Frontrunning Attacks Exercise 3

Intro

It's Sandwich time!

And this time, we are going back to a code you might be familiar with (maybe because you wrote it ^^).

In the first DEX exercise we implemented different functions in `Chocolate.sol` smart contract:

- `addChocolateLiquidity`
- `removeChocolateLiquidity`
- `swapChocolates`

These functions lack of slippage protection and you are going to exploit it to sandwich users that are using the `swapChocolates` function!

Note: This exercise is executed on an Ethereum mainnet Fork block number `15969633`. Everything is already configured in the `hardhat.config.js` file

Accounts

- 0 - Deployer
- 1 - User1
- 2 - User2
- 3 - Attacker

Tasks

Task 1

Get all the pending transactions from the mempool, find the transactions to the `swapChocolates` function, and perform a sandwich attack to ALL the users in order to generate MAX PROFIT in ETH.

Useful Link

[Hardhat Mining Modes](#)