Lecture 5: Miner Extractable Value (MEV) and Atomicity

Guillermo Angeris Theo Diamandis

June 2022

Outline

Administrative stuff

CFMM review and oracles

MEV

The good (?) stuff

Outline

PSets and notes

- Previous lecture's derivation notes are up!
- Problem sets 2 and 3 are up
- Problem sets 4 and 5 will (hopefully) go out this week/end
- Feel free to ask questions in the Telegram group

Last two lectures

- Lecture on Tuesday will be remote (by Tarun)
- Lecture on (next) Thursday will be given by Theo

Outline

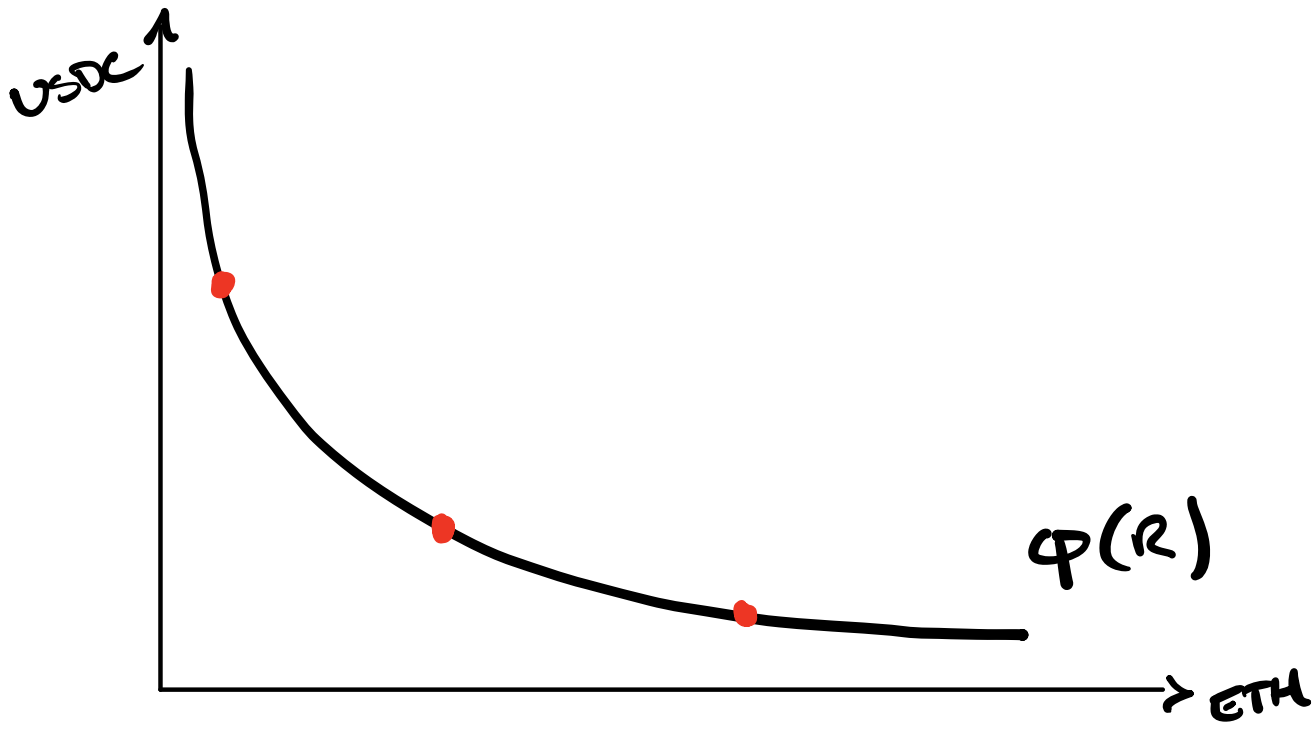
Recap: CFMMs

- Most decentralized exchanges (DEXs) are implemented as constant function market makers (CFMMs)
- A CFMM accepts a trade (Δ, Λ) if

$$\varphi(R + \gamma\Delta - \Lambda) \geq \varphi(R)$$

  where $0 < \gamma \leq 1$ is a *trading fee* and $R \in \mathbf{R}_+^n$ are the *reserves*
- Reserves are updated as: $R \leftarrow R + \Delta - \Lambda$, if accepted
- φ is concave and nondecreasing

