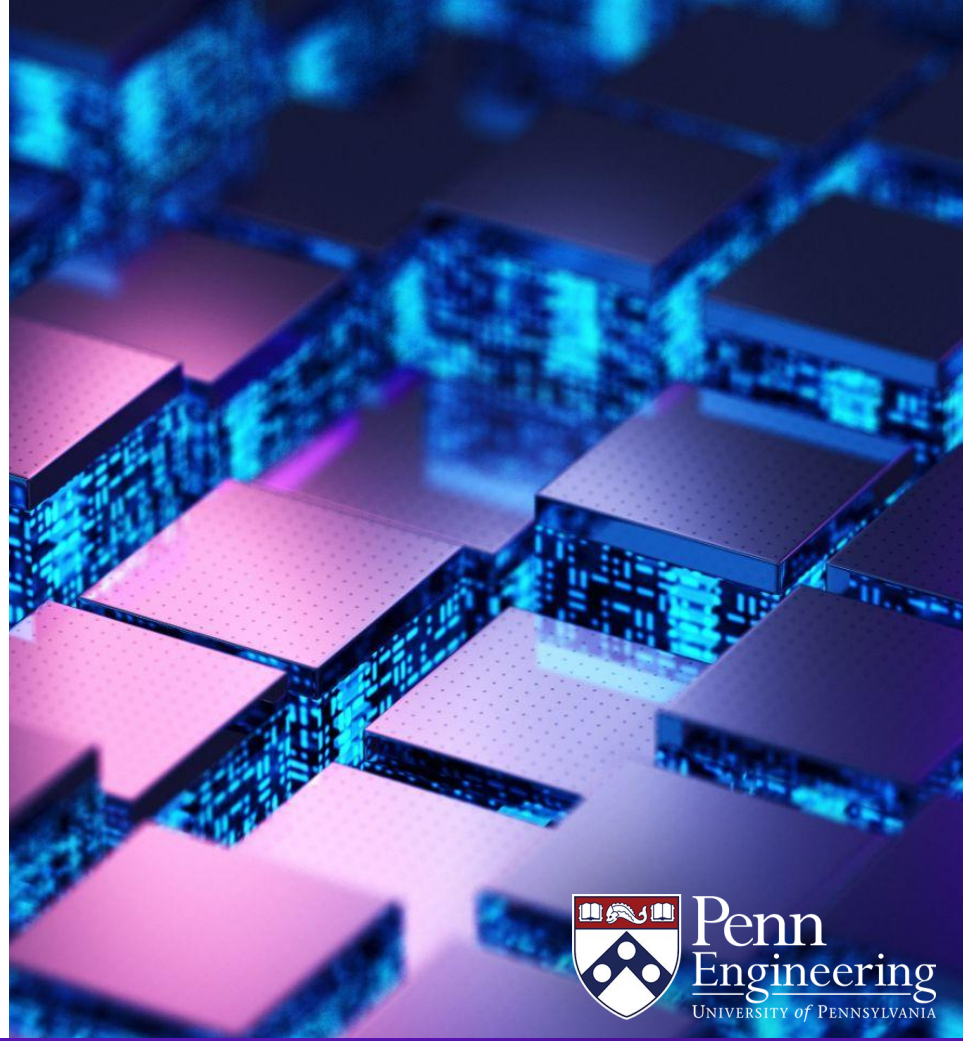
EAS 5830: BLOCKCHAINS

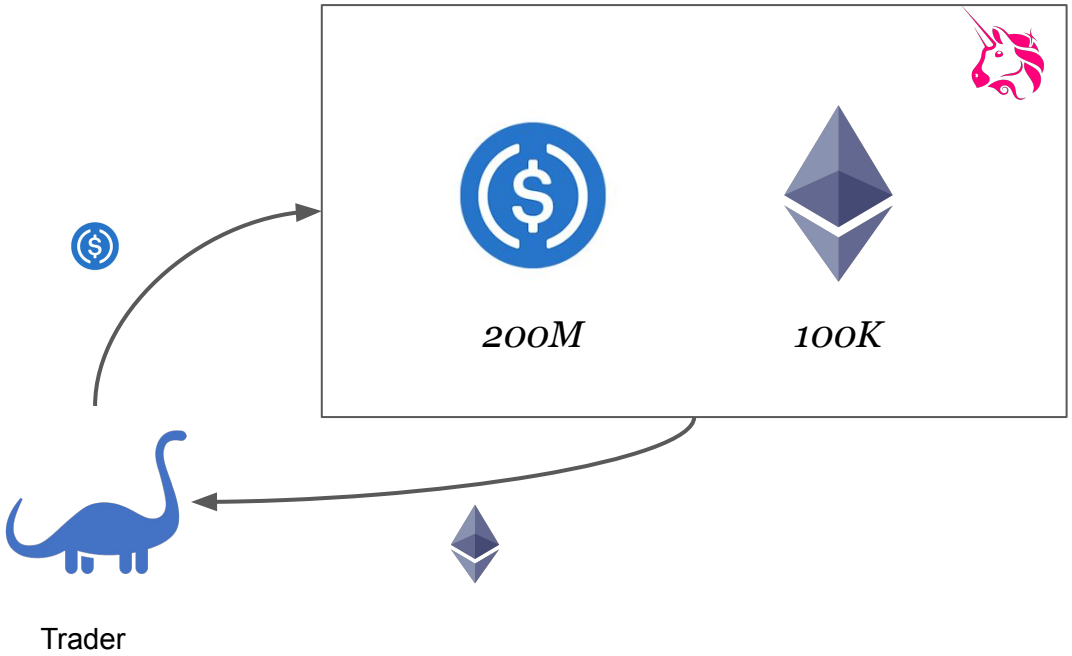
MEV

Professor Brett Hemenway Falk

