Introduction

SUAVE's design is still an area of open research with questions around economic security, incentive compatibility, social alignment, technical risk, and feasibility. All are important if SUAVE is to be successful. Feedback from the EF, rollups, EigenLayer, and others would be valuable. So far we know:

- "No plans at the moment [for a SUAVE token], ETH is the SUAVE Chain token."

- "We don't currently have plans to use Eigenlayer restaking. For now, we will use ETH bridged to SUAVE Chain as the native token (for paying network fees, executor rewards, etc)."

- "We are currently iterating on the economics and validator set for SUAVE. At a high level we envision that validators would be incentivized by network fees collected from transactions."

The rest is mostly TBD. This post will introduce some of the potential economic security models. I'll argue that SUAVE should be a rollup or consider re-staking.

SUAVE Validators' Responsibilities

For background, SUAVE executors output (full or partial) blocks that other domains using SUAVE may accept. For example, Ethereum validators could profit-switch between a SUAVE block, a block made by traditional centralized builders, or a locally built block.

[

1600×900 168 KB

](https://collective.flashbots.net/uploads/default/original/1X/bc0b38ad4ca8b09900c2908abf94a7bcb00a7987.png)

The following is based off of this description of SUAVE.

Users can deposit funds on SUAVE and commit to unlock them if their preferences are met. They write smart contracts (called "bonds") on SUAVE Chain that validate whether the preference was fulfilled and conditionally transfer a payment if so.

The incentives to participate are:

- Executors

- Incentivized by bonds

- Validators

- Incentivized by network transaction fees

SUAVE can be viewed as having two layers:

- Messaging layer (i.e., mempool)

- Transmits preferences to be executed

- Settlement layer (i.e., SUAVE Chain)

- Processes bonds

The chain is primarily intended to check the results of execution and settle payments after the fact. It processes transactions to:

1. Bridge funds

2. Initialize bond contracts

3. Submit oracle updates about the state of another domain

4. Claim the payment from a bond contract after a preference is fulfilled

5. Other - SUAVE is a permissionless EVM chain, so anything could be deployed on it. Native activity outside of its "intended" use is unclear.

SUAVE block times are only relevant if you have to do one of the actions above in the process of executing a preference. Executors aren't generally expected to need to take these actions while constructing a block, so SUAVE block times

wouldn't be a bottleneck in producing blocks for other domains. (I.e., SUAVE validators aren't signing off on what block is the one they want to send to Ethereum, or any other chain using it).

Native Activity on SUAVE

Back to that "other" stuff. <u>"The chain is being built specifically for sequencing/block building/MEV and [Flashbots has] 0 intention of rivaling ETH/other smart contract chains. [Flashbots] will put 0 resources to that."</u> However, <u>"SUAVE Chain is permissionless and anyone can deploy whatever contracts and make whatever transaction."</u> It's anyone's guess what actually ends up going on there in addition to the "intended" use cases.

Let's be real, degens gonna degen. SUAVE will have a bunch of the smartest searchers/builders/DeFi degens/etc. working around it. I'd be shocked if none of them natively deploy on SUAVE some creative leveraged trading uncollateralized NFT yield farming ponzis, because why not.

Interestingly, this native MEV could increase SUAVE validators' desire for some kind of solution to build their blocks for them too. This would ensure that SUAVE validators have equitable access to MEV, avoiding centralization. They could actually have SUAVE executors building blocks for SUAVE Chain too, in much the same way that these executors would create blocks for other domains like Ethereum.

And that's all fine. "Un-intended" native use just has to be acknowledged as a possibility and properly addressed. Additionally, there are always the "unknown unknowns." Does it make sense to have some other important activities we haven't even thought of to be done natively on this coordination chain? Seems very possible to me. All the more reason it needs to have a resilient security model.

SUAVE L1 Without a Subsidy

The simplest economic model here in isolation is insufficient - SUAVE as a standalone L1 with bridged ETH securing the chain. You could also of course secure SUAVE Chain with a hypothetical "secondary" token if you wanted to remove bridged asset risk in consensus (and could still just use ETH for gas, etc.). But this is just rehashing every L1 EVM-fork we've seen in the past, so I won't bother going any further on why that's problematic.

The economics would look like this (I assume SUAVE Chain would use an EIP-1559-like fee mechanism here):

[

1600×849 158 KB

](https://collective.flashbots.net/uploads/default/original/1X/ff2104df00734668f70ef06b6ee8569670933c1f.png)

To win blocks, SUAVE will be competing against centralized builders on other domains. These builder margins are already thin - they bid almost all of the value back to Ethereum validators today. If additional SUAVE fees meaningfully cut into margins, it will likely not be competitive in winning blocks. Since these fees are the stated incentive for SUAVE validators, they would receive negligible revenue (at least early on). I also note that SUAVE Chain validators could receive MEV from activity on SUAVE Chain itself as discussed earlier.

