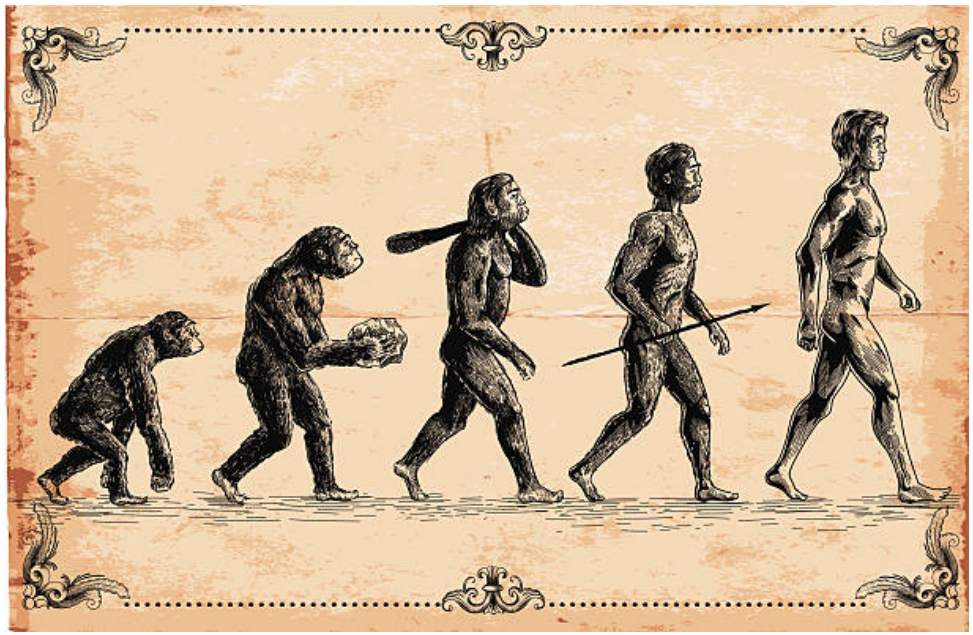
ePBS design evolution

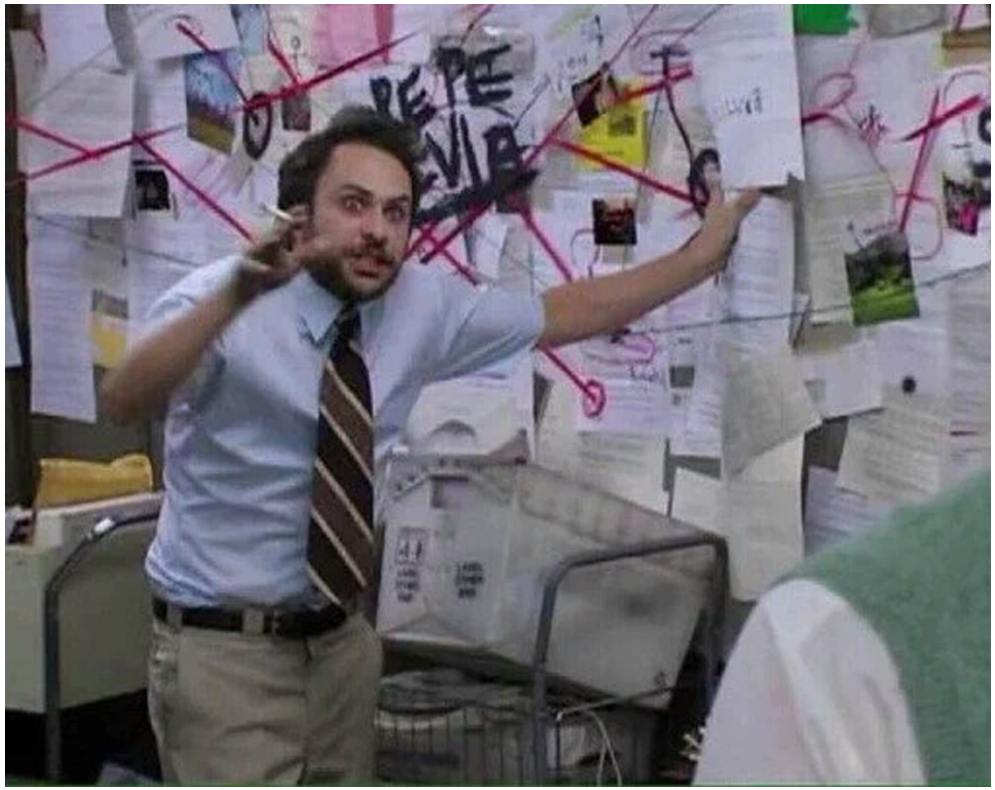


mike neuder – ethereum foundation

pbs.salon – july 17, 2023

Outline

- Desiderata
- Two-slot PBS
  - Sketch
  - Reorgs
- Desiderata pt. II
- Payload Timeliness-Committee
  - Sketch
  - Splitting
- Juxtaposition
  - Sub-slot mechanics
  - Builder fork-choice



Desiderata

https://ethresear.ch/t/why-enshrine-proposer-builder-separation-a-viable-path-to-epbs/15710

Desiderata

- *honest builder publication safety*

https://ethresear.ch/t/why-enshrine-proposer-builder-separation-a-viable-path-to-epbs/15710

Desiderata

- *honest builder publication safety*
- *honest builder payment safety*

https://ethresear.ch/t/why-enshrine-proposer-builder-separation-a-viable-path-to-epbs/15710

Desiderata

- *honest builder publication safety*
- *honest builder payment safety*
- *honest proposer safety*

https://ethresear.ch/t/why-enshrine-proposer-builder-separation-a-viable-path-to-epbs/15710

Desiderata

- *honest builder publication safety*
- *honest builder payment safety*
- *honest proposer safety*
- *permissionlessness*

https://ethresear.ch/t/why-enshrine-proposer-builder-separation-a-viable-path-to-epbs/15710

Desiderata

- *honest builder publication safety*
- *honest builder payment safety*
- *honest proposer safety*
- *permissionlessness*
- *censorship resistance*

https://ethresear.ch/t/why-enshrine-proposer-builder-separation-a-viable-path-to-epbs/15710

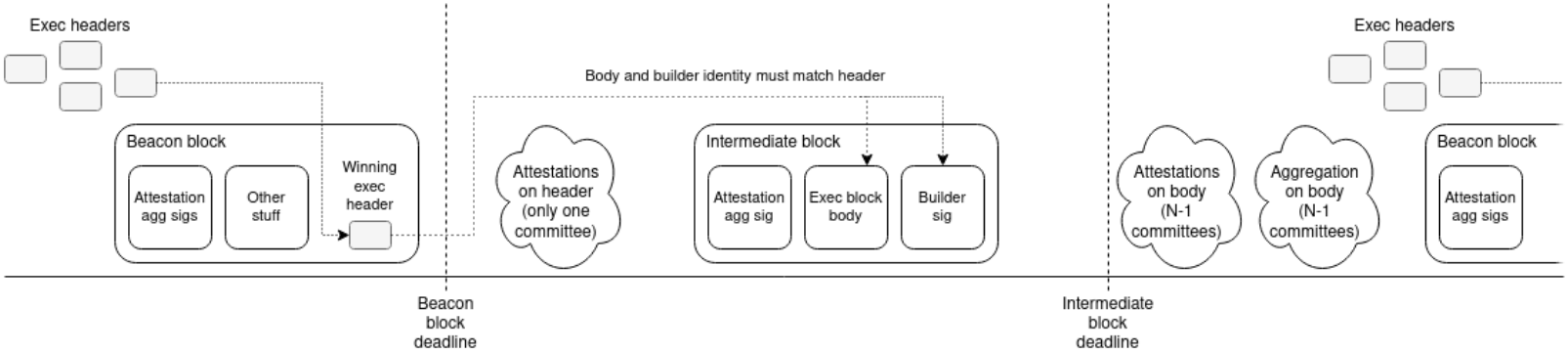
Desiderata

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

https://ethresear.ch/t/why-enshrine-proposer-builder-separation-a-viable-path-to-epbs/15710