Recap: Product trading function $\varphi(R) = \sqrt{R_1 R_2}$



Recap: arbitrage problem

- The arbitrage problem given an external reference market is convex ($\approx$ easy)

Recap: arbitrage problem

- The arbitrage problem given an external reference market is convex ($\approx$ easy)
- Therefore, can expect CFMM prices to track external market prices
- We can use the CFMM as a *price oracle*

Oracles

- Many protocols need a way to query the price of an asset
  - Betting markets
  - Options protocols
- They query a *price oracle* to get the market price
- Often, this is a CFMM
- We rely on the fact that if the price is inaccurate, there is an arbitrage opportunity

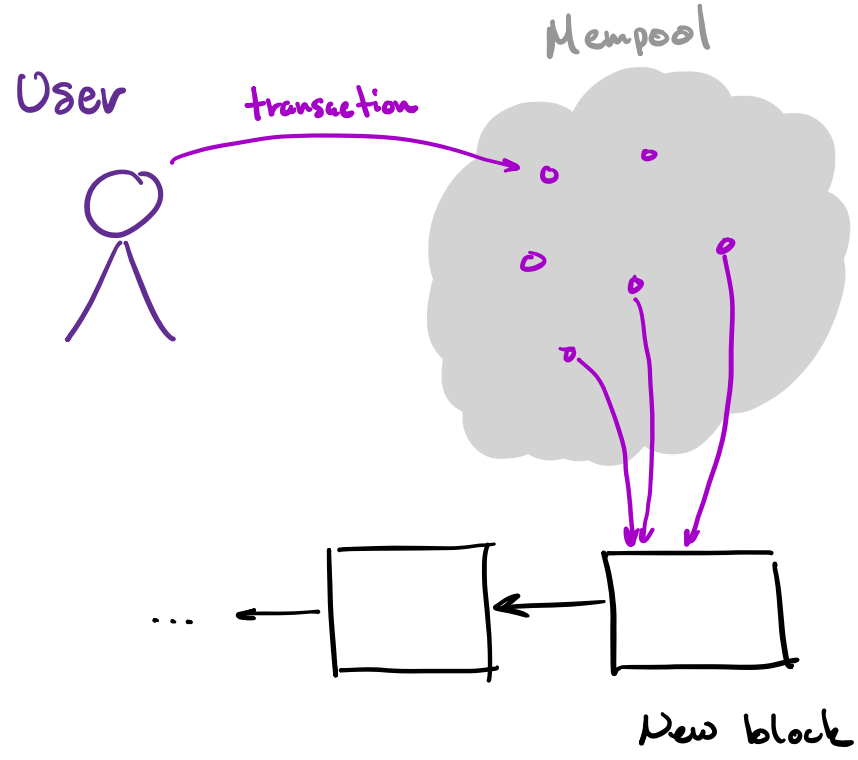
Oracles

- Many protocols need a way to query the price of an asset
  - Betting markets
  - Options protocols
- They query a *price oracle* to get the market price
- Often, this is a CFMM
- We rely on the fact that if the price is inaccurate, there is an arbitrage opportunity
- But the blocked nature of transactions will introduce complexity...