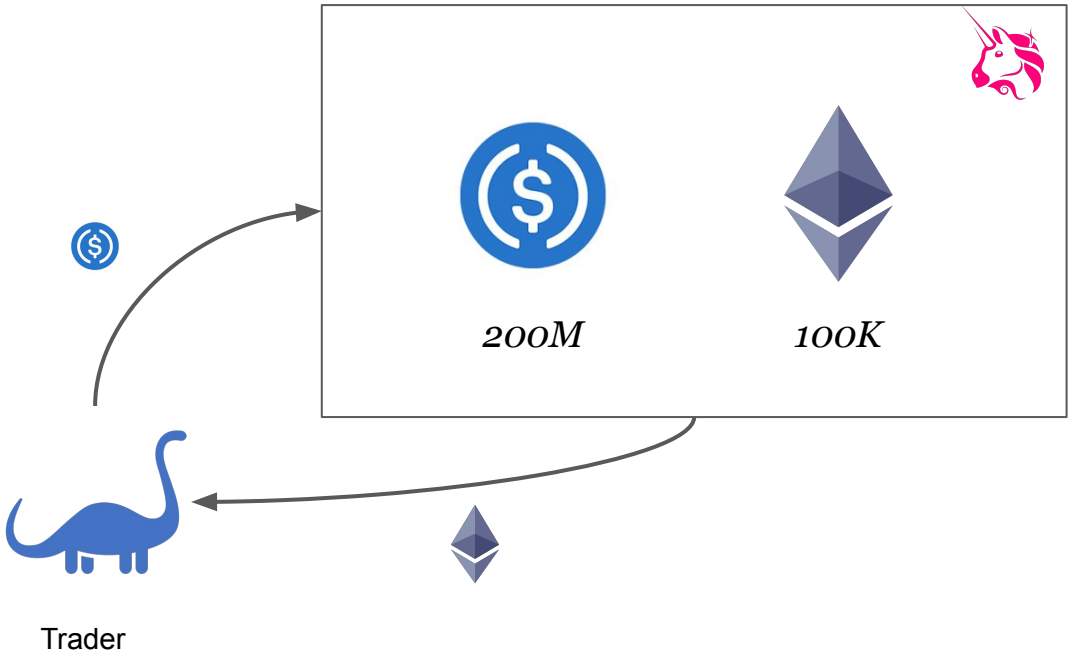


MEV is the value that can be extracted by re-ordering, inserting or removing transactions

