Lecture #27:
Proposer-Builder Separation

COMS 4995-001:
The Science of Blockchains

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

Tim Roughgarden

Goals for Lecture #27

1. Relay nodes for private order flow.
   - trusted intermediaries between searchers and block producers
2. Validator centralization.
   - worry: heterogeneity in MEV extraction leads to centralized validator set
3. Proposer-builder separation (PBS) and MEV-Boost.
   - outsourcing block-building rights to third parties
4. Censorship-resistance.
   - experimental ideas to mitigate dangers with centralized builders

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)

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 assembles, proposes block (using bundles + txs)

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 assembles, proposes block (using bundles + txs)
  - incentivized to include only bundles that complete successfully
  - losing txs now filtered off-chain, not included on-chain (as in a PGA)

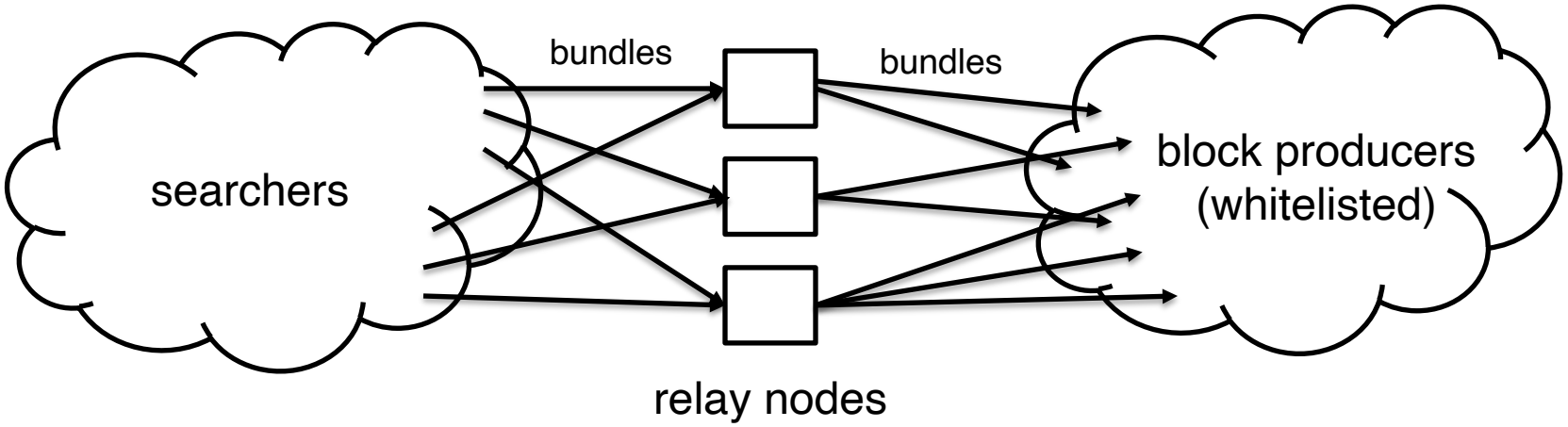
Relay Nodes

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.)

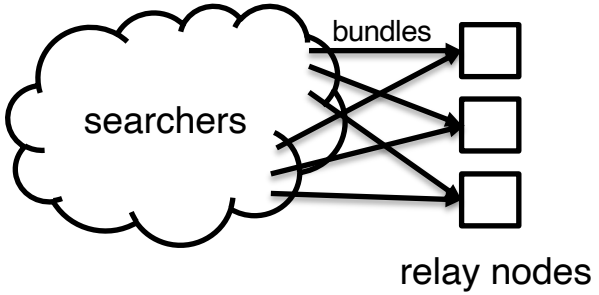


Relay Nodes

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

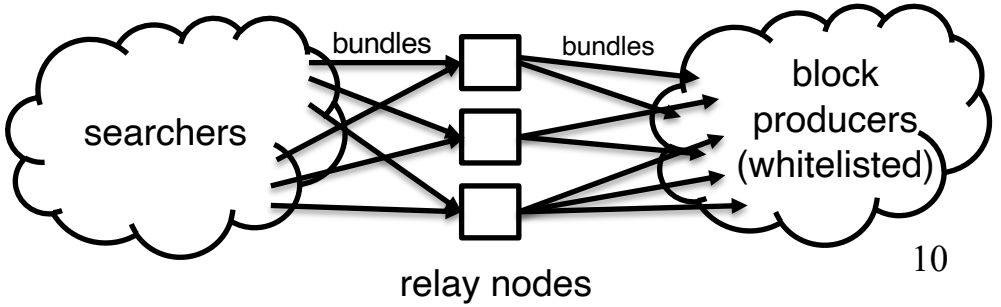


Relay Nodes

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

Note: for "obvious" MEV, searcher competition ➔ expect most of value of MEV opportunity to be competed away to block producers.

- like with PGAs, but now also with "middle-of-block MEV"

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

Note: for "obvious" MEV, searcher competition ➔ expect most of value of MEV opportunity to be competed away to block producers.

- like with PGAs, but now also with "middle-of-block MEV"
- reflects monopoly power of the current block producer

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

Note: for "obvious" MEV, searcher competition ➔ expect most of value of MEV opportunity to be competed away to block producers.

- like with PGAs, but now also with "middle-of-block MEV"
- reflects monopoly power of the current block producer
- clever searchers may be able to retain much of the "long-tail" MEV

MEV and Centralization

Permissionless consensus: “anyone” can be a validator.

MEV and Centralization

Permissionless consensus: “anyone” can be a validator.

Refined goal: all validators earn the same (per-unit-stake) rewards.

MEV and Centralization

Permissionless consensus: “anyone” can be a validator.

Refined goal: all validators earn the same (per-unit-stake) rewards.

