

WCDPQ

Verifiable Velocity

Liquidez global, execução verificável e controle que permanece com o titular da conta

Spot · Perpetuals · Early-Stage Allocation

Desenho de Protocolo · Arquitetura de Risco · Modelo Criptoeconômico

WHITEPAPER · VERSÃO 1.0

Sumário

Resumo

1.0 A Lacuna de Acesso do Varejo

2.0 Visão Geral do Sistema

3.0 Garantia Criptográfica

4.0 Topologia Modular

5.0 A Pilha de Produtos com Segregação de Risco

6.0 Acesso via Stablecoin e Liquidação Financeira

7.0 AI Sentinel e Execução Restrita por Política

8.0 Democratização de Capital

9.0 WCDP: Utilidade do Protocolo e Economia Sustentável de Recursos

10.0 Governança de Parâmetros

11.0 Equipe de Arquitetura Central

12.0 Roadmap de Evolução

13.0 Fatores de Risco, Divulgações e Apêndices

Apêndice: Especificações do Sistema de Prova Criptográfica

Resumo

O WCDPQ especifica uma arquitetura de protocolo aberto para roteamento

verificável de liquidez, liquidação de alta performance e verificação de custódia de ativos em modelo não custodial, projetada para corredores mobile-first. O problema de projeto que este documento aborda é o fato de o usuário de varejo não dispor de meio prático para verificar o estado de uma plataforma que custodia o seu saldo; as opções disponíveis têm sido ler um relatório contratado pela própria plataforma ou sacar os recursos.

O protocolo responde com três mecanismos. Saldos e movimentações são comprometidos em uma estrutura de passivos Merkle-sum com provas de conhecimento zero agregadas recursivamente, publicadas a cada época, de modo que o titular de uma conta possa verificar a sua própria inclusão por meio de um celular e uma parte independente possa verificar o estado agregado sem software fornecido pelo protocolo. A execução roda sobre um núcleo de matching shardizado, com sequenciamento determinístico e relógio unificado, o que torna o replay possível e permite atribuir a latência a um subsistema específico, em vez de a uma impressão subjetiva. Os canais Spot, Perpetuals e Launch mantêm colaterais separados, protegidos por gates aplicados no ledger, de modo que uma falha em um deles não alcança os demais.

O WCDP é o token utilitário por meio do qual os recursos operacionais da rede são alocados e validados, incluindo staking de verificação, computação medida e ponderação de governança. As distribuições de taxas da rede são geridas de forma transparente por meio de reservas algorítmicas do protocolo. O protocolo não faz qualquer declaração ou representação quanto ao valor de mercado ou à liquidez secundária do WCDP.

1.0 A Lacuna de Acesso do Varejo

Um participante de varejo em um mercado emergente dispõe hoje de mais plataformas para escolher do que em qualquer momento da história desses mercados, e de menos razões para confiar a qualquer uma delas dinheiro que não pode perder. A lacuna em torno da qual este documento se organiza não é escassez de plataformas. É a distância entre o que um usuário baseado em celular consegue alcançar e o que aquela tela de fato lhe permite fazer — e quão pouco do meio do caminho ele consegue inspecionar.

1.1 Três Atritos

Colocar dinheiro para dentro e para fora é o primeiro obstáculo e, para um usuário fora dos grandes centros financeiros, costuma ser o decisivo. Os trilhos bancários em boa parte da América Latina liquidam rapidamente — um usuário ali está acostumado a ver uma transferência chegar antes de pousar o celular —, mas a rota de uma conta local até uma plataforma que precifica em dólares ou stablecoins não é um salto único. Ela atravessa um provedor de pagamentos, uma etapa de liquidação financeira e uma conversão de moeda, cada um com seus próprios horários, limites e modos de falha. Uma plataforma que recebe os recursos no dia útil seguinte não falhou em nada em particular; ela simplesmente herdou o ritmo do corredor que está por trás dela, e o usuário experiencia isso como dinheiro parado em algum lugar que ele não consegue enxergar.

A lacuna de execução é mais estreita de descrever e mais difícil de fechar. O que uma mesa profissional tem e o usuário de celular não tem não é, primariamente, uma conexão mais rápida. É o ferramental em torno da ordem: a capacidade de trabalhar uma entrada ao longo do tempo em vez de aceitar o preço na chegada, de definir saídas condicionais que sobrevivem ao trader adormecer, de ver o quanto suas posições se tornaram correlacionadas antes que a correlação importe, e de saber onde a liquidez do livro realmente está, e não apenas onde o topo dele é exibido. Nada disso exige habilitação especial, e tudo isso está ausente das interfaces disponíveis à maior parte dos usuários de varejo nesses mercados. O usuário absorve a diferença como slippage, como saídas perdidas durante a noite, como um portfólio que acabou se revelando uma única posição.

O terceiro atrito diz respeito ao que o usuário consegue estabelecer por conta própria. Um titular de conta de varejo nunca teve meio prático de responder a perguntas básicas sobre a plataforma que custodia o seu saldo — se os ativos estão onde a plataforma diz que estão, se o seu próprio saldo está incluído em qualquer número publicado, se o número que ele vê na tela corresponde a um estado demonstrado, e não apenas afirmado. Historicamente, a resposta disponível tem sido ler algo contratado pela plataforma ou sacar. Nenhuma das duas é um padrão de evidência razoável para alguém conferindo uma posição às duas da manhã, e o fato de participantes institucionais negociarem arranjos privados de reporte enquanto o varejo não tem nada é uma diferença na qualidade da informação sobre a qual cada lado age.

Esses três atritos interagem. Um usuário que não consegue verificar a plataforma manterá o saldo pequeno, o que limita quanto capital ele colocará atrás de uma estratégia que o exige. Um usuário sem ferramentas de ordem trabalhada não manterá posição overnight, que é justamente onde uma visão direcional remunera. O efeito composto é um usuário que opera pequeno, opera rápido e opera apenas o que pode perder — o que não é a descrição de uma população com apetite elevado a risco, mas de uma população que precificou corretamente a plataforma.



1.2 O Trader Mobile-Native

O usuário para quem este sistema foi construído faz tudo no celular, e o celular está frequentemente em uma rede que cai. Sua sessão começa em um aplicativo de mensagens e termina em uma posição, sem nada no meio que se pareça com um fluxo de pesquisa. Ele se sente confortável mantendo saldo em stablecoin e desconfortável deixando dinheiro em moeda local por uma semana. Instrumentos derivativos não lhe são estranhos; o segundo conselho de trading mais comum em suas comunidades diz respeito a alavancagem, e não a spot.

Duas propriedades decorrem disso para o sistema. As requisições precisam sobreviver à repetição, porque em uma conexão ruim o usuário apertará enviar mais de uma vez e o cliente fará retry, e nenhum dos dois pode produzir duas ordens. E a interface precisa distinguir com clareza o que está ao vivo do que está sendo lembrado de antes, já que um preço que parou de atualizar há quatro segundos parece idêntico a um preço corrente, a menos que o desenho force uma diferença visual.

As expectativas de latência nessa população são definidas pelo aplicativo de mensagens que ela usou cinco minutos antes. Isso estabelece um piso de responsividade, mas não de confiabilidade: um usuário tolera trezentos milissegundos e não tolera uma ordem que trava sem resolução. O restante deste documento pondera a confiabilidade de acordo com isso, razão pela qual o comportamento de degradação do §4.3 reserva capacidade para saídas e o cliente do §4.4 se recusa a submeter ordens que aumentam exposição sem uma ida e volta ao servidor.

1.3 Corredores de Mercados Emergentes como Super-Nós de Execução

Corredores de mercados emergentes de alta velocidade servem como referência operacional para a arquitetura do protocolo.

Infraestruturas regionais de pagamento na América Latina — caracterizadas por expectativas de liquidação bruta instantânea e densidade de varejo mobile-first — fornecem as condições de base rigorosas necessárias para submeter a teste de estresse a verificação criptográfica de alta frequência. Projetar para ambientes com dinâmica volátil de moeda fiduciária doméstica e demandas de alto throughput garante que os mecanismos subjacentes de comprometimento de estado permaneçam resilientes sob restrições de rede não triviais.

O que o protocolo implanta é um template de infraestrutura: um padrão de adapter para conectividade multi-trilho, parâmetros de risco unificados e sincronização de borda móvel. A arquitetura é agnóstica a corredor, tratando gateways locais como implementações independentes de uma interface padrão de liquidação financeira, e não como implantações sob medida.



1.4 Tese de Design

Os cinco invariantes apresentados no §2.1 constituem o conteúdo operacional da tese aqui defendida. Em termos simples: o estado sob controle da plataforma deve ser conferível por partes que não trabalham para a plataforma; o resultado de uma ordem deve ser determinado por regras publicadas, e não por acidentes de temporização no software; uma falha em um produto não deve alcançar o colateral de outro; a rota entre uma conta local e um saldo de negociação deve ser construída de modo que adicionar um corredor seja configuração, e não construção; e o token da rede deve ser exigido por funções operacionais reais, e não oferecido como instrumento de fidelidade.

Nenhum desses pontos é incomum como valor de engenharia. O que é incomum é aplicá-los onde as contrapartes são usuários de varejo em celulares com saldos pequenos, e aceitar os custos que decorrem disso — as obrigações de divulgação, a eficiência de capital reduzida pelo isolamento, a performance deixada na mesa por sistemas de prova transparentes, o trabalho de corredor que não pode ser pulado contornando um regulador. O restante deste documento é, em grande medida, uma descrição desses custos e dos mecanismos que os assumem.

2.0 Visão Geral do Sistema

Este capítulo situa as cinco camadas e, em seguida, declara contra o que o sistema não foi construído para se defender. A segunda metade é a mais útil para quem está avaliando a primeira.

2.1 Invariantes do Protocolo e Arquitetura em Camadas

Estado verificável. Saldos, movimentações e a correspondência entre eles são comprometidos em um formato que uma parte externa pode conferir. O sistema de prova e o ledger que o sustenta são definidos uma única vez no Cap.3.

Execução determinística. Entradas idênticas produzem ordenações idênticas em todo replay. A disciplina de sequenciamento e as razões pelas quais a arquitetura aceita pagar por ela em latência entre shards estão no Cap.4.

Segregação de risco. Spot, Perpetuals e participação em lançamentos mantêm colaterais separados, com gates unidirecionais entre eles, aplicados no ledger. O Cap.5 define as fronteiras; o funding do pool de isolamento é tratado no §9.5.

Abstração de liquidação financeira. Os corredores se conectam por meio de um contrato de adapter, e não por integrações codificadas em duro, o que é justamente o que permite adicionar um corredor sem alterar a plataforma. Cap.6.

Utilidade do token vinculada a recursos. O WCDP é exigido para funções operacionais — validação, computação medida, elegibilidade a alocação, peso de governança —, e não oferecido como desconto. Cap.9.

As camadas se empilham na ordem em que a confiança flui.

Camada	Função	Capítulo
Verificação	Geração de provas, compromissos, interfaces de verificador	3
Execução central	Contas, dados de mercado, matching, risco, ledger	4
Canais de produto	Spot, Perpetuals, Launch	5
Inteligência	Telemetria, sentinelas, compilação de intenções	7
Acesso e liquidação financeira	Adapters de corredor, roteamento de stablecoin, borda do cliente	6

Dois fluxos entre camadas merecem ser nomeados, porque não são óbvios a partir da tabela. Sinais de risco vindos da camada de inteligência sobem para dentro da máquina de estados de degradação descrita no §4.3 e para dentro do caminho de liquidação, o que significa que uma entidade fora do núcleo de matching pode influenciar decisões de admissão; as restrições sobre essa influência são o objeto do §7.2. Compromissos de prova descem da verificação para a borda do cliente, e é assim que um celular acaba executando trabalho de verificação localmente, em vez de ler uma página de status. Nenhum dos fluxos é uma dependência no sentido comum de pilha de chamadas; ambos são interfaces definidas, com contratos publicados, e cada um é delimitado de modo que a camada inferior não possa ser usada como substituta das obrigações da superior.



2.2 Modelo de Ameaças, Premissas de Confiança e Não-Objetivos

O adversário contra o qual esta arquitetura foi escrita é um insider com acesso legítimo, e não um atacante externo. A intrusão externa é um risco real e é tratada por meios convencionais — distribuição de chaves, separação de acessos, monitoramento —, mas é uma categoria resolvida, no sentido de que as defesas são bem compreendidas. Um operador capaz de mover um saldo, alterar uma taxa ou suprimir um relatório sem deixar rastro detectável por outra pessoa é o problema mais difícil, e é esse o problema que a camada de verificação endereça.

Três premissas são adotadas e não provadas.

A primeira é que as funções de hash usadas nos compromissos mantêm resistência a colisão e que os parâmetros do FRI publicados no Apêndice permanecem sólidos no nível de segurança declarado. Uma quebra aqui invalida provas, e não ativos, e o caminho de migração é uma decisão de governança que não pode ser pré-comprometida em detalhe.

A segunda é que as entradas externas são aquilo que afirmam ser. Mark prices compostos, confirmações de pagamento e dados de referência entram como valores atestados, de fontes nomeadas. O sistema os filtra, limita sua influência e registra seu uso. Ele não estabelece de forma independente que uma confirmação proveniente de um gateway parceiro corresponde a recursos liquidados nos próprios livros do parceiro. Execução correta sobre uma entrada errada produz um resultado errado corretamente provado.

A terceira é que pelo menos algumas partes independentes de fato verificarão. Toda afirmação criptográfica neste documento é uma afirmação sobre o que um ator motivado *consegue* conferir a baixo custo. Se ninguém conferir, os compromissos são decoração. A mitigação do protocolo é tornar a verificação trivialmente barata e publicar falhas de forma ruidosa, o que eleva o custo de um comportamento indevido não percebido sem eliminá-lo.

O que o sistema não tenta fazer é tão delimitado quanto a lista acima, e mais curto do que um leitor poderia esperar de um documento deste tamanho.

Ele não tenta eliminar risco de mercado, e nenhum mecanismo aqui altera o fato de que uma posição alavancada pode perder mais do que a conta possui. Não tenta remover a necessidade de entidades legais, licenças ou decisões de produto específicas por jurisdição; a posição societária descrita no §13.2 existe precisamente porque a verificação criptográfica endereça alegações de solvência, e não a situação regulatória. Não oferece uma plataforma de contratos inteligentes de propósito geral, uma rede pública ou uma camada de liquidação financeira para aplicações de terceiros. E não reivindica ser descentralizado no sentido em que o termo é usado na literatura de governança — o controle de parâmetros é um escopo delimitado e publicado, que o Cap.10 especifica, e chamar isso de governança comunitária seria uma descrição incorreta na direção lisonjeira.

3.0 Garantia Criptográfica

Quem quer que mantenha saldo em uma plataforma que custodia ativos teve historicamente duas formas de formar um juízo sobre essa plataforma: ler um relatório escrito por uma firma que a plataforma paga, ou sacar. Nenhuma das duas está disponível a um usuário de varejo conferindo uma posição no celular às duas da manhã. Este capítulo descreve a terceira opção que o protocolo constrói, e dedica esforço comparável a onde essa opção deixa de alcançar.

3.1 O que Pode Ser Verificado

A camada de verificação faz três afirmações distintas, e elas não devem ser confundidas entre si, porque falham de maneiras diferentes.

A primeira é **cobertura de reservas**: em cada época de oferta ε, os ativos que a plataforma controla e colocou dentro do perímetro provado excedem os passivos que a plataforma enumerou. A segunda é **inclusão de passivos**: o saldo de um titular de conta específico é uma folha do conjunto de passivos comprometido, com um valor que o titular pode conferir sem confiar em ninguém. A terceira é **validade de transição de estado**: o ledger passou do compromisso $C\varepsilon$ *para* $C\varepsilon{+}1$ aplicando o conjunto de regras publicado, e nenhuma outra transição poderia ter produzido aquele par.

Cobertura, inclusão e validade de transição são, cada uma, verificáveis por uma parte independente. Nenhuma delas é uma afirmação sobre a empresa como um todo, e o §3.5 traça essa linha com precisão.Uma atestação assinada e uma prova de validade têm modos de falha diferentes, que é a razão prática pela qual o protocolo constrói para a segunda. Uma atestação registra o que um profissional nomeado concluiu sobre um snapshot, e seus riscos residuais residem em amostragem, escopo de contratação e intervalo de recorrência. Uma prova é um objeto conferível por máquina cuja falsidade é, ela própria, evidência. A frequência importa aqui. Solvência conferida trimestralmente, ou anualmente, é uma afirmação sobre um estado do mundo que já transcorreu; solvência conferida a cada época é uma afirmação sobre a época corrente, e a distância entre o que é afirmado e o que é verdadeiro permanece curta o suficiente para o usuário agir sobre ela.

Code is Law é usado neste documento como restrição de projeto, e não como slogan. Significa que poderes discricionários são enumerados, codificados em circuito quando possível e delimitados quando não. Onde uma regra é política e não aritmética — quais contrapartes podem ser admitidas, como se resolve uma

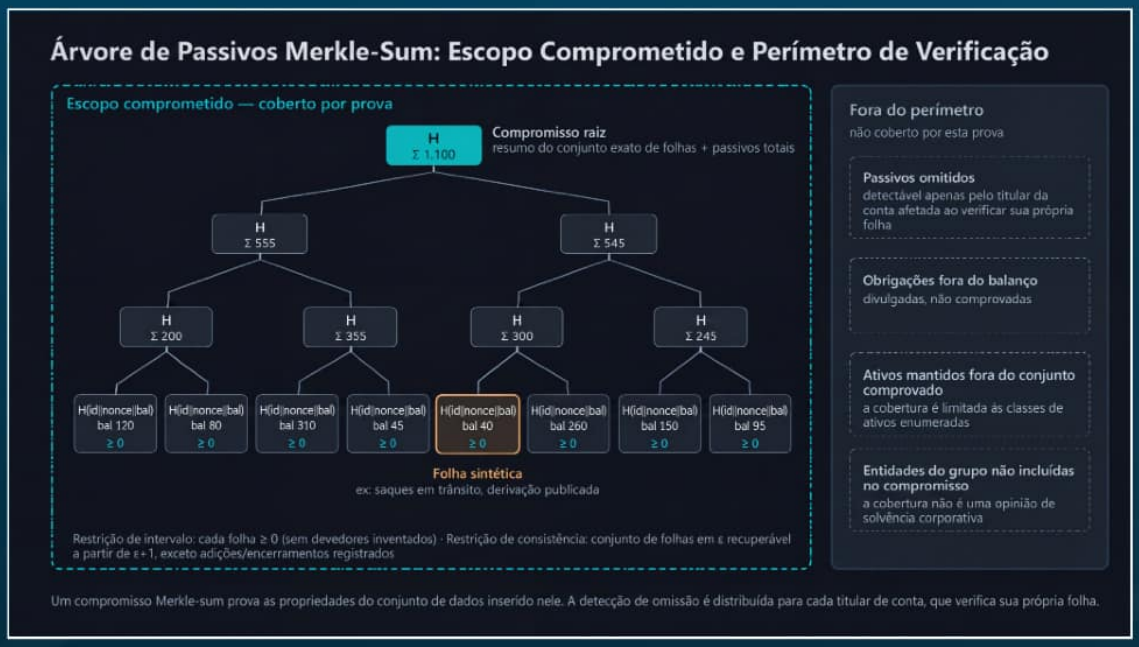
alocação de lançamento disputada —, o dispositivo de compromisso do protocolo é publicação mais detecção: a regra é escrita, sua invocação é registrada em log, e qualquer desvio da regra escrita é observável por uma parte que não deveria estar envolvida. O código restringe o que pode ser feito em silêncio. Ele não restringe o que pode ser feito abertamente e mal, e o leitor deve manter essa distinção em vista ao longo do restante deste capítulo.

