Frontrunning Simulator

CSE526 - Blockchain
Spring ‘23

Problem Statement

The problem is to develop a sandwich attack bot that can analyze pending Uniswap transactions to identify opportunities for arbitrage. The bot should extract transaction details such as token to token, amount in, expected amount out, function used, and gas details, and calculate slippage based on expected vs. actual output. The bot will then place transactions to assess pool dynamics and calculate the price impact caused by the attacker's transaction, ensuring that it is not more than the slippage to avoid the original transaction failing.

Background

DeFi

DeFi refers to a financial ecosystem that operates on a decentralized network, typically using blockchain technology, and is designed to enable more transparent, secure, and permissionless financial transactions without relying on intermediaries like banks or other financial institutions.

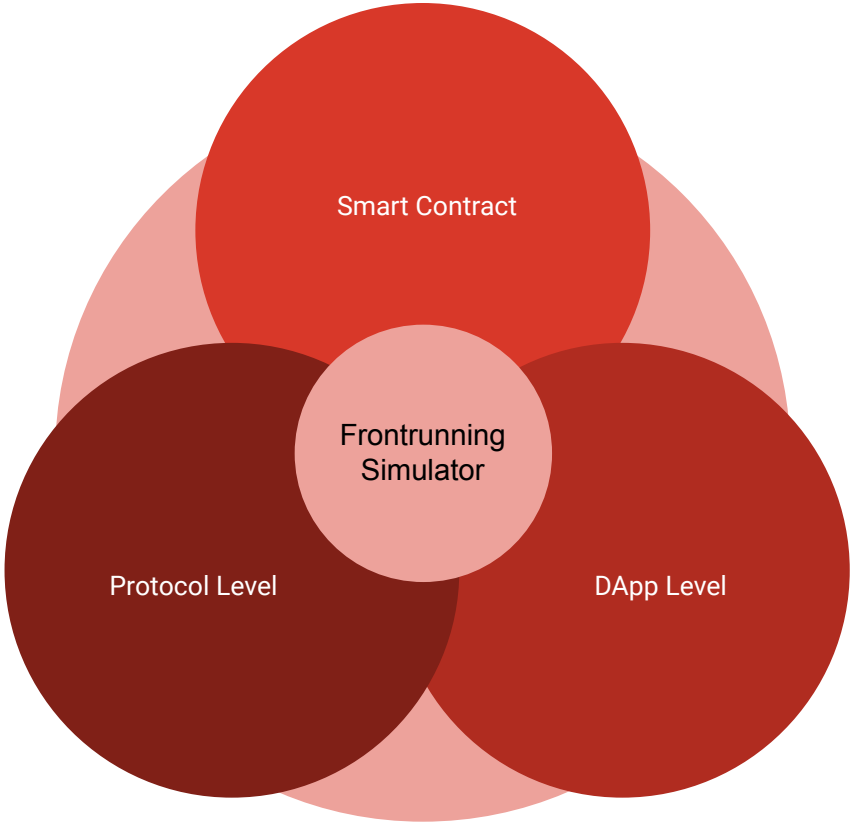
AMM

An AMM is a type of decentralized exchange that utilizes algorithms to automatically set prices for assets by balancing supply and demand based on predetermined formulas, without the need for an order book or centralized pricing authority.

Price Impact

Uniswap's price impact refers to the effect that a trade on the Uniswap AMM platform has on the price of the asset being traded, which is determined by the size of the trade relative to the total liquidity of the asset in the pool, as well as the price sensitivity of the asset itself.

Overview


Smart Contract
Frontrunning Simulator
Protocol Level
DApp Level

Protocol Level

Monitoring ETH Memory Pool

RPC Calls to Uniswap contracts to build Quote.

