Φ Phinancer Hiper-DEX — White Paper

Uma Nova Era para o Mercado Financeiro Descentralizado

Versão 0.2 • Março 2026

Pedro Pustiglione • Founder & CEO

phinancer.com

Sumário

1. Resumo Executivo

A Φ Phinancer Hiper-DEX é uma infraestrutura de exchange descentralizada de nova geração, construída sobre uma blockchain própria, que redefine a forma como os serviços financeiros são construídos, oferecidos e consumidos no ambiente cripto. Diferentemente de uma exchange tradicional, trata-se de uma Hiper-DEX: um protocolo descentralizado que possibilita a criação de múltiplas exchanges, corretoras, agentes de investimento, emissoras de ativos e prestadores de serviços tokenizados, todos interconectados em uma única camada global de liquidez.

Combinando staking, certificações, contratos inteligentes auditáveis e governança comunitária progressiva, a plataforma permite que qualquer participante — de um pequeno agente a uma grande instituição — atue com segurança, flexibilidade e reconhecimento baseado em reputação e performance.

Seu token nativo, HDEX, integra governança, segurança, incentivo e acesso a funcionalidades estratégicas do ecossistema. Todas as taxas de gas são pagas exclusivamente em HDEX, com um serviço interno de auto-conversão para facilitar o uso. O modelo econômico foi desenhado para promover a descentralização e a sustentabilidade, com

um supply máximo de 10 bilhões de tokens e uma estrutura de distribuição que privilegia o crescimento orgânico ao longo de seis fases de desenvolvimento.

A privacidade é um princípio fundamental e inviolável: todas as transações do token HDEX são anônimas por padrão, com validação cega pelos servidores, sem nenhuma master key para qualquer entidade — incluindo a própria Foundation. O remetente pode opcionalmente revelar os dados de uma transação específica para fins de compliance em jurisdições que exigem transparência.

A proposta da Φ Phinancer Hiper-DEX é ser a base da infraestrutura financeira descentralizada do futuro — como um "Shopify para DeFi" — permitindo que novos serviços surjam de forma plugável e interoperável, enquanto garante que os usuários mantenham o controle absoluto sobre seus ativos e privacidade.

2. Introdução

O ecossistema Phinancer é uma revolução no mundo das transações financeiras, trazendo infraestrutura para a criação de todo um ecossistema de plataformas descentralizadas feitas para facilitar a adoção, o crescimento e a capilaridade.

Introduzimos o conceito de Hiper-DEX: uma infraestrutura de blockchain própria que serve como base para a criação de sistemas financeiros totalmente descentralizados e ao mesmo tempo conectados, resolvendo problemas como o excesso de centralização e a falta de liquidez. Este sistema permite que exchanges criadas na Hiper-DEX, mesmo com uma pequena base de clientes, tenham acesso à liquidez global, estimulando a criação de inúmeros novos serviços financeiros. Por menor que seja, todo participante terá acesso ao mercado global.

A Phinancer Hiper-DEX é a conexão necessária para que o mercado cripto atinja o máximo de capilaridade e adoção. Incluindo múltiplos ativos (HDEX, stablecoins, commodity tokens), contratos inteligentes, flexibilidade para os usuários e uma estrutura meritocrática, a plataforma é desenhada para ser a ferramenta financeira mais capilarizada do mundo.

A blockchain será construída do zero, aplicando as tecnologias mais eficientes disponíveis, utilizando uma linguagem de programação existente adaptada ao projeto, garantindo liberdade total de design e máxima performance.

3. Problemas Atuais no Setor de Exchanges

O mercado de exchanges enfrenta desafios que limitam a verdadeira adoção em larga escala e o empoderamento dos usuários:

- Risco de custódia centralizada: Usuários dependem da guarda de ativos por terceiros, expondo-se a riscos de hacks, má administração e bloqueios de fundos.
- Falta de privacidade e anonimato: A maioria das exchanges exige KYC invasivo. A Φ Phinancer resolve isso tornando o anonimato obrigatório por design em todas as transações on-chain, com validação cega pelos servidores da rede.
- Governança centralizada e opaca: Mudanças em regras e taxas são feitas por decisões arbitrárias, sem consulta aos usuários ou transparência.
- Baixa integração com moedas fiat: A entrada e saída do ecossistema cripto ainda é complexa e dependente de gateways centralizados.
- Falta de flexibilidade regulatória: Usuários são tratados uniformemente, sem considerar contextos distintos de uso, países e tipos de operações.
- Dependência de liquidez local: Exchanges menores não conseguem competir com grandes players pela liquidez, prejudicando a inovação e limitando o acesso.

- Falta de incentivo à descentralização real: Muitas DEXs ainda concentram poder em times centrais, limitando a participação efetiva da comunidade.
- Dificuldade de escalar serviços financeiros: Não há infraestrutura para que agentes, emissores e prestadores de serviço operem de forma integrada dentro do ecossistema.

4. Visão Geral do Ecossistema

A Hiper-DEX funciona como uma infraestrutura completa onde múltiplos participantes interagem em camadas complementares:

Camada de Infraestrutura: Servidores (Processing Servers) que validam transações e armazenam dados da blockchain, garantindo segurança e disponibilidade da rede.

Camada de Serviços Financeiros: Corretoras que criam instrumentos financeiros, pares de trading e commodity tokens; Seguradoras que oferecem apólices via smart contracts; Fiat Gates que fazem a ponte entre o sistema bancário e o universo cripto.

Camada de Atendimento: Bankers (Agentes) que atendem investidores, orientam operações e fazem a aquisição de novos clientes. Todo investidor é obrigatoriamente vinculado a um Agente — seja de uma Corretora parceira ou do Agente híbrido da Foundation (bot + humano).

Camada de Desenvolvimento: Desenvolvedores Autorizados que criam smart contracts e soluções; Analistas que produzem conteúdo e análises de mercado; Plataformas terceiras que constroem front-ends acessando a rede via APIs.

Camada de Governança: A Phinancer Foundation controla as fases iniciais com descentralização progressiva rumo a uma DAO plena. Detentores de HDEX participam de votações, e a Foundation mantém tokens HDEX10 (com poder de voto 10x) como mecanismo de proteção de longo prazo.

Todos os participantes operam sobre uma camada global de liquidez compartilhada: cada pool AMM é único por par de ativos e acessível a todas as Corretoras simultaneamente, garantindo que mesmo a menor Corretora tenha acesso à liquidez do mercado global.

5. Sistema Multi-Ativos

O ecossistema Phinancer opera com múltiplos ativos, cada um com funções e regras de privacidade específicas:

5.1 HDEX — Token Nativo

O HDEX é o token principal do ecossistema, utilizado para pagamento de todas as taxas de gas, staking para certificações, participação em governança e como meio de troca principal. Todas as transações de HDEX são anônimas por padrão, com privacidade máxima e inviolável — nenhuma entidade, incluindo a Foundation, tem capacidade de rastrear transações.

O remetente de uma transação pode opcionalmente ativar a revelação binária, tornando visíveis o endereço de origem, o valor e o endereço de destino daquela transação específica. Esta opção existe para permitir o crescimento legal em jurisdições onde o anonimato total é proibido por lei. A revelação é binária: ou revela tudo ou não revela nada, sem opções intermediárias.

5.2 HDEX10 — Token de Governança Premium

O HDEX10 é uma classe especial de token com poder de voto permanente de 10x em todas as votações da rede. Inicialmente, 1 bilhão de HDEX10 estão sob controle da Foundation como mecanismo de proteção e governança de longo prazo. Os HDEX10 são fracionáveis e mantêm o poder de 10x independente da divisão, podendo ser negociados no mercado onde naturalmente terão um prêmio pelo poder de voto que conferem.

5.3 PHDSC — PH Dollar Stable Coin

Stablecoin com lastro 1:1 em dólares americanos, emitida exclusivamente pela Foundation e suas sub-estruturas especializadas (com CNPJ próprio). A Foundation custodia as garantias e obtém receita através da aplicação financeira desses recursos. A comprovação do lastro 1:1 será feita através de auditorias periódicas independentes com resultados publicados. O modelo é replicável para outras moedas fiduciárias (PHBSC para Real, PHESC para Euro, etc.), alterando apenas a nomenclatura e o lastro correspondente. A PHDSC será lançada na fase Spreading.

