Protocol services

Ethereum Protocol Studies — 28/03/2024

Barnabé Monnot

Robust Incentives Group (RIG), Ethereum Foundation

Quick intro

Jan. 2020: Joined the Robust Incentives Group at EF.

Since then, work on:

- Proof-of-Stake consensus
- EIP-1559 / Fee market mechanisms
- MEV / Proposer-Builder Separation
- Mechanism design more generally, and side quests :)

https://rig.ethereum.org

Today

Themes of the talk:

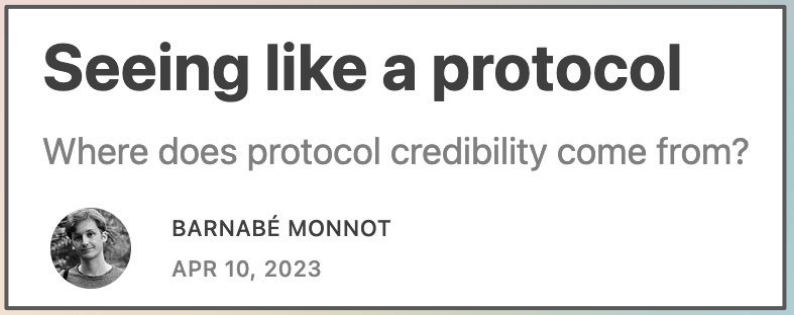
- Seeing like a protocol
- The block production service
- The consensus service

Seeing like a protocol

“Seeing”?

Post written a year ago, addressing (partly) the questions:

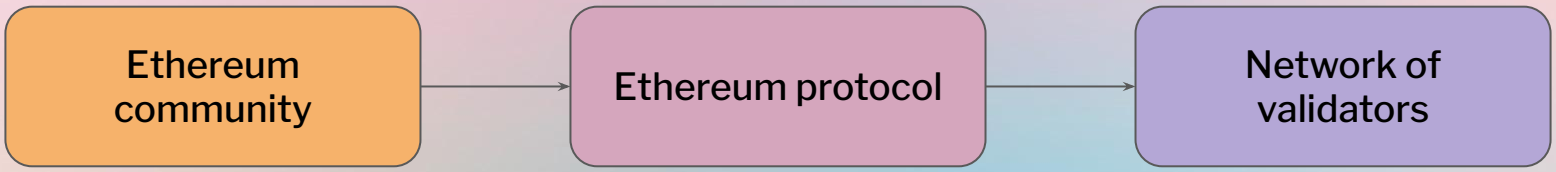
- Where does protocol credibility come from?
- How far does the protocol extend?
- What should it see?



https://barnabe.substack.com/p/seeing-like-a-protocol

tl;dr

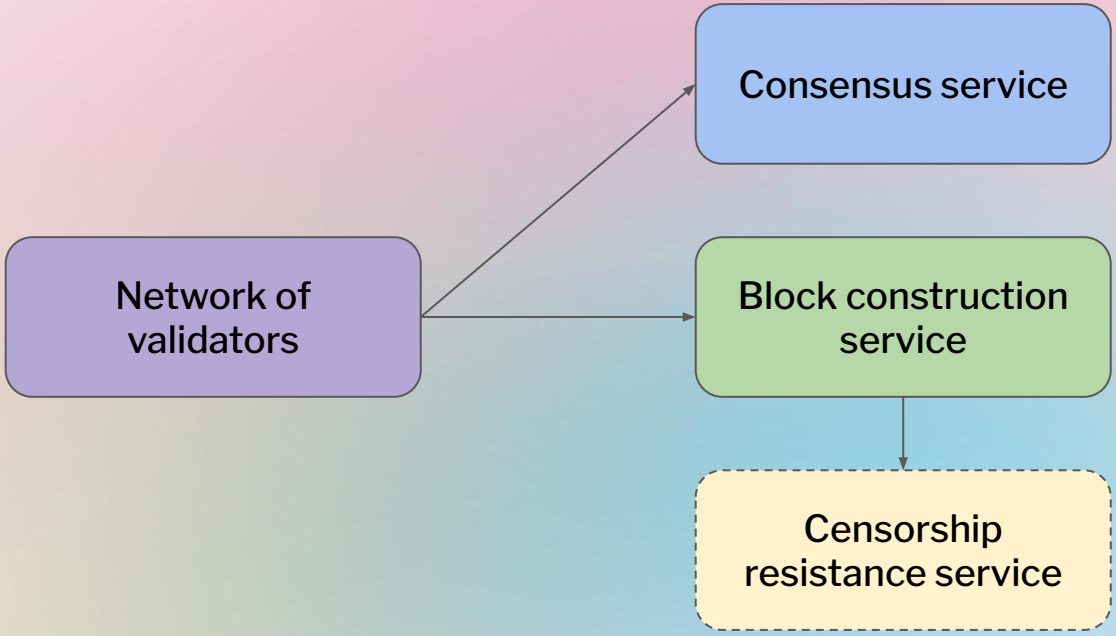
The Ethereum *protocol* is set up by a diffuse "*community*", stakeholders of the protocol. "Rough consensus" governance.



Protocol's goal: **Decentralised provision of blockspace for *users* to achieve maximal welfare ⇒ minimal rents.**

Validators run the protocol.

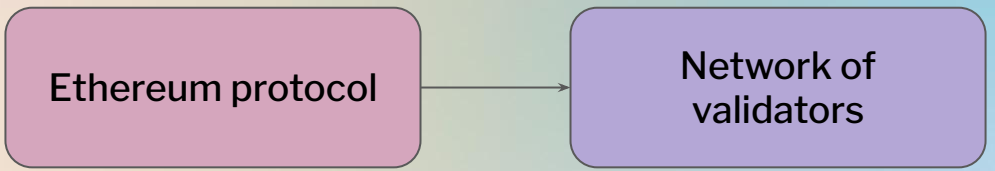
Validator services



The Protocol-Validator problem

How to make validators achieve the goals of the protocol?

- **Protocol introspection**
  Obtain credible signals of the environment in protocol state
- **Protocol agency**
  Respond to signals with updates, rewards or punishments

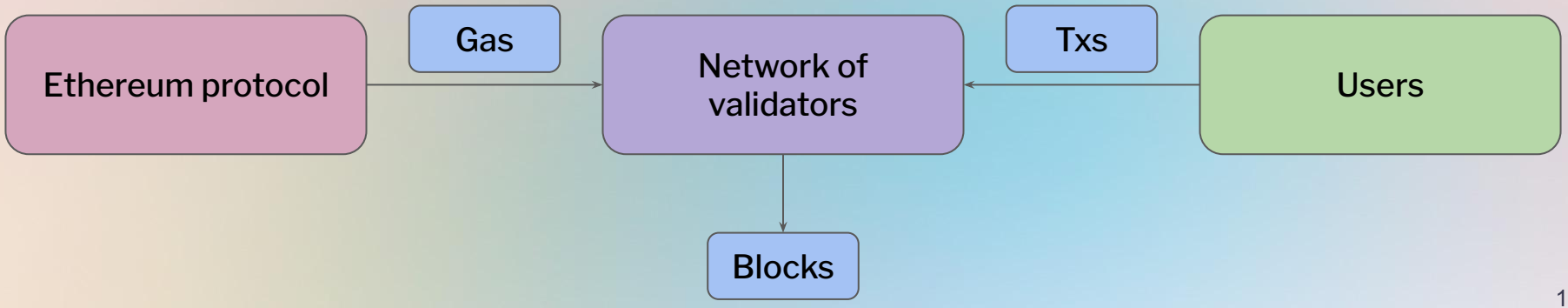


The block production service

Validators as resource allocators

Protocol lets validators-as-block-producers **consume** resources
Supply constrained to guarantee **low verification costs**

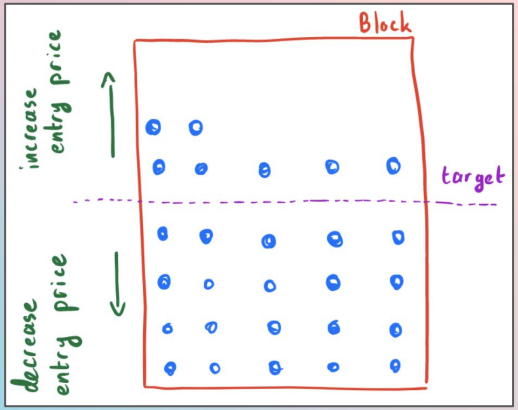
Validators produce **blocks**,
meeting **demand for transactions** with **supply of resources**



EIP-1559: Resource introspection!