3.2 Compromissos de Passivos em Merkle-Sum

O conjunto de passivos é comprometido como uma árvore Merkle-sum. Cada folha contém um compromisso cegado H(account_id ‖ nonce ‖ balance), de modo que a árvore não publique uma lista endereçável de clientes e saldos. Cada nó interno carrega um hash e a soma aritmética dos saldos abaixo dele. A raiz, portanto, publica duas coisas ao mesmo tempo: um digest criptográfico que vincula o conjunto exato de folhas e um valor de passivo total que qualquer verificador pode ler diretamente do compromisso. Uma plataforma não pode revisar o total sem alterar a raiz, e não pode alterar a raiz sem deixar evidência da revisão no log.

Duas famílias de restrições fecham os ataques óbvios. Restrições de intervalo em cada folha excluem saldos negativos, o que, de outra forma, permitiria reduzir a soma inventando um devedor. Restrições de consistência entre raízes consecutivas garantem que o conjunto de folhas da época anterior é recuperável a partir do atual, exceto por entradas explicitamente adicionadas ou encerradas, com essas operações registradas. O ataque residual é a omissão, e ele merece tratamento direto, porque implementações publicadas dessa ideia frequentemente o escamoteiam.

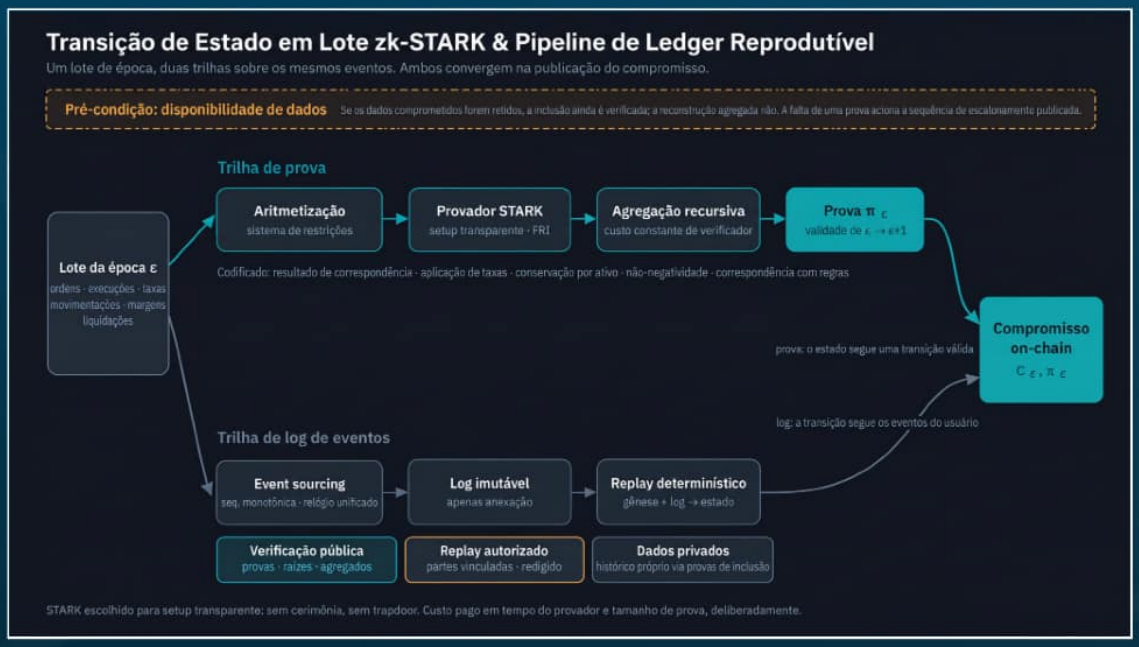
Um compromisso Merkle-sum é uma prova sobre o conjunto de dados que lhe foi fornecido. Se uma plataforma simplesmente deixa um passivo fora do conjunto de folhas, a aritmética é internamente consistente, toda prova de inclusão verifica, e a raiz não diz nada sobre a entrada ausente. Afirmações de que "passivos ocultos quebram o compromisso" estão erradas, e a documentação do protocolo não deve fazê-las. O que o desenho faz, em vez disso, é distribuir o ônus da detecção: cada titular de conta confere sua própria folha contra a raiz comprometida, de modo que uma omissão é detectável pela parte com o maior incentivo para notá-la. Passivos que não podem ser atribuídos a uma conta nomeada — valores acumulados e não liquidados, saques em trânsito e obrigações similares — são incluídos como folhas sintéticas explicitamente rotuladas, com regras de derivação publicadas, ou são divulgados como fora do perímetro provado. O Apêndice especifica a codificação.



3.3 Prova de Solvência zk-STARK e o Ledger Replayável

As transições de cada época são aritmetizadas em um sistema de restrições. As restrições codificam o resultado do matching para o lote, a aplicação de taxas, a conservação por ativo, a não negatividade de todo saldo afetado e a correspondência entre o conjunto de regras publicado e a transição efetivamente aplicada. Um prover gera uma prova π_ε de que o lote foi executado corretamente e de que o estado resultante gera hashes para as raízes comprometidas nos dois lados da época. As provas são agregadas recursivamente, de modo que o custo de verificação pago por uma terceira parte permanece aproximadamente constante à medida que o volume de lotes cresce — a propriedade que torna a verificação contínua viável, em vez de um exercício mensal.

O protocolo usa STARKs, e a razão não é performance. Setup transparente significa que não há cerimônia, não há participante que poderia ter retido uma trapdoor e não há premissa de confiança sobre uma computação multipartite que ninguém fora da sala consegue auditar. O preço é pago em tempo de prover e tamanho de prova, ambos em queda com melhor aritmetização e hashing mais rápido, e ambos gastos deliberadamente pelo protocolo. Um SNARK daria provas menores e uma cauda de verificação mais curta, ao custo de uma premissa invisível ao usuário que verifica o resultado. Dado que todo o argumento deste capítulo repousa sobre o que uma terceira parte consegue conferir sem auxílio, essa escolha é feita na direção da verificabilidade.



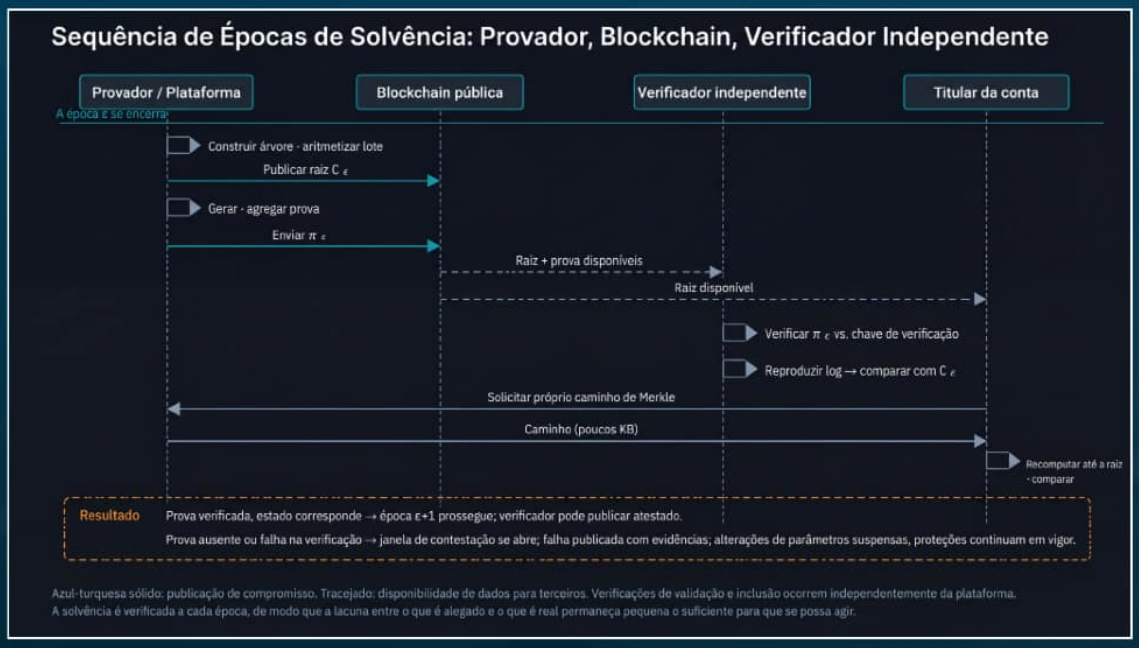
Abaixo das provas está um ledger baseado em eventos. Toda mudança de estado é um evento imutável, com número de sequência monotônico e timestamp extraído do relógio unificado do §4.2. Dado o estado de gênese e o log de eventos, o estado do ledger é reconstruível por replay determinístico. É isso que torna uma prova significativa: uma prova mostra que o estado comprometido decorre de alguma transição válida, e o log mostra que a transição decorre dos eventos que os usuários efetivamente geraram.

O acesso ao replay é escalonado em níveis, e os níveis são uma concessão deliberada, e não um descuido.

- **Verificação pública.** Qualquer pessoa pode conferir a validade das provas, ler as raízes de compromisso e ler estatísticas agregadas publicadas junto a cada época. Nenhum dado em nível de conta é exposto.
- **Replay autorizado.** Uma parte vinculada por acordo de acesso — uma autoridade supervisora, um verificador independente designado, um parceiro de liquidação financeira auditando um corredor específico — pode reconstruir o estado completo a partir do log, sujeito à redação de contas não relacionadas.
- **Dados privados.** Os titulares de conta veem seu próprio histórico por meio de provas de inclusão e do SDK. Ninguém mais vê.

A disponibilidade de dados é precondição para as duas primeiras. Se dados comprometidos forem retidos, o titular de conta ainda pode verificar sua própria inclusão contra a raiz publicada, mas terceiros não conseguem reconstruir o comportamento agregado, e a resposta do protocolo é definida, e não improvisada: uma prova ausente ou uma verificação falha na fronteira de época dispara uma sequência de escalonamento publicada — as mudanças de

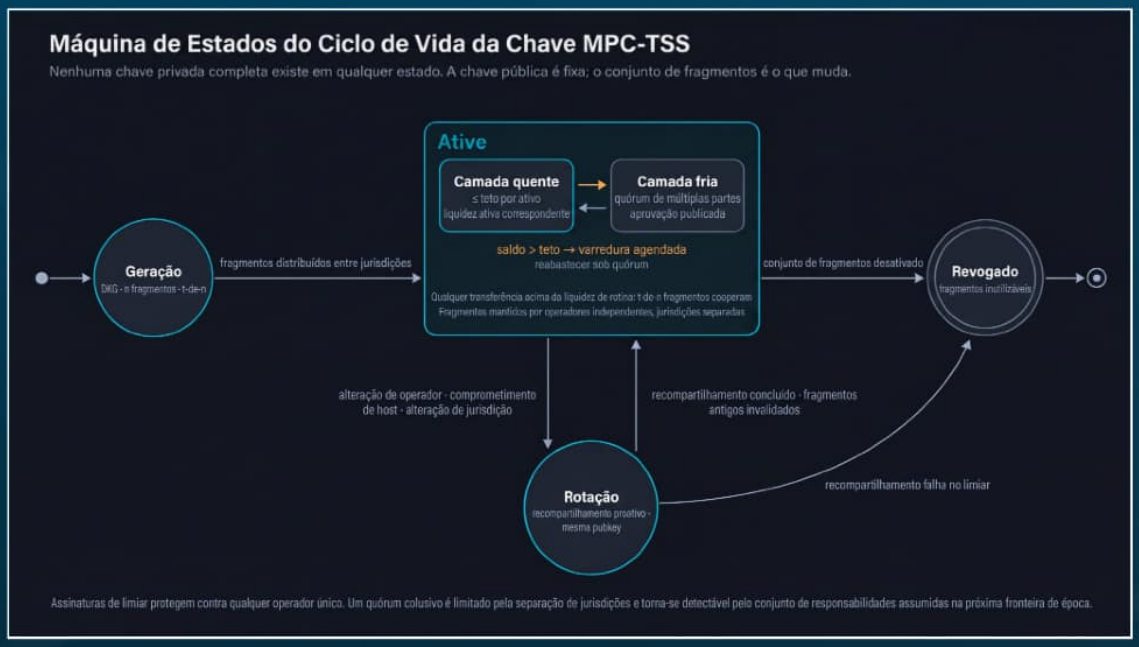
parâmetros ficam suspensas, as proteções existentes permanecem em vigor e a falha é anunciada com a evidência que a produziu. A verificação só tem valor se a sua falha tiver consequências.



3.4 Custódia MPC-TSS e Ciclo de Vida das Chaves

A autoridade de assinatura é distribuída por meio de esquemas de assinatura de limiar. Nenhuma chave privada completa é montada em momento algum; os shares ficam com operadores independentes, em jurisdições separadas, e qualquer transferência acima da liquidez rotineira exige a cooperação de t-de-n shares. A chave pública é fixa, enquanto o conjunto de shares pode ser redistribuído de forma proativa, o que permite rotacionar operadores — um custodiante que se retira, um host comprometido, uma mudança de jurisdição — sem alterar o endereço on-chain para o qual todos apontam.

O envelope operacional é uma camada de política sobre a criptografia. Uma camada quente mantém apenas a liquidez de que o matching ao vivo e o fluxo típico de saques necessitam, com o teto definido por ativo e ajustado por governança dentro de limites. Saldos acima do teto são varridos para cold storage segundo um cronograma, e transferências de cold exigem shares reunidos sob autorização multipartite, com o quórum de aprovação publicado. O material de chave percorre um ciclo de vida definido, em vez de permanecer indefinidamente em um único estado.

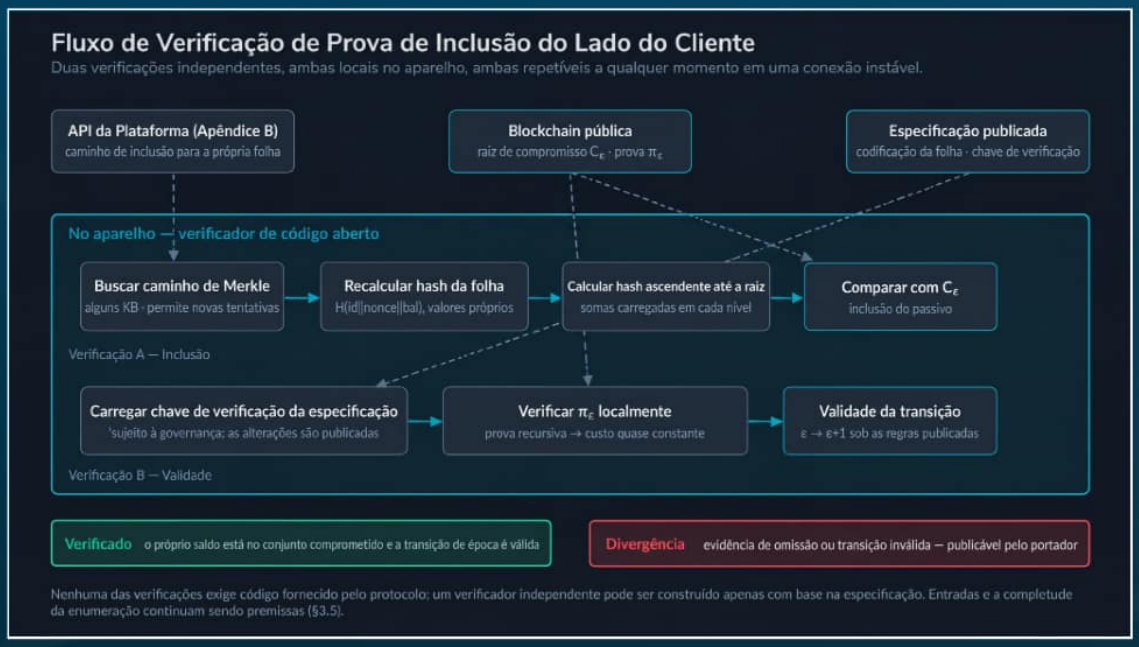


Assinaturas de limiar protegem contra qualquer operador individual. Não protegem contra um quórum que decida agir em conjunto, e descrever o esquema como se conluio fosse impossível seria deturpá-lo. As defesas relevantes nessa camada são a separação jurisdicional dos detentores de shares, regras de quórum publicadas que tornam mais difícil arranjar uma coalizão montada em silêncio, e o fato de que o conjunto de passivos comprometido restringe o que um quórum conluiado poderia sacar sem deixar uma inconsistência visível na próxima fronteira de época. Essa última propriedade é uma garantia de detecção, não uma garantia de prevenção. Ativos podem se mover; a movimentação não pode permanecer não registrada.

3.5 Verificação no Lado do Cliente e as Fronteiras da Garantia

Um titular de conta que verifica sua própria posição precisa de um caminho de Merkle e de uma raiz de compromisso — alguns kilobytes, não o download de uma cadeia. O verificador móvel busca o caminho, recalcula o hash de baixo para cima até a raiz usando a mesma codificação de folha que o protocolo publica, e compara com a raiz do compromisso corrente. Separadamente, verifica se a prova da época valida contra a chave de verificação publicada. Ambas as operações rodam localmente em um celular, sobre uma conexão instável, e qualquer uma delas pode ser repetida a qualquer momento.

Implementações de verificador, a CLI e as interfaces do SDK são de código aberto.



O que a camada **não** estabelece importa tanto quanto o que ela estabelece.

- **A cobertura tem escopo.** Uma prova de cobertura de reservas refere-se às classes de ativos dentro do perímetro. Ativos mantidos em outro lugar, obrigações fora do balanço e qualquer entidade do grupo não incluída no compromisso estão fora dele. Cobertura não é uma opinião de solvência sobre a empresa.
- **A inclusão depende da enumeração.** O protocolo consegue provar que um passivo alegado está na árvore. Não consegue provar que a regra de enumeração usada para construir a árvore era completa; a defesa é que cada parte afetada pode conferir sua própria folha.
- **A validade é relativa às regras.** Uma transição que seguiu as regras publicadas é validamente provada mesmo que a regra em si seja pouco atrativa para os usuários. A prova responde se o protocolo fez o que disse que faria, e a governança — Cap.10 — responde se o que ele disse deveria mudar.
- **As entradas são assumidas, não provadas.** Feeds de mark price, confirmações de gateways de pagamento e dados de referência externos entram no sistema como entradas atestadas, com fontes nomeadas. Comportamento correto sobre uma entrada errada produz um desfecho ruim corretamente provado.
- **A criptografia tem premissas.** A solidez repousa na resistência a colisão das funções de hash e nos parâmetros do FRI que o protocolo publica. Uma quebra nessas premissas quebra a garantia, e o caminho de migração para um evento desse tipo é uma questão de governança que o protocolo não pode pré-comprometer em detalhe.

