

CPSC 3640/5400: Decentralized Payments, Contracts, and Finance for Humans and AI

Lecture 14: DeFi Risk of MEV

Fan Zhang
Yale University
2026 Fall

Roadmap so far

- **DeFi Primitives:** What they are, how they are implemented
 - Apps: [Tokens](#), [Tokenization](#), [Decentralized Exchanges](#), Oracles, lending/borrowing, (re-)staking
 - Infra for fast transactions
- **DeFi advantages:** things not possible in TradFi
 - [Privacy](#), Interoperability, and Censorship Resistance
- **DeFi risks:** new problems unique to DeFi & mitigation
 - [order manipulation \(today\)](#), human factors, bugs

Ordering manipulation

Alice: sell @ \$90

Adv : buy @ ~~\$90~~0

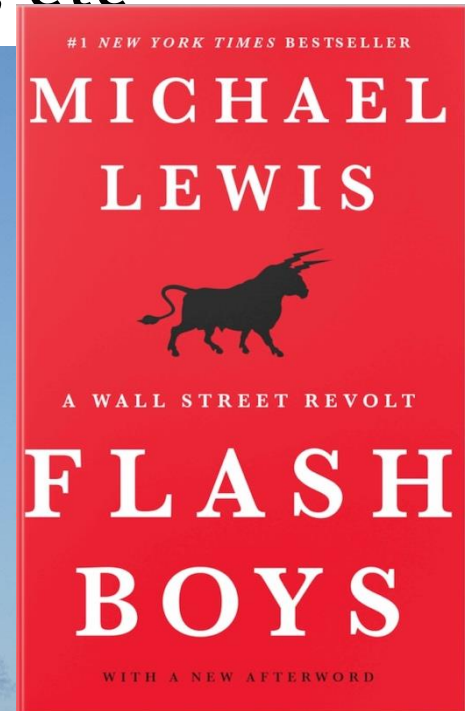
Adv : sell @ \$100

- How to insert txns?
- E.g., HFT firms gain timing advantage through co-location, low-latency networks, etc

Frontrunning attack

Bob	-10
Adv	+10

Adv “extracted” \$10
by ordering txns
cleverly



Ordering manipulation

Alice: sell @ \$90
Adv : buy @ \$90
Adv : sell @ \$100
Bob : buy @ \$100

Frontrunning attack

Bob	-10
Adv	+10

Adv “extracted” \$10
by ordering txns
cleverly

- How to insert txns to **exchanges on blockchain**?
- **Block producers** see all transactions and completely controls transaction ordering.
- Power -> money
- **Maximal Extractable Value (MEV):** value block producers extract from application layer.

MEV: the formal definition

MEV is the **most** a block producer **p** can gain on chain state **s**:

$$\text{MEV}(p, s) = \max_{B \in \text{validBlocks}(p, s)} \text{EV}(p, B, s)$$

where

- **validBlocks(p, s)**: blocks p can build from mempool transactions plus its own
- **EV(p, B, s)**: total balance gain across p's accounts after executing txs in B on s

This problem is hard to optimize in general. In practice, block producers focus on specific MEV opportunities.

Roadmap

- MEV extraction practice & implications to DeFi
- MEV mitigation ideas
- MEV mitigation on Ethereum
- Batch auction: an MEV-aware AMM design

1

MEV extraction practice & implications to DeFi

2

MEV mitigation ideas

3

MEV mitigation on Ethereum

4

Batch auction: an MEV-aware AMM design

MEV extraction practice & Implications to DeFi

Common types of MEV

Transactions “carry MEV” if they create profit opportunities for block producers.

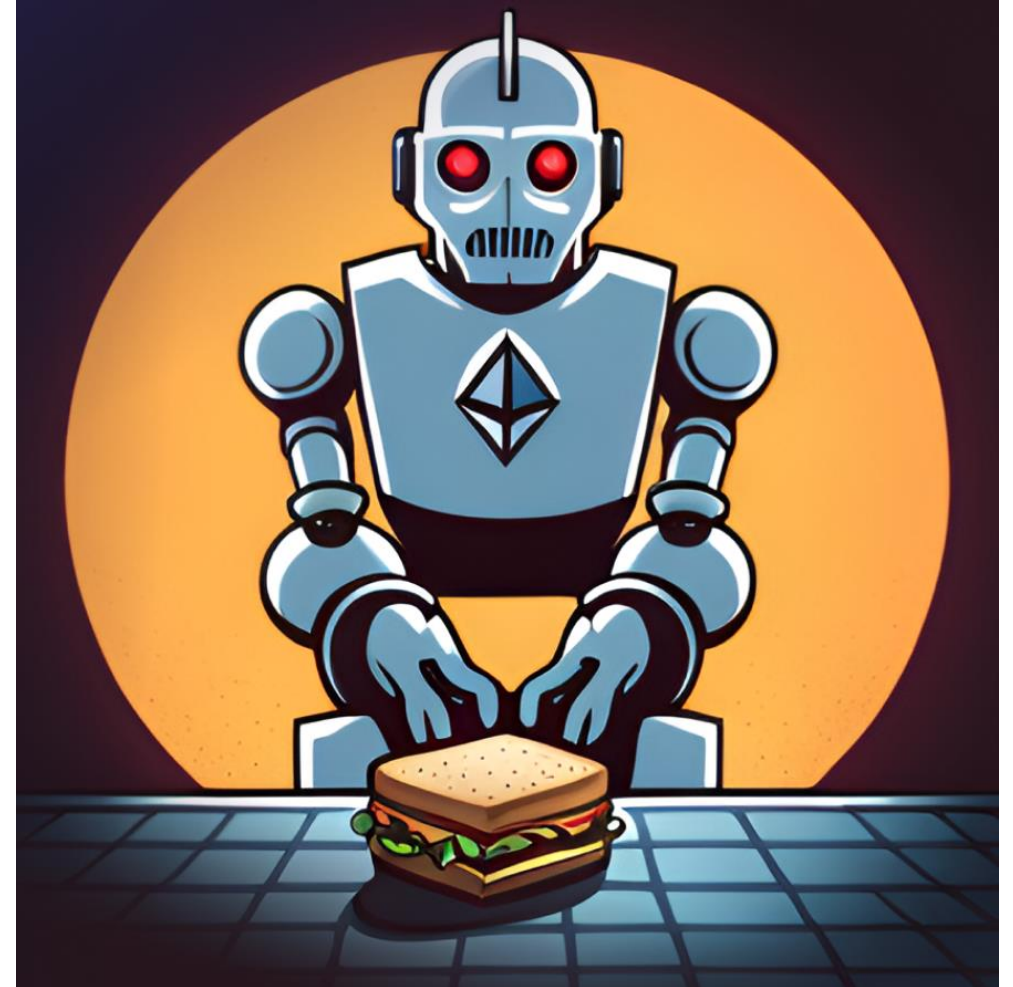
Say transaction T sells ETH on Uniswap, how to extract profit from order manipulation?

- Arbitrage (place TX_{arb} after T, **before** other arbitrageurs)
- Sandwich (place T_{sell} before T and T_{buy} after)
 - Note: losing money if order is wrong

