

Lecture #26: MEV

COMS 4995-001:
The Science of Blockchains

URL: <https://timroughgarden.org/s25/>

Tim Roughgarden

Goals for Lecture #26

1. On-chain/decentralized exchanges (DEXes).
 - can swap one asset for another (e.g., Uniswap); primary source of “MEV”
2. Priority gas auctions (PGAs).
 - using transaction fees/bids to compete for the first tx in a block
3. Middle-of-block MEV.
 - frontrunning, backrunning, and sandwich attacks
4. Searchers, relay nodes, and private order flow.
 - Ethereum’s block production supply chain circa 2021-22

Top-of-Block MEV

Fact: a block producer (e.g., leader of a view) may have an outside incentive to make particular tx (e.g., its own) the first tx of its block.

Top-of-Block MEV

Fact: a block producer (e.g., leader of a view) may have an outside incentive to make particular tx (e.g., its own) the first tx of its block.

- called “top-of-block MEV”

Top-of-Block MEV

Fact: a block producer (e.g., leader of a view) may have an outside incentive to make particular tx (e.g., its own) the first tx of its block.

- called “top-of-block MEV”

Maximal Extractable Value (MEV): reward that a block producer can extract from the application layer.

Top-of-Block MEV

Fact: a block producer (e.g., leader of a view) may have an outside incentive to make particular tx (e.g., its own) the first tx of its block.

– called “top-of-block MEV”

Maximal Extractable Value (MEV): reward that a block producer can extract from the application layer.

- third source of revenue (adding to block/staking rewards + tx fees)

Top-of-Block MEV

Fact: a block producer (e.g., leader of a view) may have an outside incentive to make particular tx (e.g., its own) the first tx of its block.

– called “top-of-block MEV”

Maximal Extractable Value (MEV): reward that a block producer can extract from the application layer.

- third source of revenue (adding to block/staking rewards + tx fees)

Examples of top-of-block MEV: DEX arbitrage (next)

Top-of-Block MEV

Fact: a block producer (e.g., leader of a view) may have an outside incentive to make particular tx (e.g., its own) the first tx of its block.

– called “top-of-block MEV”

Maximal Extractable Value (MEV): reward that a block producer can extract from the application layer.

- third source of revenue (adding to block/staking rewards + tx fees)

Examples of top-of-block MEV: DEX arbitrage (next), loan liquidations (of undercollateralized loans)

Top-of-Block MEV

Fact: a block producer (e.g., leader of a view) may have an outside incentive to make particular tx (e.g., its own) the first tx of its block.

– called “top-of-block MEV”

Maximal Extractable Value (MEV): reward that a block producer can extract from the application layer.

- third source of revenue (adding to block/staking rewards + tx fees)

Examples of top-of-block MEV: DEX arbitrage (next), loan liquidations (of undercollateralized loans), NFT mints, etc.

Decentralized Finance and Exchanges

Decentralized Finance (DeFi): most consistently successful genre of applications on Ethereum, Solana, etc.

Decentralized Finance and Exchanges

Decentralized Finance (DeFi): most consistently successful genre of applications on Ethereum, Solana, etc.

- **key themes:** self-custody of assets, fewer/no intermediaries
 - e.g., permissionless buying/selling/borrowing/lending

Decentralized Finance and Exchanges

Decentralized Finance (DeFi): most consistently successful genre of applications on Ethereum, Solana, etc.

- **key themes:** self-custody of assets, fewer/no intermediaries
 - e.g., permissionless buying/selling/borrowing/lending
- **basic primitive:** swap one asset for another (e.g., USDC for ETH)

Decentralized Finance and Exchanges

Decentralized Finance (DeFi): most consistently successful genre of applications on Ethereum, Solana, etc.

- **key themes:** self-custody of assets, fewer/no intermediaries
 - e.g., permissionless buying/selling/borrowing/lending
- **basic primitive:** swap one asset for another (e.g., USDC for ETH)

Exchange: enables swaps. (centralized exchanges = Coinbase, Binance)

Decentralized Finance and Exchanges

Decentralized Finance (DeFi): most consistently successful genre of applications on Ethereum, Solana, etc.

- **key themes:** self-custody of assets, fewer/no intermediaries
 - e.g., permissionless buying/selling/borrowing/lending
- **basic primitive:** swap one asset for another (e.g., USDC for ETH)

Exchange: enables swaps. (centralized exchanges = Coinbase, Binance)

Decentralized exchange (DEX): (Uniswap, etc.)