A verificação muda quais falhas podem ser detectadas, por quem e com que rapidez. É isso, e nada além disso, o que se afirma.

4.0 Topologia Modular

Uma plataforma que promete execução sub-segundo e depois perde seu motor de liquidação durante a única hora em que a liquidação importa não entregou execução sub-segundo. A arquitetura deste capítulo se organiza em torno de quais funções precisam sobreviver à carga de pico e quais podem degradar, porque um sistema que trata todo o tráfego como igualmente importante acabará, sob estresse, protegendo o que chegar primeiro.

4.1 Domínios de Serviço Desacoplados e Sequenciamento Determinístico

O núcleo é dividido em cinco domínios, cada um proprietário do seu estado e cada um com o seu próprio eixo de escala.

Domínio	Estado próprio	Escala ao longo de
Contas	Identidade, permissões, estado de credenciais, superfície de API keys	Número de usuários
Dados de mercado	Snapshots do livro de ofertas, diffs incrementais, prints de negócios	Número de plataformas e símbolos
Matching	Ciclo de vida da ordem, fills, atribuição de sequência	Símbolo (shardizado)
Risco	Estado de margem, exposição, filas de liquidação	Clusters de risco
Ledger	Saldos, movimentações, registros de liquidação financeira	Shard de ativo e de conta

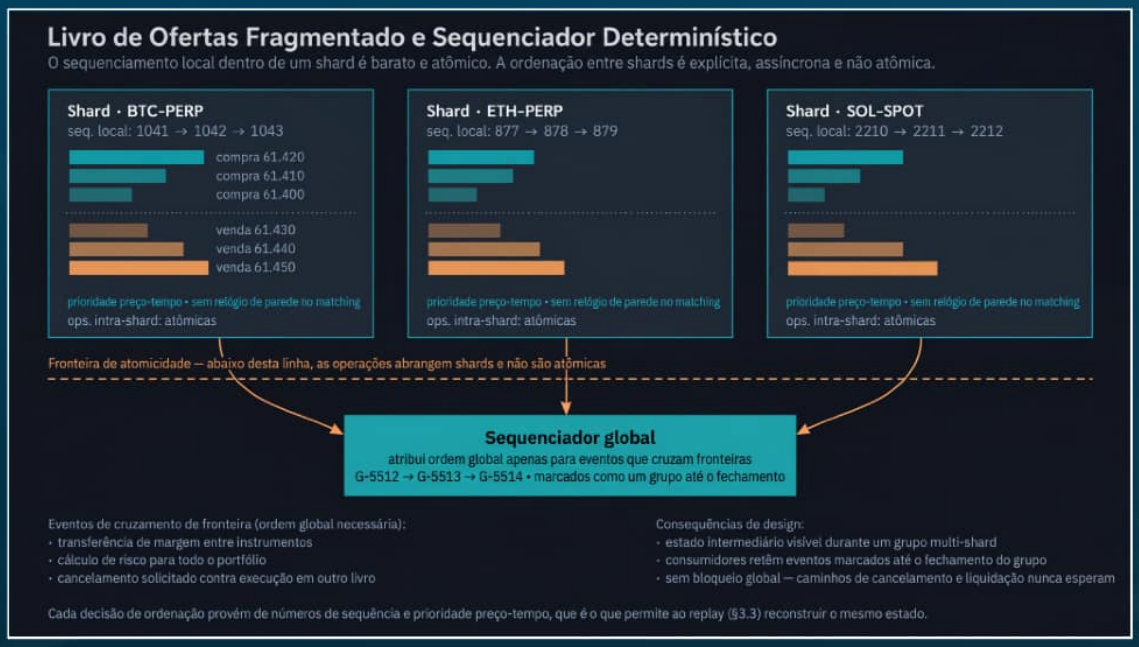
A comunicação ocorre por um barramento de eventos com schemas tipados. Um domínio pode ser replicado, movido ou substituído sem que os outros saibam como ele foi construído e — a parte que importa operacionalmente — uma falha em um deles não se propaga por memória compartilhada nem por um pool de conexões compartilhado. Um fan-out de dados de mercado sobrecarregado degrada a latência de dados de mercado. Ele não pode, por construção, consumir as filas das quais a liquidação depende.



Os livros de ofertas são shardizados por instrumento. Cada shard mantém seus próprios níveis de preço e atribui números de sequência monotônicos aos eventos que produz. Um sequenciador central atribui ordem global apenas a eventos que cruzam fronteiras de shard — uma transferência de margem entre instrumentos, um cálculo de risco em nível de portfólio, um cancelamento que precisa ser ordenado em relação a um fill em outro livro. Dentro de um shard, o sequenciamento é local e barato. Entre shards, é explícito e assíncrono.

Essa escolha impõe uma fronteira que vale declarar com clareza: operações restritas a um shard são atômicas, e operações que atravessam shards não são. Um ajuste de margem cruzada que toque três livros produzirá um estado intermediário visível no barramento, e um cliente que leia no meio do voo pode observar um portfólio momentaneamente inconsistente. A resposta do protocolo é tornar a janela curta, marcar eventos multi-shard para que os consumidores possam retê-los até o grupo fechar, e recusar qualquer desenho que exigisse um lock global entre livros para parecer atômico a um leitor. O lock global restaura precisamente o acoplamento que o sharding existe para eliminar, e o custo recai exatamente sobre os caminhos de cancelamento e de liquidação, que nunca podem esperar por nada.

O determinismo é a razão pela qual essa estrutura é compatível com o ledger replayável do §3.3. Uma prova atesta que o estado passou de um compromisso ao seguinte sob regras publicadas. Se dois motores de matching processando entradas idênticas pudessem produzir ordenações diferentes — por comparação de relógio de parede, por iteração sobre um mapa não ordenado, por um empate desfeito pelo escalonamento de threads —, então o replay reconstruiria um estado diferente e a prova não seria evidência de nada. Toda decisão de ordenação no caminho de matching é, portanto, tomada a partir dos números de sequência do sequenciador e da prioridade preço-tempo, e os próprios motores não carregam relógios que afetem resultados.

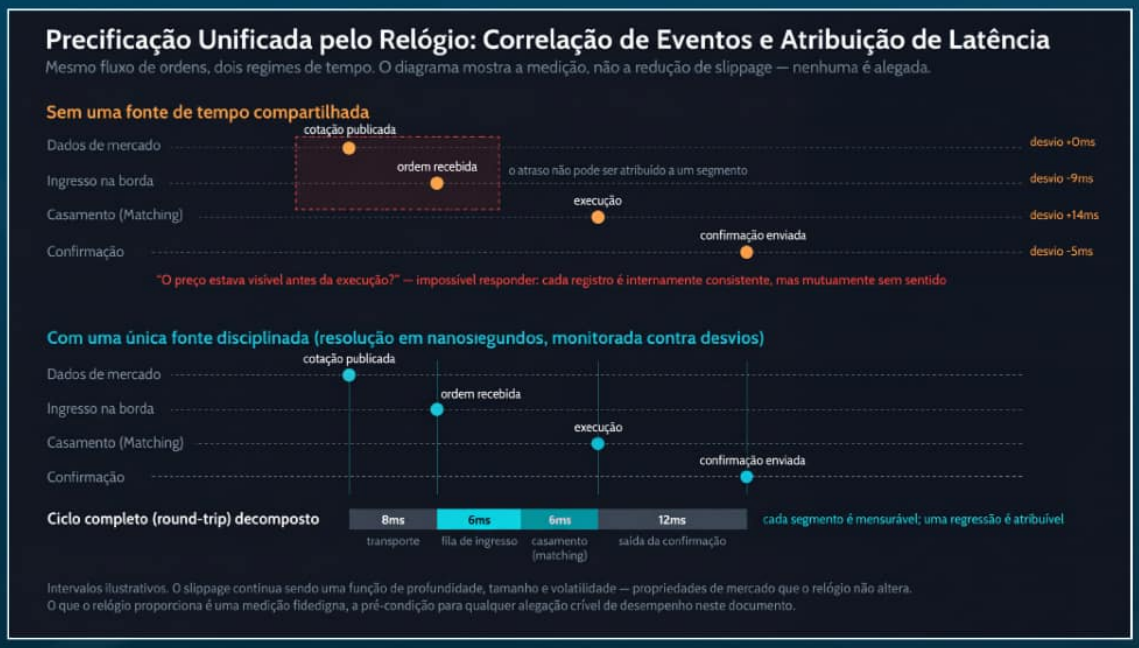


4.2 Precificação com Relógio Unificado e Atribuição de Latência

Todo evento que entra no sistema carrega um timestamp de uma única fonte de tempo, exposta aos clientes com resolução de nanossegundos. A fonte é disciplinada contra múltiplas referências externas, com monitoramento de drift, e uma divergência além da tolerância publicada dispara um alarme operacional, em vez de ser silenciosamente absorvida.

O efeito prático é que cotações e fills se tornam comensuráveis. Quando a ordem limitada de um usuário é executada a um preço que ele acredita não ter visto, a pergunta "o preço estava visível antes do fill?" tem resposta definida, porque o timestamp de publicação da cotação e o timestamp do fill vêm do mesmo relógio e estão no mesmo log ordenado. Sem um relógio comum, essa pergunta é irrespondível — os timestamps de cada subsistema são internamente consistentes e mutuamente sem significado, e a disputa se reduz a qual log a plataforma escolhe apresentar.

A latência se torna atribuível pela mesma razão. O intervalo entre a publicação da cotação e a confirmação do fill se decompõe em segmentos mensuráveis separadamente: transporte da exchange até a borda, enfileiramento da borda até a ingestão do matching, computação do matching e confirmação de saída. Operadores conseguem ver qual segmento se moveu quando um cliente relata degradação, e clientes com infraestrutura colocada conseguem medir seu próprio lado da fronteira contra a mesma referência.



Um relógio único não torna a execução barata. O slippage é função da profundidade do livro, do tamanho da ordem em relação à liquidez disponível e da volatilidade ao longo do intervalo entre a decisão e a chegada. Essas são propriedades de mercado, e uma plataforma que anuncia uma disciplina de timestamp como se fosse garantia de preço está vendendo algo que não controla. O que o relógio compra é uma medição verídica, que é a precondição para as ferramentas de orçamento de latência do lado do usuário e para qualquer afirmação crível de performance feita em qualquer ponto deste documento.

4.3 Degradação Graciosa sob Carga de Pico

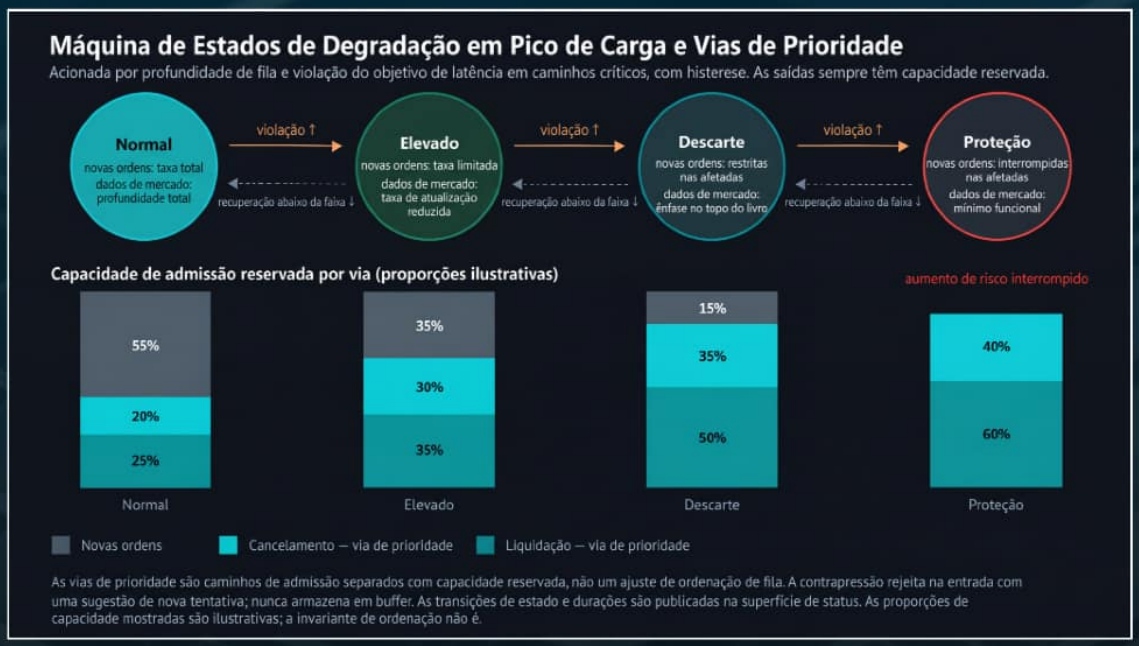
O tratamento de carga é definido como uma máquina de estados com quatro níveis, acionada por profundidade de fila e por violação dos objetivos de latência nos caminhos críticos, sujeita a histerese para que o sistema não oscile em torno de um limiar.

Estado	Admissão de novas ordens	Cancelamento	Liquidação	Dados de mercado
Normal	Taxa integral	Prioridade	Prioridade	Profundidade integral
Elevated	Limitada por taxa na plataforma	Prioridade	Prioridade	Taxa de atualização reduzida
Shed	Restrita nos instrumentos afetados	Prioridade	Prioridade	Ênfase no topo do livro
Protect	Interrompida nos instrumentos afetados	Prioridade	Prioridade	Mínimo funcional

As lanes prioritárias não são um ajuste de ordenação de fila. São caminhos de admissão separados, com capacidade reservada, de modo que uma enxurrada de novas ordens não possa ocupar a capacidade de que um cancelamento precisa, e uma enxurrada de cancelamentos não possa atrasar uma liquidação da qual depende a solvência de outras contas. No estado Protect, a plataforma deixa de aceitar ordens que aumentam risco nos instrumentos afetados e continua aceitando as que reduzem risco — cancelamentos, fechamentos e liquidações. Um trader que não consegue sair de uma posição porque a plataforma está ocupada está carregando um risco que não aceitou.

O backpressure é aplicado na borda de ingresso, e não dentro do caminho de matching. Clientes que excedem seus limites de taxa publicados recebem rejeição explícita com uma dica de retry, em vez de serem silenciosamente enfileirados, porque uma ordem parada em uma fila sem limite definido é uma ordem de idade desconhecida, e o seu timestamp na chegada representaria incorretamente o momento em que o usuário tomou a decisão. A profundidade da fila é limitada por configuração e monitorada como métrica de primeira classe; quando o limite é atingido, o controle de admissão rejeita, em vez de bufferizar.

As transições de estado e suas durações são publicadas na superfície de status. Uma plataforma que entra silenciosamente em um estado degradado e dele sai silenciosamente deixa seus usuários inferindo o que aconteceu a partir de resultados, que é exatamente o padrão que esta arquitetura pretende eliminar.



4.4 Sincronização de Estado na Borda Móvel

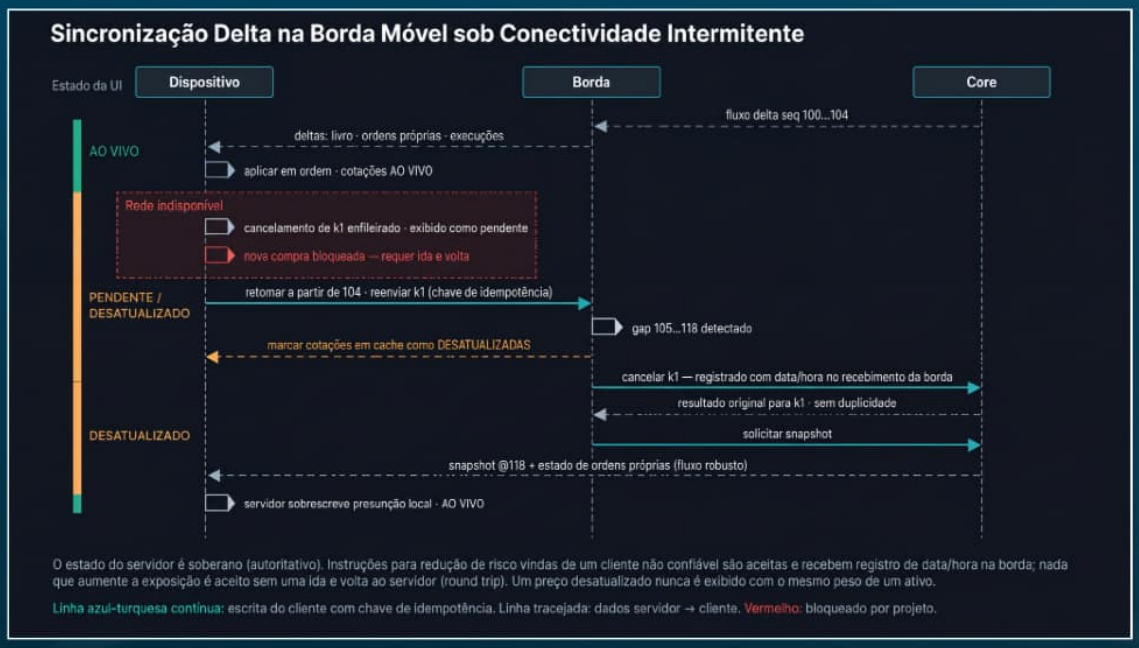
As conexões vindas de celulares são lentas, intermitentes e frequentemente trocadas de rede no meio da sessão. O modelo de sincronização assume as três coisas, em vez de tratá-las como exceções.

Os clientes mantêm um fluxo de deltas de atualizações do livro de ofertas, do estado de ordens por conta e de fills, com chave por número de sequência. Cada evento se aplica a um estado que o cliente já possui, e qualquer lacuna na sequência invalida a visão local, em vez de ser remendada com um patch. Um cliente que detecta uma lacuna solicita um snapshot, marca as cotações em cache local como obsoletas na interface até que o snapshot chegue, e continua exibindo o estado das suas próprias ordens, que é servido por um fluxo separado e mais robusto. Exibir um preço obsoleto com o mesmo peso visual de um preço ao vivo é a forma mais comum de uma interface móvel de negociação enganar seu usuário, e o cliente foi construído para tornar a defasagem visível.

As escritas usam chaves de idempotência. Um envio ou cancelamento carrega uma chave gerada pelo cliente, e um retry através de uma troca de rede a reutiliza; o servidor devolve o resultado original, em vez de criar uma ordem duplicada. Isso importa sobretudo exatamente na condição que gera retries, que é um usuário em conexão fraca observando uma ordem que ele não consegue confirmar.

O servidor é a autoridade em toda questão de estado. A exibição otimista local de uma ordem pendente é permitida — a interface pode mostrar uma ordem que o servidor ainda não reconheceu, marcada como pendente —, mas o cliente nunca trata o seu próprio estado como registro. Na reconexão, o cliente reaplica suas intenções pendentes contra o estado real do servidor e descarta qualquer presunção local que o servidor contradiga.

