Mapping the MEV solution space (mostly for DEX trading)

Hasu (Uncommon Core, Paradigm, Deribit)

What is MEV?

- MEV = permissionless incentives in blockchains

What is MEV?

- MEV = permissionless incentives in blockchains
- extractable on a first-come basis

What is MEV?

- MEV = permissionless incentives in blockchains
- extractable on a first-come basis
- good: liquidations, arbitrage

What is MEV?

- MEV = permissionless incentives in blockchains
- extractable on a first-come basis
- good: liquidations, arbitrage
- bad: frontrunning/sandwich attacks

Risks and benefits

- risks
  - financial loss for users

Risks and benefits

- risks
  - financial loss for users
  - consensus instability

Risks and benefits

- risks
  - financial loss for users
  - consensus instability
  - BP centralization

Risks and benefits

- risks
  - financial loss for users
  - consensus instability
  - BP centralization
- benefits
  - core defi functionality (liquidations + arbitrage)

Risks and benefits

- risks
  - financial loss for users
  - consensus instability
  - BP centralization
- benefits
  - core defi functionality (liquidations + arbitrage)
  - adds to security budget

Risks and benefits

- risks
  - financial loss for users
  - consensus instability
  - BP centralization
- benefits
  - core defi functionality (liquidations + arbitrage)
  - adds to security budget

Financial loss

- ~70% of gas used on Ethereum is for DEX trades

Financial loss

- ~70% of gas used on Ethereum is for DEX trades
- many of these trades unintentionally create MEV

Financial loss

- ~70% of gas used on Ethereum is for DEX trades
- many of these trades unintentionally create MEV
    - backrunning

Financial loss

- ~70% of gas used on Ethereum is for DEX trades
- many of these trades unintentionally create MEV
  - backrunning
  - sandwich attacks

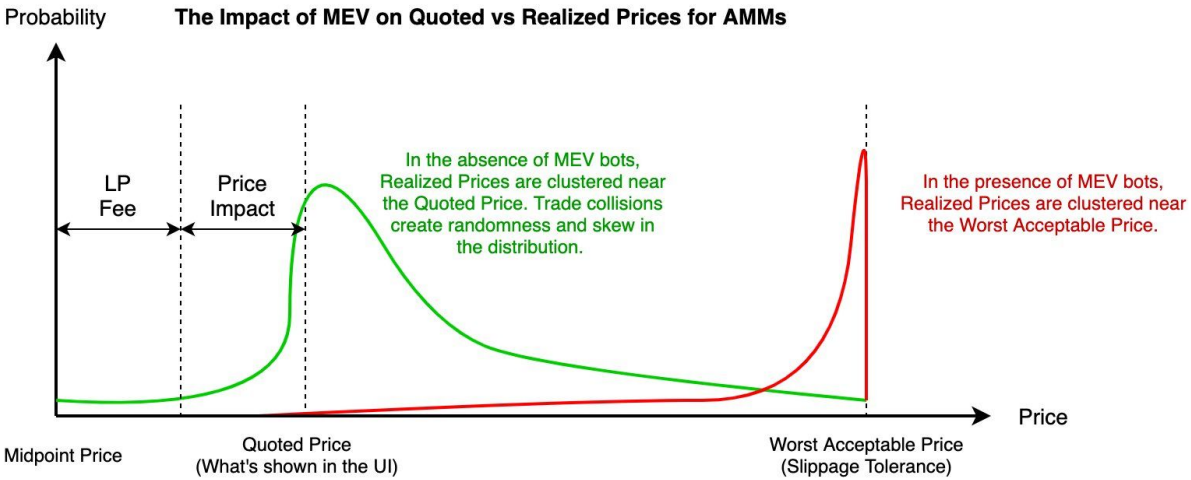
Backrunning

- there are 3 markets (Uniswap, Sushiswap, Binance). Alice buys only from Uniswap

Backrunning

- there are 3 markets (Uniswap, Sushiswap, Binance). Alice buys only from Uniswap
- if she pushes up the price on Uniswap enough, arbitrageurs can “run it back” to the fair market price

Sandwich attacks



Source: Will Warren, 0x

Two goals

1) Minimize MEV as much as possible

Two goals

1) Minimize MEV as much as possible
2) What we can’t minimize, democratize

How to minimize MEV

- consensus layer
  - fair ordering

How to minimize MEV

- consensus layer
  - fair ordering
  - privacy

How to minimize MEV

- consensus layer
  - fair ordering
  - privacy
- p2p layer
  - gasless txns

How to minimize MEV

- consensus layer
  - fair ordering
  - privacy
- p2p layer
  - gasless txns
  - mempool segregation