Protocol quotes a reserve price,
dynamic congestion pricing

- **Demand signal**
  Blocks target 15 million gas use, block limit 30 million
- **Update rule:** Gas use > Target
  ⇒ Reserve price increases



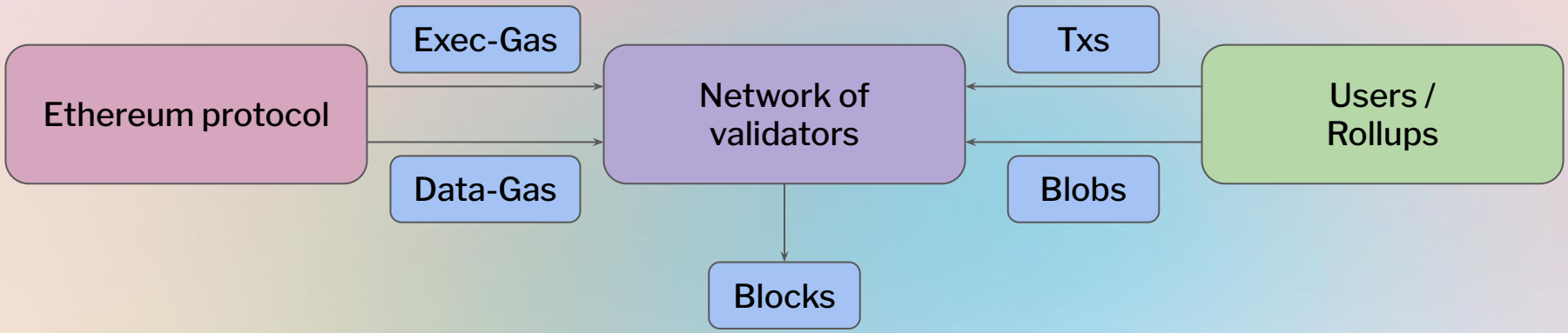
$$b_{n+1} = b_n \cdot (1 + \gamma \cdot \frac{g_n - T}{T})$$

2-dimensional EIP-1559

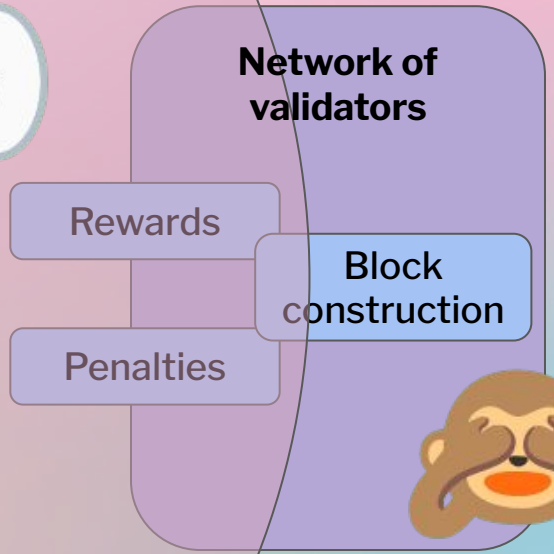
Live!!