Two-slot PBS

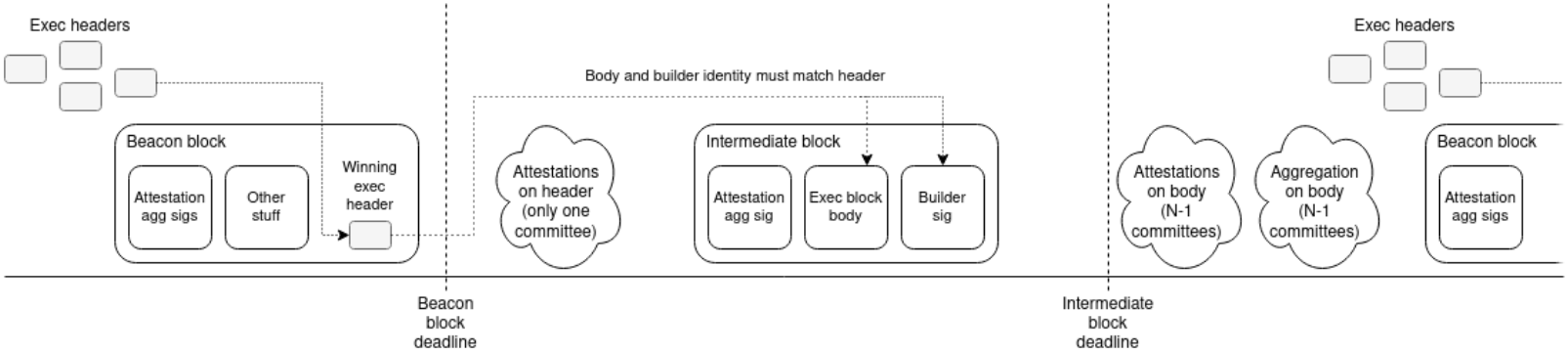
Sketch



https://ethresear.ch/t/two-slot-proposer-builder-separation/10980

Two-slot PBS

Sketch

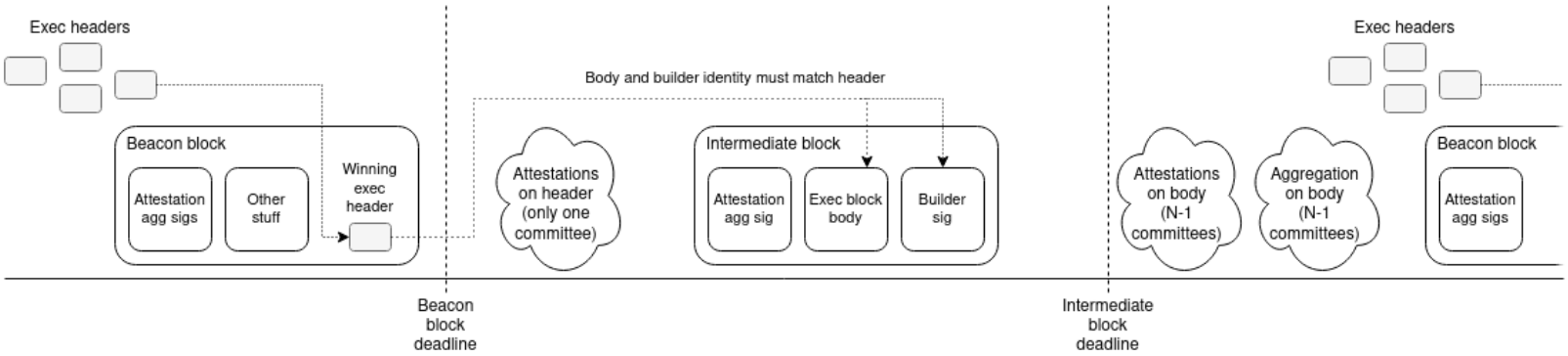


- Original desgin from Vitalik in October 2021

https://ethresear.ch/t/two-slot-proposer-builder-separation/10980

Two-slot PBS

Sketch

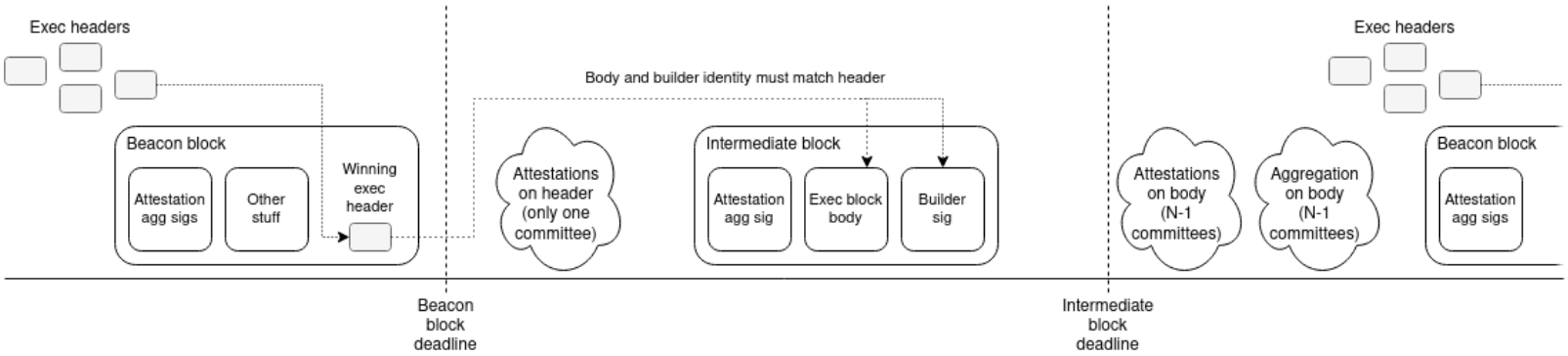


- Original desgin from Vitalik in October 2021
- Partition attesting committee over beacon block and intermediate block

https://ethresear.ch/t/two-slot-proposer-builder-separation/10980

Two-slot PBS

Sketch

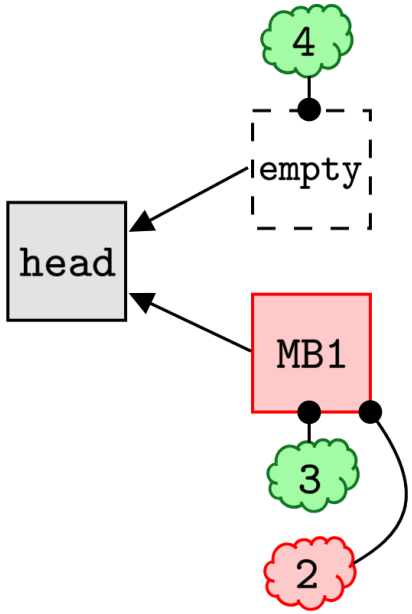


- Original desgin from Vitalik in October 2021
- Partition attesting committee over beacon block and intermediate block
- Became the canonical design. What people referred to when they discussed ePBS

https://ethresear.ch/t/two-slot-proposer-builder-separation/10980

Two-slot PBS

Ex-ante reorg

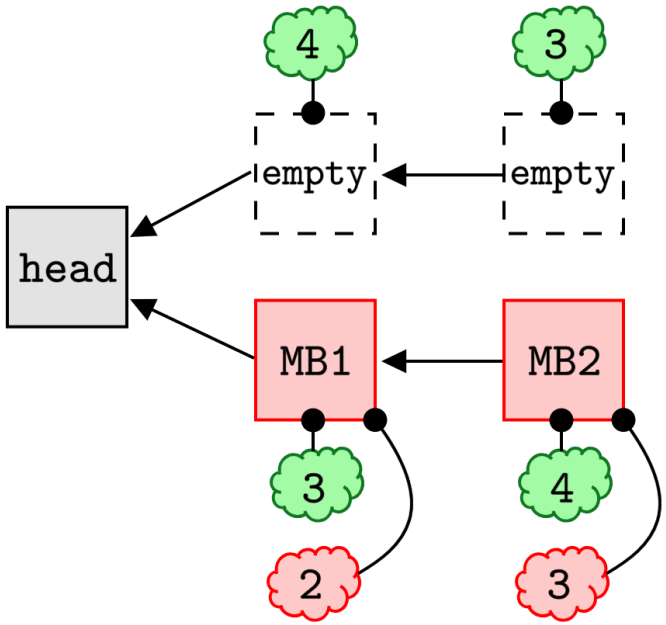


- Malicious proposer splits the honest attesting committee

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

Two-slot PBS

Ex-ante reorg

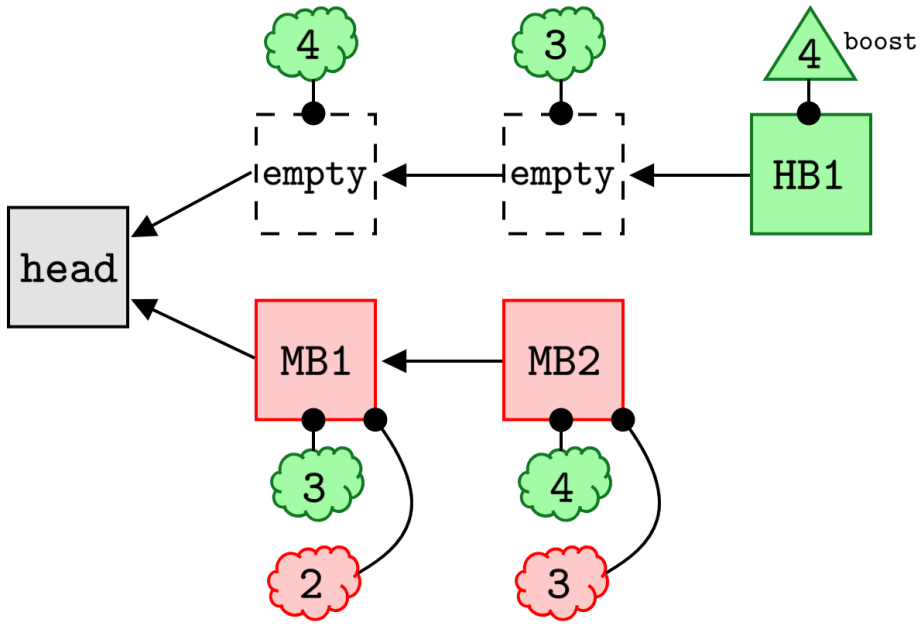


- Malicious proposer splits the honest attesting committee
- Malicious proposer continues the split over a second slot

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

Two-slot PBS

Ex-ante reorg

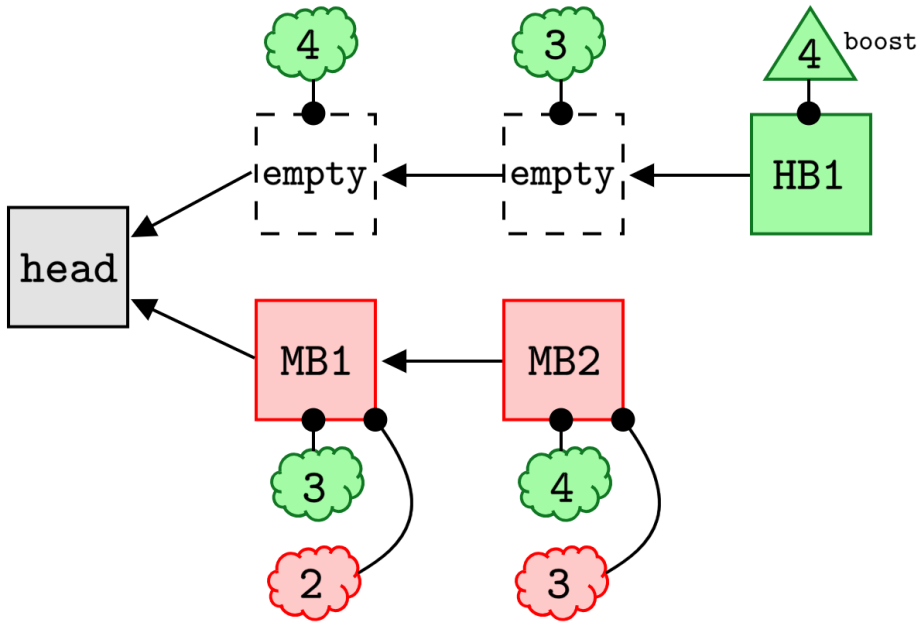


- Malicious proposer splits the honest attesting committee
- Malicious proposer continues the split over a second slot
- Honest proposer builds on the empty chain