Smart Contract Level

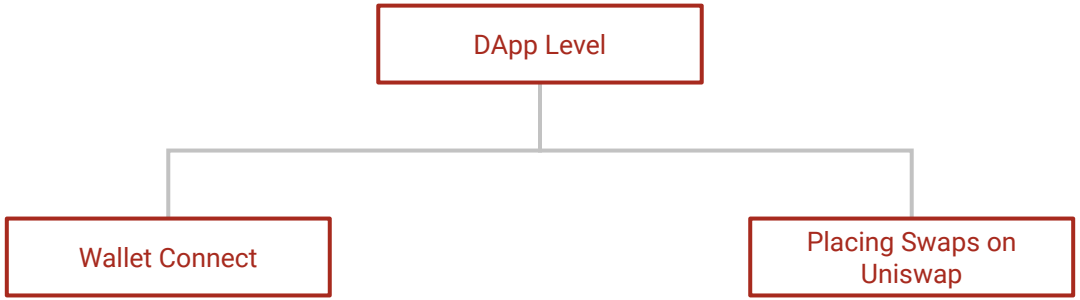
01 **Flash Loans**

- Flash loans are a type of uncollateralized loan in the DeFi ecosystem that allow users to borrow a large amount of funds for a very short period of time, typically less than a few seconds, without the need for any collateral or credit checks.

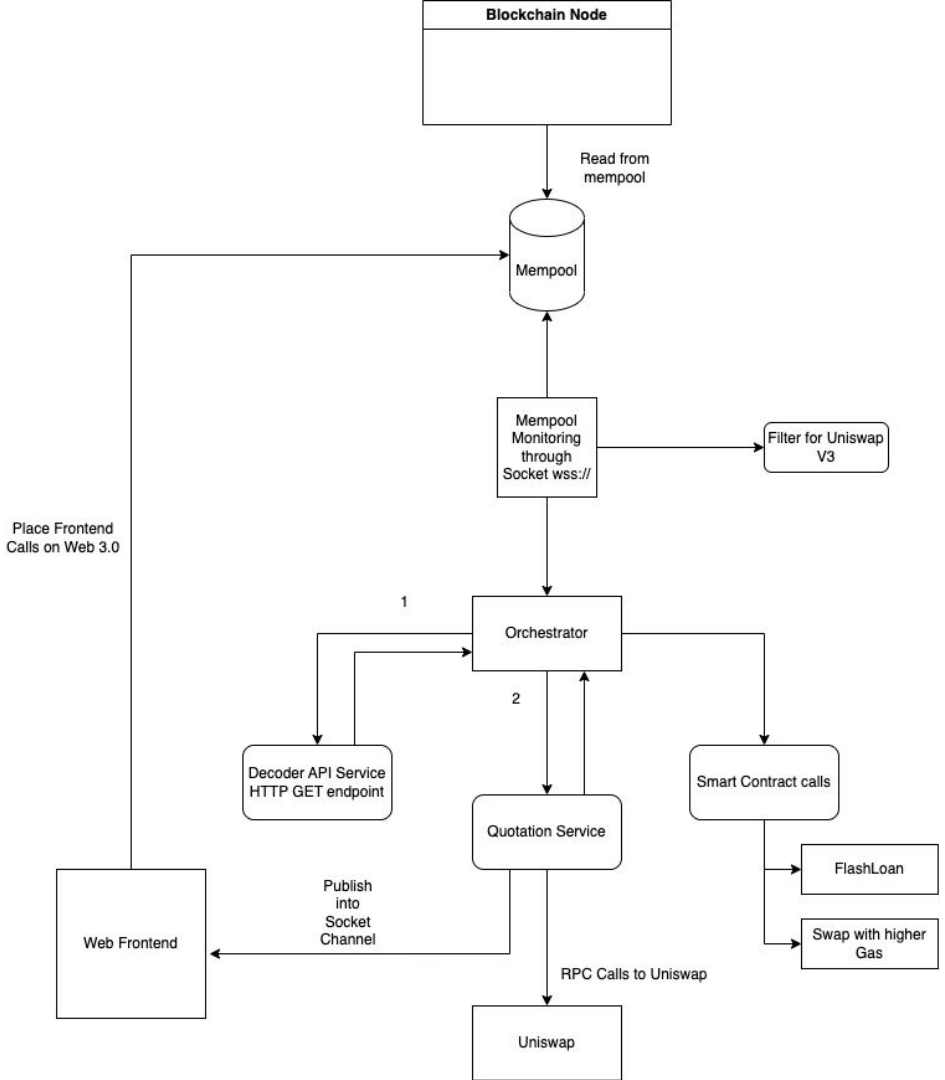
02 **Swapping with Uniswap Router V3 contracts**

- A swap on Uniswap is a decentralized exchange transaction that involves swapping one cryptocurrency for another based on the current price ratio determined by the Uniswap AMM algorithm, with fees paid to liquidity providers for providing liquidity to the asset pools.

