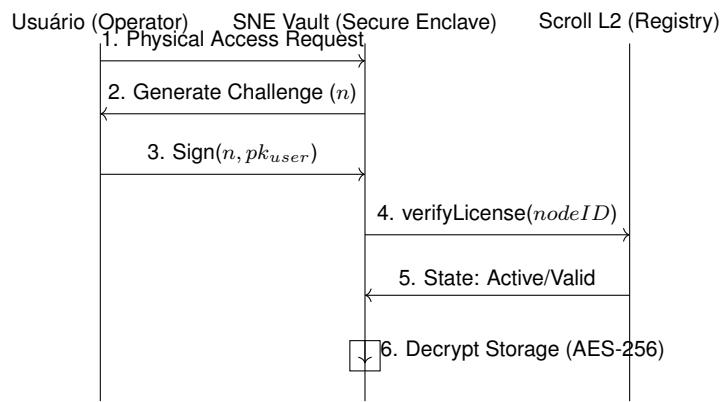


Figura 1: Protocolo de Abertura do Cofre: Validação Física e On-Chain [cite: 125-128].

## 2. DESCRIÇÃO DO NÓ DE BORDA

O Nó de Borda (Edge Node) é a unidade física de execução do protocolo, projetada para operar como um ambiente de computação isolado. A arquitetura do nó é dividida em duas camadas funcionais distintas: a Camada de Inteligência e a Camada de Resiliência. Esta separação garante que a integridade dos cálculos de mercado não seja comprometida por falhas na conectividade ou tentativas de manipulação externa.

### 2.1 Arquitetura Heterogênea

Para atingir o equilíbrio entre performance e segurança, o nó utiliza uma configuração de processamento heterogêneo:

- Módulo de Inteligência (Controlador de Borda):** Responsável pela ingestão de dados em tempo real e execução do Neural Trading Engine (NTE). Em instâncias de alta performance (Tier 1), o controlador utiliza instruções vetoriais  $AVX - 512$  para processar o tensor de estado  $V_t$  com latência submilissegundo.

**Módulo de Resiliência (Cripto-Acelerador ASIC):** Atua como o Root of Trust do hardware. Este módulo executa uma carga de trabalho de hashing contínua que serve como o batimento cardíaco (heartbeat) do sistema. A prova de trabalho gerada pelo ASIC é vinculada à identidade do nó na rede *Scroll L2*, impossibilitando a simulação de nós via instâncias virtualizadas em nuvem.

## 2.2 Ambiente de Execução Confiável e Memória Volátil

A lógica de decisão e os pesos do modelo  $\theta$  nunca são persistidos em armazenamento não-volátil em estado legível. Após o handshake bem-sucedido com o registro de licenças na *Scroll L2*, o NTE é descriptografado via *AES – 256* diretamente na memória RAM.

Este design garante que, em caso de interrupção de energia ou reinicialização do sistema, qualquer vestígio operacional da lógica proprietária seja eliminado. A execução em memória volátil protege a propriedade intelectual contra análise forense e extração física de dados.

## 2.3 Conectividade e Ingestão de Dados

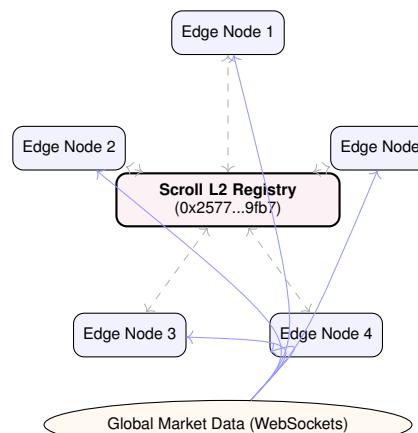
O nó é projetado para minimizar a dependência de infraestruturas terrestres de internet. A integração opcional com comunicação via satélite permite que o nó receba transmissões de dados de mercado diretamente, contornando gateways de Provedores de Serviço de Internet (ISP) que podem introduzir latência artificial ou censura de pacotes. O fluxo de dados segue o princípio de "Entrada Direta", onde o tensor  $V_t$  é construído localmente a partir de pacotes brutos (raw packets).