- Nakamoto consensus: each hash equally likely to unlock block reward
- question: is this goal still possible with MEV?

MEV and Centralization

Permissionless consensus: “anyone” can be a validator.

Refined goal: all validators earn the same (per-unit-stake) rewards.

- Nakamoto consensus: each hash equally likely to unlock block reward
- question: is this goal still possible with MEV?

Motivation: preserve “decentralization” (want many validators, with different owners/operators).

- note: centralization (i.e., too few participants) potentially threatens consistency and liveness of the blockchain protocol

MEV and Centralization (con’d)

Worry #1: heterogeneity in validator rewards ➔ centralization.

MEV and Centralization (con'd)

Worry #1: heterogeneity in validator rewards ➔ centralization.

Bad scenario #1: all but the highest-earning validators are unprofitable (due to capital/operating costs) and stop participating.

- economic forces ➔ centralized validator set at equilibrium

MEV and Centralization (con'd)

Worry #1: heterogeneity in validator rewards ➔ centralization.

Bad scenario #1: all but the highest-earning validators are unprofitable (due to capital/operating costs) and stop participating.

- economic forces ➔ centralized validator set at equilibrium

Bad scenario #2: highest-earning validators reinvest profits, eventually control ≥ 51% of hashrate or ≥ 34% of stake.

- long-run dynamics ➔ validator set eventually centralizes

MEV and Centralization (con'd)

Worry #1: heterogeneity in validator rewards ➔ centralization.

- bad scenario #1: all but the highest-earning validators are unprofitable and stop participating
- bad scenario #2: highest-earning validators reinvest profits, eventually control ≥ 51% of hashrate or ≥ 34% of stake.

Worry #2: "professional" validators will be much better at capitalizing on MEV opportunities than "rank-and-file" validators.

MEV and Centralization (con'd)

Worry #1: heterogeneity in validator rewards ➔ centralization.

- bad scenario #1: all but the highest-earning validators are unprofitable and stop participating
- bad scenario #2: highest-earning validators reinvest profits, eventually control ≥ 51% of hashrate or ≥ 34% of stake.

Worry #2: "professional" validators will be much better at capitalizing on MEV opportunities than "rank-and-file" validators.

- partially mitigated by searcher competition

MEV and Centralization (con'd)

Worry #1: heterogeneity in validator rewards ➔ centralization.

- bad scenario #1: all but the highest-earning validators are unprofitable and stop participating
- bad scenario #2: highest-earning validators reinvest profits, eventually control ≥ 51% of hashrate or ≥ 34% of stake.

Worry #2: "professional" validators will be much better at capitalizing on MEV opportunities than "rank-and-file" validators.

- partially mitigated by searcher competition
- but block-building still could be hard problem
  - e.g., determining the optimal set of bundles to include in block

Proposer-Builder Separation (PBS)

Idea: validators outsource block-building to specialized “builders.”

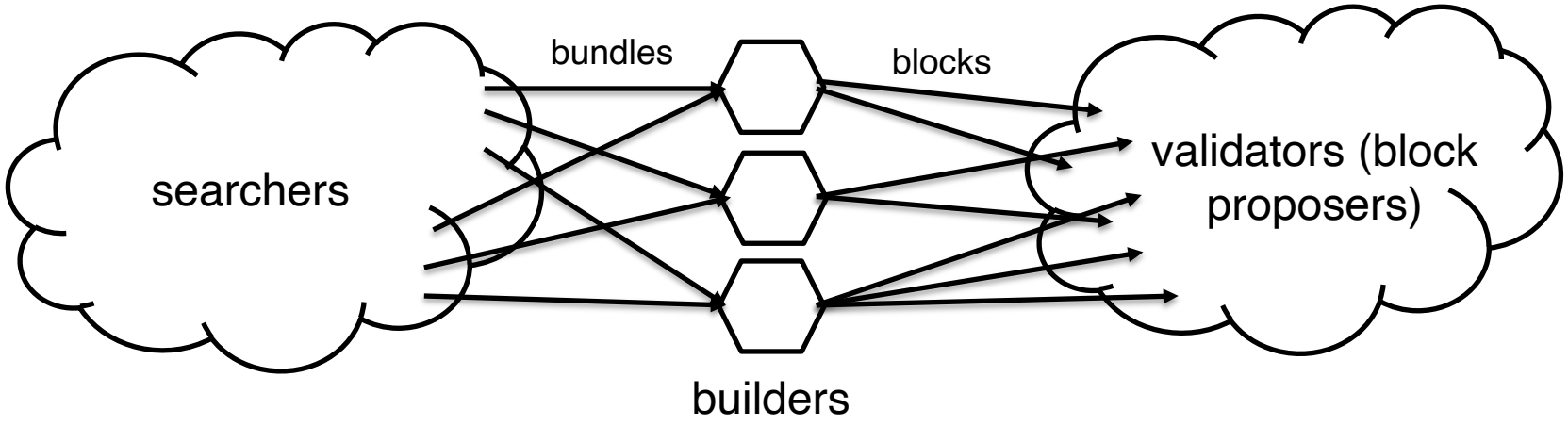
- leader of current view effectively auctions off its block-building rights

Proposer-Builder Separation (PBS)

Idea: validators outsource block-building to specialized “builders.”