However, the opportunity cost of ETH staked on SUAVE = rewards from ETH staked on Ethereum L1. Assuming staked ETH is to reach equilibrium at equivalent yields on SUAVE and Ethereum L1:

[

1600×161 55.1 KB

](https://collective.flashbots.net/uploads/default/original/1X/926fe61baaf6255ff3a854f9e78cf15705c8f8b6.png)

It's clear that total revenue to Ethereum stakers > total revenue to SUAVE stakers by a huge margin.

[

912×723 190 KB

](https://collective.flashbots.net/uploads/default/original/1X/49e7e325eeef3e1186b3f484ea196b732d5ac710.jpeg)

Additionally, SUAVE validators should demand a higher yield than Ethereum L1 staking. It's riskier (new chain, bridge risk, etc) and requires more resources to operate. In the absence of any additional incentive mechanism, an incredibly small amount of ETH should rationally be bridged to SUAVE for staking.

There's a reasonable argument that long-run sustainable value capture is possible. However, it will certainly be negligible for at least a while. It will have limited functionality/adoption to start, and it will need to be cost-competitive.

Looking at the numbers, there's <u>~16mm ETH staked on Ethereum</u> <u>earning a yield of ~7.5%</u>. You can play around with the

assumptions below:

[

1600×418 122 KB

](https://collective.flashbots.net/uploads/default/original/1X/f65c2611af8cd9f913a63d2ff4060c7fecc53d74.png)

SUAVE L1 - Parasitic to Ethereum Security

If this SUAVE L1 is eventually highly profitable (and attracts a large volume of bridged ETH), it is then somewhat parasitic to Ethereum L1's economic security. Validators are forced to choose between validating either Ethereum or SUAVE as contemplated here. If SUAVE manages to offer higher and higher rewards, then rational actors will progressively unstake from Ethereum L1, bridge to SUAVE, and stake there.

This is analogous to the classic problem we've seen in DeFi - when lending rates are above the staking rate, participants are incentivized to unstake and use their collateral in DeFi. This has largely been addressed by liquid-staking derivatives (LSDs) or superfluid staking. These enable base layers to keep a reasonable inflation rate while maintaining sufficient collateral staked.

[

|317x461.0617760617761

1098×1600 541 KB

](https://collective.flashbots.net/uploads/default/original/1X/c2ebaa15f772daadcf58df44477a61acf438c647.jpeg)

Alternative Economic Models

1. Rollup

2. Make SUAVE a rollup

3. EigenLayer

4. Use EigenLayer, attracting ETH re-stakers to secure SUAVE chain

5. SuaveLayer

6. Fork EigenLayer, implement a new Ethereum re-staking protocol just for SUAVE, attracting ETH re-stakers to secure SUAVE chain

7. L1 + Bridged LSDs

8. Allow LSDs to be bridged and staked (e.g., you could stake stETH on SUAVE)

9. L1 + Decentralized Subsidy

10. Inflationary SUAVE token issuance

11. L1 + Centralized Subsidy

12. Flashbots directly pays you to stake

Each would alleviate the economic opportunity cost issue to varying extents. Note that these options are not mutually exclusive. For example, some form of "subsidy" is potentially applicable in all cases. All scenarios contemplated include some meaningful smart contract and/or proof implementation risks:

[

1600×602 128 KB

](https://collective.flashbots.net/uploads/default/original/1X/ad23e63b6cba01bfe762dea8c2896a28f6113970.png)

1. Rollup

This is the most preferable option in my view. You get full Ethereum security. You can still capture value for your rollup as desired (rollups will pay a very small margin to Ethereum). You can actually safely capture more

value, because it's now reasonable to use the "secondary" token for sequencer leader selection (or local consensus if

desired). It wins out on all fronts I can think of, except arguably complexity (which also = risk). Something like the [OP Stack](#) should sufficiently address this concern for me. It would greatly ease initial deployment and allow upgrade flexibility overtime.

Additionally, safeguards can be implemented as we see with most "rollups" today. There are some tradeoffs (e.g., centralized sequencers, smart contract upgrade keys, etc.), but this is acceptable short-term to mitigate risk. The smart contract bridge risk is also greatly reduced compared to an L1 option - the bridged asset is no longer required for consensus.

Staked ETH (or a "secondary" token) could be used though for decentralized rollup sequencer leader election. It could also be used for a local consensus giving stronger pre-confirmations if desired (but it's unnecessary). For example, [StarkNet plans to do something like this](#). This SUAVE rollup would presumably be an optimistic rollup, with the ability to transition to ZK over time as it makes sense (or maybe a [2FA SGX rollup](#) while you're at it).

It's also cool that a rollup built on top of Ethereum could be building blocks for Ethereum, and those blocks would be securing the rollup built on top of it that's building those blocks.

[

1280×666 242 KB

](https://collective.flashbots.net/uploads/default/original/1X/2e13e57de0832f26d7b8ab5996144d394794b3b1.jpeg)

For a deeper analysis of rollup considerations (particularly economics), I recommend:

- [Understanding Rollup Economics From First Principles](#) - [Barnabé Monnot](#)

- [The Complete Guide to Rollups](#) - [yes I'm shilling myself](#)

2. EigenLayer

Also appealing, and reasonable to implement in the relatively short-term. Ethereum staking revenue is no longer an opportunity cost for SUAVE re-stakers. They can just stack the yield from securing SUAVE Chain on top of their initial revenue. This makes it far easier to bootstrap security from a subset of Ethereum's validators.

