SUAVE's Potential in DeFi: A focus on decentralized exchanges (DEX) and auction mechanisms

Abstract

This piece contains a deep dive into problems in DeFi, technical properties of SUAVE and how these properties can address some of the problems faced by DEXs and auction protocols.

Decentralized Finance (DeFi) is arguably the most important application vertical within blockchain technology and has the most significant potential to drive mass adoption of this technology. Central to the DeFi ecosystem is the non-custodial decentralized exchange (DEX) trading. However, trading on centralized exchanges (CEX) provides a better user experience due to improved execution, lower cost of trading and more profitable liquidity provisioning. Privacy preserving and credible computation guarantees SUAVE provides by leveraging Trusted Execution Environments (TEEs), coupled with low latency design offer a design space that can improve auctions and DEXs, which may help DeFi and blockchain application adoption in the long run.

This study synthesizes market data, academic research, and insights from comprehensive interviews with diverse DeFi stakeholders, including market makers, venture capitalists, Miner Extractable Value (MEV) supply chain participants, and industry experts. These interviews offer firsthand perspectives on operational dynamics, existing inefficiencies, and the key adoption hurdles in the DEX arena. Additionally, the study conducts an in-depth analysis of the DeFi ecosystem, with an emphasis on Decentralized Exchanges (DEXs) and auction mechanisms, to explore prevalent problems, proposed mitigation strategies, and the role of privacy for an improved user experience. The study also evaluates the potential of SUAVE-based approaches in offering solutions to these challenges and in enhancing existing practices.

The findings indicate that DEXs often provide a suboptimal trading experience compared to CEXs, primarily due to factors like lower liquidity and higher cost of trading. Two principal reasons contribute to this situation:

1. The inherent discrete-time nature of blockchain operations, typically 12 seconds on Ethereum, compared to the continuous price movement on CEXs, which serve as reference points, creates arbitrage opportunities. Delayed price updates on DEXs enable arbitrageurs to exploit passive liquidity providers, a phenomenon termed Loss-Versus-Rebalancing by Milionis et al. [6].

2. The high cost of actively managing liquidity positions on DEXs, in contrast to the cost-free order placement and cancellation on CEXs, leads most LPs to set wider ranges for their positions, thereby spreading liquidity over a larger spectrum and reducing active liquidity near the market price, as observed by Caparros et al. [41].

Moreover, the public nature of blockchain transactions exposes traders to adversarial ordering attacks, diminishing the quality of trade execution and increasing trading costs.

As a result, trading and providing liquidity is less profitable on DEXs. In order to mitigate these problems, there's a trend towards auction based solver and Request For Quote (RFQ) based DEXs, which prioritize active liquidity management. These auctions are currently held off-chain in centralized systems that require trust, due to current limitations of blockchain based auction protocols to meet the demands of efficient trading systems. Furthermore, credibility of digital auctions is a problem that extends far beyond blockchains. The DoJ recently sued Google over auction manipulation and distorting auction competition [41].

SUAVE has the potential to emerge as a promising solution for the DeFi ecosystem given its focus on privacy, fast finality, credible off-chain computation properties and Ethereum compatibility. SUAVE can allow DEXs to be competitive with CEXs by:

- ensuring fair trade execution via credible blockchain based auctions and eliminate reliance on centralized parties in solver and RFQ DEXs that are already gaining traction

- reducing value lost to arbitrageurs through privacy (traders) and fast finality (liquidity providers) and reduce the overall cost of trading

In conclusion, SUAVE's characteristics could substantially contribute to addressing current inefficiencies in DeFi, particularly in decentralized exchanges and auction mechanisms.

Introduction

DeFi and DEXs are the strongest product market verticals in blockchain applications

Since it's inception in 2018, the decentralized finance (DeFi) market has witnessed remarkable growth, reflecting its potential for widespread adoption of blockchain technology. Today DeFi accounts for majority of the value and user activity on Ethereum.

Total value locked (TVL), a metric akin to assets under management, in DeFi

on Ethereum surged from approximately $600 million in January 2020 to approximately $30 billion in January 2024, while reaching a stunning $108 billion in November 2021 [1]. Today Ethereum only accounts for 55% of the TVL in DeFi markets, while other lower fee blockchain and scaling solutions capture the remaining liquidity. The growth of DeFi is not just in terms of market value but also in user engagement.

Users (unique wallets)

interacting with DeFi protocols reached 2.7 million in October 2023, marking a 9x growth over the last three years. Approximately one in every two Ethereum users (unique wallets), interacted with DeFi protocols in October 2023 [2]. Uniswap, which is the most popular DeFi protocol that uses an Constant Function Market Maker (CFMM) based DEX, has alone accounted for 8% of unique Ethereum users in the seven day period starting on January 3, 2024 [3].