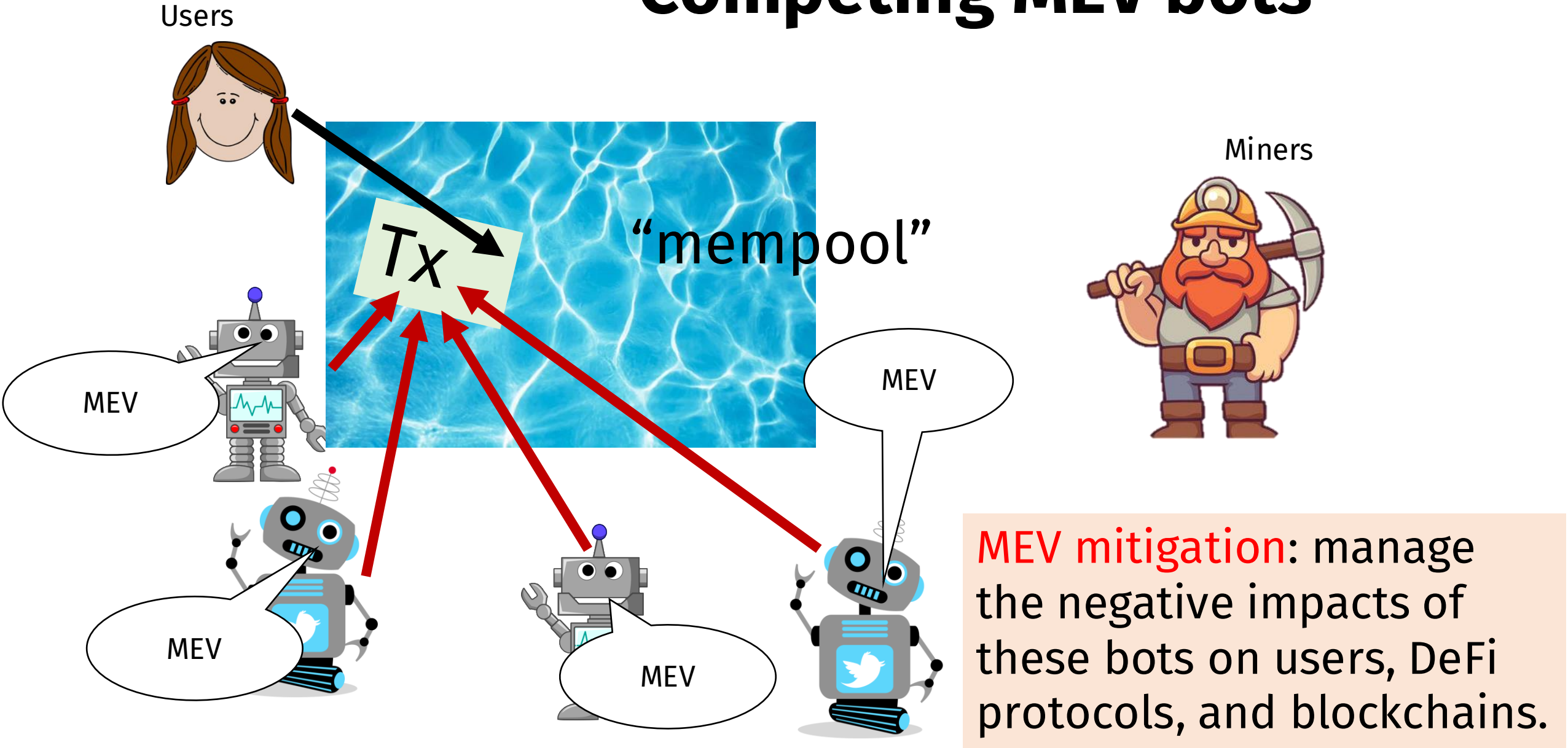
Question: is there MEV on Bitcoin blockchain?

Emergence of MEV Bots

- Anyone can attempt to capture these MEV opportunities
- Circa 2017, an ecosystem of **competing MEV bots** emerged.



Competing MEV bots



Implications of MEV

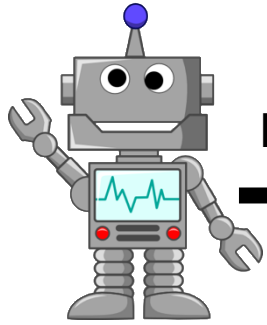
- **User loss:** some (but not all) MEV extraction harm users
 - Harmful or not: arbitrage v.s. sandwich
- **Introducing instability to consensus:** mev dominates fees
 - Essentially, a stream of validator profit that was not accounted for by consensus protocols.
- **Centralization force:** not all block producer benefit equally from MEV (will come back)
- **Leads to PGA that has its own problems (next)**

Prior 2020: priority gas auction (PGA)

- **Fact:** many block producers order txs in decreasing order of fees.
- Bots pay high gas fees to place txns at top-of-block



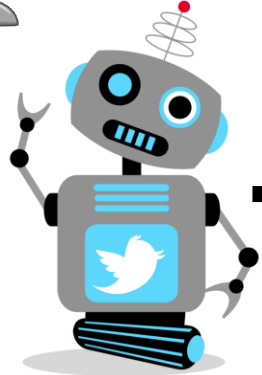
block producer



Please include **my TX** first



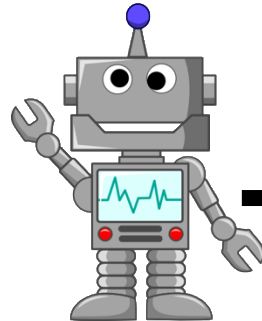
I pay **1** ETH in fee



Please include **my TX** first



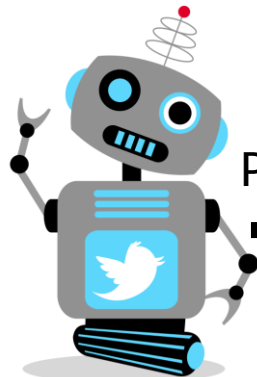
I pay **1.1** ETH in fee



Please include **my TX** first



I pay **1.2** ETH in fee



Please include **my TX** first



I pay **2** ETH in fee

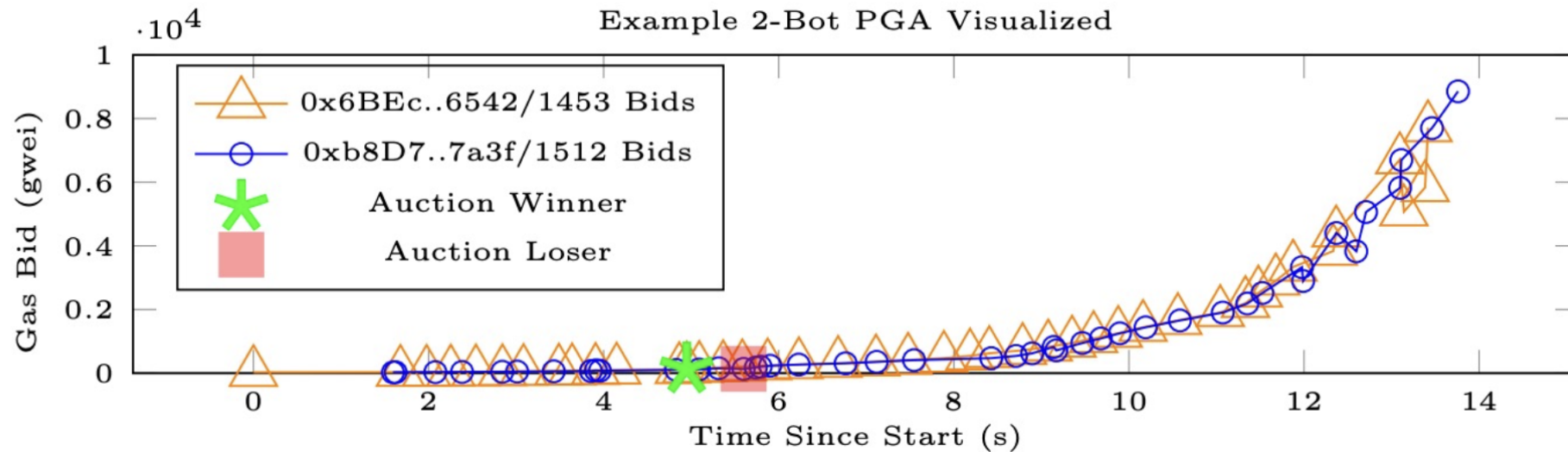
Priority gas auction:

- Item to buy: top-of-block inclusion
- Payment via gas fee
- One winner and possibly many losers



block producer

Prior 2020: priority gas auction (PGA)



- First studied by Flashboys 2.0 by Daian et al
- PGA competition → block producer gets most of the value
 - Also, block producer can always include its own tx

Issues with PGA

Waste block space on failed extraction (included but abort)

Inflexible for competing for MEV requires more than just “getting ahead of others” (e.g., sandwich)

- What might happen as a result?

1

MEV extraction practice &
implications to DeFi

2

MEV mitigation ideas

3

MEV mitigation on Ethereum

4

Batch auction: an MEV-aware
AMM design

MEV mitigation ideas

Two schools of thoughts on mitigation

- **MEV minimization:** Prevent MEV extraction
 - Encrypting mempool (recently deployed by Aptos, Monad, etc.)
 - Order by a committee (e.g., Fair Ordering Service by Chainlink)
 - Batch auctions with uniform prices (e.g., CoW Swap)
- **MEV maximization:** facilitate competition, minimize waste of block space, preserve decentralization.
- Ethereum as a platform takes the second approach.
- Some applications implement MEV minimization on top.

1

MEV extraction practice &
implications to DeFi

2

MEV mitigation ideas

3

MEV mitigation on Ethereum

4

Batch auction: an MEV-aware
AMM design

MEV mitigation on Ethereum

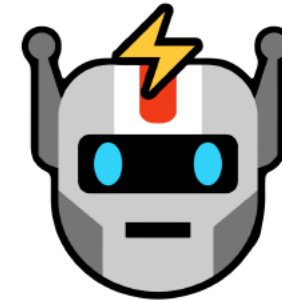
Flashbots v1 ($\approx$ 2021-2022)

#flashbots ~~t~~

- Leaving Cornell PhD program, Phil Daian co-founded **flashbots** to build a series of **MEV maximization** protocols for Ethereum.