## 2.4 Especificações de Segurança Física (Tamper-Resistance)

O chassi do nó contém uma malha de sensores de continuidade elétrica (Tamper-Detection Line). Qualquer tentativa de abertura física do invólucro interrompe o circuito, disparando um evento de Zeroization de hardware. Este mecanismo remove instantaneamente a alimentação do elemento seguro onde residem as chaves de sessão, tornando o nó um dispositivo inerte e protegendo a custódia dos ativos e a lógica do sistema.

## 3. ESCALABILIDADE E TOPOLOGIA DA REDE

A rede é composta por nós independentes que operam em uma topologia de malha (mesh). Para eliminar o gargalo de servidores centrais, cada nó consome dados de mercado diretamente via protocolos de baixa latência (WebSockets) e verifica o estado de acesso de forma síncrona na rede *Scroll L2*. A escalabilidade horizontal é definida pela capacidade da rede de integrar  $N$  nós sem incremento na latência sistêmica, visto que o processamento é isolado e local.



Escalabilidade Horizontal:  $N$  Nós  $\rightarrow 0$  Impacto em Latência Sistêmica

Figura 2: Topologia de Rede: Processamento isolado e descentralizado[cite: 239, 264].

## 4. O MOTOR DE INFERÊNCIA DETERMINÍSTICO (NTE)

A soberania começa na capacidade de processar dados sem interferência. O Neural Trading Engine (NTE) utiliza uma função de agregação ponderada para converter sinais brutos em uma decisão binária ou probabilística de execução.

### 4.1 Função de Execução

A saída do sistema ( $y_t$ ) é um escalar de probabilidade calculado via função Softmax sobre a soma ponderada das camadas de análise::

$$y_t = \text{Softmax} \left( \sum_{i \in \text{Layers}} w_i \cdot \text{Score}_i(\mathbf{V}_t) \right) \quad (1)$$

### 4.2 Execução em Memória Volátil

A computação de  $y_t$  ocorre exclusivamente na memória RAM (Volátil). Os pesos do modelo ( $\theta$ ) são carregados apenas após a validação do handshake com a rede Scroll. Não há persistência de logs de decisão em disco, mitigando a análise forense em caso de apreensão física do dispositivo.

### 4.3 Composição do Tensor de Estado $V_t$

O estado do mercado no tempo  $t$  é representado por um tensor  $V_t \in \mathbb{R}^n$ , resultante da concatenação de seis domínios analíticos:

$$\mathbf{V}_t = [\mathbf{O}_t, \mathbf{T}_t, \mathbf{U}_t, \mathbf{B}_t, \mathbf{P}_t, \mathbf{D}_t] \quad (2)$$

Onde cada componente ( $O_t$  momentum,  $T_t$  tendência,  $U_t$  volume, etc.) é processado em tempo real via instruções vetoriais AVX – 512:

- $\mathbf{O}_t$ : Osciladores de Momentum  $\{RSI, Williams\%R, CCI\}$ .
- $\mathbf{T}_t$ : Indicadores de Tendência  $\{EMA_{8,21}, ADX, PSAR\}$ .
- $\mathbf{U}_t$ : Dinâmica de Volume  $\{MFI, OBV, VolumeProfilePOC\}$ .
- $\mathbf{B}_t$ : Bandas de Volatilidade  $\{KeltnerChannels, Donchian\}$ .
- $\mathbf{P}_t$ : Heurística de Padrões  $\{Wedges, Head\&Shoulders, Triangles\}$ .
- $\mathbf{D}_t$ : Fluxo DOM  $\{Bid/AskRatio, LiquidityDensity\}$ .

