By Quintus and @Christoph with thanks to Julian, Sarah and Data Always for review.

tl;dr:

this article frames the discussion around proposing rights allocation in Ethereum, provides a quick (opinionated) overview of the current discourse and highlights a few open questions at the end.

The goal of preventing MEV-driven centralisation that undermines Ethereum's core properties has led to a variety of proposed schemes that change the way blocks are built and proposed in the network. These schemes like ePBS, MCP or execution tickets would replace the market based around MEV-Boost that we have today (although the MEV-Boost software may still play a role).

All of these designs have two goals in common: As a primary goal, we want to avoid any incentive for attesters to behave strategically.

Rewards in skill and benefits to colocation create centralising pressures on the network which we want to avoid. As a secondary goal, we want to keep

the builder market "good"

. By "builder market" we refer to the market that emerges around servicing the additional role that all of these schemes create in addition to the attester role. "Good" involves navigating a tradeoff space between decentralisation, efficiency, and protocol revenue.

During initial explorations of this solution space the ~consensus position was that we want a large degree of decentralisation among attesters even if this means that the builder market is fairly "bad" (e.g. the endgame post). However, it has never been clear at what point we draw the line and are willing to have less decentralisation among attesters for a better builder market. This post doesn't attempt to take a stance here, but simply to make accessible the landscape of tradeoffs. This is a complex problem and there are few arguments that we can really take as watertight and perfectly predictive so this post should be seen as an interpretation of the work that has been done but is certainly subject to change.

Since the Multiple Concurrent Proposer (MCP) family of designs, of whichBRAID is the foremost design effort, is still quite new and must be fleshed out first, the article discusses single-proposer designs in greater depth and dedicates a brief section to discussion of MCP at the end.

Note: "attester" is used instead of "validator" to emphasise the relatively simple consensus role of attesting to blocks and participating in the p2p layer in contrast to the more complex role of block production and proposal which the network technically currently allocates to the same actor. Attester and validator can loosely be treated as interchangeable.

The Tools We Know

Attesters benefit most from strategic behaviour when selected as consensus leader to propose blocks to the rest of the attester set for a given slot. Hence, most of the designs we have come up for protecting attesters have focused on the proposer role. Each of these uses some combination of three techniques:

1. Moving responsibility to a non-validator role known as the "execution proposer" (eprop):

while some tasks like determining which transactions are in the block can be easily moved to the eprop, other tasks like aggregating attestations must be left to the selected attester (now called the "beacon proposer", or "bprop"). Posting inclusion lists and facilitating the selection of future execution proposers are also duties we tend to leave up to the bprop. This is the defining characteristic of Attester-Proposer-Separation (APS) designs which include slot-based ePBS [1]

, Execution Tickets and Execution Auctions.

If one wanted to be pedantic, the exception of block-based ePBS can be pointed to as a case in which the non-validator role is technically not a proposer as the attester set is not expecting a signature form their pubkey.

1. Constraining (either e/b) proposer powers through the use of a committee:

for instance, if we expect the bprop to aggregate bids for eprop rights, we can use a committee of validators to each supply their view of which bids have arrived and force the bprop to consider at least some of their views. Similarly, inclusion list designs like FOCIL leverage a committee of attesters to constrain the eprop's ability to exclude transactions. Mike and Barnabe's "Mechanstein" is another good example for this technique.

1. Reducing bprop incentives to behave strategically by doing things early and/or privately:

The main example here is when the bprop is expected to facilitate the allocation of eprop rights, most commonly by providing a view of messages from the builder market in which builders make investment decisions like auction bids. On one extreme, the value of being the eprop 12 seconds from now can be very volatile as it is sensitive to the arrival of new information like changes in the Binance ETH price. On the other extreme, the value of being the eprop a year from now is unlikely to change in the next 12 seconds even with wild market swings. Thus, asking the bprop to play a role in selecting the eprop further in the advance reduces the incentive for the bprop to play latency games. It also gives time to allow investment decisions to be incorporated over several slots, making bprop censorship much less profitable. Obscuring bids also denies the bprop information which it could otherwise use to profitably interfere with the allocation of eprop rights.

Execution tickets and execution auctions (of which slot-based ePBS is a special case) all move things further in advance (covered well by Barnabe's More Pictures About Proposers And Builders) while Anders has described an auction protocol that targets privacy of auctions.