How to minimize MEV

- consensus layer
  - fair ordering
  - privacy
- p2p layer
  - gasless txns
  - mempool segregation
- app layer
  - DEX aggregators

How to minimize MEV

- consensus layer
  - fair ordering
  - privacy
- p2p layer
  - gasless txns
  - mempool segregation
- app layer
  - DEX aggregators
  - backrunning service

How to minimize MEV

- consensus layer
  - fair ordering
  - privacy
- p2p layer
  - gasless txns
  - mempool segregation
- app layer
  - DEX aggregators
  - backrunning service
  - off-chain ordering

How to minimize MEV

- consensus layer
  - fair ordering
  - privacy
- p2p layer
  - gasless txns
  - mempool segregation
- app layer
  - DEX aggregators
  - backrunning service
  - off-chain ordering

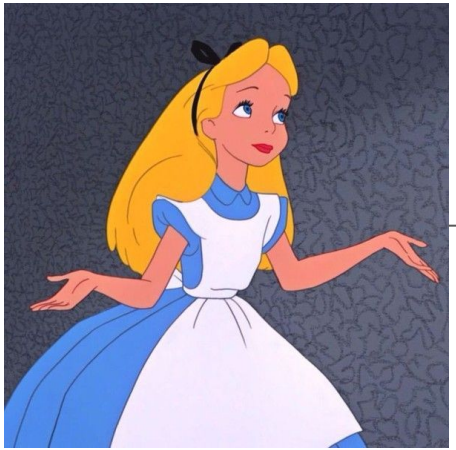
Gasless txns

- concept: gas payment conditional on success of the txn

Gasless txns

- concept: gas payment conditional on success of the txn
- requires support from: wallet + BP client