- leader of current view effectively auctions off its block-building rights

Ideal block production supply chain with PBS:



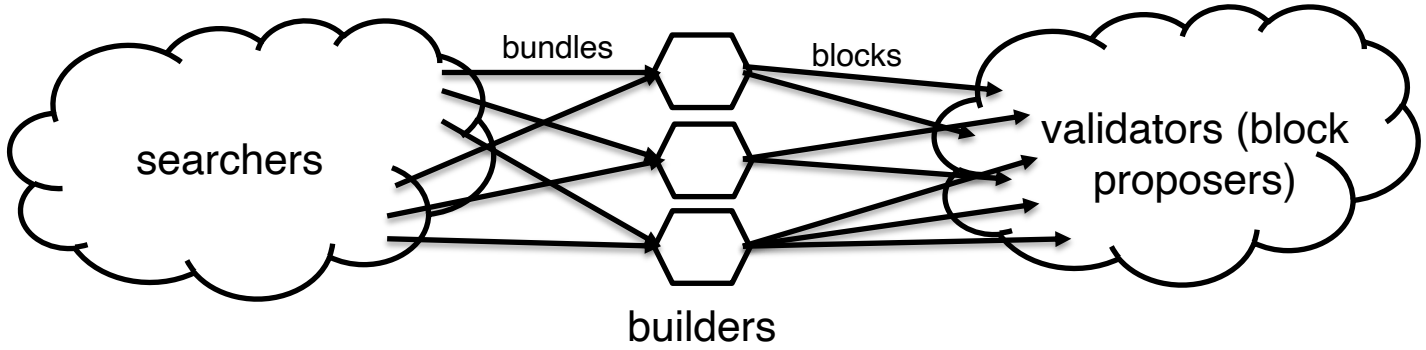
Block	Slot	Age	Txn	Fee Recipient	Gas Used	Gas Limit	Base Fee	Reward	Burnt Fees (ETH)
22330775	11548010	14 secs ago	184	Titan Builder	14,024,967 (38.96%)	35,999,965	1.166 Gwei	0.01742 ETH	0.016360 (48.42%)
22330774	11548009	26 secs ago	228	Titan Builder	17,704,576 (49.23%)	35,964,845	1.168 Gwei	0.02039 ETH	0.020692 (50.36%)
22330773	11548008	38 secs ago	204	beaverbuild	20,131,027 (55.92%)	36,000,000	1.151 Gwei	0.01934 ETH	0.023184 (54.52%)
22330772	11548007	50 secs ago	173	beaverbuild	16,695,651 (46.38%)	36,000,000	1.162 Gwei	0.01824 ETH	0.019404 (51.53%)
22330771	11548006	1 min ago	324	Titan Builder	35,644,314 (99.01%)	36,000,000	1.035 Gwei	0.0492 ETH	0.036904 (42.86%)
22330770	11548005	1 min ago	115	quasarbuilder	7,545,978 (20.96%)	36,000,000	1.116 Gwei	0.00557 ETH	0.008424 (60.18%)
22330769	11548004	1 min ago	186	beaverbuild	17,009,799 (47.25%)	35,999,965	1.124 Gwei	0.04548 ETH	0.019121 (29.59%)
22330768	11548003	1 min ago	214	beaverbuild	21,519,909 (59.84%)	35,964,845	1.097 Gwei	0.04709 ETH	0.023610 (33.39%)
22330767	11548002	1 min ago	244	Titan Builder	21,948,869 (60.97%)	36,000,000	1.067 Gwei	0.01889 ETH	0.023438 (55.37%)
22330766	11548001	2 mins ago	146	beaverbuild	10,282,523 (28.56%)	36,000,000	1.128 Gwei	0.00775 ETH	0.011602 (59.95%)
22330765	11548000	2 mins ago	211	Titan Builder	22,679,059 (63.00%)	35,999,931	1.092 Gwei	0.01958 ETH	0.024784 (55.85%)
22330764	11547999	2 mins ago	315	Titan Builder	30,120,386 (83.75%)	35,964,811	1.007 Gwei	0.0271 ETH	0.030355 (52.82%)
22330763	11547998	2 mins ago	43	Lido: Execution Layer Rew...	2,326,986 (6.48%)	35,929,725	1.13 Gwei	0.00809 ETH	0.002631 (24.52%)
22330762	11547997	2 mins ago	274	Titan Builder	25,964,257 (72.19%)	35,964,845	1.071 Gwei	0.03609 ETH	0.027818 (43.53%)
22330761	11547996	3 mins ago	216	beaverbuild	24,057,554 (66.83%)	36,000,000	1.028 Gwei	0.04062 ETH	0.024735 (37.84%)
22330760	11547995	3 mins ago	165	Lido: Execution Layer Rew...	11,446,914 (31.80%)	36,000,000	1.077 Gwei	0.00408 ETH	0.012330 (75.12%)

Proposer-Builder Separation (PBS)

Idea: validators outsource block-building to specialized “builders.”

- leader of current view effectively auctions off its block-building rights

Ideal block production supply chain with PBS:



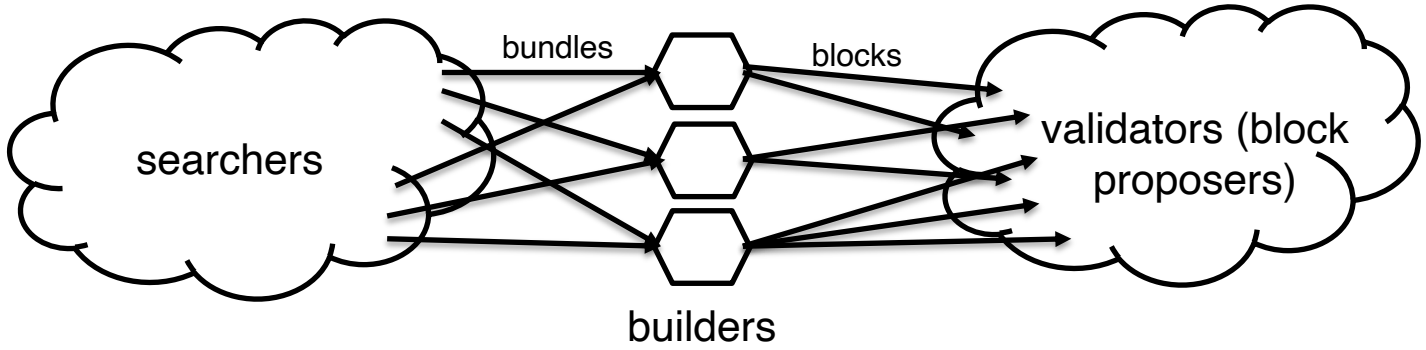
Goal: builder competition ➔ validators get most of the MEV.