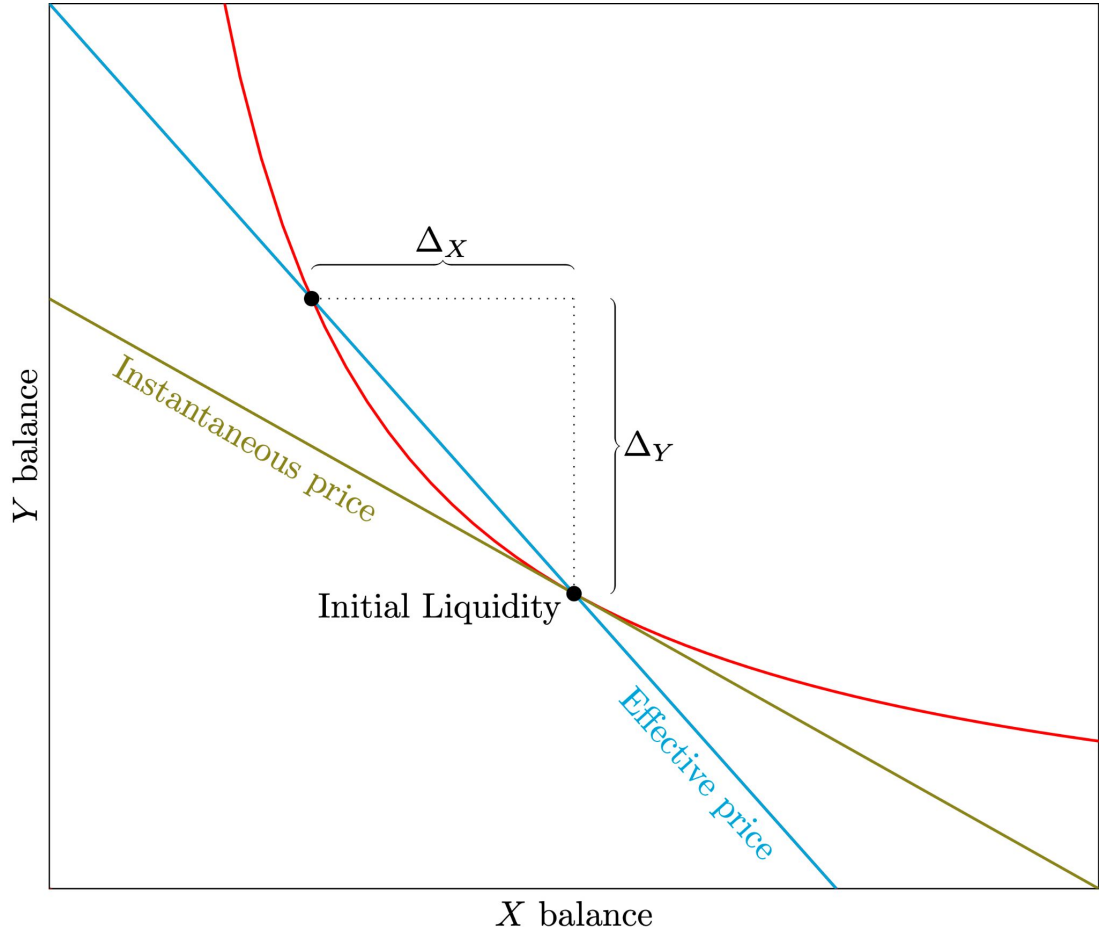
Arbitrage



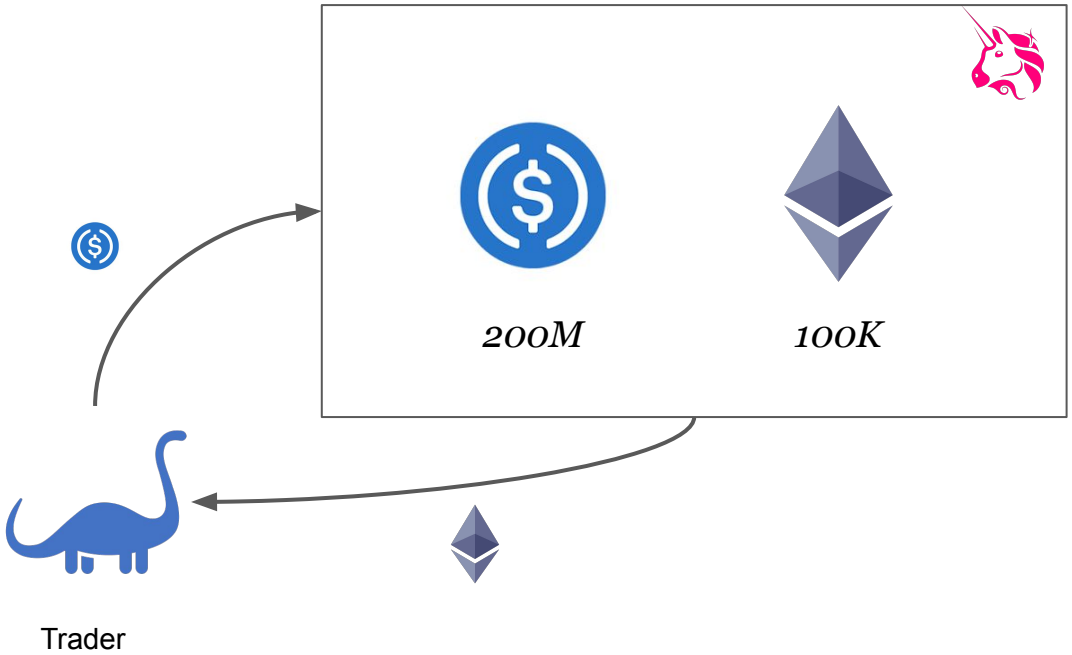
Arbitrage



ETH trading at $2,255


Δ_X
Δ_Y
Instantaneous price
Initial Liquidity
Effective price
Y balance
X balance

