TL;DR

A merged mined chain can be used as a fully decentralized rollup alternative to achieve 1000 tps, while using the current ETH1, and 100K+ tps using ETH2 data chains.

Description

Here is how this would work:

1. To participate in the network, a node would register in a smart contract on the main net.
2. There would be a single, randomly selected proposer for each epoch (block range)
3. Transactions would use aggregated BLS signatures instead of ECDSA, otherwise, the merged mined chain would be identical to ETH1.
4. Each proposer would submit a block by
5. submitting block body as calldata, and
6. submitting the state root to the ForkTree smart contract.

The block would aggregate all transaction BLS sigs into a single BLS sig. A fund transfer transaction would then take as little as 10 bytes or 160 gas (100 times less compared to what it takes now)

1. The fork choice used by the ForkTree

contract would be simply the longest chain.

1. To exit, one would simply burn the funds on the merge mined chain and submit the receipt against a finalized root on in the ForkTree

smart contract

Advantages:

- full ETH compatibility
- immediate exit
- no need to wait for 7 days as in optimistic rollup
- fully decentralized - no single operator
- security: identical to the main net

!

- Satoshi Nakamoto saw merged mining as a way to scale blockchain!

Future: one could use each of ETH2 data chains as data storage for merge mined chains. This could bring TPS to 100,000+!!!