Proposer-Builder Separation (PBS)

Idea: validators outsource block-building to specialized “builders.”

– leader of current view effectively auctions off its block-building rights

Ideal block production supply chain with PBS:



Goal: builder competition ➔ validators get most of the MEV.

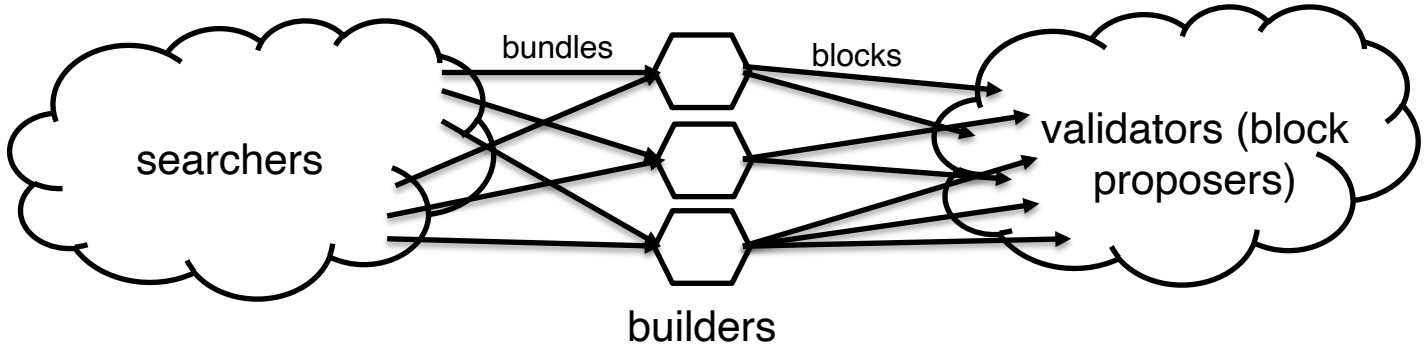
- ➔ (expected) rate of (per-stake) rewards same for all validators

Proposer-Builder Separation (PBS)

Idea: validators outsource block-building to specialized “builders.”

- leader of current view effectively auctions off its block-building rights

Ideal block production supply chain with PBS:

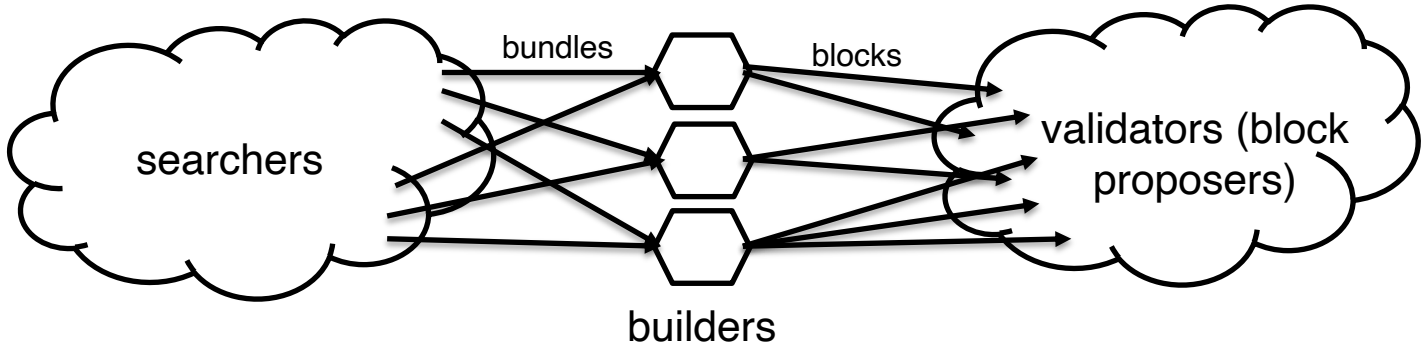


Goal: builder competition ➔ validators get most of the MEV.

- ➔ (expected) rate of (per-stake) rewards same for all validators
  - ➔ hopefully no centralization in validator set, only in the builder set

Proposer-Builder Separation (PBS)

Ideal block production supply chain with PBS:



Goal: builder competition ➔ validators get most of the MEV.

- ➔ (expected) rate of (per-stake) rewards same for all validators
  - ➔ hopefully no centralization in validator set, only in the builder set

Question: why wouldn't validators steal MEV opportunities?

- e.g., replace backrunning txs in block with its own

MEV-Boost (≈ Flashbots v2)

MEV-Boost: out-of-protocol implementation of PBS.

MEV-Boost (≈ Flashbots v2)

MEV-Boost: out-of-protocol implementation of PBS.

