Single Slot Finality
And the future of staking

Francesco
Researcher, EF

What are we trying to achieve

- ❏ Improve the consensus protocol: get provable, optimal security properties
- ❏ Faster finality:
  - ❏ No UX/security tradeoff
  - ❏ Rollup interop speed not bottlenecked by L1

What’s blocking us?

1M+ validators, too many signatures per slot.

❑ High verification time

❑ High bandwidth required

What's blocking us?

1M+ validators, too many signatures per slot. In the worst case:

- ❑ High verification time
- ❑ High bandwidth required

… but we don't actually have 1M independent validators: 11k nodes according to https://monitoreth.io/nodes. We already have 34k validators voting every slot, so we know we can handle this number.

What's blocking us?

1M+ validators, too many signatures per slot. In the worst case:

- ❏ High verification time
- ❏ High bandwidth required

… but we don't actually have 1M independent validators: 11k nodes according to https://monitoreth.io/nodes. We already have 34k validators voting every slot, so we know we can handle this number.

=> Maxeb (EIP-7251) allows up to 2048 ETH validators, and gives a way for existing validators to consolidate

What else do we need?

❑ **Fast-finalizing, dynamically available consensus protocol**:

a provably (ideally optimally) secure consensus protocol with all the properties we care about

❑ **(Active) validator set capping:** a way to **ensure** that the load is always manageable. Can’t just go from 1M validators to 30k, “turn on SSF” and then go back to 1M

What else do we need?

❑ **Fast-finalizing, dynamically available consensus protocol**:

a provably (ideally optimally) secure consensus protocol with all the properties we care about

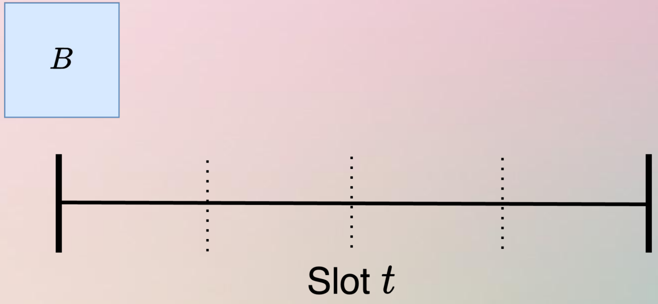
❑ **(Active) validator set capping:** a way to **ensure** that the load is always manageable. Can't just go from 1M validators to 30k, "turn on SSF" and then go back to 1M

3SF:
3-Slot Finality

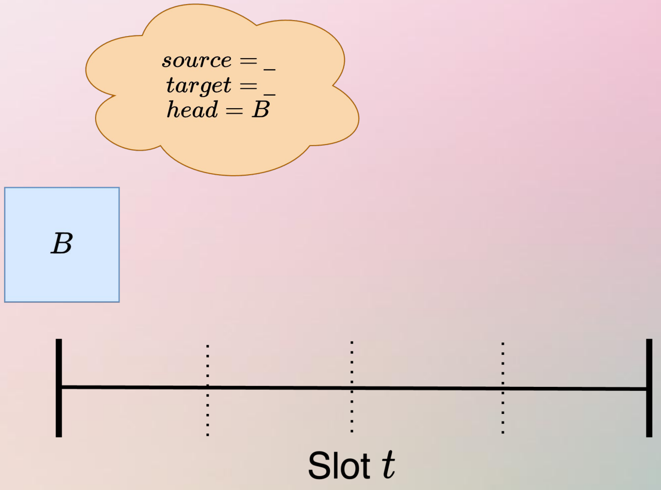
3SF: 3-Slot-Finality

- Like the current protocol, the fork-choice combines a version of LMD-GHOST with Casper-FFG as a finality gadget
- Finality is pipelined over multiple slots: only one voting round per slot