PHILIP
DAIAN

Researcher
and PhD Student
Cornell Tech / IC3

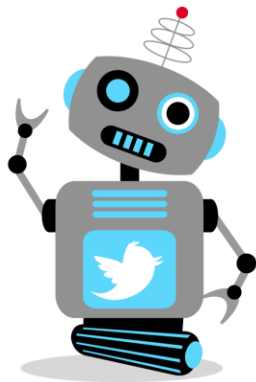
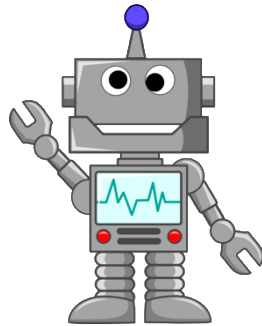


Flashbots v1 ($\approx$ 2021-2022)

#flashbots 

- Leaving Cornell PhD program, Phil Daian co-founded **flashbots** to build a series of MEV maximization protocols for Ethereum.
- **High-level ideas:** facilitate communication between block producer and bots (aka “searchers”) so that
 - Only winners are included on-chain (save block space)
 - Failed attempts are canceled for free (also save gas)
 - Bots can extract middle-of-block MEV
- **How?** Atomic inclusion of “bundles” (seq of txns)

Ideal work flow



$\text{Bundle} = (T_{\text{buy}}, T, T_{\text{sell+pay}})$

$\text{Bundle}' = (T'_{\text{buy}}, T, T'_{\text{sell+pay}})$

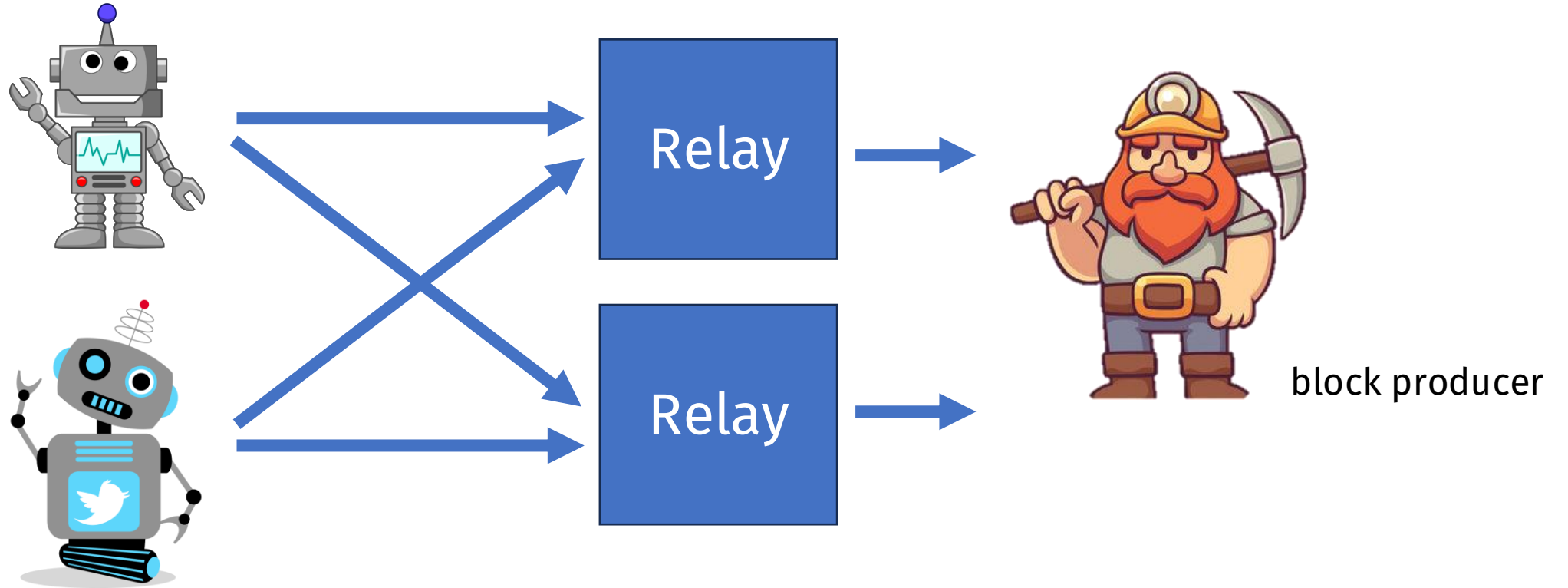


block producer

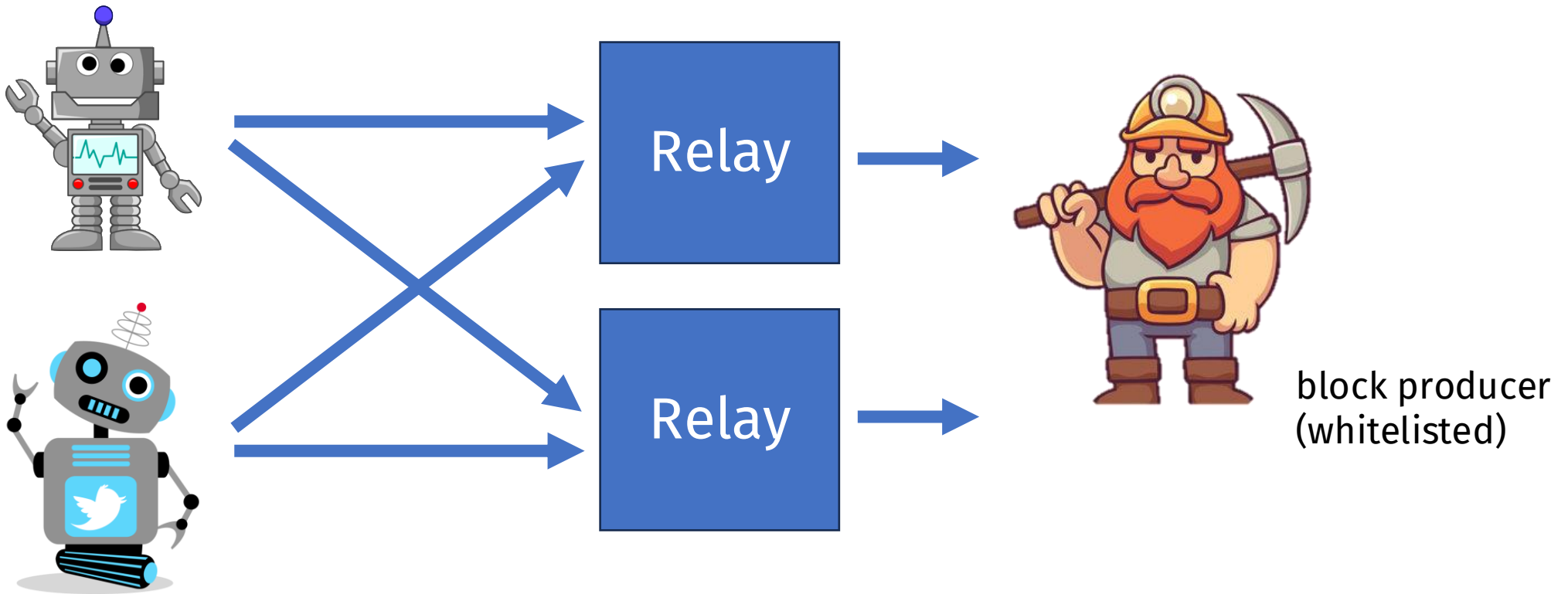
Problem: What if block producer steals MEV?

- Ideally, bundles sent to block producers directly (off-chain)
- Block producer incentivized to include at most one bundle corresponding to a given MEV opportunity (others would fail)

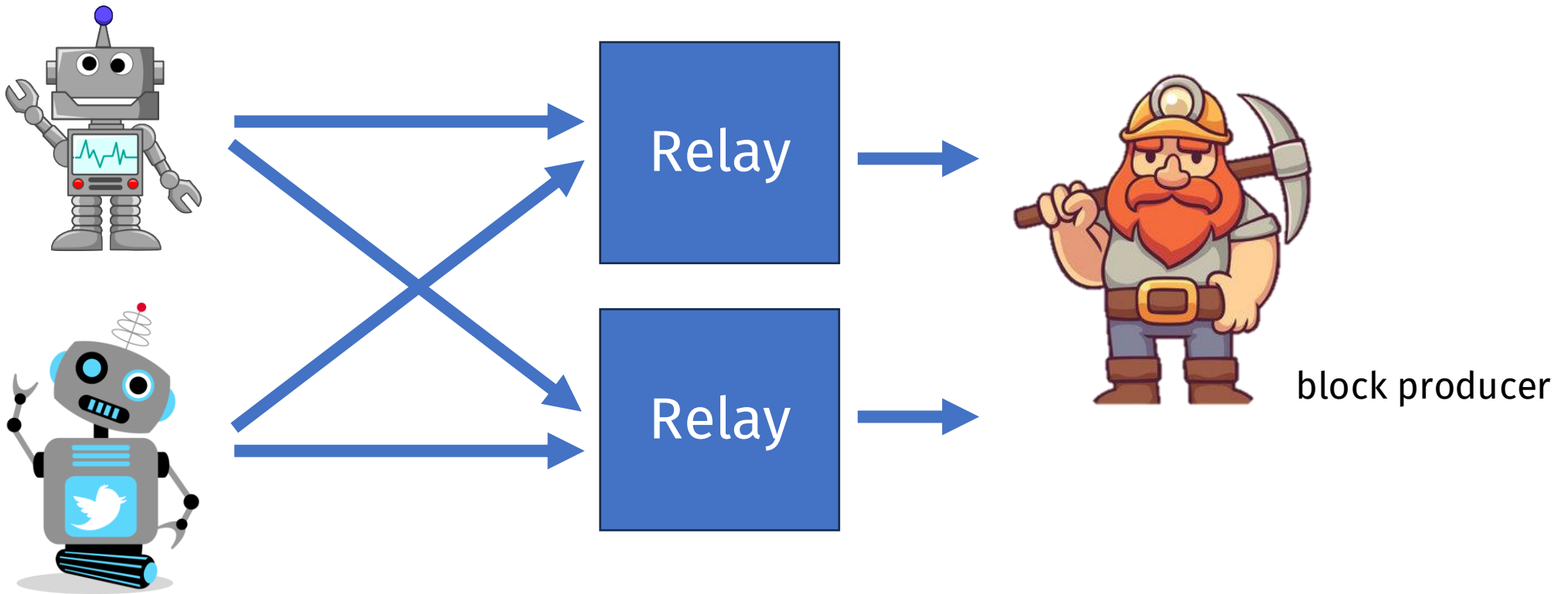
Idea (Relay)