Arbitrage



ETH trading at $2,255

Common Sources of MEV

- **Liquidations (necessary)**
  - When a loan become under-collateralized, the collateral is liquidated. It's sold at a discount to the first buyer
- **Arbitrage (necessary)**
  - Every time someone trades on an AMM like Uniswap, their trade pushes the price. The first trader to "arb" the price back makes a profit
  - Every time the price changes on an off-chain exchange (e.g. Binance) there is an arbitrage opportunity
- **Exploiting Slippage (toxic)**
  - Every time someone trades on an AMM like Uniswap, they set a "slippage" parameter. Suppose trader buys ETH for USDC. Attacker buys ETH first (pushing the price up). Then sells ETH after the trade (at a higher price)

Categories of MEV

- **Front-running**
  - Being first to arbitrage AMM to price of off-chain exchange
- **Back-running**
  - Being the first to exploit an opportunity after an on-chain trade (on-chain trade moves AMM pool away from “true” price)
  - Being first to capture liquidation (after a price-oracle update)
- **Sandwiching**
  - Trading before and after an AMM trader to exploit their slippage parameter

Ethereum is a Dark Forest

Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges

Philip Daian
Cornell Tech
phil@cs.cornell.edu

Steven Goldfeder
Cornell Tech
goldfeder@cornell.edu

Tyler Kell
Cornell Tech
sk3259@cornell.edu

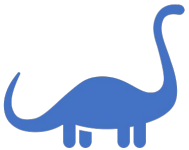
Yunqi Li
UIUC
yunqil3@illinois.edu

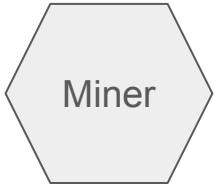
Xueyuan Zhao
CMU
xyzhao@cmu.edu

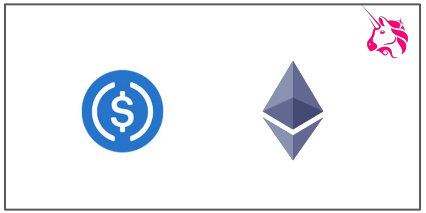
Iddo Bentov
Cornell Tech
ib327@cornell.edu

Lorenz Breidenbach
ETH Zürich
lorenz.breidenbach@inf.ethz.ch

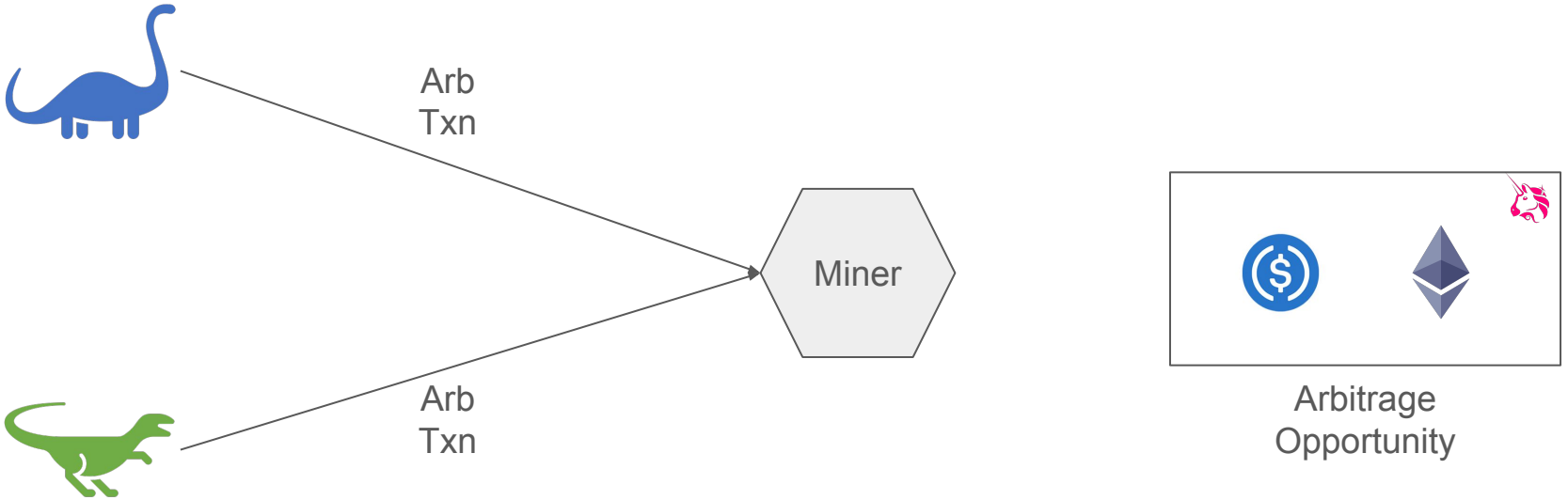
Ari Juels
Cornell Tech
juels@cornell.edu