Por ser um ativo regulado, a PHDSC pode ter módulos de controle administrativo operados pela Foundation, incluindo a possibilidade de bloqueio global de carteiras específicas mediante ordem judicial. O nível de privacidade da PHDSC é definido pela Foundation e pode diferir do HDEX para atender requisitos legais.

5.4 PH Commodities — Tokens de Commodities

Tokens lastreados em commodities, emitidos por Corretoras que definem as regras do contrato, incluindo o nível de privacidade do ativo. A garantia é financeira — a Corretora bloqueia capital suficiente em HDEX ou stablecoin (o que melhor se enquadrar) dentro do próprio smart contract do commodity, que contém todas as regras e garantias de forma autônoma e auditável. Cada commodity token pode ser negociado em qualquer Corretora da rede, não apenas na emissora, e a Corretora criadora recebe um royalty sobre toda a corretagem daquele contrato em qualquer Corretora. O royalty está incluído dentro do cap de 10% de taxas de serviço da rede, evitando abusos. O valor do royalty é definido livremente pelo criador, e a adoção pelo mercado funciona como regulador natural — quanto menor a taxa, maior a adoção.

5.5 PHIPC — Inflation Proof Currency

Moeda projetada para ser resistente à inflação. Os detalhes e implementação estão previstos para as fases Takeover/Legacy do projeto.

5.6 sHDEX — Token de Liquid Staking Nativo

sHDEX é o token de liquid staking nativo da rede, emitido quando um holder delega HDEX para uma certificação Server. Único na Phinancer, sHDEX é privacy-preserving (emitido para o stealth address do delegator via uma prova zero-knowledge Halo2 — escondendo tanto a identidade do Server quanto do delegator), aplica um hard cap de 10% do total de sHDEX por Server (resolvendo preventivamente o problema de centralização estilo Lido visto em outros ecossistemas de staking) e segue um modelo accruing (1 sHDEX começa igual a 1 HDEX e cresce ao longo do tempo conforme rewards de staking acumulam, evitando o depeg drift observado em LSTs estilo rebase como stETH). sHDEX pode ser negociado em pools AMM, usado como collateral, ou mantido passivamente para acumular yield. Para sair do staking de fato, o holder queima sHDEX após um cooldown de 21 dias para receber HDEX de volta. O cap de concentração de 10% é governance-tunable pela Foundation e, pós-fase Legacy, pelo DAO.

6. Sistema de Certificações

O ecossistema Phinancer opera com 8 tipos de certificações, obtidas através de staking de HDEX. Investidor não é uma certificação — é o estado base de qualquer carteira criada na rede. Todos os clientes certificados são também investidores.

6.1 Mecânica Geral de Certificações

Ativação: O participante faz stake do valor mínimo correspondente à certificação desejada. Após o stake, há um período de confirmação de 12 horas durante o qual o pedido pode ser cancelado. Passadas as 12 horas, o valor correspondente à certificação entra em lockup de 30 dias.

Acúmulo: É possível acumular múltiplas certificações no mesmo endereço, desde que o stake total cubra o valor de todas as certificações ativas. Não há restrições de combinação — uma Corretora pode também ser Investidora com sua própria carteira de criptoativos.

Desativação: O participante solicita a desativação de uma certificação específica. O valor correspondente permanece em lockup por 30 dias, durante os quais o pedido pode ser cancelado. Após os 30 dias, o valor é desbloqueado e a certificação é definitivamente desativada.

Stake sem certificação: O cliente pode fazer stake de HDEX sem escolher uma certificação, participando apenas dos mecanismos de recompensa. Nesse caso, o unstake pode ser solicitado a qualquer momento sem período de lockup. Stakers sem certificação também têm direito a voto, desde que mantenham os tokens em stake por pelo menos 60 dias consecutivos, seguindo a mesma regra aplicada a todos os votantes.

Imutabilidade: As certificações são inquestionáveis — nem mesmo a Foundation pode bloquear ou retirar uma certificação. O único mecanismo de controle é através do sistema de avaliações e reputação.

Valores de stake dinâmicos: Os valores mínimos de stake para cada certificação podem ser ajustados a qualquer momento para incentivar ou equilibrar o mercado. Um algoritmo de automação será desenvolvido para auxiliar esses ajustes. Se o valor mínimo sobe, participantes já certificados mantêm sua certificação sem necessidade de complemento. Se o valor cai, participantes existentes podem retirar a diferença.

KYC é opcional em todos os tiers de certificação — incluindo os tiers de maior stake. O protocolo Phinancer nunca requer verificação KYC. Cada cert holder (Server, Insurer, Corretora, Gate, Plataforma, Agente, Analista, Desenvolvedor) escolhe individualmente se faz KYC e qual a intensidade (KYC pessoa física, KYB pessoa jurídica, beneficial owner disclosure, AML check). Corretoras servindo clientes regulamentados tipicamente optam por fazer KYB próprio e exigir KYC dos clientes; Corretoras operando em jurisdições ou mercados que permitem anonimato não fazem nada. A Phinancer fornece a infraestrutura de verificação (PaddleOCR self-hosted para OCR de documentos, dlib face_recognition para matching facial, WebRTC para liveness check, com zero retenção dos documentos originais — apenas um hash SHA-256 é registrado on-chain pra provar que o KYC foi feito sem expor o documento). A responsabilidade legal de cumprir as regulamentações locais é do cert holder, não do protocolo nem da Foundation. Isso posiciona Phinancer como a primeira L1 fundamentalmente permissionless quanto a KYC mesmo nos tiers de infraestrutura — mercados avaliam confiança baseado em badges KYC/KYB visíveis combinados com stake bond on-chain e histórico de slashing.

6.2 Tabela de Certificações

| Certificação | Stake Mínimo Inicial | Descrição |

| --- | --- | --- |

| Corretora (Broker) | 1.000.000 HDEX | Cria instrumentos financeiros, pares de trading e commodity tokens. Opera exchange dentro da rede e gerencia uma rede de Agentes. Define tetos de corretagem para seus Agentes dentro do limite máximo da rede. Recebe royalty sobre commodity tokens criados quando negociados em outras Corretoras. Para solicitar a desativação da certificação, a Corretora deve primeiro encerrar o vínculo com todos os Agentes e transferir seus contratos de Commodities para a Foundation. Os royalties dos contratos já existentes permanecem válidos e continuam sendo pagos ao endereço original de criação do contrato. Novos contratos passam a apontar para a Corretora da Foundation; na indisponibilidade desta, será sorteada entre as 50 Corretoras mais ativas. |

| Banker (Agente) | 10.000 HDEX | Atende investidores, orienta operações e faz aquisição de novos clientes. Vinculado exclusivamente a uma Corretora. Pode sugerir operações aos clientes através de notificações no app que funcionam como smart contracts pré-montados — o cliente recebe a sugestão e aceita ou rejeita com um clique, sem que o Agente jamais tenha acesso direto aos recursos dos clientes. As sugestões são transações on-chain cujo gas fee é pago pelo próprio Agente como custo operacional do seu trabalho. Se o Agente ficar sem HDEX suficiente para gas, as funcionalidades que exigem transações on-chain deixam de funcionar até que o saldo seja reposto. Limite inicial de 10.000 clientes simultâneos, com meta de redução para 1.000 para garantir qualidade de atendimento. |

| Server | 1.000.000 HDEX | Provê infraestrutura de processamento e armazenamento para a rede. Valida transações usando provas criptográficas (validação cega) e armazena dados da blockchain. Cada Server mantém os últimos 12 meses de operações mais 1 ano adicional aleatório sorteado pela rede, totalizando no máximo 24 meses. A remuneração é proporcional ao trabalho executado. A rede define especificações mínimas de hardware. |

| Gate (Fiat) | 50.000 HDEX | Operador de entrada/saída fiat para cripto. Pode ser pessoa física (PF) ou pessoa jurídica (PJ), sem diferença de regras entre eles. A permissão de PF visa facilitar operações em países emergentes com sistema bancário precário. Vinculado a uma Corretora nos mesmos moldes do Agente. Mantém reserva própria (separada do stake) dos tokens que ofertar, idealmente cobrindo 100% dos depósitos de seus clientes em todos os momentos. Pode cobrar taxas a seu critério. Responsável por seguir ou não a regulamentação local. |