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

Two-slot PBS

Ex-ante reorg

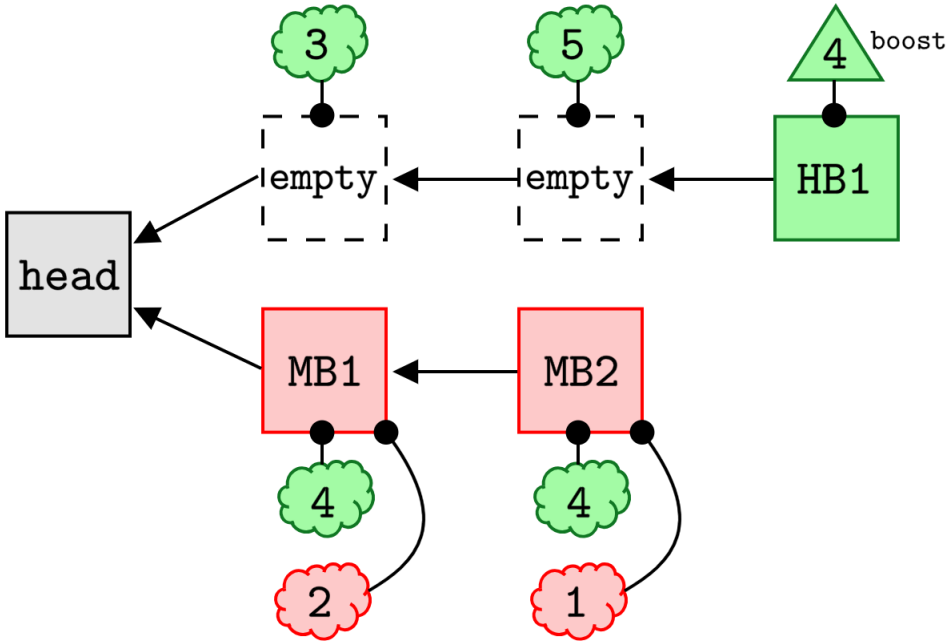


- Malicious proposer splits the honest attesting committee
- Malicious proposer continues the split over a second slot
- Honest proposer builds on the empty chain
- Malicious proposer releases private attestations, orphaning HB1

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

Two-slot PBS

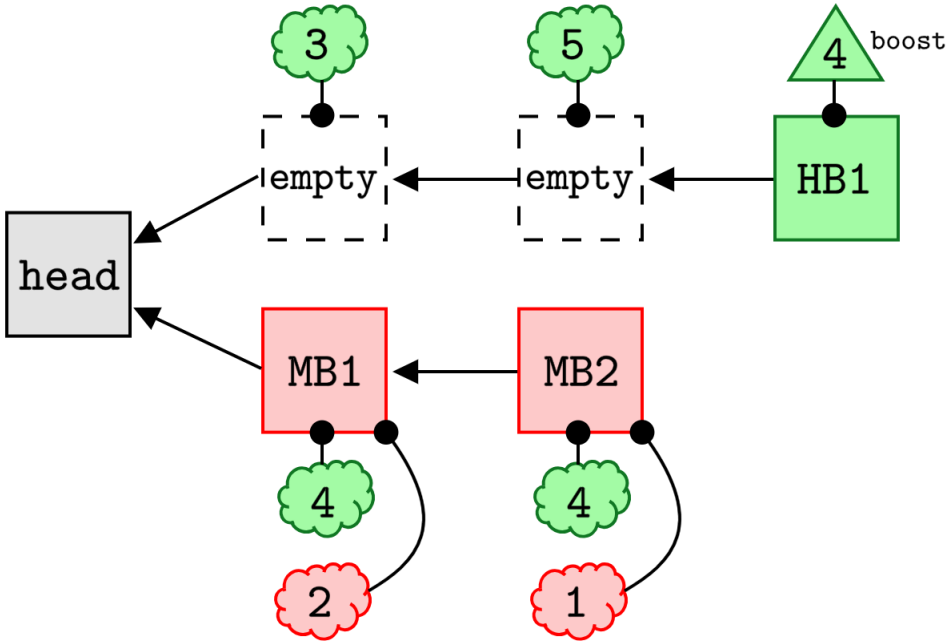
Reorgs



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

Two-slot PBS

Reorgs

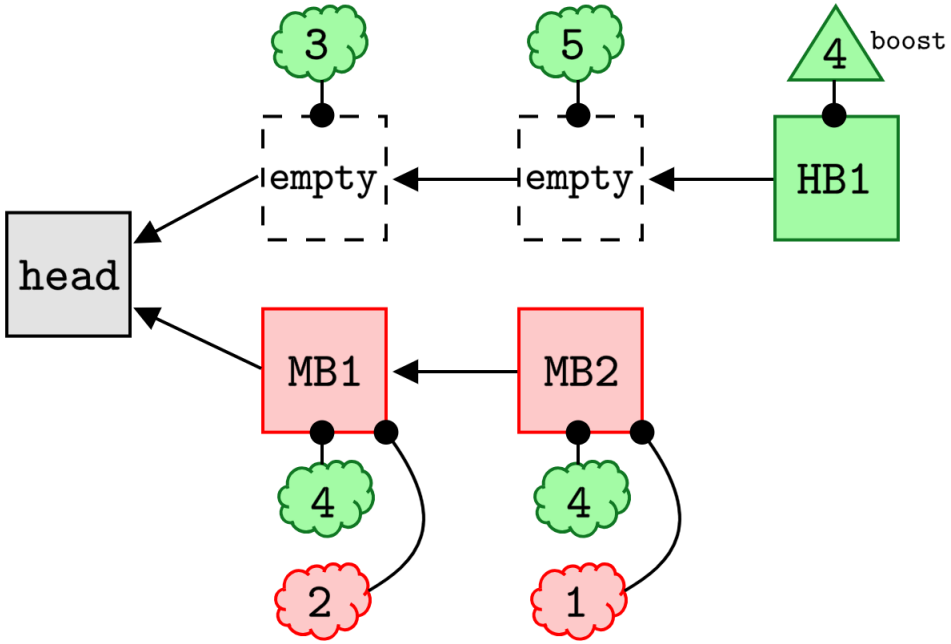


- Malicious proposer still controls two slots, but not enough attestations to beat proposer boost

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

Two-slot PBS

Reorgs

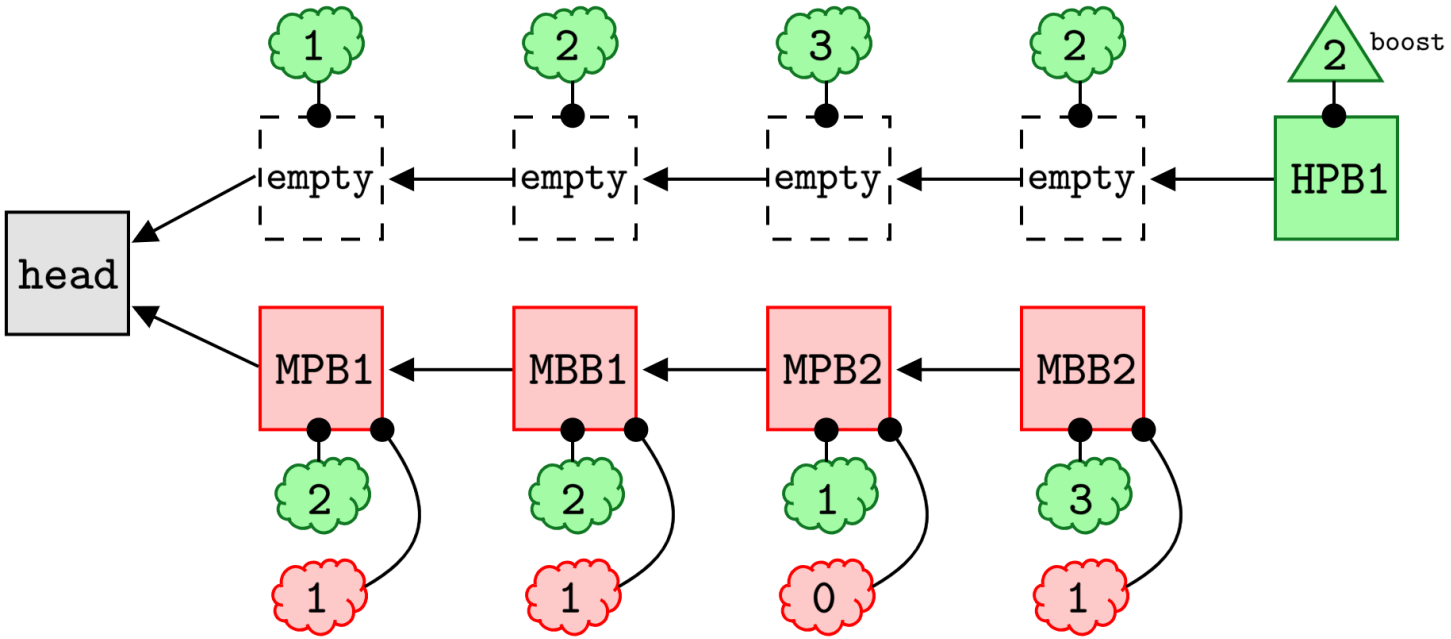


- Malicious proposer still controls two slots, but not enough attestations to beat proposer boost
- No ex-ante reorg possible in this case