DeFi also accounts for majority of demand on Ethereum.

Gas, which is the cost of computations on Ethereum, is a measure of usage. During the seven day period starting on January 2, 2024, Uniswap alone accounted for ~33% of gas fees on Ethereum These statistics show the importance of DeFi and specifically DEXs on demand for Ethereum [5].

While trading in traditional markets is mostly done on central limit order book (CLOB) exchanges, DeFi has evolved around the CFMM model also know as Automated Market Makers (AMMs).

CLOBs use a centralized database to manage the order book and a order matching engine run by the exchange operator. AMMs have become the dominant form of exchange in DeFi, as running an on-chain order book and matching orders are highly inefficient given the computational and storage limitations of blockchains. AMMs enable continuous liquidity and an automated price discovery and execution mechanism which are well suited for blockchains.

However, DEX trading experience still lag significantly behind CEX trading experience except custody risks

Popularized by Uniswap, AMMs have become a compelling and a trust-less alternative to CEXs. DEX monthly trading volume grew significantly over the last 3 years, from $15 billion in November 2020 to $80 billion in November 2023, recording a 75% annual growth. Over the last 12 months, Uniswap consistently accounted for at least 60% of all DEX volume [7]. However despite its staggering growth, DEX volume and DEX trading experience still lags significantly behind that of CEXs. Over the last 12 months, the share of DEX volume in spot trading has ranged between 7-18%, averaging approximately at 13%[8]. While trustless and permissionless, DEXs introduce several inefficiencies for traders (taker) and liquidity providers (makers), which result in a more expensive trading experience and worse execution.

Problems AMMs face

Cost of trading is higher in DEXs

The following cost items create the total cost of trading on DEXs for swappers:

- Gas cost: Each transaction on Ethereum requires a gas payment. Unlike in CEXs, in order to trade on DEXs takers need to incur gas fees
- Protocol / pool (liquidity) fees: On AMMs pools have LP fees which range from 0.01 to 0.3%. Almost half oftrading volume on Uniswap come from 0.05% fee pools [9]. However these pools are known to be unprofitable for liquidity providers.
- Ordering based slippage: There are two types of transaction ordering in DEXs, adversarial and benign, that incur cost for traders:
- AMM transactions are vulnerable to transaction ordering attacks due to the public nature of blockchains. These attacks are also known as sandwich attacks (front-running attacks and back-running attacks) [10]. In December 2023, sandwich attacks impacted approximately 67 thousand traders and cost them approximately $16mn [11].
- Trade collisions occur when two traders want trade in the same block and the ordering of their transactions within block result in a difference between in execution price for each trader. This problem also exists in CEXs, however unlike AMMs that execute orders every block (12 seconds), CEXs execute orders continuously. As a result the probability and cost of order collusion is much lower.
- AMM transactions are vulnerable to transaction ordering attacks due to the public nature of blockchains. These attacks are also known as sandwich attacks (front-running attacks and back-running attacks) [10]. In December 2023, sandwich attacks impacted approximately 67 thousand traders and cost them approximately $16mn [11].
- Trade collisions occur when two traders want trade in the same block and the ordering of their transactions within block result in a difference between in execution price for each trader. This problem also exists in CEXs, however unlike AMMs that execute orders every block (12 seconds), CEXs execute orders continuously. As a result the probability and cost of order collusion is much lower.
- Liquidity based slippage: Liquidity of a pool determines how much a given order moves prices. While it's hard to

compare these figures given hidden orders in centralized exchanges, interviewees constantly underline the limited liquidity in DEXs. AMMs have lower capital efficiency because liquidity is spread over a larger range as it's hard and costly to update price ranges actively.

A recent paper, analyzes the cost of trading on Uniswap for the highest volume pool ETH-USDC (0.05% fee) and a lower volume, higher volatility pool ETH - PEPE (0.3% fee)[12]. This research suggests that average cost of trading for ETH-USD and ETH-PEPE pairs are 22bps and 140bps respectively. Price impact adjusted costs (to make sure we have an apples to apples comparison), which are respectively 17bps and 106bps, are still significantly higher than 10bps trading cost on Binance for retail traders.

[

image

1472×722 86.6 KB

](https://collective.flashbots.net/uploads/default/original/2X/3/32925c91ab135eebe7dd24f45c8e032aceff617c.jpeg)

While gas costs and LP fees are network and pool specific metrics that are easily monitored by users, slippage due to adversarial transaction ordering becomes a hidden cost item for the traders. Adversarial ordering creates risk-free atomic arbitrage opportunities for arbitrageurs and approximately cost Ethereum users $150 million each year[11].