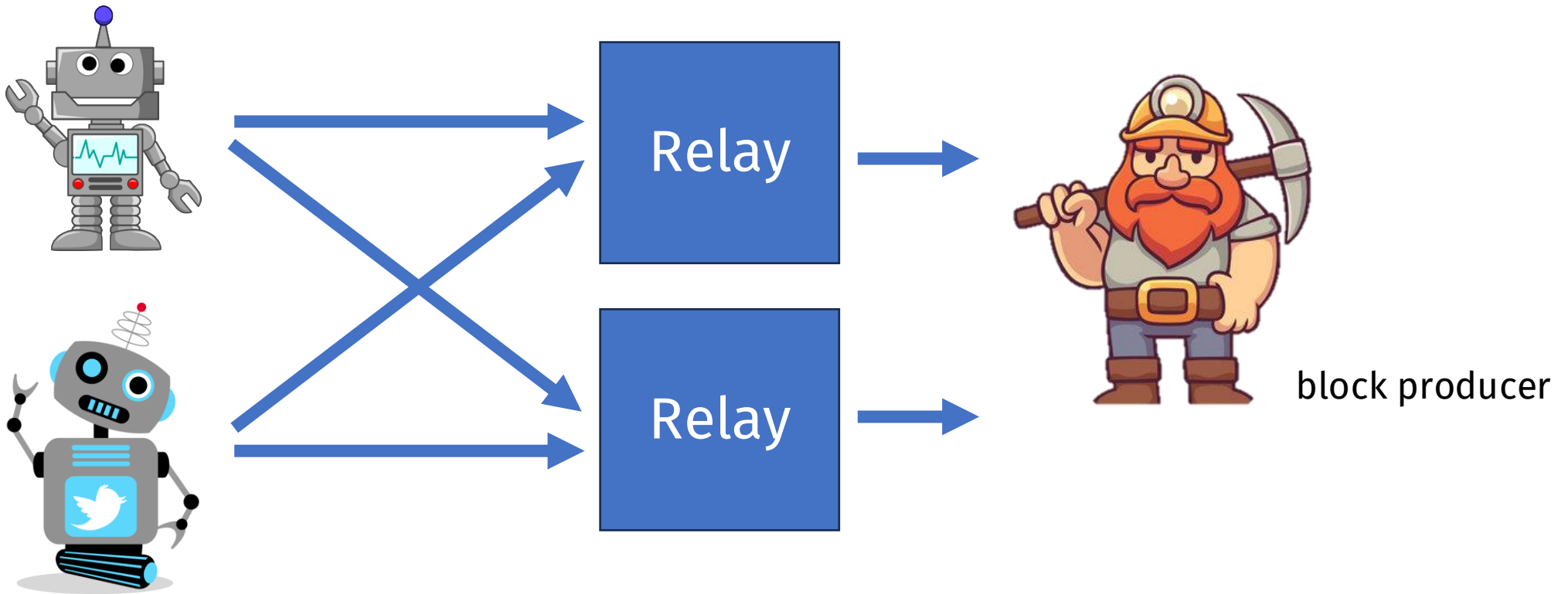
- **Relay nodes:** trusted servers that act as intermediaries between searchers and block producers. (run by Flashbots, bloXroute, etc.)



- 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



- **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
 - Same as PGA but now also supports “middle-of-block MEV”
 - clever searchers may be able to retain most of “**long-tail MEV**”



- **Good news:** design addresses inefficiencies of PGAs.
- **Limitations:**
 - Trusted relay (addressed much later, actually, only very recently)
 - Reliance on reputation (addressed in v2 + PoS)

MEV-Boost (flashbots v2)

MEV and Centralization

- **Permissionless consensus:** “anyone” can participate.
- **Refined goal:** all earn equal rewards per unit invested.
- True for Bitcoin: each hash equally likely to win block reward
- Question: is this goal still possible with MEV?

MEV and Centralization

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 $\geq 51\%$ of hashrate or $\geq 34\%$ of stake.

- long-run dynamics → validator set eventually centralizes

MEV and Centralization

Worry #1: heterogeneity in validator rewards → centralization

Worry #2: “professional” validators will be much better at capitalizing on MEV opportunities than “hobbyist” 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

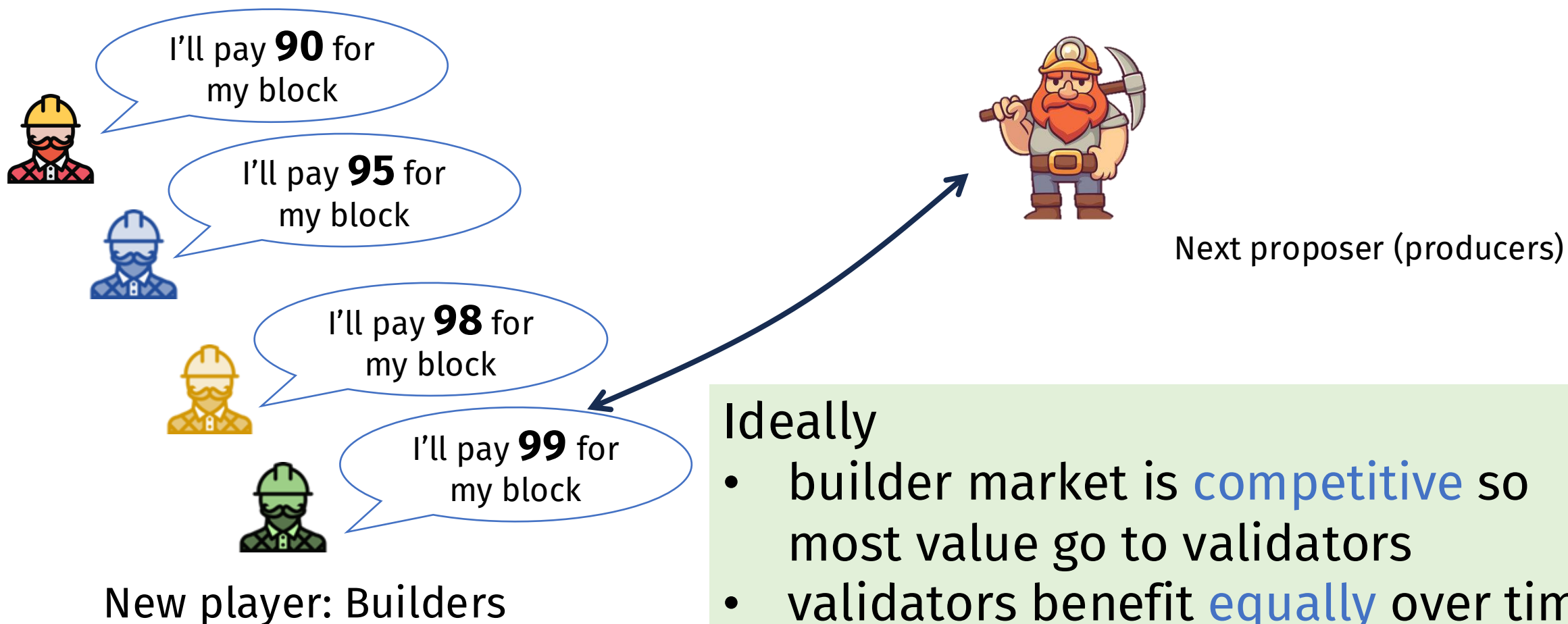
[Learn](#)[Use](#)[Build](#)[Participate](#)[Research](#)

PBS and MEV

Maximum extractable value (MEV) refers to validators maximizing their profitability by favorably ordering transactions. Common examples include arbitraging swaps on decentralized exchanges (e.g. frontrunning a large sale or purchase) or identifying opportunities to liquidate DeFi positions. Maximizing MEV requires sophisticated technical know-how and custom software appended to normal validators, making it much more likely that institutional operators outperform individuals and hobbyist validators at MEV extraction. This means staking returns are likely to be higher with centralized operators, creating a centralizing force that disincentivizes home staking.

