ePBS design evolution

mike neuder – ethereum foundation
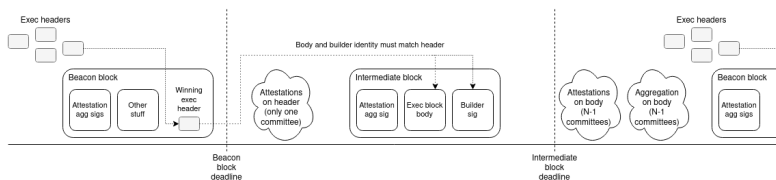pbs.salon – july 17, 2023

Outline

Desiderata
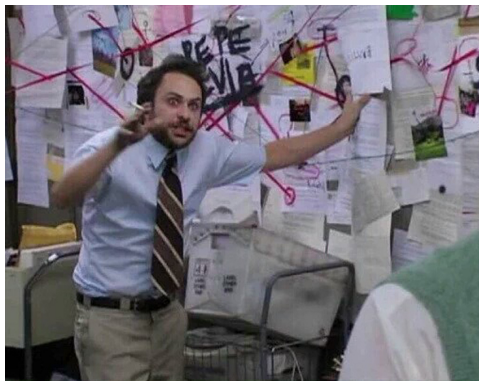
- *honest builder publication safety*
- *honest builder payment safety*
- *honest proposer safety*
- *permissionlessness*
- *censorship resistance*
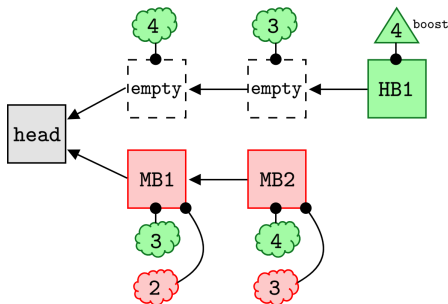- *roadmap compatibility*

Two-slot PBS
Sketch

- Original desgin from Vitalik in October 2021
- Partition attesting committee over beacon block and intermediate block
- Became the canonical design. What people referred to when they discussed ePBS

Two-slot PBS

- ○ Malicious proposer splits the honest attesting committee
- ○ Malicious proposer continues the split over a second slot
- ○ Honest proposer builds on the empty chain
- ○ Malicious proposer releases private attestations, orphaning HB1

https://notes.ethereum.org/@mikeneuder/epbs-reorgs
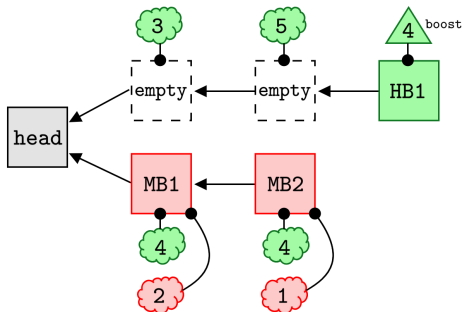
Two-slot PBS

- Malicious proposer still controls two slots, but not enough attestations to beat proposer boost
- No ex-ante reorg possible in this case

https://notes.ethereum.org/@mikeneuder/epbs-reorgs
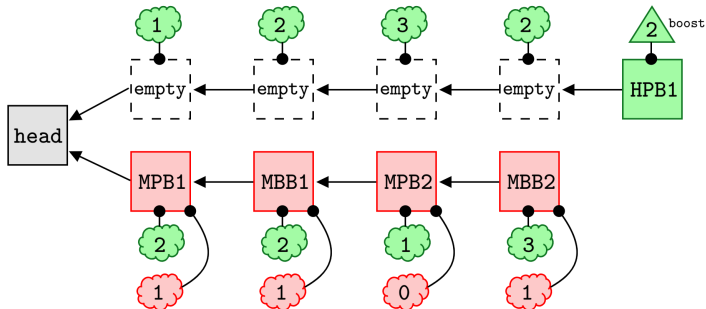
Two-slot PBS

- Same allocation as before
- The ex-ante reorg *is possible* because the proposer boost is weaker

Two-slot PBS
Reorg probabilities

○ Just ex-ante reorg probabilities, lower bound on all reorgs

○ *Conclusion* – significantly weakens the protocol against reorgs

https://notes.ethereum.org/@mikeneuder/epbs-reorgs

Desiderata
Part II

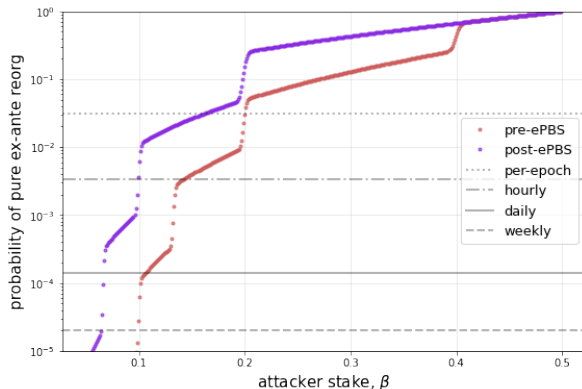A total of 211,902 forked blocks found

Height	Age	Txn	Uncles
17710885	20 mins ago	105	0
17710773	43 mins ago	164	0
17710754	47 mins ago	157	0
17710630	1 hr 12 mins ago	113	0

