We present rainbow staking

, a conceptual framework allowing protocol service providers, whether "solo" or "professional", to maximally participate in a differentiated menu of protocol services, adapted to their own strengths and value propositions.

Why rainbow?

We intend to convey that the architecture below is appropriate to offer services provided by a wide spectrum of participants, such as professional operators, solo home stakers, or passive capital providers.

Additionally, the [spectrum](#) may remind the reader of eigen

values, while we intend for this proposal to partially enshrine a structure similar to re-staking.

TLDR

- We take a first principles approach to identifying the services that the Ethereum protocol intends to provide, as well as the economic attributes of various classes of service providers

(e.g., professional operators vs solo stakers).

- Heavy and light categories of services:

We re-establish the separation between heavy

(slashable) and light

(non- or partially slashable) services. Accordingly, we essentially unbundle the roles that service providers may play with regard to the protocol. This allows for differentiated classes of service providers to be maximally effective in each service category, instead of lumping all under a single umbrella of expectations, asking everything of everyone.

- Delegators and operators:

For each category of services, we further distinguish capital delegators

from service operators

. We obtain a more accurate picture of the principal–agent relationships at play for each service category, and the ensuing market structure which resolves conflicting incentives.

- Heavy services:

The requirements of heavy services such as FFG, Ethereum's finality gadget, are strengthened to achieve Single-Slot Finality (SSF). We suggest options to provide more protocol-level enshrined gadgets, helping foster a safe staking environment and a diversity of heavy liquid staking tokens

. These gadgets include flavours such as liquid staking module (LSM)-style primitives to build liquid staking protocols on top of, as well as enshrined partial pools or DVT networks, all allowing for fast re-delegation among other features.

- Light services:

Meanwhile, the protocol offers an ecosystem of light services such as censorship gadgets, which are provided using weak hardware and economic requirements. These light services are compensated by re-allocating aggregate issuance towards their provision, a pattern already in use today for sync committees. Additionally, "light", trustless LSTs may be minted from the delegated (non-slashable) shares who contribute weight to light service operators, by capping operator penalties or making all light stake non-slashable.

- Intended goals:

We believe the framework of rainbow staking helps to achieve several goals: * The correct interface to integrate further "protocol services" in a plug-and-play manner.

- Targeting Minimum Viable Issuance (MVI) and countering the emergence of a dominant LST replacing ETH as money of the Ethereum network.
- Bolstering the economic value and agency of solo stakers by offering competitive participation in differentiated categories of services.

- Clearing a path to move towards SSF with good trade-offs.

- The correct interface to integrate further "protocol services" in a plug-and-play manner.

- Targeting Minimum Viable Issuance (MVI) and countering the emergence of a dominant LST replacing ETH as money of the Ethereum network.

- Bolstering the economic value and agency of solo stakers by offering competitive participation in differentiated categories of services.

- Clearing a path to move towards SSF with good trade-offs.

Operator–Delegator separation

Discussions around staking have pointed out the natural separation between node operators and capital delegators, inherited from the perennial distinction between labor and capital. The separation is natural. Many parties wish to obtain yield, and yield is generated from the issuance rewarding participants who place their assets at stake to secure FFG, Ethereum's finality gadget, and more largely to operate Gasper, Ethereum's consensus mechanism. Along with placing assets at stake, the work of validation must be properly done to obtain rewards (more yield) and avoid penalties (less yield). This validation work is however costly, and may be performed by operators on behalf of delegators. The operator set is decomposed in two classes:

- Professional operators

, whose higher sophistication, trustworthiness or reputation affords them capital efficiency. Delegators receive a credible signal attesting to the honesty of professional operators, and these operators may receive multiples of delegated stake against low or no collateral. For instance, Lido operators are vetted by the Lido DAO, creating a credible signal and allowing these operators to participate with no stake of their own, and thus maximal capital efficiency.

- Solo stakers

, the set of permissionless operators participating in the provision of staking services. The permissionless nature means that solo stakers are fundamentally untrusted

, and a delegator does not have access a priori

to a credible signal of the reliability of a solo staker. Solo stakers may stake entirely with their own stake, or participate in protocols which create credibility by construction, e.g., requiring the operator to put up stake of their own (Rocket Pool), or joining a Distributed Validator Technologies (DVT) network (Diva).