São aceitas de um cliente não confiável: instruções que reduzem risco. Um cancelamento feito offline ou enfileirado na borda recebe timestamp na recepção, na borda, e não no dispositivo, e o usuário vê qual referência se aplica. Nada que aumente exposição é aceito sem uma ida e volta ao servidor, e o protocolo publica essa restrição, porque uma ordem a mercado cujo preço é determinado no celular é uma ordem a mercado cujo preço foi determinado pelo relógio e pela conexão do usuário, e não pelo livro.



5.0 A Pilha de Produtos com Segregação de Risco

Três negócios compartilham uma mesma plataforma, e a falha que importa é a contaminação: um lançamento que sai mal não deve alcançar as contas de negociação de usuários que nele não participaram, e uma posição de perpétuo que salta através do seu preço de liquidação não deve tocar um saldo de spot que o usuário mantém por outras razões. A separação é estrutural, implementada no ledger e não na política, e custa algo aos usuários — custo que esta seção declara com a mesma franqueza com que declara o benefício.

5.1 Isolamento de Três Canais e Gates de Capital

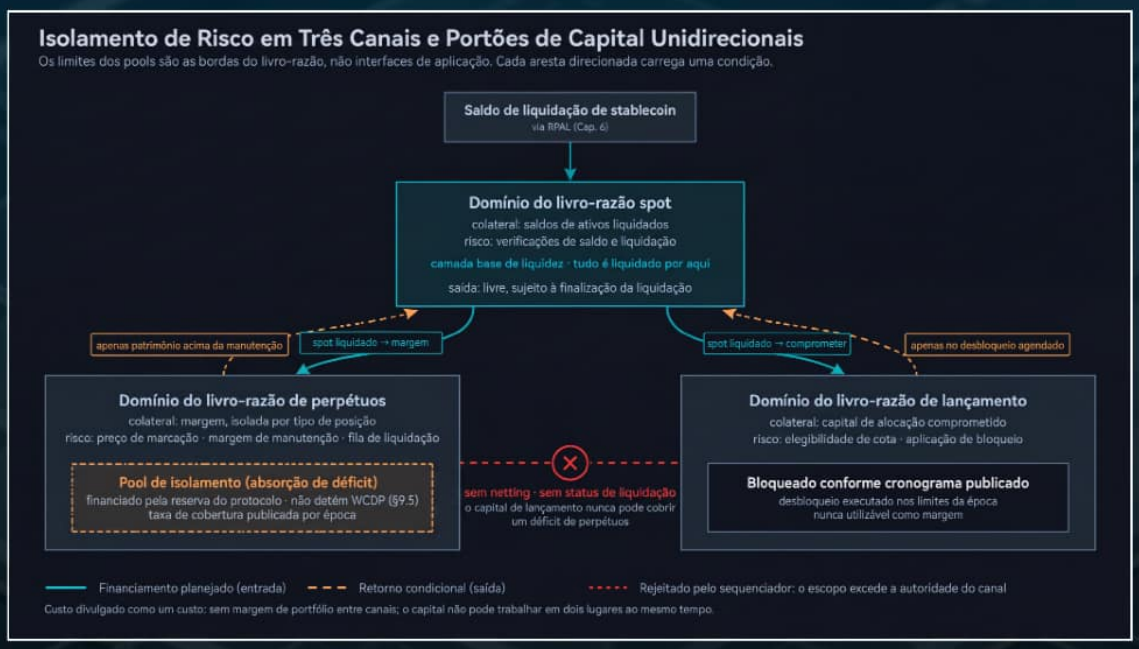
Cada canal mantém o seu próprio domínio de ledger, o seu próprio pool de colateral e a sua própria computação de risco.

Canal	Colateral	Motor de risco	Transferência entre canais
Spot	Saldos de ativos liquidados (settled)	Verificações de saldo e de liquidação financeira	Saída livre, sujeita à finalidade de liquidação financeira
Perpetuals	Saldo de margem, isolado por tipo de posição	Mark price, margem de manutenção, fila de liquidação	Entrada apenas a partir de spot liquidado; saída sujeita à exigência de manutenção
Launch	Capital de alocação comprometido	Elegibilidade de cota e aplicação de lock	Entrada a partir de spot liquidado; saída apenas no desbloqueio

Os gates são unidirecionais e condicionados. O colateral de spot pode ser movido para a conta de perpétuos, porque isso é o usuário financiando deliberadamente uma posição. O patrimônio de perpétuos pode ser movido de volta para fora somente acima da exigência de manutenção, e nunca como mecanismo para cobrir um déficit de liquidação. Compromissos de lançamento podem retornar ao spot ao final do seu lock, e não podem ser usados como margem em nenhum momento — o protocolo não permitirá que uma alocação travada se torne colateral de uma posição alavancada, já que isso converte um compromisso de longo prazo em um instrumento que pode ser encerrado à força no pior momento possível.

Os custos são reais e vale nomeá-los. Capital parado no canal de lançamento não rende nada nos canais de spot ou de perpétuos enquanto espera; um usuário que queira o mesmo capital trabalhando em dois lugares não poderá tê-lo, por desenho. A margem de portfólio entre os três canais está fora de questão, o que reduz a eficiência de capital em relação a um desenho totalmente fungível e, junto com isso, elimina uma classe inteira de colapsos movidos por correlação. O protocolo faz essa troca e a divulga como troca.

O isolamento é aplicado no ledger, e não nas verificações de risco do motor de matching. Uma instrução de liquidação de perpétuo não consegue referenciar um saldo de spot porque o escopo de ativos da instrução não inclui o shard de spot, e o sequenciador rejeitará um evento entre shards cujo escopo declarado exceda a autoridade do canal de origem. A aplicação no nível do ledger sobrevive a bugs no motor de risco, a erros de configuração durante um release e a uma conta de serviço comprometida. A aplicação no código de aplicação não sobrevive a nenhum desses casos.



5.2 Perpetuals: Mark Price, Waterfall de Liquidação e Isolamento do pool de isolamento

A liquidação do contrato corre contra um mark price construído a partir de um composto de plataformas de referência externas, ponderado por volume e filtrado antes do uso.

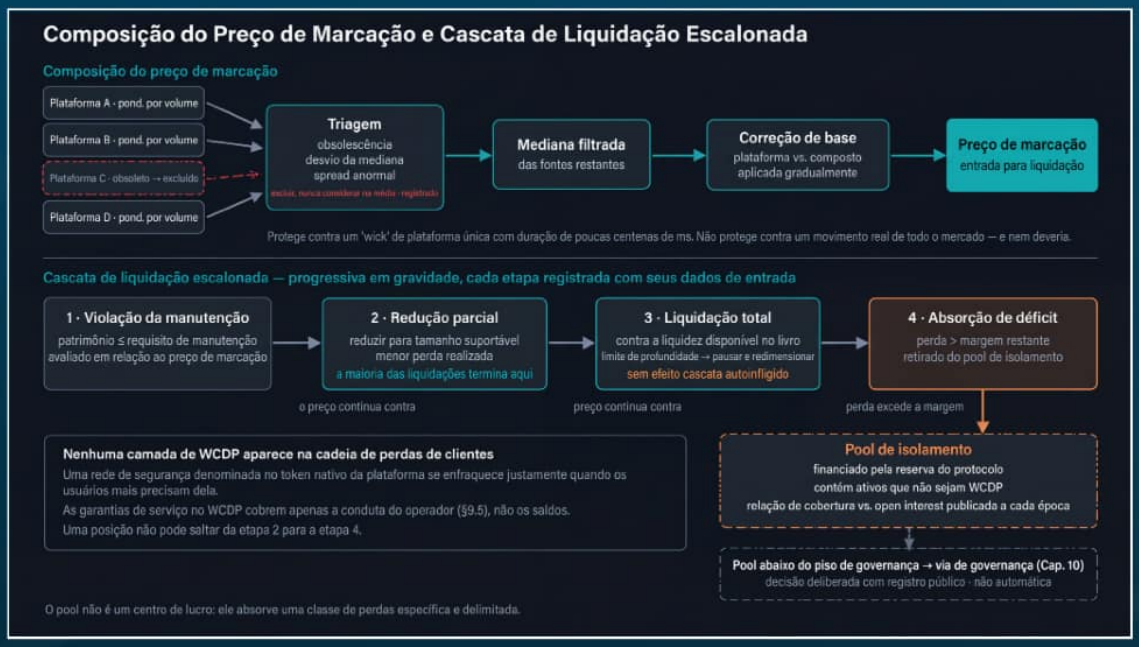
As fontes são triadas quanto a defasagem, desvio da mediana do composto e spread anormal em relação ao seu próprio histórico recente. Uma fonte fora da banda de tolerância é excluída durante o intervalo, em vez de ser incorporada à média, e a exclusão é registrada em log com o motivo. A mediana filtrada é então corrigida pelo basis da própria plataforma contra o composto, aplicada gradualmente, de modo que um desequilíbrio persistente de funding mova o mark price, e não uma única ordem. O resultado é um preço que responde a movimento real de mercado e é resistente a um print que existe apenas em uma plataforma por algumas centenas de milissegundos. Essa é toda a defesa contra o wick que dispara liquidações, e é uma defesa contra manipulação barata de tentar; não é uma defesa contra um movimento genuíno de mercado inteiro, que liquidará posições e deve liquidá-las.

Quando o patrimônio de uma posição cai até a exigência de manutenção, a liquidação prossegue em etapas, e não como um evento único.

Redução parcial primeiro. O motor reduz a posição ao tamanho que a conta consegue sustentar com a margem corrente, tipicamente com uma perda realizada menor do que o fechamento da posição inteira. A maior parte das liquidações termina aqui, e os usuários frequentemente não percebem nada além de uma posição que encolheu durante a noite.

Liquidação total em seguida, se o preço continuar contra a posição reduzida, executada contra o livro na liquidez que existir. Aqui o motor não continuará empurrando para dentro de um livro fino: se a ordem consumiria além de um limiar de profundidade, o matching pausa enquanto o dimensionamento é recalculado, o que evita a cascata autoinfligida em que uma ordem de liquidação varre o livro e dispara liquidações nas posições que forneciam a liquidez.

Absorção de déficit por último. Quando a perda realizada em uma liquidação total excede a margem remanescente da conta, a diferença é sacada do pool de isolamento. Esse pool é financiado pela reserva do protocolo, e a reserva é mantida em ativos que não incluem o WCDP — o raciocínio para isso está no §9.5. Quando o pool cai abaixo do seu piso governado, a resposta do protocolo é uma mudança de parâmetro governada, e não um mecanismo automático, porque as alternativas disponíveis para uma plataforma nesse ponto — socializar perdas entre traders lucrativos ou reduzir posições de contraparte — são suficientemente consequentes para exigir uma decisão deliberada com registro público.



Duas propriedades deste desenho merecem a atenção normalmente dedicada ao mark price. A sequência de liquidação é monotônica em severidade — uma posição não pode saltar da redução parcial para a absorção de déficit, e cada etapa é registrada em log com os insumos que a dispararam. E o pool não é um centro de lucro. Ele existe para absorver uma classe específica e delimitada de perda; a sua taxa de cobertura é publicada a cada época, e o leitor pode compará-la com o open interest em aberto sem precisar confiar na palavra da plataforma.

5.3 Camada Base de Spot e o Firewall do Launch

O canal Spot é o mais simples e aquele por meio do qual todo o restante liquida. Profundidade e spread são publicados por instrumento, medidos em vários tamanhos nocionais e não apenas no topo do livro, pois uma plataforma com um impressionante melhor preço de compra e sem liquidez por trás dele é uma plataforma que mostrará aos usuários um preço que não conseguirão obter. A finalidade de liquidação financeira é explícita por classe de ativo: o que o usuário vê como saldo disponível é definitivo, não provisório, e a diferença entre os dois nunca é deixada para ser inferida a partir de uma correção posterior.

O canal de Launch não herda nenhuma das características de risco da conta de spot. A cota é alocada por meio do protocolo descrito no Cap.8, o capital é comprometido no domínio do lançamento e o compromisso é travado conforme o cronograma publicado. O desbloqueio é aplicado pelo ledger nas fronteiras de época programadas. O fracasso de um projeto em entregar, um atraso na listagem ou um colapso no preço de mercado do token não alcança os saldos de spot do usuário nem sua conta de margem e — a metade do firewall que mais importa — perdas do usuário no canal de perpétuos não podem ser quitadas com capital comprometido em um lançamento. Posições nos dois domínios nunca são neteadas, e nenhum processo de liquidação tem autoridade para cruzar a fronteira.

O que o firewall não faz é avaliar nada. Ele mantém um desfecho ruim contido entre os participantes que o aceitaram; o Cap.8 aborda o maquinário de divulgação e de alocação que determina quem são esses participantes e em que termos.

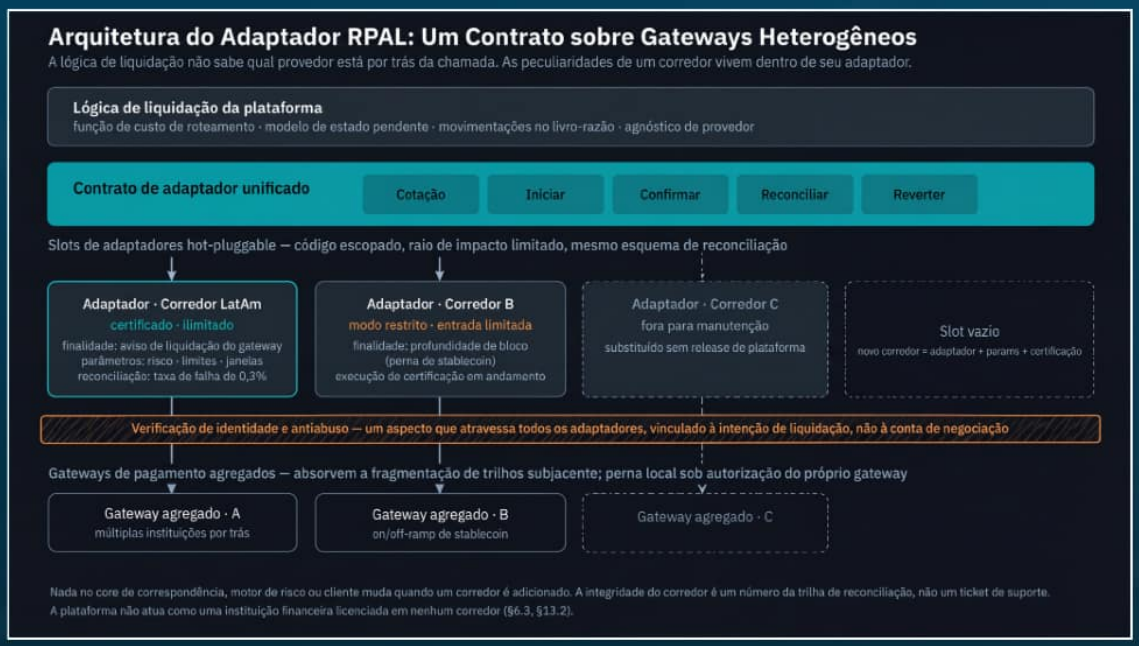
6.0 Acesso via Stablecoin e Liquidação Financeira

Dinheiro chegando de uma conta bancária brasileira e dinheiro chegando de uma conta mexicana devem encontrar o mesmo contrato interno. A camada de abstração de pagamentos regionais existe para tornar isso verdade, e existe como arquitetura, e não como lista de parceiros, porque a lista muda e o contrato não.

6.1 O Modelo de Adapter

Toda integração de corredor implementa uma única interface: solicitar uma cotação para uma conversão ou transferência, iniciá-la, confirmar o resultado, reconciliar contra o próprio registro do corredor e revertê-la quando ela falha. Acima dessa interface está a lógica de liquidação financeira da plataforma, que não sabe qual provedor está por trás da chamada. Abaixo dela está um adapter, e um adapter é um trecho de código com escopo e raio de impacto delimitado — as particularidades de um corredor vivem dentro dele e não podem vazar para o motor de roteamento.

A plataforma conecta-se a soluções líderes de gateway de pagamento agregado na América Latina, que é o nível de especificidade que a interface exige. Gateways agregados são a abstração correta para essa camada porque já absorvem a fragmentação dos trilhos subjacentes: um usuário em um estado pode liquidar por uma instituição diferente da de um usuário em outro estado, e a plataforma não precisa distinguir entre eles. O que ela precisa é de um contrato estável, semântica de finalidade publicada e rastro de reconciliação.



Duas decisões de design nessa camada importam mais do que o formato da interface. Os adapters são hot-pluggable, de modo que um corredor pode ser retirado de serviço para manutenção ou um provedor pode ser substituído sem um release da plataforma; e todo adapter deve produzir registros no mesmo schema de reconciliação, que é o que torna a saúde de um corredor mensurável. Um corredor que falha na reconciliação com mais frequência do que seus pares é visível como um número, e não como um ticket de suporte, e pode ser throttled de forma independente.

Adicionar um novo corredor, portanto, é um adapter, um conjunto de parâmetros e uma rodada de certificação contra a suíte de reconciliação. Nada no núcleo de matching, no motor de risco nem no cliente muda. Essa propriedade é a que o termo super-nó do §1.3 designa no nível técnico: o padrão de implantação é o mesmo a cada vez, razão pela qual um segundo corredor é um projeto de semanas, e não uma reconstrução.

6.2 Roteamento de Stablecoin e Orquestração de Liquidação Financeira

O corredor entre moeda local e saldo de negociação tem quatro etapas, e a lógica de liquidação financeira da plataforma cobre todas elas, e não apenas a primeira.

Entrada de recursos. Um usuário expressa uma intenção em moeda local; o adapter cota a taxa, as tarifas e a janela de liquidação esperada; o usuário aceita; o gateway confirma. A plataforma registra a intenção, a cotação e a confirmação como eventos separados, porque uma disputa sobre taxa é uma disputa sobre qual desses três um intermediário alterou.

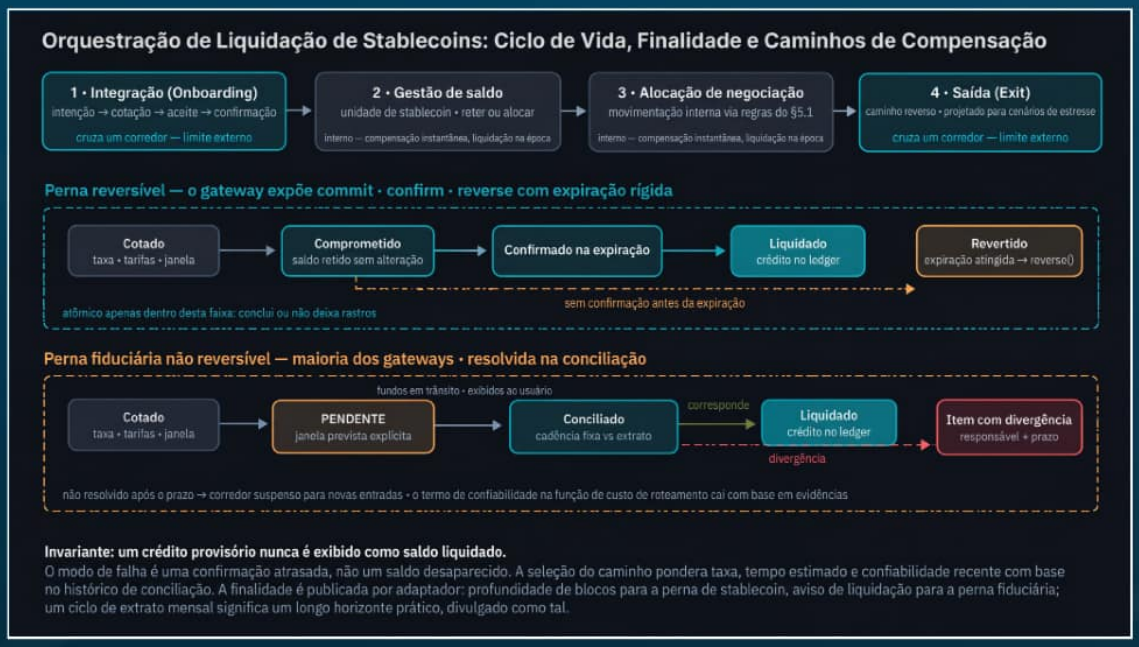
Gestão de saldo. Saldos em stablecoin ficam na conta do usuário, denominados na unidade da stablecoin, disponíveis para saque por qualquer corredor que a plataforma suporte ou para implantação em negociações. Usuários que mantêm saldo sem negociar são um estado legítimo, e não uma conversão abandonada.