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

Two-slot PBS

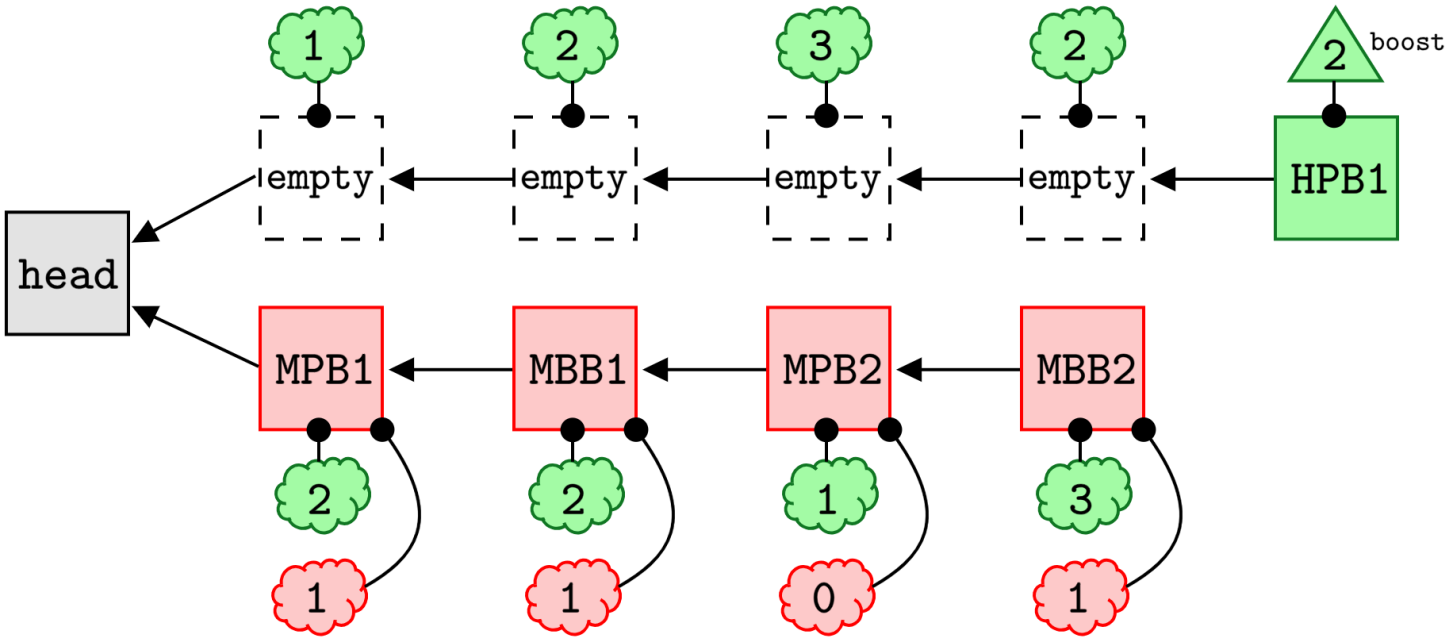
Reorgs



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

Two-slot PBS

Reorgs

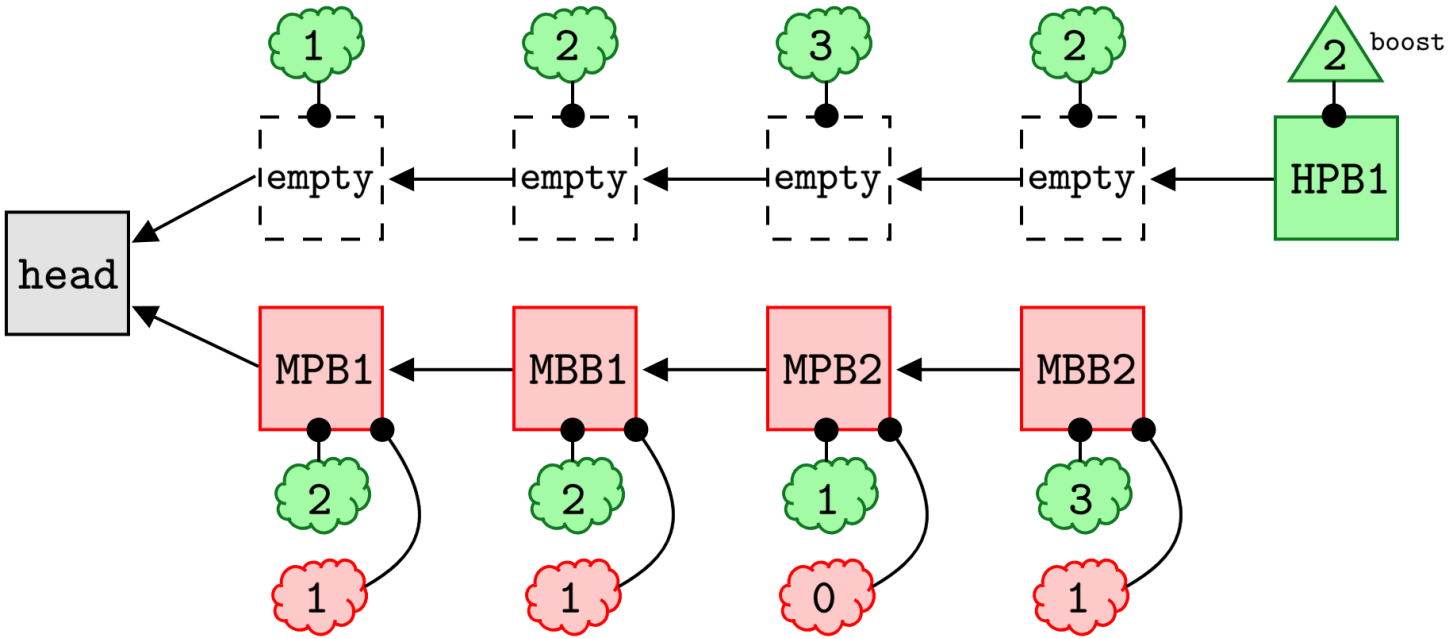


- Same allocation as before

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

Two-slot PBS

Reorgs

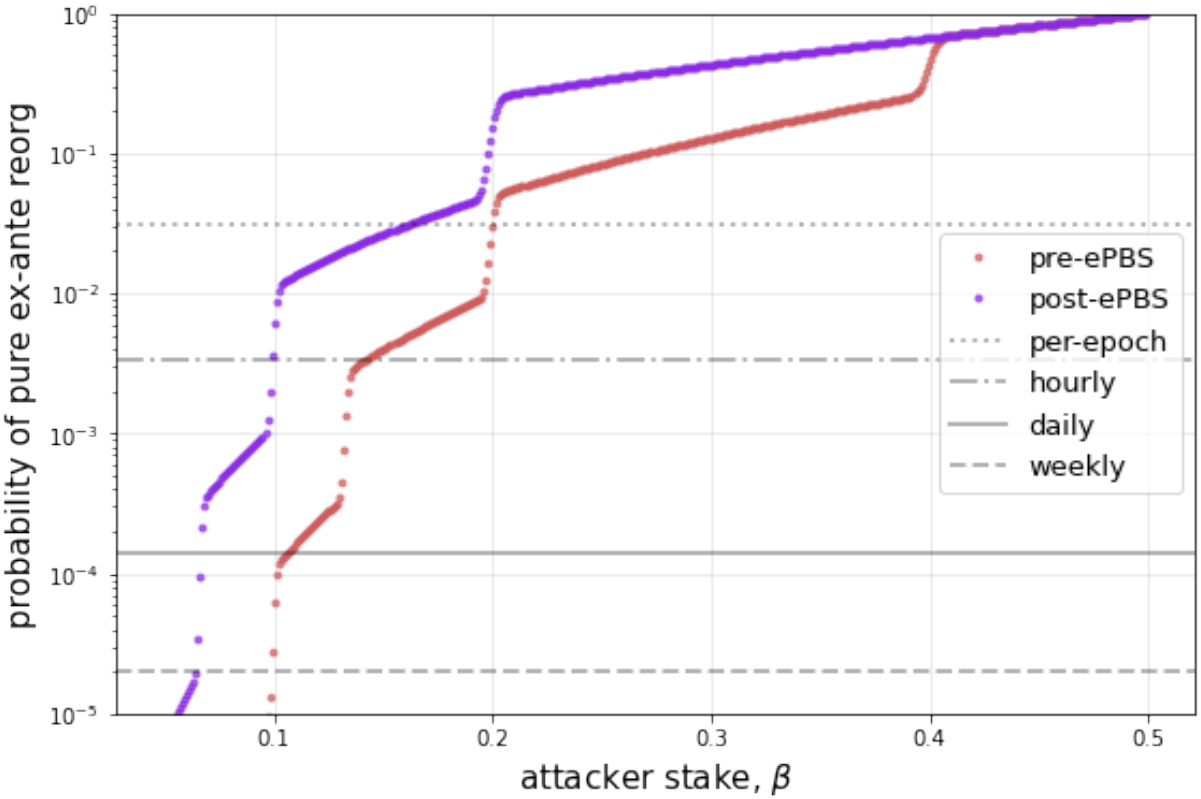


- Same allocation as before
- The ex-ante reorg *is possible* because the proposer boost is weaker

