

6th Workshop on Trusted Smart Contracts

In Association with Financial Cryptography 2022

May 6, 2022

Title: Lissy: Experimenting with On-chain Order Books,

Authors: Mahsa Moosavi and Jeremy Clark.

Abstract

Financial regulators have long-standing concerns about fully decentralized exchanges that run `on-chain' without any obvious regulatory hooks. The popularity of Uniswap, an automated market makers (AMM), made these concerns a reality. AMMs implement a lightweight dealer-based trading system, but they are unlike anything on Wall Street, require fees intrinsically, and are susceptible to front-running attacks. This leaves the following research questions we address in this paper: (i) are conventional (i.e., orderbooks), secure (i.e., resistant to front-running and price manipulation) and fully decentralized exchanges feasible on a public blockchain like Ethereum, (ii) what is the performance profile, and (iii) how much do Layer 2 techniques (e.g., Arbitrum's optimistic roll-up) increase performance? To answer these questions, we implement, benchmark, and experiment with an Ethereum-based call market exchange called Lissy. We confirm the functionality is too heavy for Ethereum today (you cannot expect to exceed a few hundred trade executions per block) but show it scales dramatically (99.88% gas cost reduction) on Arbitrum.