- released by Flashbots at same time as “the Merge” (August 2022)
  - i.e., Ethereum’s migration from proof-of-work to proof-of-stake

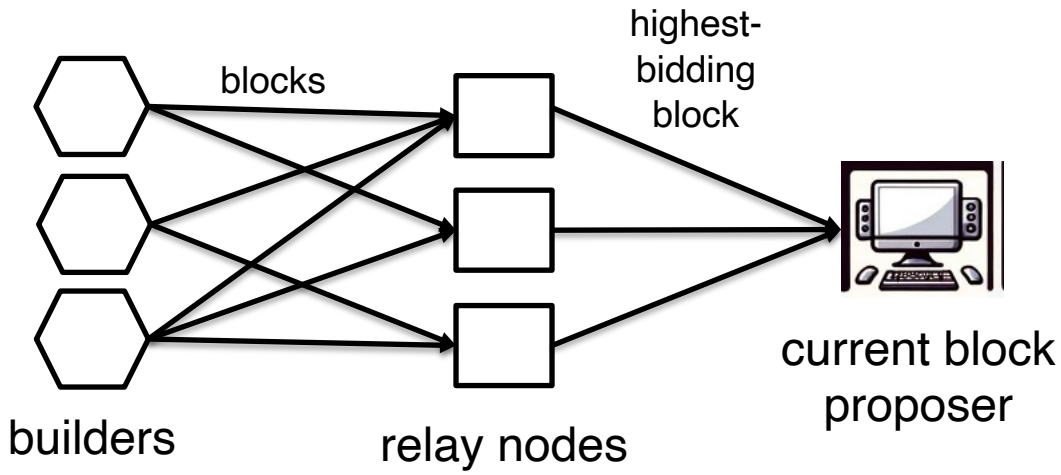
MEV-Boost (≈ Flashbots v2)

MEV-Boost: out-of-protocol implementation of PBS.

- released by Flashbots at same time as “the Merge” (August 2022)
  - i.e., Ethereum’s migration from proof-of-work to proof-of-stake
- open question how to implement PBS purely in-protocol

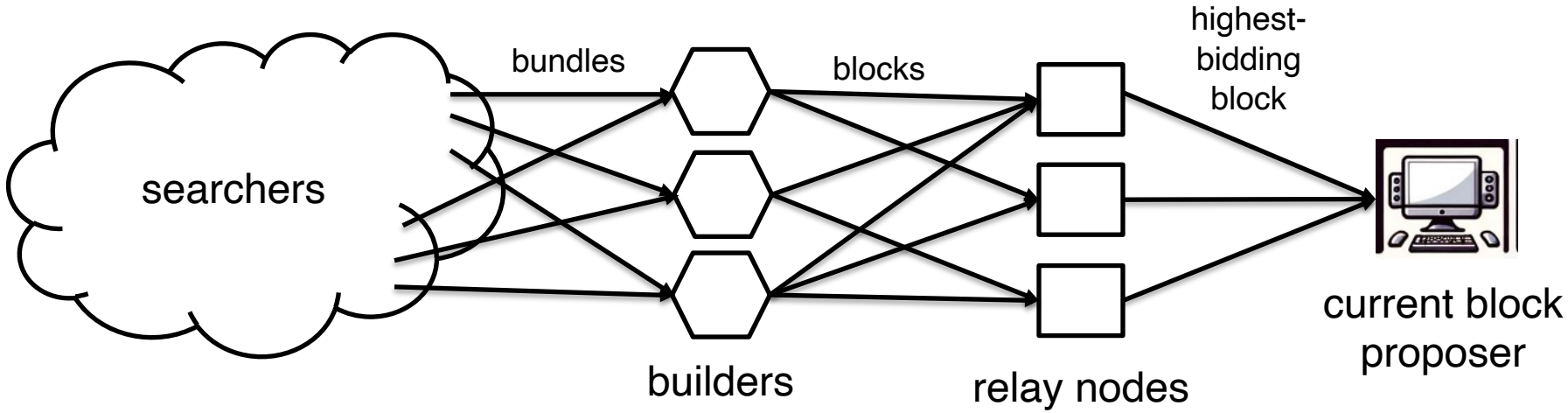
MEV-Boost (≈ Flashbots v2)

Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)



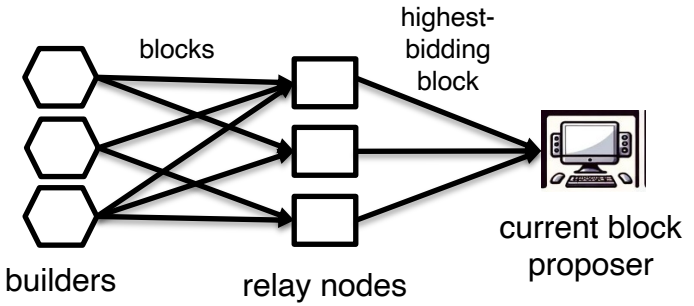
MEV-Boost (≈ Flashbots v2)

Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)



MEV-Boost (≈ Flashbots v2)

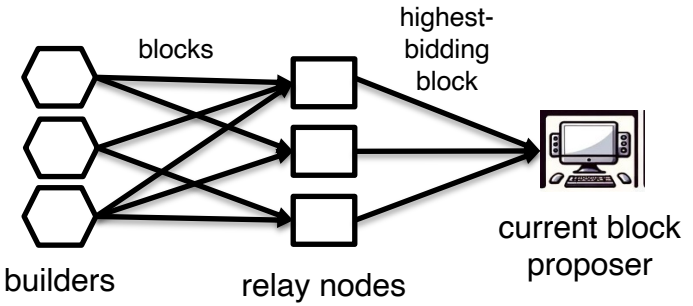
Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)



MEV-Boost (≈ Flashbots v2)

