slug: the-future-of-mev-is-suave title: The Future of MEV is SUAVE authors: [flashbots] tags: [suave, sgx, orderflow auction, roadmap] image: /img/posts/suave/logo-landscape.jpg hide_table_of_contents: false description: After successfully isolating the centralizing effects of MEV to the block builder role, we turn ourselves toward a new challenge - to decentralize block building itself. forum_link: https://collective.flashbots.net/t/the-future-of-mev-is-suave/762

TLDR:

- After successfully isolating the centralizing effects of MEV to the block builder role, we turn ourselves toward a new challenge: *to decentralize block building itself* Exclusive orderflow and cross-domain MEV present emerging centralization threats to all cryptocurrencies, so **we must make sure to keep MEV decentralized, or the decentralization of crypto will be lost.**
- To hold ourselves to our decentralization commitments, we are building **SUAVE - the Single Unifying Auction for Value Expression**.
- SUAVE **unbundles the mempool and block builder role** from existing blockchains and offers a highly specialized and decentralized **plug-and-play alternative**. Sharing the same sequencing layer allows crypto to stay decentralized, block builders to capture cross-domain MEV, validators to maximize their revenue, and users to transact with the best execution, while reducing the economic centralization pressure on each domain.
- We are building SUAVE in the open and invite all interested parties — users, wallets, searchers, builders, researchers, and blockchain developers — to work with us.

I. Our Journey So Far

Two years ago, we published Flashbots: Frontrunning the MEV crisis as a call-to-action for the entire community as we embarked on our collective journey to mitigate the negative externalities of MEV on public blockchains, starting with Ethereum. What we proposed was radical—and radically different from traditional finance standards: a permissionless, transparent, and fair ecosystem for MEV extraction that would protect and reinforce the ideals of Ethereum.

When we began, the MEV market was much different than today. Of the MEV theoretically available on Ethereum, very little was realized. MEV was primarily extracted by independent network participants called *MEV searchers,* who are (as the name implies) searching for profitable MEV opportunities with the help of complex algorithms, and automatically submitting them to the network for inclusion. These searchers competed in priority gas auctions (PGAs) by paying high transaction fees and optimizing network latency on Ethereum, causing network congestion while driving up gas prices for users.

These *negative externalities* from MEV extraction increasingly hurt users, yet the market structure was suboptimal for miners and searchers as well. Because miners controlled ordering, they were in the best position to extract that MEV themselves. Meanwhile, the searchers were handicapped by the execution risks of their bids in the PGA games, the limitation of expressivity in Ethereum's native transaction types, and fears of miners frontrunning their own strategies.

As a result, miners and searchers would have been rational to *integrate with each other*: miners could increase their share of the MEV pie by making bespoke deals with searchers and outsourcing the finding of MEV opportunities to them, and searchers could gain greater control over the transaction ordering by having relations with miners they trust. The question that kept us awake at night was not *whether* this integration would occur but *how* — and what it would mean for Ethereum.

In particular, we were concerned that MEV extraction would disappear into permissioned dark pools and exclusive off-chain deals between large trading firms and miners. Over time, such an integrated block producer could earn outsized MEV profit over other block producers and reinvest into better MEV search and more hashrate. Eventually, they would grow to dominate block production — compromising the security model of Ethereum and other smart contract platforms. Such a cycle would create massive centralization pressure, concentrating power to the least scrupulous actors while degrading network execution and user guarantees.

In response to this existential MEV crisis, a handful of concerned researchers and whitehats came together as a collective. We formed a research and development organization - Flashbots, a response to Flashboys 2.0, the research paper that defined MEV. We believed that the next natural step would be to tackle MEV head-on by building a more decentralized financial system to correct the failures of traditional, centralized execution venues. In its name, Flashbots embodies our values — replacing the "good old boys" of Wall St. and Flash Boys with interfaces for cutting-edge bots that keep user execution **permissionless** and **decentralized**.