EIP-4844: Separate “exec-gas” and **data availability (DA) gas**

DA: Consumed by rollups, L2 solutions secured by Ethereum



Ethereum protocol



Ethereum protocol

Rewards

Penalties

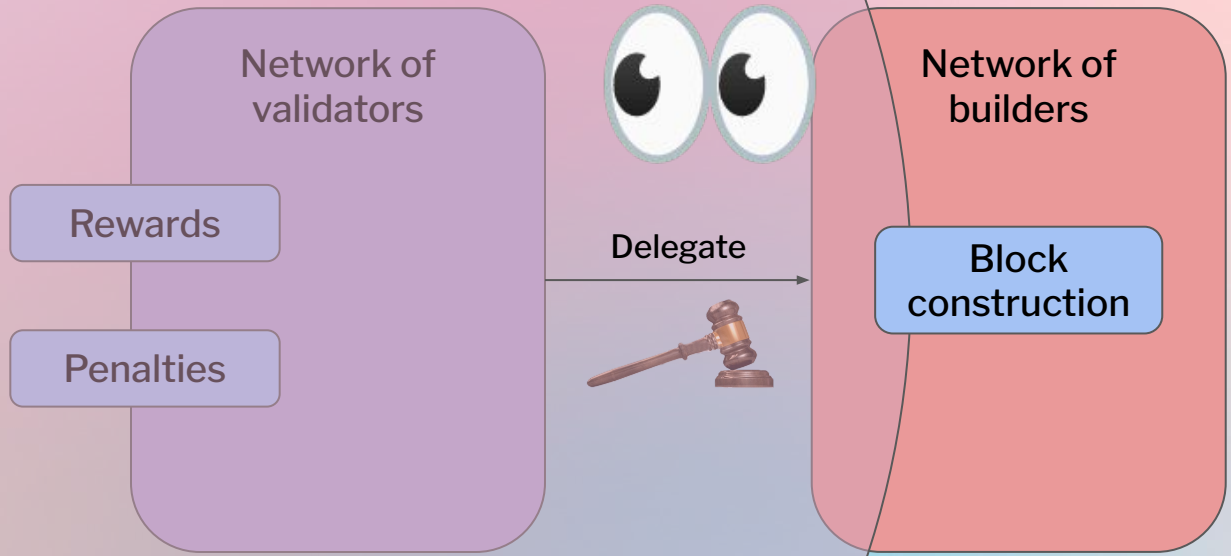
Network of validators

Delegate

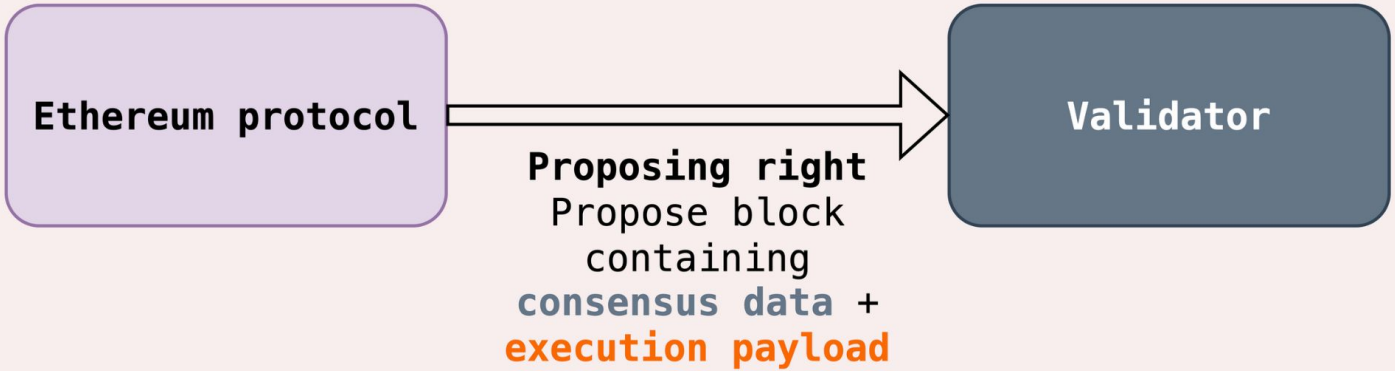
Network of builders

Block construction

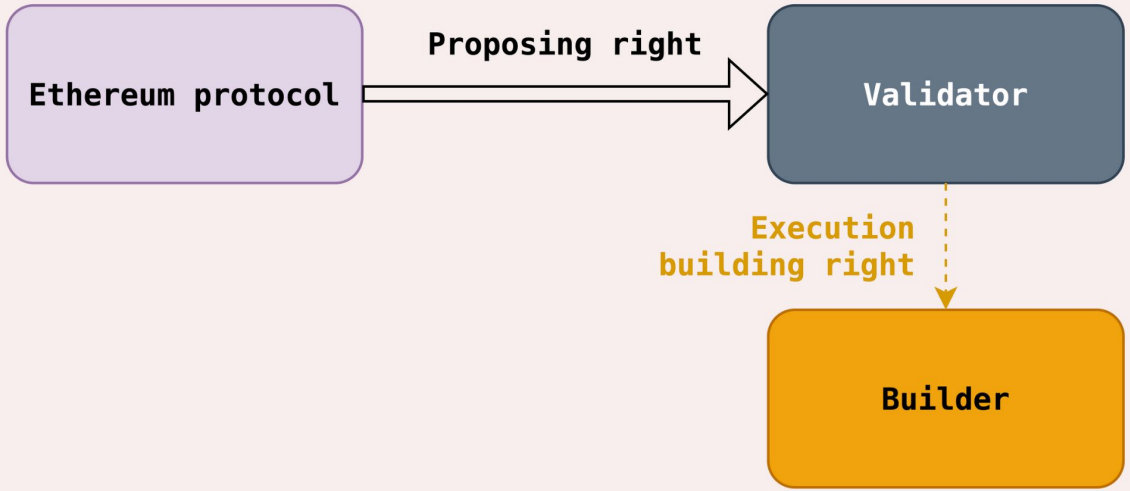
Ethereum protocol

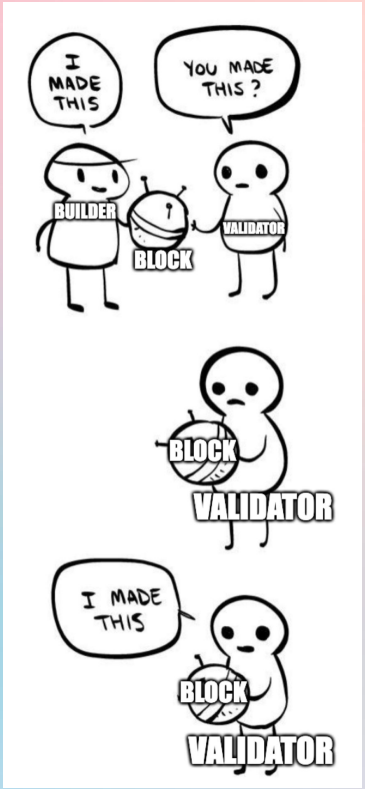


Focus on proposing rights



MEV-Boost: Validators call upon builders





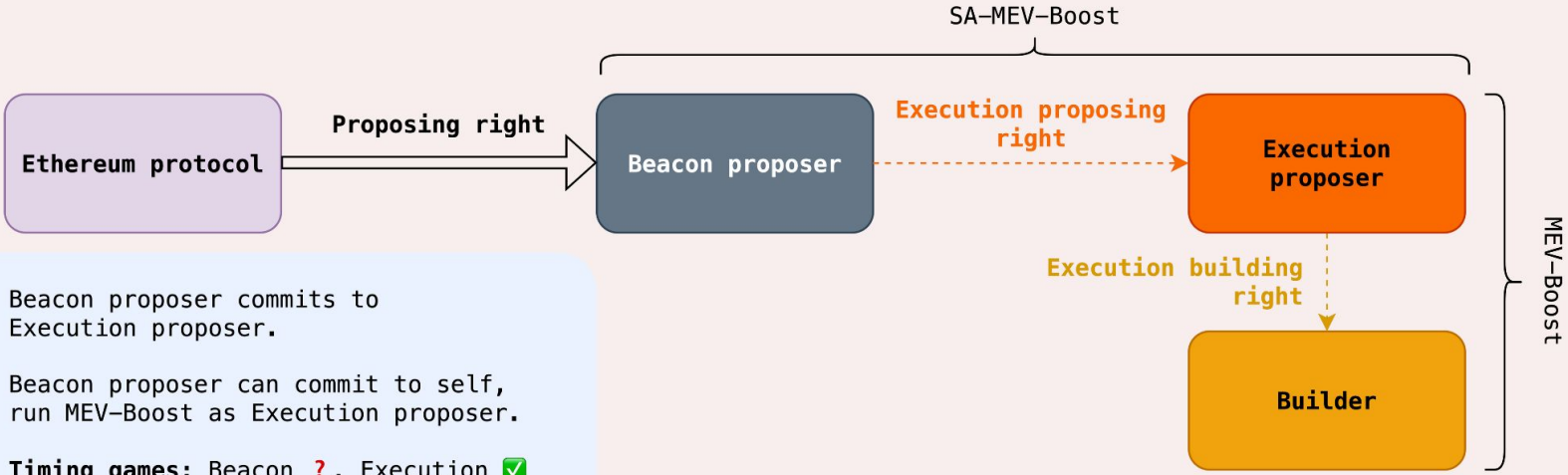
Block-auction ePBS: Execution-consensus separation

Beacon proposer commits to
Execution proposer+builder.

Beacon proposer can commit to self,
~ local building.

Timing games: Beacon ✅, Execution ❌

Slot-auction ePBS



Beacon proposer commits to Execution proposer.

Beacon proposer can commit to self, run MEV-Boost as Execution proposer.

Timing games: Beacon ❓, Execution ✅

Block-auction ePBS: Execution-consensus separation

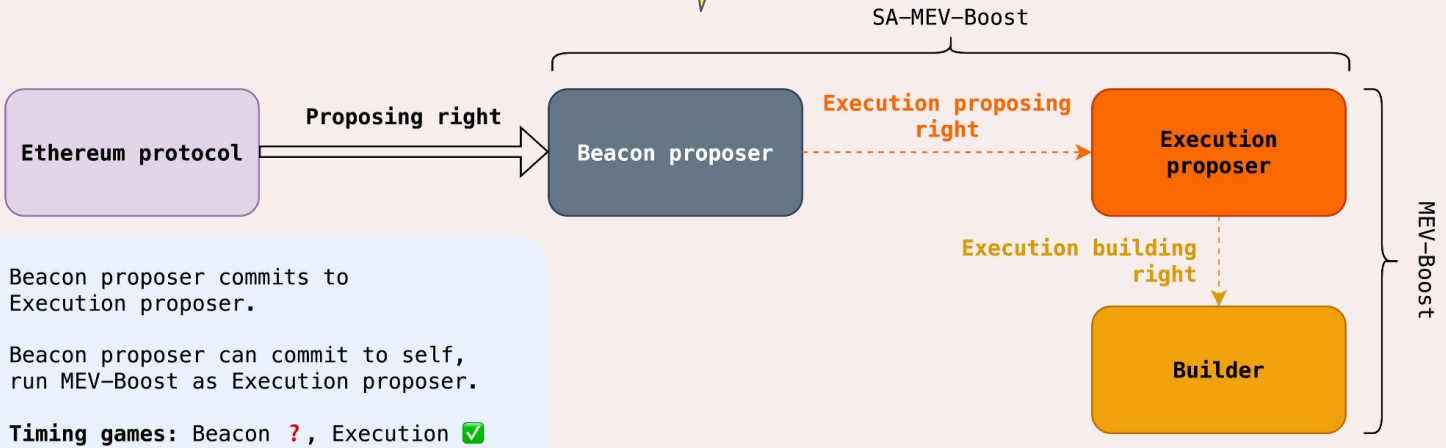
Beacon proposer commits to
Execution proposer+builder.