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

Two-slot PBS

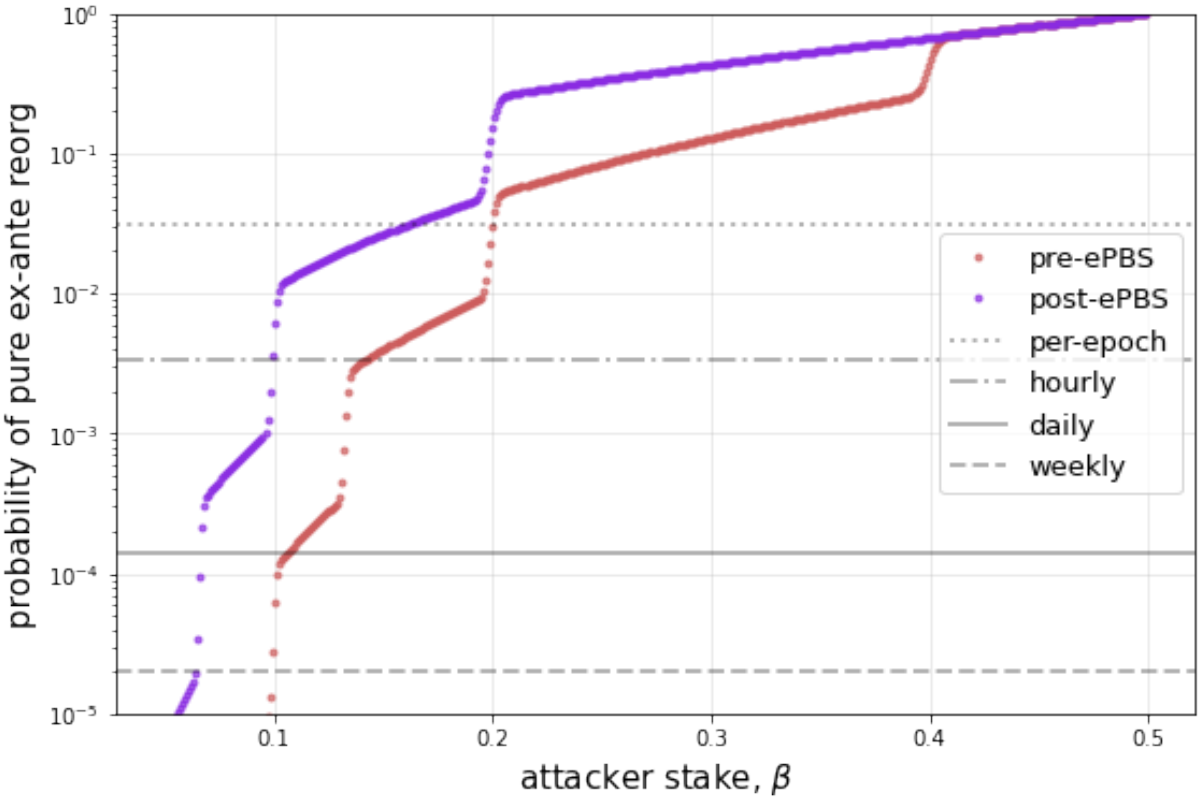
Reorg probabilities



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

Two-slot PBS

Reorg probabilities

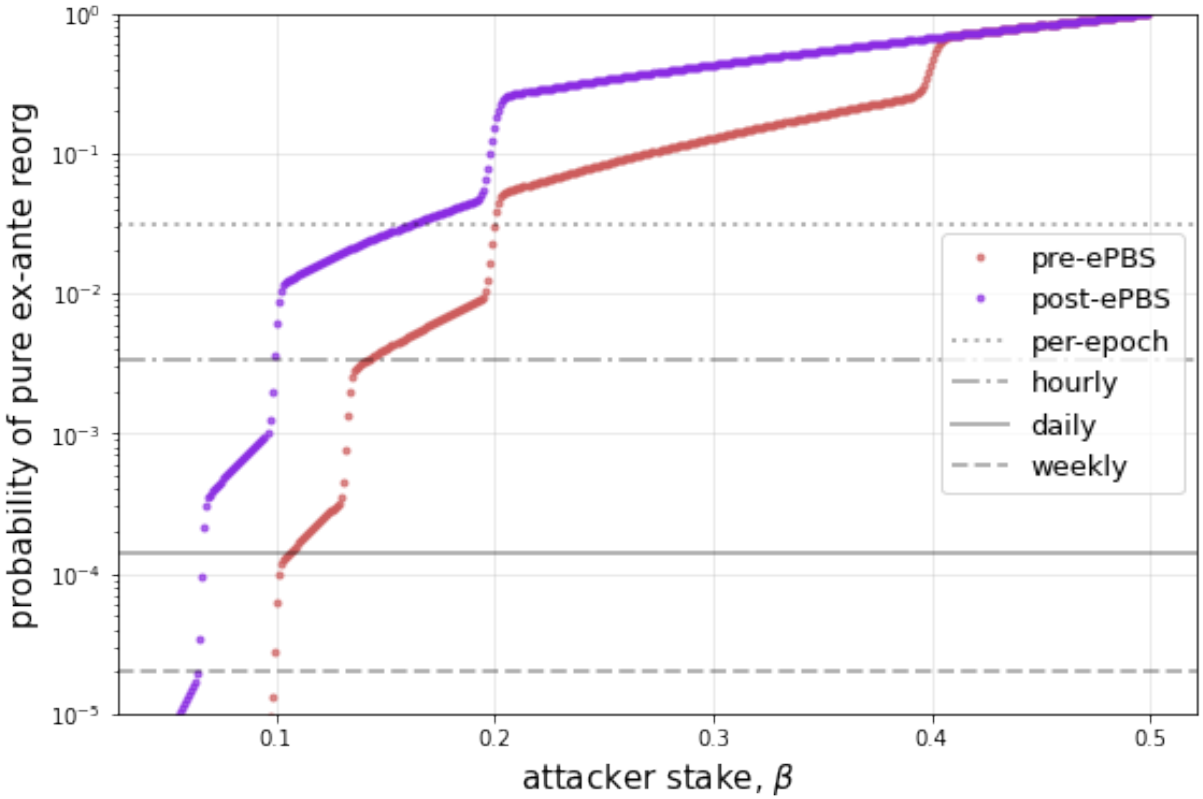


- Just ex-ante reorg probabilities, lower bound on all reorgs

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

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

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

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*

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

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*

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

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`

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

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

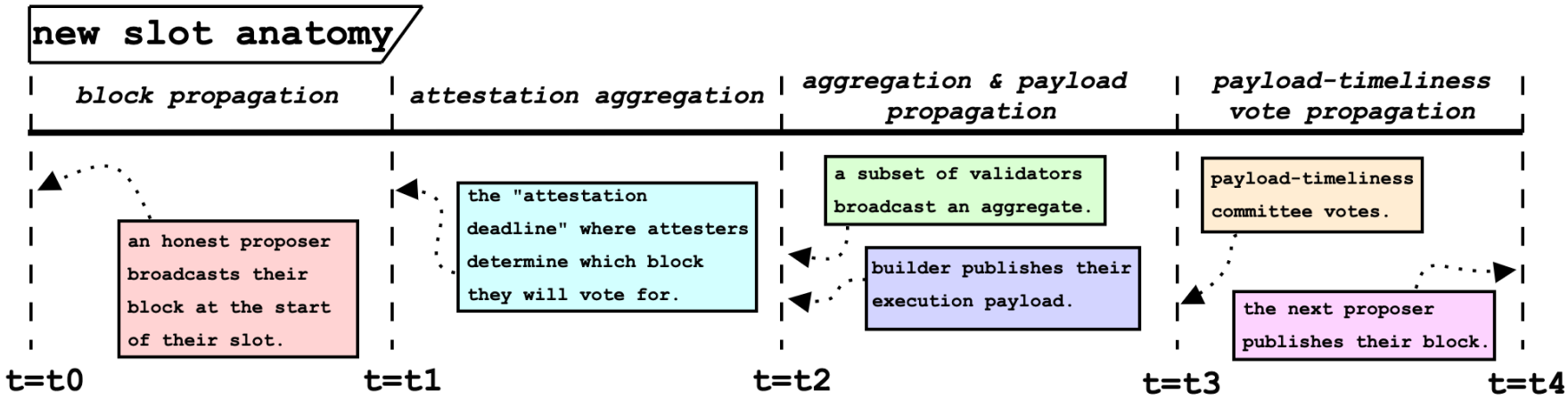
- Replace *honest builder publication safety*
- With *honest builder same-slot publication safety*
- This is pretty much the model today with `mev-boost`
- Low-Carb Crusader was so effective because it was a *same-slot* unbundling

---

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

Payload-Timeliness Committee

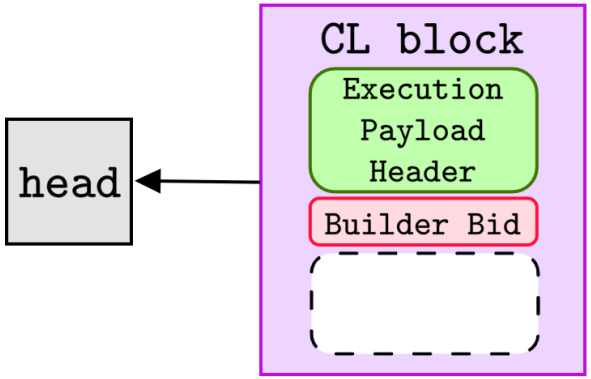
Sketch



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

Payload-Timeliness Committee

Sketch

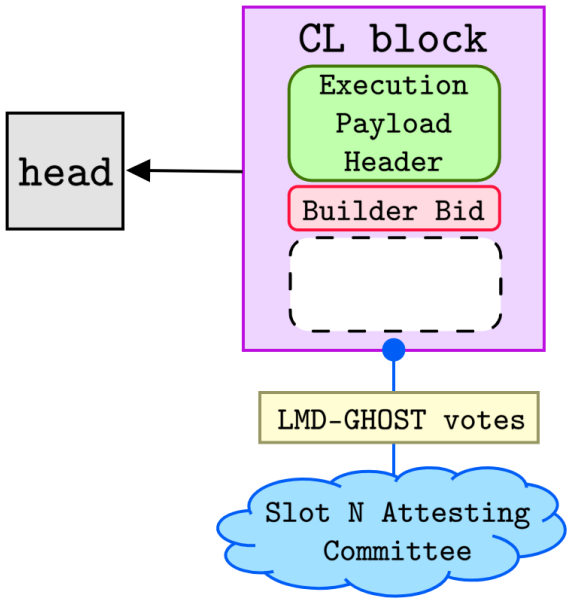


- Consensus-layer block is produced *without* any transactions

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

Payload-Timeliness Committee

Sketch

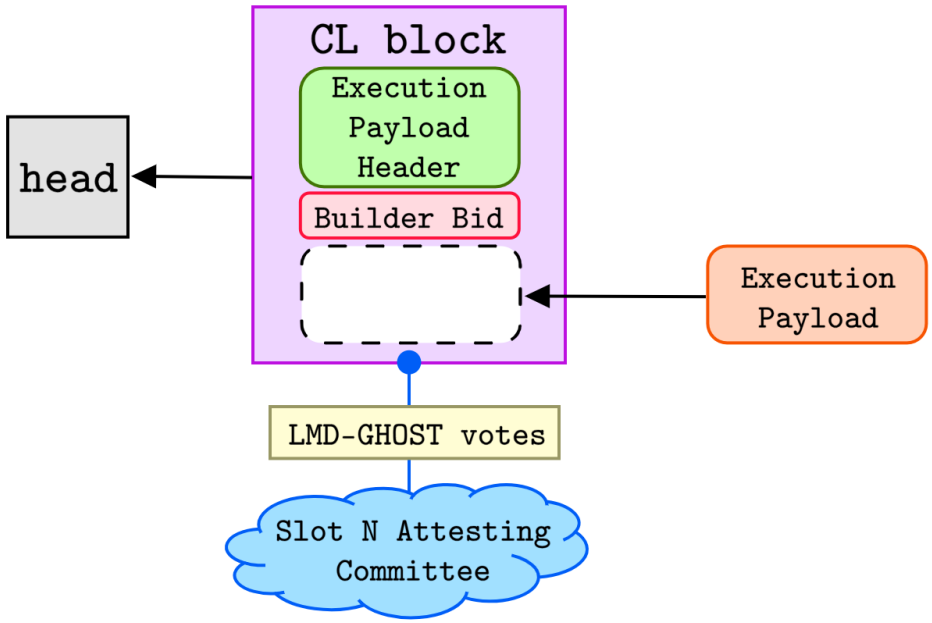


- Consensus-layer block is produced *without* any transactions
- Consensus-layer attestations remain the same

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

Payload-Timeliness Committee

Sketch

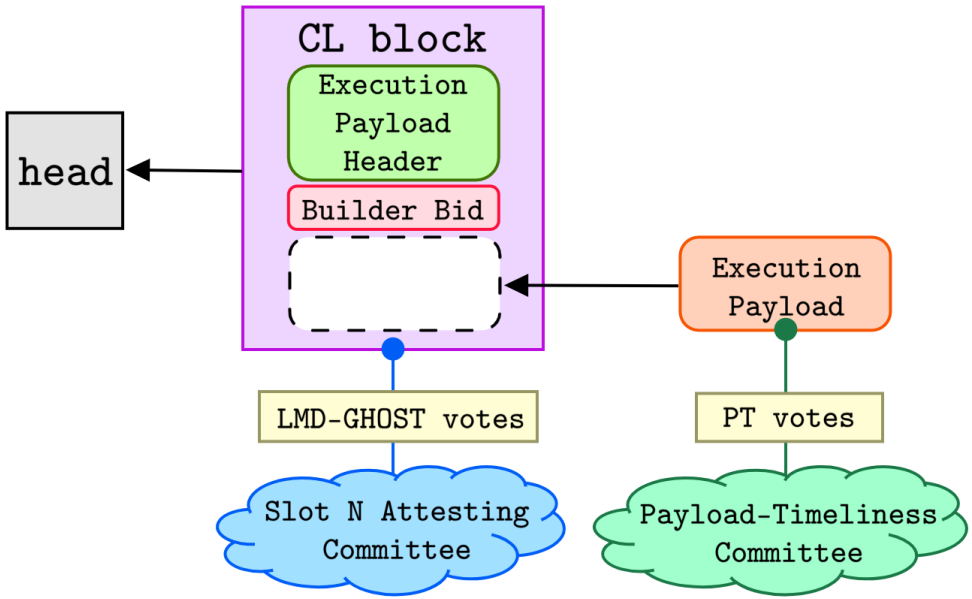


- Consensus-layer block is produced *without* any transactions
- Consensus-layer attestations remain the same
- Builder reveals the payload (list of transactions)