Each of these has its own limitations:

1. MEV incentives for bprops despite introducing the eprop

: Some tasks that we leave up to the bprop are still subject to MEV incentives. This may be true for handling inclusion lists, depending on the scheme we use, and it is certainly true for allocating eprop rights. If we were to assign these tasks to the current eprop, we risk creating a feedback loop in which the current eprop has an advantage in capturing the right to be the future eprop due to latency advantages if not also other advantages offered up by the chosen mechanism. For example, in the unrealistic extreme case, the eprop at block n could be expected to run an auction to allocate the eprop rights for n+1. In this case, the incumbent eprop could always incorporate the most information like changes in ETH price and (if unencrypted) the bids of other actors.

This feedback loop may not undermine our primary goal all that much, but has the potential to impact the builder market - for example, when investments decisions are not made far in advance and the proposing right value changes rapidly with time.

The magnitude of such an effect is not yet well understood and may well not be significant.

1. Limited censorship resistance in committees

: This discussion must be separated to discuss two approaches. The most developed line of research has taken an approach aiming to constrain proposers using a committee. FOCIL was designed to augment the current Ethereum protocol for this purpose. These committees only limit some

censorship and accordingly only erase some

opportunity for strategic behaviour. The committee is employed to establish a minimum bid or inclusion list of transactions, however, as these designs allow the proposer to include data (transactions/bids) after the committee has published the list of included data, the protocol cannot ascertain if late bids or transactions were excluded. This limitation comes primarily from the design approach which seeks to make minimal changes to the existing protocol, leaving the proposer role in its central position, it is not a fundamental limitation of committees. It may even be possible to largely remove much of the influence of the special proposer role with FOCIL, although this is not the intended use as proponents favour giving “last look” to the proposer so as to minimally perturb the current market.

On the other hand, we have the less fleshed-out MCP direction which does take on a fundamental redesign of the consensus protocol so that the proposer role is completely distributed to a committee (each committee member now being referred to as a “proposer”), without explicitly privileging a singular actor. While MCP holds promise to significantly strengthen the guarantees provided by the committee-to-constrain approach, the changes of using a committee in this way likely constitute a fundamental change and still leave many details unspecified. Hence, one cannot assume surrounding behaviour remains fixed and considerable additional analysis into timing incentives, spam incentives, network throughput and similar is required. For more, see this post comparing BRAID and FOCIL, this analysis, this panel and the section at the end of the post for more.

1. “Bad” eprop market structure and secondary markets due to early auctions

: All of the proposed eprop rights allocation mechanisms require some message exchange between participants and the attester set such as for bidding in an auction or buying an execution ticket. Moving this message deadline further in advance of the slot in question: 1. Runs the risk of a secondary market emerging. 1. If this happens on-chain, either the eproposer or the bproposer has to handle it. Both defeat the point of running this market in advance. The former has the feedback loop problem and the latter creates bprop MEV incentives.

1. If this happens off-chain (e.g. because prop. rights are tied to a specific public key), we may satisfy our primary goal, although there are open questions around how this is to be implemented and what the impact on the builder market will be. As an aside, this situation describes the status quo in which validators make investment decisions far in advance (staking) of receiving rights and MEV-Boost is an emergent offchain secondary market.

2. If this happens on-chain, either the eproposer or the bproposer has to handle it. Both defeat the point of running this market in advance. The former has the feedback loop problem and the latter creates bprop MEV incentives.

3. If this happens off-chain (e.g. because prop. rights are tied to a specific public key), we may satisfy our primary goal, although there are open questions around how this is to be implemented and what the impact on the builder market will be. As an aside, this situation describes the status quo in which validators make investment decisions far in advance (staking) of receiving rights and MEV-Boost is an emergent offchain secondary market.

4. Undermines our secondary goal of keeping the builder market “good” since there is less information available about the item on sale, lowering revenue and increasing builder market centralisation. The argument for centralisation is that the further the auction is run in advance, the less room there is for differentiation among builders as every block looks roughly the same, rendering the hierarchy of valuations unchanging. Roughly this point has been made on several occasions like this paper and this older post. The most interesting treatment comes from this paper though which makes the point that we see increased concentration even in the presence of a secondary market.

Additionally, one may point to the increased importance of non-commodified builder characteristics like price prediction and risk tolerance to make similar arguments for centralisation due to ahead-of-time bidding.

1. Runs the risk of a secondary market emerging.

2. If this happens on-chain, either the eproposer or the bproposer has to handle it. Both defeat the point of running this market in advance. The former has the feedback loop problem and the latter creates bprop MEV incentives.

