Lecture 6

—

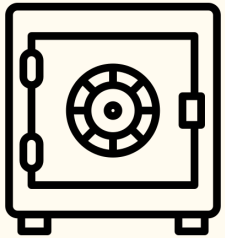
Further DeFi Applications

MakerDAO - Dual token CDP

Collateral Auction

- Takes ETH available and starts auctioning for DAI.
- Bid Duration - Auction ends when no new bids within timeframe
- Auction Duration - Auction ends regardless

Vault is "bitten"



Stability Fee in DAI

Maker Buffer

50k DAI

Buffer attempts to absorb bad debt

Surplus Auction
Triggered when total DAI and debt reaches a certain ratio.

DAI auctioned for MKR.

Received MKR gets burnt. Decrease supply

Reverse collateral Auction
After initial interest and DAI availability, converts to auctions for purchasing DAI at decreasing ETH amounts

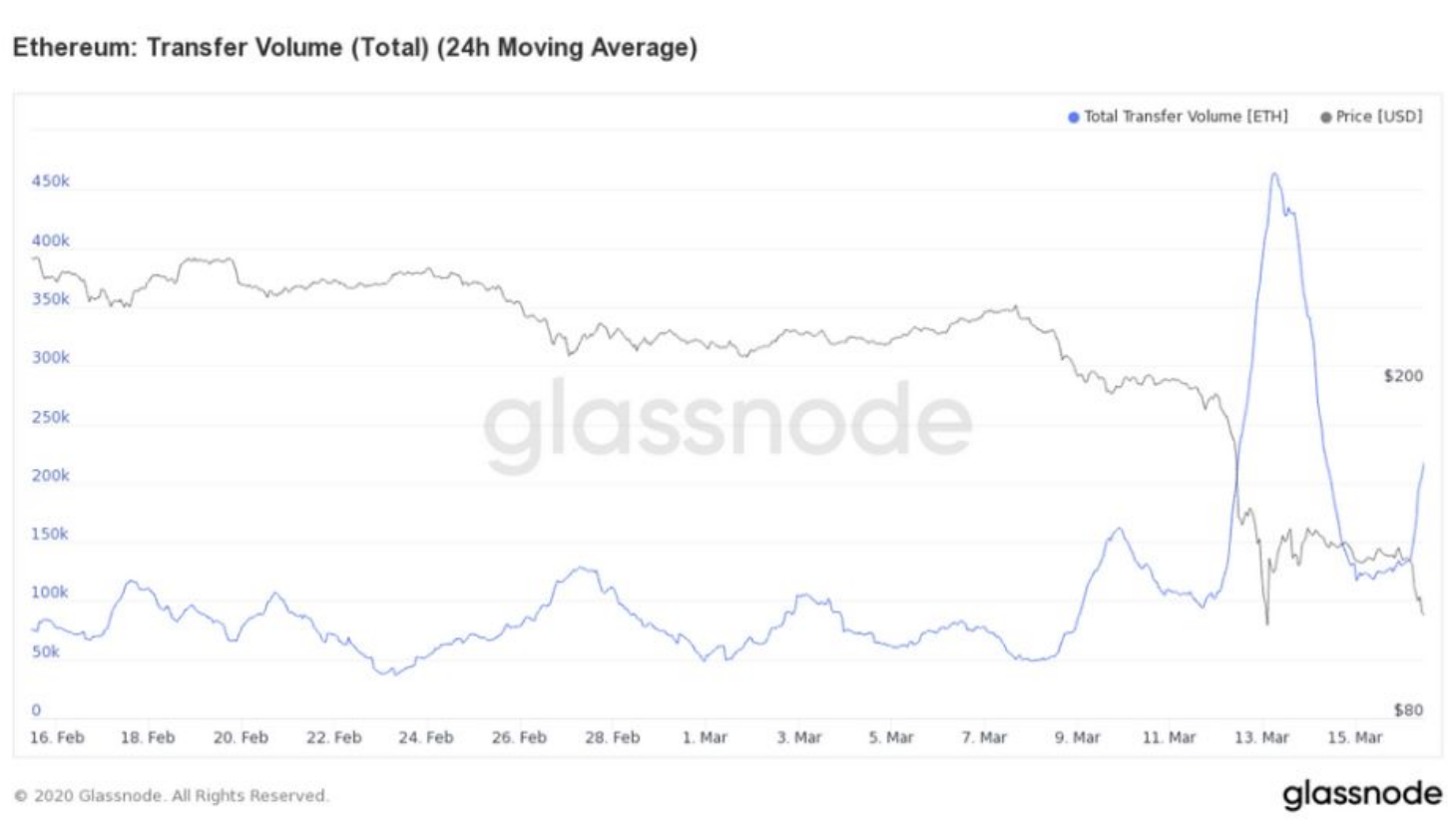
Debt Auction
No enough DAI was raised in the Collateral Auction.
Not enough DAI in buffer. System in in net debt state. Debt limit set through a vote.
Reverse auction occurs.
Amounts of DAI for decreasing amout of MKR tokens.
MKR tokens gets minted. Supply increase.