| Insurer (Seguradora) | 1.000.000 HDEX | Seguradoras que operam na rede criando apólices via smart contracts, a critério próprio. Só podem criar apólices sobre assuntos dos quais tenham controle e capacidade de verificação — ou seja, apólices cujo sinistro possa ser verificado sem depender de dados privados inacessíveis. Devem travar recursos suficientes em smart contracts como garantia de cada contrato que fechar, garantindo pagamento de sinistros de forma programática e auditável. O stake da certificação é separado das reservas operacionais. |

| Desenvolvedor Autorizado | 5.000 HDEX | Categoria B (cert opcional) per docs/decisions/20260501-platform-cert-software-distribution-gate.md. Desenvolvedores com selo de reputação e confiança no ecossistema. Têm acesso ao time da Foundation e a eventos exclusivos. A certificação traz segurança e credibilidade aos seus clientes. Política alvo: depois que os gates de deploy de contrato passarem, submissão de contratos não deve exigir cert; o SR12 atual não claim readiness de bytecode Move público arbitrário. A certificação diferencia pela reputação + reputational signal. |

| Analista | 10.000 HDEX | Analistas de mercado financeiro que produzem conteúdo, relatórios e análises. Podem produzir conteúdo para fora da rede exibindo o certificado, e enviar conteúdos distribuídos pelos Apps do sistema. A responsabilidade pelo conteúdo publicado é integralmente do Analista — a certificação indica apenas participação na rede e habilitação para receber avaliações, não constitui endosso da Foundation ou da rede. Podem cobrar por seus serviços através de smart contracts (planos pagos/gratuitos). A curadoria é feita pelo mercado através de notas dos consumidores de conteúdo, com API disponível para integração em sites pessoais. |

| Plataforma | 25.000 HDEX | Categoria B (cert opcional) per docs/decisions/20260501-platform-cert-software-distribution-gate.md. Front-ends terceiros server-side que querem acesso a uma futura camada de APIs privadas (target: SLA 99.9% + mTLS + 10K req/s + endpoints exclusivos depois dos gates relevantes). "Consumir Phinancer" não deve exigir cert quando os gates de API pública abrirem: o target da API pública é 100 req/s por IP + self-hosted full nodes. Foundation pode discretionary review high-risk applications (advisory, NÃO mandatory protocol-level — preserva CLAUDE.md §7.9 KYC opt-in policy). Têm autonomia para cobrar como quiserem fora da rede, mas dentro da rede seguem as regras do ecossistema. |

6.3 Sistema de Avaliações

As avaliações são anônimas — é divulgada apenas a quantidade de avaliações e a nota final consolidada. As avaliações podem ser alteradas pelo avaliador a qualquer momento.

Para Agentes: Apenas clientes com ao menos 10.000 HDEX em stake e que estejam sendo atendidos pelo Agente há pelo menos 30 dias podem avaliar. A Foundation pode intervir em avaliações exclusivamente em situações de suspeita de fraude ou para aprimorar o modelo de cálculo da reputação.

Para Analistas: A nota é dada pelos consumidores de conteúdo, com critérios menos rigorosos por se tratar de serviço informativo.

Consequência de notas baixas: Notas muito baixas travam a conexão com novos clientes e exigem um curso de reciclagem para destravar e resetar a nota. A Foundation fornece os materiais e provas online de forma automatizada.

Limite de clientes do Agent: O limite de clientes simultâneos por Agent é definido e ajustado pela Foundation. Se o limite for reduzido, Agents que já possuem mais clientes que o novo limite mantêm os clientes excedentes (direito adquirido), porém não podem aceitar novos clientes até que o número esteja dentro do novo limite.

6.4 Vinculação e Mobilidade

Agentes com Corretoras: O Agente se vincula exclusivamente a uma Corretora. Para trocar, solicita a mudança com 30 dias de antecedência (pode cancelar durante o período). Ao se vincular a uma nova Corretora, fica em espera até o aceite da nova parceira.

Investidores com Agentes: Todo investidor é vinculado a um Agente. Se a carteira foi criada sem convite, é automaticamente associada a um Agente da Foundation (bot ou pessoa com fees baixos/zero). O investidor pode trocar de Agente com uma janela de 7 dias (pode cancelar durante o período). Durante os 7 dias, o investidor permanece com o Agente antigo e tudo funciona normalmente. Após a troca ser efetivada, smart contracts de sugestão pendentes continuam válidos mas a corretagem passa para o novo Agente, e o antigo perde a capacidade de enviar novas sugestões. Sair da Foundation para um Agente de Corretora também segue a regra dos 7 dias.

Gates com Corretoras: O Gate se vincula a uma Corretora nos mesmos moldes do Agente. Para transações fiat-cripto, pode operar diretamente através da Corretora da Foundation se não for parceiro de outra.

7. Arquitetura Técnica

7.1 Blockchain Própria e Arquitetura de Execução Paralela

A Phinancer Hiper-DEX opera sobre uma blockchain L1 própria, construída em Rust (linguagem existente adaptada ao projeto, não uma linguagem nova), com infraestrutura inteiramente proprietária.

A arquitetura alvo da mainnet implementa execução paralela com estado compartilhado ("Path III"), combinando três camadas técnicas:

1. Consenso DAG-based (adaptado de protocolos como Narwhal+Bullshark, Tusk ou Mysticeti): separação entre disseminação de transações e ordenação, mirando alto throughput e finality abaixo de 1,5 segundo apenas depois dos gates de evidência de finality hard passarem.

2. Execução paralela via committees rotativos de K Servers (selecionados por VRF a cada epoch): cada committee processa um subconjunto de transações em paralelo com outros committees.

3. Estado global compartilhado: árvore de commitments única (Poseidon Merkle com root recursivo Halo2 periódico) + conjunto global de nullifiers (SMT atestado por committees) que preservam anonymity set monolítico — cada usuário contribui para o anonimato de todos os outros, sem fragmentação por shards ou rollups.

Escala horizontal organicamente alinhada com as 6 fases de progressão: mais Servers entrando na rede criam mais committees paralelos, aumentando a capacidade total modelada de TPS. A fase Aurora (30 Servers) mira ~1.500-2.500 TPS shielded; Rising (100+ Servers) mira o piso alvo ≥5.000 TPS; fases posteriores miram 30.000-60.000+ TPS conforme o ecossistema amadurece. Estes números são metas arquiteturais, não claims públicos atuais de benchmark. O marco de MVP é definido por evidência medida e auditável de TPS sustentado (número fixado por benchmark, nunca publicado antes da medição), com o piso ≥5.000 TPS permanecendo como gate da fase Rising via committees paralelos. O hardware exigido por Server diminui com o crescimento da rede (cada Server processa uma fração menor do total à medida que committees se multiplicam) — propriedade da fase de disseminação roteada; nas fases iniciais, o piso de hardware por Server é de datacenter (~1 Gbps), publicado com transparência no onboarding.

Metas de performance (hard caps não-negociáveis da mainnet, não claims atuais):

- Meta de ≥5.000 TPS sustentados em transações privadas (todas as transações passam pelo stack criptográfico completo: commitment + nullifier + prova Halo2 + endereços stealth + Dandelion++)
- Meta de finality de transação <1,5s (tempo do mempool até bloco finalizado)
- Privacidade por default — toda transação de usuário é shielded, operações transparentes existem apenas quando a mecânica de protocolo requer (preços de pool AMM, stake visível para ponderação BFT)

Textos públicos atuais devem tratar TPS e finality como metas gated até que P9/P12 e release review aprovem claims mais fortes.

O consenso é Proof-of-Stake com validação exclusiva por Processing Servers certificados (cert holders com bond de 1M HDEX + 30-day lockup). A integridade da validação cega é garantida pela natureza matemática das provas zero-knowledge: cada prova gerada por um usuário é verificada pelo committee assignado sem acesso aos dados originais da transação, e periodicamente todos os Servers validam a consistência global via provas recursivas Halo2. Servers maliciosos são penalizados com slashing; parâmetros exatos de redundância e penalização são definidos durante o desenvolvimento (sprints SR3 e SR7).