Beacon proposer can commit to self,
~ local building.

Timing games: Beacon ✅, Execution ❌

VS

Slot-auction ePBS

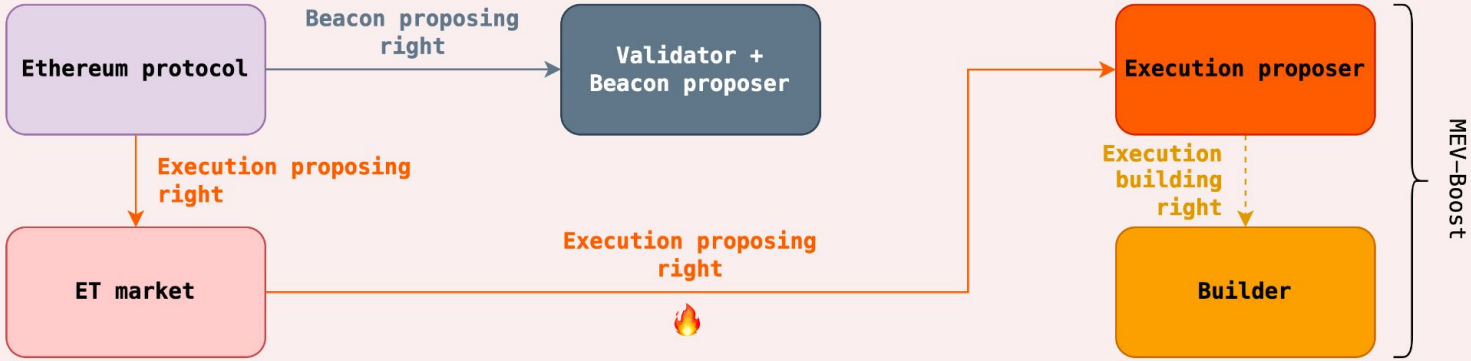


Beacon proposer commits to
Execution proposer.

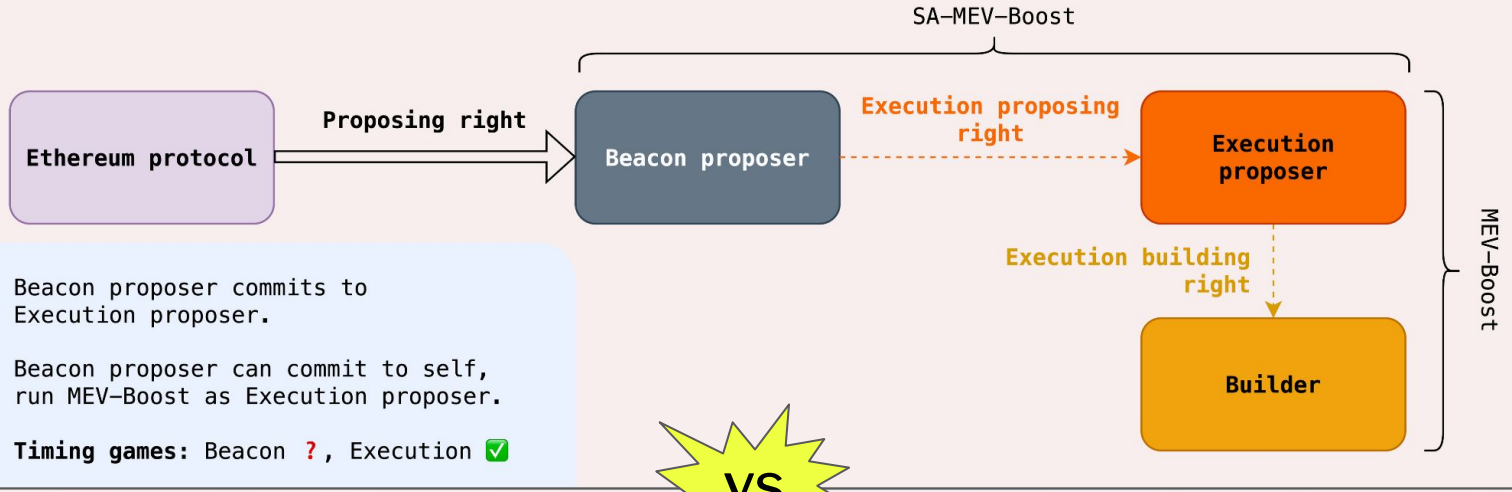
Beacon proposer can commit to self,
run MEV-Boost as Execution proposer.

Timing games: Beacon ?, Execution ✅

Execution Tickets (ETs)



Slot-auction ePBS



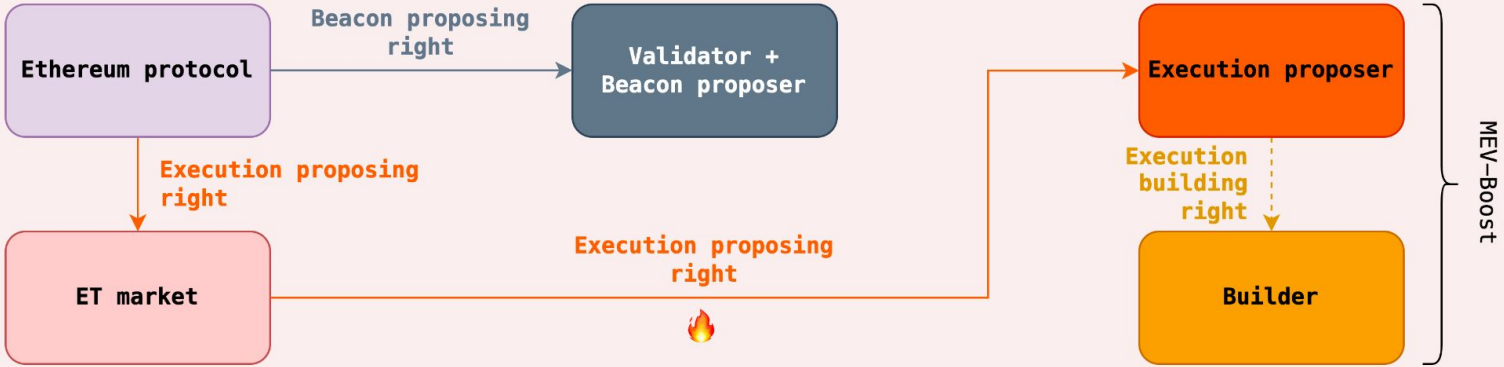
Beacon proposer commits to Execution proposer.

Beacon proposer can commit to self, run MEV-Boost as Execution proposer.