Outline

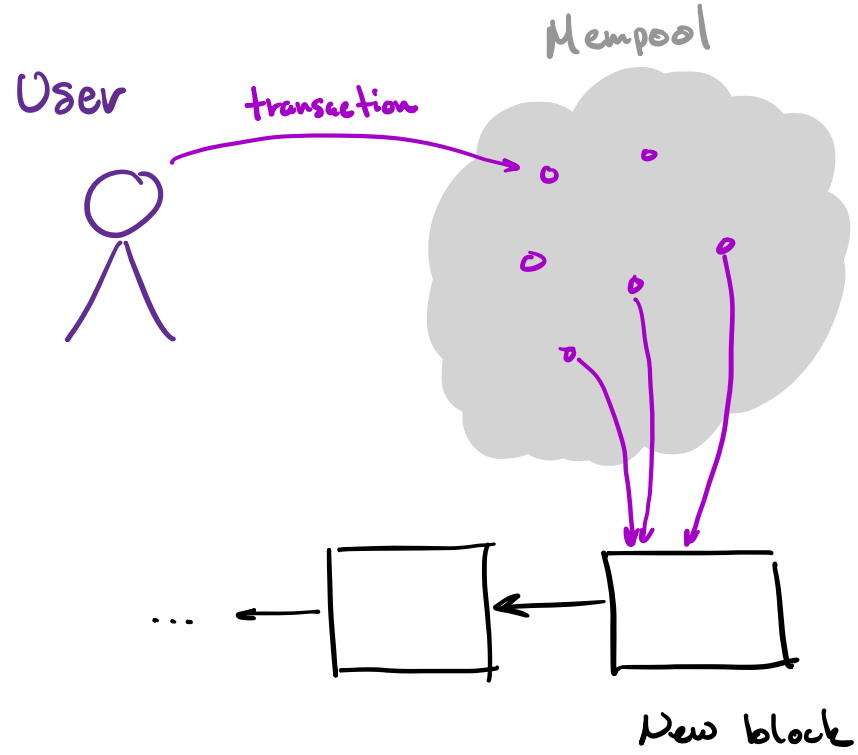
Block ordering

- Recall that transactions are grouped into blocks by miners



Block ordering

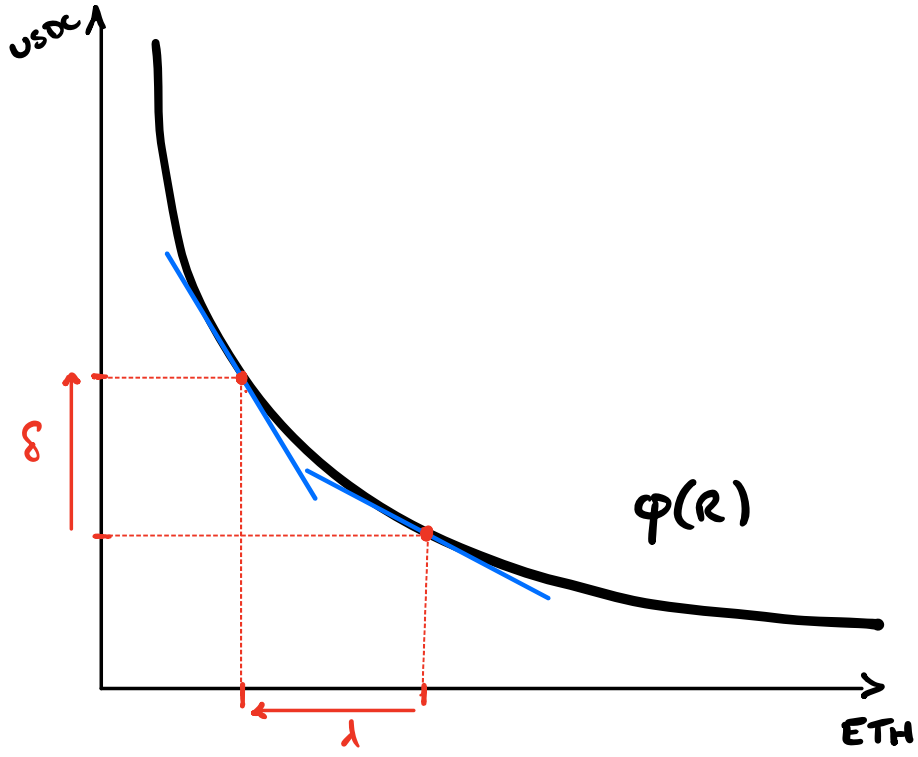
- Recall that transactions are grouped into blocks by miners



- Miners are allowed to reorganize transactions prior to block inclusion (but not after!)

- Reorganization $\rightarrow$ opportunities to extract value (MEV!)