7.2 Smart Contracts

O deploy de contratos é uma meta permissionless depois que os gates de MoveVM/deploy controlado passarem. O SR12 atual não claim readiness de bytecode Move público arbitrário. A listagem desses contratos nas Corretoras para negociação é uma decisão comercial de cada Corretora, separando a camada de protocolo (alvo aberta) da camada

de negócio (curada). Novos instrumentos financeiros criados por Corretoras são anunciados com detalhes e código aberto para apreciação da comunidade. A Foundation, com ajuda da comunidade, autoriza ou não a criação, podendo estabelecer modelos de aprovação automática para contratos que se enquadrem em padrões pré-definidos.

7.3 Modelo de Liquidez — AMM Global

Na fase Aurora, o sistema opera com Automated Market Maker (AMM) como modelo principal de liquidez. Cada pool AMM é único por par de ativos e global — todas as Corretoras acessam o mesmo pool de liquidez, sem duplicação. Isso garante máxima profundidade de mercado e o melhor preço para o investidor.

Os pools AMM exibem publicamente preços e tamanhos das ordens, porém sem revelar a origem das transações, mantendo a privacidade dos participantes. A criação de novos pools AMM pode ser feita por qualquer Corretora, incluindo a Corretora da Foundation, sem necessidade de anúncio prévio — a criação é uma operação imediata. A Corretora que cria um novo pool é responsável por fornecer a liquidez inicial, que entra em lockup de 30 dias para garantir estabilidade mínima ao pool recém-criado. Qualquer participante pode ser provedor de liquidez (LP). O AMM é um produto da rede com taxa própria: operações realizadas via AMM cobram uma taxa específica destinada exclusivamente à remuneração dos LPs, separada do gas fee e fora do cap de 10% de taxas de serviço. Esta taxa existe porque o AMM tem custos operacionais próprios e é uma opção de mercado, não uma obrigação — os investidores terão alternativas como o order book tradicional (sem esta taxa). Para proteger contra retiradas abruptas de liquidez, saques de LP que excedam 2% do volume total de reserva do pool não poderão ser feitos de uma só vez, sendo obrigatório programar múltiplos saques em horários diversos. Os parâmetros exatos serão simulados e testados. O modelo específico de AMM será desenhado e testado extensivamente para atender às necessidades do ecossistema. Se problemas de impermanent loss não puderem ser adequadamente mitigados, o sistema pode migrar para um order book tradicional.

Na fase Rising, está prevista a adição de um order book tradicional como alternativa, sujeito à viabilidade técnica considerando a segurança e o desempenho dentro do modelo de privacidade da rede.

7.4 Servidores e Armazenamento

Os Servidores são uma classe única que combina processamento de transações e armazenamento de dados da blockchain. Cada Server armazena os últimos 12 meses de operações mais 1 ano adicional aleatório sorteado pela rede, totalizando no máximo 24 meses por Server. Os dados históricos são armazenados de forma criptografada, de modo que o Server não identifica a qual ano correspondem os dados que armazena. Os Servers podem se comunicar entre si para remontar virtualmente o histórico completo e disponibilizá-lo à rede quando necessário.

A rede como um todo, pela quantidade de Servers, garante redundância completa de todos os dados históricos. Em caso de insuficiência de Servers, os disponíveis podem armazenar mais que os 24 meses padrão. Dados muito antigos passam por um processo de "resfriamento", sendo divididos em blocos anuais e distribuídos pela rede, com um número menor de cópias para reduzir custos, mas sempre com redundância. A somatória da rede mantém todas as informações, porém não de forma centralizada.

A remuneração dos Servers é proporcional ao trabalho executado (quantidade de processamento), incentivando o desenvolvimento de mais servidores e garantindo justiça na distribuição. Servers que ficam offline perdem a receita correspondente ao período de inatividade.

7.5 Transações Off-Chain

Se as metas de performance na rede principal forem atingidas, transações off-chain podem não ser necessárias. Caso sejam implementadas, deverão obrigatoriamente seguir as mesmas garantias de privacidade e segurança da camada on-chain, utilizando o mecanismo mais eficiente disponível. O conceito e implementação serão definidos durante o desenvolvimento, priorizando performance, segurança e preservação do modelo de privacidade.

7.6 Bridges com Outras Redes

A comunicação com outras blockchains será implementada a partir da fase Rising, através de bridges e protocolos de interoperabilidade disponibilizados em código aberto ao mercado. O objetivo é não dificultar a conexão com outras redes, mas a privacidade fora da rede Phinancer não é responsabilidade do ecossistema — dentro da rede a

privacidade é mantida, mas ao cruzar para outra rede, as regras de privacidade da rede de destino se aplicam.

7.7 Auto-Conversão de Gas Fee

Todas as taxas de gas são pagas exclusivamente em HDEX. Quando um usuário deseja realizar uma transação mas não possui HDEX suficiente para o gas fee, o sistema realiza automaticamente a conversão de parte do ativo sendo negociado para HDEX ao preço de mercado atual no AMM. A operação é atômica: o gas fee da própria conversão é descontado automaticamente do output da conversão, eliminando o problema de o usuário não ter nenhum HDEX para iniciar o processo. O modelo de privacidade oculta a correlação entre a transação de conversão e a transação principal, impedindo que observadores vinculem as duas operações. Toda a operação — conversão de gas e transação principal — é tratada preferencialmente como uma transação atômica única, evitando que a conversão de gas impacte o preço do pool antes da execução da operação principal. Os gas fees são proporcionais aos valores movimentados, com um componente aleatório dentro de faixas definidas (ex: ±30-50%) para preservar a privacidade — impedindo que observadores estimem o valor de uma transação pelo gas pago. Internamente, o cálculo das EMAs utiliza o valor base (sem ruído) para refletir corretamente a demanda real da rede; o ruído é aplicado apenas no valor efetivamente cobrado ao usuário. O custo médio permanece proporcional (a rede não perde receita), mas o valor individual de cada transação fica protegido. Como proteção contra manipulação de preço no pool, a auto-conversão utiliza um mecanismo de desvio padrão: se o preço atual do par no AMM estiver fora de um desvio padrão aceitável em relação à média recente, a conversão não é executada e o usuário recebe um aviso de baixa liquidez no mercado, devendo tentar novamente quando o preço se estabilizar. Em pools recém-criados sem histórico suficiente para calcular média e desvio padrão, esta proteção fica desabilitada até que dados suficientes sejam acumulados.

8. Modelo de Privacidade e Anonimato

A privacidade é um princípio fundamental e inviolável da Hiper-DEX. O modelo de privacidade é modular por ativo, permitindo diferentes níveis de controle conforme a natureza de cada token.

8.1 HDEX — Privacidade Máxima

Para o token HDEX, a privacidade é absoluta e inegociável:

Anonimato por padrão: Todas as transações são totalmente anônimas. Nenhuma entidade — nem a Foundation, nem reguladores, nem servidores — consegue ver remetente, destinatário ou valor. O staking também é privado: embora os valores mínimos para cada certificação sejam públicos, o saldo total de uma carteira e a composição do seu stake permanecem anônimos. Uma carteira pode ter muito mais em stake do que o mínimo necessário para suas certificações, sem que isso seja visível para terceiros.

Validação cega: Os Processing Servers validam transações usando provas criptográficas sem jamais ter acesso aos detalhes da transação. Isso elimina o risco de vazamento por parte dos validadores.

Sem master key: Não existe nenhuma chave mestra que permita a qualquer entidade acessar dados de transações. Nem a Foundation possui acesso especial.

Revelação voluntária: O remetente de uma transação pode opcionalmente ativar a revelação binária, tornando visíveis o endereço de origem, o valor e o endereço de destino. A revelação é sempre binária (tudo ou nada) e limitada à transação específica. Esta opção existe para permitir compliance em jurisdições onde o anonimato total é proibido por lei. Para verificações mais amplas (como auditorias de seguradoras), pode ser necessária a abertura do histórico completo de transações, ficando a critério de cada parte definir os requisitos de transparência exigidos nos seus contratos.

8.2 Outros Ativos — Privacidade Configurável

Ativos como a PHDSC (stablecoin) e PH Commodities podem ter módulos de controle regulatório configuráveis, sem comprometer a privacidade do ativo principal. Para a PHDSC, por exemplo, a Foundation define os parâmetros de privacidade, podendo implementar controles como bloqueio global de carteiras específicas mediante ordem judicial. Para PH Commodities, o criador do ativo define as regras de privacidade.