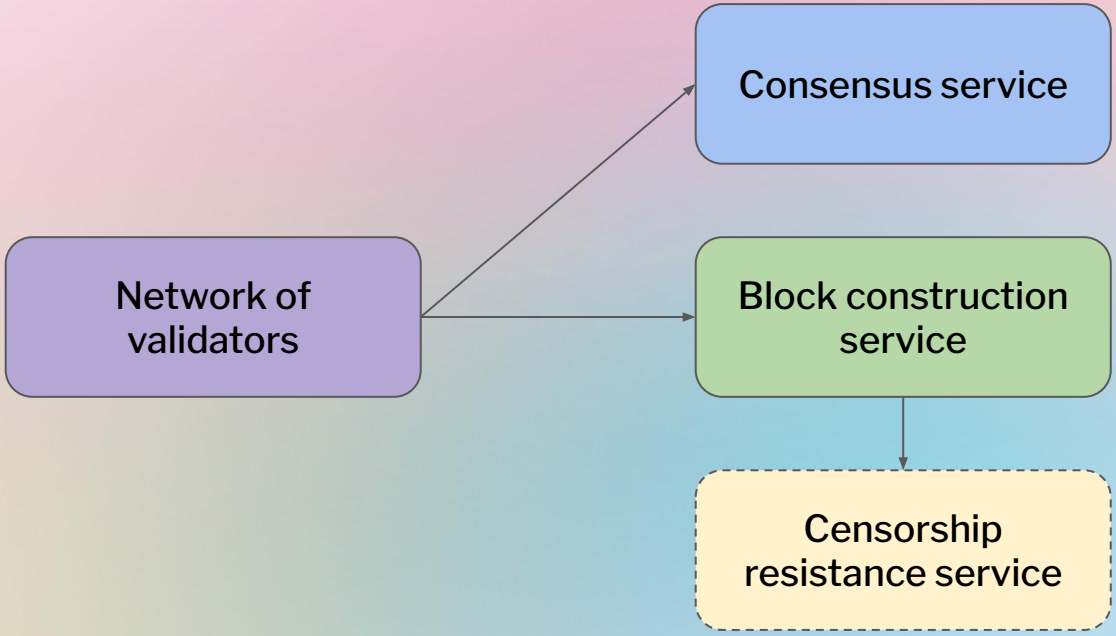
Timing games: Beacon ❓, Execution ✅

VS

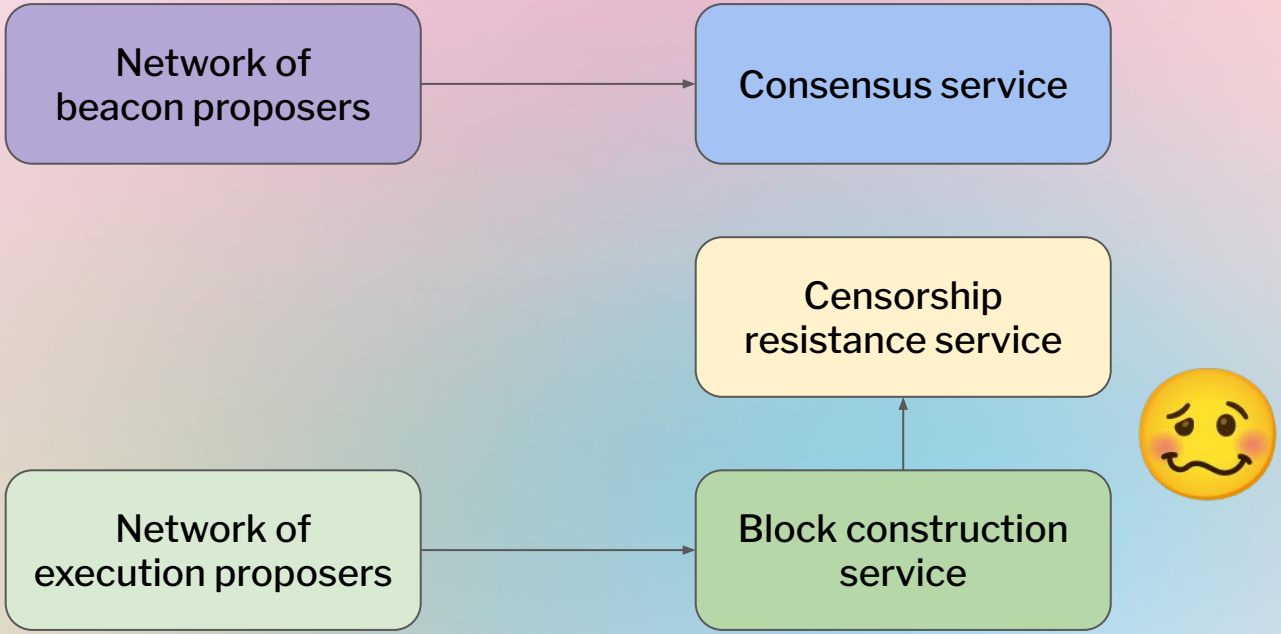
Execution Tickets (ETs)

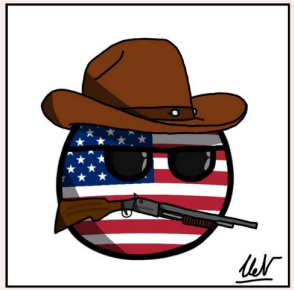


Validator services

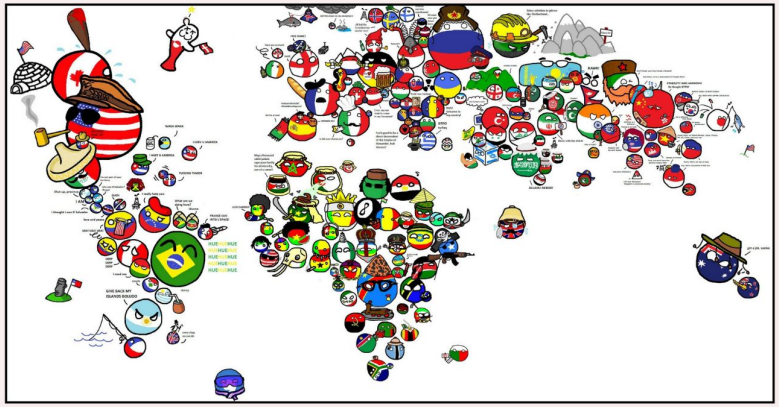


Validator services





Low preference entropy



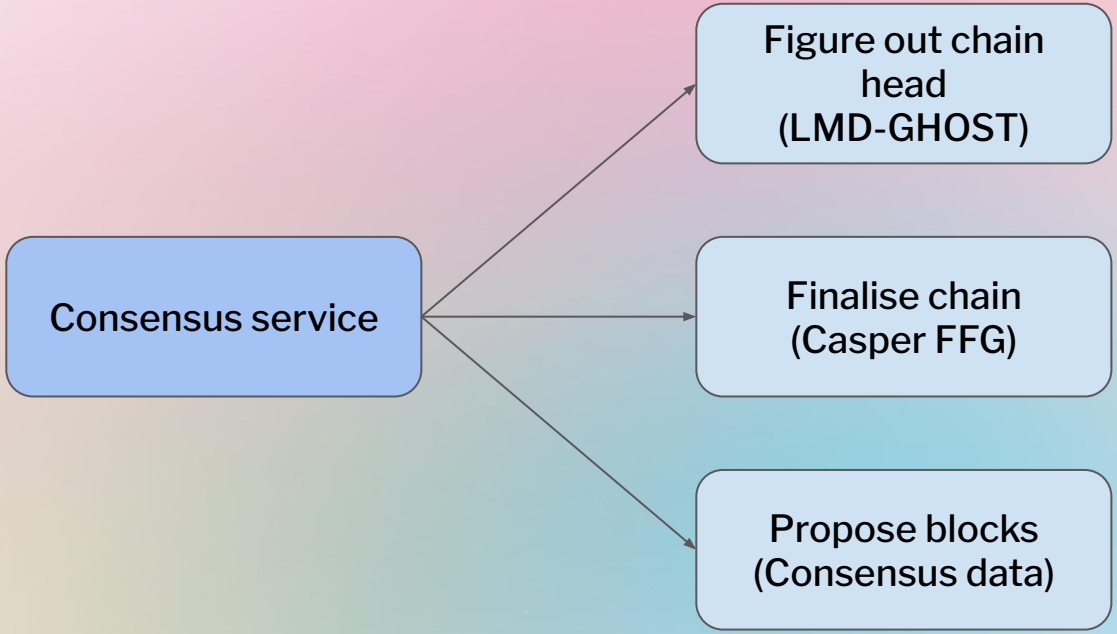
High preference entropy

We want a **decentralised** set of operators because they express a wider set of preferences!