Black Thursday

Irrationality overwhelms Technology

12 / 13 March 2020 - Financial markets fall

Investors scramble to move ETH into stablecoins



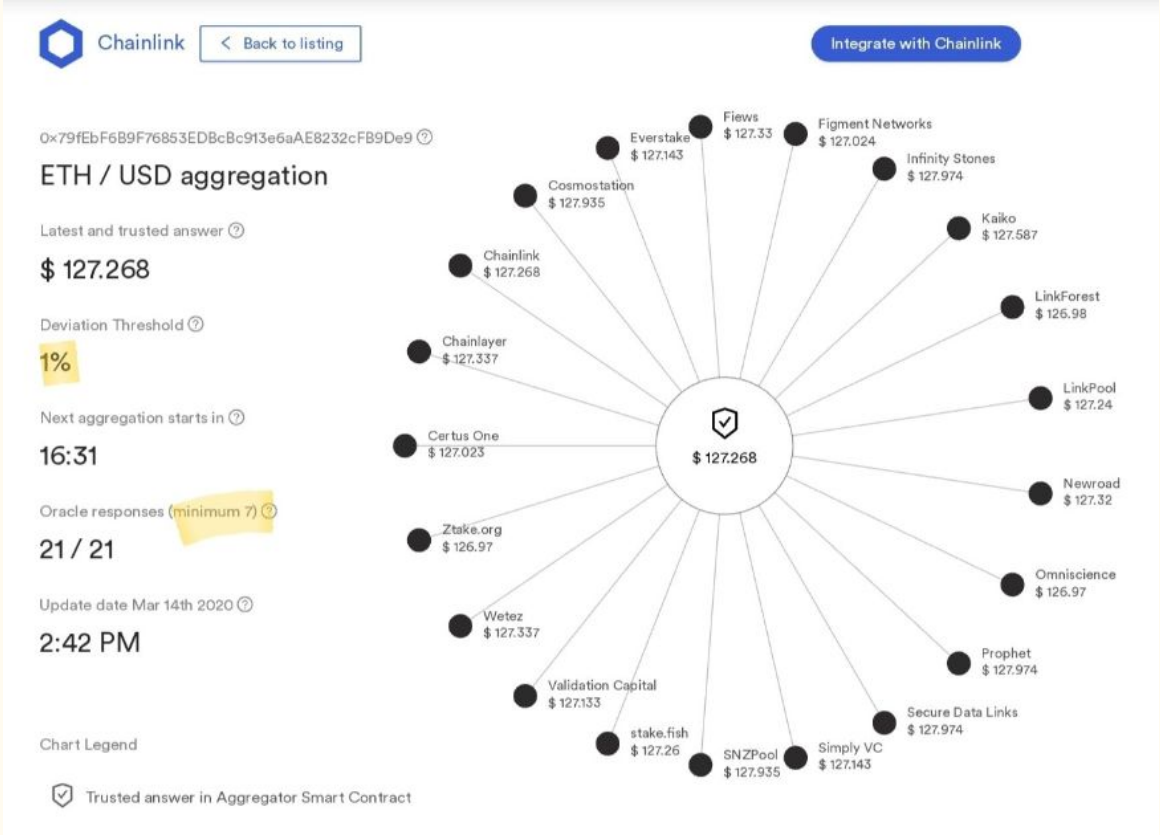
High trading volumes spike gas prices

Chainlink oracles fail, company suffers high gas fees

Default settings:
need 7 /21 quorum
updates every 20min

Under congestion:
- Nodes could not get responses timely.
- Oracle starts requesting more often. Pay LINK and ETH gas to talk to nodes.
- Answers could not reach quorum, answers too stale.

Chainlink had SLAs to maintain. Paid heavily to keep things going.



Massive liquidations - All parties struggled

CDP owners - network so congested they could not add in more collateral or close their positions. Extremely high gas fees for any transaction.

Auctions - 1200 positions liquidated, 4447 auctions triggered

Keepers - So many auctions immiediately drained available DAI that Keeper bots had.

Exchanges - became the only real source of liquidity, but could not determine prices due to oracles being overwhelmed or process the transactions due to network congestion.

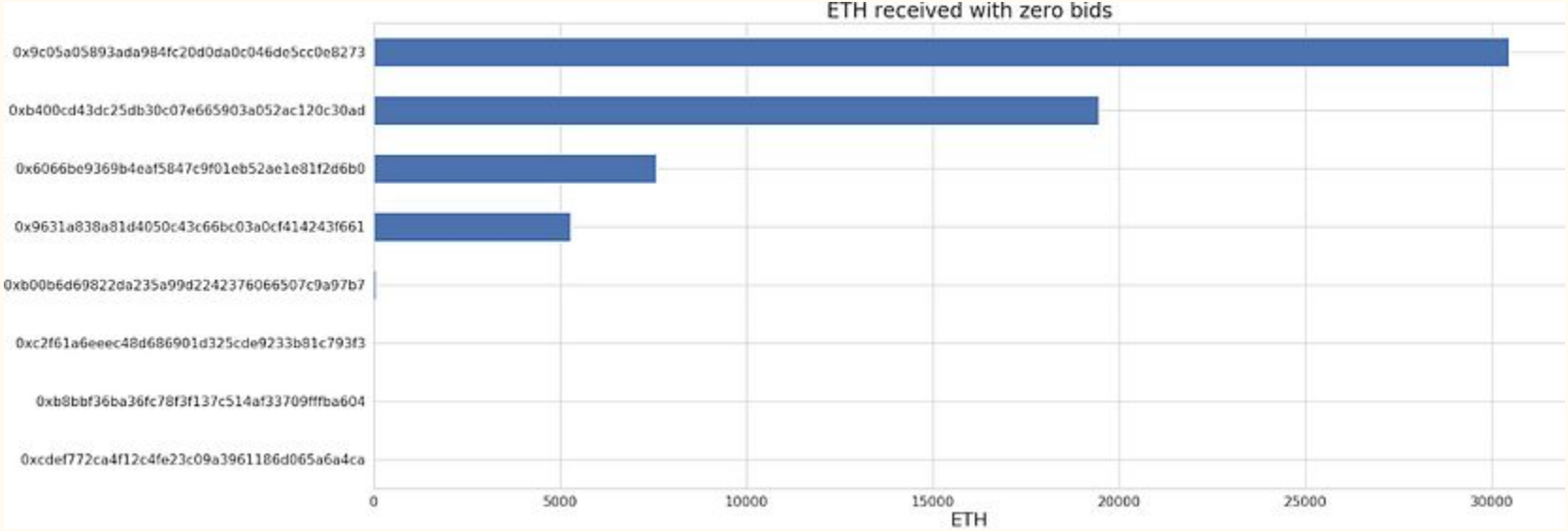
Unstoppable zero bids

$13 Million worth of zero bids

DEAL >> 3/12/2020, 9:19:03 AM | ID: **789** | Paid Rate: $0.00 dai/eth (-100.00%) ~ **Won!** | Price: $166.47 | from: 0x9631...F661 | Tx:..b6f Info >>