Operators as part of a Liquid Staking Protocol (LSP) may offer to issue a liquid claim for the delegators, known as Liquid Staking Tokens (LSTs). These LSTs represent the principal which delegators have provided, along with the socialised rewards and losses collected by operators, net of fees.

We review recent proposals to enshrine the separation of operators and delegators further into the protocol. Such attempts naturally target the formation of "two tiers", an operator tier and a delegator tier (see Dankrad, Arixon, Mike on the topic). A recent idea suggests that by capping slashing penalties to only the operator's stake, assets of delegators are no longer at risk.

[

rainbow-staking-0

2802×1152 212 KB

](https://ethresear.ch/uploads/default/original/2X/f/fc8ef60bb44452ff9b021fcc0c5dee8ce4ae6b08.png)

If this sounds too good to be true, then why should delegators earn any yield? Vitalik lists two possibilities in his post, "Protocol and staking pool changes that could improve decentralization and reduce consensus overhead":

1. The curation of an operator set:

Opinionated delegators may decide to choose between different operators based on e.g., fees or reliability.

1. The provision of small node services

:

The delegators may be called upon to provide non-slashable, yet critical services, e.g., input their view into censorship-resistance gadgets such as inclusion lists, or sign off on their view of the current head of the chain, as alternative signal to that of the bonded Gasper operators. Should a mismatch be revealed, the community would be brought in to decide whether

to manually restart the chain from the delegators' view, or go along with a possibly malicious FFG checkpoint.

In other words, delegators in this model

do not exactly contribute economic security to FFG, their stake being non-slashable, but they are able to surface discrepancies in the gadget's functioning. Their denomination as "delegators" remains somewhat contrived. We see three issues with the model of two-tiered staking as presented above:

1. Delegators in the two-tiered staking model are unlike delegators of current LSPs, who bear the slashing risk.

2. Some agents would wish to delegate their assets to "two-tier operators" and

subject themselves to the slashing conditions, in search for yield.

1. Some agents would wish to not

operate small node services themselves, yet participate in their provision by delegating operations instead.

Heavy and light services separation

To resolve these issues, we take the view here of two

distinct types of protocol services

, each type inducing within itself a market structure of delegators and operators. The fully unbundled picture becomes:

[

rainbow-staking-1

3302×1152 278 KB

](https://ethresear.ch/uploads/default/original/2X/b/b161b303703991be074a722dcf785a018cd86fb8.png)

The two categories are functionally different, but both feature the Delegator–Operator Separation

Economics of heavy services

- Heavy services use stake as economic security

, making a credible claim that should the service be somehow corrupted, all or part of the stake will be destroyed. Gasper makes such a claim when it binds Gasper participants to slashing conditions, in particular the condition that should their stake participate in an FFG safety fault (conflicting finalised checkpoints), all of their stake will be lost.

- The heaviness of the service induces specific market structures. The heightened risk of slashing, coupled with the high amount of revenue paid out in aggregate to Gasper service providers via issuance, results in long intermediated chains of principal-agent relationships, with delegators providing stake to operators who participate in Gasper on their behalf.

- An architecture akin to the Liquid Staking Module (LSM), originally proposed by Zaki Manian from Iqlusion, may be deployed to enshrine certain parts of the heavy service provision pipeline, and allow for the emergence of competitive LSPs. In the LSM, delegators provide stake to some chosen operator. An LSM share

may be minted from the delegate stake, representing the delegation from a given delegator to a given operator. Shares are then aggregated by an LSP, which mints a heavy LST

backed by the set of shares it owns.

- Fast re-delegation is allowed, with the re-delegated stake remaining slashable for some unbonding period, all the while accruing rewards from the new operator it was re-delegated to (similar to Cosmos).

Economics of light services

- Light services use stake as Sybil-control mechanism

and as weight functions

, akin to Vitalik's first point on light delegators curating a set of operators. The low capital requirements and low sophistication necessary to provide light services adequately, mean that the playing field is level for all players.

- Nonetheless, a holder may still decide to delegate their assets to a light service operator. The light service operator would offer to perform the service on behalf of the delegator against fees, which aligns the incentives of the operator to

maximise the reward for the delegator. In a competitive marketplace of light operators, along with re-delegation allowing for instant withdrawal from a badly performing operator, light operators would be expected to provide the service for marginal profitability and with cost efficiency.