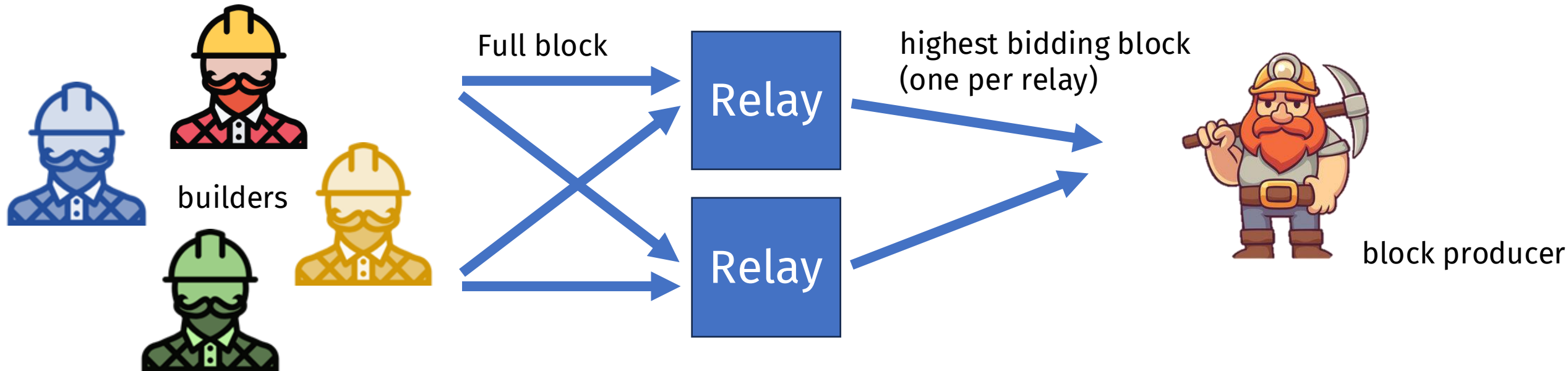
Proposer-builder-separation (PBS)

- Idea: allow outsourcing of block building (i.e., MEV extraction) to builder market.



MEV Boost ($\approx$ Flashbots v2)

- **MEV-Boost**: out-of-protocol implementation of PBS.
- released by Flashbots at same time as “the Merge” (August 2022), i.e., when Ethereum switches to Proof of Stake.



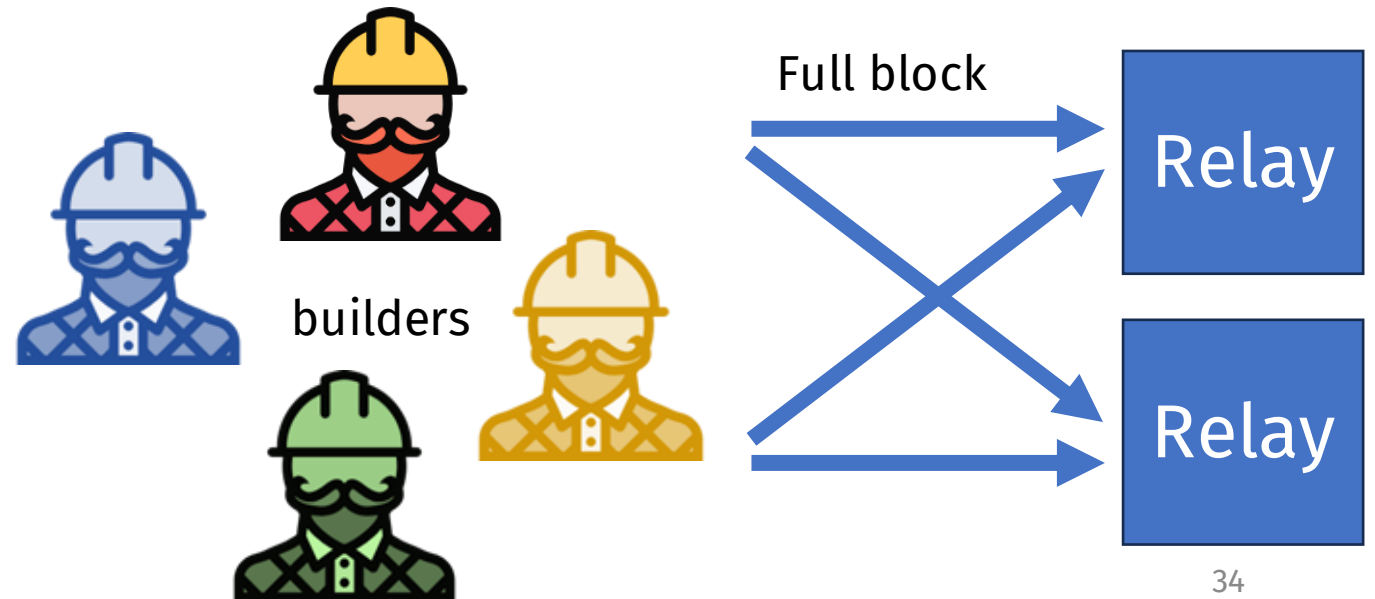
Just enough to know about Proof of Stake

- To address issues of proof of work (e.g., energy consumption)
- Idea: one lottery per → one lottery per coin
- Miners now called **validators**. To become a validator in Ethereum, one deposits stake (e.g., at least 32 ETH)
 - Fractional stake possible via stacking pool
 - Elected as leader with probability proportional to stake
- **Slashing**: take away one's stake if they take malicious actions
 - penalty depends on the offense
 - E.g., proposing two blocks at the same slot leads to significant stake loss and forced exit

MEV Boost (≈ Flashbots v2)

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

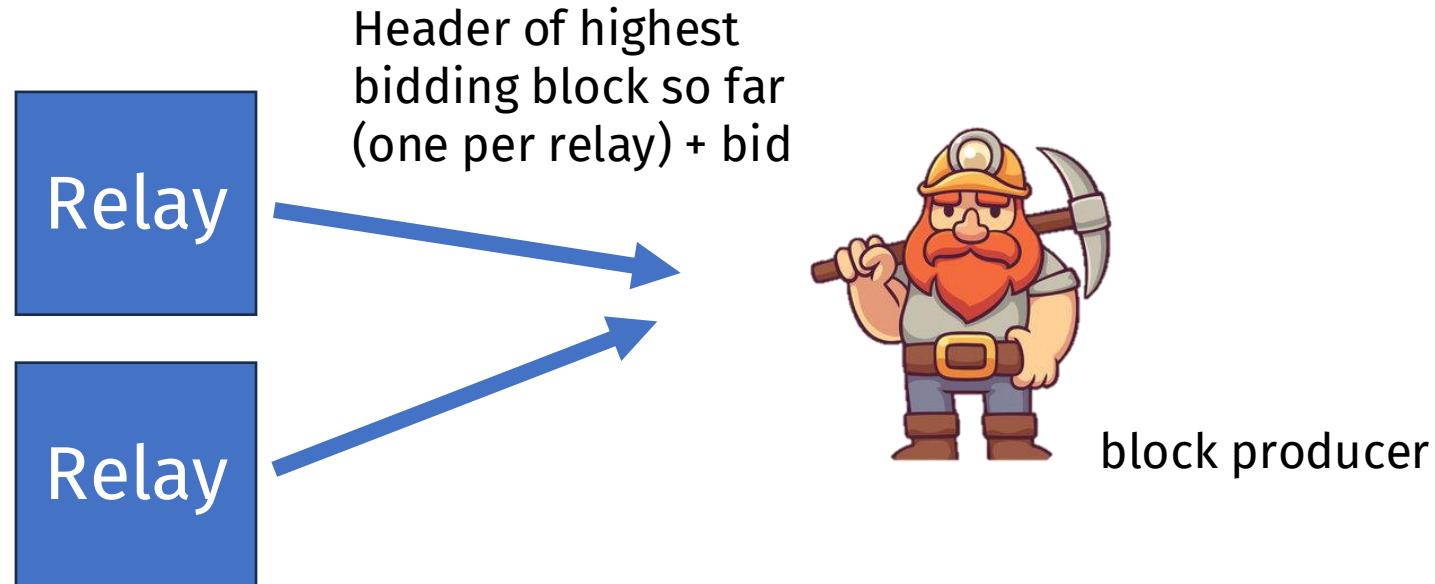
- builders submit **blocks** to relay nodes along with **bids** (paid to proposer if selected)
- relay nodes check block validity



MEV Boost (≈ Flashbots v2)

Relay nodes (cont)