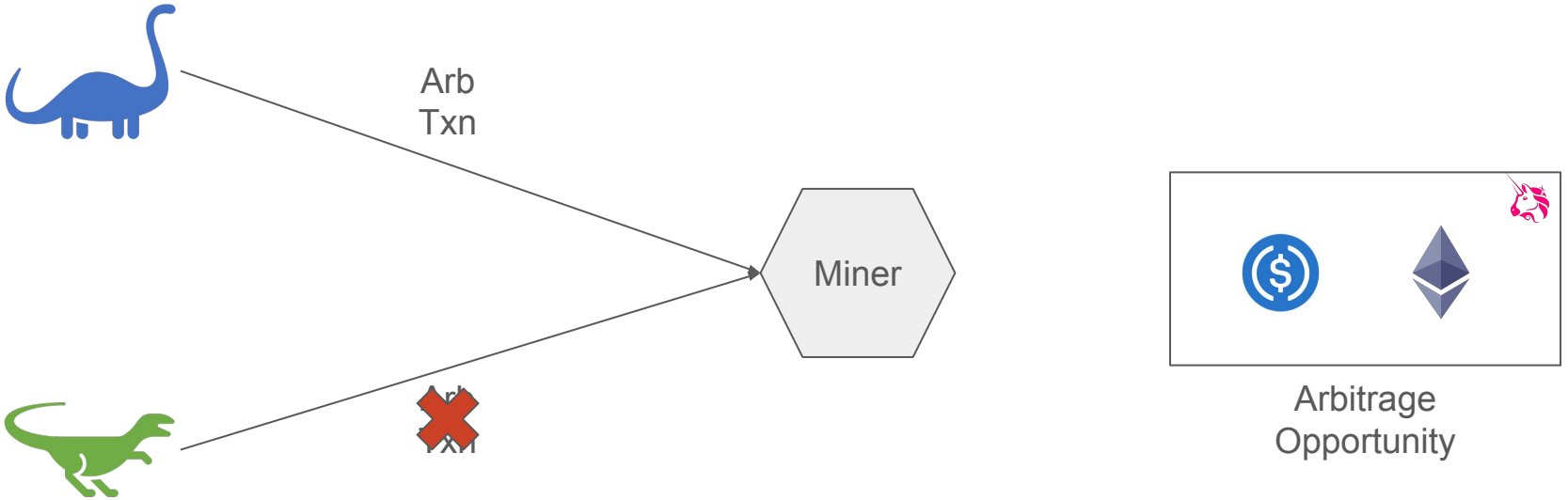


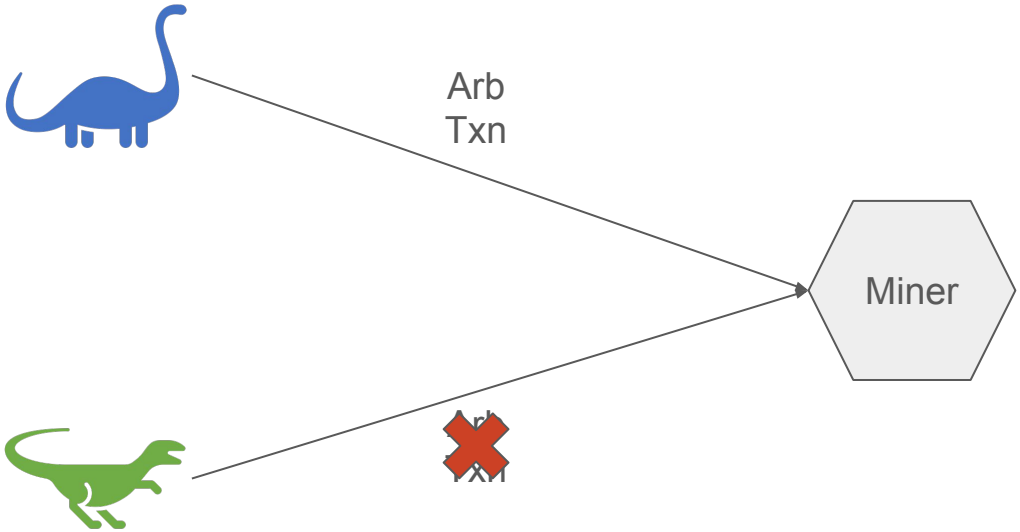


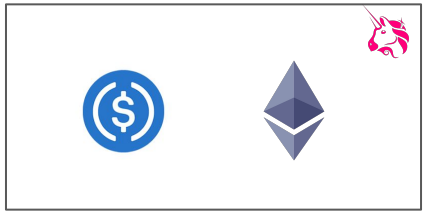


Arbitrage
Opportunity


Arb
Txn
Miner
Arb
Txn
Arbitrage
Opportunity

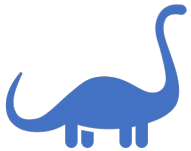

Arb
Txn
Miner
Arbitrage
Opportunity





Arbitrage
Opportunity

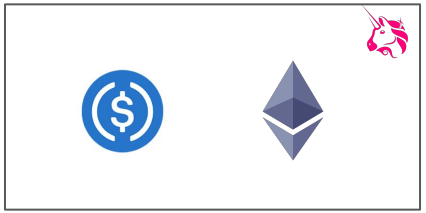
Both transactions can still be included, and both users pay gas fees



