

Why it's hard to enshrine Proposer-Builder Separation...



Mike Neuder – Ethereum Foundation
Columbia Center for Digital Finance and Technologies Annual Summit
December 1, 2023

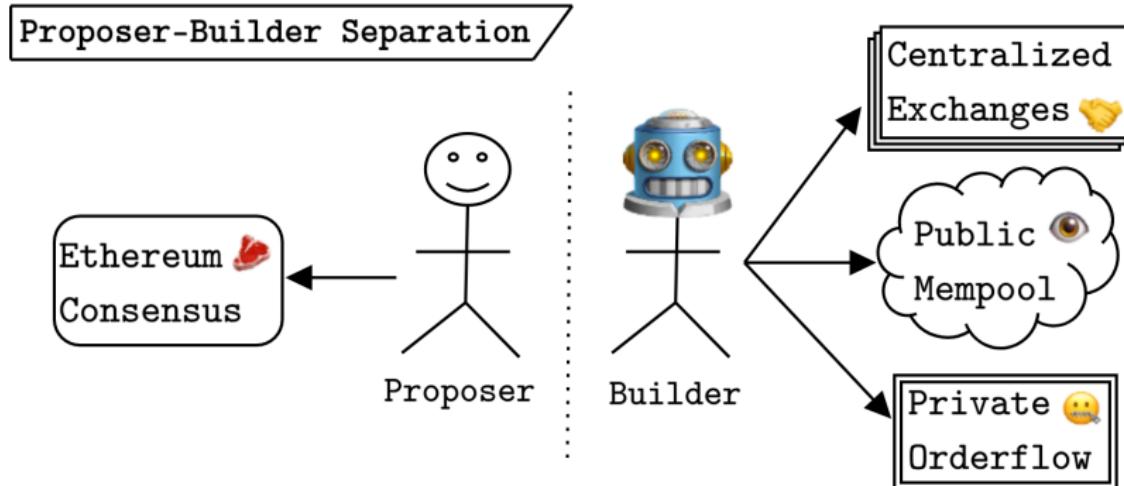
Outline

- What we are trying to do...
 - What is PBS?
 - What is out-of-protocol PBS?
 - What is in-protocol PBS?
 - “Simplest” ePBS instantiation.
- What would actually happen...
 - Bypassability and relay advantages.
 - “Trustless” relays?
 - Cryptographic enhancements.



What we are trying to do...

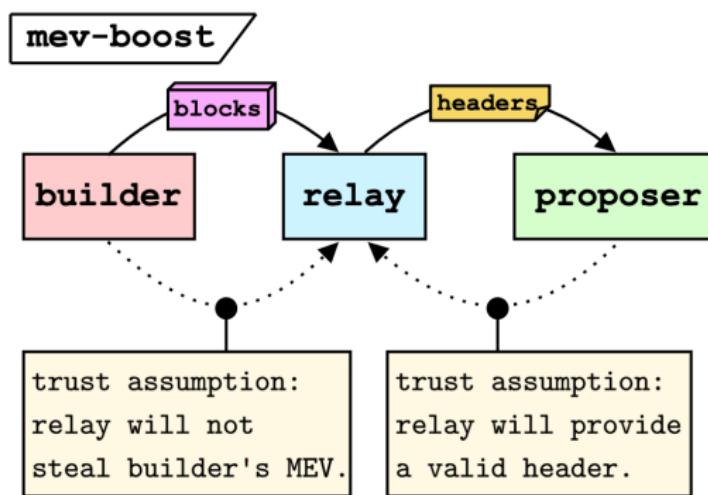
What is PBS?



- The proposer is a validator in the Proof-of-Stake system.
- The builder is a sophisticated actor positioned to extract value from transaction ordering.
- These are very distinct roles.

What we are trying to do...

What is out-of-protocol PBS?



- Relay serves as a mutually trusted auctioneer.
- Validators run sidecar software to interact with relays.
- Massive adoption: 95% of blocks are built using mev-boost.

What we are trying to do...

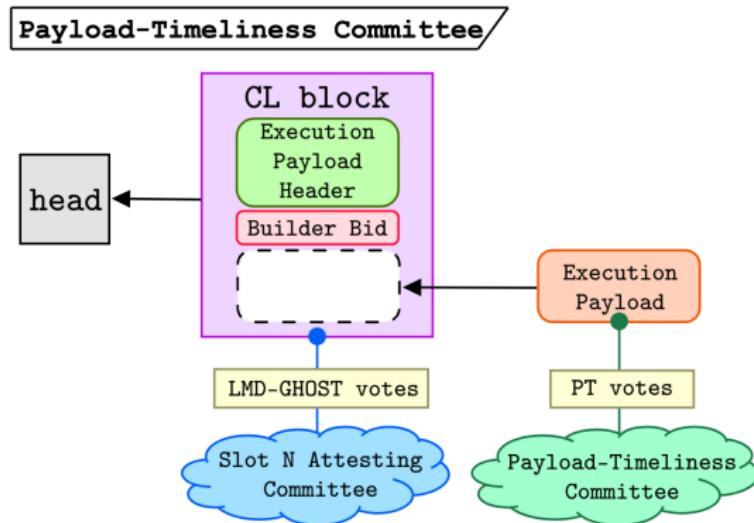
What is in-protocol PBS?