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

Payload-Timeliness Committee

Sketch

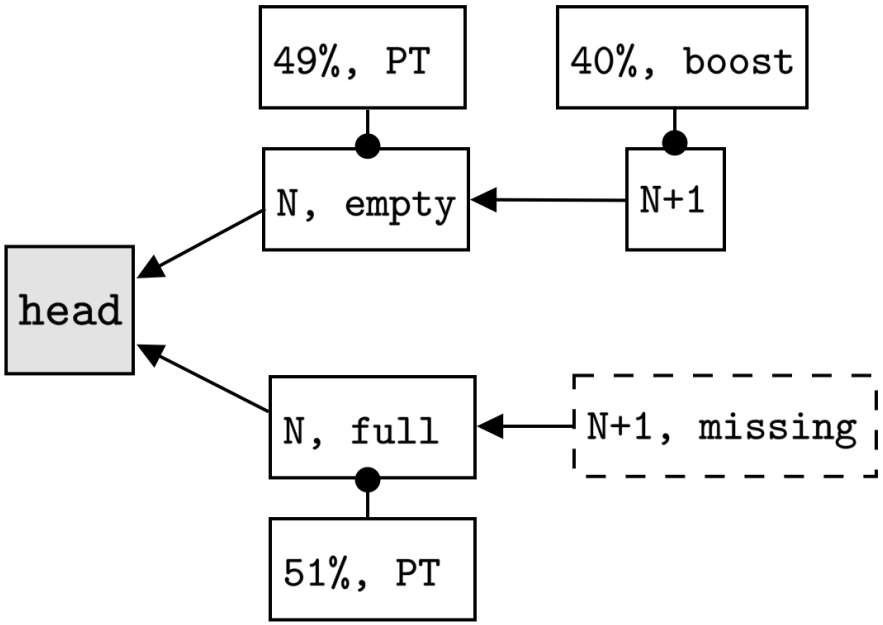


- Consensus-layer block is produced *without* any transactions
- Consensus-layer attestations remain the same
- Builder reveals the payload (list of transactions)
- Payload-Timeliness Committee votes on if the payload was published