8.3 Mecanismo Criptográfico

O mecanismo criptográfico específico será desenvolvido como área central de pesquisa na fase Aurora. O objetivo é criar um modelo proprietário otimizado para as necessidades da Phinancer, inspirado nos melhores elementos de tecnologias existentes como stealth addresses (proteção do destinatário), zk-STARKs (sem cerimônia de confiança, resistência quântica) e batch proving (performance), mas adaptado para atingir throughput competitivo com validação cega. O mecanismo de prevenção de double-spending também será desenvolvido e testado especificamente para o modelo de privacidade adotado.

9. Modelo Econômico e Tokenomics

9.1 Supply e Distribuição

O supply máximo total é de 10 bilhões de tokens HDEX, distribuídos da seguinte forma:

| Alocação | Percentual | Quantidade | Descrição |

| --- | --- | --- | --- |

| Phinancer Foundation | 41% | 4.100.000.000 | Controle, governança, desenvolvimento e operações da Foundation |

| Capitalização (ICO) | 24% | 2.400.000.000 | Vendas ao mercado em seis rodadas progressivas ao longo das fases |

| Bonificações & Incentivos de Servidores | 10% | 1.000.000.000 | Recompensas de validadores, bonificações por desempenho, subsídios iniciais |

| Estímulos de Mercado | 10% | 1.000.000.000 | Pagamento a parceiros, bounties, airdrops, marketing, programadores |

| Bônus Aurora + Reserva | 10% | 1.000.000.000 | Pool de bônus de stake Aurora; excedente retorna à Foundation |

| Reserva de Liquidez | 5% | 500.000.000 | Injeção de liquidez nos AMMs e vendas diretas ao mercado |

Adicionalmente, o ecossistema inclui o HDEX10 — um token de peso de governança com 10× poder de voto, supply total de 1 bilhão de HDEX10, 100% alocado à Foundation e liberado linearmente ao longo de 10 anos (diariamente). O HDEX10 confere à Foundation o poder de governança necessário para proteger o ecossistema durante o período de crescimento, com diluição gradual que permite uma transição suave para a governança comunitária.

9.2 Capitalização por Fase (ICO)

A alocação de 24% para ICO (2,4B tokens) é vendida em seis rodadas progressivas com preços crescentes, desde a fase Aurora até o final da fase Legacy. As vendas são abertas ao público global.

| Fase | % do Supply | Tokens |

| --- | --- | --- |

| Aurora | 10% | 1.000.000.000 |

| Rising | 5% | 500.000.000 |

| Spreading | 2,5% | 250.000.000 |

| Firming | 2,5% | 250.000.000 |

| Takeover | 2,5% | 250.000.000 |

| Legacy | 1,5% | 150.000.000 |

Na fase Aurora, os 10% incluem o seed (negociação mais flexível com investidores estratégicos) e o ICO inicial. O preço e a forma de venda em cada rodada são definidos pela Foundation. A captação ocorre preferencialmente após os tokens estarem disponíveis na rede principal (mainnet). Caso a mainnet não esteja pronta a tempo para o financiamento inicial, será lançado um token na rede Solana como mecanismo provisório de captação, que será convertido 1:1 para HDEX oficial quando a mainnet for lançada.

9.3 Bonificações & Incentivos de Servidores

A alocação de Bonificações & Incentivos de Servidores (10% — 1B tokens) financia recompensas de validadores (Servidores), bonificações por desempenho e subsídios nas fases iniciais. Este pool garante que os Servidores sejam adequadamente remunerados mesmo antes do volume de taxas de transação atingir níveis autossustentáveis.

- Recompensas de bloco: Distribuídas aos Servidores como recompensas complementares durante as fases iniciais, quando a receita de taxas por si só é insuficiente.
- Bonificações de desempenho: Concedidas com base em uptime, taxa de atestação correta e sucesso de proposta — incentivando infraestrutura confiável.
- Cronograma de redução: O subsídio da Foundation a partir deste pool decresce conforme o volume de taxas on-chain cresce, visando economia de taxas autossustentável entre o ano 3 e 5.

A distribuição de taxas de transações on-chain segue um split 60/40: 60% para Servidores (com o proponente do bloco recebendo peso 2× em relação aos atestadores) e 40% para Stakers (delegadores). Nenhum token novo é jamais cunhado — toda a economia de validadores é financiada pelo supply existente e taxas de transação.

9.4 Estímulos de Mercado por Fase

| Fase | % do Supply |

| --- | --- |

| Aurora | 2% |

| Rising | 2% |

| Spreading | 2% |

| Firming | 2% |

| Takeover | 2% |

Os estímulos são utilizados a critério da Foundation para pagamento direto a parceiros, bounties, airdrops, marketing, programadores e quaisquer outras ações de desenvolvimento do ecossistema.

9.5 Bônus Aurora + Reserva

A alocação de Bônus Aurora + Reserva (10% — 1B tokens) é dedicada ao financiamento do programa de bônus de stake da fase Aurora (veja Seção 9.8). Este pool define o teto máximo de pagamento para incentivos de staking nas fases iniciais. Quaisquer tokens excedentes remanescentes após a conclusão do programa de bônus Aurora retornam à Foundation para uso geral no ecossistema.

9.6 Reserva de Liquidez

A Reserva de Liquidez (5% — 500M tokens) fica em uma carteira específica controlada pela Foundation, podendo ser injetada nos pools AMM ou vendida diretamente ao mercado para dar liquidez, a critério da Foundation.

9.7 Lockup da Foundation

Os 41% da Foundation (4,1B tokens HDEX) seguem o seguinte cronograma de lockup:

- 21% (2,1B): Liberados proporcionalmente ao longo de 10 anos, com liberação diária em valores iguais (linearmente).
- 20% (2,0B): Destinados a dar força de negociação e pagar o time de desenvolvimento, liberados em 20 parcelas mensais iguais.

O token de governança HDEX10 (1B, separado do supply de 10B HDEX) também é liberado linearmente ao longo de 10 anos, proporcionalmente a cada dia.

A Foundation tem autonomia para fazer stake com seus tokens e participar dos mecanismos de recompensa da rede.

9.8 Stake Bonus — Fase Aurora

Durante a fase Aurora, investidores que comprarem HDEX e realizarem stake recebem um bonus como incentivo ao crescimento inicial do ecossistema. O bonus é exclusivo para tokens adquiridos por compra (não se aplica a tokens da Foundation ou de alocações internas) e é financiado pela alocação de Bônus Aurora + Reserva (10% do supply total — 1B HDEX):

- O bonus começa em 2% ao mês no primeiro mês.
- Decresce de forma linear até chegar a 0% ao final de 36 meses.
- O pagamento é realizado semanalmente (dia 7 de cada semana).
- O valor é calculado sobre o saldo em stake no início da semana anterior (dia 1), medido em HDEX.
- O bonus é pago apenas sobre tokens vendidos na fase Aurora, limitando o montante total de pagamentos.
- Não há previsão de bônus de stake para fases futuras. O objetivo é atrair participantes no início do ecossistema.

9.9 Fontes de Receita da Foundation

A Foundation se sustenta através de múltiplas fontes de receita:

- Stake rewards: Participação nos mecanismos de recompensa da rede com seus próprios tokens.
- Corretagens: A Foundation opera como Corretora com as menores taxas do ecossistema e mantém Agentes próprios (incluindo o Agent híbrido bot+humano), recebendo as taxas correspondentes. A Corretora da Foundation não faz marketing ativo — está disponível para quem procurar, sem competição agressiva com outras Corretoras. Seu papel é funcionar como um farol para o ecossistema: testar funcionalidades, modelos de negócio e estruturas de mercado, divulgando os aprendizados para que outras Corretoras possam se beneficiar.
- Rendimento sobre garantias da PHDSC: A Foundation aplica financeiramente os recursos que servem como lastro da PHDSC, obtendo rendimento sem cobrar taxa pela custódia.

O foco é criar receita suficiente para que a expansão do projeto seja constante e sustentável.