- all liquidity + swapping logic on-chain (“liquidity” = assets available)
- swap = an atomic blockchain transaction (self-custody preserved)

DEX Designs

Decentralized exchange (DEX): all liquidity, swapping logic on-chain.

DEX Designs

Decentralized exchange (DEX): all liquidity, swapping logic on-chain.

Design #1: limit order book (LOB).

- a la NYSE (exchange matches buy and sell orders that agree on price)
- relatively computationally expensive (matching logic, frequent cancels, etc.)

DEX Designs

Decentralized exchange (DEX): all liquidity, swapping logic on-chain.

Design #1: limit order book (LOB).

- a la NYSE (exchange matches buy and sell orders that agree on price)
- relatively computationally expensive (matching logic, frequent cancels, etc.)

Design #2: automated market maker (AMM).

DEX Designs

Decentralized exchange (DEX): all liquidity, swapping logic on-chain.

Design #1: limit order book (LOB).

- a la NYSE (exchange matches buy and sell orders that agree on price)
- relatively computationally expensive (matching logic, frequent cancels, etc.)

Design #2: automated market maker (AMM).

- liquidity providers (“LPs”) deposit both assets into “trading pool”
 - in exchange for share of the trading fees

DEX Designs

Decentralized exchange (DEX): all liquidity, swapping logic on-chain.

Design #1: limit order book (LOB).

- a la NYSE (exchange matches buy and sell orders that agree on price)
- relatively computationally expensive (matching logic, frequent cancels, etc.)

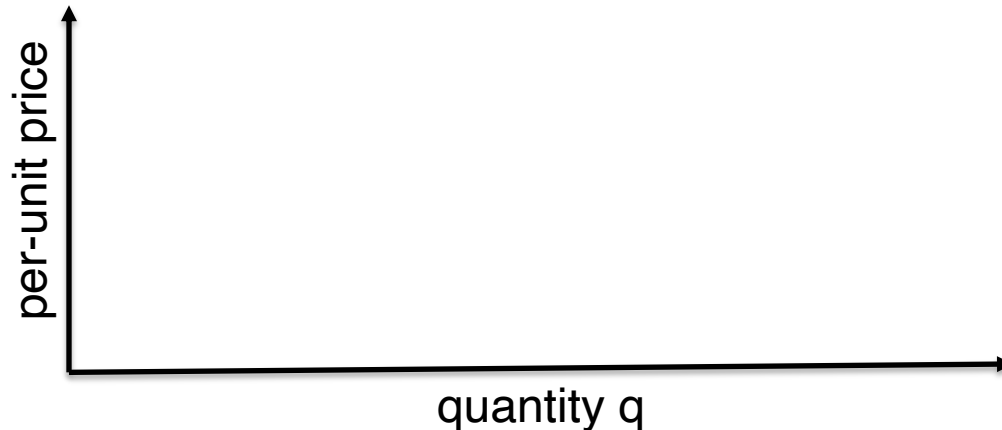
Design #2: automated market maker (AMM).

- liquidity providers (“LPs”) deposit both assets into “trading pool”
 - in exchange for share of the trading fees
- anyone can buy/sell from pool at “spot price” at any time
 - AMM serves as counterparty; any trade can be “reversed”

Price Curves

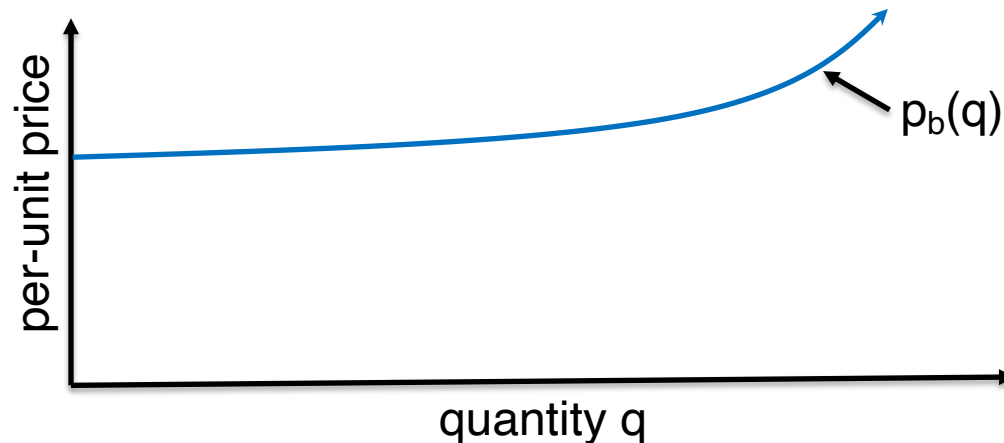
Decentralized exchange (DEX): all liquidity, swapping logic on-chain.