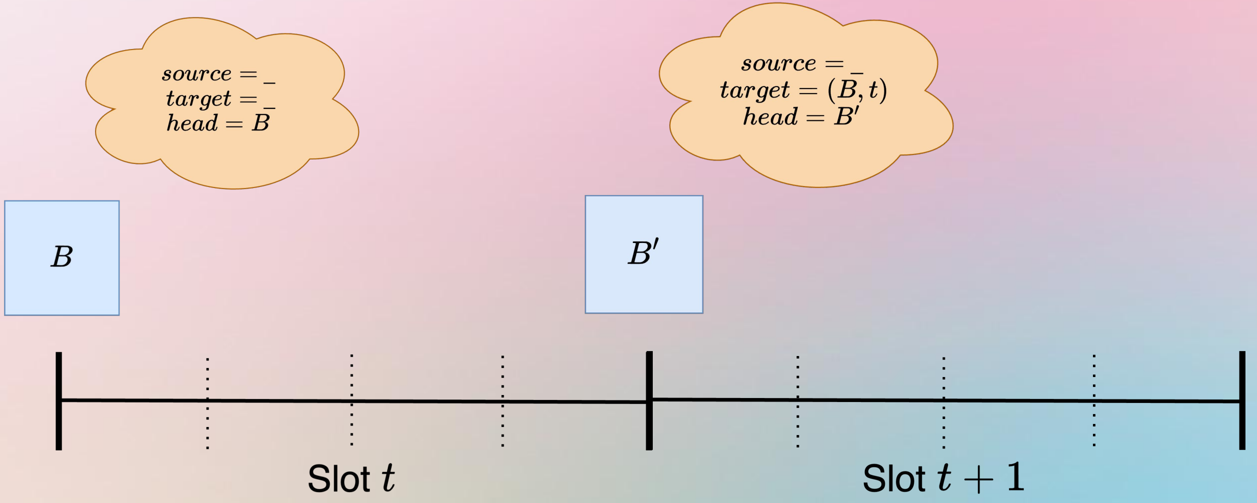
3SF: 3-Slot-Finality



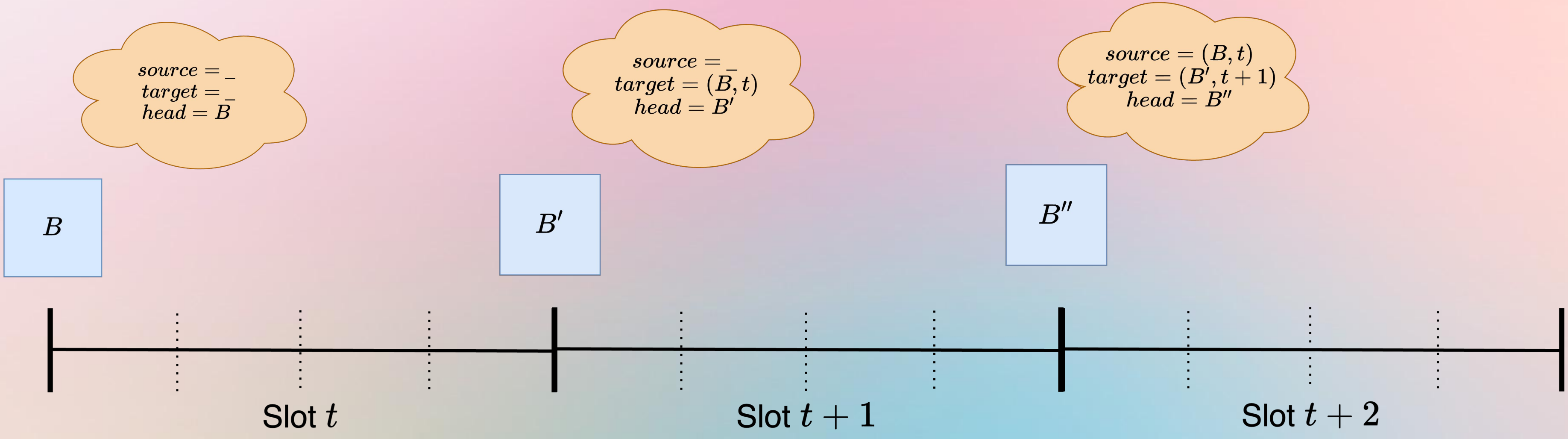
3SF: 3-Slot-Finality



