A recent blog post by Vitalik stated that block production (building) will be “centralized” but does not provide any details about how centralized. Is it possible that we end up with a single block builder?

The ultimate goal for a block builder is to build the highest-value block that it can. To do this, it needs to build from high-value transactions. The combined value of MEV opportunities at any point in time will in general outweigh any delta that could be obtained by smart block building algorithms, so access to a high-value transaction pool will be the defining advantage for block builders.

There is a significant change to transaction inclusion in blocks post-merge. Because validators are considered untrusted, individual transactions or transaction bundles are no longer provided to proposers. Instead, validators are presented with the hash of a list of transactions by the builder. And because validators only have a hash of the full list of transactions the validator’s acceptance is all-or-nothing; it is not possible for a validator to alter the transactions. As such, if a new searcher finds an MEV opportunity they can either build a full block themself or they can submit it to an existing block builder. If they try to build a full block themself they need to build a higher-value block from their transactions and the public mempool than that made by a block builder with access to an existing MEV transaction pool, which is going to be tough. So they are most likely to submit it to existing block builders, increasing the value of the builders’ transaction pools and hence the blocks they build.

Which block builders are they likely to submit to? If they submit their bundle to more than one builder it is possible for one of the builders to reverse engineer the bundle without the searcher being able to identify which builder stole it. This is equally true of sandwich-style transactions, where the builder can remove the “meat” of the sandwich and wrap it with their own transactions, as with more generative transactions such as on-demand liquidity provision, where the builder can supply their own liquidity ahead of the transaction that requires it. If they only submit to a single block builder they need to pick the one that has the most chance of building a block that will be selected by the next block proposer (as many MEV opportunities are time-limited in some way). As such, the only logical choice is to send it to the single builder that already has the highest-value transaction pool. And as searchers are financially driven, they are all likely to make the same choice.

This appears to create a positive feedback situation, leading to the end result of a single large high-value transaction pool, and a single major builder. Smaller transaction pools may survive if backed by validators willing to sacrifice financial rewards for some other value, however for validators that are monetarily-driven they will end up taking the block from the single major builder.

There are various detrimental impacts to having a single block builder, however at this point I’m interested in hearing if others disagree with the above logic and can explain why we will not end up with a single dominant block builder.