9.10 Controle de Supply

- Supply máximo fixo de 10 bilhões de tokens, sem emissão de novos tokens e sem mecanismo de burn.
- Incentivo ao staking prolongado através de certificações e mecanismos de recompensa, reduzindo tokens em circulação ativa.
- Demanda induzida por certificações: cada função exige staking proporcional à responsabilidade no sistema, criando pressão constante de demanda.
- Redução gradual dos incentivos de stake conforme maturidade do ecossistema.

10. Estrutura de Taxas e Fees

10.1 Cap de Taxas de Serviço

A rede define um cap máximo sobre a somatória de todas as taxas de serviço cobradas em uma transação (corretagem da Corretora + taxa do Agente + quaisquer outras taxas). O cap inicial é de 10%, definido e ajustável pela Foundation. O sistema simplesmente não permite que a soma das taxas de serviço exceda o teto vigente.

Gas fees ficam fora deste cap, sendo calculados separadamente.

10.2 Cascata de Corretagem

A estrutura de corretagem segue um modelo de cascata hierárquica:

1. A rede (Foundation) define o cap máximo total (inicialmente 10%).

2. A Corretora escolhe sua taxa dentro do cap máximo.

3. A Corretora define o teto máximo que seus Agentes podem cobrar.

4. O Agente escolhe sua taxa dentro do teto definido pela sua Corretora.

Não existem valores mínimos — tanto Corretoras como Agentes têm liberdade para cobrar zero se desejarem ganhar mercado por outros meios.

10.3 Taxas dos Gates

Os Gates podem cobrar taxas pelas operações de on/off ramp fiat, a critério deles e separado das taxas de corretagem. Via de regra no mercado atual não há taxa para este tipo de transação, mas a possibilidade existe para incentivar a prestação do serviço em locais e ocasiões específicas.

10.4 Taxas Diversas

Taxas para serviços que não se enquadram na estrutura de corretagem (como serviços de Analistas, Plataformas terceiras, etc.) são livres, sem teto.

10.5 Modelo de Gas Fee

O gas fee utiliza um modelo de três camadas com Médias Móveis Exponenciais (EMA) e limitador de variação:

- EMA de 60 dias: Controla as bandas do gas fee (valores máximo e mínimo permitidos).
- EMA de 5 dias: Calcula o preço-alvo do gas dentro das bandas com base na demanda recente.
- Limitador de variação horária: O gas fee efetivo não pode variar mais que um percentual máximo por hora em relação ao valor da hora anterior (ex: 5%/hora). Na subida, o gas efetivo é o menor entre o valor da EMA5 e o valor da hora anterior × (1 + limite). Na descida, é o maior entre o valor da EMA5 e o valor da hora anterior × (1 − limite). Sempre limitado pelas bandas da EMA60. Este mecanismo impede manipulação por spam: mesmo com demanda artificial sustentada, o gas sobe lentamente, tornando o ataque economicamente inviável — o custo acumulado do spam supera qualquer benefício potencial.

Essa estrutura permite que o gas fee se adapte organicamente à demanda da rede, evitando picos extremos, quedas bruscas e manipulação. O objetivo é manter os custos iguais ou inferiores aos da Solana, sem que isso comprometa a saúde econômica do sistema — deve prevalecer um tokenomics saudável.

A Foundation pode fazer override dos parâmetros quando necessário. No lançamento da rede, os valores de gas fee serão fixos até que haja dados históricos suficientes para as médias móveis funcionarem adequadamente. Os parâmetros exatos serão definidos através de simulações.

10.6 Distribuição do Gas Fee

O gas fee arrecadado é dividido da seguinte forma (defaults iniciais — todos os valores são parâmetros governance-tunable):

- Base fee 60% para os Servers, distribuídos proporcionalmente ao trabalho executado.
- Base fee 40% para os stakers da rede (incluindo delegators sHDEX), distribuídos proporcionalmente ao valor em stake de cada participante, sem distinção entre stakers com ou sem certificação. A Foundation também recebe proporcionalmente ao stake realizado com seus próprios tokens.
- Priority tip 100% para o Server que incluiu a transação, fornecendo incentivo direto pra priorização.

O modelo evolui pra auto-adjustment estilo EIP-1559 (base fee respondendo à utilização per-bloco) durante a fase Spreading, substituindo o modelo apenas-EMA descrito acima. A Foundation pode ajustar o split 60/40, a alocação do priority tip e todos os parâmetros relacionados via on-chain governance proposals.

Zero queima — compromisso arquitetural. O design econômico Phinancer proíbe queima de fees, stakes slashed, ou qualquer outro valor on-chain. Toda unidade coletada pelo protocolo flui de volta pros participantes da rede que fazem o trabalho (Servers + Stakers). 90% do valor slashed em qualquer offense vai direto pro pool de 40% Stakers, recompensando o stake honesto pelo seu comportamento honesto. Seguros opcionais são oferecidos por cert holders Insurer individuais (modelo seguro tradicional — cada Insurer com capital próprio paga indenizações das próprias policies; delegator opt-in paga +1% commission como prêmio ao Insurer escolhido). Não há "Insurance Fund" centralizado da Foundation; é mercado de seguros descentralizado. Burn transferiria valor de "workers" pra "passive holders", contrariando a tese Phinancer de que contribuição de infraestrutura deve ser recompensada. Mudar o compromisso no-burn requer hard fork, não governance proposal.

O sistema como um todo é projetado para ser auto-sustentável sem emissão de novas moedas e sem destruição de valor. A receita da rede provém exclusivamente das taxas (gas fees e taxas de serviço). Se a capacidade de processamento da rede diminuir (menos Servers), o base fee auto-adjustável aumenta naturalmente, tornando mais atrativo para novos Servers entrarem no ecossistema e criando um mecanismo de equilíbrio orgânico.

11. Governança e Descentralização

11.1 Descentralização Progressiva

A governança da Phinancer segue um modelo de descentralização progressiva:

- Fases iniciais (Aurora a Spreading): A Foundation tem poder de decisão unilateral sobre a maioria dos parâmetros do ecossistema.
- Fases intermediárias (Firming a Takeover): Abertura gradual para votações comunitárias conforme a comunidade cresce.
- Fase final (Legacy): Fortalecimento do sistema de votação e planejamento da descentralização plena rumo a uma DAO.

As fases são um meio de organizar o andamento do projeto. A transição entre fases é decidida pela Foundation a seu critério, com base no progresso geral do ecossistema.

11.2 Sistema de Votação em Três Turnos

Para garantir que propostas sejam adequadamente avaliadas sem exigir participação irrealista, o sistema de votação opera em três turnos progressivos. Os "votos válidos" em cada turno referem-se aos votos efetivamente registrados, não ao total de votos possíveis na rede.

Quem pode propor: Para submeter uma proposta, é necessário ter alguma certificação ativa na rede.

As votações ocorrem 3 vezes por ano, em sessões fixas com cronograma definido:

Primeiro turno (7 dias): Qualquer proposta submetida por um participante certificado entra no primeiro turno. Para avançar, a proposta precisa obter o apoio de 5% dos votos válidos registrados. Este turno funciona como filtro inicial para eliminar propostas sem suporte mínimo. Após o primeiro turno, há uma janela de 7 dias antes do segundo turno.

Segundo turno (7 dias): Apenas propostas aprovadas no primeiro turno. Para avançar, a proposta precisa obter 20% dos votos válidos registrados. Este turno valida que a proposta tem suporte substancial da comunidade. Após o segundo turno, há uma janela de 7 dias antes do terceiro turno.

Terceiro turno (14 dias): Apenas propostas aprovadas no segundo turno. Para aprovação final, a proposta precisa obter 50% + 1 dos votos válidos registrados. A votação sempre prevalece.

Cada sessão de votação completa dura 42 dias (7+7+7+7+14). As propostas são organizadas em subcategorias para facilitar a gestão pela Foundation.

Poder de voto: Cada HDEX confere 1 voto. Cada HDEX10 confere 10 votos. Apenas tokens em stake há mais de 60 dias têm direito a voto, prevenindo ataques via empréstimos instantâneos ou acúmulo oportunista de tokens para influenciar votações. Enquanto a Foundation mantiver posse dos tokens HDEX10, terá naturalmente o voto principal, garantindo controle efetivo durante as fases iniciais do ecossistema. A longo prazo, o poder pode ser diluído na

comunidade se e quando a Foundation decidir vender parte dos HDEX10.