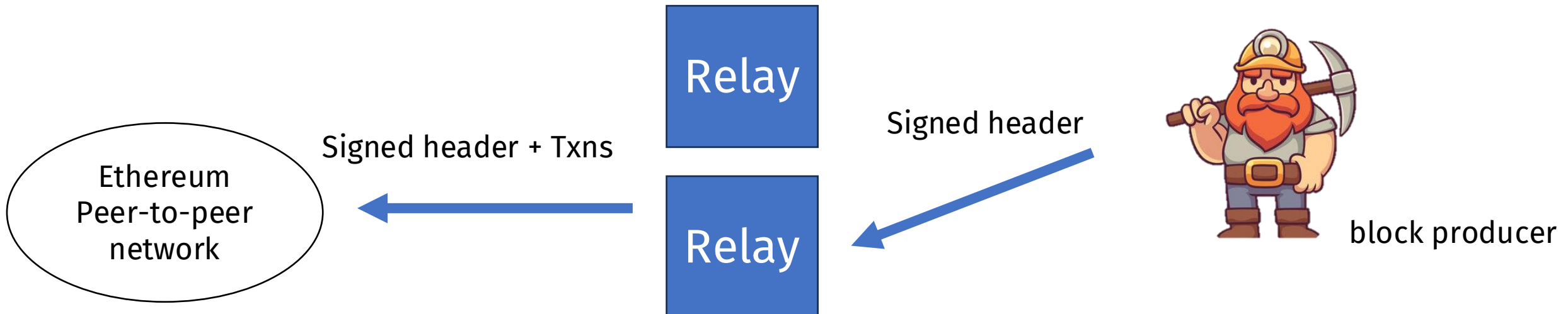
- relay nodes forward **header (only)** of block with **highest bid** to the current block proposer (known in advance in proof-of-stake)



MEV Boost ($\approx$ Flashbots v2)

Relay nodes (cont)

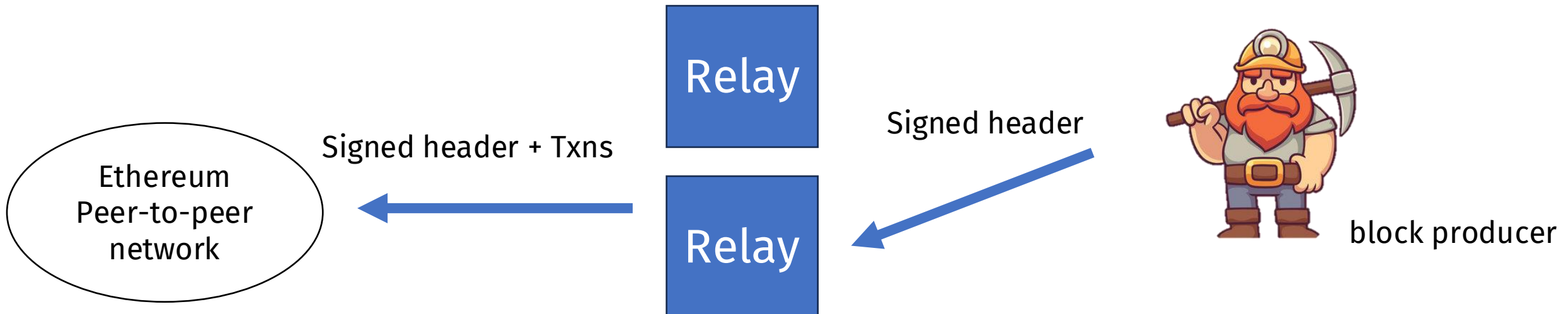
- proposer signs block header, returns it to relay node
- Relay assembles a full block (header + txs) and broadcast
- **Purpose:** prevent block producer from stealing MEV.



MEV Boost (≈ Flashbots v2)

The point: Replay prevents stealing of MEV

- **Fact:** signing two different block is slashable in proof of stake
- Knowing that relay's block will be accepted, block producer is disincentivized to sign another block (to steal MEV).



The Peraire-Bueno case



BUSINESS INSIDER

Zacharia Out · Tesla Roadster Fine Print · Inflation · The AI Data Grab · Books Insider **NEW** · The Long Play **NEW** · Wa

CRYPTOCURRENCY

Jury says it's 'struggling' to reach a verdict for MIT-educated brothers accused of pulling off a \$25 million crypto heist in 12 seconds

- They ran their own proposer
- They exploited a bug in a Flashbots relay and made it reveal the block's transactions after receiving an invalid signed header
- They didn't just steal MEV; they baited sandwich bots into the trap
- Gained ~\$25M, taken from the MEV searchers running the sandwich bots
- Retrial possible late 2026 or 2027

MEV Boost ($\approx$ Flashbots v2)

- Look at live data at <https://bids.pics/>
- Statistics at <https://mevboost.pics>

MEV supply chain

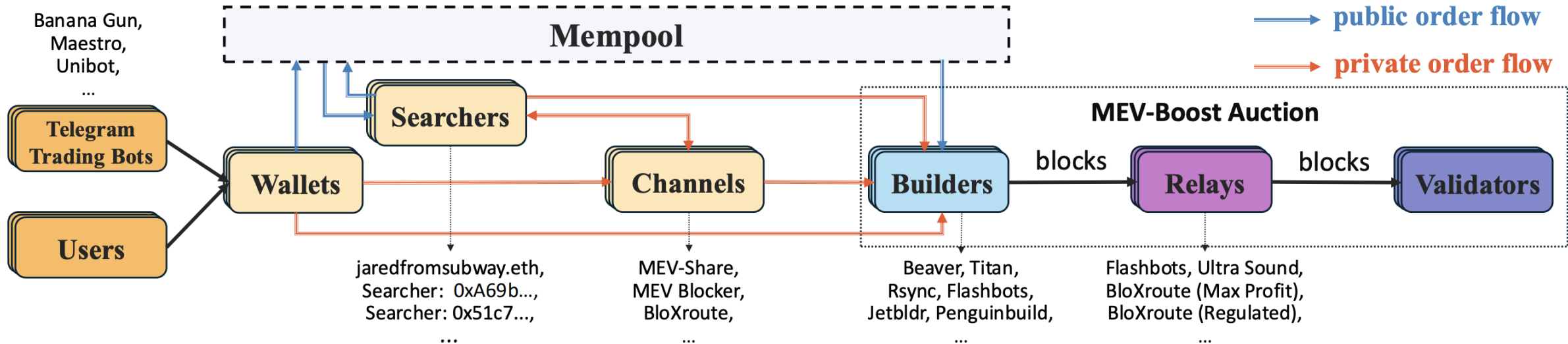


Figure 3: Illustration of the MEV supply chain in the PBS scheme.

PBS only governs **block/proposer operations**, not **searcher/builder**.

Open issues: Trusted Relays

Relay nodes: trusted servers that act as intermediaries.

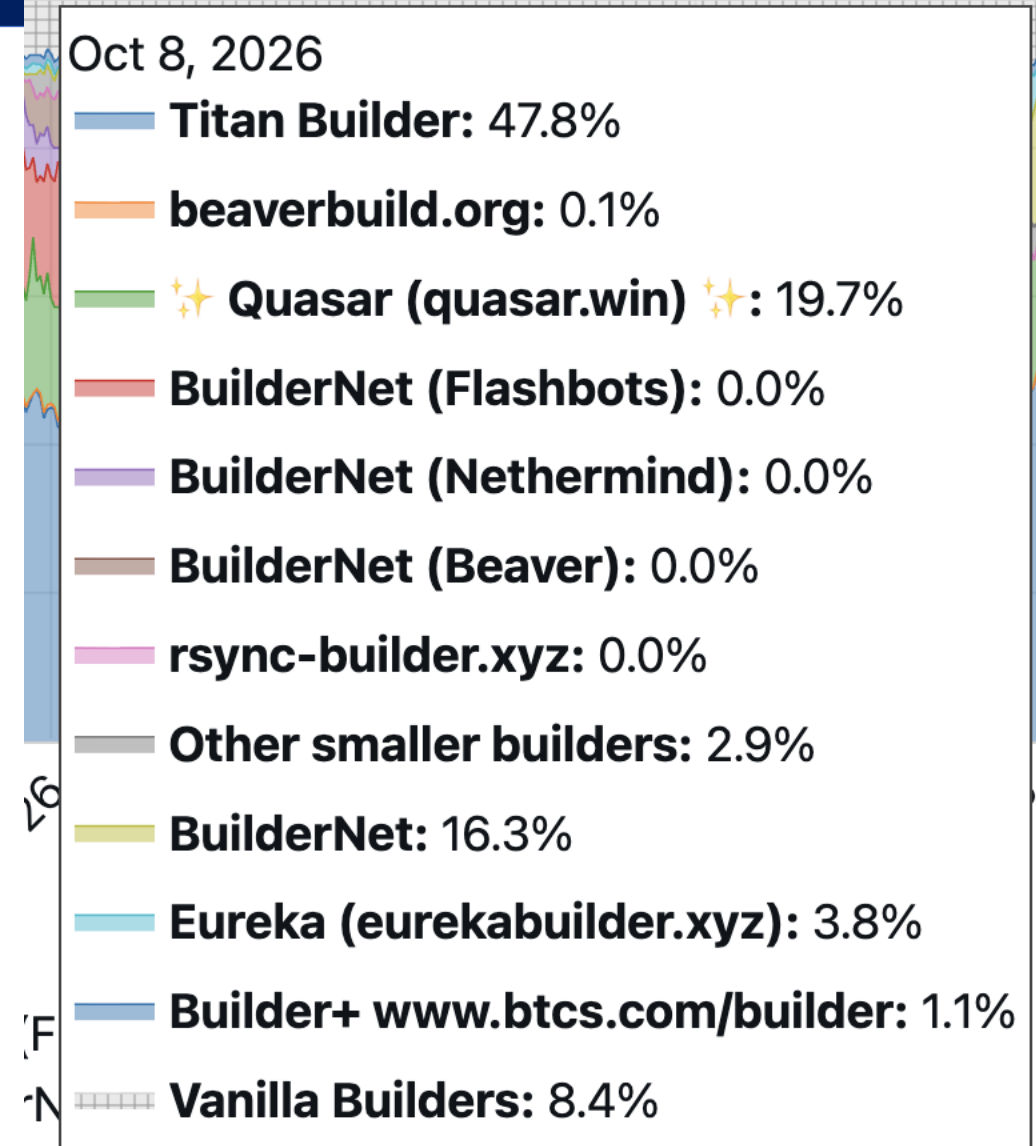
- between searchers and validators in v1, builders and validators in v2

