Decentralized exchanges (DEXes) provide effective price discovery and fair trading while dealing with the drawbacks of centralized exchanges, e.g., lack of transaction transparency and exclusive control of user assets and transaction fees. However, many DEXes suffer from frontrunning and transaction reordering, which fundamentally flaw their design. In this paper, we present a novel incentive mechanism design for mitigating frontrunning and transaction reordering even if frontrunners pay high transaction fees in DEXes. We utilize a weighted counting sort algorithm to order transactions based on the users' multi-dimensional private information (e.g., transaction delay and confidentiality). To elicit users' private information, we consider a multi-dimensional contract-theoretic design based on the users' willingness to share their private information. We show that the miner can always maximize its utility under the complete and incomplete information scenarios. We implement solutions to our multi-dimensional contract and sorting algorithm on a decentralized oracle network to create a decentralized system and design a web application to extensively evaluate the performance of our proposed incentive mechanism. We further show that ordering transactions based on users' private information increases the miner's utility by 78.42%-84.57% and reduces the users' cost by 64.47% compared with the state-of-the-art fair sequencing services, automated arbitrage market maker, and miner extractable value auctions.

Link to work: https://ieeexplore-ieee-org.ezproxy.lib.uh.edu/document/10016729