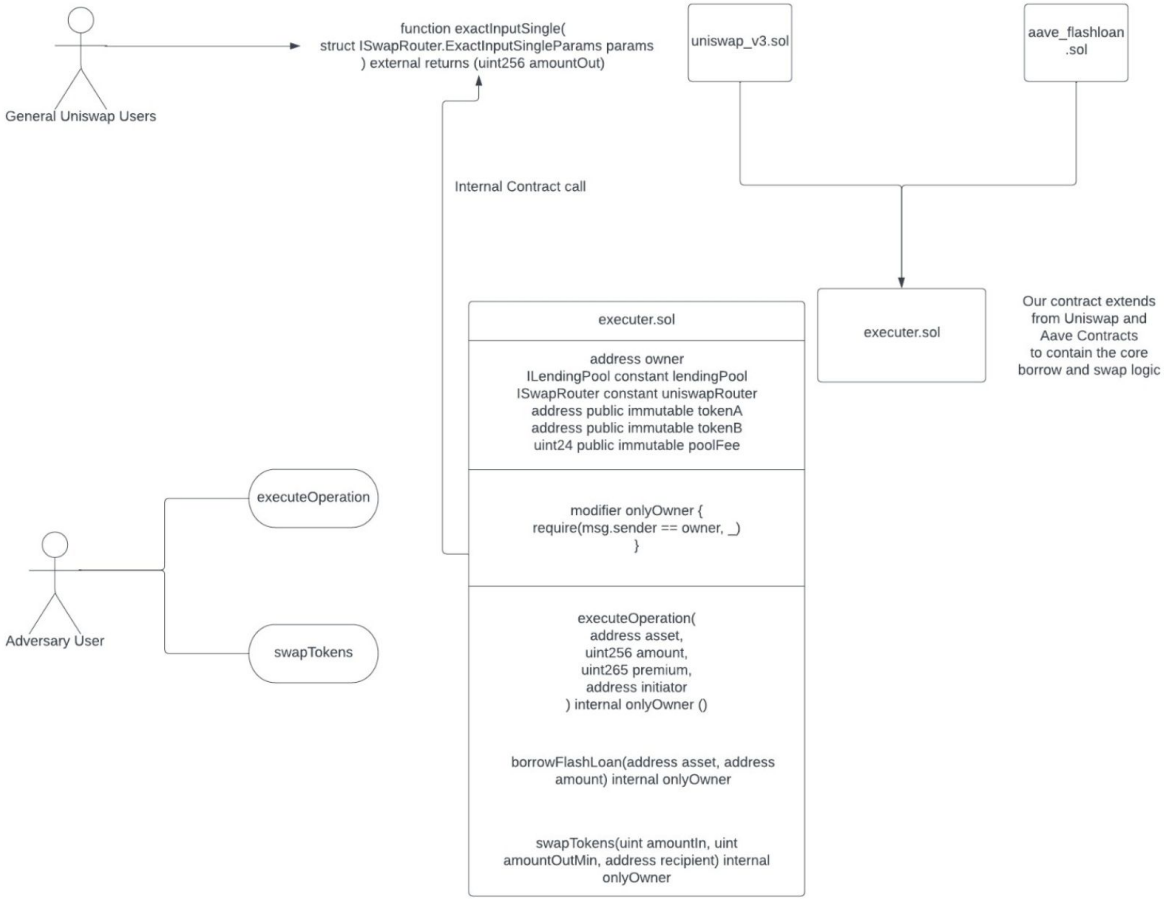
DApp Level

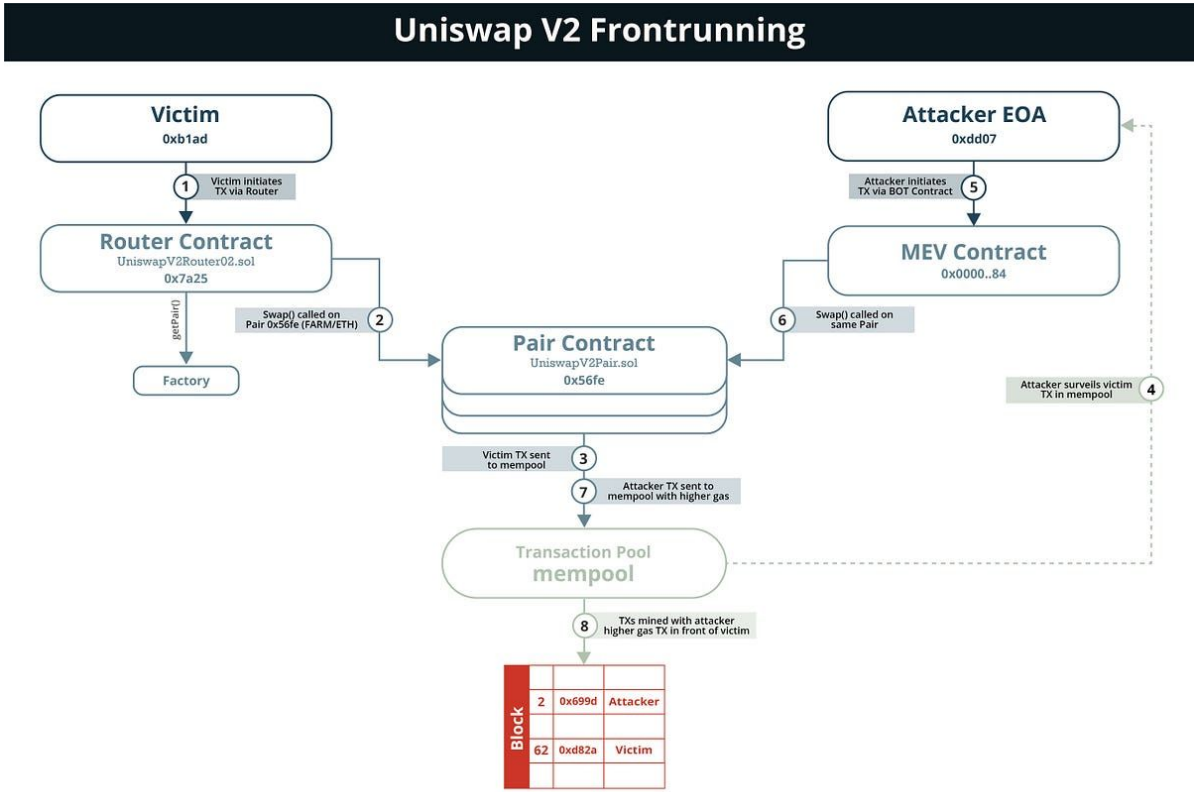


HLD


Blockchain Node
Read from mempool
Mempool
Mempool Monitoring through Socket wss://
Filter for Uniswap V3
Place Frontend Calls on Web 3.0
1
Orchestrator
2
Decoder API Service HTTP GET endpoint
Quotation Service
Smart Contract calls
FlashLoan
Swap with higher Gas
Web Frontend
Publish into Socket Channel
RPC Calls to Uniswap
Uniswap