- **Goal:** get rid of relays.
- Two features of a PBS system...
 - ▶ *Commit-reveal* to protect builder.
 - ▶ *Unconditional payment* to protect proposer.

What we are trying to do...

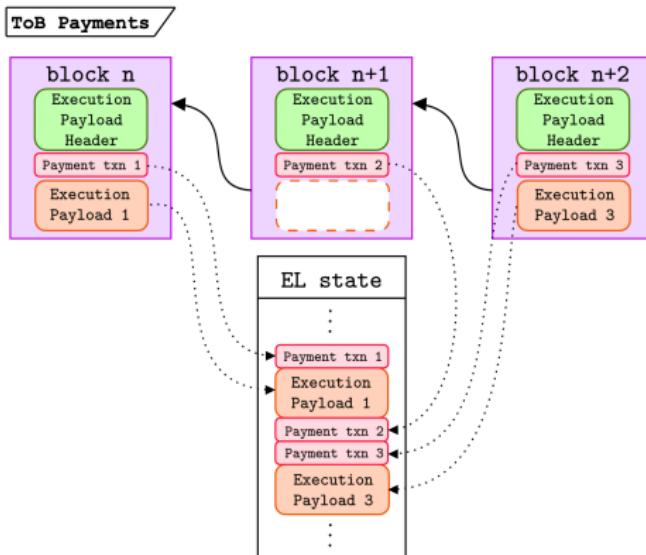
"Simplest" ePBS instantiation. (1/2)



- *Commit-reveal* with a payload-timeliness committee.

What we are trying to do...

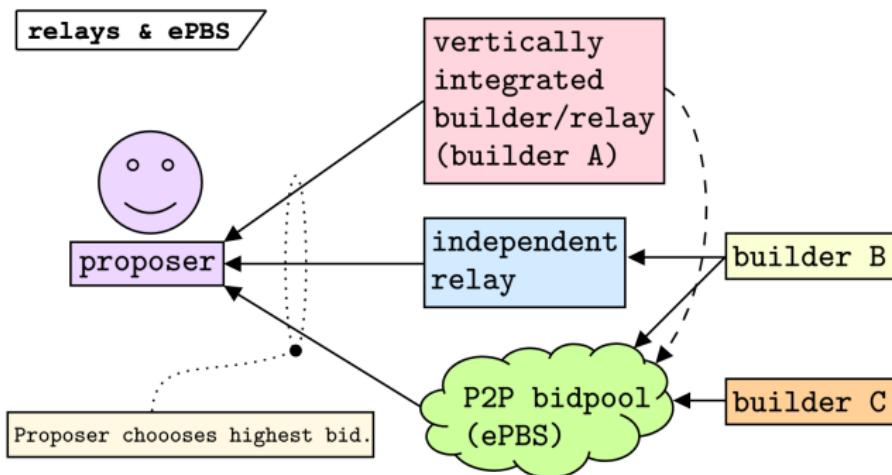
"Simplest" ePBS instantiation. (2/2)



- *Unconditional payment* with Top-of-Block payments.

What would actually happen...

Bypassability and relay advantages.

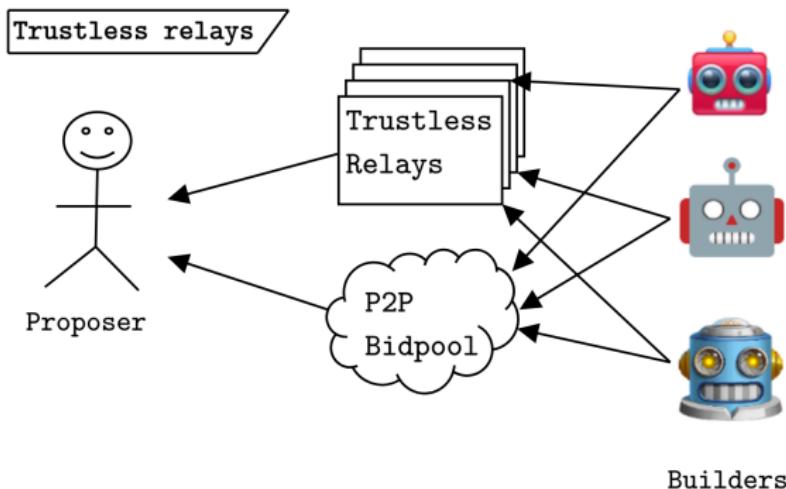


- **Relay advantages.**

- ▶ Lower liquidity requirements.
- ▶ Reduced latency.
- ▶ *Perhaps the most important:* bid cancellations.

What would actually happen...

"Trustless relays".



- Components of a “trustless relay”.

- ▶ No trust on either end.
- ▶ Only used as a *networking accelerator*.
- ▶ Probably could be called something else all together ... “forwarder” ?

What would actually happen...

Cryptographic enhancements.

Cryptographic enhancements

Encrypted
block



Bid validity
ZK proof

Decryption
method



- A lot of ifs...

thanks! :-)



PBS is an infinite buffet!

reach out if you are hungry – @mikeneuder on tg and twitter.