Update 10/10: added header availability attestations

Update 9/28: removed provers

, added hybrid sequencing

(an adaptation of Ethereum Hybrid-PBS)

This is a new sequencer selection proposal. The current block proposer

role in Fernet gives advantage to centralized MEV operators and prover pools over unsophisticated stakers, requiring stakers to make out-of-protocol market connections to compete. Proposer/builder separation (PBS) splits block proposer

into proposer

, and builder

roles. This allows proposers to be stateless and run on low-cost hardware, improving decentralization and censorship resistance.

proposers

are assigned L2 slots using RANDAO. Bonded builders

submit bids alongside blinded block headers for the current proposer

to accept. The winning block data is then published to L1 (soft finality), followed by a proof within MAX_PROVER_TIME.

Staking

Stakeholder tokens are deposited/withdrawn on L1 alongside proposer public keys, with fixed-rate queues to limit churn.

Protocol phases

Blocks are first proposed, then proved. Transactions achieve soft finality when proposed.

---------- L1 blocks -> |proposal| proving | |proposal| proving | |proposal| proving | |proposal| proving |

---------- L1 blocks -> |proposal| proving | | |proposal| missing | | |proposal| proving (orphan)| | |proposal| proving (orphan)| ---------->|proposal| proving |

During each slot:

1. A proposer

is chosen using the L1 RANDAO two epochs prior (like L1)

1. The proposer

broadcasts an inclusion-list that builders must include

1. builders

broadcast block headers with bids + bond * the required bond amount adjusts dynamically as proof slots are missed

1. the required bond amount adjusts dynamically as proof slots are missed
2. proposer

signs and broadcasts the winning header * Unselected candidates attest to timely availability of the winning header * Majority signed headers can be submitted to slash builders if the block is not posted

- Majority signed headers can be submitted to slash builders if the block is not posted
- Unselected candidates attest to timely availability of the winning header
- Majority signed headers can be submitted to slash builders if the block is not posted
- Majority signed headers can be submitted to slash builders if the block is not posted
- builder

publishes the block data to L1 (proposal phase)

(up to MAX_PROVER_TIME later…)

1. builder

publishes the block proof to L1 (proving phase)

1. builder bond released

Batching

Fernet batching can be added by replacing:

- builder

publishes proof to L1

with:

1. builder

broadcasts proof

1. the next-block builder

broadcasts a signature of the proof

If at the end of M slots a final proof fails to hit L1, all builders

have bonds burned unless they publish these signed messages.

If the next-block builder does not broadcast a signature, the builder

must submit proof data to L1.

Hybrid L1 Sequencing

Every other block, anyone may submit block data (with bond)directly to L1.