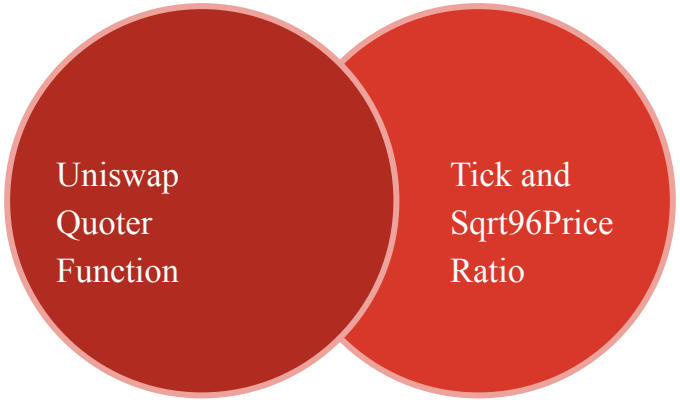
Use Case and Contract Diagram



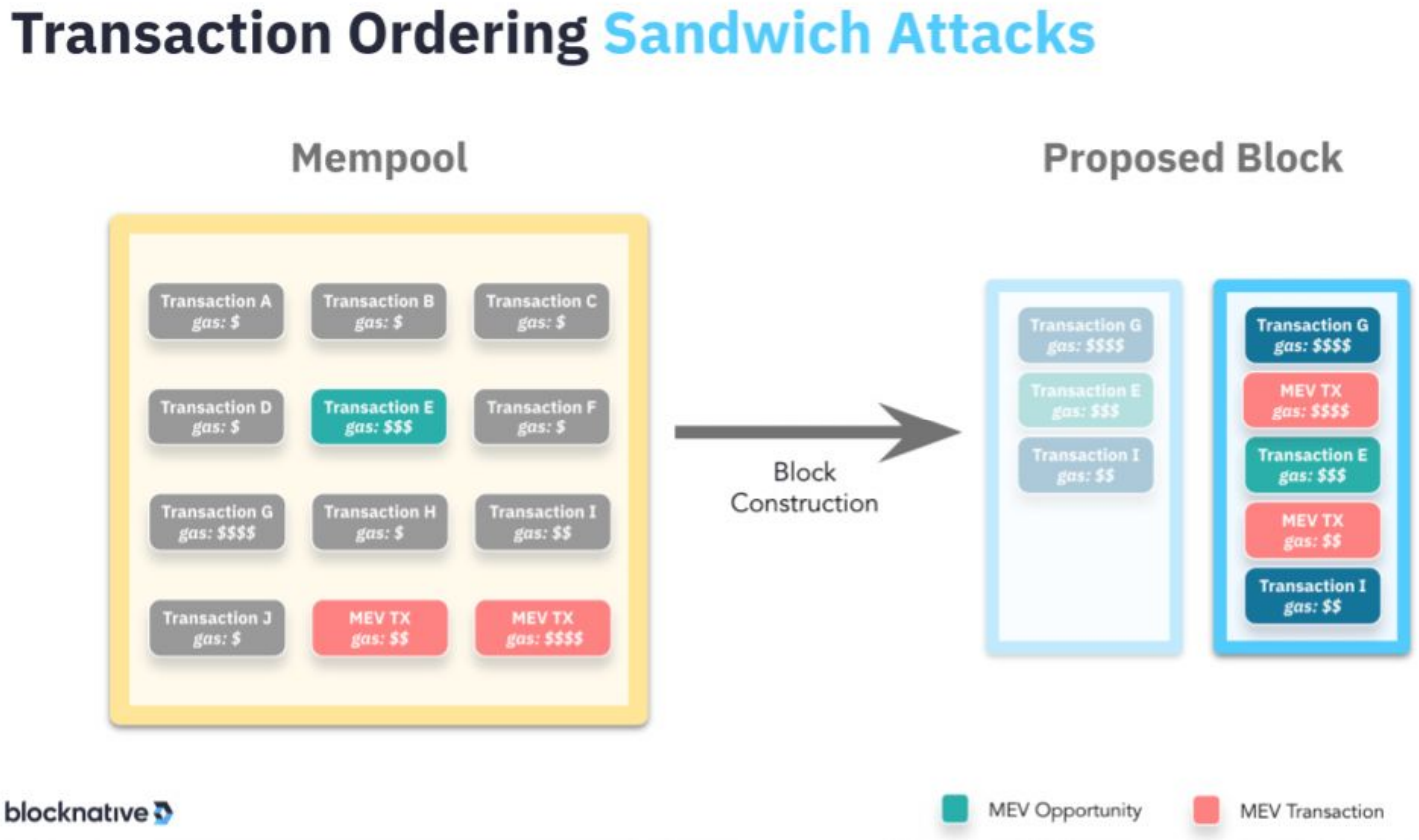


Reference :
https://medium.com/@j2abro/how-to-identify-a-defi-sandwich-attack-ea4208a85b17