3. If this happens off-chain (e.g. because prop. rights are tied to a specific public key), we may satisfy our primary goal, although there are open questions around how this is to be implemented and what the impact on the builder market will be. As an aside, this situation describes the status quo in which validators make investment decisions far in advance (staking) of receiving rights and MEV-Boost is an emergent offchain secondary market.

4. If this happens on-chain, either the eproposer or the bproposer has to handle it. Both defeat the point of running this market in advance. The former has the feedback loop problem and the latter creates bprop MEV incentives.

5. If this happens off-chain (e.g. because prop. rights are tied to a specific public key), we may satisfy our primary goal, although there are open questions around how this is to be implemented and what the impact on the builder market will be. As an aside, this situation describes the status quo in which validators make investment decisions far in advance (staking) of receiving rights and MEV-Boost is an emergent offchain secondary market.

6. Undermines our secondary goal of keeping the builder market “good” since there is less information available about the item on sale, lowering revenue and increasing builder market centralisation. The argument for centralisation is that the further the auction is run in advance, the less room there is for differentiation among builders as every block looks roughly the same, rendering the hierarchy of valuations unchanging. Roughly this point has been made on several occasions like this paper and this older post. The most interesting treatment comes from this paper though which makes the point that we see increased concentration even in the presence of a secondary market.

Additionally, one may point to the increased importance of non-commodified builder characteristics like price prediction and risk tolerance to make similar arguments for centralisation due to ahead-of-time bidding.

Where does this leave us?

Looking at these tradeoffs we can make some broad recommendations. Firstly, using a committee to constrain proposers doesn’t seem to have a deep tradeoff (perhaps broad timing incentives and complexity, but these seem less significant than other dynamics mentioned) while providing the benefit of providing censorship resistance and reducing the impact of eprop feedback loops or bprop MEV, depending which actor we choose to run the allocation mechanism. Hence, we should use something like FOCIL in any scheme. In future, we will hopefully find that the MCP direction bears the fruits of an even more appealing committee-based design which can then take the place of FOCIL.

Introducing the eprop role also seems inevitable. There are several reasons for this. Apart from most proposals involving an eprop role, we can look at the current protocol which does not explicitly introduce this role but instead had it organically emerge in an out-of-protocol market (MEV-Boost), indicating that incentives lead to a specialised role emerging even if the protocol design does not intend it. This leaves us with three important choices for creating this eprop role: who

allocates eprop rights (eprop or bprop), when

do participants have to make “investment decisions” (bidding, staking, buying tickets etc) and how

is the eprop chosen?

Looking at the who and when decisions we arrive at the following diagrams

eprop handles the allocation mechanism

bprop handles the allocation mechanism

The first option indicated on the left shows a world in which we leave as many roles as possible up to the eprop. The remaining choice is then around timing, in particular the timing of investment decisions relative to allocated slots. Tuning the timing will allow us to navigate two forces that negatively impact the builder market structure. Running things further in advance brings the aforementioned negative impacts on the builder market (like concentration and loss of revenue) while less of a delay risks creating positive feedback loops for incumbents, although its not clear what the magnitude of such an advantage would be. Based on the factors we have outlined above, this heavy eprop design space does best to isolate the bprop. Of course, there may be other relevant interactions we haven't explored yet.

Alternatively, we could leave the allocation of eprop rights to the bprop. In this world, the bprop would be taking on roles like determining the highest bid in an auction or including execution ticket purchase messages. Tuning timing in such a world allows us to choose between sacrificing bprop "strategy-freeness" (i.e. attester decentralisation) for builder market concentration.

Block vs Slot Auctions

The block vs slot auctions discussion in ePBS can be seen as a discussion about running the allocation mechanism with no delay (block auction) vs with a small delay (slot auction). The linked article provides a relatively comprehensive overview, but we wanted to add two points about this "phase transition"

- In block auctions, transactions are packaged in blocks by builders who do not know if they will be chosen to build the block. This can make transactions submission more complicated as the user or some intermediary has to reason about where to send transactions (although several services exist to handle this), but also prevents monopoly pricing as builders are competing with one another. As soon as the block is being built by an actor who knows that they are the sole block producer (i.e. eprop) they can invoke monopoly pricing and have much less incentive to abstain from behaviour that negatively impacts the end user (like sandwiching and frontrunning). This point was originally made here.