### 4.4 A Função de Confluência Ponderada

Diferente de modelos de aprendizado profundo, o NTE utiliza uma soma ponderada explícita seguida por uma função Softmax para normalização:

$$y_t = \text{Softmax} \left( \sum_{i \in \text{Layers}} w_i \cdot \text{Score}_i(\mathbf{V}_t) \right) \quad (3)$$

O protocolo impõe pesos canônicos que priorizam a microestrutura e a liquidez:

- $w_{MTF} = 3.0$  (Multi-Timeframe Dominance)
- $w_{DOM} = 2.5$  (Fluxo de Liquidez Imediato)

- $w_{ZONES} = 2.0$  (Zonas Magnéticas / Suporte e Resistência)
- $w_{SENT} = 1.5$  (Sentimento de Mercado / Fear & Greed)
- $w_{VOL} = 1.0$  (Volume Base)

#### 4.5 A Ontologia da Prova de Uptime (PoU)

O Proof of Uptime (PoU) é a formalização da corporeidade digital. Ele prova que o nó não é uma simulação em nuvem, mas um objeto físico ocupando espaço e consumindo energia.

A Carga de Trabalho do ASICO módulo de resiliência (BitAxe) executa uma função de hashing contínua  $H$  sobre um nonce  $n$  e o identificador do nó  $ID_{node}$ :

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

Este "batimento cardíaco" é enviado à rede Scroll L2 para validar a existência do hardware dedicado.

Poder de Voto e Governança Na governança (SNIPs), o peso do voto  $P_{voto}$  de um operador é uma função do seu histórico de disponibilidade comprovada:

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

Isso garante que aqueles que mantêm a integridade física da rede tenham maior autoridade sobre sua evolução.

#### 4.6 A Lógica de Zeroization e a Raiz de Confiança

A segurança final do protocolo é expressa por um estado binário absoluto condicionado à integridade física. O Estado da Chave ( $State_{Key}$ ) O acesso ao material criptográfico ( $Key_{session}$ ) em memória RAM volátil é regido pela integridade da Tamper-Detection Line :

$$State_{Key} = \begin{cases} Active, & \text{se } TamperLine = Intact \\ \emptyset, & \text{se } TamperLine = Violated \end{cases}$$

Uma violação física (*Violated*) interrompe o fluxo elétrico, resultando na purga instantânea ( $\emptyset$ ) das chaves de sessão e tornando o nó inerte.

#### 4.7 O Handshake de Ativação

A liberação das chaves em repouso ( $\theta$ ) exige uma assinatura do operador  $\sigma$  e a validação do contrato na Scroll :

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

Somente após essa validação síncrona o storage volátil é descriptografado via AES-256.

### 5. ESPECIFICAÇÕES DE HARDWARE E TOPOLOGIA

A rede opera em uma topologia de malha (mesh) onde nós de borda (Edge Nodes) comunicam-se diretamente com fontes de dados e validadores L2, sem servidores centrais de retransmissão.

#### 5.1 Verificação de Acesso (Scroll L2)

O controle de acesso utiliza a rede Scroll como um registro imutável de estado. O contrato inteligente atua como autoridade de carimbo de tempo, retornando um booleano de validação mediante assinatura criptográfica do nó.

## 5.2 Handshake de Ativação

O processo de inicialização do nó de borda segue o fluxo lógico em `license_manager.py`:

1. **Challenge:** O nó local gera um desafio aleatório.
2. **Signature:** O usuário assina o desafio com a chave privada vinculada à licença on-chain.
3. **Validation:** O contrato inteligente `0x2577...9fb7` verifica a validade da licença via `checkAccess`.
4. **Activation:** O NTE é descriptografado em memória RAM (AES-256) apenas se o estado da rede for favorável.

