Abstract: Decentralized Finance (DeFi) has witnessed remarkable growth and innovation, with Decentralized Exchanges (DEXes) playing a pivotal role in shaping this ecosystem. As numerous DEX designs emerge, challenges such as price inefficiency and lack of user privacy continue to prevail. This paper introduces a novel DEX design, termed COMMON, that addresses these two predominant challenges. COMMON operates as an order book, natively integrated with a shielded token pool, thus providing anonymity to its users.

Through the integration of zk-SNARKs, order batching, and Multiparty Computation (MPC) COMMON allows to conceal also the values in orders.

This feature, paired with users never leaving the shielded pool when utilizing COMMON, provides a high level of privacy.

To enhance price efficiency, we introduce a two-stage order matching process: initially, orders are internally matched, followed by an open, permissionless Dutch Auction to present the assets to Market Makers. This design effectively enables aggregating multiple sources of liquidity as well as helps reducing the adverse effects of Maximal Extractable Value (MEV), by redirecting most of the MEV profits back to the users.