Alocação de capital de negociação. Transferências do saldo de liquidação financeira para o canal de perpétuos ou de lançamento são movimentações internas de ledger governadas pelos gates do §5.1. Elas não tocam um corredor, liquidam instantaneamente e são finalizadas na fronteira de época como qualquer outra movimentação interna.

Saída. O saque percorre o caminho de roteamento em sentido inverso, com a mesma estrutura de cotação e confirmação. A saída merece mais atenção no projeto do que a entrada, porque é a operação que os usuários tentam sob pressão, e é a que torna o comportamento de fila de uma plataforma visível.

A seleção de caminho entre múltiplos gateways otimiza uma função de custo que combina taxa, tempo esperado de liquidação e confiabilidade recente medida a partir do rastro de reconciliação. O termo de confiabilidade não é ornamental: um gateway que oferece a melhor taxa de manchete enquanto falha uma requisição em cinquenta é mais caro do que uma cotação ligeiramente pior que completa, e o motor de roteamento foi construído para notar a diferença sem que um operador precise intervir.

A liquidação pelo corredor é atômica apenas em um intervalo definido. Onde um gateway expõe uma sequência de compromisso-confirmação-reversão com um prazo rígido, a plataforma pode manter o saldo do usuário inalterado até que a confirmação chegue e reverter de forma limpa no vencimento; dentro dessa faixa, a transação ou se completa ou não deixa rastro, e a expressão é usada de forma deliberada e restrita. Onde um gateway não expõe tal sequência — a maioria deles, para pernas em moeda fiduciária — a plataforma registra um estado pendente com uma janela de liquidação esperada explícita, mostra ao usuário que os fundos estão em trânsito e resolve o estado na reconciliação. O modo de falha é uma confirmação atrasada, não um saldo desaparecido. O que a plataforma se recusa a fazer é exibir um crédito provisório como saldo liquidado, porque um usuário que negocia contra fundos que posteriormente não chegam assumiu uma posição com dinheiro que não existia.



6.3 Finalidade, Reconciliação e Interfaces de Conformidade

Finalidade tem significados diferentes em corredores diferentes, e cada adapter publica a sua própria definição, em vez de ser nivelado a uma única declaração aplicável a toda a plataforma. Para uma perna de stablecoin, é a profundidade de confirmação de bloco. Para uma perna fiduciária, é o aviso de liquidação financeira do gateway, que a plataforma trata como definitivo para fins contábeis e reconcilia contra o extrato periódico do gateway. Um corredor cujo ciclo de extrato é mensal tem um horizonte prático de finalidade longo, e a plataforma divulga esse horizonte aos usuários em vez de descrever todos os corredores como instantâneos.

A reconciliação roda em cadência fixa contra os registros de cada gateway, sobre uma janela que se estende além do horizonte de liquidação. Discrepâncias abrem um item com um responsável e um prazo; itens não resolvidos após o prazo suspendem a capacidade do corredor de aceitar novo tráfego de entrada. O resultado da reconciliação também alimenta a função de custo de roteamento acima, de modo que um corredor não confiável sai do conjunto preferencial com base em evidência, e não em decisão.

Os controles de verificação de identidade e de combate a abusos ficam como um aspecto da camada de adapter. A plataforma coleta o que um corredor exige para movimentar fundos e o que a sua própria política de risco exige, e vincula o resultado à intenção de liquidação, e não à conta de negociação. Isso evita que requisitos específicos de corredor se cristalizem no modelo de usuário da plataforma: uma exigência que se aplica por causa das regras de um corredor não se impõe a um usuário em outro corredor, e quando uma exigência muda, ela muda em um único lugar.

O que essa camada não faz é atuar como instituição financeira licenciada em qualquer corredor, nem oferecer serviços de depósito, crédito ou custódia fiduciária em moeda local. Ela roteia entre o gateway escolhido pelo usuário e o próprio saldo de liquidação da plataforma, e a perna local é realizada pelo gateway sob sua própria autorização. O §13.2 declara a posição societária.

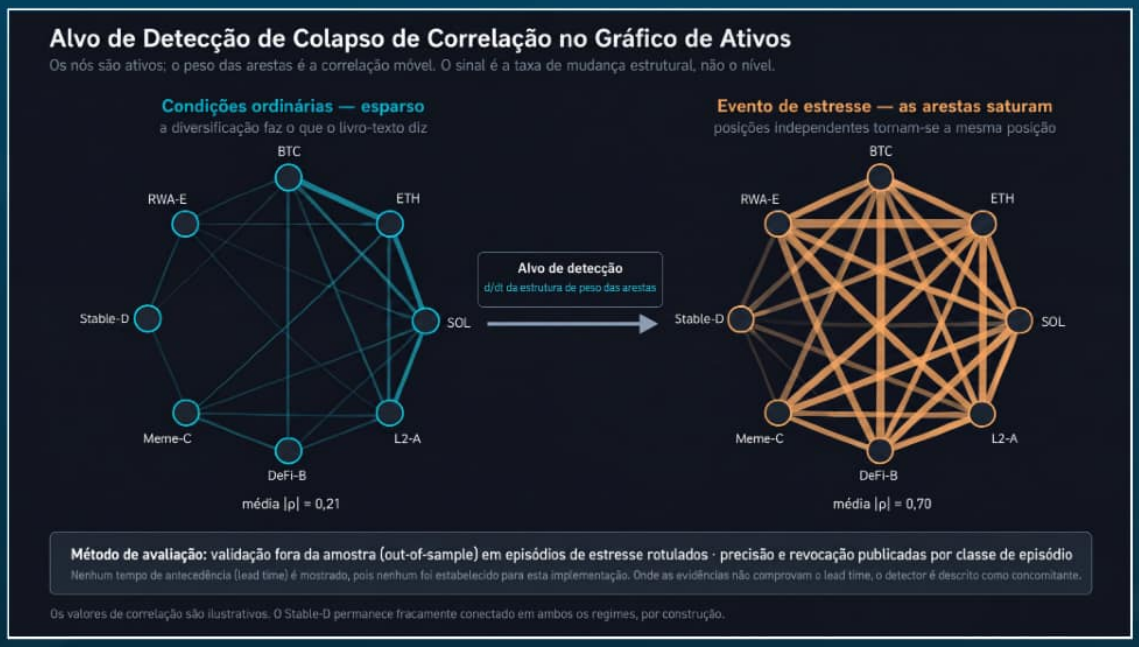
7.0 AI Sentinel e Execução Restrita por Política

Um sistema de vigilância que prevê preços é um ativo de marketing. Um sistema de vigilância que vê um livro perdendo profundidade mais rápido do que está perdendo preço, e consegue agir antes que a fila de liquidação se torne uma cascata, é um ativo operacional. Este capítulo trata da segunda categoria e de o que um modelo tem permissão de fazer na conta de um usuário sem que o usuário esteja presente.

7.1 Telemetria e Detecção de Colapso de Correlação

Todo evento no núcleo — ordens, cancelamentos, fills, mudanças de estado de margem, acúmulos de funding, instruções de liquidação, tentativas de saque — chega a um barramento que a camada de inteligência assina. A camada lê. Ela não executa ordens, não mantém saldos e não está no caminho crítico entre a instrução de um usuário e o motor de matching. Essa separação é aplicada no nível da interface, e é o que permite que o sentinela falhe sem arrastar a plataforma consigo.

O estado de posição e de mercado é representado como um grafo, com ativos como nós e correlação como pesos de arestas, calculado sobre janelas deslizantes em vários horizontes. O sinal interessante não é o nível de correlação, mas a taxa na qual a estrutura de arestas se reorganiza. Em condições normais, o grafo é esparso: a maioria dos ativos tem relação fraca ou nenhuma, e a diversificação de portfólio faz o que o livro-texto diz. Em um evento de estresse, as arestas se saturam — posições que eram independentes se tornam a mesma posição, e um usuário que acreditava estar hedgeado descobre que está dobrado. Detectar essa transição cedo o suficiente para mudar o comportamento de admissão é o objetivo.



Se a transição é detectável antes do evento de preço que normalmente a acompanha é uma questão empírica, e a resposta não é assumida aqui. A camada mantém um histórico rotulado de episódios de estresse, avalia a detecção contra janelas nas quais o modelo nunca foi treinado e publica precisão e recall por classe de episódio. Um detector com precisão adequada e recall ruim é útil para uma decisão de throttling e inútil para um alarme, e os números publicados informam o operador ou o leitor qual dos dois ele tem. Onde a evidência suporta um tempo de antecedência, ele é declarado com a amostra na qual foi medido; onde não suporta, o detector é descrito como concomitante e usado de acordo.

7.2 Sentinelas Anti-Cascata e o Conjunto de Ações

A distribuição de profundidade é mapeada continuamente, e não apenas o topo do livro. Um livro pode mostrar um respeitável melhor preço de compra e estar efetivamente vazio nos dois por cento seguintes, e a variação do perfil de profundidade ao longo de uma janela deslizante é um preditor melhor de condições de cascata do que o próprio nível de preço. Onde o perfil enfraquece abaixo de uma faixa de percentil enquanto o open interest no instrumento afetado se concentra em um lado, o motor sinaliza um precursor de cascata: uma configuração na qual uma única ordem de liquidação pode consumir a liquidez da qual as margens de outras posições dependem.

Os precursores alimentam o conjunto de ações, que é deliberadamente pequeno e graduável.

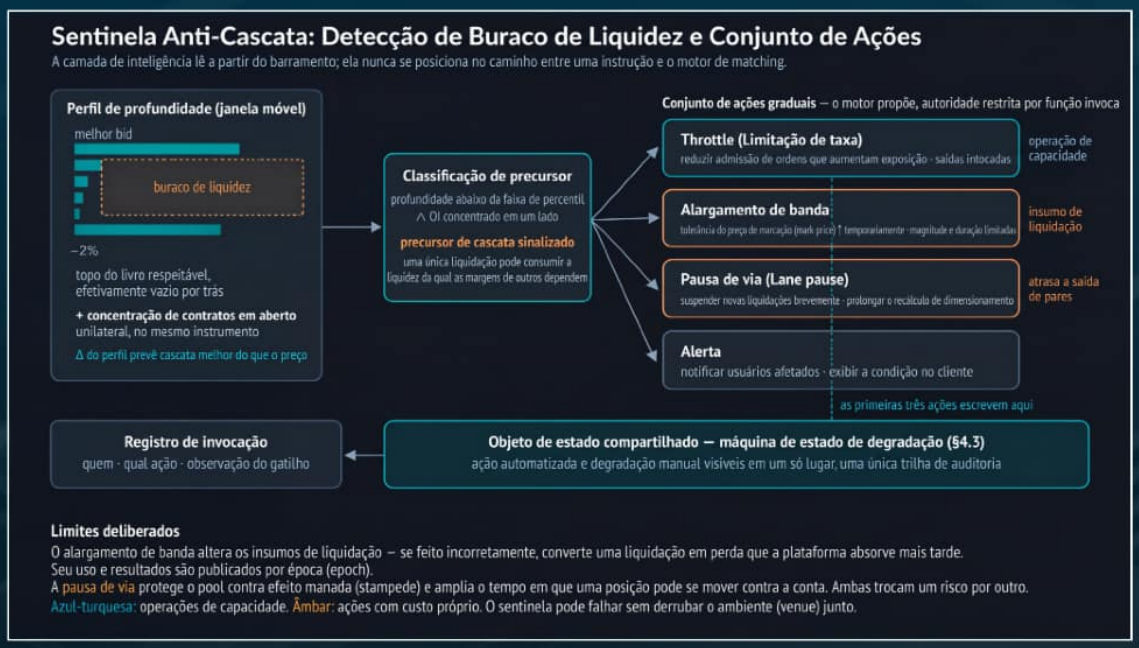
Throttle. Reduzir a taxa de admissão de ordens que aumentam exposição nos instrumentos afetados, mantendo as saídas intocadas.

Alargamento de banda. Expandir temporariamente a tolerância de fonte do mark price e estender a resposta da correção de basis, de modo que os prints de um livro fino tenham menor probabilidade de conduzir a liquidação no intervalo.

Pausa de lane. Suspender novas instruções de liquidação no instrumento afetado por um intervalo delimitado, ou estender o recalculo de dimensionamento descrito no §5.2, de modo que as liquidações já em trânsito não estampem a mesma liquidez.

Alerta. Notificar os usuários afetados com posições na configuração sinalizada e expor a condição no cliente.

As três primeiras são operações de capacidade no caminho de admissão do §4.3 e compartilham sua máquina de estados, o que significa que uma ação automatizada e uma degradação manual são visíveis em um único lugar com uma única trilha de auditoria. Quem pode invocar o quê, e sob quais limiares de evidência, é uma questão de parâmetro; o motor propõe, e a autoridade para alargar uma banda de mark price ou pausar uma lane de liquidação é restrita por função, com cada invocação registrada contra a observação que a disparou.



Dois limites no conjunto de ações são deliberados e devem ser declarados. O alargamento de banda muda insumos de liquidação, e fazê-lo de forma errada converte uma liquidação em uma perda que a plataforma absorve depois; ele é delimitado em magnitude e duração, e seu uso é publicado por época com os resultados. A pausa de lane atrasa liquidações, o que protege o pool de uma estampida e estende o período durante o qual uma posição pode se mover ainda mais contra a conta. Ambas são ferramentas de limitação de danos com seus próprios custos, e não melhorias gratuitas, e um titular de conta que lê isso deve entender que, em condições de cascata, a plataforma pode estar trocando um risco por outro.

7.3 Compilação de Intenções sob Gates de Política

A assistência de execução nessa camada transforma a instrução de um usuário em linguagem ordinária em um artefato de regra que o motor consegue executar deterministicamente: trabalhar uma entrada em cinco tranches ao longo de uma sessão, sair se a correlação da posição contra uma referência declarada exceder um limite, rebalancear para pesos-alvo em um cronograma. O artefato é um conjunto de regras — parâmetros, condições, limites — que um usuário pode ler, alterar ou recusar, e ele é registrado em log em uma forma que permite responder a uma pergunta posterior sobre o que o sistema fez a partir do registro, e não da memória.

Entre a instrução do usuário e qualquer execução há um gate de política com quatro componentes. **Escopo de permissão** define quais contas, instrumentos e ações o artefato pode tocar — uma regra de rebalanceamento para a conta de spot não tem acesso à margem. **Limites** delimitam o nocional por ação, a exposição agregada e a atividade cumulativa ao longo do período de autorização. **Revogação** entra em vigor na próxima avaliação do gate, e as instruções pendentes ainda não executadas são canceladas com um recibo. **Recibos** registram o que foi executado contra qual versão de artefato, com os insumos que satisfizeram cada condição, e são retidos na conta.



A operação padrão é confirmação por instrução. Um usuário que deseja que um artefato rode sem a sua presença pode conceder uma pré-autorização delimitada — um período fixo, um teto nocional fixo, um conjunto de instrumentos definido — que o gate aplica mecanicamente, e não comportamentalmente. Quando as condições de um artefato só podem ser satisfeitas por uma ação fora do seu escopo, o gate para e solicita confirmação; ele não amplia sua própria autoridade. E os artefatos são versionados, de modo que alterar uma regra em andamento

encerra a versão em execução e exige a etapa de confirmação para a nova, o que impede que uma pequena mudança de parâmetro herde silenciosamente uma autorização ampla.

O que o usuário retém ao longo de tudo isso é a parte que não pode ser delegada. Uma regra pode executar uma estratégia declarada; não pode estabelecer que a estratégia era sólida, e uma posição encerrada por uma condição predeterminada ainda é uma perda incorrida pelo usuário. A contribuição do sistema é consistência — a saída acontece na condição especificada, e não no momento em que o usuário estava acordado para notá-la —, e consistência de execução não converte uma visão perdedora em uma vencedora.

7.4 Governança de Modelos e Responsabilidade Humana

Detectores decaem. Um modelo calibrado em um regime de mercado registra o próximo como ruído até ser retreinado, e o retreinamento em si é um risco: ajustar o modelo ao episódio de estresse mais recente e ele estará exquisitamente ajustado às condições que acabaram de passar. A camada mantém um registro versionado com a janela de treinamento, o conjunto de características e a avaliação de performance vinculados a cada versão em produção, e rastreia precisão e recall ao vivo contra o histórico rotulado. Qualidade de detecção que cai abaixo de um limiar rebaixa o modelo a apenas-consultivo, removendo sua autoridade para invocar uma ação, e esse rebaixamento é automático e registrado em log.

Backtests são tratados como filtro, nunca como evidência de performance ao vivo. Um detector deve superar uma barreira fora da amostra antes da implantação e depois continuar superando-a ao vivo; os dois números são publicados separadamente, porque a distância entre eles é a única figura mais informativa sobre um sistema de detecção — e a mais frequentemente omitida.

A responsabilidade pelos resultados cabe ao titular da conta. As ações do sentinela operam sobre os parâmetros de risco de toda a plataforma — taxas de admissão, insumos de liquidação, lanes de liquidação — e não sobre a estratégia do usuário nem sobre a solidez de sua posição. Uma entrada throttled, uma banda alargada ou uma liquidação pausada muda as condições sob as quais um usuário negocia, e a plataforma divulga quando isso ocorre; nenhuma delas é uma recomendação ou garantia, e nenhuma transfere a perda do usuário para a plataforma. Um operador que invoca uma ação fora do seu limiar de evidência publicado fica exposto ao processo de contestação do §9.5 nos mesmos termos de qualquer outra obrigação de serviço.

8.0 Democratização de Capital

A alocação de early-stage é onde a desvantagem do usuário de varejo é mais visível e menos defensável. Mesas institucionais recebem ligações; usuários de varejo recebem uma página que pode ou não carregar a tempo, e o que quer que recebam reflete a velocidade de sua conexão naquela manhã. O protocolo deste capítulo substitui uma alocação por ordem de chegada por uma alocação por função publicada, e aceita a consequência de que alguns usuários receberão menos do que a velocidade lhes teria dado.