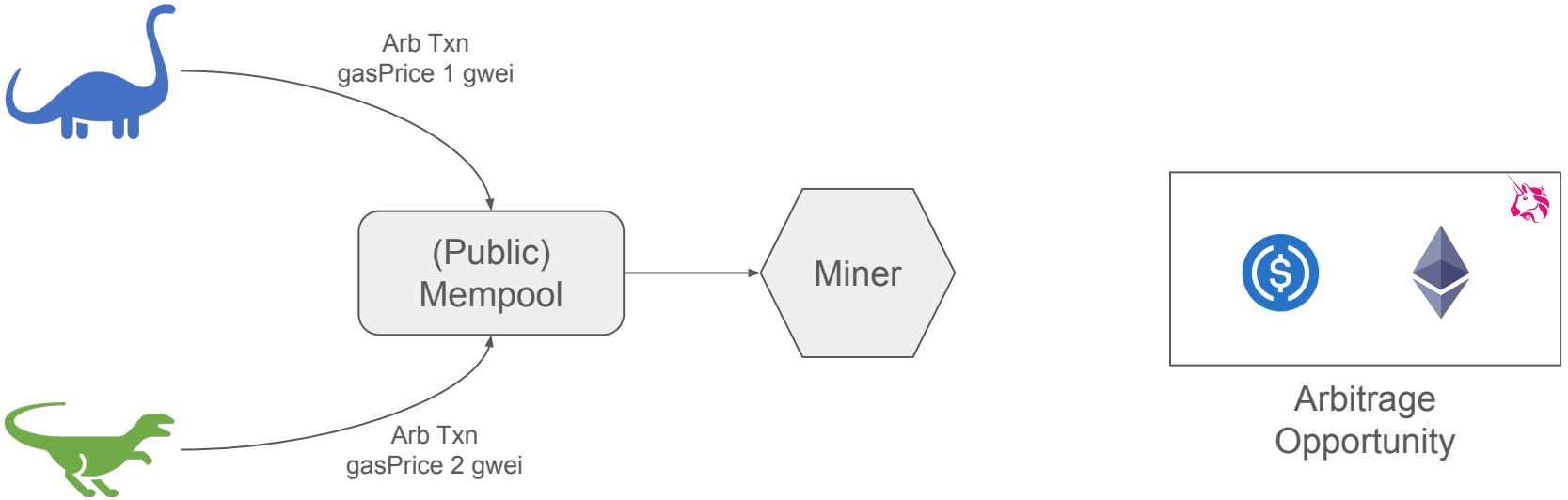
Arb Txn
gasPrice 1
gwei

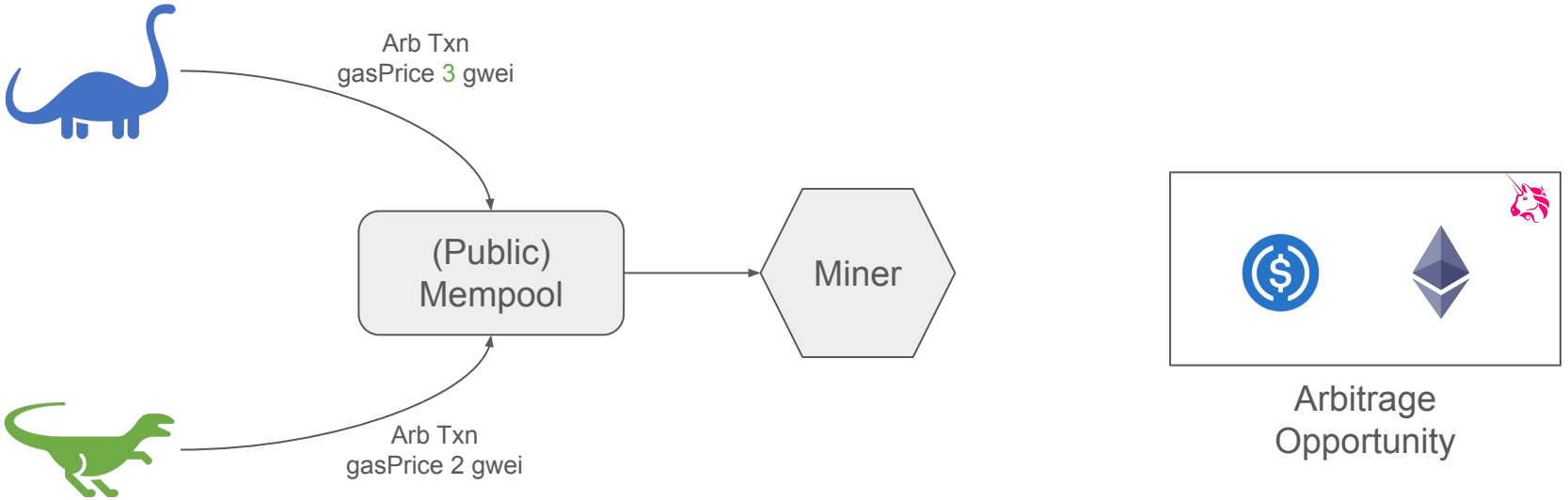
(Public)
Mempool

Miner



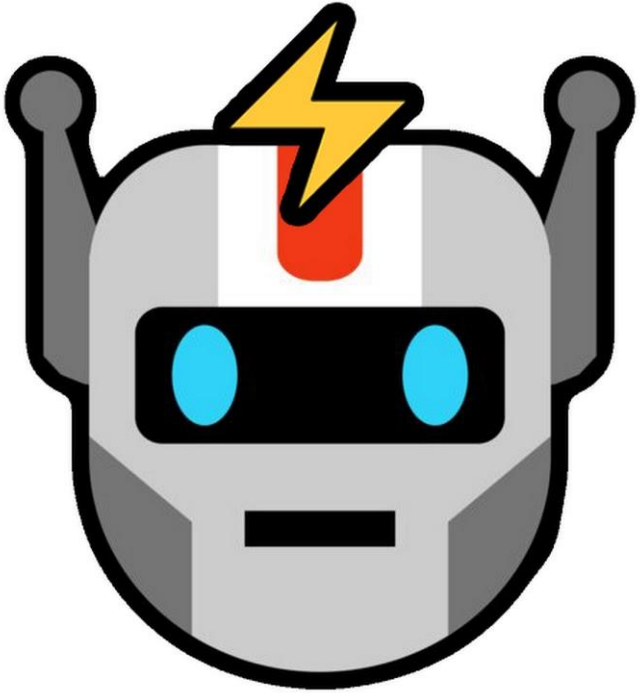
Arbitrage
Opportunity


Arb Txn
gasPrice 1 gwei
(Public)
Mempool
Miner
Arb Txn
gasPrice 2 gwei
Arbitrage
Opportunity


Arb Txn
gasPrice 3 gwei
(Public)
Mempool
Miner
Arb Txn
gasPrice 2 gwei
Arbitrage
Opportunity

Priority Gas Auctions

- Ethereum node software prioritizes transactions by gasPrice (maxPriorityFeePerGas after EIP1559)
- There is no direct way to “cancel” a transaction in the mempool
  - You can submit a new transaction with the same nonce but higher gas price
- “Searchers” engage in an ascending price auction to try to grab profit opportunity
- **Problem**: This clogs the blockchain with failed transactions



Flashbots

- **Problems**
  - Priority Gas Auctions cause massive externalities
    - Failed bids clog blocks
  - Ethereum gas fees are not nuanced enough to “bid” for ordering
    - Can’t cancel bids
    - No way to “back-run” or “sandwich” transactions
- **Solution**
  - Introduce a private channel where “searchers” can submit “bundles” of transactions
  - Searchers include a “tip” that is paid directly to miner for including the bundle

Opinion

Miners, Front-Running-as-a-Service Is Theft

There's a simple word for projects that seek to advantage miners while systematically exploiting blockchain users, say three researchers.

By Ari Juels, Ittay Eyal, Mahimna Kelkar

Apr 7, 2021 at 2:19 p.m. EDT

Fairness is complicated

- First-Come First-Serve transaction ordering has issues:
  - High-Frequency Traders built (competing) microwave relay networks that cost hundreds of millions of dollars
  - Nasdaq sells colocation services

Businessweek | Feature

The Gazillion-Dollar Standoff Over Two High-Frequency Trading Towers

The hunt for a millionth-of-a-second advantage in the town best known for *Wayne's World* is getting heated.