- Some light services may require sticks in addition to carrots, i.e., must allow for slashable or penalisable stake. We suggest here to enforce penalties capping

, where only the stake put up by the operator is slashable. We call these partially slashable light services

.

[

rainbow-staking-2

3302×1152 350 KB

](https://ethresear.ch/uploads/default/original/2X/0/0b0516b17f26b1a323fc9a70cacfc5c48d3f7822.png)

By bonding light operators, penalties may be doled out to service providers with bad quality of service.

- A delegator receives a tokenised representation of the assets they delegate towards the provision of light validation services. We call this tokenised claim a light LST

. When delegator Alice deposits her assets to operator Bob, she receives an equal amount of LightETH-Bob

. * This LST is trustless

in the sense that Alice may never lose the principal she delegates to Bob, as Bob's penalties are capped to his own bond. Accordingly, even an untrusted operator such as solo staker is able to mint their own trustless light LSTs.

- However, the light LSTs are not fungible between different operators. If Alice deposits with Bob and Carol deposits with David, Alice obtains LightETH-Bob

while Carol receives LightETH-David

. The non-fungibility comes from the internalisation of light rewards. Bob may set his commission to 5% of the total rewards received on the delegated stake, while David may set his own commission to 10%. Even at equal commission rates, the two operators may not perform identically, with one returning a higher value to its delegators or holders of their associated light LST. The value returned may be internalised with e.g., making the light LSTs rebasing tokens.

- Contrary to heavy LSTs which are market products, the light LSTs are protocol objects. Light LSTs have properties resembling LSM shares, rather than LSTs as traditionally known.

- This LST is trustless

in the sense that Alice may never lose the principal she delegates to Bob, as Bob's penalties are capped to his own bond. Accordingly, even an untrusted operator such as solo staker is able to mint their own trustless light LSTs.

- However, the light LSTs are not fungible between different operators. If Alice deposits with Bob and Carol deposits with David, Alice obtains LightETH-Bob

while Carol receives LightETH-David

. The non-fungibility comes from the internalisation of light rewards. Bob may set his commission to 5% of the total rewards received on the delegated stake, while David may set his own commission to 10%. Even at equal commission rates, the two operators may not perform identically, with one returning a higher value to its delegators or holders of their associated light LST. The value returned may be internalised with e.g., making the light LSTs rebasing tokens.

- Contrary to heavy LSTs which are market products, the light LSTs are protocol objects. Light LSTs have properties resembling LSM shares, rather than LSTs as traditionally known.

- Note that we already have light services in-protocol today! The sync committee duty is performed by a rotating cast of validators, and is responsible for about 3.5% of the aggregate issuance of the protocol (including the proposer's reward for including aggregate sync committee votes). This level of this allocation is based on a reasonable guess with respect to the value and incentives of the service (e.g., cost of attacking by accumulating weight).

- Consequently, we are already in a world where the protocol remunerates (via issuance) the provision of some chosen light services. We can add more to these light services if we believe these to be valuable enough to warrant either additional issuance or a redistribution of our issuance budget away from the Gasper mechanism remuneration and towards more of these light services. A thesis of this framework is that we indeed have such services at hand, including censorship-resistance gadgets.

- Admittedly, sync committees are not a great archetype of light services. First, these committees will be obsolete after SSF, which rainbow staking aims to achieve. Second, these committees exhibit strong synergies with activities performed by heavy operators, so they do not confer an overwhelming advantage to solo stakers. Our point here is to recognise that issuance is already diverted away from only Gasper

, but it is not to advocate for sync committees as being the archetype for light services. Censorship-resistance gadgets fit the bill much more, if they are able to reward participants for increasing CR by surfacing censored inputs to the protocol via some gadget such as inclusion lists.

- Consequently, we are already in a world where the protocol remunerates (via issuance) the provision of some chosen light services. We can add more to these light services if we believe these to be valuable enough to warrant either additional issuance or a redistribution of our issuance budget away from the Gasper mechanism remuneration and towards more of these light services. A thesis of this framework is that we indeed have such services at hand, including censorship-resistance gadgets.