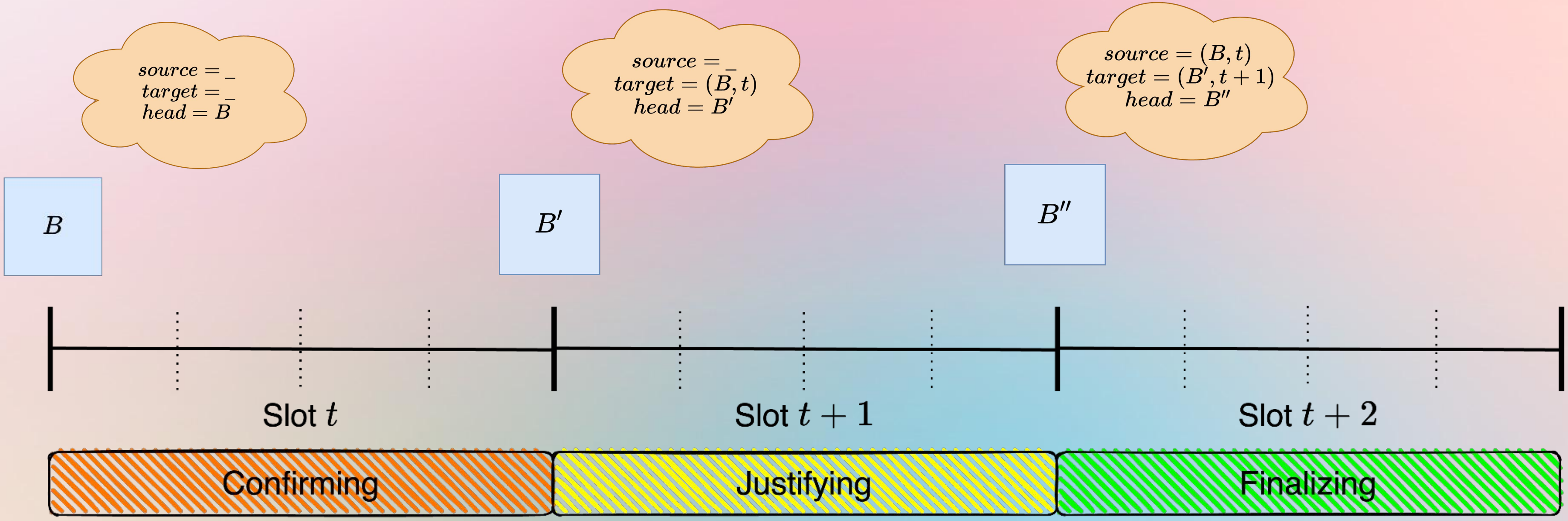
3SF: 3-Slot-Finality



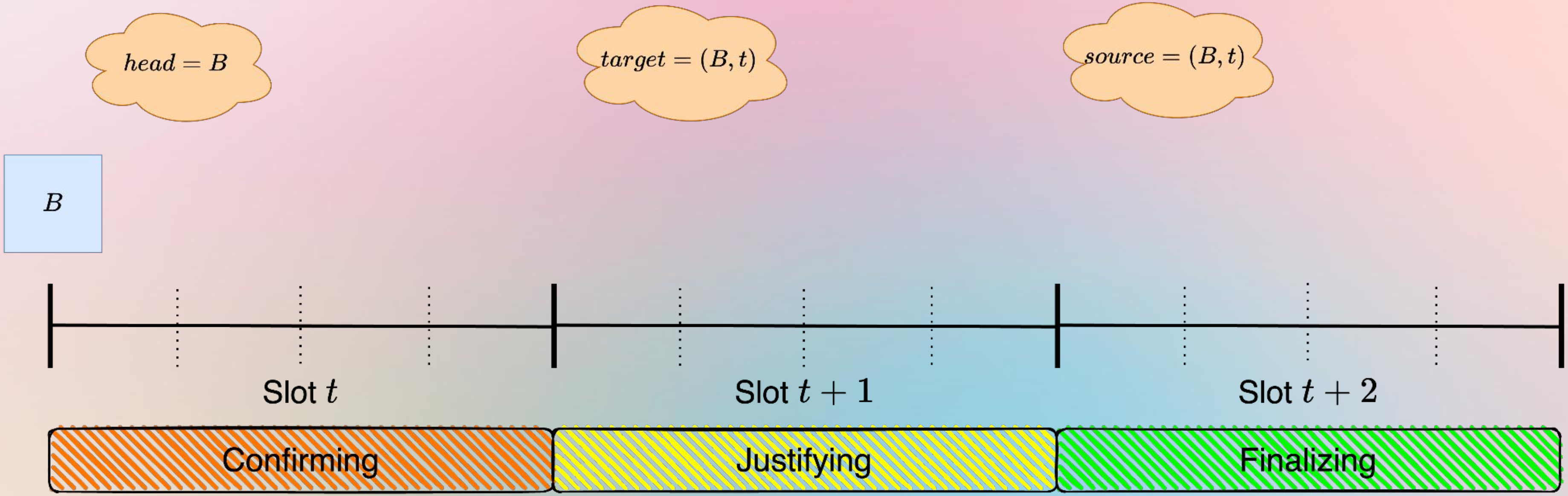
3SF: 3-Slot-Finality