8.1 Pipeline de Descoberta, Divulgação e Ciclo de Vida do Launch

Os projetos entram por um pipeline por etapas, e cada etapa tem uma condição de saída, e não uma votação.

Submissão. Um projeto fornece o pacote padrão de divulgação: o que o token faz, o que os recursos financiam e em qual cronograma, quem controla o quê, os termos de vesting para cada classe de titular, o cronograma de desbloqueio e a base legal pela qual o emissor acredita poder oferecer o instrumento. Omissões materiais nessa etapa encerram o processo, e o motivo é registrado.

Revisão técnica. A divulgação é verificada contra o contrato, se houver um. Oferta de tokens, autoridade de mint, autoridade de atualização, capacidade de pausa e restrições de transferência são lidos do código implantado onde o código existir, e as intenções declaradas são comparadas com o que o código permite. Um token cujo contrato concede ao emissor uma função de mint ilimitada não é desqualificado automaticamente; a discrepância entre a divulgação e o contrato é, e ela é publicada de qualquer forma.

Revisão de termos. Os termos de alocação, o cronograma de lock e as obrigações do emissor são fixados, versionados e publicados antes de a janela de subscrição abrir. Uma vez que a janela abre, os termos não podem mudar — um lançamento cujos termos podem ser alterados durante a subscrição não é um lançamento com termos, e o compromisso do ledger com o hash de versão torna isso aplicável, e não meramente prometido.

Subscrição. Os usuários comprometem capital no canal de lançamento contra a elegibilidade de cota. O capital é travado pelo cronograma declarado no nível do ledger.

Desbloqueio e migração. Os tokens e qualquer capital devolvido tornam-se disponíveis nas fronteiras de época programadas. A migração do domínio de lançamento para o domínio de spot ocorre por um caminho controlado, com limites de taxa e uma janela de monitoramento, de modo que as condições de liquidez de abertura de uma listagem sejam observáveis, e não emergentes de um release simultâneo.



O template de divulgação é uniforme entre os lançamentos precisamente para que um usuário possa comparar dois deles sem conhecer nenhum dos emissores. Uniformidade não é um julgamento de qualidade, e nada no pipeline constitui uma avaliação sobre se o token vale o seu preço. O que o pipeline faz é tornar os termos legíveis e fazer o comportamento aplicado coincidir com o comportamento declarado; a partir daí, o usuário está comprando um projeto, e não um selo de plataforma.

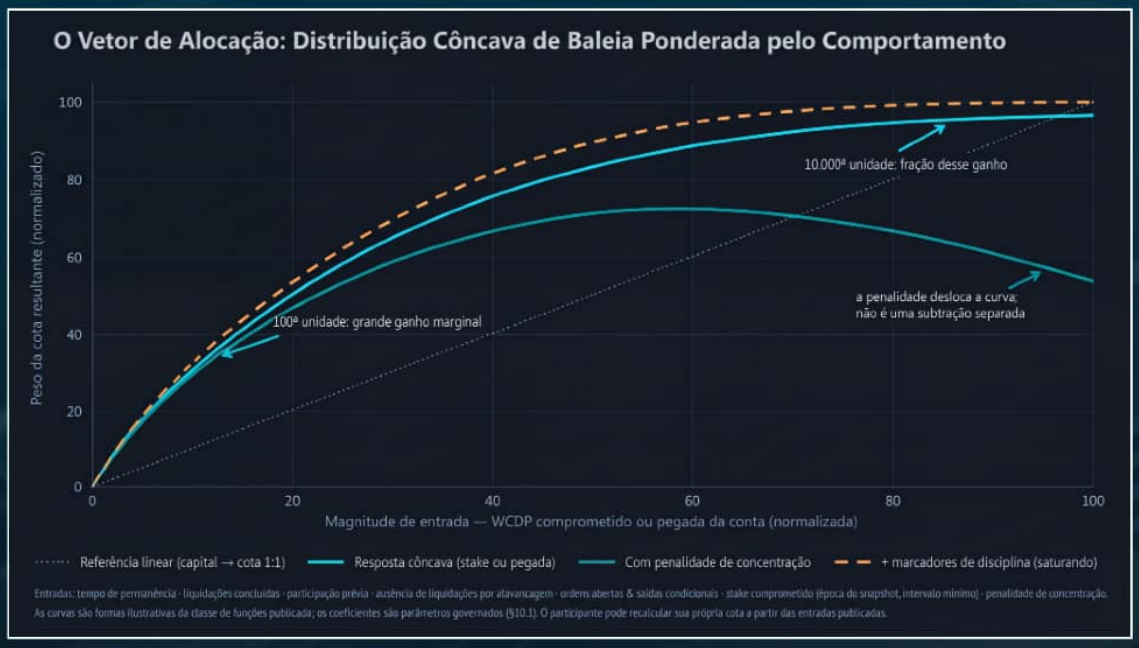
8.2 O Vetor de Alocação

A cota é calculada a partir de um vetor com duas classes de insumo: um perfil de comportamento construído a partir do histórico de conta do usuário, e o peso comprometido de WCDP. A função de alocação é côncava em ambos, e a concavidade é o design.

Classe de insumo	Exemplos	Direção
Histórico de conta	Tempo de cadastro, liquidações financeiras concluídas, participação anterior em lançamentos, ausência de liquidações atribuíveis a alavancagem excessiva	Crescente, saturante
Marcadores de disciplina	Uso de ordens trabalhadas e saídas condicionais, utilização de margem abaixo dos limites declarados, ausência de infrações repetidas	Crescente, saturante
Stake comprometido	WCDP comprometido antes da janela	Crescente, côncavo
Penalidade de concentração	Capital total comprometido, tamanho de alocação anterior em relação ao pool	Decrescente

O termo saturante faz a maior parte do trabalho de anticoncentração. Um usuário com um histórico grande ganha sobre um usuário novo, e o ganho marginal da décima milésima unidade de histórico é uma fração do ganho marginal da centésima. O stake comprometido tem a mesma forma: o peso cresce com o compromisso, e a taxa de crescimento declina, de modo que o capital não pode se converter linearmente em alocação. Combinado com a penalidade de concentração, um saldo comprometido grande produz uma parcela menor de um pool fixo do que a sua proporção nominal, que é o mecanismo pelo qual um pool de lançamento permanece distribuído, e não capturado.

O compromisso deve preceder a janela por um intervalo mínimo, e o intervalo é longo o suficiente para que tomar stake emprestado para uma janela não seja viável. O peso é medido na época de snapshot, e não de forma contínua, de modo que a elegibilidade de uma submissão é fixada em um momento que todo participante pode ver com antecedência.



Duas coisas que essa função faz mal, declaradas em vez de descobertas pelos participantes. Um usuário disciplinado com muito tempo de cadastro que não compromete nada pode receber uma cota menor do que um trader ativo esperaria, porque o termo de stake comprometido é real e não cosmético — o pool é um recurso escasso e a elegibilidade compete. E o perfil de comportamento usa histórico nesta plataforma, o que significa que um usuário com histórico estabelecido em outro lugar começa em desvantagem. Essa desvantagem é deliberada no curto prazo; o perfil acumula aqui, e importar reputação não é suportado porque não há fonte de reputação que o protocolo possa verificar, em vez de confiar.

Os resultados de alocação, os insumos de elegibilidade e a versão da função em vigor são publicados por janela. Um participante pode recalcular sua própria cota a partir dos insumos publicados, e um participante que acredita que o cálculo estava errado tem o mesmo recurso de qualquer outra contestação prevista no §9.5.

9.0 WCDP: Utilidade do Protocolo e Economia Sustentável de Recursos

O WCDP é a unidade na qual os recursos escassos da rede são precificados, alocados e dados em bond. Sua proposta de valor é inseparável da questão de se esses recursos são genuinamente escassos e genuinamente necessários; um token que não é demandado por operadores e usuários não tem economia para analisar, e nenhum cronograma de oferta repara isso.

9.1 Demanda por Serviço e Obrigações dos Provedores

A rede consome trabalho real em cinco lugares.

Validação de estado. Operadores verificam as provas de época, monitoram a publicação de compromissos e emitem alertas quando uma prova está faltando ou uma raiz é inconsistente. Sua obrigação é disponibilidade e reporte honesto, e a evidência de falha é objetiva: uma época não verificada ou um alerta demonstravelmente falso.

Computação de provas. Gerar provas STARK recursivas para épocas de alto volume é computacionalmente caro. Operadores de prover fornecem essa capacidade sob um acordo de serviço com metas de throughput e latência publicadas, e a prova ou verifica ou não verifica.

Resolução de intenções. A camada de execução do §7.3 requer computação para compilar intenções de usuário em artefatos de regra determinísticos e para avaliar os gates de política. Largura de banda premium — filas de compilação mais curtas, mais intenções ativas simultâneas — é um recurso medido.

Participação em alocação. O protocolo de lançamento do Cap.8 pondera os compromissos elegíveis ao distribuir cotas. Elegibilidade é um recurso do protocolo, não uma reivindicação sobre uma oferta específica, e a cota que um participante recebe é determinada pela função de alocação publicada.

Governança. O voto de parâmetros carrega peso em proporção ao stake comprometido e à duração do lock, conforme o Cap.10 estabelece.

Cada uma dessas funções tem uma contraparte que pode falhar nela e pode ser penalizada por falhar. É daí que origina a demanda pelo token. Operadores devem manter e dar em bond WCDP para serem elegíveis a qualquer dos papéis acima; usuários consomem recursos medidos ou comprometem stake por prioridade e peso. Nenhuma das categorias é um desconto, e nenhuma é discricionária.

9.2 Quatro Recursos do Protocolo

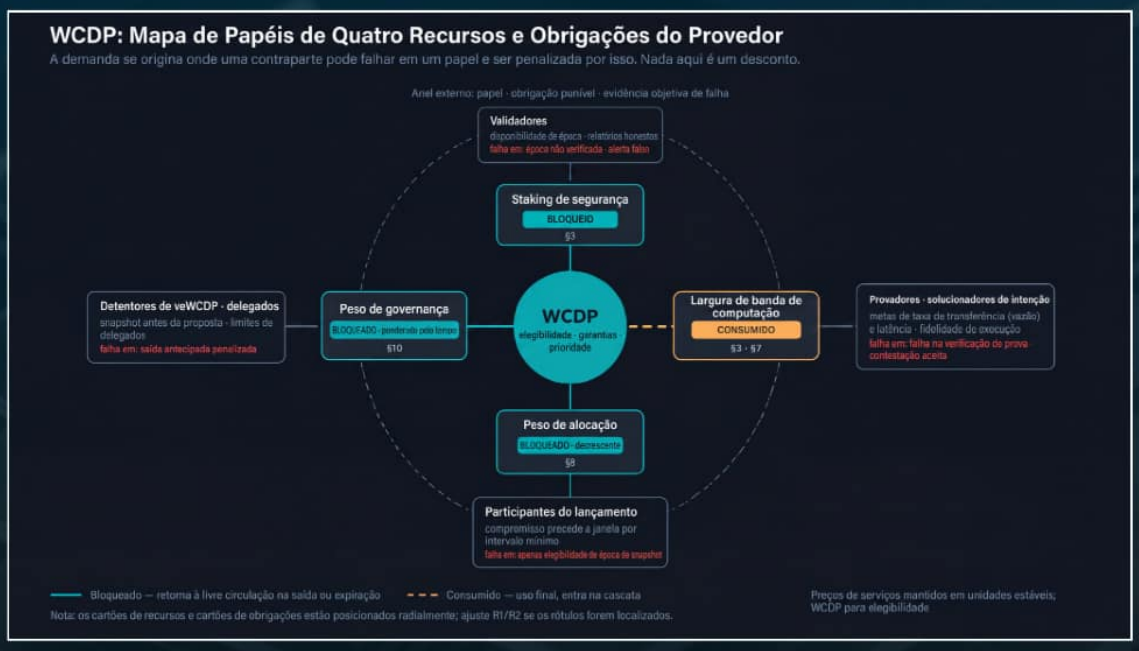
O WCDP acessa quatro recursos distintos, e a distinção entre consumido e travado importa para como cada um se comporta no quadro de oferta.

Staking de segurança é um lock. Validadores aportam WCDP em garantia como condição para verificar épocas e levantar contestações; o stake é devolvido na saída após um período de unbonding, reduzido ou confiscado se o trabalho do operador for considerado desonesto ou negligente por meio do processo de contestação do §9.5.

Largura de banda de computação é consumida. A aquisição de geração de provas e a capacidade de compilação de intenções são compradas com WCDP, e os tokens pagos não são devolvidos — eles são roteados para o waterfall de receitas do §9.4, que é um uso terminal, e não um lock temporário.

Peso de alocação é um lock com efeito decrescente. O stake comprometido antes de uma janela de lançamento carrega peso por meio da função de alocação; o peso não se transfere após a alocação e não sobrevive à janela.

Peso de governança é um lock com uma dimensão temporal. Compromissos mais longos comandam mais peso, conforme o §10.1 especifica, e o lock é liberado apenas no vencimento ou pelo caminho de saída.



Precificar em uma unidade volátil cria fricção que deve ser reconhecida, e não eliminada por pressuposto. O protocolo mantém **os preços de serviço em unidades denominadas em stable** e usa o WCDP para elegibilidade, bonds e prioridade. Um operador aporta WCDP em garantia para se qualificar e depois paga pela computação medida a um preço stable traduzido para WCDP na execução. Isso mantém o contrato legível para um operador com orçamento enquanto mantém a elegibilidade escassa. Significa também que a demanda pelo token vem da exigência de manter e comprometer, que é uma fonte mais durável do que uma unidade de conta flutuante — e menos elástica ao movimento de preço de curto prazo, o que corta nos dois sentidos.

9.3 Arquitetura de Oferta e Lógica de Emissão

A oferta total é fixada em 1,000,000,000 WCDP. Os números abaixo são os parâmetros de gênese; são ajustáveis pela governança apenas dentro dos limites publicados, e os próprios limites são objeto do lock descrito no §10.2.

Alocação	Participação	Termos
Incentivos a validadores e provers	30%	Emitidos contra trabalho verificado por época
Ecossistema e integração	18%	Desenvolvimento de adapters e corredores, condicionado a marcos
Distribuição de lançamento	12%	Distribuída pelo protocolo de alocação do Cap.8
Contribuidores centrais	18%	Cliff, depois linear ao longo das épocas subsequentes
Reserva do protocolo	12%	Mantida em ativos distintos do WCDP; ver §9.5
Provisão de liquidez	10%	Operações de mercado, divulgadas por período

A emissão é o mecanismo de compensação pelo trabalho que a receita de taxas ainda não cobre. O cronograma é indexado por época, não por calendário, e decai por um fator governado a cada época até um piso definido pelo parâmetro mínimo de incentivo. A intenção de design é que a parcela de emissão na remuneração dos operadores caia à medida que a receita proveniente do uso cresce, e o protocolo publica ambas as figuras a cada época para que a substituição seja observável, e não apenas afirmada.

O vesting é expresso em épocas pelo mesmo motivo: a pergunta relevante para o leitor é quanto da oferta se torna líquido em relação aos marcos da rede, e datas de calendário obscurecem isso.

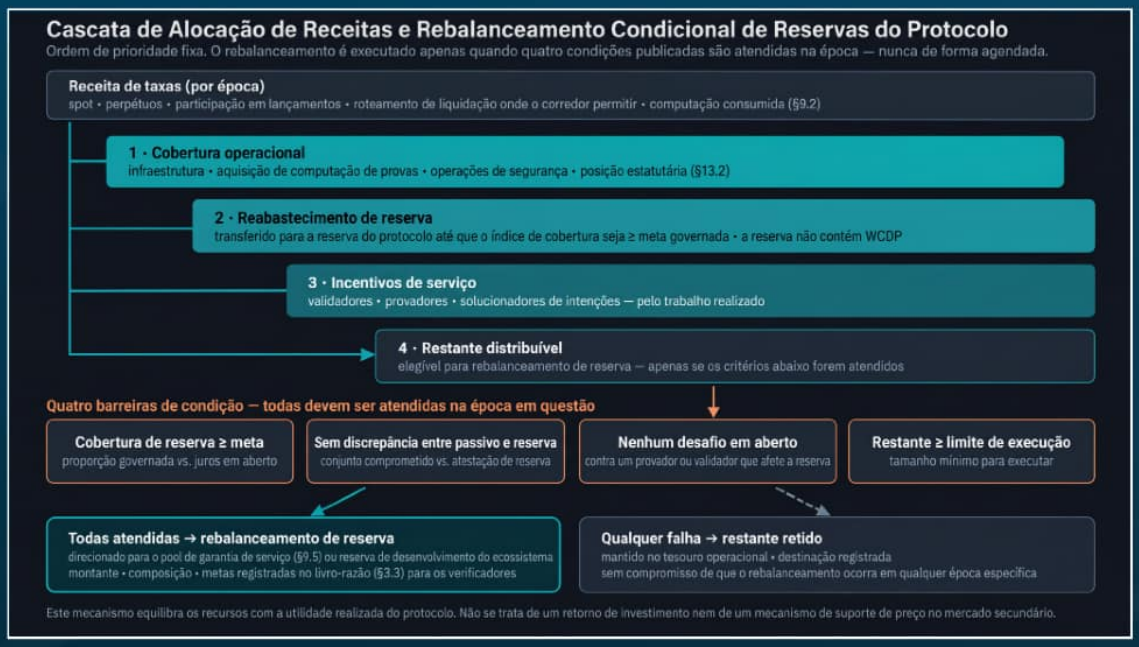
9.4 Alocação da Reserva do Protocolo e Sustentabilidade do Ecossistema

A receita de taxas — spot, perpétuos, participação em lançamentos e roteamento de liquidação onde o corredor o permite — entra em um waterfall com uma ordem de prioridade fixa.

1. **Cobertura operacional.** Infraestrutura, aquisição de computação de provas, operações de segurança e o custo de manter a posição estatutária descrita no §13.2.
2. **Recomposição da reserva.** Varrida para a reserva do protocolo até que a taxa de cobertura da reserva esteja no seu alvo governado ou acima dele.
3. **Incentivos de serviço.** Pagamentos a validadores, provers e solvers de intenções pelo trabalho realizado.
4. **Remanescente distribuível.** O que sobreviver às três primeiras etapas é elegível para rebalanceamento da reserva do protocolo.

O rebalanceamento da reserva do protocolo é governado por regras determinísticas, e não por intervenção arbitrária. Quatro condições publicadas devem ser satisfeitas na época em questão: cobertura da reserva no alvo ou acima dele; nenhuma discrepância não resolvida entre o conjunto de passivos comprometido e a atestação da reserva; nenhuma contestação aberta contra um prover ou validador cujo resultado pudesse afetar a reserva; e um remanescente distribuível acima do limiar mínimo de execução. Quando uma condição falha, o remanescente é retido na tesouraria operacional e a sua destinação é registrada. O rebalanceamento da reserva do protocolo não é executado em um calendário arbitrário.

