DISCLAIMER: This is something to think about, but it's by no means a priority item. It's more something to consider after all the major upgrades are done.

Proof of Burn is an established consensus mechanism, similar to PoS, where validators compete to burn the native currency (in the case of Ethereum, ether) to get the right to build the next block.

Conventional Proof of Burn, compared to Proof of Stake, has some obvious downsides. I propose the following modification:

1. The [EIP-1559](EIP-1559) priority fee must be zero for type 2 transactions.

2. A third transaction type (transaction type 3) is added:

3. Transactions with type 3 take a transaction hash (tx

), a block hash (block

), a positive number of blocks less than or equal to 1 (perhaps this could be increased) (numblocks

), and an amount of wei to burn (amount

).

- 21k gas is consumed (but this doesn't count towards the block gas limit)

- amount

wei is sent to address(1)

.

1. Transactions with type 3 take a transaction hash (tx

), a block hash (block

), a positive number of blocks less than or equal to 1 (perhaps this could be increased) (numblocks

), and an amount of wei to burn (amount

).

1. 21k gas is consumed (but this doesn't count towards the block gas limit)

2. amount

wei is sent to address(1)

.

1. Block validity is changed:
2. Type 3 transactions must be followed with either another type 3 transaction with an identical tx

and lower amount

(in the case of a tie, the transaction with the lower transaction hash is included first) or a transaction with transaction hash equal to tx

.

- Each non-type 3 transaction must be preceded with a type 3 transaction with tx

equal to its transaction hash

- The first type 3 transaction in each block must have the highest value of amount

of any type three transaction in the block

- Any type 3 transaction that proceeds a non-type 3 transaction must have a lower value of amount

than any preceding type 3 transaction that proceeds a non-type 3 transaction.

- A type 3 transaction can only be included in a block if block

is in the first numblocks

ancestors of the block.

1. Type 3 transactions must be followed with either another type 3 transaction with an identical tx

and lower amount

(in the case of a tie, the transaction with the lower transaction hash is included first) or a transaction with transaction hash equal to tx

.

1. Each non-type 3 transaction must be preceded with a type 3 transaction with tx

equal to its transaction hash

1. The first type 3 transaction in each block must have the highest value of amount

of any type three transaction in the block

1. Any type 3 transaction that proceeds a non-type 3 transaction must have a lower value of amount

than any preceding type 3 transaction that proceeds a non-type 3 transaction.

1. A type 3 transaction can only be included in a block if block

is in the first numblocks

ancestors of the block.

1. At the end of each block, address(1)

loses an amount of wei equal to the integer value of the block hash times $2^{16}$

(to prevent ties and to encourage fewer blocks).

1. The "correct" chain is the one in which address(1)

has the most ether. This should be re-selected every twelve seconds, but tracked in real-time.

Possible addendum:

1. The block gas limit is equal to the amount transferred to address(1)

in that block divided by the gas price

Upsides:

- There's a low cost to becoming a validator

- People pay for the security they want. L2s aren't as necessary if people don't want to pay for as much security, and if there's some crucial transaction that must be included at all costs, then potentially one could pay for security above what one could get from PoS.

- MEV gives a normal profit (if there's profit to be had, anyone can just burn more in order to capture all the MEV). 100% of MEV is used to secure the blockchain.

- Simpler mechanism

- Transactions cannot be censored

- No weak subjectivity assumption

Downsides:

- There's a low benefit to becoming a validator

- We just switched to PoS. Validators would be unhappy.

- Liveliness assumption

- This might actually be useful to reduce mempool congestion

- This might actually be useful to reduce mempool congestion

- Higher chance of transactions getting reorged due to selecting non-optimal parent blocks

- Lower reorg cost

- 1/3 of staked ether is 5,166,823.67 ETH

- Amount of MEV per block is 0.0333 ETH (derived from flashbots dashboard)

- Amount of priority fee per block is roughly 0.0623 ETH (average of 50 most recent blocks)

- Total MEV + priority fee = 0.0956 ETH per block

- Thus, it would take about 20.5 years for genesis to be as secure as it is with PoS today, assuming validators do not collude

([which is not a reasonable assumption](#))

- How do we prevent Ethereum from becoming too

deflationary?