- leading designs: LOBs and (especially) AMMs



Price Curves

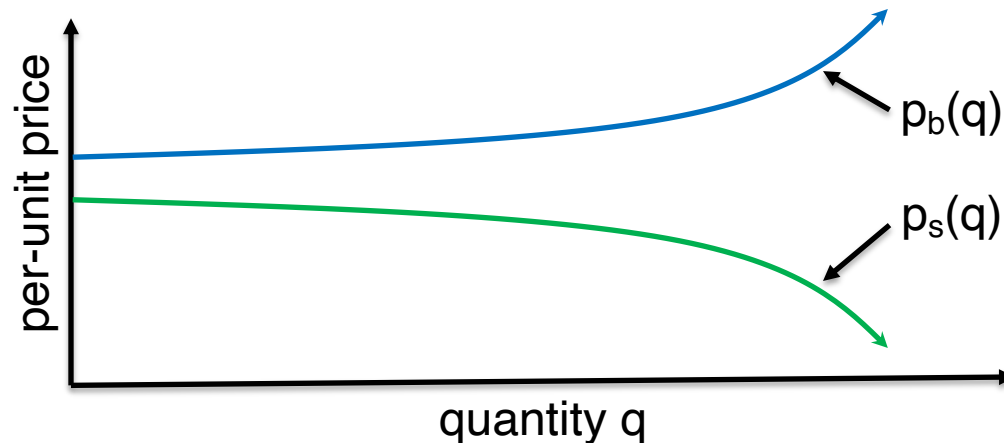
- Decentralized exchange (DEX):** all liquidity, swapping logic on-chain.
- leading designs: LOBs and (especially) AMMs
 - can buy q units of a token from a DEX for $p_b(q)$ per unit
 - $p_b(q)$ increases with q (the bigger the buy, the worse the price)



Price Curves

Decentralized exchange (DEX): all liquidity, swapping logic on-chain.

- leading designs: LOBs and (especially) AMMs
- can buy q units of a token from a DEX for $p_b(q)$ per unit
 - $p_b(q)$ increases with q (the bigger the buy, the worse the price)
- can sell q units of a token from a DEX for $p_s(q)$ per unit
 - $p_s(q)$ decreases with q (the bigger the sell, the worse the price)



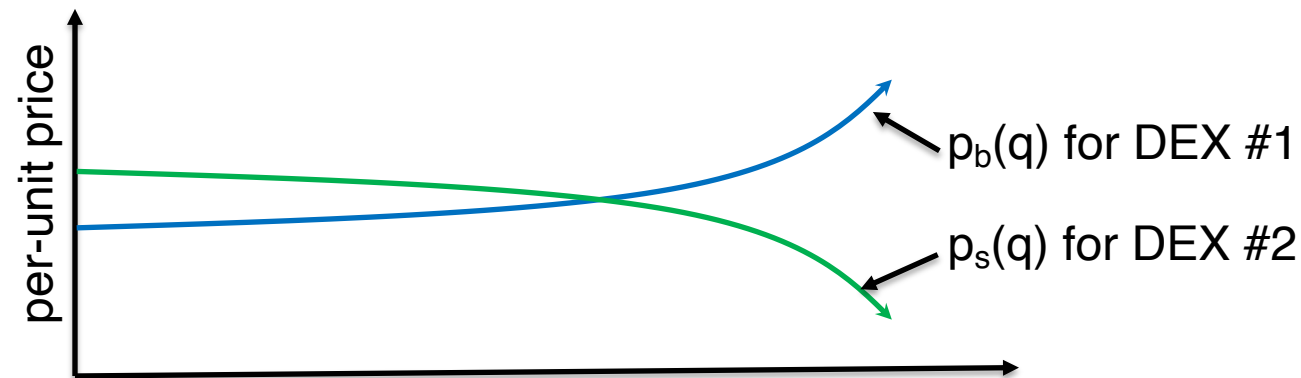
Top-of-Block Arbitrage

Scenario: two DEXes on the same blockchain, same asset pair.

Top-of-Block Arbitrage

Scenario: two DEXes on the same blockchain, same asset pair.