- Even a small delay requires builders to start making block value predictions and take on risk. This advantages builders of a certain profile who usually are also market makers and integrate their trading and block building activities. A market in which blocks are constructed by entities who place themselves in the best position to trade is clearly less neutral than one in which the role of block production is carried out by actors who do not actively trade as well.

How To Allocate Rights

The diagrams above only capture the direction of different predicted effects, but the degree to which these effects are present naturally depends on the type of allocation mechanism. The jury is certainly still out on this, but there are some relevant works to point to that allow us to discriminate between the many possible designs:

- In this post, @Christoph (Flashbots) argues that allocation mechanisms that have greater elasticity in the supply of proposing rights allow for a more diverse market. This would explain why models that assume a fixed number of tickets like this one predicts a single owner of all tickets while the Ethereum PoS system currently supports a diversity of actors.

- This post by Mike, Tim and Pranav point out that different auction formats (e.g. all pay vs winner-pays) allow us to tradeoff different properties of the builder market such as revenue and market concentration and can be seen as a predecessor to Christoph's post.

- This paper formally argues that any mechanism that doesn't give proposing rights to the highest bidder must give up at least one of sybil-proofness and incentive compatibility. One can interpret this result as similar to the one above: if you want to depart form winner-takes-all auction formats, you have to give up some (potentially desirable) properties.

Our takeaway from these is that if one wants the builder market to be minimally concentrated, one may have success by spreading the allocation of proposing rights as broadly as possible, but this comes at the cost of efficiency and revenue. Having an allocation mechanism that favours market decentralisation would hopefully soften the cost of requiring investment decisions being made further in advance.

Multi-block MEV

Broadly, we have argued that we want to avoid market concentration and employ committees to reduce the ability for any individual actor to undermine the neutrality of the blockspace market (by censoring or front-running competing trades for example). A more specific concern is that if an actor knows that they hold proposing rights on consecutive blocks, they will be able and incentivised to take additional actions that negatively impact the operation of markets. For example, if a builder knows that they will produce two blocks in a row (with high probability), they may censor some trades in the first block knowing that they can more profitably execute them in the next (see here for more detail).

We want to avoid this kind of dynamic for two reasons:

- Returns to scale (having more blocks) acts as a concentrating force in the market, undermining market neutrality

- The extraction of multiblock MEV negatively impacts market participants (delays, slippage etc)

We could try to address this problem by:

1. Reducing the chances that one actor is allocated two slots in a row. We can reduce this into the aforementioned goal of targeting low market centralisation, along with some means of preventing concentration after the initial allocation in a secondary market (hard).

2. Implementing “single-slot single-leader election”[2]

3. i.e. removing the certainty at slot n as to which actor will produce the block at slot n+1. To the best of our knowledge, we don’t know how to do this in general, although the Mechanstein proposal could be seen as a way of approximately achieving this. While the MEV-Boost market doesn’t provide the ability to sell slots in bundles, slots are allocated per epoch, i.e. 32 slots at a time, which means that big actors like Coinbase are currently regularly able to sell or take advantage of the right to build multiple consecutive slots and simply don’t (thanks!).

4. Reducing the action space of those who hold proposing rights. This amounts to the committee-based approach mentioned above. Inclusion lists limit the amount of censorship a builder can carry out. The Mechanstein proposal is a more complex instantiation of this idea and, as we elaborate on below, the MCP direction tries to take this approach to its logical conclusion.

A related direction is simply to disincentivise certain misbehaviours. In particular, imposing missed slot penalties reduces incentives to leave blocks empty as a means to circumvent inclusion lists.

Points 1 and 3 are already discussed above and the implementation of 2 would largely leave other discussions unchanged.

What about MCP?

As mentioned before, Multiple Concurrent Proposers can be thought of as a design property which takes the use of committees to their fullest extreme. Instead of having a committee constrain a single actor like inclusion list designs attempt to do (or, as otherwise stated, leave a special actor with “last look”), MCP would have a committee of actors “equally” constructing a block or at least take action at the same time. The foremost MCP design is BRAID which is still at the phase of figuring out consensus details with no specific ordering scheme having been proposed yet.

In some sense, MCP fits perfectly into what has been discussed above. MCP calls for the ability to elect multiple proposers per block, but does not stipulate when investment decisions by builders should be made or how proposing rights should be allocated. The separation between eprops and bprops is also not necessarily to be taken for granted in this model. Some may argue that distributing proposing within a slot across actors can sufficiently reduce MEV incentives that assigning attesters to this task will not lead to a secondary market.