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

Payload-Timeliness Committee

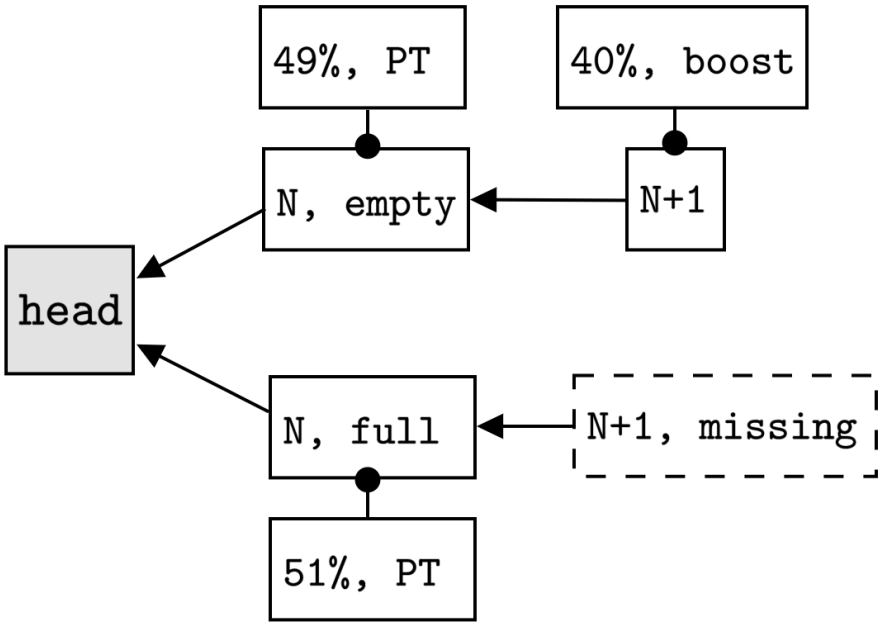
Case 1



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

Payload-Timeliness Committee

Case 1

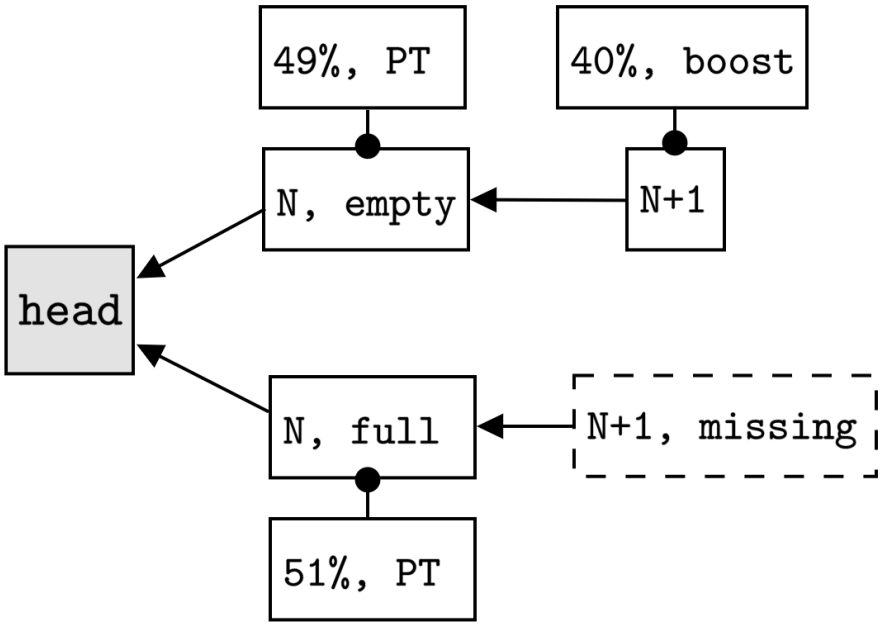


- PTC is split

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

Payload-Timeliness Committee

Case 1

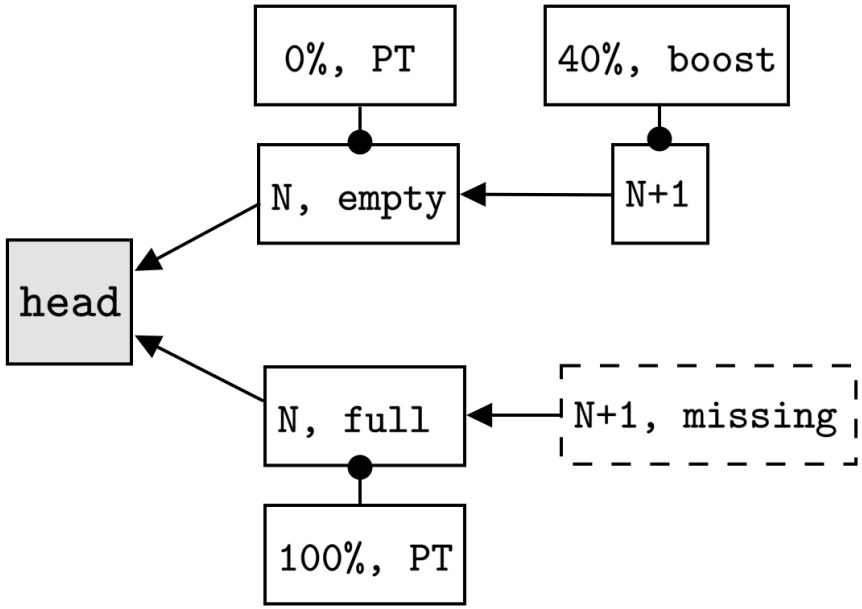


- PTC is split
- Boost gives N+1 sufficient weight to win the fork

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

Payload-Timeliness Committee

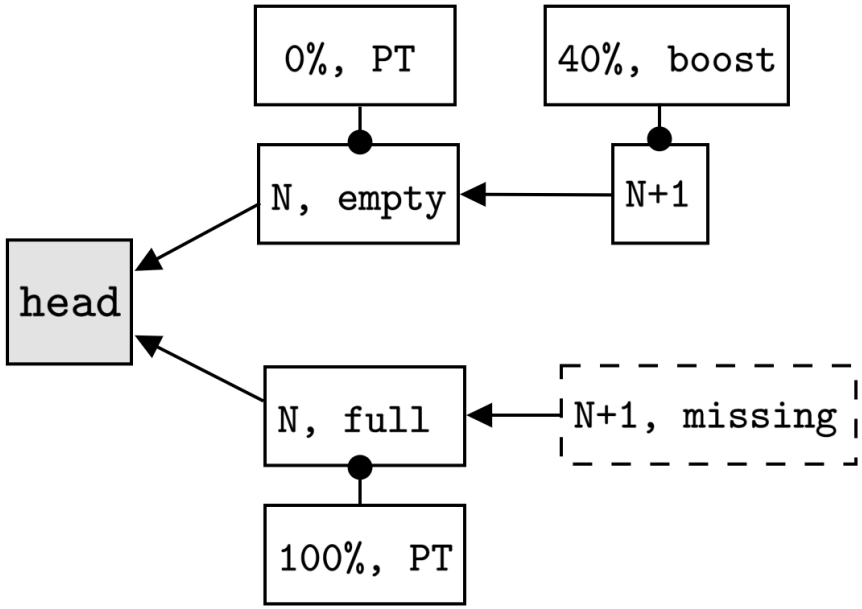
Case 2



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

Payload-Timeliness Committee

Case 2

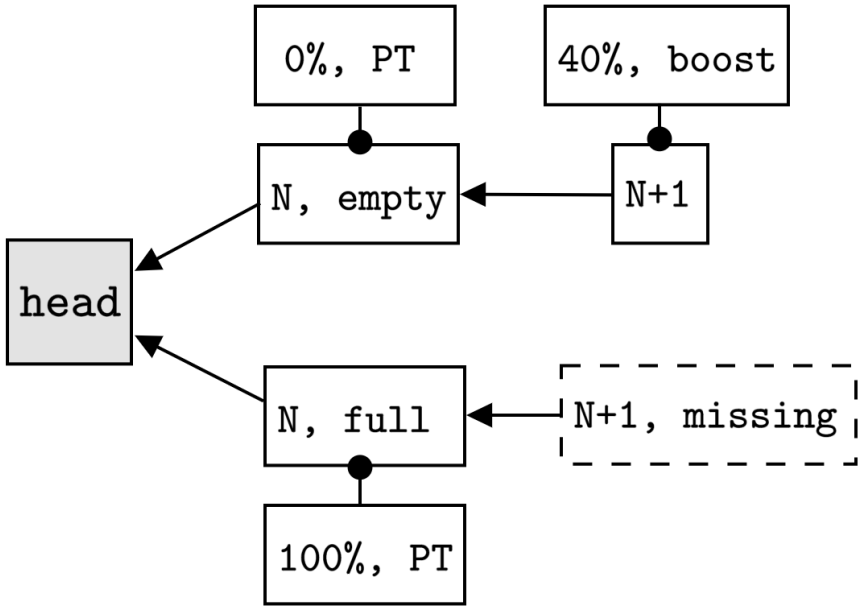


- PTC is in agreement

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

Payload-Timeliness Committee

Case 2

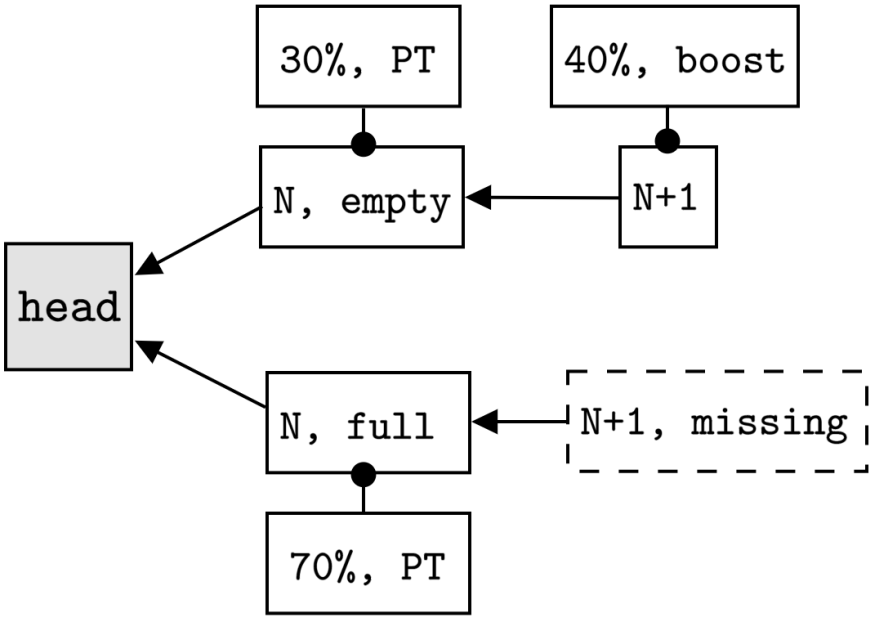


- PTC is in agreement
- N+1 proposer differs, and gets orphaned as a result

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

Payload-Timeliness Committee

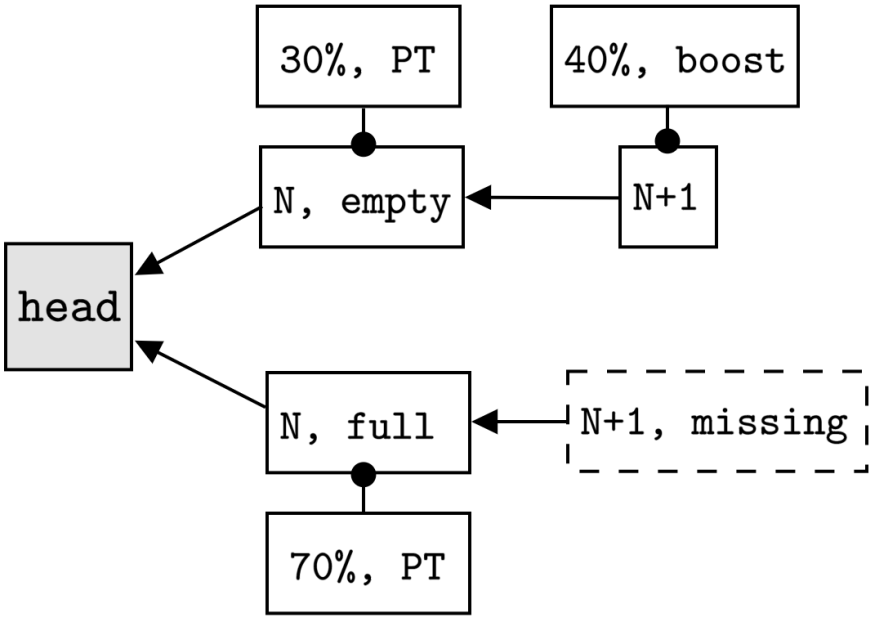
Case 3



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

Payload-Timeliness Committee

Case 3

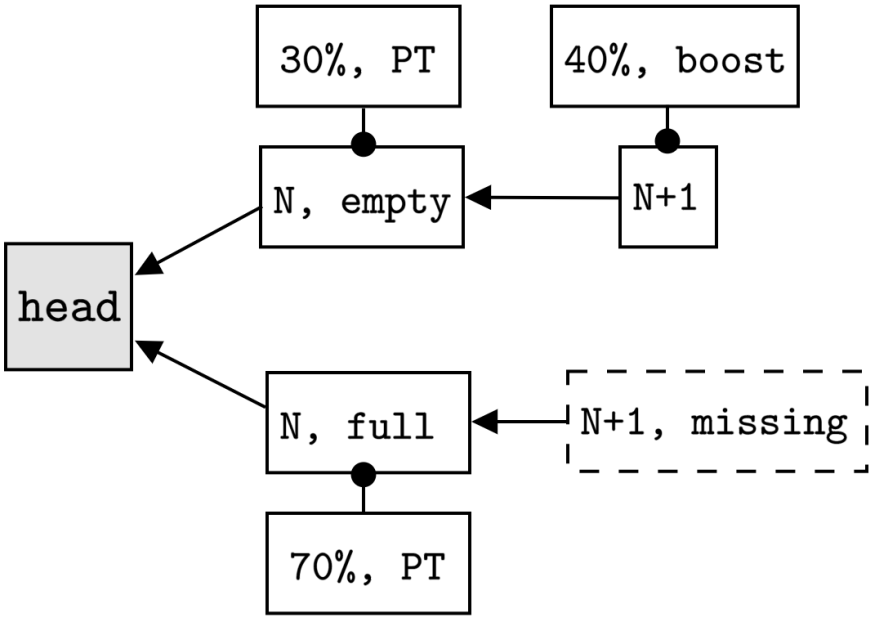


- PTC is split

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

Payload-Timeliness Committee

Case 3

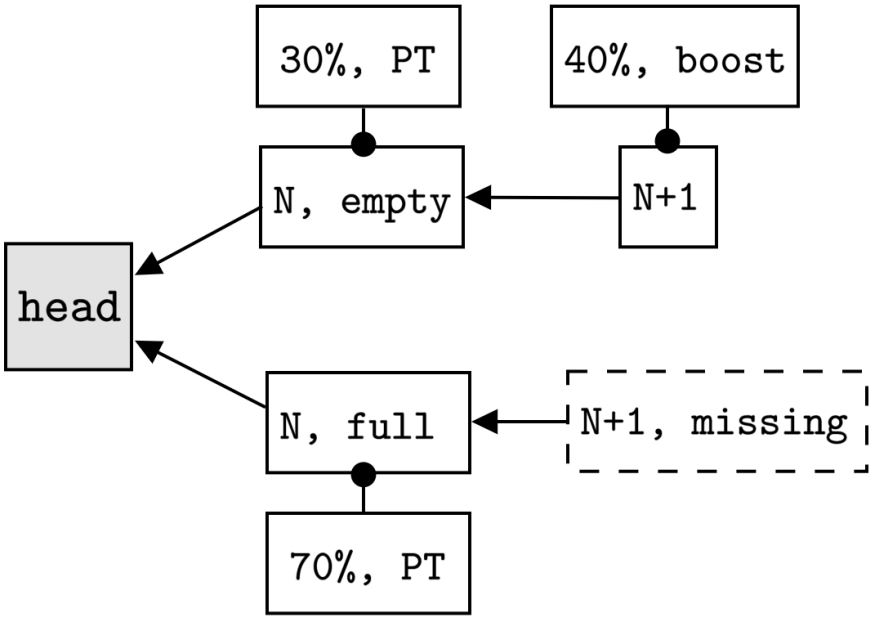


- PTC is split
- Results in a tie (worst case)