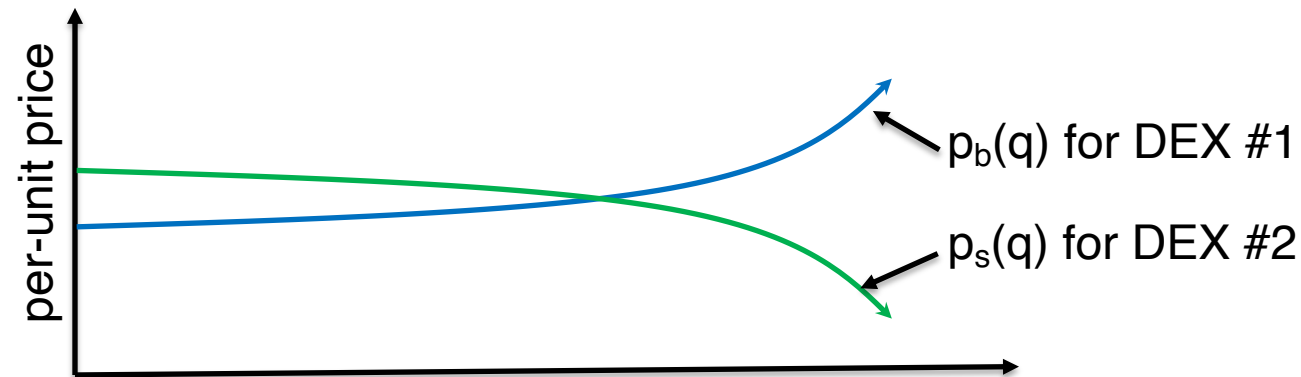
Suppose: after execution of last block, have inversion between the buy curve of DEX #1 and the sell curve of DEX #2:



Top-of-Block Arbitrage

Scenario: two DEXes on the same blockchain, same asset pair.

Suppose: after execution of last block, have inversion between the buy curve of DEX #1 and the sell curve of DEX #2:

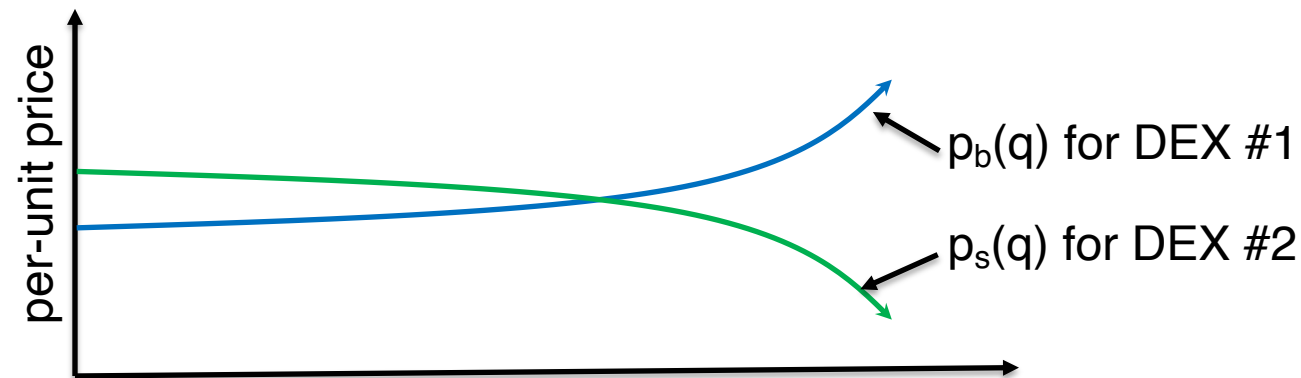


- anyone can profit by buying on DEX #1, selling on DEX #2

Top-of-Block Arbitrage

Scenario: two DEXes on the same blockchain, same asset pair.

