Someone told me this is a better place to post it than discord.

This is Uniswap V2 AMM implementation but without LP tokens because I couldn't figure out how to mint them without slippage (inconsistency between public total_supply at the time of the execution on PXE and execution on sequencer). Any ideas how to implement this logic in Noir inside a #[aztec(private)]

:

uint256 shares = _min((_amount0 * totalSupply) / reserve0, (_amount1 * totalSupply) / reserve1);

Repository includes a web demo runnable via "yarn dev".

GitHub

GitHub - olehmisar/shieldswap: A Decentralized Exchange on Aztec Network

A Decentralized Exchange on Aztec Network. Contribute to olehmisar/shieldswap development by creating an account on GitHub.