Transactions with CFMMs change the price



- Buying ETH with USDC will increase the price of ETH

Miner information

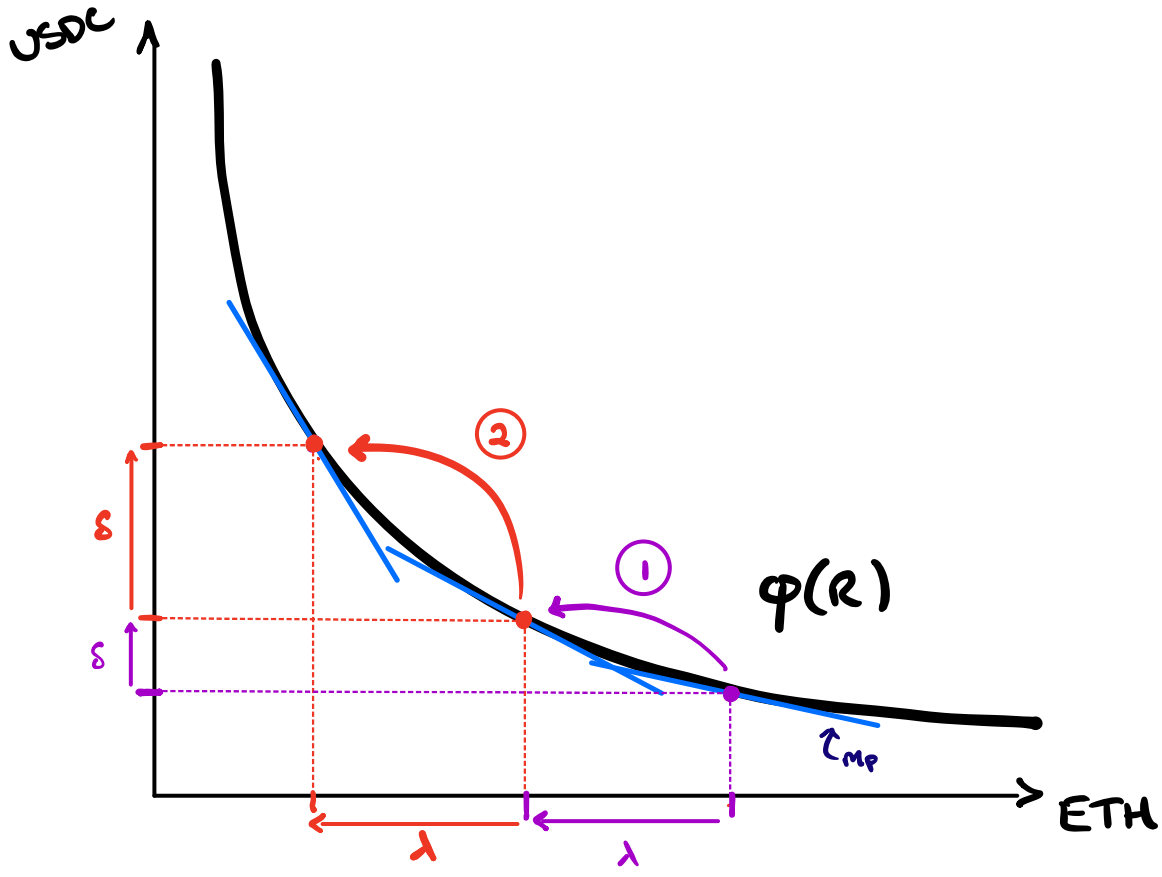
- **Problem:** Miner can see your trade and then put in a trade before/after yours

Miner information

- **Problem:** Miner can see your trade and then put in a trade before/after yours
- This introduces many types of miner extractable value (MEV)