[

1600×849 161 KB

](https://collective.flashbots.net/uploads/default/original/1X/f5f9177ff770fd3038107ca76a38ed0eb3ab391b.png)

Re-staking smart contract risk is preferable over the bridged ETH risk in my opinion (in the case where bridged ETH is actually used to secure SUAVE, as would be the case if SUAVE were to be its own L1). There are concerns around accidental slashing using re-staking. However, this could be mitigated with safeguards such as a trusted committee with the right to veto. This option is also potentially easier to implement than building a new rollup, and alleviates many of its associated risks (proof system, bridge risk, etc.).

Applications leveraging EigenLayer (e.g., SUAVE) could flexibly impose limits on the validators opting in. For example, "you're only allowed to re-stake on SUAVE if you aren't re-staking for other applications." This reduces the "leverage" placed on economic security if that is desired.

The reduced leverage also comes at some cost - it's more difficult to have higher stake securing the chain. It's easier on the margin to attract re-stakers if they're allowed to stack yield by securing other EigenLayer applications. It's more capital efficient. So allowing for higher leverage increases the barrier to collude, but it also increases the incentive to do so. It's a tradeoff.

There's also an underlying centralization risk to Etherum itself. One concern regarding re-staking is that it can incentivize validators to be more sophisticated. For example, let's say:

- Average Joe validator

- can get 7.5% yield (just vanilla Ethereum staking)

- Sophisticated re-staker

- can get 10% yield (assume SUAVE gets you an extra 2.5% for easy math)

Sophisticated stakers will compound earnings, and others are also incentivized to give their money to the sophisticated validator to stake for them. It's quite similar to why MEV-Boost seeks to give all validators equitable access to MEV. You can think of any potential income to be earned via re-staking similarly to MEV in this context.

For the health of Ethereum's validator set, re-staking is best suited to horizontally scalable applications which keep individual re-staker node requirements very low (e.g., [EigenDA](#)). Throwing a potentially high-resource requirement L1 with strong

incentives (as SUAVE could be) on top of EigenLayer is not the best fit.

3. SuaveLayer

Similarly, SUAVE could fork EigenLayer and create their own re-staking contract. This could enable the same deleveraging if desired (i.e., don't let SUAVE re-stakers secure anything else). This also allows for better control of their stack and associated safeguards. For example, SUAVE could choose the slashing veto committee, parameters, etc. However, this also introduces similar centralization concerns on the Ethereum validator set.

Additional benefit - SuaveLayer sounds cool.

4. L1 + Bridged LSDs

This removes the opportunity cost to secure SUAVE (net of LSD fees), allowing SUAVE validators to continue capturing Ethereum staking revenue. However, "kingmaking" certain LSDs and further entrenching LSD centralization is problematic (sorry @Hasu). You now have severe bridge risk and LSD contract risk - these bridged assets secure the chain. Bad trip.

[

1283×805 374 KB

](https://collective.flashbots.net/uploads/default/original/1X/7d2e79c5fc2ce3f4999035b0ecbfb74986e46c64.jpeg)

5. L1 + Decentralized Subsidy

This would presumably be some form of secondary inflationary token that could be used to incentivize SUAVE validators. Staked ETH would still secure the chain and capture the majority of value. This could bootstrap economic security, borrowing from future expected cash flows.

[

1600×849 170 KB

](https://collective.flashbots.net/uploads/default/original/1X/69008a00d8cf8f0184820d36217cdd92c253ee36.png)

This still retains the issue of being somewhat parasitic to Ethereum L1's own economic stake. Bridge risk is again severe, as bridged ETH secures the chain.

If SUAVE were to decide any "secondary" future asset is desirable, it's better suited to a rollup or a re-staking construct. Neither limit this ability to further decentralize, capture value, etc. (e.g., you could have dual-token staking with re-staking). A rollup/re-staking construct would just remove the aforementioned concerns around economic security, being parasitic, etc.

A SUAVE Chain makes a lot of sense. But while you're at it, you might as well post your data and some proofs to Ethereum. What are those called again…? I'm quite surprised an L1 secured by bridged ETH would get any meaningful consideration as an option.

6. L1 + Centralized Subsidy

No. Severe bridge risk. Still parasitic to Ethereum L1's own economic stake. Unnecessary and unsustainable. Flashbots employees get sad.

TLDR

SUAVE should strongly consider a rollup or re-staking for its eventual chain. Both alleviate the economic incentive concerns and retain flexibility for further decentralization mechanisms. My preference would be a rollup.

[

1600×1600 317 KB

](https://collective.flashbots.net/uploads/default/original/1X/99c8d2ae88c6c17521c14d616d5baccddd1d18d5.jpeg)

Disclaimer: I have no personal or professional financial stake in Flashbots (current or planned), other than hoping they make Ethereum work so that my ETH goes up. I have a small personal stake in EigenLayer. Would also appreciate it if they make ETH go up.