- Admittedly, sync committees are not a great archetype of light services. First, these committees will be obsolete after SSF, which rainbow staking aims to achieve. Second, these committees exhibit strong synergies with activities performed by heavy operators, so they do not confer an overwhelming advantage to solo stakers. Our point here is to recognise that issuance is already diverted away from only Gasper

, but it is not to advocate for sync committees as being the archetype for light services. Censorship-resistance gadgets fit the bill much more, if they are able to reward participants for increasing CR by surfacing censored inputs to the protocol via some gadget such as inclusion lists.

Heavy services

Light services

Service archetype

Gasper

Censorship-resistance gadgets

Reward dynamics

Correlation yields rewards usually, anticorrelation is good during faults

Anticorrelation yields rewards (surface different signals)

Slashing risk

Operators and delegators

None or operators only

Role of operators

Run full node to provide Gasper validation services

Run small node to provide light services

Role of delegates

Contribute economic security to Gasper

Lend weight to light operators with good service quality

Operator capital requirements

High capital efficiency (high stake-per-operator) + high capital investments

Not really a constraint (operators receive weight) + small node fixed cost

Solo staker access

Primarily as part of LSPs (e.g., as DVT nodes)

High access for all light services

Liquid stake representation

Market-driven plurality of heavy LSTs

In-protocol light LSTs

Link to re-staking

"Provision of validation services

" sounds eerily familiar. We now draw a direct link between the discussion above and re-staking.

When a party re-stakes, they commit to the provision of an "actively validated service" (AVS). In our model, we may identify different types of re-staking:

- Re-staking into heavy services burdens your ETH asset with slashing conditions.

- Re-staking into light services may not burden you with slashing conditions, yet would offer rewards for good service provision.

So we claim that the model above is a partial enshrinement of re-staking, in the sense that we determine a "special" class of protocol AVS

for which rewards are issued from the creation of newly-minted ETH. We then allow holders of ETH to enter into the provision of these services, either directly as operators, or indirectly as delegators.

Staking economics in the rainbow world

This section presents a general discussion of the framework and its implications on the Ethereum network's economic organisation.

We regard Gasper (and in the future, a version with Single-Slot Finality, SSF) as the heaviest protocol AVS, one that is rigidly constrained by its network requirements (e.g., aggregation and bandwidth limitations), and which receives the highest share of aggregate issuance minted by the protocol. As such, its locus attracts a great many parties wishing to provide the stake which the service demands for its core functioning, while inducing market structures of long intermediated chains of principal-agent relationships.

Yet, it is unnecessary to offer unbounded amounts of stake to the Gasper mechanism in order to make its security claim credible. In addition, given the induced intermediation of stake, it is necessary to prevent the emergence of a single dominant liquid staking provider collateralised by the majority of the ETH supply. This means that measures such as MVI are critical to target sufficient security, by creating sufficient pressure to keep the economic weight of Gasper in the right proportion. However, MVI drives competitive pressures ill-suited to solo stakers, who are, besides, mostly unable to issue credible liquid staking tokens from their collateral and have thus low capital efficiency.

What is the role of solo stakers in our system? Their economic weight means their group is not pivotal to the Gasper mechanism. In particular, they cannot achieve liveness of finality by themselves, which requires 2/3 of the weight backing Gasper. Solo stakers find solace in two core value propositions which they embody ideally:

- Bolster network resilience:

Solo stakers bolster the resilience of the network to failures of larger operators who operate without solo stakers' input, for instance by progressing the (dynamically available) chain while large operators go offline. Constructions such as Rocket Pool or Diva provide access to low-powered participants in liquid staking protocols. These features are considered by large liquid staking protocols to improve the credibility of their liquid staking token, as measured by the degree of alignment between operators and delegators. In this sense, solo stakers function as hedges for the large liquid staking protocols: Not their main line of operators due to capital and cost-efficiency limitations, yet a strong fallback in the worst case. While the road to SSF may introduce additional pressures for solo stakers who are not part of pools (detailed in a section below), options also exist to preserve the presence of more yield-inelastic participants.

- Generators of preference entropy:

Solo stakers may contribute by additive means, the most potent one being as censorship-resistance agents. Performing such a light service is at hand for a wide class of low-powered participants. Additionally, mechanisms exist to remunerate "divergent opinions", rewarding the contributions of operators who increase [preference entropy

](https://x.com/cwgoes/status/1635617303810170880?s=20). Preference entropy denotes the breadth of information surfaced by protocol agents to the protocol, allowing the protocol to see more and serve a wider spectrum of users. For instance, solo stakers of one jurisdiction may not be able to surface certain censored transactions to a censorship-resistance gadget, while others in a different jurisdiction would, and could be rewarded based on the differential between their contribution and that of others. Over time, such mechanisms would tilt the economic field towards solo stakers who express the most highly differentiated preferences, in particular, towards non-censoring solo stakers rather than censoring ones.