Future Ethereum protocol will have “**enshrined**” relay

- **ePBS** (EIP-7732): protocol runs the builder–proposer exchange
 - Proposer includes the winning builder’s signed bid in its block
 - Builder then reveals the block; a committee checks it was on time
 - Payment enforced on-chain, so neither side needs to trust a relay
- Status: scheduled for the Glamsterdam fork; testnet Oct 2026

Builder Centralization

- Top 3 builders build 83.8% of blocks [as if Oct 2026]
- Not a lot of decentralization!



Builder Centralization

- **Question:** is it big problem if a blockchain protocol has only a few **validators (miners)**?
 - Answer: **yes**, largely defeats the point of a blockchain protocol
- **Question:** big problem if only a few **block builders** (but lots of validators)?
 - Might be inevitable: block-building might be an intrinsically specialized skill
- One issue: **censorship**, i.e., systematic exclusion of certain txs
 - e.g., for financial or legal/regulatory reasons
 - We will come back to this in future lectures.
- Other issues: reduced competition (see our paper in SP'2025).

1

MEV extraction practice &
implications to DeFi

2

MEV mitigation ideas

3

MEV mitigation on Ethereum

4

**Batch auction: an MEV-aware
AMM design**

Batch auction: an MEV-aware AMM design

THE QUARTERLY JOURNAL OF ECONOMICS

Vol. 130

November 2015

Issue 4

THE HIGH-FREQUENCY TRADING ARMS RACE: FREQUENT
BATCH AUCTIONS AS A MARKET DESIGN RESPONSE*

ERIC BUDISH
PETER CRAMTON
JOHN SHIM

The high-frequency trading arms race is a symptom of flawed market design. Instead of the continuous limit order book market design that is currently predominant, we argue that financial exchanges should use frequent batch

Batch auctions in practice

CoW Protocol (CoW Swap)

Ethereum, Gnosis Chain, Arbitrum, Base, ...

- **Origin:** Gnosis Protocol (2020) → CoW Swap (Apr 2021) → CoW DAO spin-off (Mar 2022)
- **How:** users sign off-chain **intents**; **solvers** bid to settle each batch and pay the gas
- **Matching:** **Coincidence of Wants** first, AMMs for the rest
- **Scale:** >\$80B cumulative volume by mid-2026
- **Caveat:** ~28 solvers, but the top 3 settle >50% of volume (early 2025)

Penumbra

Cosmos-based privacy chain (Penumbra Labs)

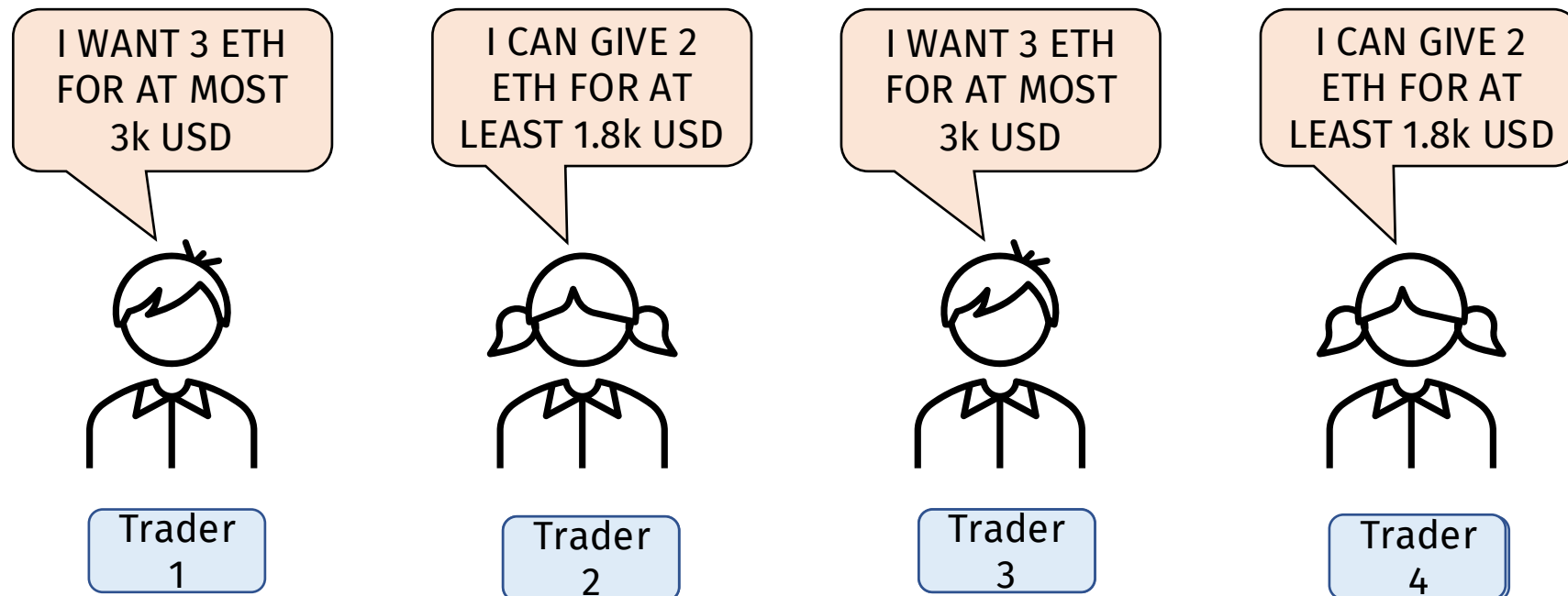
- **Origin:** mainnet launched 2024
- **How:** all swaps in a block are batched and cleared at one **uniform price** per pair
- **Privacy:** **sealed** (encrypted) orders; only batch totals are revealed
- **Why it matters:** MEV resistance enforced by the chain itself, not by one app

Both apply the *frequent batch auction* idea of Budish, Cramton & Shim (QJE 2015). Other intent DEXs (UniswapX, 1inch Fusion) use Dutch auctions instead.

Batching trades

- Collect all trades within a block into a batch
- Compute a uniform **clearing price**
- All trades executed at the same price

