Problem

Index tokens (i.e. $DPI) needs periodically balance its constituents to meet the weighting target of the index token. For example, an index token might have constituents $A,$B,$C, and the each token is supposed to take 20%,20%,60% of the index token. If the value of any of the the three token changes, the index token need to sell the ones with higher weights and buy the ones with lower weights.

The problem is the weighting target of the constituents is known to the public ahead of the time, and the current weights of the constituents is also known to the public, if the index token is deployed to a public chain. Automated keeper service will periodically execute the rebalancing act, and the timing of the execution is also known ahead of the time. Thus it is possible to front-run the rebalancing trade of an index token.

Solution

Constituent hiding

The front-running opportunity arises from the fact that both target and current constituent percentage are publicly known, thus giving the front-runner the opportunity to calculate the direction and amount of the trades that the rebalancing process will execute. As a solution, the index token contract could be deployed in a TEE, such that the current constituent percentage is not publicly known, while the target constituent percentage is still publicly available to provide sufficient information to index token holders. It’s worth noting that the redemption requests should be batched instead of executed immediately, as the current constituent percentage could be leaked if the redemption is executed immediately.

Rebalancing

The rebalancing process can be split into two categories: active rebalancing and passive rebalancing. Active rebalancing executes on-chain swaps to correct the index token constituent percentages to match the target constituent percentages. Because the current constituent percentage is hidden to the public, external actors cannot expect the direction and amount of token that the active rebalancing is trying to execute.

However, the index token will also need passive rebalancing, which places rebalancing trades into a dark pool throughout the day. Even the index token current constituent percentage is hidden in the TEE, one can still calculate the current constituent percentage based on 1. knowing when the index token is last rebalanced to meet the target percentages 2. knowing the price changes of constituents since the last rebalance. Therefore, the index token need to periodically place rebalancing limit orders to dark pools between two rebalances, to obfuscate the current constituent percentages.