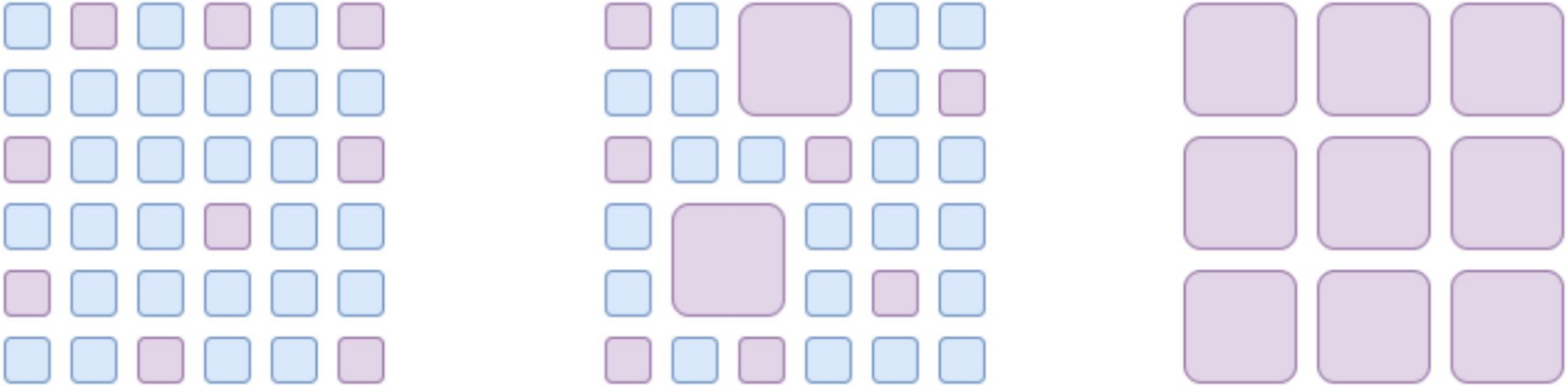
3SF: 3-Slot-Finality



3SF: 3-Slot-Finality



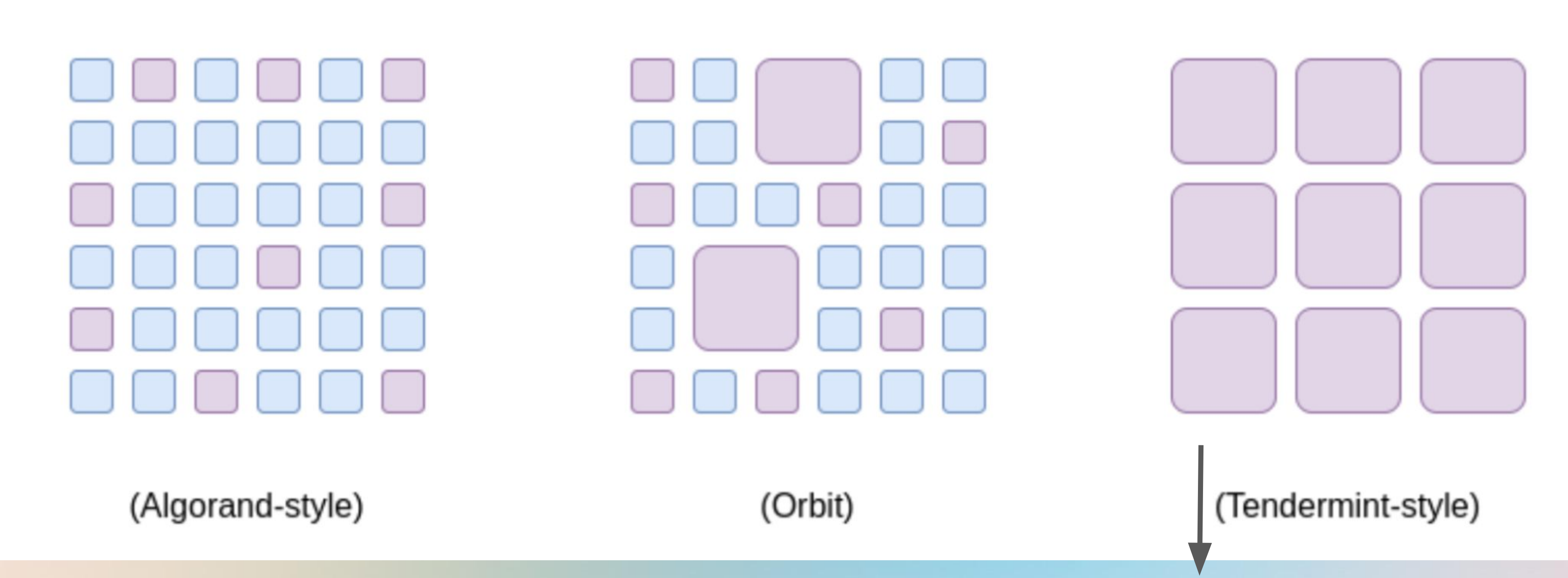
Validator Capping: Orbit



(Algorand-style)

(Orbit)

(Tendermint-style)



(Algorand-style)

(Orbit)

(Tendermint-style)