As discussed with regard to committees above, utilising committees reduces the impact of MEV incentives, barring total collusion, so the consequences of asking builders to make investment decisions closer to the slot are likely reduced and we don’t have to eat as much of the “market badness” we are arguing comes with making investment decisions far in advance. An additional benefit of MCP over committee-based solutions that constrain proposers is that MCP improves liveness guarantees as no single proposer can cause a missed slot.

That said, MCP/BRAID is both a fundamental and currently under-specified change with many unknowns which must be addressed. For example, being the last proposer to act can provide some informational advantages which could create new timing game incentives and (intentional) discoordination among concurrent proposers may lead to inefficiencies like duplicate transactions being included in slots. Some of these points were discussed in more detail a recent panel.

Summary

The main aim of this post was to layout the tradeoff space. This can be summarised as follows:

- when:

it seems that requiring builders to make decisions further in advance can reduce the resultant MEV for either bprops or eprops, however current research suggests that doing so reduces protocol revenue and concentrates the builder market. There may be a phase transition moving from no delay in “block auctions” to doing things slightly in advance.

- who:

we can leave the role of facilitating the proposing rights allocation market up to either eprop or bprop. If we choose bprop we (hopefully) avoid feedback loops where incumbent eprops are benefitting themselves at the cost of attester decentralisation. If we choose to rely on eprops, we protect the bprops but may undermine the builder market

- how:

it seems like lottery systems are better for decentralisation but lead to the loss of desirable properties like efficiency and high revenue

- what:

the more constrained proposers are the less proposing rights are worth and the smaller impact proposers can have on the system. With greater constraints on proposers, the benefits of requiring investment decisions to be made in advance becomes smaller. In general, it makes sense to involve committees but there are of course nuances to any specific design.

Opinionated Conclusion

- One could argue that today's system's timing is optimal. According to the arguments cited above, the builder market is most efficient and decentralised when run just-in-time as it is today and the impact of proposer timing games doesn't seem too bad (yet?). That said, the current market appears quite concentrated so we should both poke at these arguments to see if the conclusion is indeed reasonable and explore other forms of changes.
- MCP seems like a really promising direction to pursue but there are still many questions. We're most excited about MCP with an eprop role. In the meantime, we clearly need FOCIL.
- It feels like a broad takeaway from all the work we've done so far is that you can either have a decentralised market by making everyone homogeneous and commodified and (maybe adding diminishing returns due to risk aversion) OR you take a heterogeneous market and make sure that the dimensions along which market participants are different are such that the hierarchy of competitors depends on parts of the environment that are always changing. We are in the latter camp we think.

Open questions

Naturally, there are many open questions and perhaps the best to ask are not known to me. Here are a few questions that seem important to me though:

- How does price/systemic risk play into the market concentration for systems that require the allocation of a lot of capital such as execution tickets?
- We look at the current market today where we have multiple builder concurrently constructing a block and extrapolate from that that the most profitable blocks are often built in a non-neutral way by integrated parties. However, this may not carry over to (MEV-Geth-like) regimes in which there is a single entity constructing a block. Presumably this builder must balance auction revenue and their own trading profit as skewing the market in their favour may cause other bidders to shade their bids in anticipation of adverse selection.
- The "eprop feedback loop" problem is currently not well understood. For some concrete designs, can we ascertain whether this is a legitimate concern?
- Much of this line of thinking stems from concern around timing games incentives which caused missed slots and incentivise colocation of attesters. We can likely address the missed slot incentives by imposing a missed slot penalty so we are left with colocation incentives.
- Can we make some statements about the magnitude of these incentives?
- We have focused mainly on reducing colocation incentives, but what about explicitly incentivising geographic distribution? Recent works like PoLoc and VerLoc have made progress in credibly ascertaining node location in a byzantine setting. Could we leverage this technology (perhaps with additional privacy guarantees) to actively reward nodes for being located in a desirable geographic location?

- Can we make some statements about the magnitude of these incentives?
- We have focused mainly on reducing colocation incentives, but what about explicitly incentivising geographic distribution? Recent works like PoLoc and VerLoc have made progress in credibly ascertaining node location in a byzantine setting. Could we leverage this technology (perhaps with additional privacy guarantees) to actively reward nodes for being located in a desirable geographic location?

- the definition of APS we are using is one in which the proposer need not be an attester and the proposer is defined as the holder of the private key which the attester set expects to sign the execution payload ↩
- This is not to be confused with single secret leader election (SSLE) which is a related but different concept.↩