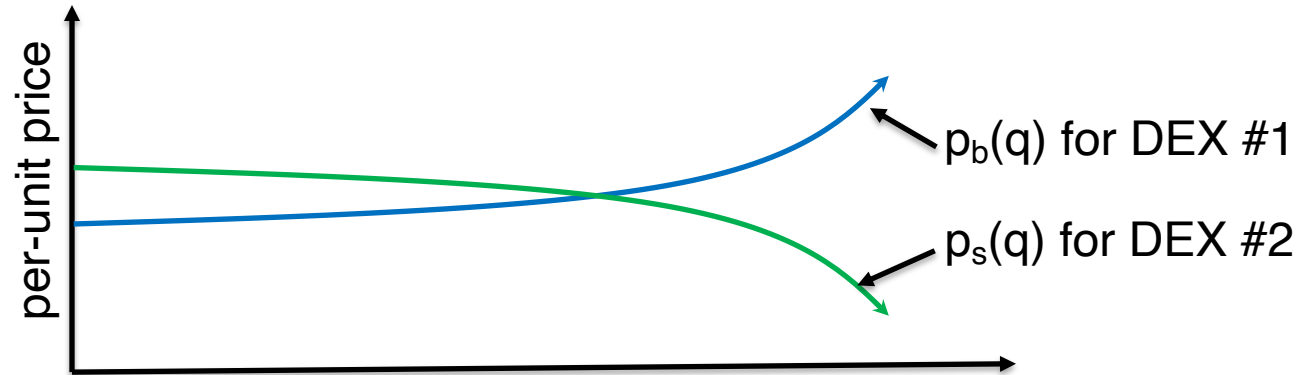
Suppose: after execution of last block, have inversion between the buy curve of DEX #1 and the sell curve of DEX #2:



- anyone can profit by buying on DEX #1, selling on DEX #2
 - **flash loans:** don't even need capital to be able to do this!

Top-of-Block Arbitrage

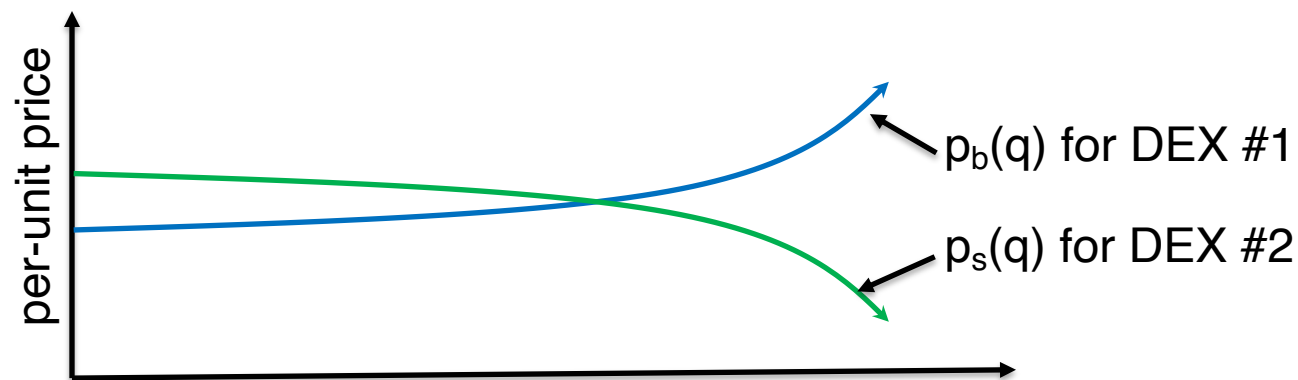
Suppose: after execution of last block, have inversion between the buy curve of DEX #1 and the sell curve of DEX #2:



- anyone can profit by buying on DEX #1, selling on DEX #2
- arbitrage opportunity available only to the first mover
 - post-arbitrage trade → spot price of the two DEXes will be equalized

Top-of-Block Arbitrage

Suppose: after execution of last block, have inversion between the buy curve of DEX #1 and the sell curve of DEX #2:



- anyone can profit by buying on DEX #1, selling on DEX #2
- arbitrage opportunity available only to the first mover
- expect would-be arbitrageurs to compete over opportunity
 - or opportunity to be taken by block producer itself

Priority Gas Auctions (PGAs)

Suppose: block producers order txs in decreasing order of bid.
– where bids are per-unit-size, as usual

Priority Gas Auctions (PGAs)

- Suppose:** block producers order txs in decreasing order of bid.
- where bids are per-unit-size, as usual
 - greedy algorithm for maximizing revenue from tx fees

Priority Gas Auctions (PGAs)

Suppose: block producers order txs in decreasing order of bid.