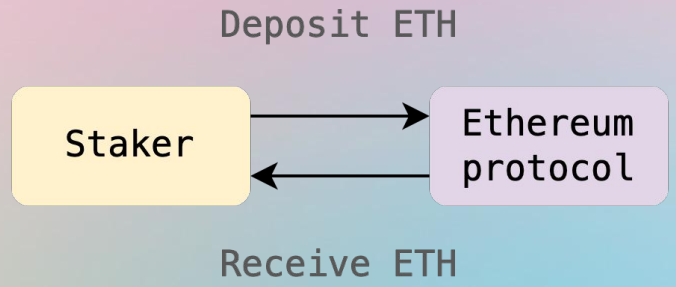
- When **making a block**, include txs that others dislike!
- When **participating in consensus**, decorrelation => resilience!

The consensus service

Validator services



The world according to eth



Why stake?

Credible commitment to good service provision, the protocol can make statements such as

“**If X happens, Y billions of dollars are lost**”.

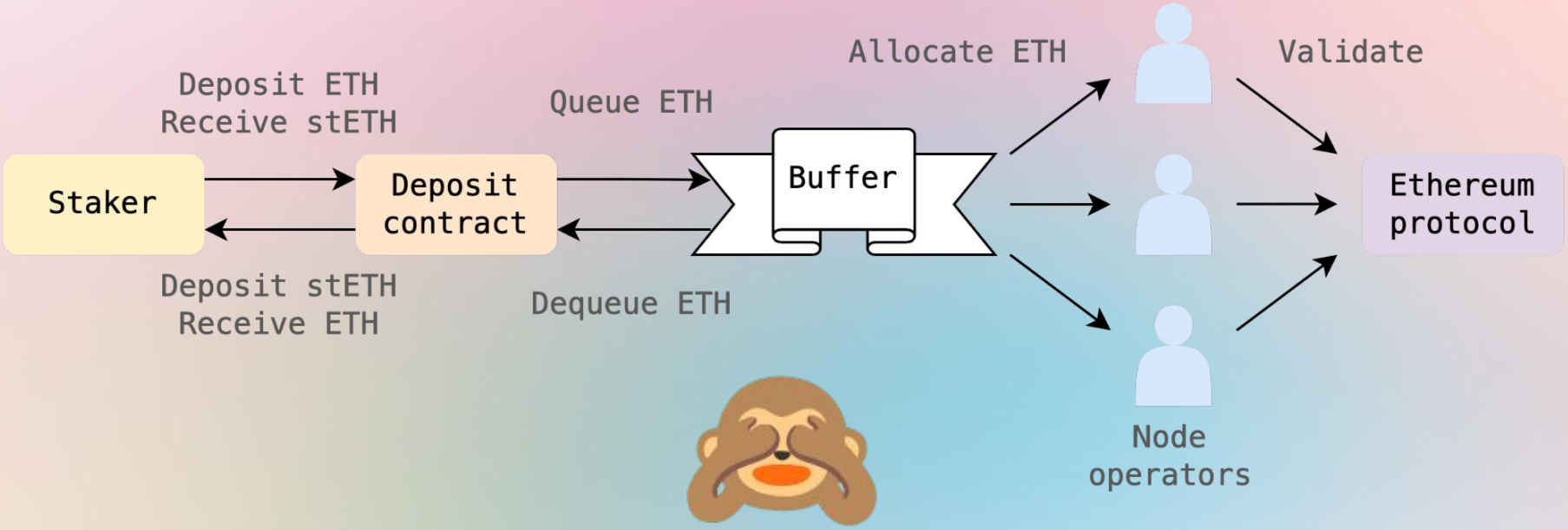
Commitment requires capital, capital wants to be free,

enter Liquid Staking Protocols…

Note that the statement above doesn’t specify whose dollars…

Protocol doesn’t see delegations!

The world out there



Protocol service providers

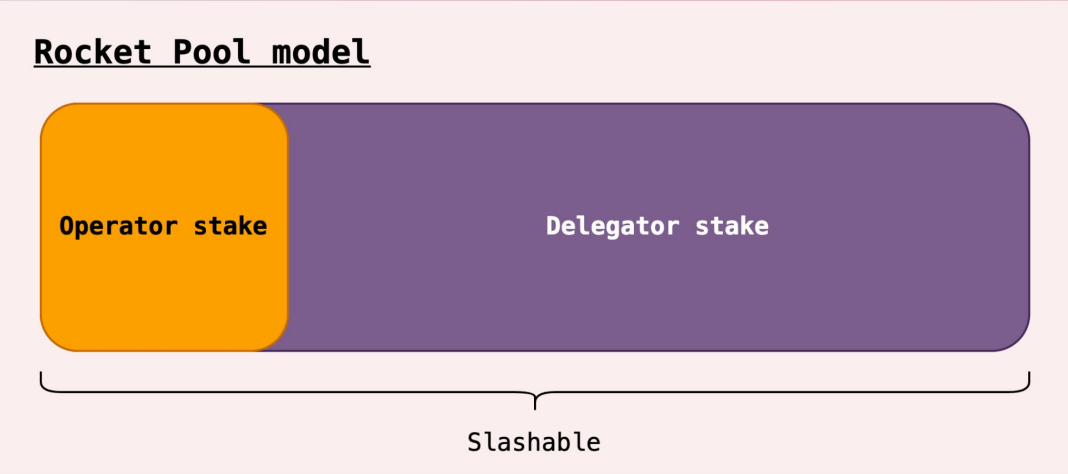
Two classes of providers:

- **Solo operators:** *A priori* untrusted, think living room validators, solo stakers (operators + own capital)
- **Professional operators:** *A priori* trusted, think registered companies, big staking providers

Not a binary distinction!

More like credible signal, to be learned over time.

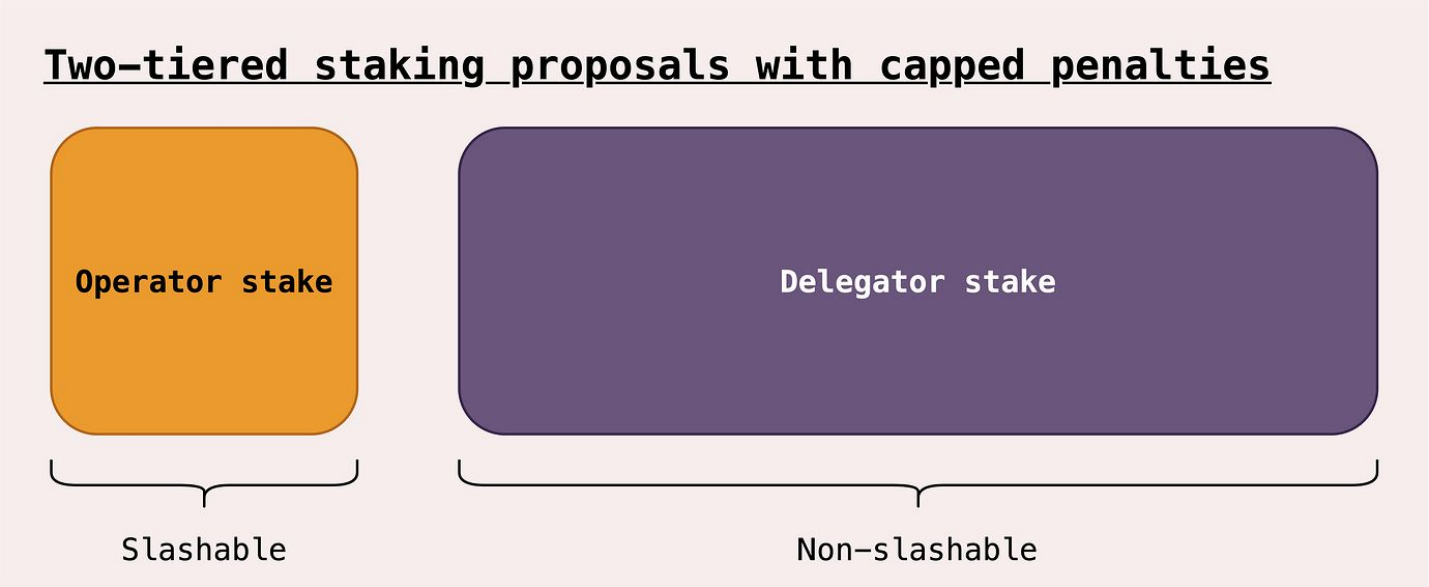
(Liquid) Staking Protocols may employ a mixture of both types.