We had three goals in mind:

- **Illuminate the Dark Forest.** Our first priority was to reveal to a broader audience what was happening in this opaque MEV ecosystem, quantify its impact, and break down information asymmetry between participants.
- **Democratize Extraction**. To prevent MEV from centralizing Ethereum's block production layer via exclusive integration and scale economies, we wanted miner-searcher integration to happen on an *open platform* that maximizes

competition between searchers and is freely available to all miners.
- **Distribute Benefits.** Return the MEV to those who create it — users of Ethereum.

Two years later, we want to evaluate our progress against these goals.

- We have published data and research on MEV to bring more transparency and awareness to the space. We created a community around MEV via events like our Roasts, MEV.day, and MEV-SBC.
- We released **MEV-geth and MEV-relay**, a private transaction pool and sealed bidblockspace auction that allowed a *marketplace for MEV opportunities* to arise. *First*, searchers would send *bundles* to our relay. The bundle was a new transaction type with favorable properties for MEV extraction, most of all the ability to express a preference on the placement of your transaction in relation to another. *Next*, the relay forwarded valid bundles to miners, who ran our custom Ethereum client, MEV-geth. This client would include the most profitable bundle at the top of the block, giving searchers better expressivity and miners a bigger profit share. *Later*, **Flashbots Protect** extended the benefits of bundles (pre-trade privacy + no reverts) to regular users.
- MEV-geth quickly became successful and reached over 90% adoption among Ethereum miners. Most importantly, it shifted the MEV market structure just like we hoped: bundles allowed searchers to extract more of the theoretical MEV through higher expressivity. The competition between searchers shifted the profit split dramatically towards miners.

Exclusive integration and scale economies had been curtailed, for the time being. However, despite its success, the auction we built still had significant limitations:

- **Permissioned miner participation:** While searchers can submit bundles without permission, miners can see all bundles in clear text. As a result, we could allow only mining pools with credible operations to participate.
- **Lack of client diversity:** As a fork of geth, it only worked with a single Ethereum client.
- **Centralized infrastructure:** Our auction was still running on centralized infrastructure, posing a risk to Ethereum over the long term.

As the Merge finally came around, we predicted that MEV would become an even biggercentralizing force in Proof-of-Stake. With the extra responsibility on our shoulders, we designed our next iteration, **MEV-Boost,** to respond to some of these issues.

- The addition of a commit-reveal scheme relaxed the required trust in block producers, thereby allowing every staker to participate on equal footing — from single-validator enthusiasts to the largest staking pools.
- To address the lack of client diversity, MEV-boost was designed as a sidecar for the beacon node - a separate piece of open-source software that works with any Ethereum client through the Builder API.
- Opening up this Builder API had a pleasant side effect — instead of Flashbots being the sole channel to block producers, anyone could become a block builder now. A competitive builder market emerged, letting validators automatically choose the highest bid.

Like MEV-Geth, MEV-Boost has quickly **gained almost 90% network adoption**.

Top diagram: Block building today in the lens of transaction supply chain, excluding tx origins (mempool, private orderflow, etc.). Bottom diagram: zoomed in on the inspired by diagrams from Barnabe Monnot and Hasu.

II. The Challenges Ahead

While MEV-Geth and MEV-Boost successfully isolated centralizing economies of scale to the block builder role and kept block building open to all validators and searchers thus far, **builder centralization** becomes the Damocles' Sword that poses significant challenges ahead.

Builder centralization risks **erosion of Ethereum's network neutrality and resilience, in particular censorship resistance of L1** - ensuring all valid and fee-paying transactions reliably get included on chain.

Over the last 30 days, only five block builders have built80% of all Ethereum blocks. These five entities can impose many arbitrary rules on how blocks are constructed, including choosing to decline to process specific transactions. Transactions are the only way users can interact with any applications on-chain, so block building centralization risks a few actors being able to discriminate against users and/or applications.

The barriers to entry for becoming a builder must be as low as possible, but this is just a necessary, not a sufficient condition. Simply speaking, **the existence of scale economies in the builder market**suggests that a diversity of builders is not guaranteed and a small number of builders may emerge dominant.