Votação emergencial: Em caso de vulnerabilidades críticas ou situações que exijam decisão urgente fora do calendário regular, a Foundation pode convocar uma votação emergencial com regras específicas criadas para a emergência em questão. Independente das regras definidas, toda votação emergencial exige um quórum mínimo de 50% + 1 dos votos válidos registrados para aprovação.

11.3 Imutabilidade das Certificações

As certificações são um direito inquestionável do detentor. Nem mesmo a Foundation pode bloquear ou retirar uma certificação. O único mecanismo de controle é o sistema de avaliações, que pode resultar em bloqueio de novos clientes e exigência de reciclagem, mas nunca na perda da certificação em si.

12. Aplicativos e Experiência do Usuário

12.1 Dois Aplicativos

O ecossistema conta com dois aplicativos distintos:

App Investidor: Interface leve e intuitiva, similar a uma carteira cripto moderna. A página inicial exibe gráficos e informações de mercado, com menu para criar ou abrir carteiras. Destinado a todos os investidores (com ou sem certificação). Disponível em mobile, desktop e web.

App Certificado: Interface profissional com módulos que aparecem conforme as certificações ativas do usuário. Cada certificação desbloqueia funcionalidades específicas (ferramentas de corretagem, painel de gestão de Agentes, dashboard de Server, etc.). Destinado a participantes com certificações ativas. Disponível em mobile, desktop e web.

12.2 MVP (Produto Mínimo Viável)

Para o lançamento na fase Aurora:

- App Investidor: Versão mobile como prioridade, com versão web complementar.
- App Certificado: Versão desktop como prioridade (maior segurança para operações profissionais), com versão web complementar.

12.3 Fluxo de Entrada do Investidor

O aplicativo funciona como uma carteira cripto na página inicial, com gráfico e informações de mercado. No menu, o investidor pode abrir ou criar uma nova carteira de duas formas:

- Com convite: A carteira é criada a partir de um convite de um Agente ou Corretora, ficando automaticamente vinculada a eles.
- Sem convite: A carteira é criada sem vínculo prévio e é automaticamente associada a uma Corretora e a Agentes da Foundation, que funcionam como rede de atendimento básico (bot + humano com fees baixos ou zero).

Um usuário pode criar quantas carteiras desejar, sem limite e sem necessidade de vincular identidade. Por padrão, carteiras são anônimas. A vinculação de identidade a uma carteira é opcional e está disponível para usuários em jurisdições onde o anonimato total é proibido por lei. O limite de clientes por Agent é contabilizado por carteiras conectadas, não por pessoas físicas.

12.4 Carteira Non-Custodial

A carteira é non-custodial — o usuário guarda suas próprias chaves, que durante o uso ficam salvas localmente no dispositivo. A rede não tem acesso às chaves em nenhum momento.

Formato padrão de backup: BIP-39 mnemonic de 24 palavras, universal em todos os surfaces Phinancer. Todas as carteiras — App Investidor (modos regular e profissional), App Certificado, Foundation Console, FROST cold keys — usam 24 palavras (256-bit de entropia, quantum-resistant sob algoritmo de Grover até 128-bit de segurança efetiva). A

opção de 12 palavras comum em wallets casuais é rejeitada mesmo no App Investidor: Phinancer é projetado pra um lifetime de múltiplas décadas mirando mainnet 2027 e além, onde segurança post-quantum tem que ser baked-in desde o dia um. O Foundation Console adicionalmente requer uma BIP-39 passphrase (a 25ª palavra opcional) pra plausible-deniability e entropia extra ao controlar operações tokenomics-level.

A stack completa de derivação de chaves usa BIP-39 (mnemonic) + BIP-32 (hierarchical deterministic) + BIP-44 (esquema de path) + BIP-85 (sub-mnemonics — um único paper backup pode derivar múltiplas wallets para usuários holding múltiplas certificações). Encryption-at-rest aplica derivação de chave Argon2id (≥ 64 MB memory cost, ≥ 3 iterations) seguido por encryption autenticado XChaCha20-Poly1305. O backup do device, onde suportado, alavanca secure storage nativo (Apple Secure Enclave, Android Keystore, Windows Hello TPM).

Suporte a hardware wallet é tiered ao risco: App Investidor mira integração de hardware wallet no MVP (Ledger via WebUSB no desktop e BLE no mobile, Trezor via USB no desktop). O App Certificado obrigatoriamente requer hardware wallet pro tier de certificação Server (o bond de 1M HDEX justifica custódia de chave por hardware — YubiKey no mínimo, Ledger preferido). Outros tiers de certificação e o Foundation Console suportam hardware wallets como uma opção fortemente recomendada mas nunca forçam a escolha — o committee FROST multisig acomoda preferência de tooling per-member.

12.5 Herança Digital e Recuperação

Funcionalidade prevista para o final da fase Rising. O mecanismo funciona como um smart contract configurável na carteira principal:

- A carteira possui uma chave principal e chaves secundárias (herdeiras).
- O usuário programa um período de inatividade da chave principal, com um mínimo obrigatório de 90 dias.
- Atingido o período de inatividade, o smart contract envia automaticamente os ativos para as carteiras herdeiras conforme as porcentagens definidas.
- O usuário define a porcentagem dos ativos destinada a cada chave herdeira.
- Este mecanismo também funciona como sistema de recuperação de acesso em caso de perda da chave principal.
- A detecção de inatividade é feita através de um mecanismo obrigatório de heartbeat: a carteira principal envia periodicamente (semanal ou mensalmente) uma mensagem ao smart contract de herança, com um pequeno custo de gas fee. O envio do heartbeat é de responsabilidade exclusiva do titular — sem ele, não há como a rede saber se o cliente está ativo. A ausência dessas mensagens por tempo superior ao período configurado aciona a transferência automática. Este modelo preserva a privacidade, pois o heartbeat é uma transação anônima como qualquer outra.
- Para ativar a funcionalidade de herança, o smart contract exige uma reserva pré-bloqueada de HDEX destinada a cobrir o gas fee da execução automática da transferência. Sem esta reserva, a herança não pode ser ativada.

Perda de mnemonic é recuperável apenas via configuração de Inheritance. Como Phinancer não implementa social recovery centralizada (que violaria os princípios de privacy e self-custody documentados em §8 e §12), e como o BIP-39 mnemonic de 24 palavras é o único seed autoritativo pra cada wallet (ver §12.4), perder o paper backup sem ter uma configuração ativa de Inheritance resulta em perda permanente de fundos. O onboarding flow do App Investidor consequentemente encoraja todo usuário a configurar pelo menos uma carteira herdeira no momento de criação, com defaults sensatos (heartbeat de 365 dias, herdeira primária única). Usuários que explicitamente declinam devem reconhecer "Aceito que perder minhas chaves significa perder meus fundos" antes de continuar.

- A herança transfere não apenas os ativos, mas também as certificações ativas, o stake correspondente e os clientes vinculados a essas certificações. As carteiras herdeiras recebem uma verdadeira sucessão operacional, permitindo continuidade dos serviços. A herança não altera vínculos existentes da carteira herdeira (ex: se o herdeiro já é Agent de uma Corretora, continua vinculado a ela e recebe a certificação herdada separadamente, podendo reorganizar manualmente). Caso haja conflitos de lockup (tokens em período de espera por desativação de certificação), a herança prevalece e os ativos são transferidos integralmente.

- É de responsabilidade exclusiva do usuário a correta configuração das carteiras herdeiras. A rede não valida a identidade dos destinatários.

