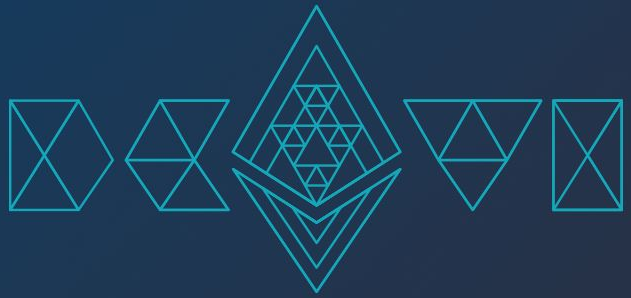


Future-block MEV

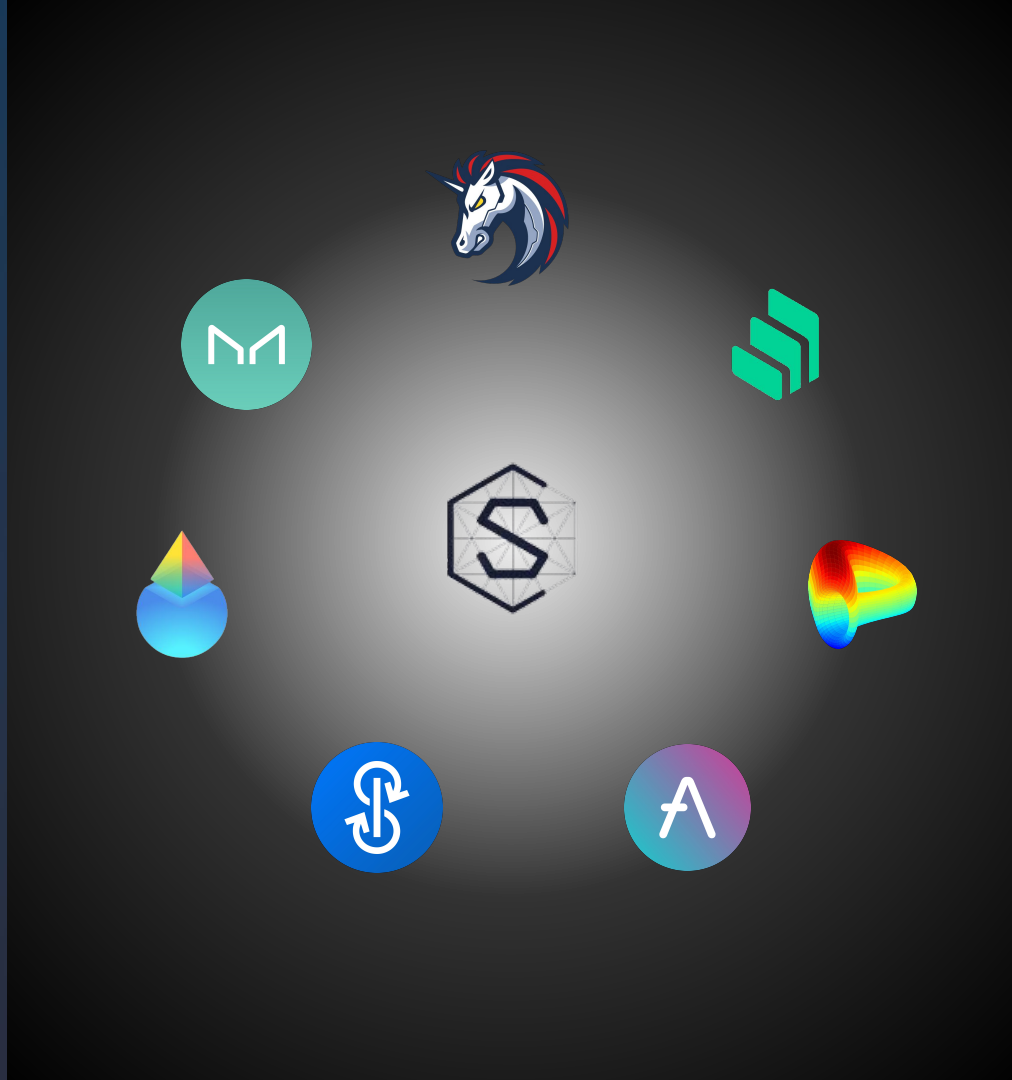
in Proof of Stake

Torgin Mackinga

ChainSecurity

About ChainSecurity

- We are focused on blockchain security
- Smart contract audits
- Some of our clients:
  - Maker
  - Curve.fi
  - Compound
  - Aave
  - Yearn
  - 1inch
  - Lido