In Ethereum: Rainbow staking

Orbit committee

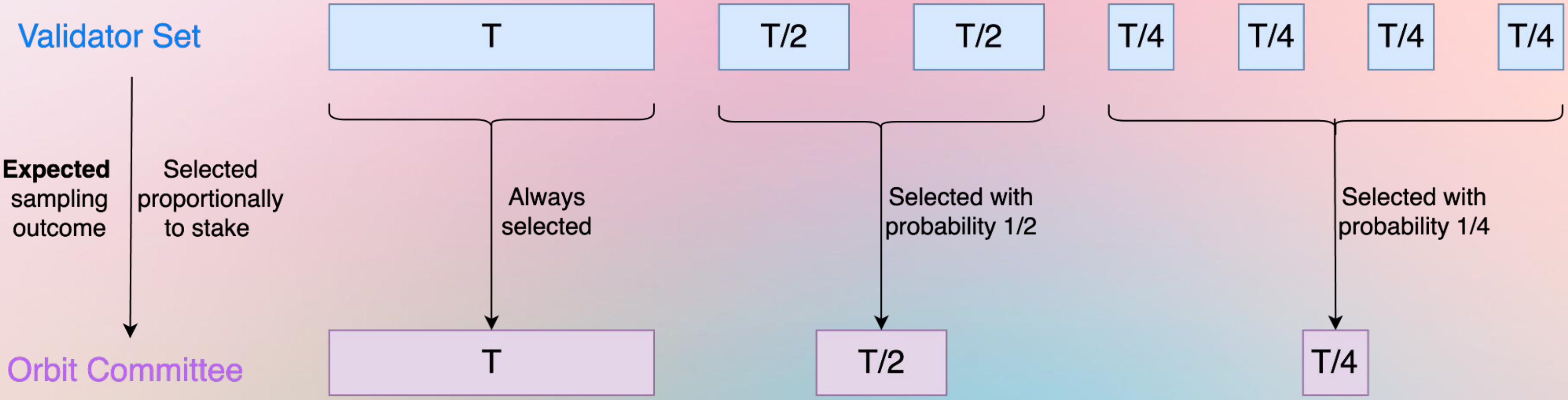
Let T = MAXIMUM_EFFECTIVE_BALANCE (2048 ETH)

A staker with S stake gets:

1. Selected in the **Orbit committee** with probability p(S) = S/T
2. A constant **(not dependent on balance)** reward R **when in the set**

Expected reward R*p(s) = R * S/T, proportional to stake (as it should)