DEAL >> 3/12/2020, 9:19:03 AM | ID: **788** | Paid Rate: $0.00 dai/eth (-100.00%) ~ **Won!** | Price: $166.47 | from: 0x9631...F661 | Tx:..b51 Info >>

DEAL >> 3/12/2020, 9:19:03 AM | ID: **787** | Paid Rate: $0.00 dai/eth (-100.00%) ~ **Won!** | Price: $166.47 | from: 0x9631...F661 | Tx:..d00 Info >>

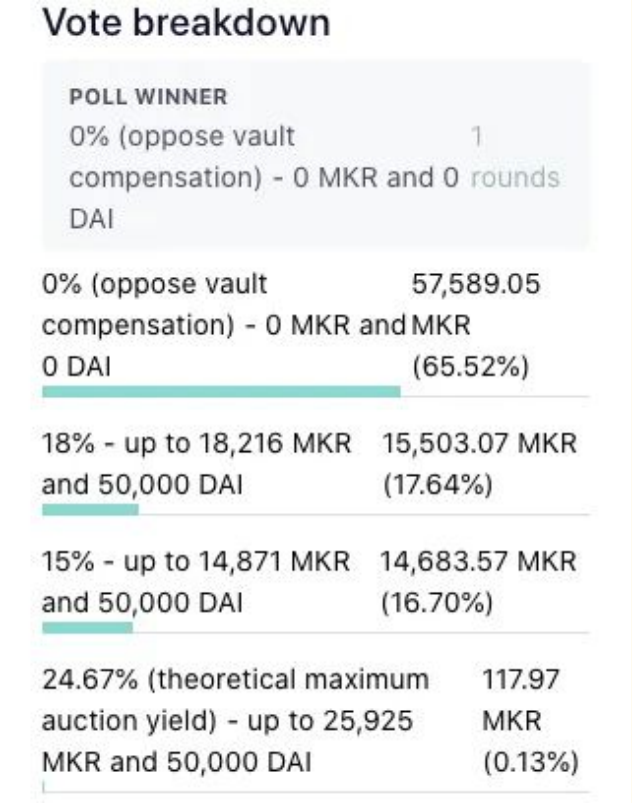


Aftermath - Community votes for **no** compensation

Mint some new MKR tokens for debt auction? Supply increase, price decrease.

Plus some DAI compensation? Decrease in DSR, stability fees unattractive.

Proposal here: https://forum.makerdao.com/t/vault-compensation-plan-v2/3584



Aftermath - US class action lawsuit

"While misrepresenting to CDP Holders the actual risks they faced, The Maker Foundation neglected its responsibilities to its investors by either fostering or, at the very least, allowing the conditions that led to Black Thursday, all after actively soliciting millions of dollars of investment into its ecosystem."

Plaintiff: Class Action
Defendants: Maker Foundation, DAI Foundation, Maker Growth Foundation

Aftermath - Maker wins $28 Mil lawsuit

- End of February 2023, MakerDAO wins lawsuit and do not need to compensate victims.
- Plaintiff did not have sufficient supporting facts and evidence.
- Plaintiff modifies lawsuit. 3 times.
- Maker Growth Foundation became MakerDAO. No more proper entity of defense.
- Settles outside of court for $1mil to stop chain lawsuits.

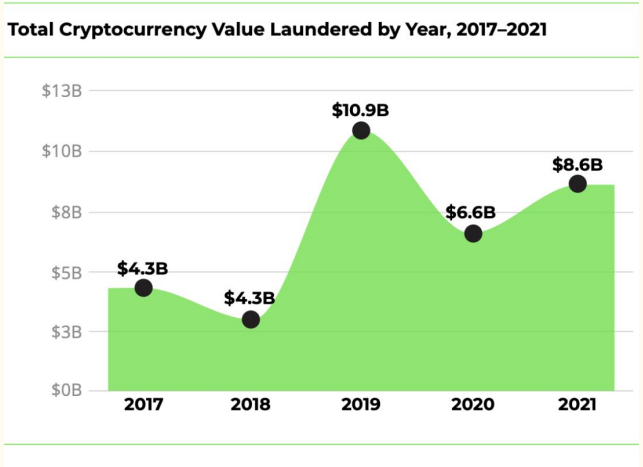
Lending and Borrowing Cont.

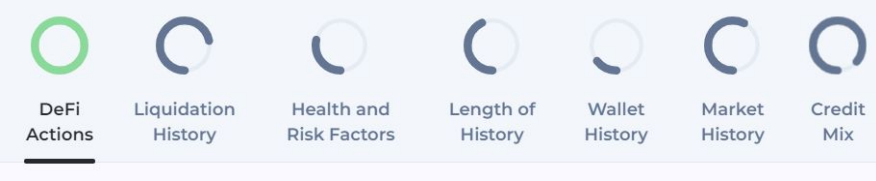
Fair and Under-Collateralization

Fair Collateralization - copying TradFi mechanisms

Using techniques found in TradFi:

1. KYC & AML companies
    a. Know your customer - identity, risk scoring and suspicious activity detection
    b. Anti Money Laundering - KYC and token movement.
2. On chain credit scoring
    a. Spectral Finance, similar to TradFi account check
    b. Difficult to aggregate multiple identities across many protocols.
3. Soulbound Tokens - Onchain credit reputation
    a. New concept proposed by Vitalik in May 2022. Increases NFT utility.
    b. Aspects of living become "Souls" - eg. Medical records become "Medical Souls"
    c. Credit Soul - Binance Account Bound token if you complete KYC