- where bids are per-unit-size, as usual
- greedy algorithm for maximizing revenue from tx fees

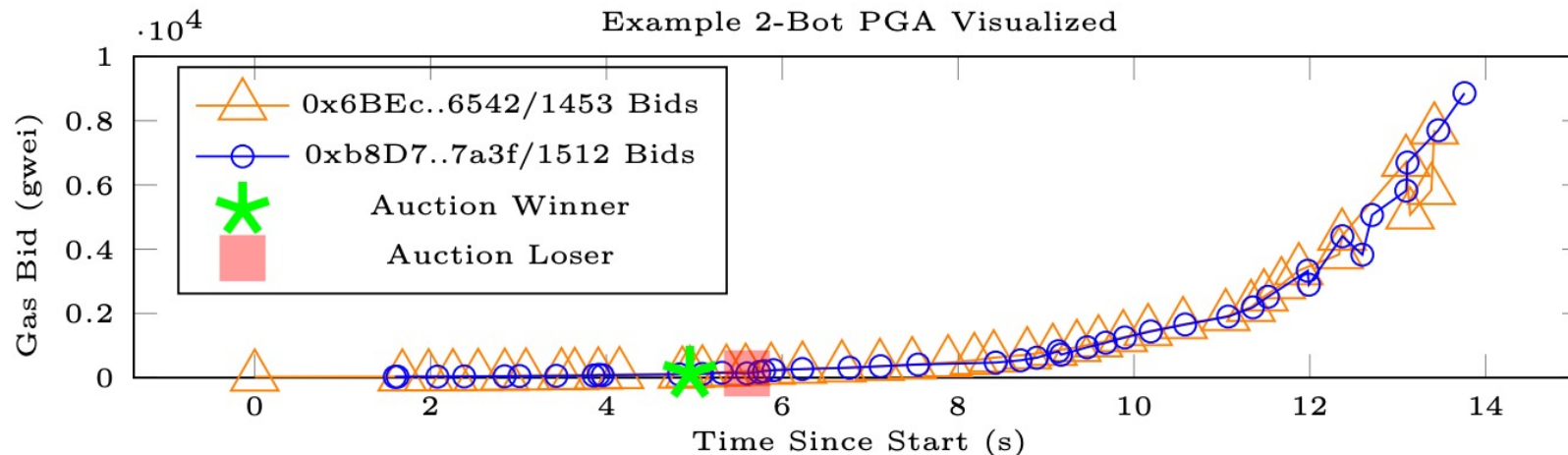
Priority gas auction: MEV-motivated users compete for first position in block through their (public) bids.

Priority Gas Auctions (PGAs)

Suppose: block producers order txs in decreasing order of bid.

- where bids are per-unit-size, as usual
- greedy algorithm for maximizing revenue from tx fees

Priority gas auction: MEV-motivated users compete for first position in block through their (public) bids.



source: “Flash Boys 2.0”
(paper by Daian et al.)

Priority Gas Auctions (PGAs)

Suppose: block producers order txs in decreasing order of bid.

Priority gas auction (PGA): MEV-motivated users compete for first position in block through their (public) bids.

Note: PGA competition → block producer gets most of the value.

Priority Gas Auctions (PGAs)

Suppose: block producers order txs in decreasing order of bid.

Priority gas auction (PGA): MEV-motivated users compete for first position in block through their (public) bids.

Note: PGA competition → block producer gets most of the value.

- reflects monopoly power of a block producer (e.g., leader of a view)
- alternatively, block producer could cash in on opportunity with its own tx

Priority Gas Auctions (PGAs)

Suppose: block producers order txs in decreasing order of bid.

Priority gas auction (PGA): MEV-motivated users compete for first position in block through their (public) bids.

Note: PGA competition → block producer gets most of the value.

Issues with PGAs:

Priority Gas Auctions (PGAs)

Suppose: block producers order txs in decreasing order of bid.

Priority gas auction (PGA): MEV-motivated users compete for first position in block through their (public) bids.

Note: PGA competition → block producer gets most of the value.

Issues with PGAs:

- losing txs waste ETH and blockspace (txs included but abort)

Priority Gas Auctions (PGAs)

Suppose: block producers order txs in decreasing order of bid.

Priority gas auction (PGA): MEV-motivated users compete for first position in block through their (public) bids.

Note: PGA competition → block producer gets most of the value.

Issues with PGAs:

- losing txs waste ETH and blockspace (txs included but abort)
- inflexible for competing for MEV that is not top-of-block (next)

Middle-of-Block MEV

More complex: incentive to be immediately before or after some tx.

Middle-of-Block MEV

More complex: incentive to be immediately before or after some tx.

Example: two categories of trades on an exchange:

Middle-of-Block MEV

More complex: incentive to be immediately before or after some tx.

Example: two categories of trades on an exchange:

- **informed:** (a.k.a. “toxic flow”) trader is buying/selling in advance of an upward/downward movement in asset’s market price
 - **note:** incentive to “frontrun” such a trade (same direction, right before)

Middle-of-Block MEV

More complex: incentive to be immediately before or after some tx.

