

HYDD Whitepaper

A tradable token with stealth payments and a vault paid by its trading fees.

Draft v1.0 — October 2026 — HYDD contributors

Abstract

HYDD is an ordinary ERC-20 launched on the Pons V2 launchpad on Robinhood Chain. It trades on its Pons bonding curve and, after graduation, on a Uniswap v4 pool, so every wallet, exchange and aggregator can handle it without special support. The HYDD vault is its private side: shielded HYDD becomes vault shares, and payments between users land on one-time *stealth addresses* (ERC-5564) that cannot be linked to the recipient's wallet. A fee harvester, set by Pons as HYDD's creator fee recipient, turns the 2% creator fee on every trade into HYDD and donates it to the vault, so yield accrues to shielded holders only. Spends from stealth addresses are authorised by EIP-712 signatures and submitted by anyone, so stealth addresses never need ETH.

This paper describes the construction, its security and privacy properties, and — explicitly — its limits.

1 Introduction

On a public blockchain every balance and every payment is visible forever. Paying someone reveals your balance and history to them and to everyone else; visible wallets become targets, and counterparties can rebuild a person's finances.

HYDD focuses on the part of that problem that can be solved without new cryptography or trusted parties: **receiving**. With stealth addresses, the person who is paid stays unlinkable. HYDD then adds an economic reason to hold privately: only the vault earns from trading.

1. **Trades anywhere.** HYDD is a plain Pons ERC-20.
2. **Unlinkable receiving.** Every payment goes to a fresh stealth address.
3. **Privacy is where holding pays.** Creator fees are harvested into the vault; public HYDD receives nothing.

2 Design goals

When two goals conflict, the earlier one wins.

1. **Honest claims.** The interface and docs state exactly what is and is not hidden.
2. **Recoverable.** Keys derive from one wallet signature; all funds are recoverable from chain data.
3. **Compatible.** Any router, wallet or scanner treats HYDD as a normal token.
4. **Few dependencies.** No oracle, no committee, no dedicated relayer. Anyone can relay or index.
5. **Invisible to the user.** One signature on first use; no extra seed phrase; no ETH on stealth addresses.

6. **No team allocation.** Public supply only.

3 System overview

```

App --buy/sell--> HyddRouter --shield--> HyddVault <--donate-- HyddFeeHarvester <--claim-- Pons FeeEscrow
|               |               |
| registerKeys  | trade         +- Announcement events --> recipients scan
v               v
HyddStealthRegistry Pons curve -> Uniswap v4 pool

```

Component	Role
HYDD	Pons ERC-20, 2% creator fee
HyddVault	Shares, stealth transfers, signed unshields, price average, network fee
HyddRouter	ETH to vault shares in one transaction
HyddStealthRegistry	Stealth meta-addresses
HyddFeeHarvester	Claims creator fees, buys HYDD, donates to the vault

4 Stealth construction

4.1 Keys. The app asks the wallet to sign a fixed message; the signature is hashed into a spending key k and viewing key v , with public keys $K = kG$, $V = vG$ on secp256k1. The meta-address (K, V) is published in the registry.

4.2 Paying. The sender draws random r , publishes $R = rG$, computes $s = \text{keccak256}(rV)$, and pays the address of $P = K + sG$. The vault emits `Announcement(1, addr(P), caller, R, viewTag || ...)`.

4.3 Receiving. For each announcement the recipient checks the view tag, then computes $s = \text{keccak256}(vR)$ and compares $\text{addr}(K + sG)$. The private key of the stealth address is $k + s \bmod n$.

4.4 Spending. The stealth key signs an EIP-712 struct in the domain `('HYDD', '1', 4663, vault)` containing owner, destination, amount, fee, nonce and deadline. Anyone submits it; the vault verifies the signature, consumes the nonce and pays the submitter the fee in shares.

5 The vault and the holder yield

The vault keeps `totalBacking` B and `totalShares` S . Assets convert to shares at $a \cdot (S + 10^6) / (B + 1)$ and back at $s \cdot (B + 1) / (S + 10^6)$, both rounding down. The virtual offset defeats inflation attacks on an empty vault; rounding down ensures the value per share never decreases.