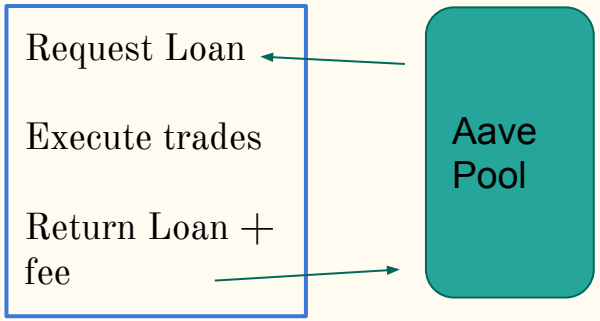


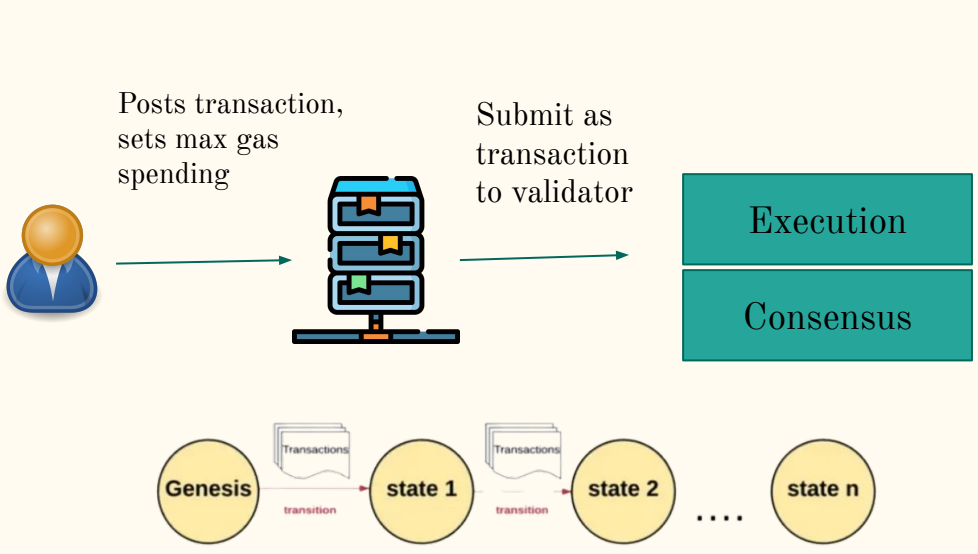


Under collateralization - Flash Loans

Take out a loan with no collateral? Okay if the loan can be repaid!

If the loan cannot be repaid, it never happened in the first place!





Flash Loans - DEX Arbitrage (The Good)

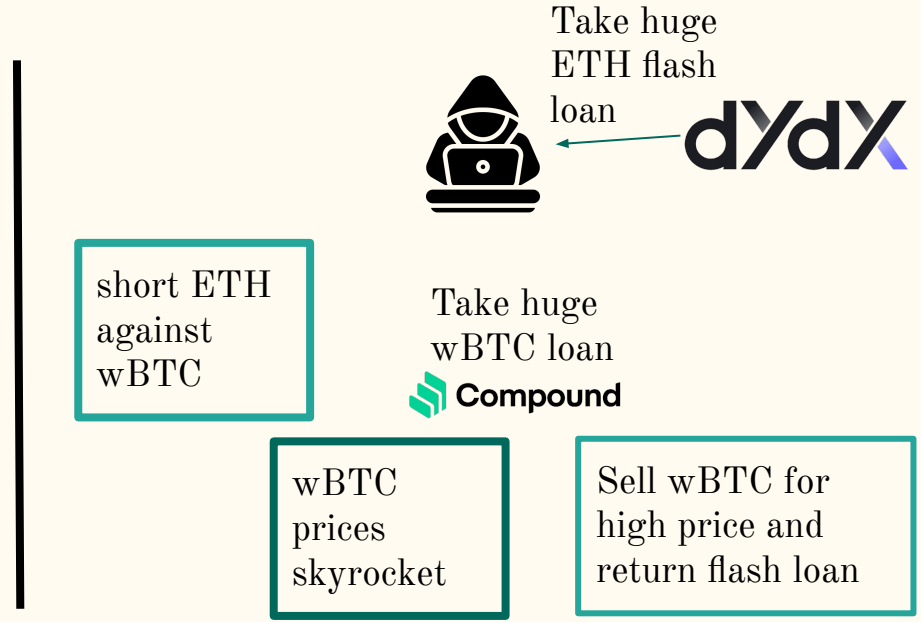
Capitalize on DEX price differences - algo trading

Capitalize on large liquidations - keepers earn liquidation fees

See it on Etherscan!

This is very transaction-order dependent
Manipulation! Moral? Legal?

Creates a standard by which DEXs are pressured to provide fair rates algorithmically or via oracles. Good for users!



Flash Loans - Price Oracle Attacks (The Bad)

Arbitrage may be good but what about all the other users right after "the big short"?

After making a token worthless for a brief instance, take out huge loans for no collateral.

Similar for synthetic assets, prediction markets, etc.

Types of Oracles

Offchain

Owned by protocol
Time Weighted Average Price
Filter outliers

Human Oracles???

Onchain

Centralized - trust reputation update
Decentralized - Sanity checking

The Future?

Data interaction on and offchain serves as the basis of many use cases, not just in DeFi, for this technology.

- IOT devices collecting data
- Gambling and games
- More sophisticated financial products.

We must solve the oracle problem!

- Constant availability
- High quality
- Scalable

MEV

Maximum Extractable Value

What are blockchains selling?

Blockspace? - Such high throughput and efficiency!

Transactions? - So cheap and fast!

New consensus mechanism?

Unimaginably advanced security?

Cool community? - Elon said it was cool

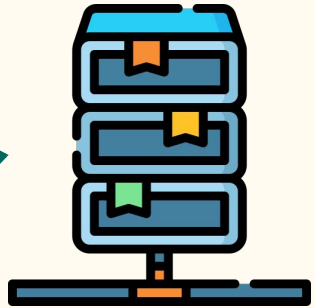
What are blockchains selling?

They are selling **gas**

Mempool/Txpool - Transaction lifecycle

Call func x at contract address 0xblahblah
The maximum (gas limit) I am willing to pay is y.

Does this exceed block gas limit?