[

rainbow-staking-3

1920×892 155 KB

](https://ethresear.ch/uploads/default/original/2X/d/d7dbff8196573f5476c3b4ed54e59b20532b1cf2.jpeg)

"Preference entropy" denotes the amount of information surfaced by protocol agents to the protocol. Agents who censor have lower preference entropy, as they decide to restrict the expression of certain preferences, such as activities which may contravene their own jurisdictional's preferences. Collectively, the set of solo stakers who operate nodes to provide services is highly decentralised, and is thus able to express high preference entropy. This economic value translates into revenue for members of the set.

This economic organisation redraws the lines of the MVI discourse. Today's 1-D MVI

optimises for competitive pressure to keep the weight of derivative assets such as LSTs in check ("minimum"), while under the constraint of safeguarding the presence of participants with lower agency over this specific mechanism, FFG ("viable"). With rainbow staking, we offer an alternative 2-D MVI

where solo stakers are maximally effective participants on their own terms

, achieving the goals which many have signed up for: Competitive economic returns with the ability to realise their preferences into the execution the chain, e.g., as ultimate backstops of chain liveness or as censorship-resistance agents. 2-D MVI no longer questions the ideal conditions of aggregate issuance with all participants lumped in a single battlefield, warring over a single scarce flow of revenue. 2-D MVI questions instead the adequate amount to allocate towards the remuneration of heavy services on one side and light services on the other.

We offer a strawman proposal for 2-D MVI determination. The first step is to port the current MVI thinking to the remuneration of heavy services, i.e., [decide on an issuance curve compatible with a rough targeting of stake backing heavy services](). This curve determines a level of issuance I_H

given some proportion of stake d

behind heavy services. The second step, given this level of "heavy" issuance, is to decide the issuance dedicated to light services. This could be determined with a simple scaling factor, i.e., set $I\_L = \alpha I\_H$

for some small α

(note that today, $\alpha \approx 3.6\%$

). The level of aggregate issuance is given by $I = I\_H + I\_L$

. The two questions 2-D MVI would be required to solve are then:

1. Which amount of stake behind heavy services should be targeted? (i.e., which I_H

do we want?)

1. How much more do we wish to issue in order to incentivise a viable ecosystem of light services? (i.e., which α

do we want?)

To provide orders of magnitude, issuance over the last year amounted to $I \approx$

875,000 ETH, close to 2 billion USD at current prices. If even $\alpha = 5\%$

of the yearly issuance was offered to the good performance of solo stakers for light censorship-resistance services, while 95% was offered to the heavy operator set, the set of light participants would collectively earn $I\_L =$

100 million USD. Assuming an investment of about 1,000 USD over the lifetime of a solo staker node (say 5 years, including upfront and running costs), we find that 100 million USD is enough to bring to marginal profitability up to 500,000 solo stakers as light operators. While this provides a generous upper bound in a world where all light service providers are also solo stakers, with no light delegators, we believe this order of magnitude is helpful to frame the terms of the debate.

[

rainbow-staking-4

1502×1252 220 KB

](https://ethresear.ch/uploads/default/original/2X/1/1c1d9fa783c18b2631fcb139f3cdede5aa94086b.jpeg)

Professional operators are well-suited to provide heavy services due to their sophistication along many dimensions (economies of scale, capital requirements, knowledge, reputation). Meanwhile, solo stakers are well-suited to provide light

services due to their high preference entropy, surfacing idiosyncratic signals to the protocol. The two groups overlap where heavy services earn credibility from the participation of solo stakers, or where light services earn efficiency from the participation of heavy operators.

Rainbow road

The next sections tackle individual facets of the rainbow staking framework, providing more colour. They are not essential to the text, and may be skipped by the reader in a hurry.

