UNISTEALTH

Trade in public. Settle in stealth.

Introduction

UniStealth is an experimental privacy primitive built on top of Uniswap V4 hooks and Ethereum stealth address standards. Rather than changing how swaps occur, UniStealth changes where assets settle.

Optional Stealth Flow

A user may buy tokens normally while simultaneously generating a stealth keypair off-chain through the UniStealth interface. The keys are derived locally from a signed message and require no transaction or gas cost. The user may later opt into stealth settlement during a sell by passing their stealth meta-address through hookData.

Technical Architecture

UniStealth combines Uniswap V4 Hooks, ERC-5564 stealth addresses, ERC-6538 meta-address registries, ECDH shared-secret cryptography, and ERC-4337 relayer infrastructure to create unlinkable settlement destinations.

LP Infrastructure and Relayer Funding

The Uniswap V4 LP NFT is held inside a UniStealth-controlled contract capable of collecting LP fees. A portion of those fees may fund ERC-4337 relayers, allowing users to perform sponsored zero-gas stealth claims without funding stealth wallets from linked public addresses.

Security Properties

UniStealth does not hide trades themselves. Swap execution, token amounts, and seller wallets remain public. What becomes hidden is the ownership relationship between the seller and the final settlement address.