Brief Description

Currently (July 2023), PBS runs only with open bids and only on Ethereum. This has several downsides like heightened traffic and undesirable impact on block building market structure (more details below). Is it possible to run a PBS block-auction with private bids for Ethereum which operates within the desired latency and does not impose additional liveness or trust assumptions on the ecosystem? What about non-Ethereum settings such as L2s with single sequencers?

More details and discussion

The brief description of why private block bidding is desirable in PBS as it relates to market structure:

We have observed that the driving force behind concentration of the block builder market on Ethereum comes from the fact that searchers are unwilling to share their order flow with all builders. This happens for several reasons. One of these reasons is that it is difficult to estimate how much a bundle should be bidding (when you cannot see your competitors bid). Because the block bidding process is public, it is easier for a searcher to only include bundles in their own blocks and adjust the bids of the blocks. Private bidding addresses this asymmetry, as part of a larger effort to make bundle-sharing a dominant strategy. A smaller benefit is that latency should matter slightly less given that the rapid one-upping bidding dynamic should fall away.

The auction is very latency sensitive so if a solution introduces a lot more latency, people may not use it. (unclear how much is too much, definitely <250ms).

This problem also requires privacy from the proposer as well since the proposer may be incentivised to share bids they have received, perhaps with partners who give some guarantees about exceeding bids. (Whether there is incentive to do this is an incentives question as well).

Questions:

- Is it possible to run a PBS block-auction with private bids for Ethereum which operates within the desired latency and does not impose additional liveness or trust assumptions on the ecosystem?
- What about non-Ethereum settings such as L2s with single sequencers?

Approaches suggested so far:

- MPC (too slow)
- Threshold encrypted bids to attesting committee (slow on its own and imposes liveness assumptions)
- FHE accumulator which keeps track of highest bid without revealing how much it is. Unclear how decryption works, maybe VDFs?

Relevant links and resources

Latest in-protocol PBS design

An impractical, but cool MPC auction