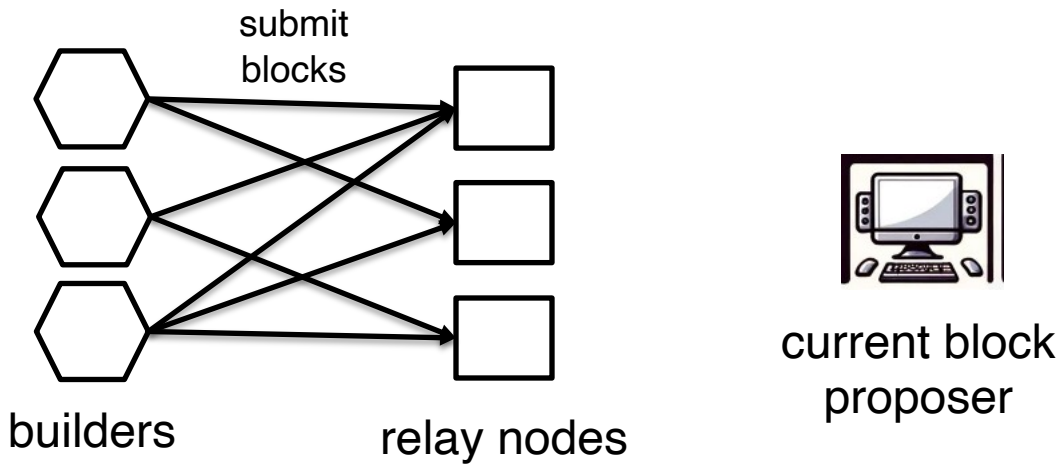
Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)

- builders submit blocks to relay nodes along with bids (paid to proposer if selected)



MEV-Boost (≈ Flashbots v2)

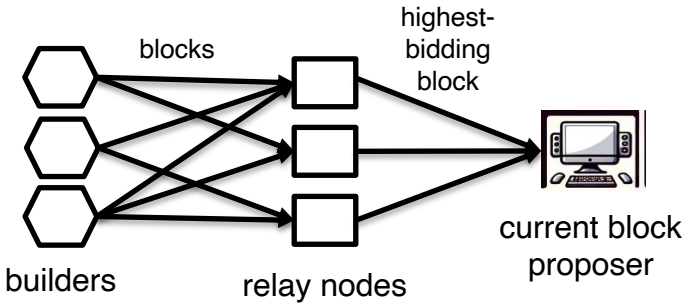
Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)



MEV-Boost (≈ Flashbots v2)

Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)

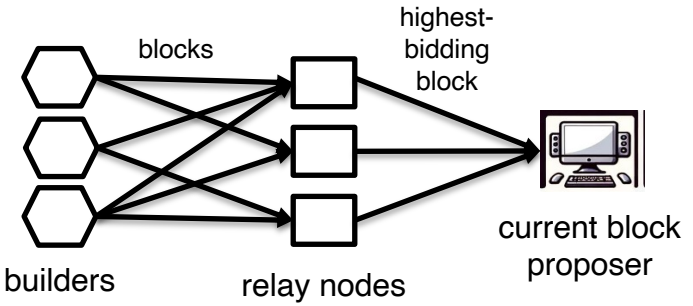
- builders submit blocks to relay nodes along with bids (paid to proposer if selected)
- relay nodes check block validity



MEV-Boost (≈ Flashbots v2)

Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)

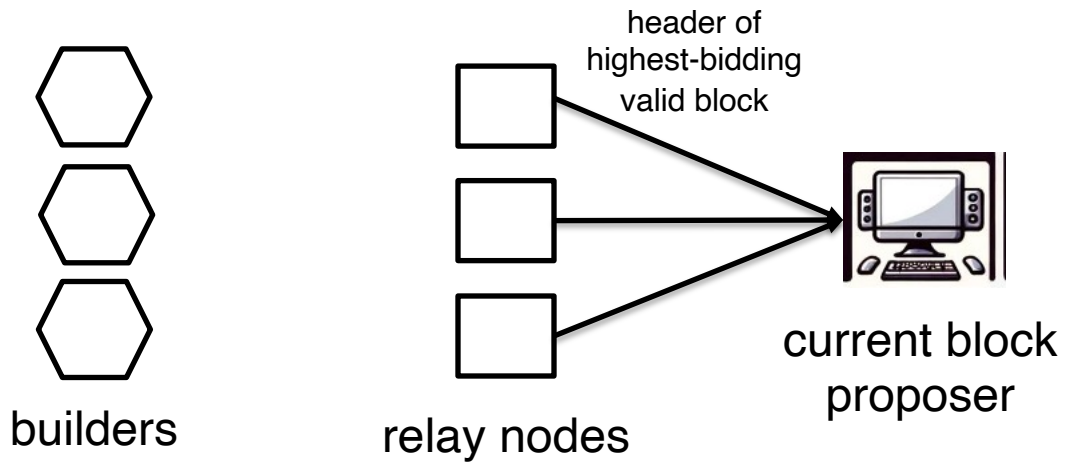
- builders submit blocks to relay nodes along with bids (paid to proposer if selected)
- relay nodes check block validity



- relay nodes forward header (only) of block with highest bid to the current block proposer (in proof-of-stake, known in advance)

MEV-Boost (≈ Flashbots v2)

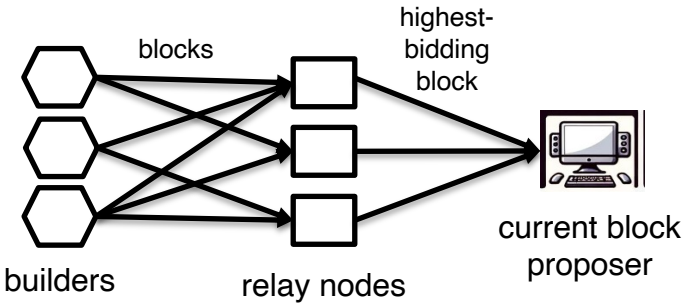
Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)



MEV-Boost (≈ Flashbots v2)

Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)