Block production

Block production

Proof of Work:

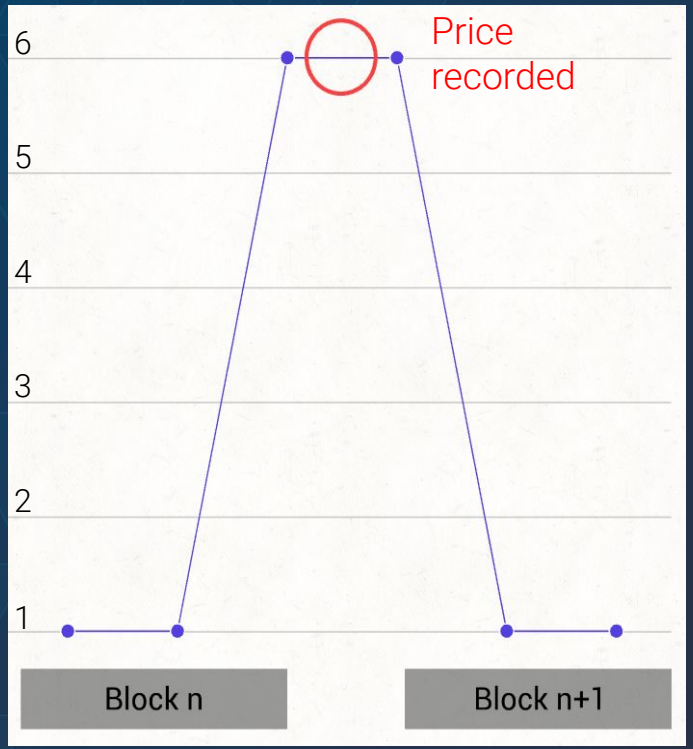
Everyone mines every block

Proof of Stake:

Block producers are determined in advance

You can know when **you** will create a block, up to 12 minutes ahead of time!

Future-block MEV



Uniswap price manipulation

Oracle manipulation

- Usually expensive due to arbitrage
- Unless you are the proposer of n+1
- You can "hide" MEV

Trigger a liquidation with **no competition!**

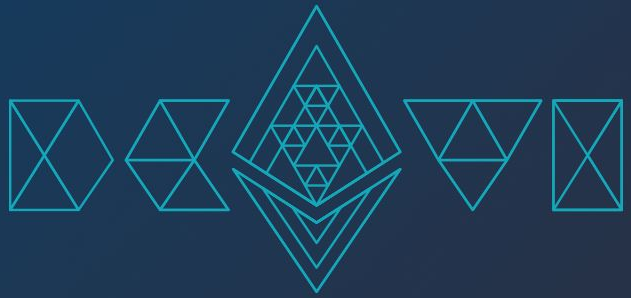
Takeaways

1. Block proposers in PoS are known in advance

2. This information is valuable

Read more:

https://chainsecurity.com/oracle-manipulation-after-merge



Thank you!