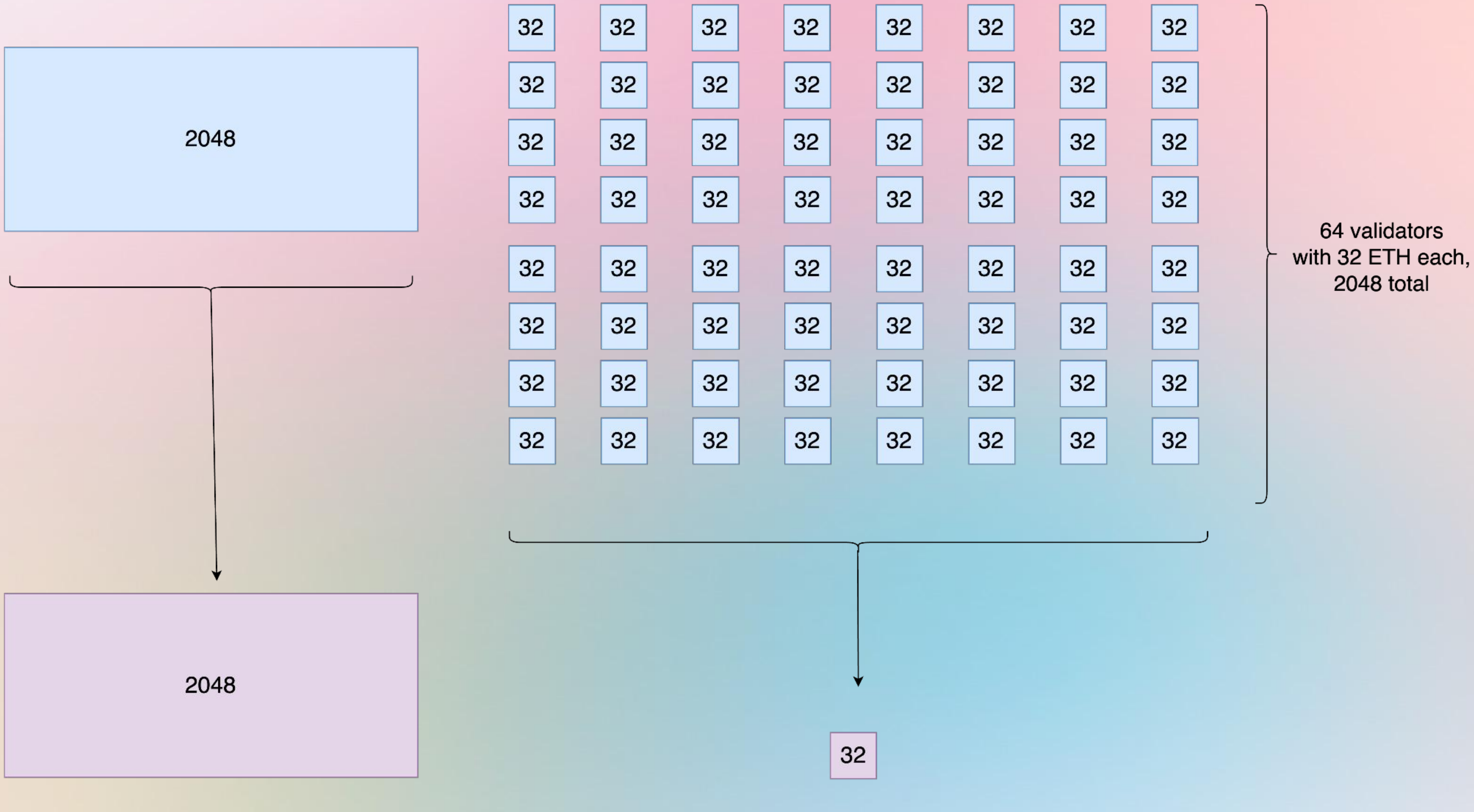
Orbit sampling


Validator Set
T
T/2
T/2
T/4
T/4
T/4
T/4
Expected sampling outcome
Selected proportionally to stake
Always selected
Selected with probability 1/2
Selected with probability 1/4
Orbit Committee
T
T/2
T/4

No matter how you split the stake, the expected size of the Orbit Committee is the same. What changes is only the amount of stake

=> Validator set capping

Orbit sampling



64 validators
with 32 ETH each,
2048 total

What does it get us

1. **Validator set capping:**
   D = total deposit size ~ 35M (now)
   E[|Orbit Committee|] = D/T ~= 35M/2048 = 17k

2. **High economic finality**: if large stakers consolidate, the Orbit committee has a lot of stake, even with few validators
   => Can get high economic finality quickly

What does it get us

1. **Validator set capping:**
   D = total deposit size ~ 35M (now)
   E[|Orbit Committee|] = D/T ~= 35M/2048 = 17k

2. **High economic finality**: if large stakers consolidate, the Orbit committee has a lot of stake, even with few validators
   => Can get high economic finality quickly

3. **Lower mineb:** not very sensitive to it, would make it *at least more plausible* to reduce it

What does home staking look like in this world?