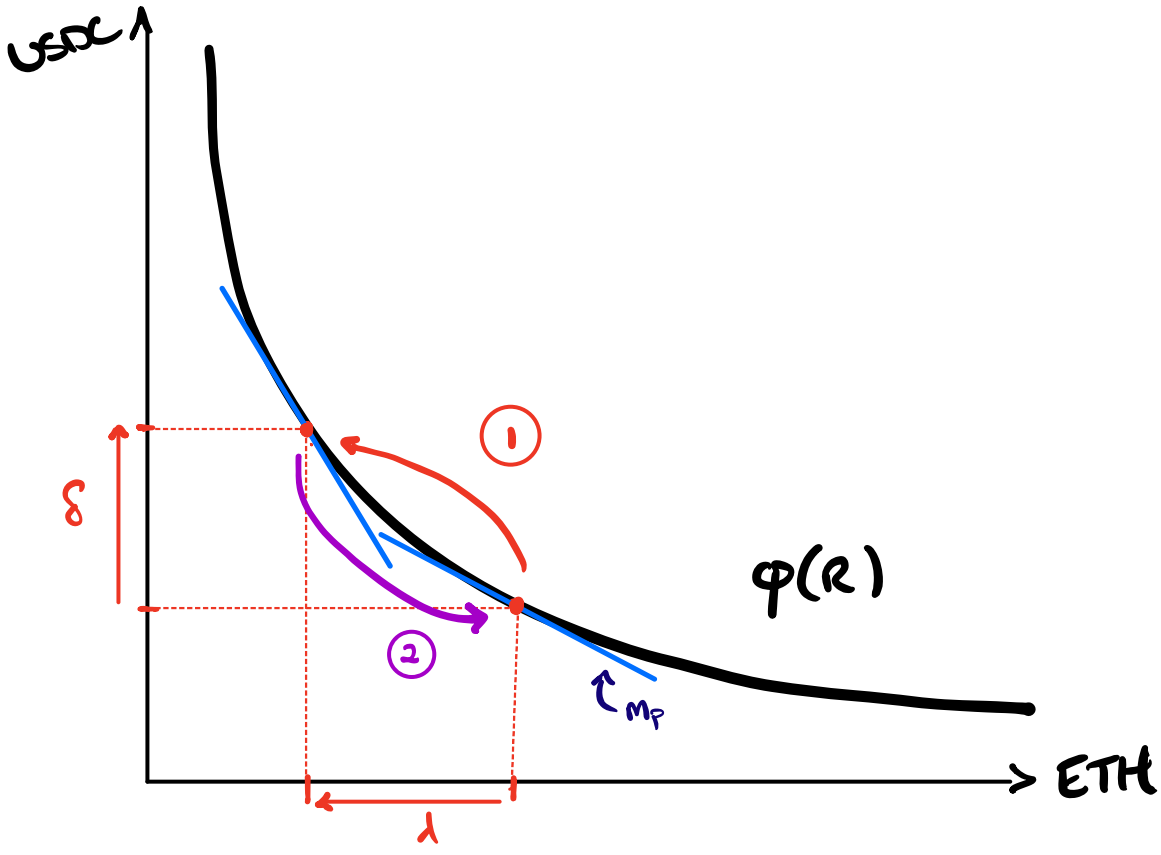
Frontrunning

- Miner can buy ETH right before you also buy



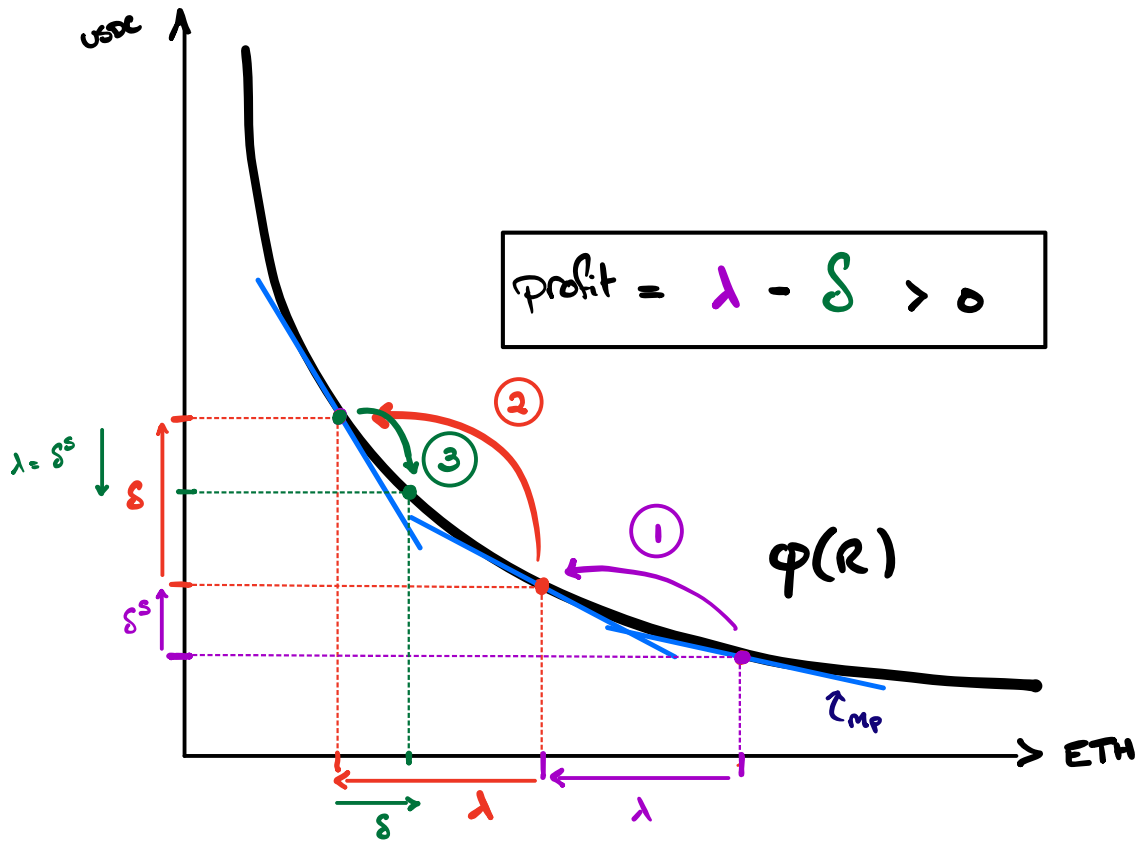
Backrunning

- Miner can take the arbitrage opportunity opened by your trade



Sandwiches

- Or the miner can do both!



Oracle manipulation

- Consider a betting protocol that uses a CFMM as a price oracle

Oracle manipulation

- Consider a betting protocol that uses a CFMM as a price oracle
- It may be profitable to manipulate the price and change outcome

Oracle manipulation

- Consider a betting protocol that uses a CFMM as a price oracle
- It may be profitable to manipulate the price and change outcome
- For example: Alice bets price $p \geq 1000$, Bob bets that $p < 1000$ on Monday 12:00 am
- If $p = 1100$ on Sunday 11:59pm, Bob is incentivized to manipulate oracle
- If manipulation is cheap enough, then Bob wins (?!)

Oracle manipulation (cont.)

- CFMMs let us reason about the *cost of manipulation*
- Very transparent (for better or worse)
- But more general ‘oracles’ may or may not

Oracle manipulation (cont.)

- CFMMs let us reason about the *cost of manipulation*
- Very transparent (for better or worse)
- But more general 'oracles' may or may not
- A tricky topic...

You don't even need to be a miner

You don't even need to be a miner

- The market has split into *searchers* and miners
- Searchers pay miners to include transactions in a certain order in the block

You don't even need to be a miner