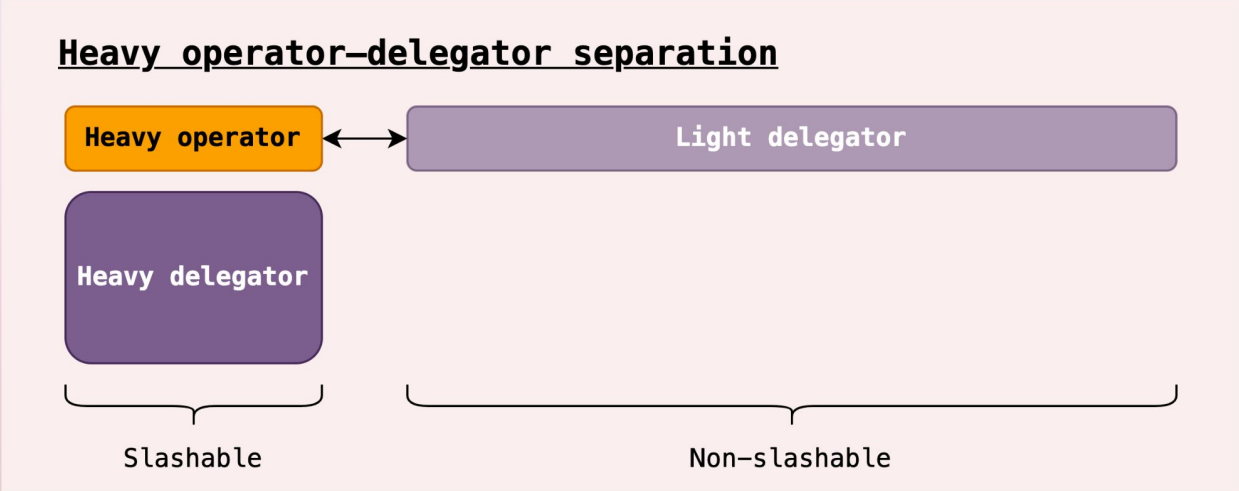
Take Rocket Pool, operator can be solo staker,
put up some **ETH as collateral**, delegators fill the **remainder**.

Still, capital efficiency + cost pressure mean
LSPs rely on professional operators significantly.

Strawman:



- **Premise 1:** People want to stake (“do something with ETH”).
- **Premise 2:** We can make *only* the people who actually perform validation (the operators) liable.



- **Issue:** People want yield, so they'll want to be slashable
  Will recreate an **operator—delegator separation** (heavy).

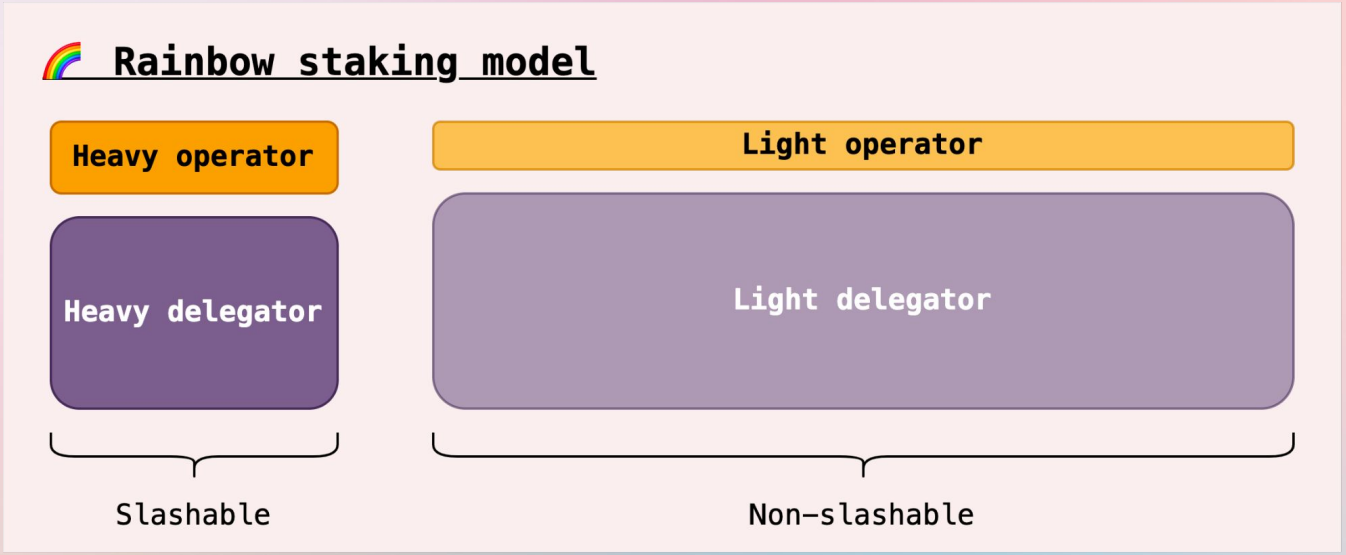
You could still have light delegators getting yield for choosing heavy delegators well, or doing something useful… **but what?**

Protocol and staking pool changes that could improve decentralization and reduce consensus overhead

[V. Buterin]

Here are a few ideas for how these **small-staking roles** could work:

- Each slot, 10000 small-stakers are randomly chosen, and they can sign off on what they think is the head of that slot. An LMD GHOST fork choice rule is run using the small-stakers as input. If the **small-staker-driven fork choice** and the **node operator-driven fork choice** ever diverge, the user's client does *not* accept any block as finalized, and displays an error. This forces the community to mediate the situation.
- A delegator can send a transaction declaring to the network that they are online and are willing to serve as a small-staker for the next hour. For a message (block or attestation) from a node to count, **both the node and a randomly selected delegator must sign off**.
- A delegator can send a transaction declaring to the network that they are online and are willing to serve as a small-staker for the next hour. Each epoch, 10 random delegators are chosen as **inclusion list providers**, and 10000 more are chosen as voters. These are chosen k slots in advance, and given a k-slot window to publish a message on chain confirming that they are online. Each confirmed chosen inclusion list provider can publish an inclusion list, and a block is invalid unless for each inclusion list, it either (i) it contains the transactions in that inclusion list, or (ii) it contains votes from 1/2 of chosen voters showing that the inclusion list is unavailable.