Refund unused gas

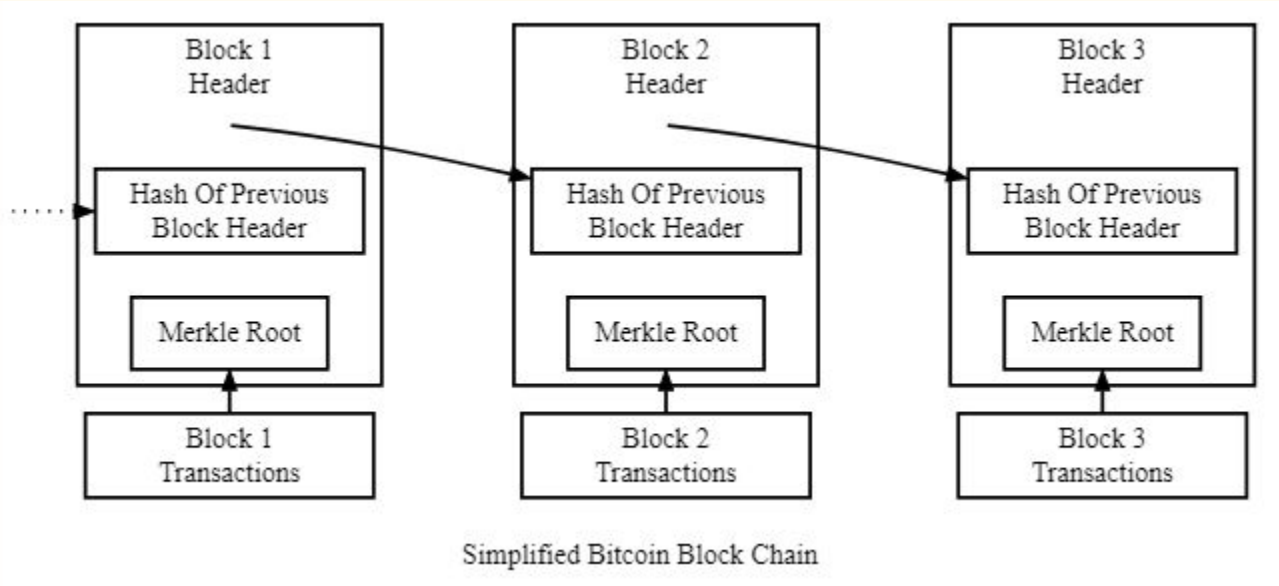
EVM

The max (gas limit) I am willing to pay
A payload of Bytecode.

https://mempool.edennetwork.io/

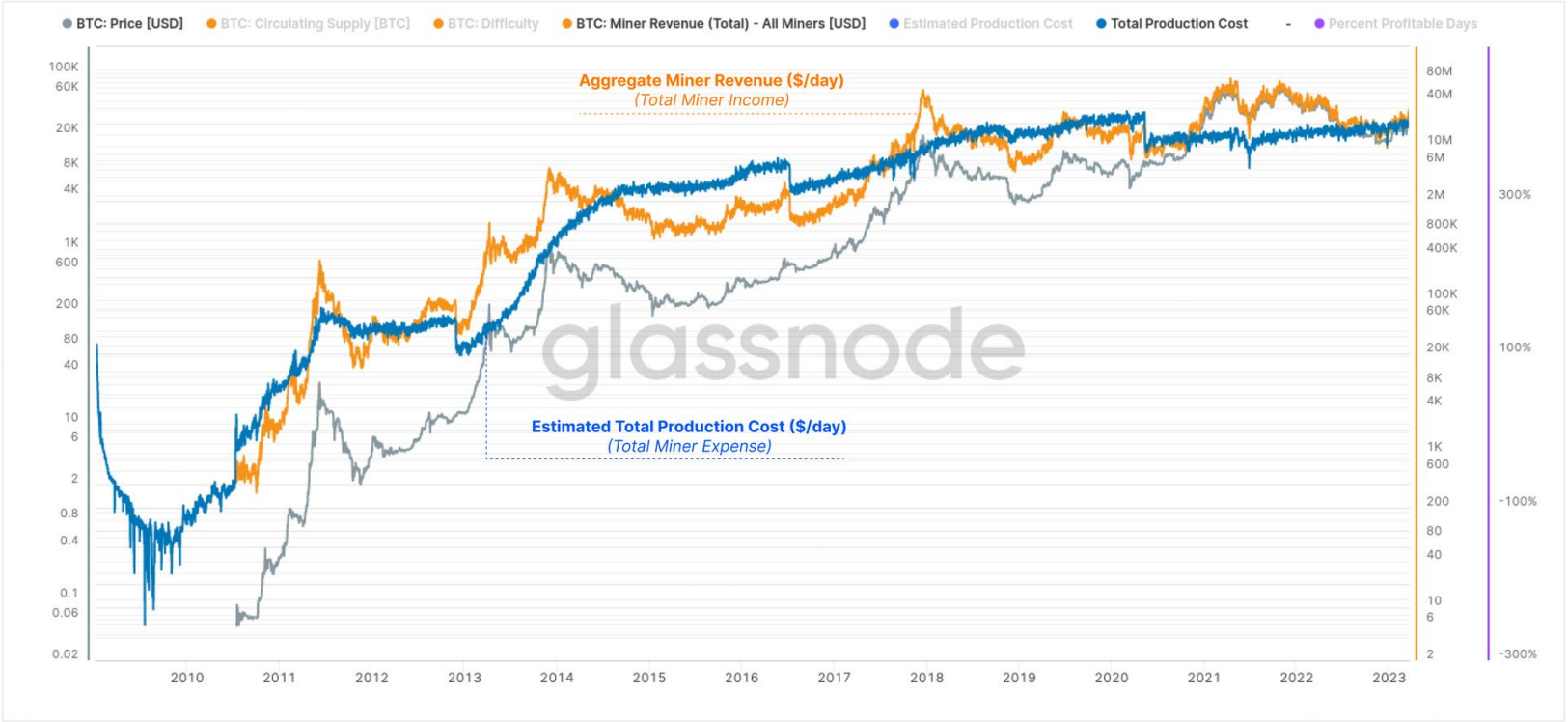
Miner to Maximizer

Next Bitcoin Halving: 22 April 2024
6.25 to 3.125 Bitcoin per validated block.