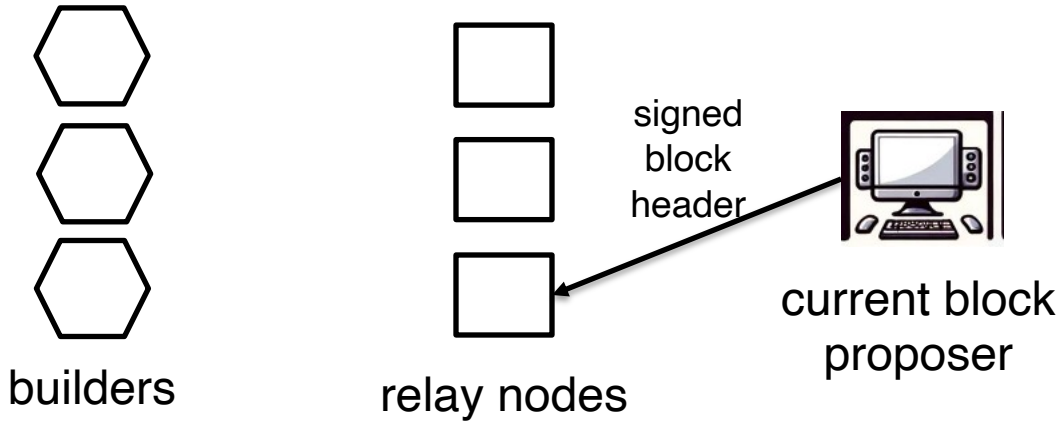
- builders submit blocks to relay nodes along with bids (paid to proposer if selected)
- relay nodes check block validity



- relay nodes forward header (only) of block with highest bid to the current block proposer (in proof-of-stake, known in advance)
- proposer signs block header, returns it to relay node
  - key point: at time of signing, txs unknown to proposer (can't steal MEV)

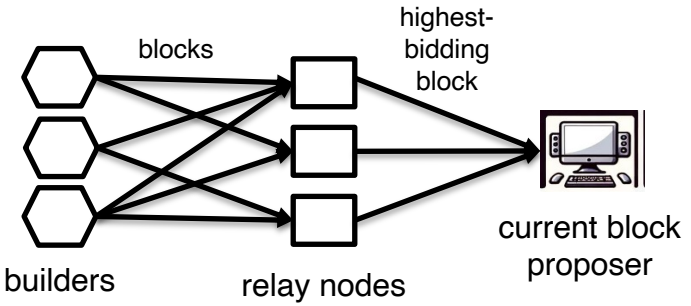
MEV-Boost (≈ Flashbots v2)

Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)



MEV-Boost (≈ Flashbots v2)

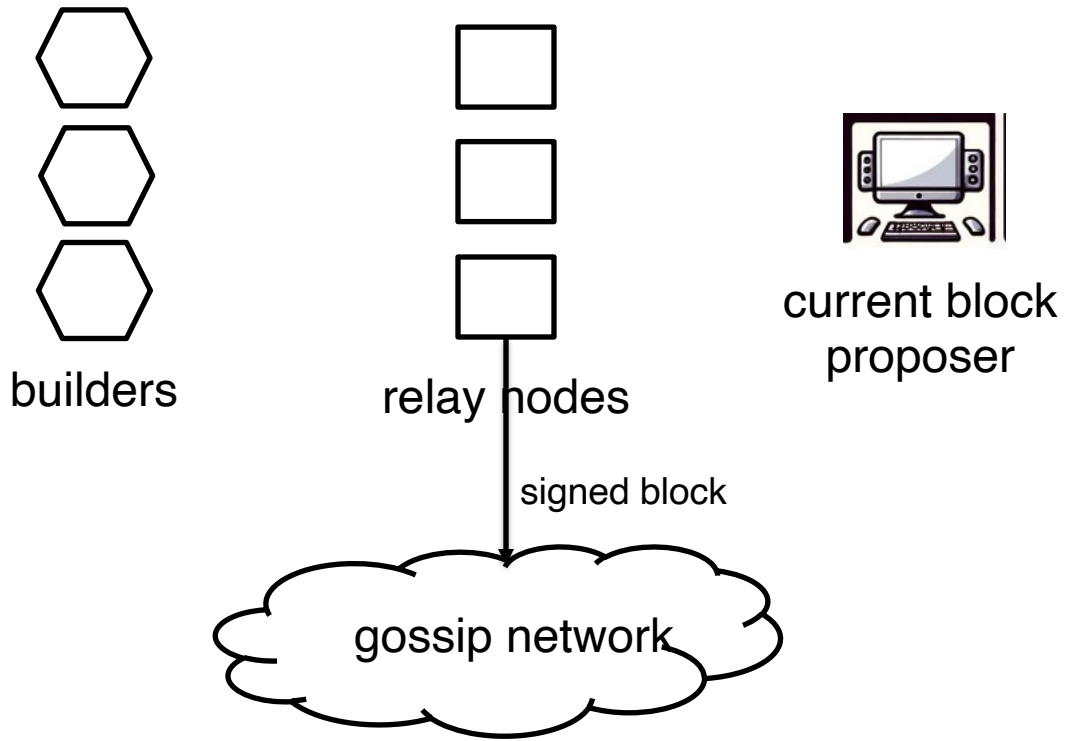
Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)



- builders submit blocks to relay nodes along with bids (paid to proposer if selected)
- relay nodes check block validity
- relay nodes forward header (only) of block with highest bid to the current block proposer (in proof-of-stake, known in advance)
- proposer signs block header, returns it to relay node
  - key point: at time of signing, txs unknown to proposer (can't steal MEV)
- relay node broadcasts signed block over gossip network

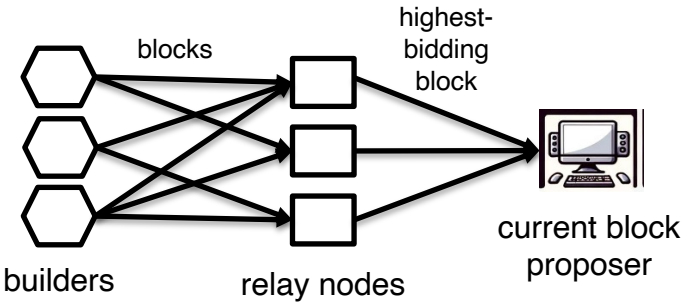
MEV-Boost (≈ Flashbots v2)

Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers). (run by Flashbots, bloXroute, etc.)