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

Payload-Timeliness Committee

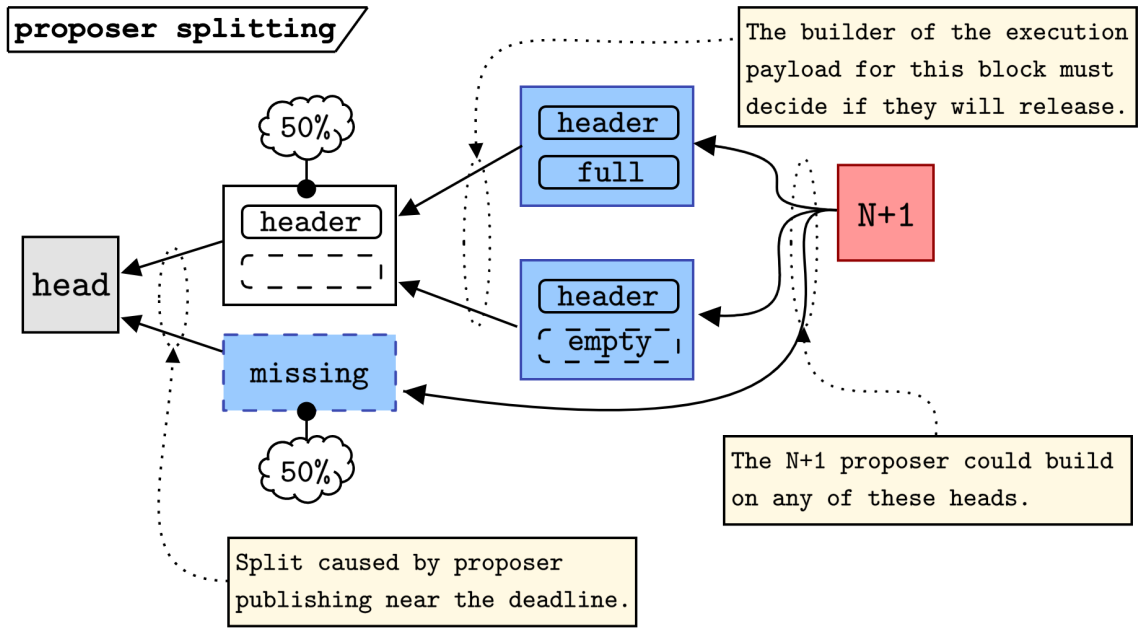
Case 3



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

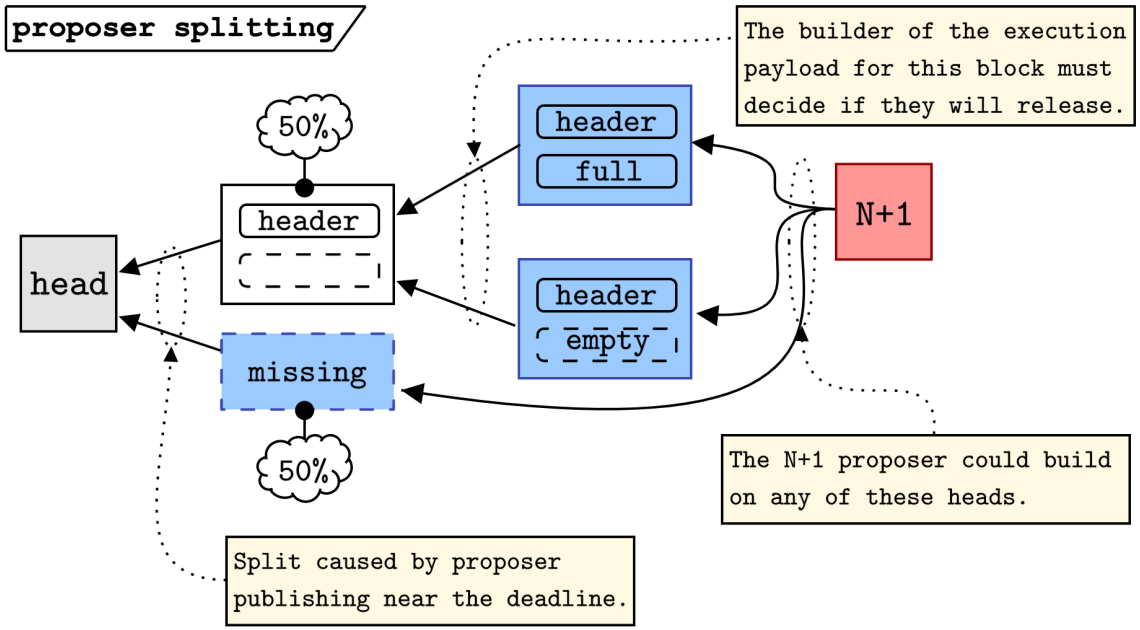
https://ethresear.ch/t/payload-timeliness-committee-ptc-an-epbs-design/16054

Proposer initiated splitting



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

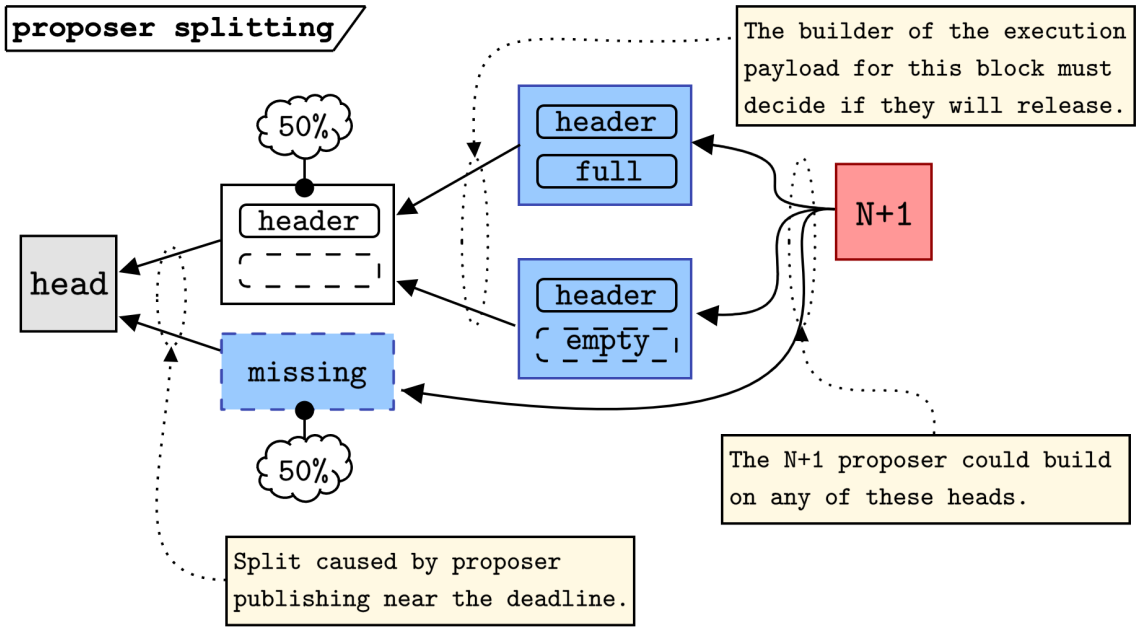
Proposer initiated splitting



- Proposer can grief the builder into a bad decision

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

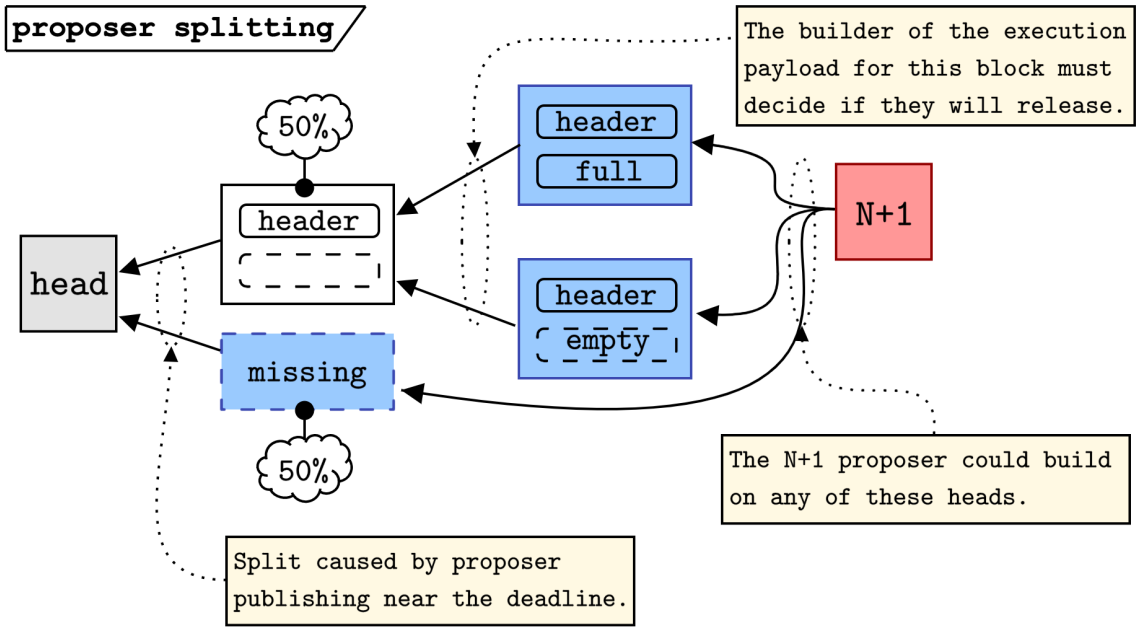
Proposer initiated splitting



- Proposer can grief the builder into a bad decision
  - Publish and run the risk of your block not becoming canonical

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

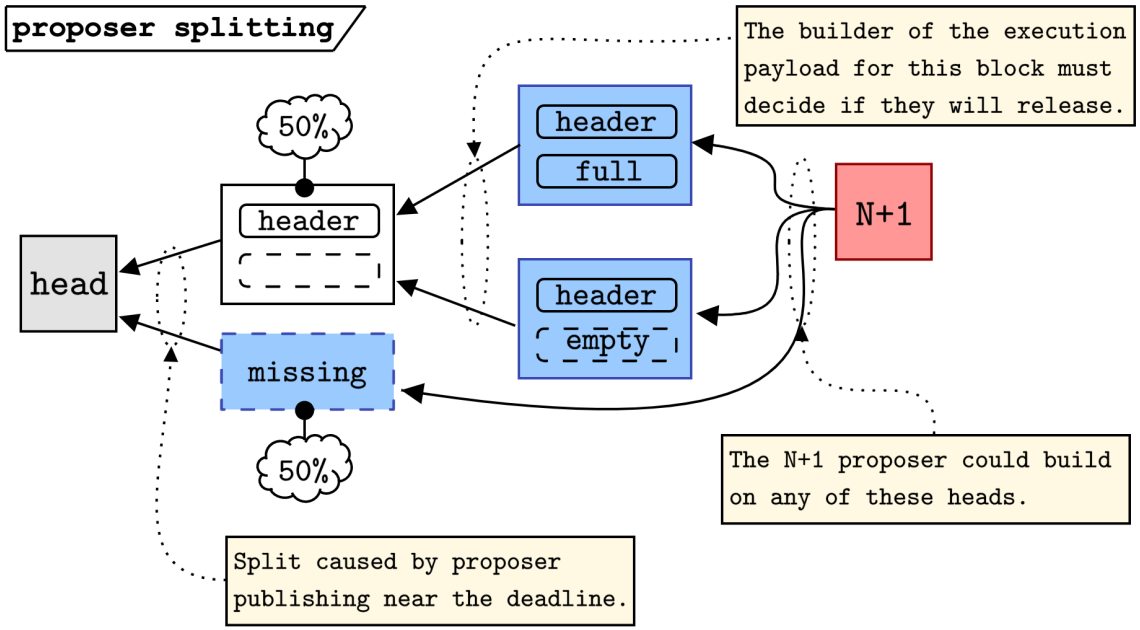
Proposer initiated splitting



- 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

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

https://i-should-write-something-on-this-lol

Juxtaposition

How do these all relate?

- Sub-slot mechanics
  - Smaller PTC avoids the need for aggregation but weakens the security model slightly

https://i-should-write-something-on-this-lol

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

https://i-should-write-something-on-this-lol

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

https://i-should-write-something-on-this-lol

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

https://i-should-write-something-on-this-lol

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

https://i-should-write-something-on-this-lol

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

https://i-should-write-something-on-this-lol

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

https://i-should-write-something-on-this-lol

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

https://i-should-write-something-on-this-lol

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

https://i-should-write-something-on-this-lol