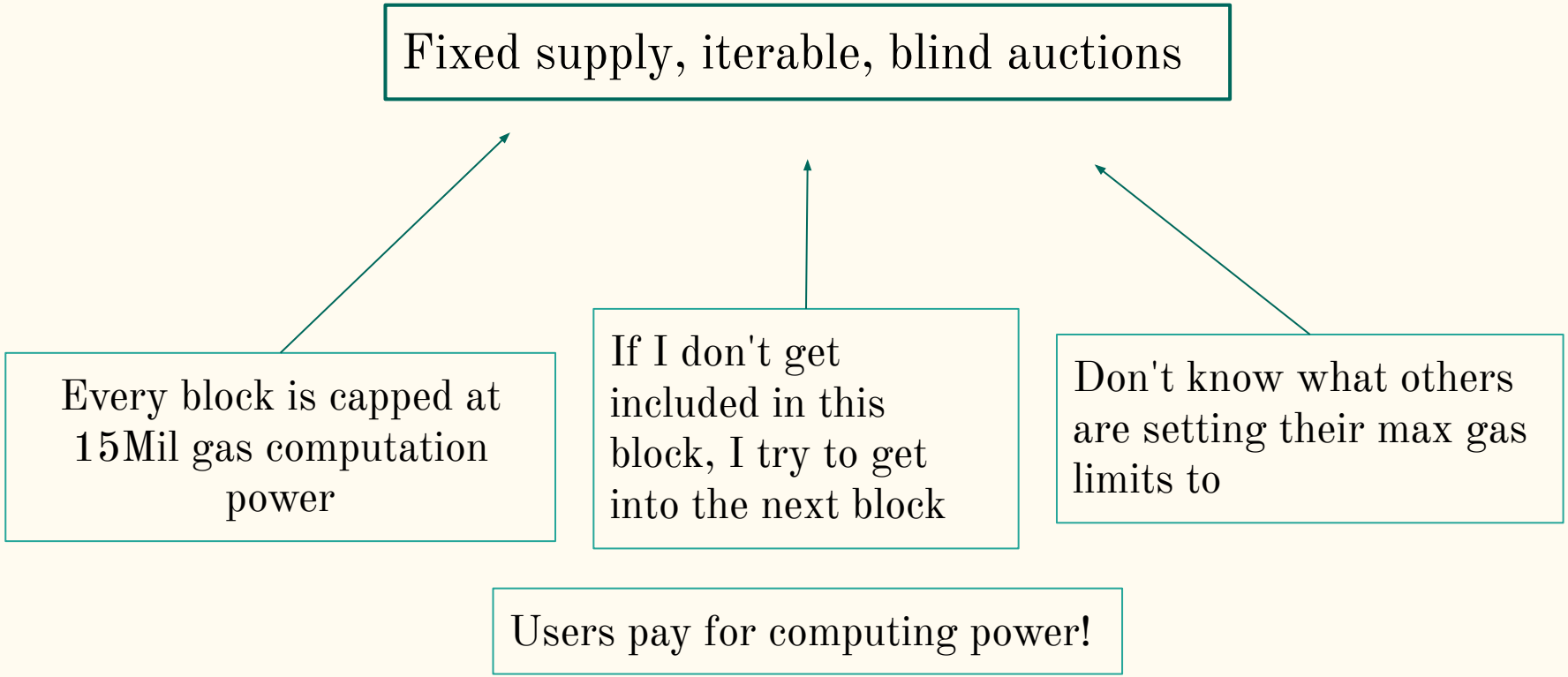
Simplified Bitcoin Block Chain

Bitcoin: Miner Revenue vs Estimated Production Cost

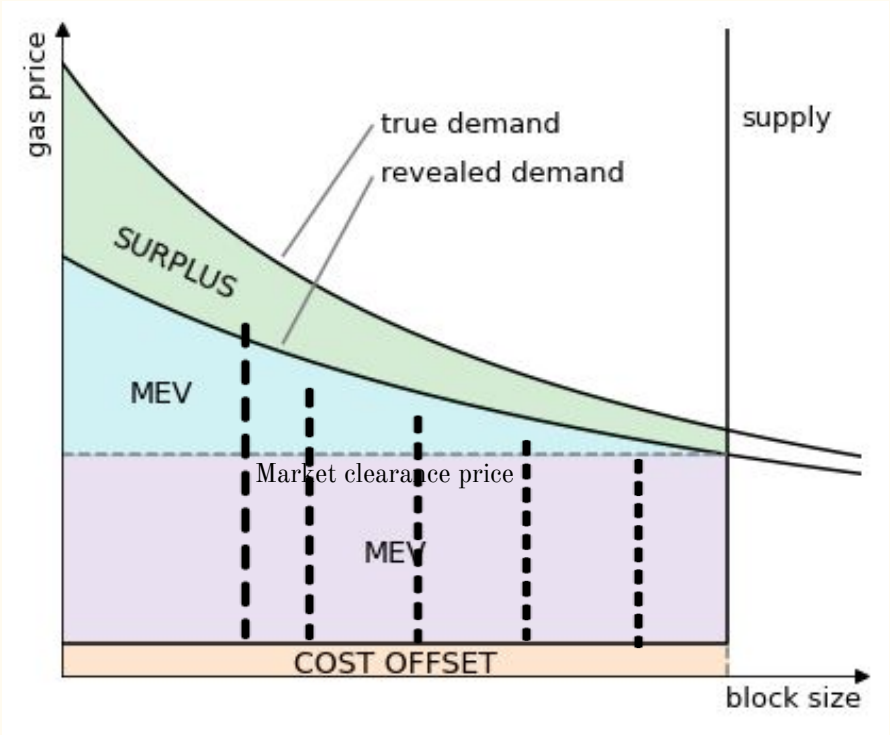


glassnode

PoW - First price auction market

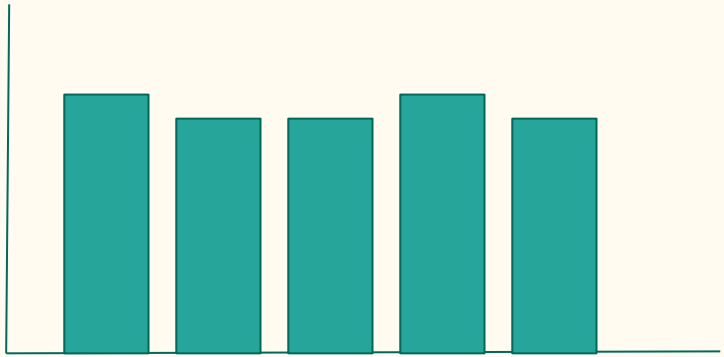


Perfectly discriminated, completely full blocks



https://hackmd.io/@adietrichs/eip-1559

What if I really want to get in but have no money? What if my txn is extremely large?