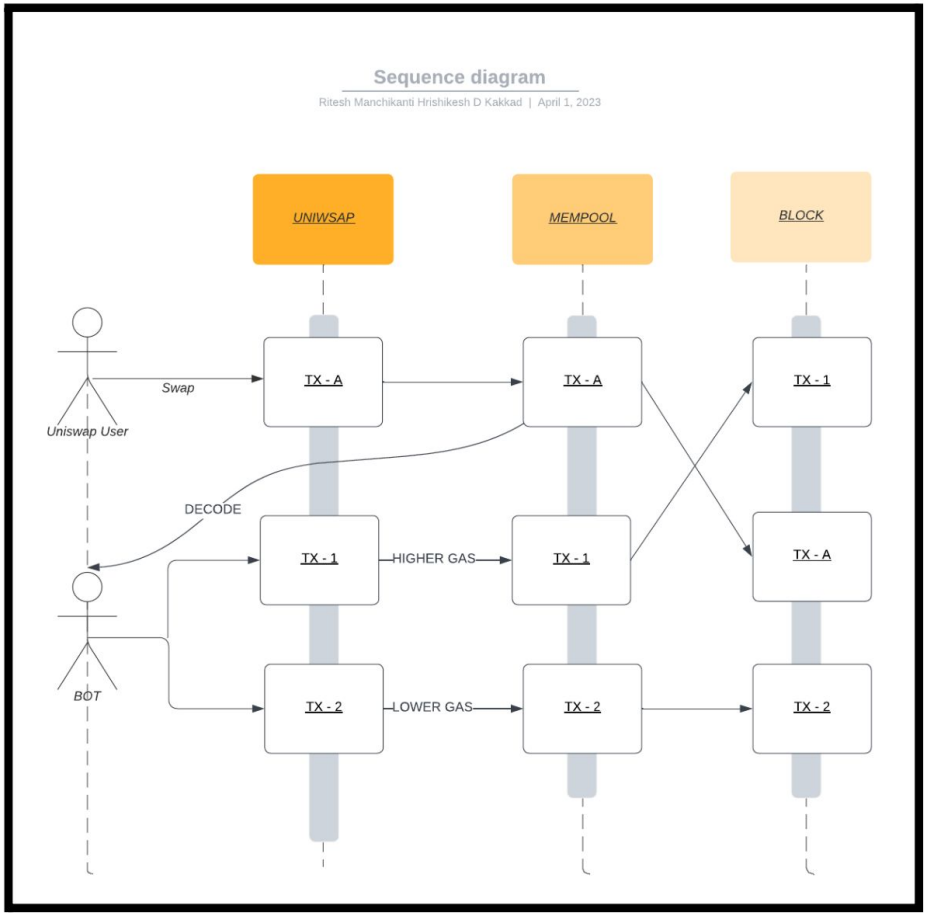
Quotation Service



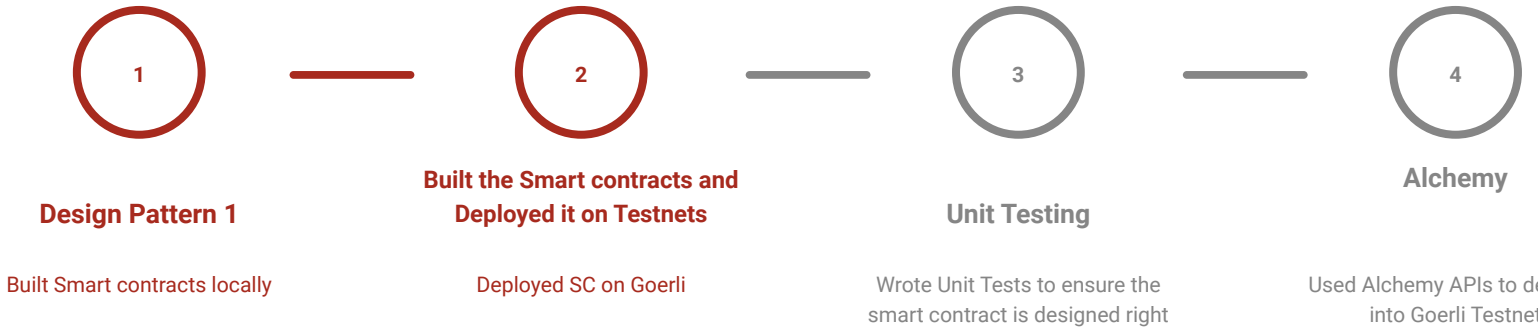
Reference: https://www.blocknative.com/



Sequence Diagram



Project to Syllabus Mapping



- Interacting with web3 through frontend
  - Metamask
- Interacting with web3 programmatically
  - through scripts

Phase 3 and Future Plans

- Fix Swap Hardcodings
- Add borrowing Flash loan programmatically into arbitrage simulator
- Add Swap programmatically on the backend during simulation