## 5.3 Arquitetura de Hardware (SNE Vault)

O nó físico é classificado em três níveis de capacidade computacional e segurança:

- **Tier 1 (Pro Node):** Servidores com suporte a instruções vetoriais AVX-512 para processamento de alta frequência.
- **Tier 2 (Edge Node):** Dispositivos de arquitetura ARM/x86 de consumo.
- **Tier 3 (SNE Box):** Hardware dedicado com Secure Enclave (TEE) e módulo de comunicação via satélite integrado. Este nível implementa isolamento galvânico entre o processador de chaves e a interface de rede pública.

## 5.4 Arquitetura Híbrida da SNE Box (Tier 3)

A **SNE Box** é implementada através de uma arquitetura de computação heterogênea, combinando um controlador de borda de propósito geral com um acelerador criptográfico de aplicação específica (ASIC)[cite: 88, 91]. Esta combinação visa garantir a integridade da leitura de mercado e a prova de existência física do nó.

- **Módulo de Inteligência (Raspberry Pi/ARM):** Atua como o *Edge Controller* e hospeda o **SNE Radar**[cite: 7, 91]. É responsável pela ingestão de dados via satélite/P2P, processamento do tensor de estado  $V_t$  e execução do motor determinístico NTE em memória volátil[cite: 40, 48, 95].
- **Módulo de Resiliência (BitAxe/ASIC):** Atua como o gerador de **Proof of Uptime (PoU)**[cite: 196, 198]. O BitAxe executa uma carga de trabalho computacional contínua (hashing) que serve como o *heartbeat* do sistema[cite: 199]. Esta atividade prova à rede Scroll L2 que o nó é uma unidade de hardware física dedicada e não uma instância virtualizada, mitigando ataques de Sybil[cite: 79, 142, 202].

## 5.5 Integração e Root of Trust

A integração entre o controlador ARM e o ASIC BitAxe estabelece o **Root of Trust** da SNE Box[cite: 156]:

1. **Sincronização de Prova:** O Raspberry Pi coleta os metadados de processamento do BitAxe e os encapsula no payload do *heartbeat* enviado para o contrato inteligente `0x2577...9fb7` na Scroll L2[cite: 85, 142, 199].
2. **Segregação de Chaves:** Enquanto o Raspberry Pi processa a lógica de mercado (*Intelligence Layer*), o **SNE Pass (Custody Layer)** opera no nível de privilégio máximo, garantindo que o material criptográfico nunca seja exposto ao tráfego de rede do ASIC[cite: 127, 129, 131].

3. **Kill Switch Físico:** O chassis da SNE Box interliga o sensor de intrusão à alimentação de ambos os módulos[cite: 145]. Uma violação física da *Tamper Line* dispara o **Zeroization** no Raspberry Pi (limpeza instantânea da RAM) e interrompe o hash no BitAxe, sinalizando a queda do nó na rede[cite: 151, 185, 186].

## 5.6 Fluxo de Dados

O sistema prioriza a conexão direta (P2P) ou via satélite para a ingestão de dados de mercado, contornando a latência introduzida por provedores de nuvem e gateways ISP tradicionais.