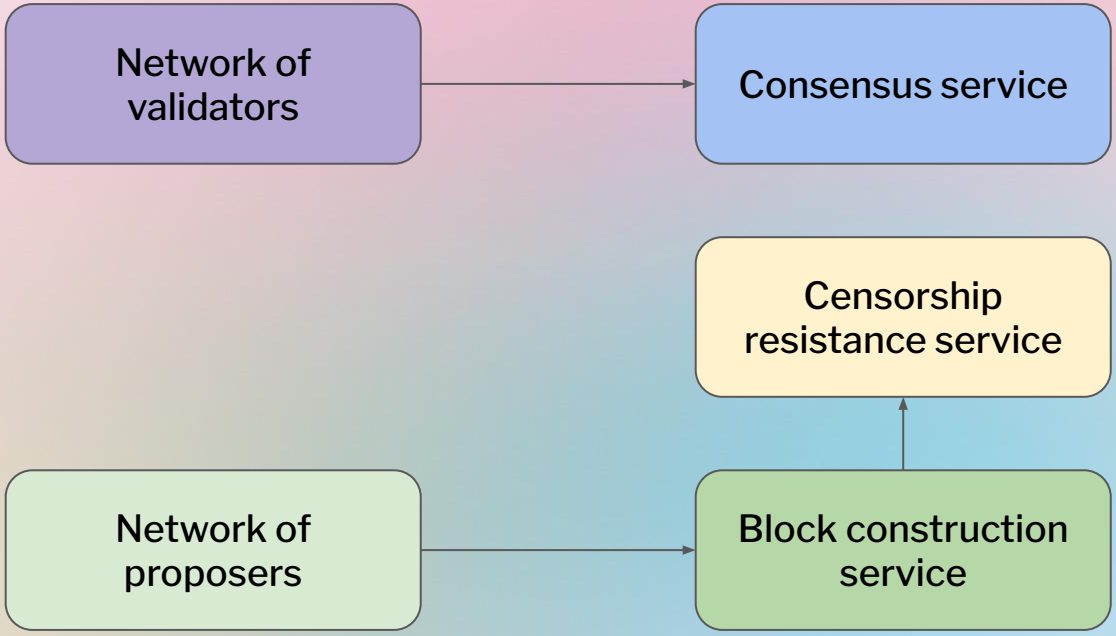


Idea: Let light delegators delegate to a **distinct set of operators**.

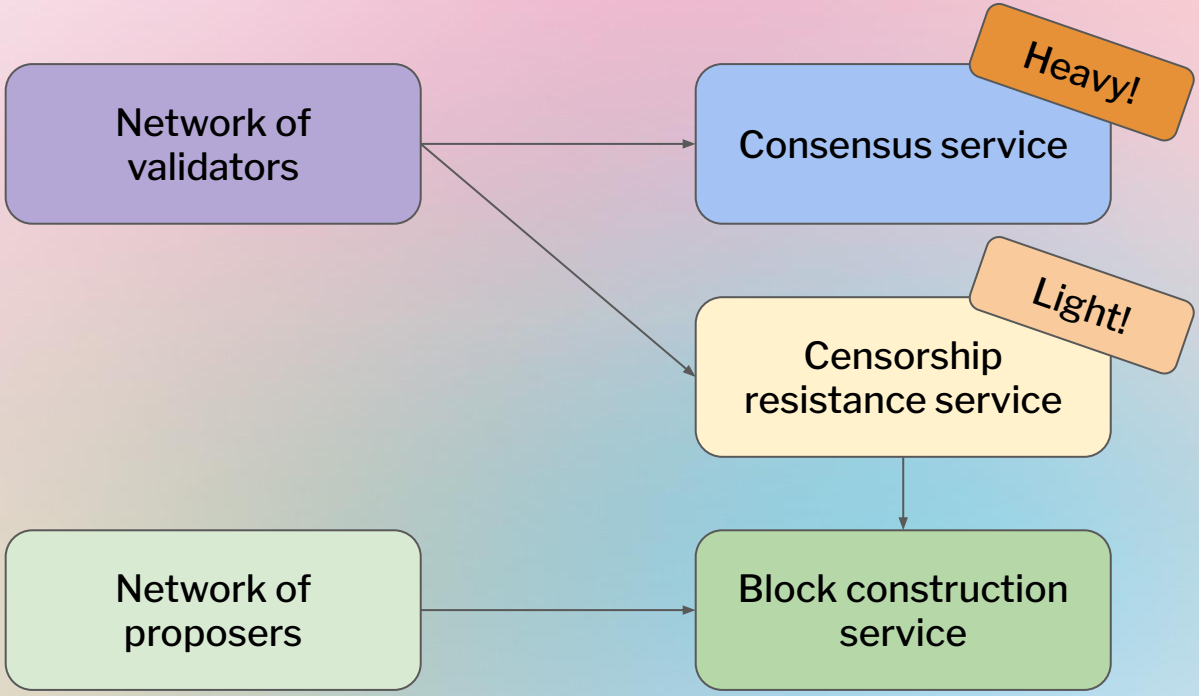
Light delegators **“back”** light operators, give them weight.

None of the light stack is slashable, no pressure to rebuild the LSP stack with centralising forces => **Solo operator-friendly!**

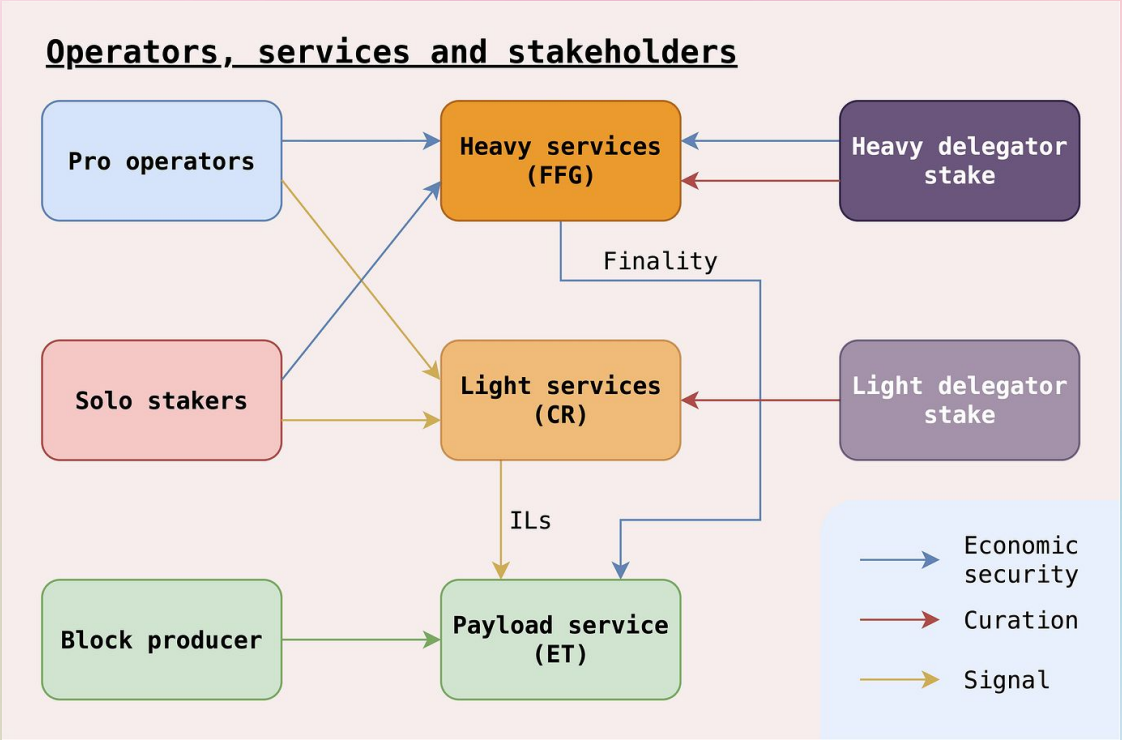
Validator services



Validator services



Validator services



About inclusion lists

The real definition of inclusion list:
“A way for the most decentralised set of Ethereum to input their preferences into the make-up of the chain.”

- EIP-7547: Inclusion lists
- ROP-9: Multiplicity gadgets
- Committee-based inclusion lists (COMIS)

Key goal: Block co-creation
👏 Get 👏 that 👏 input! 👏

Thank you!

https://rig.ethereum.org

Bonus: Issuance

Lately, discussions around issuance.
High issuance => Lots of people stake => Lots of stake under LSPs => LSTs are money

(grotesquely simplified version of the argument)

New posts on revising the current reward curve:

- Electra proposal: Moderate rewards
- Case for targeting: Tune issuance, reach range of ETH at stake

Bonus: Issuance

Rainbow staking to increase solo staker sustainability?