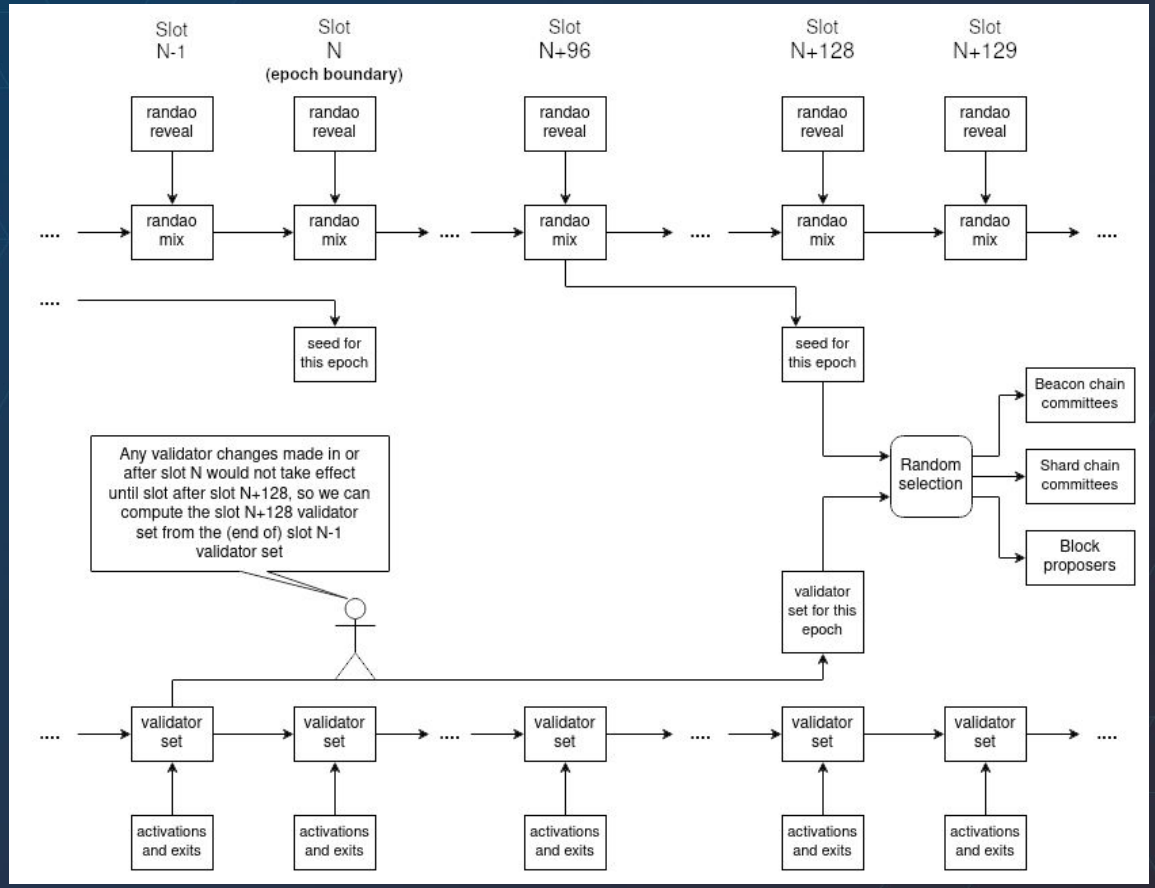
Torgin Mackinga

@MTorgin

Read more:

https://chainsecurity.com/oracle-manipulation-after-merge

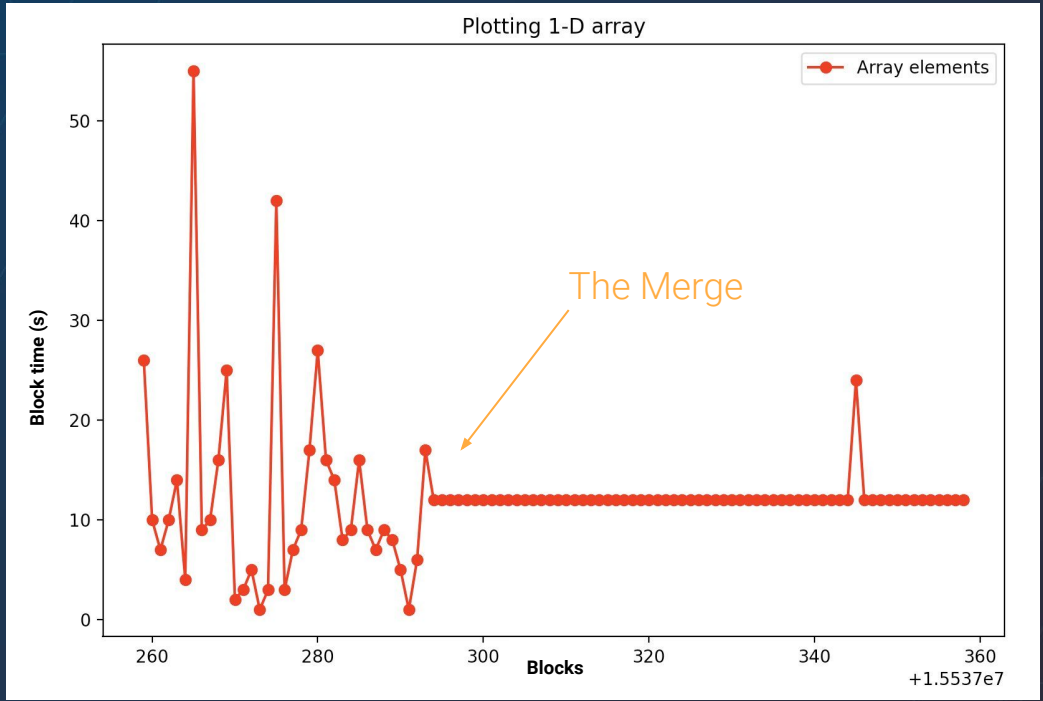
Appendix



Source: https://github.com/ethereum/annotated-spec/blob/master/phase0/beacon-chain.md

Block production

Source: [1]



Proof of Work:

- Block times are random
- Block producers are random

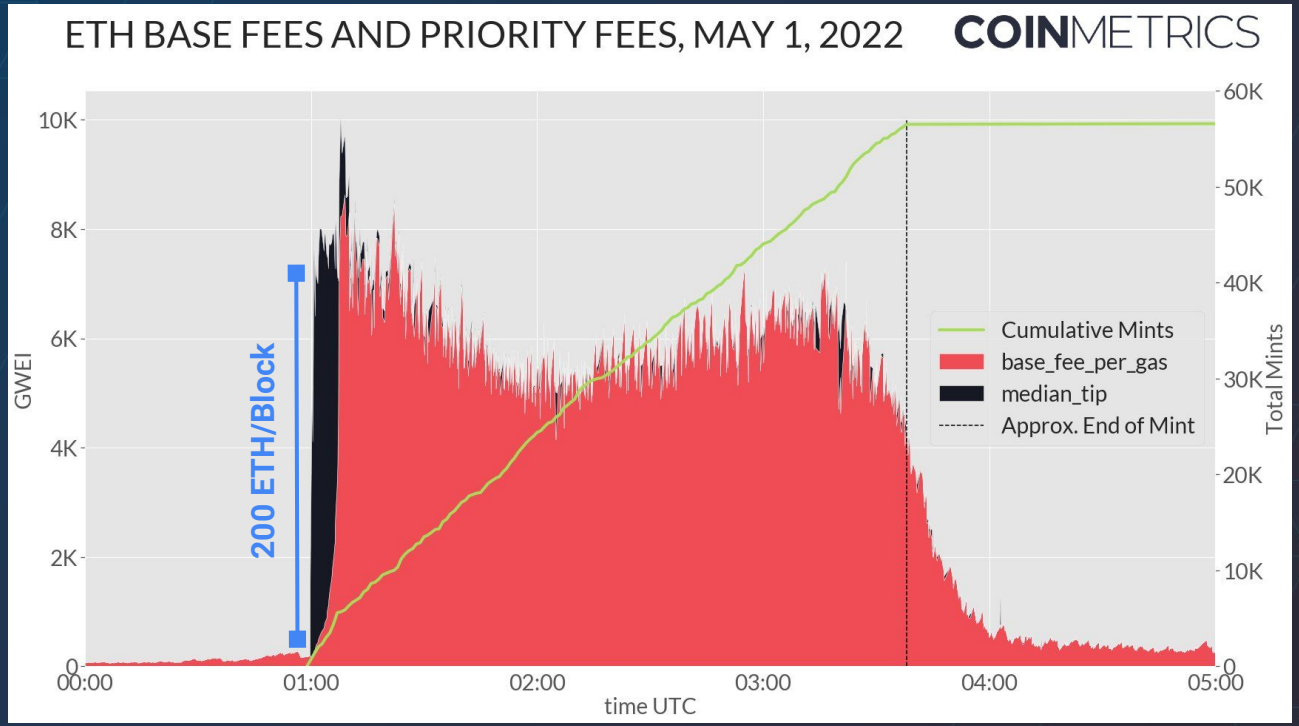
Proof of Stake:

- Block times are deterministic
- **Block producers are deterministic**

Future-block MEV

Create your own MEV!

- Launch an NFT mint in a block you control



Gas fee during Otherside NFT sale. Source: [2]

Sources

[1]: https://twitter.com/koeppelmann/status/1570306606339964929/photo/1
[2]: https://coinmetrics.substack.com/p/state-of-the-network-issue-153