13. Modelo de Segurança

- Sistema de reputação e avaliações: Toda interação afeta a reputação dos participantes. Notas muito baixas bloqueiam a conexão com novos clientes e exigem curso de reciclagem na Corretora vinculada.
- Auditoria comunitária: Contratos, operações e emissões passam por apreciação aberta à comunidade. Novos instrumentos financeiros são anunciados com detalhes e código aberto antes da aprovação.
- Carteiras com segurança adaptativa: Possibilidade de multiassinaturas (uma mesma carteira com múltiplas chaves), sujeita à compatibilidade com o modelo de privacidade — caso não se encontre um mecanismo que preserve o anonimato, esta funcionalidade pode ser excluída. Alertas de comportamento suspeito e mecanismo de herança digital como proteção contra perda de acesso.
- Validação cega: Processing Servers validam transações sem jamais ter acesso aos dados, eliminando o risco de vazamento de informações por parte dos validadores.
- Privacidade como proteção: O anonimato por padrão das transações HDEX protege contra ataques de front-running e sandwich attacks, já que nenhum participante (incluindo servidores) pode ver ordens antes da execução.
- Segurança de contratos inteligentes: Contratos seguem padrões de mercado, passam por testes públicos e revisão pela comunidade antes de serem disponibilizados para negociação.
- Staking como garantia de comprometimento: O staking obrigatório para certificações garante comprometimento econômico real dos participantes, com lockup de 30 dias que desincentiva comportamentos oportunistas.

14. Roteiro de Desenvolvimento (Roadmap)

Cada fase tem duração estimada de 18 a 36 meses. O horizonte total do projeto é de 9 a 18 anos.

Fase 1 — Aurora — Fundação e Estruturação

- Desenvolvimento da blockchain própria e testnet
- Estruturação do White Paper e modelo de negócios
- Design do ecossistema e arquitetura do token HDEX
- Captação Seed e início do ICO (após mainnet)
- Implementação do MVP com certificações essenciais: Servers, Corretoras, Agents e Gates
- Desenvolvimento do modelo de privacidade e validação cega
- Lançamento dos aplicativos MVP: mobile (investidor) + desktop (certificado) + web

Fase 2 — Rising — ICO e Solidificação

- Continuação do ICO em rodadas com preços crescentes
- Técnicas de aquisição de clientes com foco em alta adoção
- Solidificação da estrutura base e aperfeiçoamento das técnicas de aquisição
- Implementação de todas as 8 certificações do ecossistema

- Adição de order book tradicional (sujeito a viabilidade técnica)
- Desenvolvimento de bridges com outras blockchains (código aberto)
- Implementação do sistema de herança digital e recuperação de carteiras

Fase 3 — Spreading — Expansão Global

- Lançamento da PHDSC (PH Dollar Stable Coin) e modelo de stablecoins
- Foco na aquisição de novos parceiros a nível global
- Criação efetiva do ecossistema blockchain com capilarização sólida
- Expansão dos PH Commodities tokens

Fase 4 — Firming — Fortalecimento

- Implementação de leverage e perpetual futures
- Foco na aquisição de clientes finais
- Consolidação e fortalecimento de toda a base criada (Corretoras e Agentes)

Fase 5 — Takeover — Absorção do Mercado Tradicional

- Desenvolvimento do PHIPC (Inflation Proof Currency)
- Parcerias com corretoras tradicionais e derivativos de ativos tradicionais
- Momento onde corretoras tradicionais serão impelidas a estudar e adotar o ecossistema

Fase 6 — Legacy — Descentralização Plena

- Última rodada de ICO (1,5% do supply)
- Fortalecimento do sistema de votação
- Planejamento e execução da descentralização plena rumo à DAO
- Transferência progressiva do poder de decisão para a comunidade

15. Equipe e Comunidade

- Fundador — Pedro Pustiglione: Com mais de 17 anos de experiência no mercado financeiro, Pedro idealizou a Hiper-DEX como resposta a limitações estruturais das exchanges tradicionais. É responsável pela visão estratégica, controle de risco e arquitetura geral do ecossistema.

- Equipe Técnica: Desenvolvedores especializados em blockchain, smart contracts, criptografia, segurança da informação e interoperabilidade entre redes.

- Equipe de Produto e Growth: Focada na experiência do usuário, aquisição, parcerias institucionais e desenvolvimento de novos mercados.

- Rede de Colaboradores: Analistas, agentes e líderes comunitários certificados, incentivados com tokens, reputação e certificações.

- Comunidade DAO: Poder de decisão progressivo sobre desenvolvimento, alocação de recursos e ajustes no protocolo via votação comunitária.

Iniciativas de engajamento: hackathons com premiações em tokens, programas de mentoria, embaixadas locais, fóruns públicos e incentivos a educadores e Bankers.

16. Compliance e Regulação

- Privacidade estrutural do protocolo: Todas as transações HDEX são anônimas por padrão e protegidas por mecanismos criptográficos nativos. O anonimato é uma característica permanente e inviolável da infraestrutura.
- Privacidade modular por ativo: Ativos regulados como a PHDSC podem ter módulos de controle específicos, incluindo possibilidade de bloqueio de carteiras, sem comprometer a privacidade do ativo principal.
- Revelação voluntária: O remetente pode optar por tornar visíveis os dados de uma transação específica para fins de compliance em jurisdições que exigem transparência.
- Fiat Gates como pontes regulatórias: Operadores de fiat-cripto são responsáveis por seguir a regulamentação local de cada jurisdição. A rede não interfere nas práticas regulatórias locais dos Gates.
- Responsabilidade individual: Cada participante é responsável por seguir ou não a regulamentação local da sua jurisdição. A rede não impõe nem supervisiona o cumprimento de regulamentações locais para o ativo HDEX.
- Preparação para regulações futuras: Para ativos regulados, atualizações legais podem ser incorporadas de forma coordenada pela Foundation ou, futuramente, via votação na DAO.

17. Glossário

| Termo | Definição |

| --- | --- |

| AMM | Automated Market Maker — Mecanismo de liquidez automatizado que permite trocas sem necessidade de um comprador/vendedor direto. |

| Certificação | Representação de funções no ecossistema, obtida por staking de HDEX e mantida por reputação. |

| DAO | Organização Autônoma Descentralizada que governa o protocolo via votações on-chain. |

| DEX | Exchange descentralizada que permite negociação de ativos sem intermediários centralizados. |

| EMA | Exponential Moving Average — Média Móvel Exponencial usada para calibrar parâmetros de gas fee. |

| Gas Fee | Taxa paga para processar transações na rede, sempre em HDEX. |

| HDEX | Token nativo da Φ Phinancer Hiper-DEX. Motor de governança, staking, incentivos e acesso. |

| HDEX10 | Token especial com poder de voto 10x permanente, utilizado como mecanismo de governança de longo prazo. |

| Hiper-DEX | Protocolo que serve como infraestrutura para múltiplas DEXs interconectadas numa camada de liquidez global. |

| Fiat Gate | Serviço de conversão entre moedas fiduciárias e criptoativos, operado de forma descentralizada. |

| LP | Liquidity Provider — Provedor de liquidez que deposita ativos em pools AMM e recebe parte das taxas de negociação. |

| Lockup | Período durante o qual tokens ficam travados e não podem ser movimentados. |

| Non-custodial | Modelo de carteira onde o próprio usuário guarda suas chaves privadas, sem depender de terceiros. |

| PH Commodity | Token lastreado em commodities, emitido por Corretoras com garantia financeira. |

| PHDSC | PH Dollar Stable Coin — Stablecoin com lastro 1:1 em dólares americanos, emitida pela Foundation. |

| PHIPC | Inflation Proof Currency — Moeda resistente à inflação, prevista para fases futuras. |

| Smart Contract | Contrato digital autoexecutável com regras programadas diretamente na blockchain. |

| Staking | Processo de travamento de tokens como garantia de comprometimento, segurança e acesso a certificações. |

| Stealth Address | Endereço único gerado por transação, impedindo rastreamento público. |

| Validação cega | Processo onde Processing Servers validam transações através de provas criptográficas sem acesso aos dados da transação. |

| zk-STARK | Zero-knowledge Scalable Transparent Argument of Knowledge — Prova de conhecimento zero sem necessidade de cerimônia de confiança. |

18. Referências

- Bitcoin White Paper — Satoshi Nakamoto (2008)
- Monero White Paper — Moneropedia / Research Lab
- Solana White Paper — Anatoly Yakovenko (2017)
- Ethereum White Paper — Vitalik Buterin (2013)
- Zcash Protocol Specification — Electric Coin Company
- StarkWare Documentation — StarkWare Industries
- Documentações internas da Phinancer

Integrity note

This PDF is generated from the repository Markdown draft for website publication. Verify SHA-256 hashes on phinancer.com/whitepaper.html before redistribution.