[

rainbowroad

978×542 70.7 KB

](https://ethresear.ch/uploads/default/original/2X/0/071dcc962e09b2a2c00ffd4f921c9cc8bc362ded.jpeg)

Mapping the unbundled protocol

We offer the following map to represent the separation of services in our model:

[

rainbow-staking-5

2802×1852 479 KB

](https://ethresear.ch/uploads/default/original/2X/e/e13c3b5a3fa5e13e9d9c5f305b7136feb712c44e.png)

The map emphasises the resources provided by each type of operator. We also unbundled the "execution services" from the "consensus services". To achieve MVI for the heavy operator layer, it is critical to limit reward variability, and "firewall" the heavy operators reward functions from rewards not accruing from their role as heavy service providers.

While Execution Tickets (ETs) may not ultimately be the favoured approach to separate consensus from execution, we believe their essence represents this separation well. In a world with ETs, where MEV (a.k.a., the value of the block production/payload service) is separated from consensus, heavy operators are less concerned with reward variability, timing games or other incentive-warping games which may occur. The map also shows that the payload service receives (at least) two inputs from the consensus services above: Heavy services finalise the outputs of the payload service, while light services constrain payload service operators by e.g., submitting them to inclusion lists (ILs), constructed along the lines of EIP-7547 or using different methods such as Multiplicity gadgets.

But how exactly do outputs of light services such as ILs constrain execution payload producers? In today's models of inclusion lists, validators are both the producers

and the enforcers

of the list. Separating services, the light operators become responsible for the production of the list, but we still require the heavy operators to be its enforcers. Indeed, validity of the execution payload with respect to Gasper is decided by heavy operators, who attest and finalise the valid history of the chain, ignoring invalid payloads. We see two options to connect production and enforcement:

- Strong coupling:

We could make the inclusion of a light certificate

mandatory for the validity of a beacon block produced by heavy operators, where a light certificate is a piece of data attested to by a large enough share from a light committee

, randomly sampled from all the light stake. The liveness of the overall chain then depends both on heavy operators and light operators: When the latter fail to surface a certificate, the heavy operators are unable to progress the chain with a new beacon block. On the other hand, given the inclusion of a certificate attesting to the presence and availability of an inclusion list, the execution payload tied to the beacon block would be constrained by the list, according to some validity condition (e.g., include transactions from the list conditionally on the blockspace remaining, or unconditionally).

- Weak coupling:

Tying liveness of the overall chain to the light layer means opening a new attack vector, where a party controlling a sufficient amount of light stake is able to block progress by refusing to provide light certificates. Loosening this constraint, we could expect

heavy operators to include the certificate and apply the list's validity conditions, should the certificate exist, without

mandating

it. This situation is closer to the status quo: Should the validator set (respectively, the set of heavy operators) be censoring, inclusion lists will neither be produced nor enforced (respectively, enforced). In the worst case, we are indeed back to the status quo, with the additional benefit of having a more accountable object lying around, the light certificate, attesting to the potential censorship of heavy operators who refuse to include it, in lieu of a more diffuse social process relying on e.g., nodes observing their own mempools or researchers staring at censorship.pics (no shade to censorship.pics, it's amazing

) In the best case, we widen the base able to participate in the production of such lists, and distribute economic benefits of censorship-resistance more broadly, beyond the validator set and towards the ecosystem of small nodes/light operators, who may not participate in the status quo. To make the best case an even likelier outcome, we could grease the wheels further by offering a reward (paid from issuance) to heavy operators who include a light certificate in their beacon blocks.

Additional analysis is required to understand the architecture of out-of-protocol services such as pre-confirmations or fast(er) finality (EigenLayer whitepaper, Section 4.1), in relation to the rainbow staking framework. Some of these services may still benefit from overloading heavy operators with additional duties, so while this is not a total elimination of all rewards outside of protocol rewards, it is a great mitigation participating towards making MVI more palatable.

Would it be worth unbundling further? The payload service is itself a bundle of two distinct services: "Execution gas", allocated via ETs, and "data-gas/blobs", allocated via some DA market. The separation was discussed at a few points in the past. First, as a way to achieve better censorship-resistance for blobs, by creating a "secondary market" focused on blobs. Second, as a way to prevent timing games impacting the delivery of blobs Practically, a mechanism akin to partial block delivery may be required for the consensus services to finalise the delivery of both parts of the full block, with blob transactions (carrying commitments to blobs and some execution to update rollup contracts) included in an End-of-Block section. While further analysis is required to understand the costs and benefits of this separation, we believe this direction will become increasingly relevant.