EIP 1559 - Towards diversification and deflation

- Bitcoin has a supply cap of 21Mil and is halving miner rewards
- Ethereum has UNLIMITED supply. How to control?
- All MEV going towards miners. Users are maximally exploited.
- Miner monopoly on txn order leads to shady collusion. Giving more value to miners.
- **Goal: reduce mining incentive and transfer to other forms of value**

Move to a **uniform price auction model**

There are n amount of products and the top n bidders pay the first rejected bid (aka. everyone pays market clearing price)

Gas fee calculation - EIP 1559

This fee is paid regardless of outcome - success or fail

units of gas used * (base fee + priority fee)

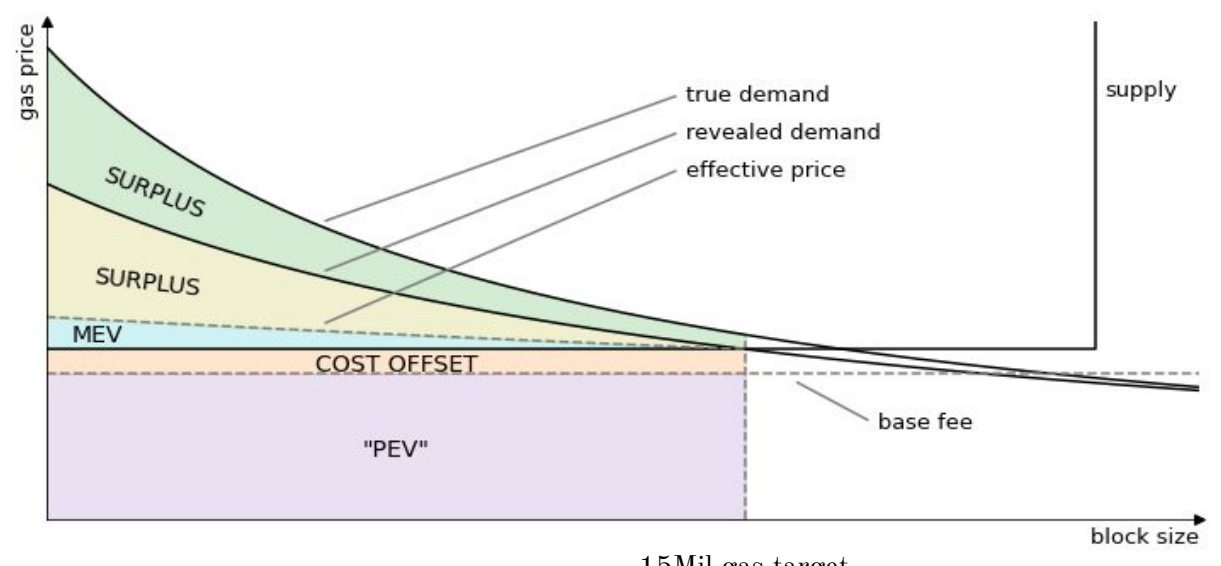
Based on transaction complexity
Deploying a contract is very expensive!

Minimum amount required for txn to be considered valid.
Affected by the queue length in mempools of many nodes.
Long queues = high txn volume = higher fees
This fee is burned upon successful incorporation into a block

A "tip" for the validator.
Remember zero bids on Black Thursday?
This fee is retained by validator
Mining pools usually set a minimum (2 gwei)
Wallets allow different settings. Or set your own through RPC.

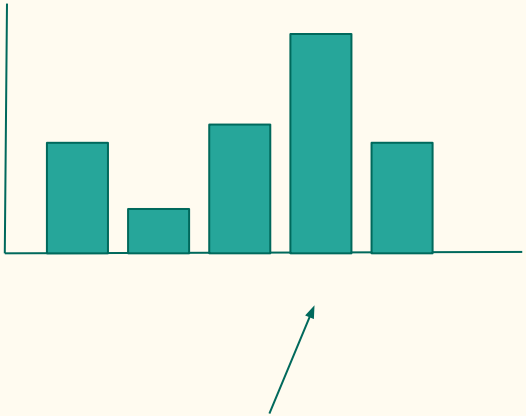
Perfect (user) competition, half filled blocks