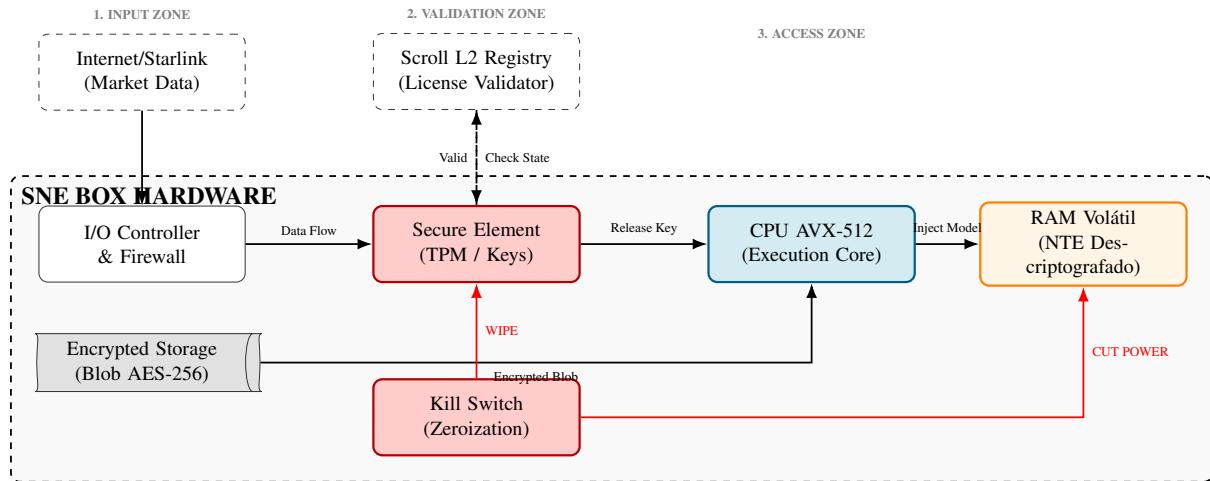


Figura 3: Fluxo Linear de Soberania: Input → Validação → Acesso (SNE Box Architecture)

## 5.7 Soberania Física: O Hardware como Refinaria

Para que a leitura de mercado seja verdadeiramente soberana, ela não pode ocorrer em "terra alheia". A latência de rede e a opacidade da nuvem introduzem incerteza.

O **SNE Box** (Tier 3) é redefinido aqui não apenas como um cofre, mas como uma Refinaria de Dados Pessoais.

- **Trusted Compute Base:** O hardware garante que os cálculos do NAE (AVX-512) ocorram em tempo real, sem disputa de recursos com outros usuários.
- **Isolamento de Ruído:** Ao conectar-se diretamente via Starlink e processar dados na borda, o SNE Box elimina a latência institucional, permitindo que o usuário "enxergue" movimentos de liquidez antes que eles sejam renderizados em interfaces web convencionais.

## 6. SNE PASS: NÚCLEO DE SOBERANIA E AUTO-CUSTÓDIA

O **SNE Pass** é definido como o Kernel de Segurança (Ring 0) do ecossistema SNE Vault, operando exclusivamente dentro do *Secure Element* (TPM 2.0)[cite: 125]. Sua função primária é a gestão de identidades e a geração de assinaturas criptográficas em ambiente isolado, garantindo que o material sensível jamais seja exposto ao *SNE Radar* ou a redes externas[cite: 126, 104].

Nota: o SNE Pass opera dentro do *Secure Element* (SE/TEE). Quando requerido processamento isolado (logic), utilizar um TEE certificado; para operações de chave (HKDF, Sign, monotonic counters) o SE/TPM provê interface segura, não execução arbitrária de código ring-0.

## 6.1 Arquitetura de Segregação (Airgap Lógico)

Diferente de sistemas de custódia centralizada, o SNE Pass implementa uma barreira determinística entre a inteligência de dados e a movimentação de ativos[cite: 128, 19].

- **SNE Radar (Intelligence Layer):** Atua em modo *Read-Only*, processando o tensor  $V_t$  para fornecer leitura de mercado em tempo real[cite: 129, 43, 68].
- **SNE Pass (Custody Layer):** Detém o privilégio exclusivo de escrita e acesso ao *Secure Enclave*[cite: 130]. Não possui dependência lógica dos resultados gerados pelo SNE Radar para manter a integridade das chaves[cite: 131, 118].