- Replace *honest builder publication safety*
- With *honest builder same-slot publication safety*
- This is pretty much the model today with `mev-boost`
- Low-Carb Crusader was so effective because it was a *same-slot* unbundling

---

https://ethresear.ch/t/payload-timeliness-committee-ptc-an-epbs-design/16054

Payload-Timeliness Committee
Sketch

new slot anatomy
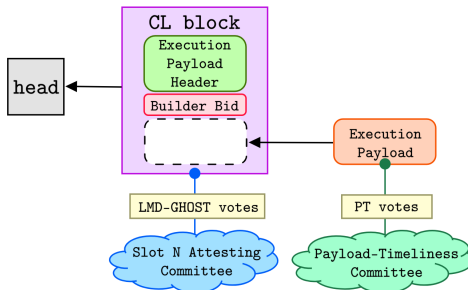
| *block propagation* | *attestation aggregation* | *aggregation & payload propagation* | *payload-timeliness vote propagation* |

an honest proposer broadcasts their block at the start of their slot.

the "attestation deadline" where attesters determine which block they will vote for.

a subset of validators broadcast an aggregate.

builder publishes their execution payload.

payload-timeliness committee votes.

the next proposer publishes their block.

t=t0   t=t1   t=t2   t=t3   t=t4
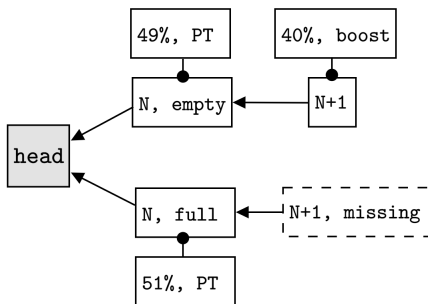
Payload-Timeliness Committee
Sketch

- Consensus-layer block is produced *without* any transactions
- Consensus-layer attestations remain the same
- Builder reveals the payload (list of transactions)
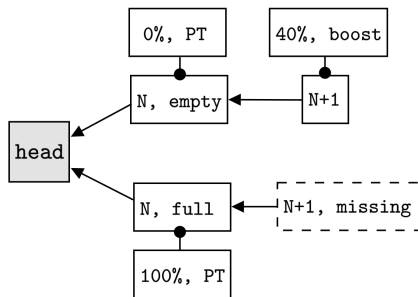- Payload-Timeliness Committee votes on if the payload was published

https://ethresear.ch/t/payload-timeliness-committee-ptc-an-epbs-design/16054

- PTC is split
- Boost gives `N+1` sufficient weight to win the fork

https://ethresear.ch/t/payload-timeliness-committee-ptc-an-epbs-design/16054
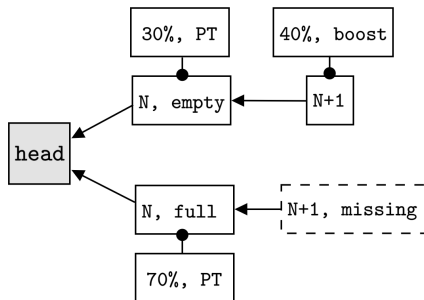
Payload-Timeliness Committee
Case 2

- PTC is in agreement
- `N+1` proposer differs, and gets orphaned as a result

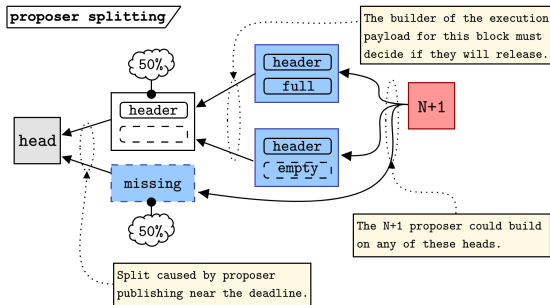# Payload-Timeliness Committee

- PTC is split
- Results in a tie (worst case)
- Hard to get the proposer to disagree with that much of the PTC

---

https://ethresear.ch/t/payload-timeliness-committee-ptc-an-epbs-design/16054

Proposer initiated splitting

- Proposer can grief the builder into a bad decision
  - Publish and run the risk of your block not becoming canonical
  - Do not publish and run the risk of paying for nothing
- … but this is worse today in `mev-boost`

---

https://ethresear.ch/t/payload-timeliness-committee-ptc-an-epbs-design/16054

Juxtaposition
How do these all relate?

- Sub-slot mechanics
  - ▶ Smaller PTC avoids the need for aggregation but weakens the security model slightly
  - ▶ Pipeline next block header publishing
  - ▶ Care needed to avoid giving too much power to the current builder
- Builder fork-choice
  - ▶ Two-slot gives full "proposer-like" privileges to the builder
  - ▶ PTC gives "slot-bounded" fork-choice weight, and is only used to differentiate between empty and full blocks
- PEPC
  - ▶ Gives block-validity enforcement guarantees for the builder
  - ▶ Builder still needs some protection from equivocation