In this initial implementation of PBS (mev-boost), to prevent things like front-running, censorship, and unauthorized data sharing, each party has to trust the parties to which they connect. When PBS is [built natively](#) into the Ethereum protocol, these trust assumptions will be reduced by eliminating the need for relays.

- Searchers have to trust the builder(s) to which they send bundles.

Builders may be the most incentivized to use

abuse your transactions to extract additional MEV. As a searcher, you must find a builder with reputation at stake, so you can trust that they won't take short-term profits in favor of your continued bundle submissions.

- Builders have to trust the relay to which they send blocks.

For background on relays, see [this post](#).

Of course, block builders have to trust that relays won't leak transaction data or use it to extract additional MEV (secretly building blocks themselves). But the other major consideration is that the relay has to respond to the validator's requests quickly, so that the validator does not miss the chance to propose a builder's block. If the validator misses the slot, the builder of the most profitable block which would have been proposed loses out on their profits as well.

- Validators have to trust the relay(s) from which they receive blocks.

A strictly rational validator won't care if a relay abuses their transaction view and extracts unfair MEV, as this is actually more profitable for the validator. That being said, if a relay abuses its power, it won't last for long.

For validators, the performance of the relay is paramount. Validators must trust that the relay(s) they connect to will respond to their requests quickly and reliably. If the relay does not respond in time, a validator may miss their window to include a block in the next slot, and will not earn any rewards for their participation.

Read more about the trust assumptions of mev-boost-enabled PBS in [Stephane's research post](#).