Aside from eroding neutrality and resilience and creating a systemic chokepoint for Ethereum, such builder centralization would open the door to significant rent extraction from users, and risk centralizing the validator set.

The builder market is prone to centralization from several vectors:

1. **Exclusive orderflow:** If a particular builder can use inputs for their blocks other builders do not have, this can create a

dangerous flywheel and allow them to dominate block production. The incentive for users to send their transactions to one builder over another, today, is two-fold: *first*, the builder can offer users pre-confirmation privacy or other new features. This has been a big driver for users to migrate out of the public mempool and toward private RPC endpoints. *Second*, the builder can *pay* users for their orderflow, for example from the MEV that their transaction creates.

2. **Cross-domain MEV:** Access to cross-domain MEV benefits builders who make blocks across multiple chains over builders that are only active on one chain, leading to entrenchment from cross-domain MEV *and* validator set centralization.

III. The Future of MEV

We are now looking at two possible paths: either we find a way to shift MEV structure a *third time*, and do so in a way that sustainably eliminates the centralizing forces in block building. In this case, the promise of crypto may be realized. Or we concede block building to a small number of centralized entities, and the decentralization of crypto will be lost.

We must align on unifying infrastructure that allows honest MEV actors to profit more than dishonest ones. We must align to preserve shared ownership and competition with a global ecosystem of permissionless actors.

There is no shortage of companies or actors who are still more than happy to centralize cryptocurrency for their own gain. There is no shortage of those willing to embrace centralization as long as it is centralization to their own wallets. There is no shortage of those who would **prefer** that cryptocurrency looks more like the traditional financial systems they currently dominate.

We must make sure the decentralized, permissionless systems that we have put our hearts and souls into building survive the incentives of these actors. We must make sure block building as a process ends up meaningfully decentralized in power, because crypto must end up decentralized, and because humanity needs decentralization in its financial systems, now more than ever.

Over the past year, we thought hard about how that market structure would have to look like, and arrived at the following principles:

First, to neutralize the pressure from exclusive orderflow, users should be empowered with pre-confirmation privacy and entitled to any MEV they create. Further, their transactions should be private, yet available to all block builders.

Second, to neutralize the pressure from cross-domain MEV, block builders across chains have to integrate with each other. But, similar to how the original Flashbots Auction integrated searchers with miners, they must do it in an open and permissionless way.

And *finally*, the first two components — a transaction system that empowers users, and a block building system that empowers builders — must themselves be decentralized or risk becoming corrupted in time.

After a year of deep research and product collaboration, both in Flashbots and with the powerful MEV community, we have found the answer: **SUAVE — the Single Unified Auction for Value Expression.** SUAVE is our attempt to empower users and maximally decentralize public blockchains.

IV. SUAVE in the blockchain stack

From a high level, SUAVE is an independent network that can act as a **plug-and-play mempool and decentralized block builder** for any blockchain. Although SUAVE is a new blockchain, it is not a general-purpose smart contract platform that rivals Ethereum or any other participating chain. Instead, SUAVE **unbundles the mempool and block builder role** from existing chains and offers a highly specialized **plug-and-play alternative**.

Importantly, SUAVE goes beyond sequencing for a single blockchain. We designed SUAVE to be **the mempool and block builder for all blockchains.**

There are many reasons why we think the market will evolve toward many chains sharing a single decentralized sequencing layer:

- Block builders who only operate on a single domain will find themselves increasingly at a disadvantage due to **cross-domain MEV**.
- There are **efficiency gains** for users from aggregating and clearing their preferences inside the same auction.
- We can leverage that credible neutrality to get many parties to share their views, strategies, and opinions in a single place, giving SUAVE an **information advantage** on centralized builders.
- Enabling computation on sensitive data (user orderflow) in a permissionless setting is a hard problem. By solving it for many chains, we can **amortize the cost** across the ecosystem and reach a solution faster and cheaper than any individual participant could.
- Because of how fundamental sequencing is to the blockchain stack, only another decentralized system can provide

the necessary **security and credible neutrality**.