## 6.2 Hierarquia de Autorização Multinível

O acesso total ao ecossistema é governado pela tríade de validação:

$$AuthStatus = (Key_{Phys} \wedge \sigma_{user} \wedge State_{Scroll}) \implies Access = True \quad (4)$$

## 6.3 Protocolo de Assinatura e Handshake de Ativação

O acesso ao material criptográfico em repouso ( $\theta$ ) é condicionado a um desafio multi-etapas registrado na rede Scroll L2[cite: 133, 93, 96]:

1. **Desafio ( $n$ ):** O nó local gera um *nonce* aleatório  $n \in \{0, 1\}^{256}$ [cite: 134].
2. **Assinatura do Operador ( $\sigma$ ):** O usuário realiza a assinatura digital do desafio:  $\sigma = Sign(n, pk_{user})$ [cite: 135].
3. **Validação On-Chain:** O contrato SNELicenseRegistry (0x2577...9fb7) verifica o booleano de acesso via `checkAccess (nodeID)` [cite: 136, 98].
4. **Liberação de Chave:** Somente após a validação síncrona, o SNE Pass descriptografa o *storage* volátil via AES-256 para permitir a assinatura de transações[cite: 137, 99, 122].

## 6.4 Soberania Física: Mecanismo de Zeroization

A *Self-Custody* é protegida contra vetores de ataque físicos (extração de hardware) através de um circuito de *Kill Switch* galvânico[cite: 139, 163, 164].

$$State_{Key} = \begin{cases} Active, & \text{se } TamperLine = \text{Intact} \\ \emptyset, & \text{se } TamperLine = \text{Violated} \end{cases} \quad (5)$$

A violação da *Tamper-Detection Line* no chassi interrompe a alimentação do *Secure Element*, resultando na purga instantânea (*Zeroization*) das chaves digitais momentâneas, tornando os dados operacionais permanentemente inacessíveis a terceiros[cite: 145, 165, 167].

## 6.5 Interação com Wallets Físicas

O SNE Pass atua como um orquestrador de *Self-Custody*, permitindo a integração de dispositivos externos via interface isolada[cite: 147]. O SNE Radar fornece a leitura de mercado para suporte à decisão humana, mas a assinatura final é delegada ao SNE Pass, exigindo prova de presença física (PoP) para qualquer transação externa[cite: 148, 11, 105].

## 6.6 SNE Physical Keys: A Raiz de Confiança (Root of Trust)

Diferente das chaves de sessão voláteis, a **SNE Physical Key** é o componente de hardware persistente que ancora a identidade soberana do sistema.

A **SNE Physical Key** NÃO contém nem exporta Kroot. Sua função é autenticar o operador para um processo de reprovisionamento seguro: após verificação física e on-chain, o SE gerará um novo Kroot (ou re-selará o anterior) sob política estrita de manufatura/operador, sendo todo o processo atestado via quote.

- **Preservação de Ativos:** Enquanto o *Zeroization* elimina a lógica do NTE e chaves de sessão em RAM, a SNE Physical Key permanece íntegra, permitindo a recuperação da custódia pelo operador legítimo.
- **Derivação de Estado:** A chave física atua como o requisito mandatório para "despertar" o nó após um evento de segurança, sendo necessária para descriptografar os pesos  $\theta$  em repouso.

## 6.7 Protocolo de Ressurreição Operacional (Post-Zeroization Recovery)

O fluxo de recuperação garante que a soberania física prevaleça sobre a destruição lógica:

1. **Restauração Física:** Validação da integridade da *Tamper Line* no chassi do *SNE Box*.
2. **Handshake de Hardware:** Reconhecimento da SNE Physical Key pelo *Secure Element*.
3. **Re-Instanciação de Memória:** Nova validação síncrona na Scroll L2 para regenerar as chaves voláteis de operação.

## 7. MODELAGEM DE AMEAÇA E SEGURANÇA FÍSICA

O protocolo assume um modelo de adversário com acesso físico ao dispositivo. A segurança baseia-se na impossibilidade de extração de chaves sem destruição do hardware.