Donations — from the harvester, from `donate()`, or HYDD sent by plain transfer — increase B without minting shares. Every change emits `VaultUpdated(B, S)`.

6 The market and the fee stream

6.1 Pons market. HYDD launches on a Pons bonding curve against native ETH and graduates to a Uniswap v4 pool. Our contracts handle both phases and can trigger graduation.

6.2 Harvesting. `harvest()` is permissionless. It graduates the market if ready, sweeps and claims creator fees from the Pons FeeEscrow, tips the caller 0.5%, uses 100% of the remainder to buy HYDD, and donates bought HYDD to the vault.

6.3 Price average. The vault keeps an EMA of spot price, each update capped at a 10% step. The harvester bounds slippage to 3% against it and halves the amount on failure up to eight times.

6.4 Router. `buy/buyToStealth` swap and shield in one transaction. `sell` consumes a signed unshield whose `extra` field binds the sale terms; only the router may submit it.

7 Gas and relaying

Stealth addresses hold no ETH. Signed operations carry a fee in shares, so any relayer can submit them profitably. The vault publishes a suggested network fee, updated at most hourly, from `maxOpCostWei` and the price average. Users always sign the exact fee they accept.

8 Denominations

Stealth payments move in fixed sizes — 1,000, 10,000, 100,000 and 1,000,000 HYDD — so payments of equal size are indistinguishable by amount.

9 Security analysis

Party	Can	Cannot
Vault owner	Transfer ownership	Move shares; sign for users; link stealth addresses
Harvester owner	Transfer ownership	Redirect the Pons creator fee; touch vault shares
Relayer	Refuse or delay	Alter a signed operation
Sequencer	Censor or delay	Forge transactions

Accepted risk. The contracts are unaudited and not upgradeable. Only deposit what you accept this risk for.

- Replay: per-owner nonces and deadlines.
- Front-running sales: terms bound in the signature, router-only submission.
- Inflation attack: 10^6 virtual shares.
- Harvest sandwiching: EMA-bounded slippage with capped steps.

10 Privacy analysis

Information	Visible?
Recipient of a stealth payment	No — unlinkable to their wallet
Sender of a payment	Yes
Amount of a payment	Yes (fixed denomination)
Shield / unshield addresses and amounts	Yes
Total vault backing and shares	Yes
Your full balance	No, unless your stealth addresses are linked by behaviour

HYDD does not use zero-knowledge proofs and does not hide senders or amounts. Privacy degrades with behaviour: spending immediately after receiving, consolidating stealth addresses, or withdrawing to the shielding wallet can re-link funds.

11 Robinhood Chain

HYDD runs on Robinhood Chain Mainnet (chain ID 4663, ETH gas). The sequencer orders transactions and can delay or censor, but cannot forge them.

12 Conclusion

HYDD combines a normal tradable token with a narrow, honest privacy guarantee — unlinkable receiving — and an economic incentive to use it: the trading fees flow only to shielded holders.

A Deployment

Contract	Address
HyddVault	0x5C5b829569A8F9a7C468472F3929D935e9Ec1F29
HyddRouter	0x1480B498F2cDCd310c89BD36e694Cdc967Dc81a4
HyddStealthRegistry	0x5bf19240105AC7c41c0dd9A3Ef5E1fd6D5B44Cf1

HyddFeeHarvester	0x32343f40Ae2230F2462e79B20677D81e8E342EFB
HYDD token	Published at launch

B Constants

Constant	Value
Creator fee	2%
Caller tip	0.5%
Default buy share	100%
Max harvest slippage	3%
Max EMA step	10%
Virtual shares	10 ⁶
Network fee interval	1 hour
EIP-712 domain	HYDD / 1 / 4663

References

1. ERC-5564: Stealth Addresses.
2. ERC-6538: Stealth Meta-Address Registry.
3. EIP-712: Typed structured data hashing and signing.
4. Uniswap v4 core.
5. Pons V2 documentation, docs.ponsfamily.com.