30Mil gas limit



15Mil gas target

15Mil block target balances out long and short term goals



Can tolerate high transaction volume but not forever

Base fee calculation - Tâtonnement

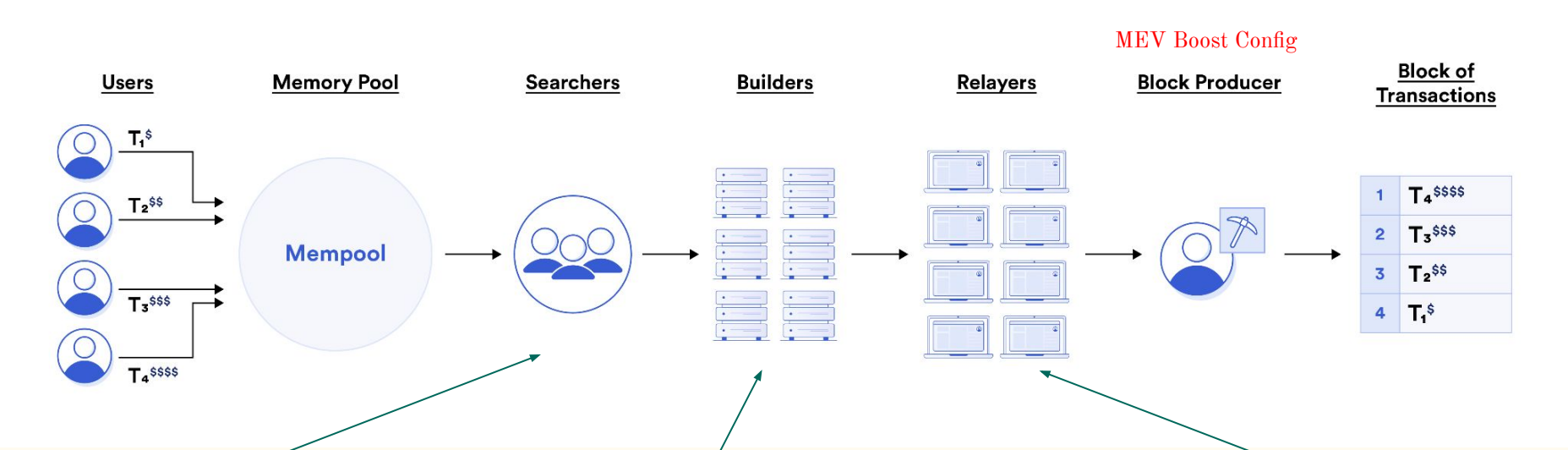
- If you can read French - https://www.jstor.org/stable/44346456
- A control method to estimate market clearing price based on revealed demand.
  - Block higher than 15Mil will increase base price and decrease txns
  - Block lower than 15Mil will decrease base price and increase txn submission
  - How to prevent miners mining zero blocks?

$$current\_base = prev\_base * (1 + \frac{actual - target}{target * k})$$

The bigger the k, the smaller the change. Current k = 8.

MEV Value Chain - All is fair in love and MEV

1 month after The Merge, only ~23% Miners remained



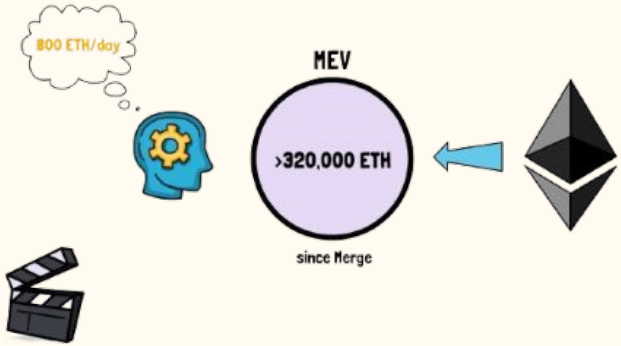
Searches for transactions in many mempools and create bundles of profitable txns through simulating txn ordering

Builders aggregate these bundles into a full block. Direct competitor to normal mempools.

Relayers aggregate builders and send most valuable blocks to validators who have memboost.
90% of blocks today are MEV bot mined.

The current state of MEV

The Good



More efficient DeFi markets, higher returns for arbitrageurs
New financial products - MEV blocker, permissioned mempools

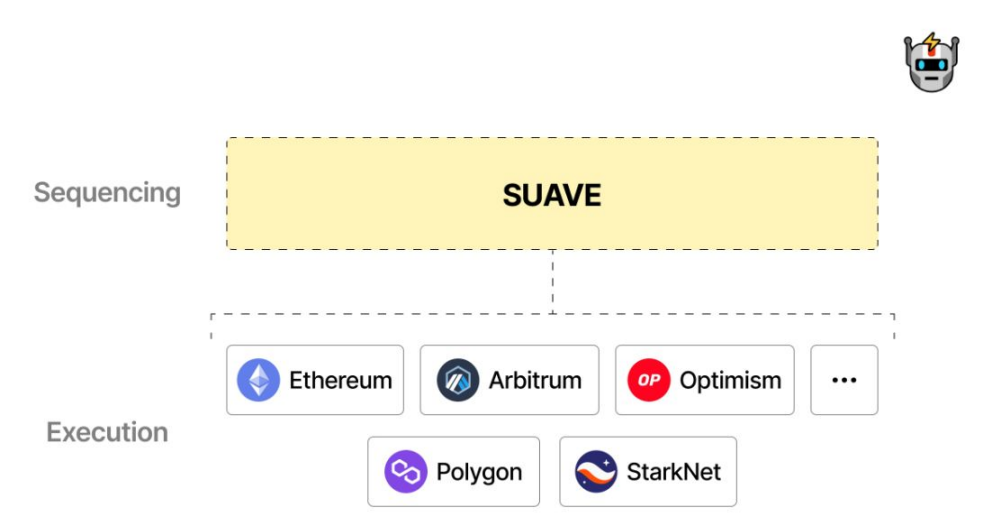
The Bad - centralization

- Builder centralization - currently 80% of blocks created by 5 groups
- Relay centralization - 7 relays controlling 90%
- Validator reordering - validators take turns, block reordering profitable
- Toxic forms of MEV - Sandwich Attacks

The future of MEV (of Blockchain?)

Once again towards decentralization....

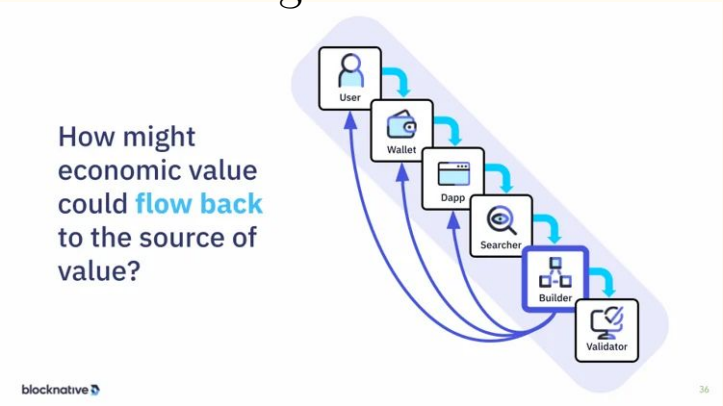
Multi-chain mempool democratization



MEV Burning vs Smoothing

- The chain takes control of the MEV and burn it like the base price.
- Mechanism for distributing MEV amongst validators
- MEV tax (half burn?)

MEV Sharing



It's NFT Paris Week!

23 - 23 Feb