Sharing SUAVE as the same sequencing layer with each other unlocks the following benefits (in order of the stack):

✓ For blockchains: maximally decentralized sequencing, maximal neutral network resilience.

✓ For validators: maximum revenue on their blockspace.

✓ For builders/searchers: open access to user and searcher transactions, express complex preferences, cross-chain coordination.

✓ For users: transact privately and with the best execution and the minimum possible fees.

We are convinced that building a decentralized sequencing layer is the only way to give domains control over their own validation guarantees and to ensure smaller domains stay decentralized in the face of centralizing MEV from both centralized venues and other blockchains. We predict that domains that seek to compete on MEV sequencing rather than collaborating will see severe network externalities and backdoor centralization induced by MEV search. So, we suggest that all domains **must work together to avoid the centralizing endgame**

V. Architecture of SUAVE

SUAVE is a single environment where parties can collaborate on the *expression, execution,* and *settlement* of preferences in a decentralized way. It is composed of three main components:

1. **Universal Preference Environment:** A chain and mempool specialized for preference expression and settlement to surface and aggregate the preferences from users and searchers from all participating chains in a single place.
2. **Optimal Execution Market:** A network of special parties called executors who listen to the SUAVE mempool and compete to provide the best execution for user preferences.
3. **Decentralized Block Building:** A decentralized network for and of block builders to access the encrypted preferences from users and merge them into partial or full blocks.

At the core of SUAVE is the concept of *preferences.* A preference is a message that a user signs to express a particular goal and that unlocks a payment if the user's conditions have been met. These preferences can range from simple transfers or swaps in a single domain to arbitrarily complex sequences of events across multiple blockchains. You can think of preferences as the native transaction type on SUAVE. They can either contain a payload to be executed on a specific domain—such as Ethereum—or make a more abstract statement of what the user wants to achieve and leave the optimal routing to the executors.

Preference Environment

The Preference Environment builds on the existing properties of bundles (pre-confirmation privacy and no reverts) and improves on existing mempools by allowing an even richer range of expression. We expect a vibrant ecosystem to arise around preference expression and execution that serves users' needs. For example, executors can specialize to "pre-process" transactions in ways that make them more valuable, such as batching similar transactions together or paying gas fees on their behalf.

The universality of the preference environment unlocks a network effect for all participants: *First*, the more preferences become aggregated in one place, the more the final blocks can optimize for the welfare of all users, e.g. via the aforementioned batch clearing. *Second*, block builders (and hence validators) also benefit because the unified auction makes them aware of cross-domain preferences, allowing them to coordinate with other builders on other domains in a credible way.

Execution Market

Once a user has submitted their preference to SUAVE, it is passed to the Execution Market. Executors compete in an auction to provide users with the best execution possible and address many users' preferences across many domains. In cases where a user's transaction creates MEV, executors would capture that as well and compete on paying as much as possible of it back to the user. The Execution Market recognizes the economic value of orderflow, aspiring to be a decentralized place where users, wallets, and other orderflow originators can earn the most for their transactions.

Decentralized Block Building

Finally, a decentralized block building **network** takes the collected preferences, many of which have their execution paths optimized by now, and turns them into blocks across all participating domains. The decentralized block-building market maximizes MEV for builders and validators while allowing the builder itself to become decentralized.

Our goal is to move past the stage of monolithic block builders and toward a world where many searchers/builders with strong geographical distribution collaborate to build the best block together. The most important step for that is to enable the sharing of orderflow/bundles between block builders without leaking their contents.

These three components will be enabled by a specialized **SUAVE Chain**. The chain will be EVM-compatible and provide the scaffolding for all these components to interact with each other and decentralize over time.

