Pre-execution privacy is a broad and ill-defined concept. In the case of PBS in Ethereum, PBS has been/is being designed such that builders do not have to trust proposers in order to interact with them. This prevents there being a size/trust-based barrier to entry for homestakers. Initially, MEV-boost leveraged Eth staking and slashing as a mechanism to enforce a commitment in a commit-and-reveal scheme.

However, unbundling attacks emphasised the inadequacy of such means as the MEV available is unbounded and can easily exceed deposited collateral. Ethereum's most-recently proposed plan to more strongly enforce commitment to block-inclusion is to leverage a decentralised committee and enshrine PBS as part of the core protocol. The tradeoffs of such an approach have yet to be fully analysed. For example, the proposed design gives the winning builder a headstart in knowing what the next state of the chain will be and an incentive to delay revelation of that state as long as possible. This constitutes a research direction in itself.

In considering domains other than Ethereum, we realise there may be other dynamics at play. For example, there may be no decentralised committee to leverage (such as the case with a single sequencer in a rollup) or the consensus protocol might be less/more amenable to an in-protocol PBS design.

Questions:

- What commitment schemes are available for a given domain or class of domains (like single sequencer rollups to Ethereum)? What are the tradeoffs to these commitment schemes? For example, do/can L1 contracts be used to slash/race sequencers who double sign?
- What are the tradeoffs of Ethereums proposed design? For example, this precludesprivate bidding.