### 7.1 Camadas de Proteção do IP (NTE)

- **Camada 1: Filtragem de pacotes e ofuscação de tráfego.)** – A primeira linha de contato, onde tráfego malicioso é filtrado antes de tocar o hardware.
- **Camada 2: Invólucro com sensores de integridade.)** – A barreira física do chassi proprietário.
- **Tamper-Detection Line** – A fronteira crítica. Qualquer violação física deste limite dispara o protocolo de *Zeroization* (auto-destruição das chaves).
- **Camada 3: Dados criptografados em repouso (AES-256.)** – Onde os pesos  $\theta$  residem como *blobs* AES-256 inúteis sem a chave volátil.
- **Camada 4: RAM Volátil (Execução)** – O único local onde o NTE existe em texto plano, e apenas durante a operação validada.

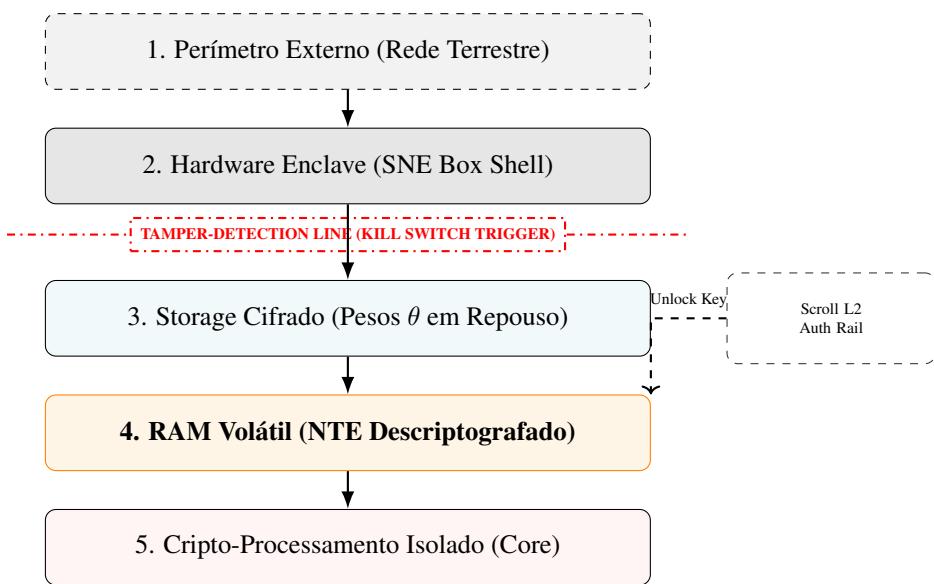


Figura 4: Modelo de Cebola: Hierarquia de Camadas de Proteção e Ponto de Ruptura (Tamper Line)

## 7.2 Mecanismo de Zeroization (Kill Switch)

A proteção contra extração física de dados é implementada através de um circuito galvânico de detecção de intrusão (Tamper-Detection Line). O estado das chaves criptográficas é definido como:

$$\text{State}_{\text{Key}} = \begin{cases} \text{Active} & \text{se TamperLine} = \text{Intact} \\ \emptyset & \text{se TamperLine} = \text{Violated} \end{cases}$$

A violação do perímetro físico resulta na purga instantânea da memória RAM e na interrupção da alimentação do elemento seguro.

## 8. GOVERNANÇA E EVOLUÇÃO DO PROTOCOLO

A atualização dos parâmetros do sistema e pesos canônicos é gerida on-chain através de votação ponderada por licença (License-Weighted Voting).

### 8.1 Gestão de Parâmetros e Propostas (SNIPs)

Mudanças na lógica do NTE ou nos parâmetros de risco são submetidas via SNIPs. A implementação técnica utiliza padrões de Proxy, permitindo a atualização atômica da lógica do contrato sem interromper a operação dos nós ativos. O poder de voto é proporcional ao tempo de atividade (uptime) comprovado do nó.