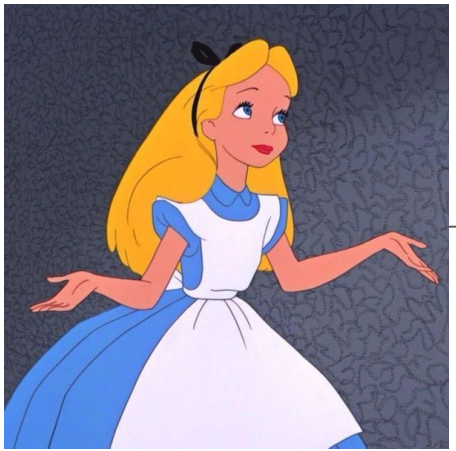
Mempool segregation

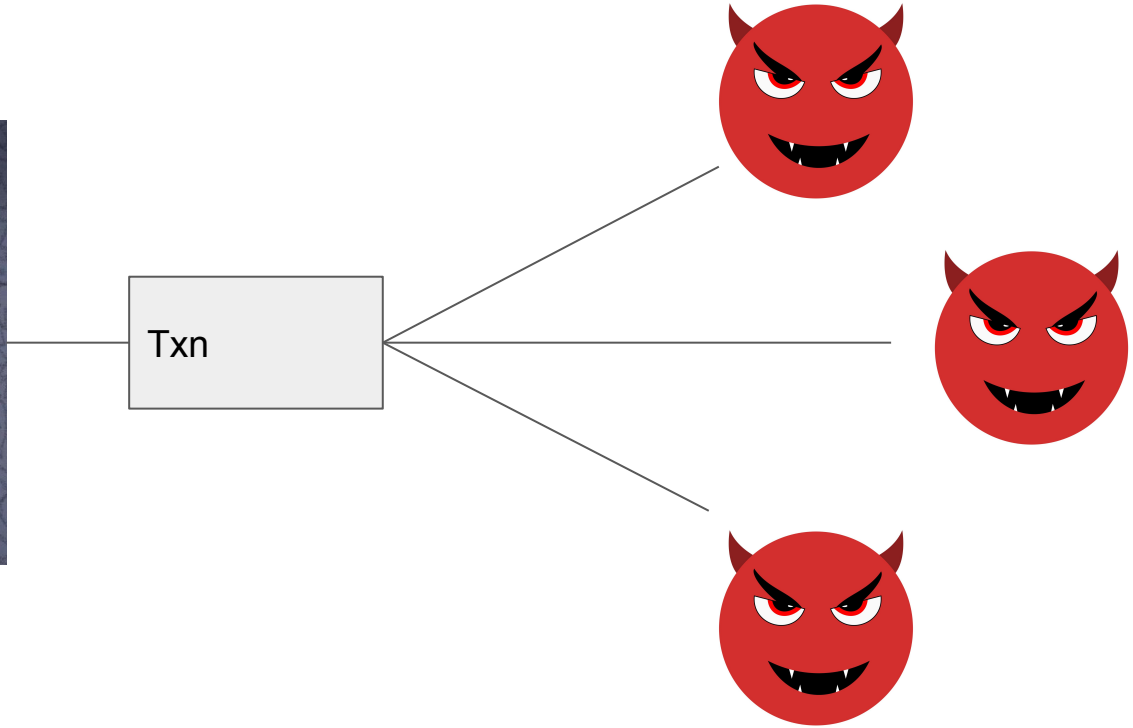


Txn

Mempool segregation

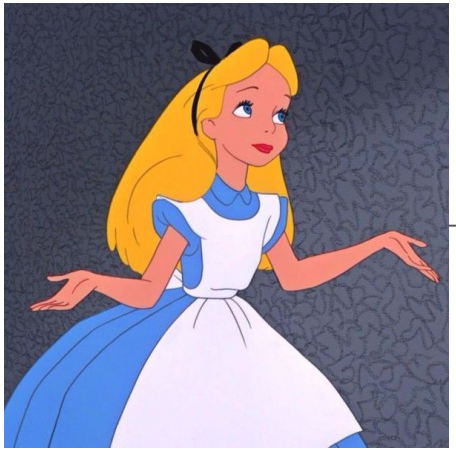
“You can all have it”



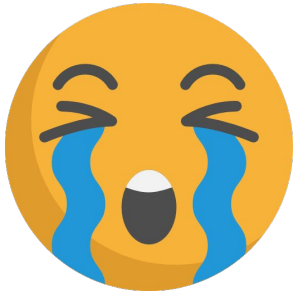


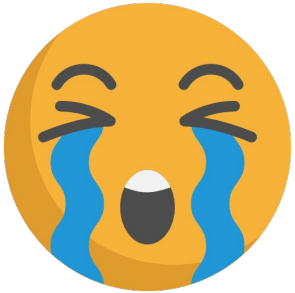
Mempool segregation

“You can have it exclusively, but…”



Txn





DEX aggregators

- buy from all markets at the same time, minimizing price impact

DEX aggregators

- buy from all markets at the same time, minimizing price impact
- no price impact -> no backrunning oppt

DEX aggregators

- buy from all markets at the same time, minimizing price impact
- no price impact -> no backrunning oppt
- the unsung heroes of MEV minimization

Backrunning service

- backrun your own trade

Backrunning service

- backrun your own trade
- not a product, but maybe a feature?

Off-chain ordering

1. Users submit txns to an off-chain oracle

Off-chain ordering

1. Users submit txns to an off-chain oracle
2. some fair ordering is applied

Off-chain ordering

1. Users submit txns to an off-chain oracle
2. some fair ordering is applied
3. trades are filled in that order

p2p layer

gasless txns

p2p layer

gasless txns

mempool segregation

p2p layer

gasless txns


mempool segregation




app layer

DEX aggregators



p2p layer

gasless txns


mempool segregation



Taichi Network




app layer

DEX aggregators



backrunning service

BackRunMe

SwapSwap

p2p layer

gasless txns


mempool segregation

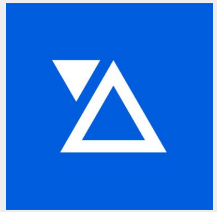

Taichi Network




app layer

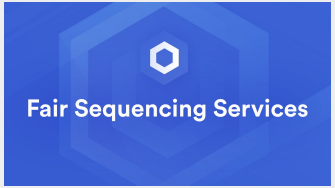
DEX aggregators





backrunning service

off-chain ordering




General improvements

- more concentrated liquidity -> lower price impact -> less MEV created

General improvements

- more concentrated liquidity -> lower price impact -> less MEV created
- an AMM pool that auctions off the “first-look”? / right to arbitrage
    - (solve IL and MEV at the same time)

...what we can’t minimize, democratize

- market for bundles, block templates

...what we can’t minimize, democratize

- market for bundles, block templates
- very important that this market is open + permissionless, not centrally controlled

Takeaways

- Not an either/or

Takeaways

- Not an either/or
- Innovation is happening on all layers

Takeaways

- Not an either/or
- Innovation is happening on all layers

Thanks!