Towards SSF

We start the discussion with the most special protocol AVS: Gasper, the consensus mechanism of Ethereum. Its reward schedule is well-known, as well as its limitations regarding the size of its validator set measured in "individual message signers", and not in "stake weight". To achieve Single-Slot Finality (SSF), a drastic reduction of the validator set size is required, but how can we achieve this without booting out the least valuable participants, as measured in units of stake-weight-per-message?

Vitalik's post "Sticking to 8192 signatures per slot post-SSF: how and why" details various approaches, including the first model presented above (Approach 2). Some trade-offs are difficult, asking the question whether to go all in on decentralised staking pools (Approach 1), or rotating participation to allow for a larger set in aggregate, if not in constant participation (Approach 3).

We advocate for something mixing both Approaches 1 and 2 (Approach 1.5!)

- A heavy layer that is liquefied as it is today, all in on decentralised staking pools but with a little help from protocol gadgets (e.g., LSM or other enshrined gadgets);

- Combined with a solo-staker-friendly light layer constituting the second-tier, with its own light LSTs.

The question of allocating one of the 8192 SSF seats to operators remains (note that this 8192 number may not be the absolutely correct one). Incentives may need to be designed in order to discourage large operators or protocols disaggregating and occupying more seats in an attempt to push out their competition. These incentives may once again favour more capital efficient players, who can amortise the cost of a seat over a larger amount of stake they control and revenue they receive. The number of available seats is constrained by the efficiency of cryptographic constructions such as aggregating signatures, but as cryptographic methods or simply hardware progress, the number of seats may increase, loosening the economic pressure to perform as a seat owner. Yet, the pressure of MVI keeping overall rewards to heavy operators low remains.

The heavy layer's layers

Are we ruling out solo stakers from the heavy layer entirely? I do not believe we are. A re-phrasing frames well the terms of the debate, by calling solo stakers operating in the heavy layer solo operators

instead. What we want here is for a low-powered participant to still perform a meaningful role in the heavy service.

Enshrining an LSM-like system, which looks a bit like Rocket Pool, already makes a significant dent into the requirements. We take the number of "seats" in SSF as given by Vitalik, i.e., up to 8192 participants. Assume that we intend for 1/4th of the total supply of ETH to be staked under SSF, which is roughly 30 million ETH today. We would then require a single participant at the SSF table to put up about 3662 ETH, or about 8 million USD. Gulp!

With an LSM-like enshrined mechanism, we favour the emergence of partially collateralised pools (partial pools

). Rocket Pool requires a minimum bond of 8 ETH for 24 units of delegated stake (1:3), while the LSM defaults to 1:250. Even a (more) conservative choice of 1:100, in-between the two, brings us back to an operator needing to put up about 36 ETH, roughly 4 ETH more than the minimum validator balance required today. Regardless of the limit allowed by the LSM defaults, an LSP may require a higher collateralisation ratio from their operators, e.g., Rocket Pool could still force the use of 1:3 shares.

Could we go further? Running the gamut of existing LSPs, Diva coordinates solo operators with low capital via Distributed Validator Technologies (DVT). A sub-protocol of Gasper could allow for the creation of DVT pools

, where a virtual operator would behave akin to a solo operator does under the enshrined partial pool model. The virtual operator meanwhile requires DVT slots

to be collateralised by partial solo operators, and the Ethereum protocol could offer the ability to condition the validity of a Gasper message on the availability of a DVT'd signature performed by a sufficient quorum of partial solo operators.

Regardless of how the solo operator is synthesised (either directly under the enshrined partial pool model, or via quorum under the enshrined DVT model), the solo operator is then provided with the ability to accept deposits from heavy delegators. Heavy delegators then tokenise their deposits as shares of an LSM-like system. These shares are received as assets by an LSP, according to the LSP's own internal rules on the composition of its basket of operators. In exchange, the LSP mints a fungible asset, better known as an LST. Voilà!

Dynamics here are interesting. An LSP wishes for their LST to be credible

, i.e., an LST is not credible if holders do not believe that the operators holding their principal are good agents. In the worst case, malicious operators may seek to accumulate as much stake as possible in order to perform some FFG safety fault, at the cost of getting slashed and devaluing the LST. An LSP curating a basket of good operators mints a credible LST, which has value to its holders.