- The market has split into *searchers* and miners
- Searchers pay miners to include transactions in a certain order in the block
- Anyone(!) can submit this to miners (via a service called Flashbots)
- See:

  `https://explore.flashbots.net/leaderboard`

Outline

Flashloans

- In traditional lending, must pay lender some interest rate over time
- But what if $T = 0$?

Flashloans

- In traditional lending, must pay lender some interest rate over time
- But what if $T = 0$?
- Atomicity of blockchains $\rightarrow$ instantaneous loans
- You can borrow as much as you want for a small fee, as long as you pay it back in the same transaction!

The implementation

- Flashloans admit a simple interface

```
flashloan(amt: uint, f: func, args: vec[any])
```

The implementation

- Flashloans admit a simple interface

```
flashloan(amt: uint, f: func, args: vec[any])
```

- Example: `flashloan(1000, f, ["hi"])`
  - Transfers 1000 token from `lender` to `sender`
  - Calls `f` with arguments `["hi"]`
  - Checks if `sender` has balance $\geq 1000 +$ `fee`
  - If so, gives $1000 +$ `fee` token to `lender`; `sender` keeps rest

What can you do with these?

- Arbitrage without capital requirements
- Oracle manipulation
- Perform no-capital liquidations in lending (next lecture)
- Many other things, too!

Next lecture

- We will talk about other applications of oracles
- These applications include lending (and stablecoins)
- Will also deal with how stablecoins are generally organized