- **Votação por Stake:** O poder de voto é diretamente proporcional ao tempo de posse e integridade do nó no contrato SNELicenseRegistry.
- **Execução via Proxy:** Para evitar interrupções na inferência, atualizações de lógica são implementadas via *Proxy Patterns* (OpenZeppelin), garantindo transições de estado atômicas sem *downtime* no *Edge Node*.

## 9. CONSENSO E DISPONIBILIDADE

A integridade da rede é mantida através do mecanismo de Prova de Uptime (*Proof of Uptime* - PoU). Este protocolo assegura que apenas nós com hardware verificado e conectividade estável participem da validação e governança, mitigando a atuação de atores maliciosos intermitentes.

### 9.1 Proof of Uptime (PoU)

A integridade da rede é mantida por registros periódicos de atividade. Nós ativos emitem periodicamente uma prova criptográfica (*heartbeat*) que é registrada imutavelmente na rede Scroll. Este mecanismo assegura que apenas hardware verificado participe da governança do protocolo. O poder de voto em propostas de atualização (SNIPs) é proporcional ao histórico de disponibilidade (uptime) comprovado e à integridade do nó. Este registro cumpre duas funções críticas:

1. **Auditória de Conformidade:** Valida que o *hardware* do nó (SNE Vault) mantém a integridade do *Secure Enclave* e não sofreu violação física.
2. **Resistência Anti-Sybil:** A exigência de uma prova de trabalho computacional associada ao *heartbeat* previne a criação de múltiplos nós falsos, garantindo que cada voto de governança corresponda a uma unidade física de processamento real.

O incentivo econômico é estruturado para alinhar a segurança do nó com a recompensa do operador. Ao condicionar a participação na rede à verificação criptográfica contínua, o sistema torna ataques de negação de serviço ou injeção de dados falsos economicamente inviáveis em comparação à operação honesta do protocolo.

## 10. CONCLUSÃO

Este documento descreveu o protocolo SNE Vault como uma infraestrutura fundamental para a soberania digital física[cite: 1, 115]. A arquitetura apresentada resolve o compromisso histórico entre a segurança do armazenamento passivo (*cold storage*) e a utilidade da leitura de mercado em tempo real através da implementação de um Ambiente de Execução Confiável (*Trusted Execution Environment - TEE*) em hardware dedicado[cite: 8, 9, 189].

Ao segregar estritamente a inteligência de dados (SNE Radar) da gestão de chaves (SNE Pass), o sistema elimina a necessidade de confiança em terceiros e a exposição a latências institucionais[cite: 19, 134]. O SNE Radar assegura a integridade da leitura do mercado via processamento vetorial (AVX-512) local [cite: 18, 102], enquanto o SNE Pass garante que a *self-custody* permaneça sob controle absoluto e físico do usuário.

A integração de mecanismos de *zeroization* e o registro de *Proof of Uptime* na rede Scroll L2 asseguram que a extração de material criptográfico seja computacional e fisicamente inviável sob qualquer modelo de adversário[cite: 10, 163, 179, 191]. Em última instância, o SNE Vault não atua como um agente de execução, mas como a refinaria tecnológica que devolve ao indivíduo a capacidade de enxergar e transacionar na economia digital de forma verdadeiramente soberana[cite: 132, 192].

## APPENDIX A: GERENCIAMENTO DE MEMÓRIA E VETORIZAÇÃO

A eficiência do **SNE Radar** e a segurança do **SNE Pass** dependem da manipulação direta de hardware e memória volátil.

## 11. REFERÊNCIAS

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*. bitcoin.org.
3. Haber, S., & Stornetta, W. S. (1991). *How to time-stamp a digital document*. Journal of Cryptology.
4. Intel Corporation. (2023). *Intel® Advanced Vector Extensions 512 (Intel® AVX-512) Technical Documentation*.
5. Scroll.io. (2024). *Scroll L2: The Community-First zkEVM Documentation*.
6. Merkle, R. C. (1980). *Protocols for public key cryptosystems*. IEEE Symposium on Security and Privacy.