A similar analysis based swaps routed by 0xSwap API [13] between May and November 2021 yields interesting findings as well; swaps are likely to execute at worst price set by the slippage tolerance of users, which means that MEV bots are extracting all possible value from user transactions. More than 5% of all swaps of size larger than $100,000 and approximately 10% of all swaps between $10,000 to $100,000 was executed at the worst price possible. It's possible in the last two years this figure has increased as MEV-bots have become ubiquitous, more sophisticated and better capitalized [14].

Similarly price impact is another consideration for DEX traders. A recurring criticism of DEXs in interviews was the lack of liquidity compared to CEXs. This results in worse execution for traders and is further observed in low liquidity pools. When we observe overall results of Adams's [12] work, we see two interesting findings:

- Most interviews suggest that DEXs have found a product market fit for long tail assets and stable swaps, in spite of data showing that trading long tails assets can be significantly more expensive on DEXs; the total cost of trading ETH-PEPE on Uniswap is 140bps. Note: ETH-PEPE pool doesn't exist on Binance, but we can assume ETH-PEPE trade on Binance can be replicated by doing two transactions, which would cost 20bps vs. 140bps.
- 22bps trading cost in Uniswap ETH-USDC 5bps pool is a lower bound

for trading fees given low LP fees and high pool liquidity. This is approximately twice as expensive as trading on Binance. Furthermore, this pool is known to be not profitable for LP according to research by Millionis [6] and CrocSwap [16]

, as we will cover below. We believe it's important to have a pool structure that's profitable for LPs and cost-competitive for traders to ensure sustainability of decentralized exchanges in the future.

Liquidity Provider or maker problems:

Liquidity providers on AMMs like Uniswap are passive liquidity providers mostly because of the high cost associated with actively updating liquidity positions on Ethereum. As a result, passive LPs face Loss Versus Rebalancing (LVR) problem [6], where they leak value to active traders who capture the arbitrage due to the price discrepancies between CEXs and DEXs. To elaborate, since transactions are processed in discrete form in blocks on Ethereum, the price of an asset in an AMM updates every 12 second. On the other hand, prices move instantaneously on centralized exchanges like Binance, where liquidity is higher and price discovery occurs. This arbitrage comes at the expense of passive liquidity providers in AMMs. Research by Frontier [15] suggests that:

- Approximately $100mn was lost to LVR in 2022
- 90% of LVR arbitrage takes place in high liquidity pairslike ETH-USDC

As shown by Moellami et al. [6], LVR is impacted primarily by the following factors; volatility of the assets in the trading pair, fee level of the trading pool and time between arbitrage opportunities (block times):

- Volatility: LVR in a pool increases quadratically with volatility. This finding is intuitive as higher volatility means higher price divergence and therefore a larger arbitrage opportunity. More specifically, the research shows that LVR for a pool can be calculated by $\sigma^2/8$

, when normalized by the pools market value, where σ

is the daily volatility of the trading pair.

- Fee level: The lower the fee model, the higher the arbitrage potential as a given price movement creates a higher

profit margin for the arbitrageur. This is the reason why Uniswap ETH-USDC pool with 30bps fee can be profitable for LPs while the 5bps fee pool is not.

- Block time: The block times are inversely proportional to LVR opportunity given that a shorter block times translate to less volatility and therefore arbitrage opportunity. The research suggests that reducing block times creates a square root reduction in LVR. In other words, 4x faster block times can reduce the LVR by a factor of 2.

Another attempt at calculating LP profitability, which uses mark-out analysis, prove some of the findings detailed above. Mark-out analysis uses reference prices of assets in a future time to calculate portfolio strategy profitability. The analysis performed by CrocSwap [16] shows that following:

- ETH-USDC 0.05% fee pool is highly unprofitable for LPs, and suggests that LPs of the pool lost more than $40mn over a 12 month period starting on August 2021 using Binance prices for the mark-out analysi
- While ETH-USDC 0.3% fee pool is more profitable, LPs of the pool has lost more than $5mn over the same period. This data points prove the

Moellami et al.[6]'s argument that higher fees reduce LVR value leakage.

- LVR value leakage increases with swap size Small swaps, which are likely to represent uninformed retail flow are profitable for LPs. Whereas large swaps, over $100,000 in notional swap size, are highly unprofitable for LPs. This can suggest large swaps which are driven by informed traders, potentially to capture price discrepencies between Binance and Uniswap extract significant value from LPs.