VI. Roadmap and First Steps

This is an ambitious vision to build. We will need to be thoughtful in progressively decentralizing SUAVE and improving its trust guarantees, while at the same time making it more expressive over time. Below is a roadmap of our planned milestones (these may be subject to change):

SUAVE Centauri

- **Privacy-aware orderflow auction** to return to users the MEV that their transactions create. In this auction, searchers compete for the right to back run a user, thereby bidding up the value returned to them. Initially, the auction assumes trust in Flashbots but is private for users and searchers.
- **SUAVE Chain devnet** for stress testing and community experimentation.

SUAVE Andromeda

- **SUAVE Chain mainnet** will allow users to express preferences and send them to the Execution Market
- **SGX-based orderflow auction** to remove trust in Flashbots and make the auction for efficient for searchers
- **SGX-based centralized block building** to enable open but private orderflow for centralized builders

☀ SUAVE Helios

- **SGX-based decentralized building network** to allow for permissionless and private collaborative block building across many entities
- **Onboard second domain to Suave** to address MEV on another domain and provide a foundation for cross-domain MEV
- **Cross-domain MEV solutions** that allow for expression and execution of cross-domain MEV preferences

Beyond SUAVE Helios, we intend to look into custom secure enclaves, as well as using cryptography and cryptoeconomics to help further reduce the trust guarantees of users in the system. These improved trust guarantees will lower the barriers to entry for new parties and be a stepping stone towards orderflow that is both private yet open to all builders.

This marketplace needs to be bootstrapped, similar to how the previous marketplaces we've built have needed bootstrapping. We'd like to make it clear: we run centralized infrastructure today with the single goal of bootstrapping SUAVE and setting a healthy baseline for quality and competition. **We do not intend to participate in the marketplace we build beyond bootstrapping it.** We consider this strategy the most aligned with our mission and the health of the entire ecosystem.

For SUAVE to succeed against centralized block builders, it needs to become a neutral home for users, searchers, builders, and validators across many blockchains alike. In the SUAVE future, Flashbots would like to be the neutral marketplace designer—not a participant—and explore incentive-compatible ways to achieve organizational sustainability.

VII. The Millennium Prize Problems of Crypto

This is a time where our individual incentives must be, briefly, for an instance in time, put aside to build something that is greater than ourselves. In the past few months, our industry has seen the devastation of unbridled, centralized greed. We have seen first hand that papered-on faux decentralization is not enough. We have seen the devastation that embracing the same old trust cartels has on those we claim to build for.

Our industry today is tiny. To face the future and the world, we have to do a lot better.

We understand that the obvious incentive in MEV is to compete. However, we would like to instead encourage the community to **collaborate**. Because we deserve to see what meaningful decentralization looks like in the context of MEV. Because we are all here thanks to cryptocurrency's unique decentralized nature, and its global reach. Because these are all important properties that we hold dear, that are worth preserving. Because the endgame of block building becoming centralized is something we must all unite against.

We do not expect you to trust us as we walk down this road. It is our commitment to **meaningfully decentralize.** It is our commitment to not hold on to more than our fair share of power as we build these systems. It is our commitment to be more open, and to make decisions that benefit the commons even when it is at our short-term expense. We cannot dictate what is best for this community, and we do not intend to try.

If we cannot accomplish this mission by walking alongside and accelerating every single ecosystem project, every single perceived competitor in our market, and every single blockchain system, towards decentralization, we have already failed.

MEV is the Millennium Prize Problem of crypto. We are deeply convinced that the value to be unlocked through coopetition in MEV is monumental. **We believe that the sum is greater than its parts** and that we can align the best possible execution with the most decentralized infrastructure. We commit to preserving the decentralization and respecting the preferences of every user and every domain that MEV touches.

We ask you to watch our actions, and to keep us to account. We ask you to walk with us on this road, so we can keep you to account as well.

Stay tuned for the SUAVE technical specs and posts that will provide more color on the different milestones on our roadmap, and how we can get there together. We look forward to iterating on and discussing them with you.

Onwards, to (more) decentralization!

The Flashbots Collective

collective.flashbots.net

writings.flashbots.net

flashbots-github