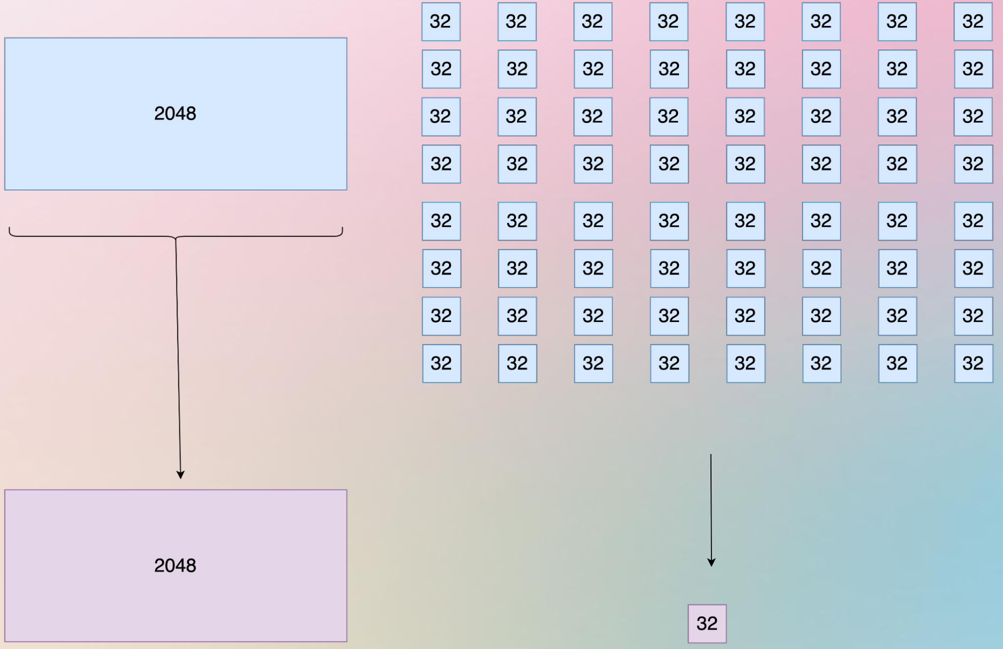
What stays the same

1. The frequency of proposing blocks and/or ILs
2. Influence over LMD-GHOST

What changes

1. Attest less often *than consolidated validators* (once every 2 epochs with 32 ETH, ½ as much as today)
2. **Less influence over finality**… *but home stakers have very little anyway (5-10% of stake?)*

What does home staking look like in this world?



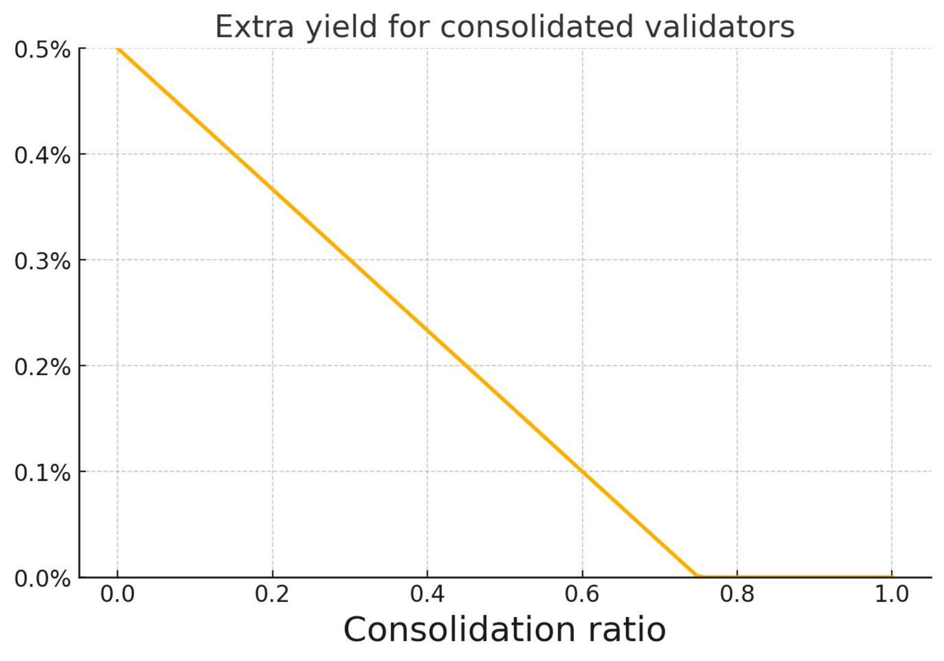
What changes

1. Attest less often *than consolidated validators* (once every 2 epochs with 32 ETH, ½ as much as today)

2. **Less influence over finality**… *but home stakers have very little anyway (5-10% of stake?)*

Consolidation incentives

1. We want to **ensure** that enough consolidation will happen, though participating more often involves higher tail risks.
2. We do not want consolidated validators to be more profitable



What's left?

3SF:

1. Speccing
2. Prototyping

Orbit:

1. The community should decide if these are the right tradeoffs
2. Choose the behavior in the failure case (low consolidation)
3. Introduce Orbit sampling in the current protocol? (pre-3SF)
4. Once there's enough consolidation, move to 3SF

Thank you!