Example: two categories of trades on an exchange:

- **informed:** (a.k.a. “toxic flow”) trader is buying/selling in advance of an upward/downward movement in asset’s market price
 - **note:** incentive to “frontrun” such a trade (same direction, right before)
- **uninformed:** (a.k.a. “retail”/“non-toxic flow”) trader just wants to trade
 - **note:** incentive to “backrun” such a trade (particularly on an AMM)
 - effectively a form of arbitrage (returns spot price to market price)

Middle-of-Block MEV

More complex: incentive to be immediately before or after some tx.

Examples:

- frontrunning an informed trade
- backrunning an uninformed trade (especially on an AMM)

Middle-of-Block MEV

More complex: incentive to be immediately before or after some tx.

Examples:

- frontrunning an informed trade
- backrunning an uninformed trade (especially on an AMM)
- “sandwich attack” = both frontrun and backrun a trade
 - in an AMM, guaranteed to be profitable (modulo gas fees + trading fees)
 - one of the least defensible forms of MEV (cf., arbitrage)

Middle-of-Block MEV

More complex: incentive to be immediately before or after some tx.

Examples:

- frontrunning an informed trade
- backrunning an uninformed trade (especially on an AMM)
- “sandwich attack” = both frontrun and backrun a trade
 - in an AMM, guaranteed to be profitable (modulo gas fees + trading fees)
 - one of the least defensible forms of MEV (cf., arbitrage)

Note: PGAs ill-suited to competing for such middle-of-block MEV.

Flashbots v1 ($\approx$ 2021-2022)

Philosophy: lean into MEV, minimize collateral damage to blockspace.

- next lecture: approaches to MEV mitigation

Flashbots v1 ($\approx$ 2021-2022)

Philosophy: lean into MEV, minimize collateral damage to blockspace.

- next lecture: approaches to MEV mitigation

High-level idea: separate roles of “searchers” and block producers.

- “searcher” = e.g. arbitrageur (blockchain user)
- block producer = blockchain validator that is leader of current view

Flashbots v1 ($\approx$ 2021-2022)

Philosophy: lean into MEV, minimize collateral damage to blockspace.

– next lecture: approaches to MEV mitigation

High-level idea: separate roles of “searchers” and block producers.

- searchers locate MEV opportunities, encapsulate in “bundles” that they send to block producers

Flashbots v1 ($\approx$ 2021-2022)

Philosophy: lean into MEV, minimize collateral damage to blockspace.

– next lecture: approaches to MEV mitigation

High-level idea: separate roles of “searchers” and block producers.

- searchers locate MEV opportunities, encapsulate in “bundles” that they send to block producers
- example bundle:

Flashbots v1 ($\approx$ 2021-2022)

Philosophy: lean into MEV, minimize collateral damage to blockspace.

- next lecture: approaches to MEV mitigation

High-level idea: separate roles of “searchers” and block producers.

- searchers locate MEV opportunities, encapsulate in “bundles” that they send to block producers
- example bundle:
 - tx #1: AMM trade taken from the public mempool

Flashbots v1 ($\approx$ 2021-2022)

Philosophy: lean into MEV, minimize collateral damage to blockspace.

- next lecture: approaches to MEV mitigation

High-level idea: separate roles of “searchers” and block producers.

- searchers locate MEV opportunities, encapsulate in “bundles” that they send to block producers
- example bundle:
 - tx #1: AMM trade taken from the public mempool
 - tx #2: searcher’s own backrunning tx (fails if not immediately after tx #1)

Flashbots v1 ($\approx$ 2021-2022)

Philosophy: lean into MEV, minimize collateral damage to blockspace.

- next lecture: approaches to MEV mitigation

High-level idea: separate roles of “searchers” and block producers.

- searchers locate MEV opportunities, encapsulate in “bundles” that they send to block producers
- example bundle:
 - tx #1: AMM trade taken from the public mempool
 - tx #2: searcher’s own backrunning tx (fails if not immediately after tx #1)
 - tx #3: payment from searcher to block producer, conditional on successful completion of tx #2 ($\approx$ conditional bid for bundle)

Searchers and Block Producers

- High-level idea:** separate roles of “searchers” and block producers.
- searchers locate MEV opportunities, encapsulate in “bundles” that they send to block producers (with conditional bids), e.g.:
 - tx #1: AMM trade taken from the public mempool
 - tx #2: searcher’s own backrunning tx (fails if not immediately after tx #1)
 - tx #3: payment from searcher to block producer, conditional on success