As alocações de protocolo excedentes são roteadas para o pool de bonds de serviço do §9.5 ou para reservas de desenvolvimento de ecossistema dedicadas, de acordo com parâmetros algorítmicos governados. Ambos os caminhos reforçam a adequação de capital da rede, assegurando profundidade de colateral de longo prazo para corredores de alto throughput. Os eventos de rebalanceamento da reserva do protocolo são publicados diretamente no ledger descrito no §3.3 — registrando valor, composição da reserva e alocações-alvo —, de modo que verificadores independentes possam reconciliar a performance da rede a cada época. Esse mecanismo mantém o equilíbrio de recursos em relação à utilidade realizada do protocolo; ele não constitui retorno sobre investimento nem mecanismo de suporte ao preço no mercado secundário.



9.5 Bonds de Serviço, Slashing e Separação da Reserva

O papel do WCDP na proteção dos usuários é delimitado e específico. Operadores aportam bonds em garantia, denominados em WCDP, que respondem pelas suas próprias obrigações de performance: correção de provas, fidelidade de execução para intenções resolvidas, reporte verídico de telemetria e disponibilidade no nível de época. O slashing é acionado por evidência verificável, e não por julgamento administrativo — uma prova que falha ao verificar, uma contestação resolvida contra um operador, um relato demonstravelmente falso contra o log de eventos brutos. A governança define o tamanho dos bonds e o cronograma de severidade. Ela não decide se uma determinada evidência conta.

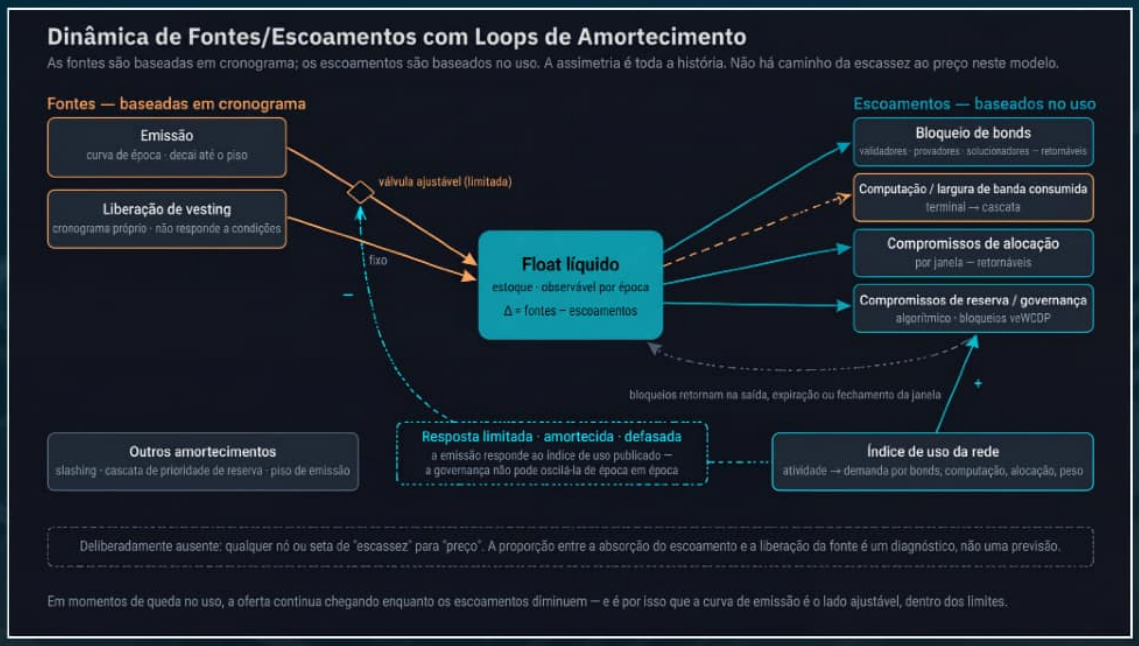
A camada de absorção de perdas para saldos de clientes está em outro lugar. O pool de isolamento que absorve déficits de liquidação, descrito no §5.2, é financiado pela reserva do protocolo, e a reserva é mantida em ativos que não incluem o WCDP. Essa separação é deliberada e é a correção de um desenho que é fácil de escrever e difícil de defender: uma plataforma cujo colchão de segurança é denominado em seu próprio token construiu um mecanismo que enfraquece exatamente quando seus usuários precisam dele, porque as condições que tensionam uma plataforma são as condições que depreciam o seu token.

O slashing transfere o WCDP aportado em garantia do operador penalizado para as partes lesadas ou para a reserva, ou o queima, dependendo do parâmetro em vigor. O capital aportado em garantia está em risco pelo comportamento do operador. Detentores de tokens que mantêm WCDP e nada mais carregam exposição à utilidade da rede, o que é diferente de uma garantia sobre depósitos, e a linguagem de divulgação do protocolo mantém as duas coisas separadas.

9.6 Dinâmica de Fontes e Sumidouros

A oferta entra por emissão e pelos cronogramas de vesting do §9.3. Ela sai do float por quatro sumidouros: locks de bond, computação e largura de banda consumidas, compromissos de alocação e compromissos algorítmicos de reserva. Os dois lados não são simétricos na forma como respondem a condições, e essa assimetria é o cerne da questão.

As fontes são, em grande parte, movidas por cronograma. A emissão segue a curva de época independentemente do uso, e o vesting libera no seu próprio cronograma. Os sumidouros são movidos pelo uso: ninguém aporta em garantia, consome largura de banda ou compromete peso de alocação na ausência de atividade. Em um período de queda de uso, a oferta continua chegando enquanto os sumidouros diminuem, razão pela qual o protocolo trata a curva de emissão como o lado ajustável e lhe dá uma resposta delimitada a um índice de uso publicado, amortecida e defasada para que a governança não consiga movê-la de época em época.



O que essa estrutura fornece é observabilidade. Um leitor ou participante pode ver, época a época, se a demanda por recursos está absorvendo oferta mais rápido do que a emissão e o vesting a liberam. Esse índice é um diagnóstico. Não é uma previsão, e tratar uma leitura favorável como evidência sobre o valor futuro do token seria interpretar erroneamente o que o mecanismo faz.

10.0 Governança de Parâmetros

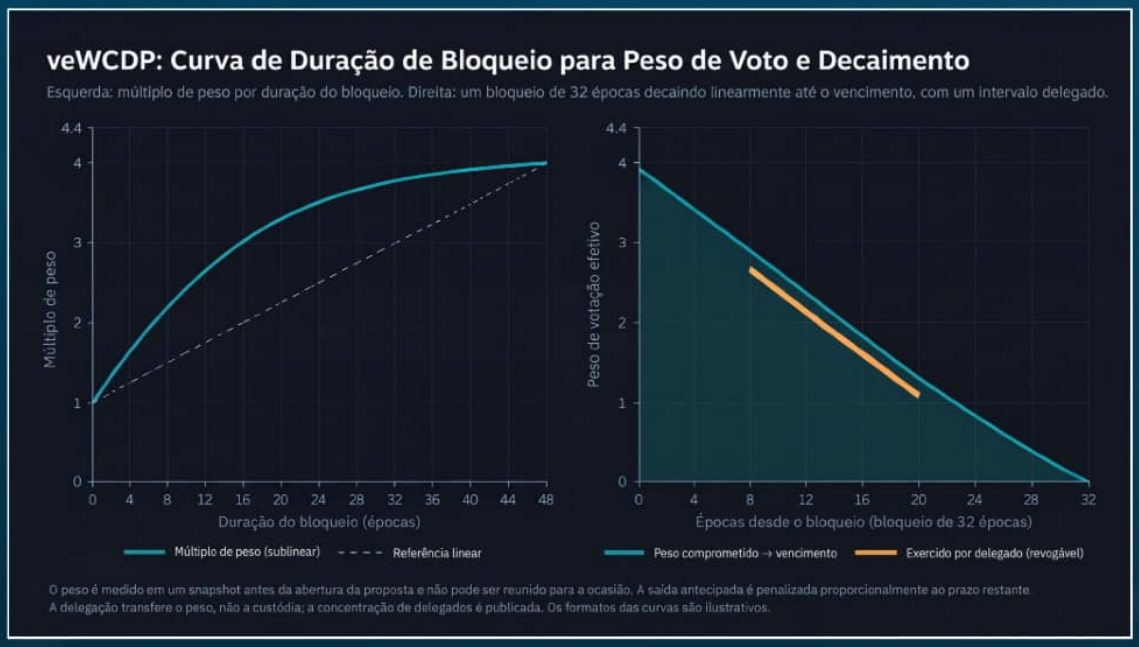
A governança em uma plataforma deste tipo tem um escopo legítimo estreito: decidir onde os controles ficam e ser incapaz de alcançar além deles. A maior parte do argumento neste capítulo diz respeito à segunda metade, já que a primeira é fácil de conceder e a restrição é o que costuma ser esquecido.

10.1 O Modelo veWCDP e o Escopo de Governança

O peso de voto deriva do WCDP comprometido e do comprimento do compromisso. O peso cresce com o valor comprometido, sobe com a duração do lock ao longo de uma curva que se achata além da extremidade longa, e decai linearmente à medida que o lock se aproxima do vencimento. Um votante que deseja influência sobre uma proposta que passa na próxima época precisa ter comprometido antes de a proposta abrir, o que significa que o peso não pode ser montado para a ocasião.

Duração do lock	Múltiplo de peso	Termos de saída
Curto (mínimo)	1×	Liberado no vencimento
Médio	Crescente, sublinear na duração	Liberado no vencimento, ou saída antecipada com penalidade
Longo	Aproximando-se do múltiplo máximo	Liberado no vencimento; saída antecipada penalizada proporcionalmente ao prazo remanescente

A delegação é suportada na medida em que permite que um detentor sem tempo ou expertise para revisar propostas transfira peso a um delegado. A delegação transfere peso, não custódia, e é revogável a qualquer momento, com efeito na próxima janela de proposta. Ela também concentra peso em um pequeno número de delegados, o que é uma fraqueza reconhecida do modelo, e não uma característica de design; a plataforma publica a distribuição de delegados para que a concentração seja mensurável, e limites no peso que um único delegado pode carregar são um parâmetro sujeito ao processo abaixo.



O que a governança pode decidir é enumerado, e a lista é fechada.

- Parâmetros de risco: cobertura-alvo do pool de isolamento, pisos de margem de manutenção, tolerâncias de triagem de mark price e seus limites de ajuste, limites de pausa de lane de liquidação.
- Parâmetros de lançamento: coeficientes da função de alocação, intervalos mínimos de stake, campos do template de divulgação, severidade da penalidade de concentração.
- Parâmetros de emissão e incentivo, dentro dos pisos e tetos fixados na gênese.
- Parâmetros de taxa dentro de limites publicados, e as participações relativas nas prioridades do waterfall de receitas.
- Filiação operacional: padrões de onboarding de validadores e provers, tamanhos de bond, cronogramas de slashing.
- Limites de peso de delegados.

O que ela não pode decidir é uma lista mais curta e mais difícil. A governança não pode mover, congelar ou realocar saldos de usuários; não pode alterar a posição aberta de um usuário nem modificar um fill passado; não pode alterar as chaves de verificação publicadas do sistema de prova nem modificar retroativamente um compromisso; não pode agir sobre o resultado de nenhuma conta individual; e não pode usar o protocolo para estender ou limitar a posição legal societária. Propostas que tentem qualquer uma dessas coisas são rejeitadas na etapa de validação, e não derrotadas em votação, de modo que o resultado não dependa de comparecimento.

10.2 Ciclo de Vida da Proposta e Guardrails de Emergência

Uma proposta passa por etapas com requisitos distintos.

Rascunho e revisão. Um rascunho entra em revisão pública com a mudança de parâmetro especificada como um diff em relação ao valor corrente, a justificativa e, quando aplicável, uma análise de impacto do subsistema afetado — uma mudança de piso de margem sem um resumo de backtest de liquidação não avança. A revisão tem uma duração mínima que escala com a magnitude da mudança.

Votação. A votação roda sobre peso comprometido medido em um snapshot antes do período de revisão abrir. Requisitos de quórum são definidos por classe de parâmetro; mudanças em parâmetros de risco da classe mais alta exigem participação mais alta e supermaioria, o que reduz a frequência com que um pequeno grupo ativo pode mover os parâmetros que determinam se as posições de outros usuários sobrevivem a um dia ruim.

Timelock. Propostas aprovadas aguardam em um timelock antes da execução. O atraso serve a dois propósitos: usuários com posições expostas a uma mudança de parâmetro podem agir durante o intervalo, e uma proposta que passou com base em uma deturpação pode ser retirada.

Execução e janela de observação. O parâmetro entra em vigor, e segue-se uma janela de observação delimitada na qual a mudança pode ser revertida por um procedimento mais estreito do que aquele que a promulgou, desde que a reversão seja também uma mudança de parâmetro publicada. A reversão não está disponível para nada executado na conta de um usuário, porque nada no escopo pode tocar uma.

A autoridade de emergência existe e é deliberadamente restringida, em vez de negada. Um pequeno conjunto de condições — uma falha detectada de verificação de prova, uma quebra de reconciliação de corredor além de um limiar de severidade, uma condição de mercado na qual o processo de quórum ordinário não consegue completar rápido o suficiente para agir — permite uma resposta definida por um grupo restrito retirado dos comitês técnicos do Cap.11, usando um arranjo de multisignatura com um conjunto de signatários publicado. As respostas permitidas são enumeradas com antecedência: suspender admissões nos instrumentos afetados, pausar uma lane de liquidação dentro dos limites do §7.2, tirar um corredor de serviço, suspender a emissão. Cada invocação exige uma justificativa assinada contra a observação que a disparou, é delimitada no tempo e caduca automaticamente se não for ratificada pelo processo ordinário. A autoridade de emergência não pode mover fundos, alterar posições nem mudar o sistema de prova.

O relato honesto desse arranjo é que ele troca um processo mais lento e mais legítimo por uma ação temporária mais rápida por um grupo menor, improvável e delimitada, e que a troca favorece velocidade durante eventos em que uma decisã

o atrasada é ela mesma uma decisão. Usuários que achem a troca pouco atrativa devem pesá-la contra a alternativa — um mecanismo automático, que é ainda mais rápido e não consegue exercer julgamento sobre uma situação que ninguém antecipou.

11.0 Equipe de Arquitetura Central

O protocolo WCDPQ é administrado por meio de um modelo de fundação de desenvolvimento de código aberto. Seguindo padrões da indústria para protocolos descentralizados, as contribuições técnicas centrais iniciais são orquestradas por fluxos de trabalho de engenharia especializados e comitês de revisão técnica independentes. A transição para governança ampla de conselho de fundação e delegações verificadas de contribuidores institucionais prossegue sob o framework de RFC delineado abaixo.

11.1 Princípios Organizacionais e Comitês Técnicos

O modelo operacional é extraído da prática de fundações de código aberto, e não de uma organização corporativa de produto, por uma razão que é técnica, e não cultural. As propriedades caras do sistema — solidez de prova, replay determinístico, isolamento de risco — são do tipo que falha silenciosamente sob pressão de cronograma. Uma estrutura na qual um engenheiro-chefe pode entregar uma mudança de restrição sem que uma segunda parte que compreenda o circuito a revise produzirá, sob prazo, exatamente essa falha.

Três coisas decorrem dessa premissa.

O trabalho prossegue por meio de RFCs publicados. Uma mudança material em um subsistema entra como uma proposta escrita, com especificação, um argumento de segurança quando aplicável e um caminho de migração. O RFC é público, sua revisão fica registrada, e a implementação resultante é rastreável até ele. Isso é mais lento do que commitar uma correção, e a alternativa foi testada extensivamente em outros lugares.

A autoridade de revisão é separada da autoria. O comitê de criptografia aprova mudanças de restrições de circuito e atualizações de parâmetros de prova; o comitê de risco aprova mudanças de margem, liquidação e metodologia de mark price junto com os backtests de suporte; o comitê de economia do protocolo aprova os parâmetros de emissão, taxa, bond e função de alocação. Um membro de comitê empregado na equipe que escreveu uma mudança pode participar, mas não conta para nenhum quórum de aprovação para ela.

A autoridade é delimitada por assunto. Nenhum dos três comitês pode revogar outro fora do seu domínio — o comitê de risco não pode relaxar uma restrição de circuito, e o comitê de criptografia não pode ajustar um piso de margem de manutenção —, o que força o desacordo a entrar em uma proposta, e não em uma escalação privada.

11.2 A Matriz de Especificação de Funções

Função	Responsabilidade central	Baseline de capacidade	Comitê
Chief Protocol Architect	Invariantes entre subsistemas; arbitragem de RFC; estabilidade de interface entre as camadas de verificação, execução e liquidação financeira	Arquitetura de sistemas distribuídos em escala de exchange ou comparável; histórico de projeto de protocolo multi-anos	Presidente, ex officio
Cryptography Lead (ZK e MPC)	Correção de sistema de restrições; seleção de parâmetros de prova; desenho de ciclo de vida de assinatura de limiar	Criptografia aplicada; sistemas de prova STARK ou SNARK em produção; implementações de assinatura de limiar; background em verificação formal	Criptografia
Formal Verification Lead	Provas conferidas por máquina de restrições críticas; suítes de teste diferencial e adversarial; argumentos de solidez do verificador	Métodos formais; provadores de teorema interativos ou model checkers; verificação de protocolo contra modelos adversariais	Criptografia
Matching Engine Lead	Determinismo de sequenciamento; desenho de livro shardizado; máquina de estados de degradação e comportamento de lane prioritária	Engenharia de sistemas de baixa latência; desenho de sistema determinístico; teste de capacidade e modo de falha sob carga adversarial	Risco

Risk Systems Lead	Metodologia de margem; waterfall de liquidação; composição de mark price; dimensionamento de pool de isolamento e procedimentos de recuperação	Risco quantitativo em plataformas de derivativos; desenho de modelo de margem; padrões de evidência de liquidação e backtesting	Risco
ML and Telemetry Lead	Desenho de detector; disciplina de avaliação fora da amostra; registro de modelo e política de rebaixamento	ML aplicado com métodos de séries temporais ou grafo; metodologia de avaliação; monitoramento em produção de decay de modelo	Risco
Protocol Economics Lead	Mecânicas de emissão e taxa; cronogramas de bond e slashing; desenho de função de alocação e simulação	Design de mecanismos ou economia de tokens com trabalho publicado; análise de jogos adversariais; disciplina de calibração empírica	Economia do protocolo
Payment Infrastructure Lead	Contrato de adapter; schema de reconciliação; certificação de corredor; semânticas de finalidade por corredor	Integração de sistemas de pagamento; operações de reconciliação e liquidação; implantação de corredor multi-jurisdição	Economia do protocolo
Security and Access Lead	Distribuição de chaves; separação de acessos; monitoramento; resposta a incidentes	Segurança de infraestrutura; gestão de chaves; comando de incidentes em sistemas financeiros	Criptografia
Governance and Open-Source Steward	Integridade do processo de RFC; ciclo de vida da proposta e operações de timelock; caminhos de contribuidor; obrigações de publicação	Governança de fundação de código aberto; gestão de processo de especificação	Ex officio, sem voto

Duas linhas nessa tabela estão fazendo trabalho que um organograma de engenharia convencional deixaria implícito. A função de verificação formal existe porque sistemas criptográficos falham na fronteira de especificação mais frequentemente do que na matemática: um circuito que prova a afirmação errada é sólido e inútil. E o steward de governança é uma função técnica aqui, não administrativa, porque o timelock, o snapshot e o maquinário de parâmetros de emissão descritos no Cap.10 são código cuja correção determina se as promessas de governança se sustentam.