MEV-Boost (≈ Flashbots v2)

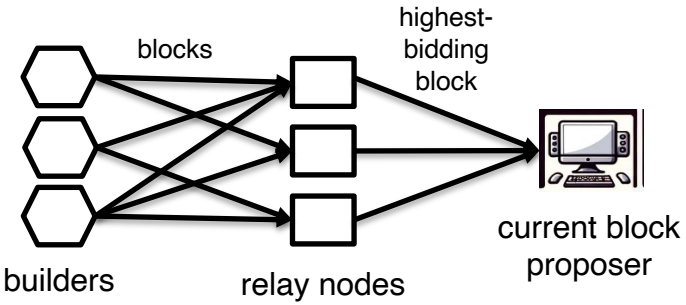
Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers).



- builders submit blocks + bid to relay nodes
- relay nodes check block validity
- relay nodes forward header of highest bidding valid block to current proposer
- proposer signs block header, returns it to relay node
  - key point: at time of signing, txs unknown to proposer (can't steal MEV)
- relay node broadcasts signed block over gossip network

MEV-Boost (≈ Flashbots v2)

Relay nodes: trusted servers that act as intermediaries between builders and validators (a.k.a. proposers).



- builders submit blocks + bid to relay nodes
- relay nodes check block validity
- relay nodes forward header of highest bidding valid block to current proposer
- proposer signs block header, returns it to relay node
  - key point: at time of signing, txs unknown to proposer (can't steal MEV)
- relay node broadcasts signed block over gossip network

Note: no longer need to trust proposer to not steal MEV.

- permissionless for validators (no whitelist), can just run MEV-Boost

Do We Need Trusted Relays?

Relay nodes: trusted servers that act as intermediaries.

- between searchers and validators in v1, builders and validators in v2

Do We Need Trusted Relays?

Relay nodes: trusted servers that act as intermediaries.

- between searchers and validators in v1, builders and validators in v2

Open question: can trusted relay nodes be eliminated?

Do We Need Trusted Relays?

Relay nodes: trusted servers that act as intermediaries.

- between searchers and validators in v1, builders and validators in v2

Open question: can trusted relay nodes be eliminated?

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

Do We Need Trusted Relays?

Relay nodes: trusted servers that act as intermediaries.

- between searchers and validators in v1, builders and validators in v2

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)
  - issue: block-builder may still have lots of side information about txs

Do We Need Trusted Relays?

Relay nodes: trusted servers that act as intermediaries.

- between searchers and validators in v1, builders and validators in v2

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)
  - issue: block-builder may still have lots of side information about txs
- via trusted execution environments (TEEs)?
  - current approach taken by Flashbots and others

Centralization and Censorship

Question: big problem if a blockchain protocol has only a few validators?

Centralization and Censorship

Question: big problem if a blockchain protocol has only a few validators? [answer: yes, largely defeats the point of a blockchain protocol]

Centralization and Censorship

Question: big problem if a blockchain protocol has only a few validators? [answer: yes, largely defeats the point of a blockchain protocol]

Question: big problem if a blockchain protocol has only a few block-builders (but lots of validators)?

Centralization and Censorship

Question: big problem if a blockchain protocol has only a few validators? [answer: yes, largely defeats the point of a blockchain protocol]

Question: big problem if a blockchain protocol has only a few block-builders (but lots of validators)?

- block-building might be an intrinsically specialized skill

Centralization and Censorship

Question: big problem if a blockchain protocol has only a few validators? [answer: yes, largely defeats the point of a blockchain protocol]

Question: big problem if a blockchain protocol has only a few block-builders (but lots of validators)?

- block-building might be an intrinsically specialized skill
- at least builders don't control consensus, right?
  - block proposer could always propose their own block if they prefer

Centralization and Censorship

Question: big problem if a blockchain protocol has only a few validators? [answer: yes, largely defeats the point of a blockchain protocol]

Question: big problem if a blockchain protocol has only a few block-builders (but lots of validators)?

- block-building might be an intrinsically specialized skill
- at least builders don't control consensus, right?
  - block proposer could always propose their own block if they prefer

One issue: censorship --- i.e., systematic exclusion of certain txs.

- e.g., for financial or legal/regulatory reasons

Censorship-Resistance

Question: big problem if a blockchain protocol has only a few block-builders (but lots of validators)?

One issue: censorship --- i.e., systematic exclusion of certain txs.

Open question: how to mitigate censorship risks.

Censorship-Resistance

Question: big problem if a blockchain protocol has only a few block-builders (but lots of validators)?

One issue: censorship --- i.e., systematic exclusion of certain txs.

Open question: how to mitigate censorship risks.

- idea #1: inclusion lists (IL) --- let validators designate txs whose inclusion is part of block validity (cf., forced inclusion in rollups)

Censorship-Resistance

Question: big problem if a blockchain protocol has only a few block-builders (but lots of validators)?

One issue: censorship --- i.e., systematic exclusion of certain txs.

Open question: how to mitigate censorship risks.

- idea #1: inclusion lists (IL) --- let validators designate txs whose inclusion is part of block validity (cf., forced inclusion in rollups)
- idea #2: multiple concurrent proposers (MCP) --- take union of multiple validator block proposals ➔ censoring requires large bribes to multiple validators [Fox/Pai/Resnick 23]