Searchers and Block Producers

- High-level idea:** separate roles of “searchers” and block producers.
- searchers locate MEV opportunities, encapsulate in “bundles” that they send to block producers (with conditional bids), e.g.:
 - tx #1: AMM trade taken from the public mempool
 - tx #2: searcher’s own backrunning tx (fails if not immediately after tx #1)
 - tx #3: payment from searcher to block producer, conditional on success
 - block producer incentivized to include at most one bundle corresponding to a given MEV opportunity (others would fail)

Searchers and Block Producers

- High-level idea:** separate roles of “searchers” and block producers.
- searchers locate MEV opportunities, encapsulate in “bundles” that they send to block producers (with conditional bids), e.g.:
 - tx #1: AMM trade taken from the public mempool
 - tx #2: searcher’s own backrunning tx (fails if not immediately after tx #1)
 - tx #3: payment from searcher to block producer, conditional on success
 - block producer incentivized to include at most one bundle corresponding to a given MEV opportunity (others would fail)
 - in effect, PGA has moved off-chain (implicitly run by block producer), losing txs/bundles never included in block

Relay Nodes

Question: why doesn't block producer take MEV opportunity for itself? (in example, by copy-pasting txs #1 and #2)

Relay Nodes

Question: why doesn't block producer take MEV opportunity for itself? (in example, by copy-pasting txs #1 and #2)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

Relay Nodes

Question: why doesn't block producer take MEV opportunity for itself? (in example, by copy-pasting txs #1 and #2)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

- searchers submit bundles to one or more relay nodes

Relay Nodes

Question: why doesn't block producer take MEV opportunity for itself? (in example, by copy-pasting txs #1 and #2)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

- searchers submit bundles to one or more relay nodes
- relay nodes forward latest bundles to whitelisted block producers
 - “private order flow” (generally never hit the public mempool)

Relay Nodes

Question: why doesn't block producer take MEV opportunity for itself? (in example, by copy-pasting txs #1 and #2)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

- searchers submit bundles to one or more relay nodes
- relay nodes forward latest bundles to whitelisted block producers
 - “private order flow” (generally never hit the public mempool)
- deviating block producers (e.g., steal MEV) removed from whitelist
 - misbehaving searchers (e.g., submit bad bundles) also filtered out

Relay Nodes (con'd)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

- searchers submit bundles to one or more relay nodes
- relay nodes forward latest bundles to whitelisted block producers
- deviating block producers (e.g., steal MEV) removed from whitelist

Good news:

Relay Nodes (con'd)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

- searchers submit bundles to one or more relay nodes
- relay nodes forward latest bundles to whitelisted block producers
- deviating block producers (e.g., steal MEV) removed from whitelist

Good news: design addresses inefficiencies of PGAs.

- txs that would have failed on-chain now filtered out off-chain

Relay Nodes (con'd)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

- searchers submit bundles to one or more relay nodes
- relay nodes forward latest bundles to whitelisted block producers
- deviating block producers (e.g., steal MEV) removed from whitelist

Good news: design addresses inefficiencies of PGAs.

- txs that would have failed on-chain now filtered out off-chain
- for “obvious” MEV, searcher competition ➔ most of value to block producers
 - like with PGAs, but now also with “middle-of-block MEV”
- clever searchers may be able to retain most of “long-tail MEV”

Relay Nodes (con'd)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

Good news: design addresses inefficiencies of PGAs.

Open question: can trusted relay nodes be eliminated?

Relay Nodes (con'd)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

Good news: design addresses inefficiencies of PGAs.

Open question: can trusted relay nodes be eliminated?

- via better design/incentives?

Relay Nodes (con'd)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

Good news: design addresses inefficiencies of PGAs.

Open question: can trusted relay nodes be eliminated?

- via better design/incentives?
 - [Bahrani/Garimidi/Roughgarden 24] maybe not

Relay Nodes (con'd)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

Good news: design addresses inefficiencies of PGAs.

Open question: can trusted relay nodes be eliminated?

- via better design/incentives?
 - [Bahrani/Garimidi/Roughgarden 24] maybe not
- via an encrypted mempool? (e.g., using threshold cryptography)

Relay Nodes (con'd)

Relay nodes: trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)

Good news: design addresses inefficiencies of PGAs.

Open question: can trusted relay nodes be eliminated?

- via better design/incentives?
 - [Bahrani/Garimidi/Roughgarden 24] maybe not
- via an encrypted mempool? (e.g., using threshold cryptography)
- via trusted execution environments (TEEs)?