Gadgets such as DVT bolster this credibility, as long as entropy of the DVT set can be ascertained. Importantly, this is not something that the Ethereum protocol needs to concern itself with. The protocol may not be able to procure itself an inviolable on-chain proof that a DVT set's entropy is high, for instance because it is composed with unaffiliated solo stakers. Yet the open market may recognise such attributes, and value the LST derived from an LSP with good curation more than an LST with poor composition. While participating in the heavy layer may not be the most effective vehicle for solo stakers to express their agency on the network, the optimist in us believes this is a potent avenue and one that just makes good business sense.

Open questions

- We would like to understand the limits of "protocol re-staking", i.e., the ability for the same stake to be burdened with the provision of both heavy and light services. We distinguish in this post only two categories of services, meaning that holders have an "opt-in" choice to make for each of the two services, but should the unbundling go further, allowing for "opt-in" choice of every heavy or light service? Is the addition of protocol services permissionless, or do they require network upgrades?

- We pose the question of service-completeness

, i.e., do we now have mechanisms addressing all services which protocol agents may wish to provision? To answer this question, we go back to a distinction already discussed in the PEPC FAQ, originally made by Sreeram Kannan about EigenLayer: According to Sreeram [in this Bell Curve podcast episode], there exists three types of use cases for Eigenlayer (timestamp 26:25):

- Economic use cases

(timestamp 27:44): The users of the Actively Validated Service (AVS, a service provided by validators via Eigenlayer) care that there is some amount at stake, which can be slashed if the commitments are reneged upon.

- Decentralisation use cases

(timestamp 30:05): The users of the AVS care that many

independent parties are engaged in the provision of the service. A typical example is any multiparty computation scheme, where collusion between parties defeats the guarantees of correct execution (e.g., yielding them the power to decrypt inputs in the case of threshold encryption).

- Block production use cases

(timestamp 40:10): Validators acting as block producers can make credible commitments to the contents of their blocks.

In the PEPC FAQ, we have argued that as an execution-layer-driven gadget, PEPC resolved primarily the third use case, i.e., block proposers making commitments about some properties which their blocks must satisfy. We ask whether the distinction of heavy and light services directly map to the other two use cases, economic security and decentralisation

services, respectively. To provide more details:

- Are there other valuable heavy services? Economic security services seek to make a claim backed by the largest amount of slashable stake. [Recent discussions on pre-confirmations](#) have hinted at this property being relevant, beyond the commitment made by a single block proposer.

- Which other valuable light services exist, for which the value proposition of solo stakers is well-suited? Censorship-resistance services are an ideal category, by rewarding participants who are uncorrelated with each other. Do other categories of protocol services exhibit the same dynamics?

- Economic use cases

(timestamp 27:44): The users of the Actively Validated Service (AVS, a service provided by validators via Eigenlayer) care that there is some amount at stake, which can be slashed if the commitments are reneged upon.

- Decentralisation use cases

(timestamp 30:05): The users of the AVS care that many

independent parties are engaged in the provision of the service. A typical example is any multiparty computation scheme, where collusion between parties defeats the guarantees of correct execution (e.g., yielding them the power to decrypt inputs in the case of threshold encryption).

- Block production use cases

(timestamp 40:10): Validators acting as block producers can make credible commitments to the contents of their blocks.

In the PEPC FAQ, we have argued that as an execution-layer-driven gadget, [PEPC](#) resolved primarily the third use case, i.e., block proposers making commitments about some properties which their blocks must satisfy. We ask whether the distinction of heavy and light services directly map to the other two use cases, economic security and decentralisation services, respectively. To provide more details:

- Are there other valuable heavy services? Economic security services seek to make a claim backed by the largest amount of slashable stake. [Recent discussions on pre-confirmations](#) have hinted at this property being relevant, beyond the commitment made by a single block proposer.

- Which other valuable light services exist, for which the value proposition of solo stakers is well-suited? Censorship-resistance services are an ideal category, by rewarding participants who are uncorrelated with each other. Do other categories of protocol services exhibit the same dynamics?

- What are the general economics of light services? What do the light capital requirements (hardware, partially slashable stake) for service provision induce for the light services economy? What is the role of the light LST minted from delegated shares of light services? How to decide on issuance towards light services, and if multiple light services are offered, how should one allocate the issuance between different services?

- … how do we implement all of this?