Metas de cobertura são publicadas, e não declaradas como intenções. Cada comitê mantém um mínimo de revisores independentes por domínio e, onde um domínio tem menos do que o mínimo — uma condição real para um protocolo jovem em um campo especializado —, o protocolo publica o déficit e restringe as classes de parâmetro que aquele comitê pode aprovar. Um comitê que não consegue prover revisão de mudanças de alta consequência não pode aprová-las por padrão.

11.3 Código Aberto e Contribuição Externa

Implementações de verificador, o verificador de linha de comando, SDKs de cliente, o schema de reconciliação e os documentos de especificação são públicos. A intenção é que uma parte independente possa construir um verificador a partir da especificação sem usar código fornecido pelo protocolo, e que o schema de reconciliação seja aberto para que um parceiro de corredor ou um órgão supervisor possa consumi-lo com seu próprio ferramental.

O caminho crítico não é aberto, e a fronteira é traçada onde está por uma razão declarada. Internos do motor de matching, implementação do motor de risco, operações de gestão de chaves e telemetria sensível permanecem fechados, porque publicá-los estreita o espaço de busca de um atacante mais rápido do que amplia o pool de revisores. O que é conferível por partes externas é a propriedade que importa para a confiança — se o estado comprometido segue das regras publicadas —, e essa propriedade é conferível por meio do sistema de prova e do cliente, ambos públicos. Um caminho de contribuição existe dos componentes abertos para dentro: contribuições verificadas às camadas públicas, participação sustentada em revisão e patrocínio de comitê são a rota para o envolvimento nos fechados.

12.0 Roadmap de Evolução

Embora a entrega técnica seja estritamente condicionada por marcos criptográficos e operacionais verificados, e não por prazos arbitrários, o protocolo alinha suas épocas de desenvolvimento com janelas de release sequenciais indicativas para coordenar auditoria e integração do ecossistema.

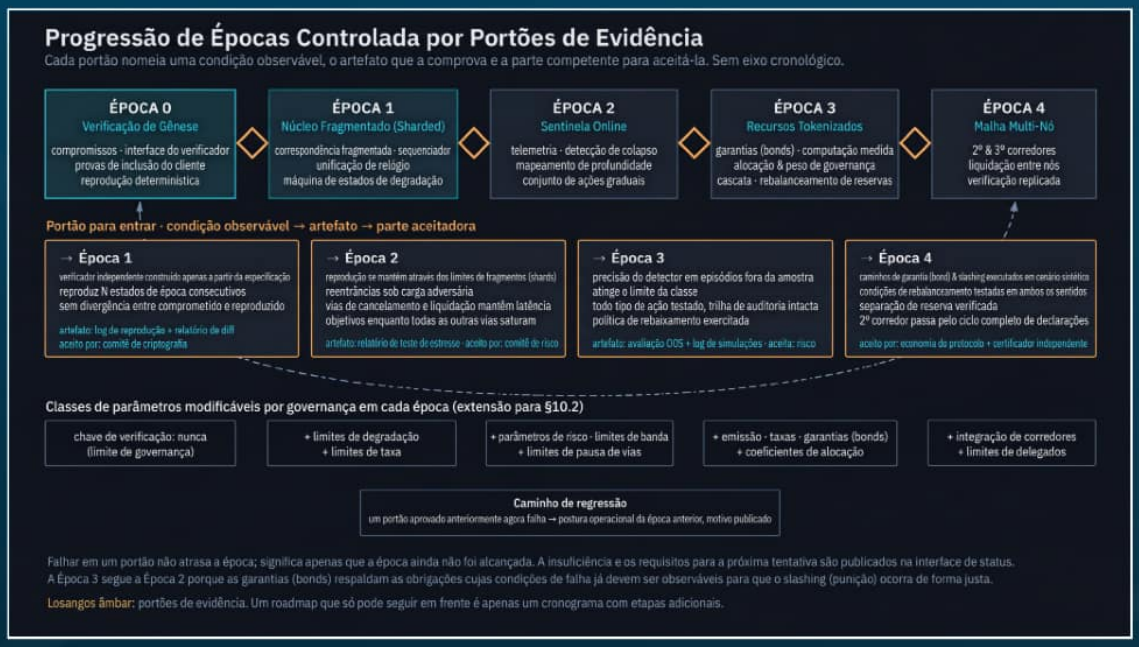
12.1 Filosofia de Condicionamento e Definições de Época

Cada transição de época é condicionada por evidência, e não por tempo transcorrido. Um gate nomeia uma condição observável, o artefato que a demonstra e a parte competente para aceitar a demonstração. Falhar em um gate não atrasa a época; significa que a época não foi alcançada, e o déficit medido é publicado com os requisitos da próxima tentativa.

Época	Escopo	Gate para entrar	**Horizonte Indicativo**
0 — Genesis Verification	Publicação de compromisso, interface de verificador, provas de inclusão no lado do cliente, replay determinístico de ledger	Verificador independente implementado apenas a partir da especificação reproduz 30 estados de época consecutivos; nenhuma divergência não resolvida entre estado comprometido e replayado ao longo da janela	2026 Q3-Q4 Foundation Release
1 — Sharded Core	Matching shardizado, sequenciamento global, unificação de relógio, máquina de estados de degradação	Replay determinístico se mantém entre eventos de fronteira de shard sob carga adversarial; lanes de cancelamento e liquidação mantêm objetivos de latência declarados por meio de uma rodada de estresse que satura todas as outras lanes	Phase I Network Calibration

2 — Sentinel Online	Telemetria, detecção de colapso de correlação, mapeamento de profundidade, conjunto de ações graduado	Performance de detector publicada em episódios fora da amostra atinge o limiar de precisão para a sua classe; cada tipo de ação invocado em exercício controlado (drill) com trilha de auditoria intacta; política de rebaixamento exercida	Phase II Advanced Telemetry
3 — Tokenized Resources	Bonds, computação medida, peso de alocação, peso de governança, waterfall de receitas, rebalanceamento de reserva	Caminhos de bond e slashing executados contra caso de evidência sintético; condições de rebalanceamento de reserva avaliadas em estados satisfeitos e não satisfeitos; separação de reserva verificada com o auditor de reserva de registro	Phase III Utility Activation
4 — Multi-Node Mesh	Implantações de segundo e terceiro corredores, liquidação entre nós, verificação replicada	Segundo corredor passa certificação de reconciliação ao longo de um ciclo de extrato completo; verificadores independentes operando de uma segunda jurisdição confirmam provas de época sem ferramental fornecido pelo protocolo	Phase IV Cross-Corridor Expansion

A Época 0 precede tudo porque uma prova que ninguém verificou é uma alegação. A Época 3 segue a Época 2, em vez de rodar em paralelo com ela, porque bonds de token ficam por trás de obrigações de operador, e uma obrigação cujas condições de falha ainda não são observáveis não pode sofrer slashing de forma justa.



O status de gate publicado é uma obrigação permanente, e não um anúncio de release. Estado corrente, último resultado medido e déficit remanescente para o próximo gate estão na superfície de status a cada época, o que significa que um leitor pode formar uma visão sobre o progresso sem depender de um resumo produzido para ele.

12.2 O Playbook de Replicação de Super-Nó e Rollback

O template do §1.3 instancia em uma ordem fixa, e a ordem é o playbook.

Um adapter é construído contra o contrato RPAL e certificado contra a suíte de reconciliação. Um conjunto de parâmetros é derivado para o corredor: parâmetros de risco localizados contra profundidade e volatilidade observadas naquele mercado, posicionamento de nó otimizado para latência e definições de finalidade específicas do corredor. A configuração de corredor do cliente móvel é adicionada. O corredor roda em modo restrito, com volume de entrada limitado, até que a reconciliação complete um ciclo completo sem itens não resolvidos, e só então carrega tráfego sem limites.

A certificação de um novo corredor é executada por partes independentes do proprietário de negócios do corredor, o que evita que uma entrada de mercado seja aprovada por quem a negociou. A liquidação entre nós é adicionada apenas após um corredor ter passado na sua própria certificação, de modo que um caminho de liquidação nunca dependa de um nó ainda se provando.



Ambos os eixos de evolução têm caminhos de rollback, e ambos são exercidos, e não apenas documentados. Uma mudança de parâmetro que produz um resultado fora do seu intervalo de impacto previsto reverte pela janela de observação do §10.2. Um corredor que falha na reconciliação além do limiar é suspenso para tráfego de entrada e reverte para sua última versão de adapter certificada, com os saldos existentes dos usuários não afetados, porque a suspensão de corredor nunca toca o ledger. Uma época que regride — uma medição subsequente falhando em um gate que ela havia passado anteriormente — devolve a rede à postura operacional da época anterior, com o motivo publicado. O tratamento de regressão é a parte de um roadmap condicional que decide se a condicionalidade é real; um roadmap que só pode avançar é um cronograma com etapas extras.

13.0 Fatores de Risco, Divulgações e Apêndices

Os riscos abaixo são aqueles que esta arquitetura não remove, e não os que ela endereça. Um leitor que acompanhou os Caps.3 a 9 viu os mecanismos; este capítulo trata do que permanece exposto após eles funcionarem como pretendido.

13.1 Riscos Técnicos, de Mercado e de Token

Defeitos de sistema de restrições. Um bug no circuito pode tornar uma transição inválida passível de comprovação formal, ou tornar uma transição válida impossível de ser provada. O primeiro é o caso sério: a prova verifica e diz a coisa

errada. A verificação formal contra a especificação reduz essa classe e não consegue eliminá-la, já que a própria especificação é escrita pelas mesmas pessoas que escreveram o circuito. As defesas práticas são a especificação ser pública, múltiplas implementações independentes do verificador e o fato de que um defeito se torna visível como divergência entre o estado comprometido e o estado replayado independentemente, e não como uma perda silenciosa.

Comprometimento de chave aquém de limiar. O roubo dos shares de um único operador não permite uma transferência, dado um esquema de limiar operando apropriadamente. Uma falha de implementação que reconstrói mais do que deveria, um backup contendo shares em um único local ou uma implantação na qual vários detentores de shares rodam imagens comprometidas idênticas permitem. A separação geográfica e operacional dos detentores de shares é uma mitigação cuja eficácia depende de ser mantida continuamente, e é uma condição que se desgasta pela conveniência ordinária.

Falha de oráculo e dados de referência. Mark prices dependem de fontes externas. Uma fonte que reporta dados obsoletos sem dizê-lo, um conjunto que se correlaciona porque várias plataformas derivam do mesmo feed subjacente, ou uma tentativa coordenada de mover um mercado de referência fino, todas degradam a precisão de liquidação. Triagem, exclusão e influência delimitada limitam o dano ao longo de intervalos curtos. Não protegem contra um erro de precificação sustentado que passe na triagem, e posições liquidadas contra tal preço são liquidadas.

Falha de detector em ambas as direções. Um detector que falha em disparar deixa a plataforma em seu estado ordinário durante uma cascata. Um detector que dispara de forma espúria restringe a admissão de ordens ou alarga as bandas de preço durante a negociação ordinária, o que custa acesso aos usuários e, no caso do alargamento de banda, desloca insumos de liquidação. Precisão e recall publicados por classe de episódio delimitam quão bem as taxas de falha são conhecidas; não as tornam pequenas, e o sinal de colapso de correlação depende de episódios históricos que uma estrutura de mercado suficientemente nova não se parecerá.

Obsolescência de modelo e parâmetro. Pisos de margem, tolerâncias de triagem e coeficientes de alocação são calibrados contra condições que mudam. Um drift lento deixa o sistema operando corretamente contra um mundo que não existe mais. A recalibração periódica é um compromisso de governança, o que significa que sua qualidade depende de a participação descrita no Cap.10 permanecer genuína.

Riscos de mercado e liquidez. Movimentos extremos podem exaurir o pool de isolamento, momento em que o caminho de recuperação é uma decisão governada com as consequências descritas no §5.2. Instrumentos de stablecoin usados na liquidação carregam riscos de emissor, resgate e peg que não estão sob controle da plataforma; um depeg afeta o valor dos saldos denominados naquela unidade independentemente da correção do ledger que os registra. Corredores

podem ser interrompidos por mudanças no gateway ou no arranjo bancário subjacente, deixando a capacidade dos usuários de mover fundos para dentro ou para fora impossibilitada, mesmo quando a plataforma está funcionando normalmente.

Riscos específicos do token. A utilidade do WCDP depende da atividade da rede. A demanda por bonds, computação medida, elegibilidade de alocação e peso de governança é demanda derivada, e se os serviços da rede perderem usuários, essa demanda cai independentemente do cronograma de oferta. O vesting das alocações do §9.3 libera oferta em um cronograma que não responde a condições. Parâmetros de governança — taxas de emissão, tamanhos de bond, prioridades do waterfall, coeficientes de alocação — podem ser alterados pelo processo do Cap.10, e a expectativa de um detentor sobre utilidade futura pode ser alterada por um voto do qual ele não participou. Bonds sofrem slashing pelo comportamento de operador, de modo que um detentor que faz stake em uma função de validação carrega exposição ao comportamento daquele operador. E o rebalanceamento da reserva do protocolo financiado por receita de taxas executa estritamente sujeito às quatro condições de sustentabilidade especificadas no §9.4; não há compromisso ou representação de que distribuições de reserva ocorrerão em qualquer época dada.

Concentração de delegados. O modelo veWCDP concentra peso de governança efetivo ao longo do tempo à medida que detentores delegam. Limites de peso de delegado são um parâmetro, e um parâmetro pode ser alterado, inclusive pelos delegados que ele restringe.

13.2 Declaração de Fronteira Regulatória

O WCDPQ é desenvolvido e publicado como uma especificação técnica de código aberto e um protocolo de software administrado por entidades de fundação internacionais. Os desenvolvedores do protocolo e os contribuidores da fundação não operam uma exchange, corretora ou clearinghouse custodial no Brasil nem em qualquer jurisdição específica.

A conversão de moeda local, a liquidação de gateway fiat e o onboarding direto de usuários são geridos independentemente por parceiros regionais terceirizados licenciados, operando sob suas respectivas autorizações regulatórias locais. A negociação de ativos digitais carrega risco de capital inerente, e performance simulada passada não indica resultados futuros. Nada aqui contido constitui oferta de valores mobiliários, esquemas de investimento coletivo ou solicitação financeira em qualquer território.

Apêndice: Especificações do Sistema de Prova Criptográfica

A.1 Corpo, hashes, separação de domínio

A aritmética roda sobre o corpo de Goldilocks de 64 bits

$$p = 2^{64} - 2^{32} + 1$$

com suporte nativo para decomposição de intervalo de 64 bits. Todo hashing em circuito usa Poseidon2 sobre esse corpo, largura 12, taxa de estado 8. Digests externos usam BLAKE3-256 sobre a codificação canônica de byte dos mesmos elementos de corpo, prefixada por um domain tag.

A.2 Estrutura de compromisso de passivos

O compromisso global sobre k ativos:

$$C_{\varepsilon} = \mathrm{BLAKE3}\left(\text{WCDP-EPOCH-v1} \parallel \varepsilon \parallel a_1 \parallel R_1 \parallel \cdots \parallel a_k \parallel R_k\right)$$

A preimagem de folha cegada para a conta u no ativo a na época ε:

$$l(u, a, \varepsilon) = \mathrm{Poseidon2}\left(H(u) \parallel \nu(u, \varepsilon) \parallel b(u, a, \varepsilon) \parallel \tau(a)\right)$$

onde a referência de conta é

$$H(u) = \mathrm{BLAKE3}\left(\text{user-id} \parallel \text{account-salt}\right) \bmod p$$

e $\nu(u, \varepsilon)$ é o nonce rotativo, b o saldo de 64 bits sem sinal em unidades base, τ a tag de ativo. Nós internos carregam um digest e uma soma aritmética:

$$\Sigma(N) = \Sigma(L) + \Sigma(R)$$

$$D(N) = \mathrm{Poseidon2}\left(D(L) \parallel \Sigma(L) \parallel D(R) \parallel \Sigma(R)\right)$$

A raiz publica o par $(D_{\mathrm{root}}, \Sigma_{\mathrm{root}})$, de modo que passivos totais por ativo são legíveis sem uma travessia de árvore. Saldos de nós internos e somas agregadas são representados usando composições de limb de 64 bits para prevenir nativamente overflow entre representações de token padrão de 18 decimais, com verificações de fronteira de corpo aplicadas pelo circuito.

A.3 Restrições de intervalo e consistência

Cada saldo é decomposto em quatro limbs de 16 bits, cada um restringido por uma busca em uma tabela comprometida na gênese:

$$b = \sum_{i=0}^{3} b_i \, 2^{16i}, \qquad b_i \in \left[0, \; 2^{16}\right)$$

Uma árvore contendo uma folha fora de intervalo falha na geração de prova para a época. Não há caminho de bypass.

A.4 Circuito de transição

Entradas públicas por lote:

$$(C_{\varepsilon-1},\ C_{\varepsilon},\ [s_{\text{lo}}, s_{\text{hi}}],\ h_{\text{rules}})$$

Contagens de restrição por lote no build de referência:

$$2^{18} \ \leq \ c_{\text{batch}} \ \leq \ 2^{21}$$

Lotes acima do teto dividem. O teto é um parâmetro de performance de prover, não uma afirmação de throughput.

A.5 Configuração e custo do FRI

O FRI roda com fator de blowup 8, fator de folding 8, contagem de query $q = 28$ e dificuldade de grinding $w = 16$ bits, visando erro de solidez conjecturado

$$\epsilon_{\text{sound}} \ \leq \ 2^{-100}$$

Medido na máquina de referência:

$$t^{\text{batch}}_{\text{verify}} < 50 \text{ ms}, \qquad t^{\text{epoch}}_{\text{verify}} < 400 \text{ ms}, \qquad 150 \text{ KB} \ \leq \ |\pi_{\text{batch}}| \ \leq \ 320 \text{ KB}$$

Um release de circuito que move o custo de verificação em mais de

$$\frac{\Delta t_{\text{verify}}}{t_{\text{verify}}} > 0.25$$

exige uma nova medição de referência antes da ativação.

A.6 Recursão e a raiz de época

Aridade e profundidade da árvore de recursão:

$$a = 8, \qquad \delta_{\max} = 3 \quad \Rightarrow \quad a^{\delta_{\max}} = 512 \text{batches per epoch proof}$$

O artefato de época que uma terceira parte verifica é a tripla $(\pi_{\varepsilon},\ C_{\varepsilon-1},\ C_{\varepsilon})$.

A.7 Fronteira de época

Uma época fecha no primeiro de:

$$n_{\text{events}} = 2^{22} \quad \text{or} \quad \Delta t = 86,400 \text{ s}$$

Ambos os disparadores são ajustáveis dentro dos parâmetros de fronteira governados definidos no Cap.10.