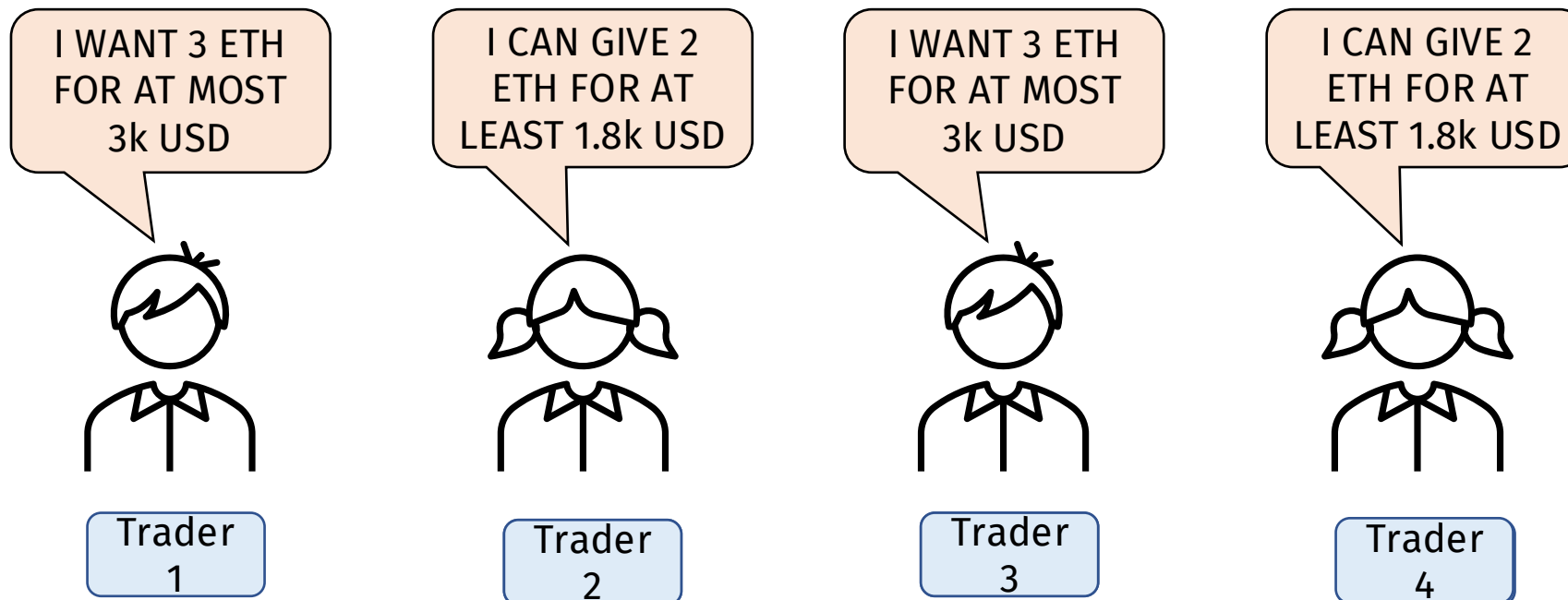
Enforcing this gets rid of
frontrunning and arbitrage
opportunities



Batching trades

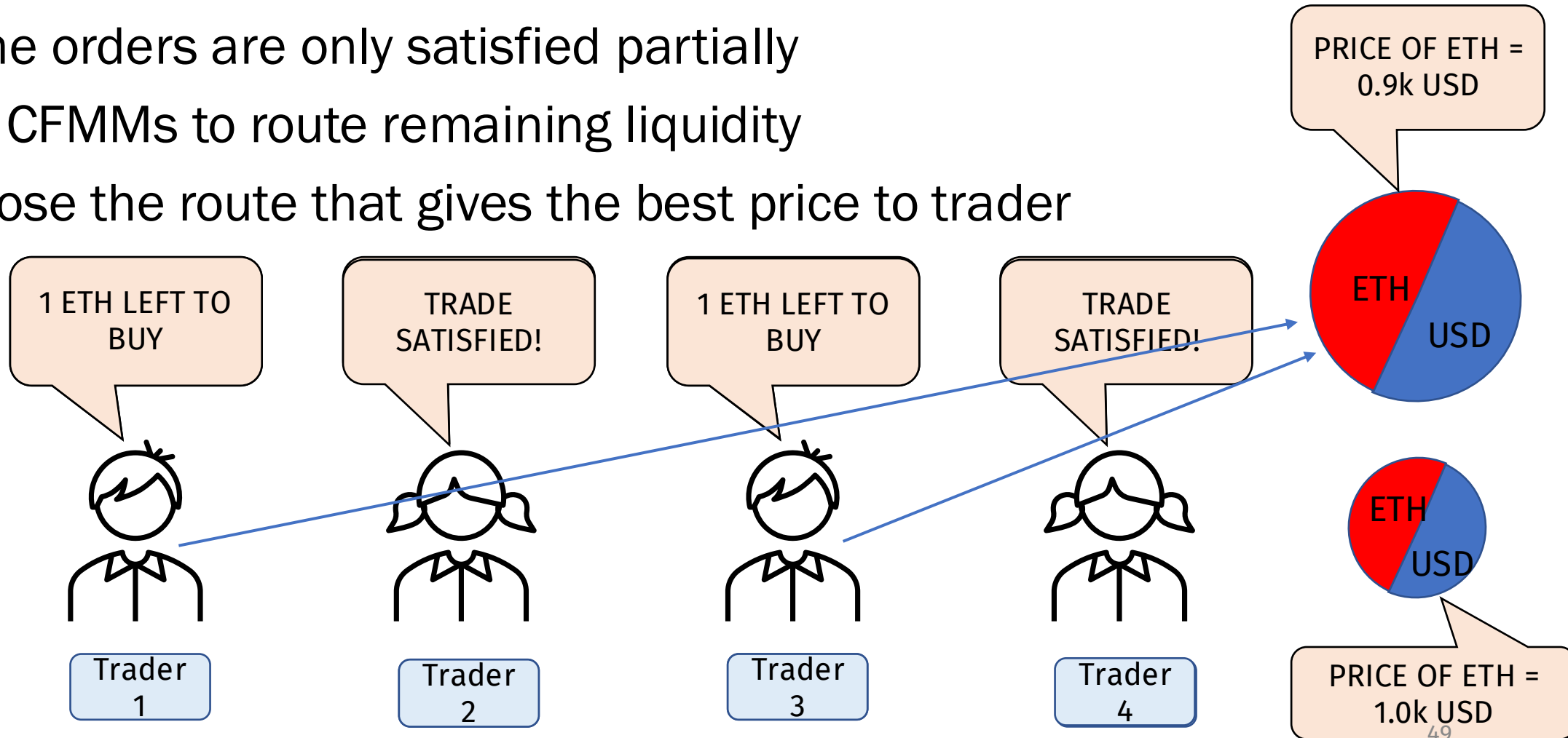
- What would be a fair clearing price be in this case?
- Buyers not willing to go above 1k USD/ETH
- Sellers not willing to go below 0.9k USD/ETH

} Clearing price = 0.95k



Batching trades

- Some orders are only satisfied partially
- Use CFMMs to route remaining liquidity
- Choose the route that gives the best price to trader



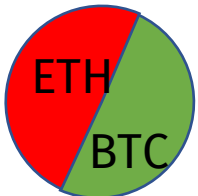
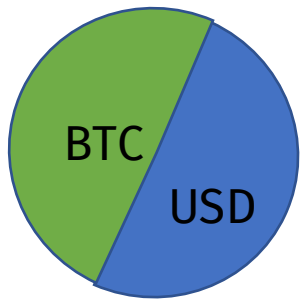
Batching trades: the general case

- Trades between different pairs of tokens
- Batch and compute a **clearing price**
- **Trades with the same pair** should be executed at the same price

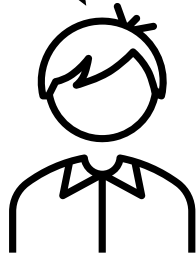
Gets rid of
frontrunning and
multi-hop arbitrage
opportunities

Computing such clearing
prices is NP-hard in general

Can use approximations

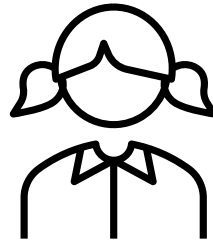


BUY 3 ETH FOR
AT MOST 3k
USD



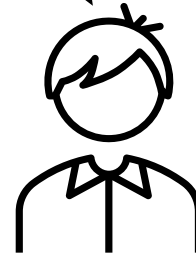
Trader
1

BUY 1 BTC FOR
AT MOST 15
ETH



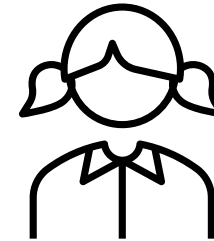
Trader
2

SELL 12 ETH
FOR AT LEAST
11k USD

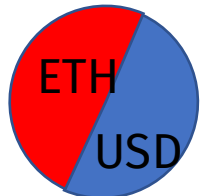
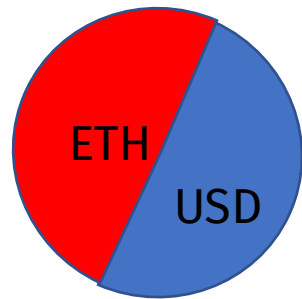


Trader
3

SELL 2 ETH
FOR AT LEAST
1.8k USD



Trader
4



Recap: MEV

1 MEV extraction practice & implications to DeFi

Block producers can profit from transaction ordering, for example through arbitrage, sandwiches and liquidations. Sandwiches cost users directly, and bots competing in priority gas auctions waste block space and destabilize consensus.

2 MEV mitigation ideas

Either minimize MEV (encrypted mempools, fair ordering, batch auctions) or accept it and organize the competition to minimize wasted block space and preserve decentralization.

3 MEV mitigation on Ethereum

Ethereum chose to organize it. Flashbots, then MEV-Boost, separate builders from proposers, so small validators can earn MEV comparable to large ones. Two problems remain open: removing the trusted relay and the concentration of block building in a few builders.

4 Batch auction: an MEV-aware AMM design

Batch auctions minimize MEV at the application level, inside the AMM rather than in the consensus protocol. Trades in a batch clear at one uniform price, so their order inside the batch can't be exploited. CoW Swap runs this on Ethereum today.