Decentralized Fairness is even more complicated

- **Problem**:
  - Different validators may have different views around which transaction arrived “first”
- **Solutions**?
  - PROF: Fair Transaction-Ordering in a Profit-Seeking World
  - Themis: Fast, Strong Order-Fairness in Byzantine Consensus
  - Order-Fair Consensus in the Permissionless Setting
  - A Fair and Resilient Decentralized Clock Network for Transaction Ordering

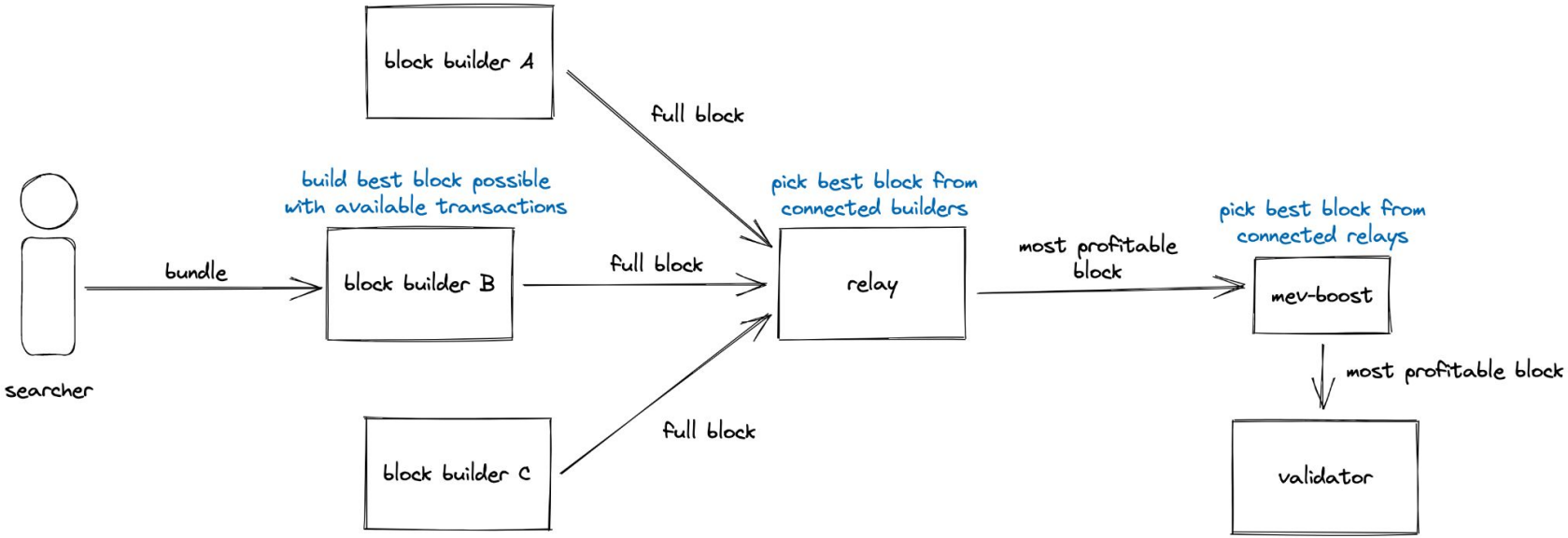
MEV geth

- Fork of the Go Ethereum client (geth)
- 80% of miners used MEV geth
- $675M in MEV extracted before the merge


ETHEREUM 2.0
THE MERGE

Proposer-Builder Separation (PBS)

- Under PoW miner (who solves hash puzzle) also built the block (ordered the transactions)
- Goal of PBS:
  - Separate block building (ordering transactions) from proposing a block (staking)
  - Proposing requires running a vanilla staking client
  - Efficient block building is extremely complicated
    - Block building will be centralized


block builder A
full block
build best block possible with available transactions
pick best block from connected builders
pick best block from connected relays
bundle
block builder B
full block
relay
most profitable block
mev-boost
searcher
most profitable block
block builder C
full block
validator

Podcasts

- Hasu's interview with a searcher
- Flashbots on the ZK Podcast
- Bell Curve Season 4:
  - A journey into the Dark Forest
  - Shining a light on MEV
  - Inside the economics of MEV
  - MEV in a modular world
  - Interview with a Searcher 2.0
  - Solana's MEV problem
  - MEV in the Cosmos
  - MEV 2.0 Order Flow Auctions & Privacy
  - MEV Masterclass

Time to Bribe: Measuring Block Construction Markets

Anton Wahrstätter[1], Liyi Zhou[23], Kaihua Qin[23],
Davor Svetinovic[1], Arthur Gervais[34]
[1]Vienna University of Economics and Business, [2]Imperial College London
[3]Berkeley Center for Responsible, Decentralized Intelligence (RDI), [4]University College London