In addition to LP profitability, LVR poses a risk to Ethereum decentralization

Capturing LVR arbitrage opportunities require significant capital resources and have high barriers of entry. An arbitrageur with a lot of capital will be able to capture more arbitrage opportunity compared to an arbitrageur with less capital in a given block and therefore will bid higher to have their transactions be inserted at the top of a block. We see this phenomenon play out as large trading firms and market makers operate their own block builder operations. Top 2 builders, which control approximately 50% of Ethereum block creation, are associated to market making firms [44,46]. These integrated builders are better capitalized to capture arbitrage opportunities and therefore able to bid more aggressively for block space and squeeze out smaller builders. According to Titan CEO, Kubi Mensah [17], Uniswap - Binance arbitrage accounts for approximately 60% of MEV on Ethereum. Thus, LVR is a problem not only for liquidity providers in DEXs but also a centralizing factor for Ethereum. Therefore it's important that we come up with DEX designs that reduce the impact of LVR.

To recap; LVR is a problem for liquidity providers as they lose money to arbitrageurs and cost of trading is a problem for users. LVR in an Ethereum AMM can only be reduced by increasing pool fees, which make cost of trading even more higher for swappers. This paradoxical situation has prompted the industry to look for design that improve AMMs.

Improved AMM design space

In order to address these inefficiencies and close the gap between the trading experiences between DEXs and CEXs, several new models have been introduced over the past years. Of these models, the ones currently used in production are based on the Solver and RFQ

model and primarily aim to address issues faced by traders, not liquidity providers. In addition to these models there are several AMM designs that have been introduced and are yet to be built in production.

Solver and RFQ models

The main property of these models is that they run off-chain auctions to provide best execution to traders using a combination of on-chain and off-chain resources. Traders submit swap intents into a private order-flow (centralized mempool), which are then matched by solvers (or market makers), using trading intents from other traders, on-chain AMM liquidity and private market maker liquidity sources. As transactions are not directly sent to Ethereum but to a private mempool, multiple trades can be batched, resulting in gas fee savings for traders. These models all involve varying levels of trust in certain entities for auction credibility and high entry barriers for order execution (solver) process.

Solver model

The prominent examples of the solver model are CoWSwap, 1inch Fusion and UniswapX. These models use different off-chain auction mechanisms to match traders with liquidity sources.

CowSwap, which pioneered the solver model, uses a batch auction method, which ensures that all swaps of the same asset pair execute at the same price. As a result, this approach prevents transaction ordering related slippage and cuts the overall cost of trading. CowSwap has a centralized database for orders. While anyone can access the orderbook, only whitelisted Solvers can submit matching orders. Solver management and governance is primarily handled by social consensus.

[

image

1414×786 72.8 KB

](https://collective.flashbots.net/uploads/default/original/2X/c/cb543c7e2a99444ed65a35aee77cda95522a2af6.jpeg)

As a result, solver participation is permissioned and requires approximately $1 million stake [43] that can be slashed by the DAO social consensus in the event of adversarial behavior [18]. Unlike other models, CowSwap makes extensive use of on-chain trading pools and fills approximately 60% of retail volume from on chain pools like Uniswap V3, Balancer and Curve [45].

1inch and UniswapX use a Dutch Auction model. In UniswapX [19], solvers are called fillers and are subject to a permissioned participation process. Solvers bid in an auction to provide improved prices over Uniswap pools. The solver that provides the best price to the user wins the auction and has a time window to fill the order. If the user filler fails to fill the order, they face penalties. Solvers in 1inch Fusion [20] are called resolvers. Resolvers are required to go through a KYC process, and are whitelisted by 1inch based on the amount of 1inch tokens they stake. The resolvers can also receive delegation from 1inch holders. The current stake/delegation requirement for 1inch is approximately $450,000 [44] 1inch tokens locked for 2 years. As these figures show, current solver model is not only highly centralized but also have extremely high barriers of entry.

When we observe retail flow going through 1inch Fusion, and UniswapX, we observe that a single player fill over 50% of the entire demand[45]. The two market making firms associated with the 2 largest block builders, which control more than 60% block building activity on Ethereum in the 30 day period ending on January 23, 2024 [46], account for 60% of all orders filled on UniswapX and 1inch Fusion [45].

As noted by Lu:

The dominance of these two market making teams across every vertical in the order flow processing network support historical observations in TradFi on the propensity of financial systems to centralize over time and just how powerful economies of scale can be. Decentralization in DeFi is far from guaranteed, so we must be intentional about the market structure that our mechanisms create. [44]

RFQ model

0x API [21], Hashflow [22] and DFlow [23] are examples of DEX models that adopt a RFQ based order model. In these models, users trade request is shown to a group of off-chain market makers who provide bids to execute these transactions. The order matching is done centrally by the RFQ DEX provider and quoted to the trader, who can then decide whether to execute the trade in a given time window. While these quoted prices ensure there's no slippage for the users, traders don't have any visibility to the auction bids that determines the RFQ winner.

[

image

1452×804 87.6 KB

](https://collective.flashbots.net/uploads/default/original/2X/b/b3ae2f3e210898e0b781eaefb43f606c49fb1574.jpeg)

While the solver and RFQ model has created an improvement in DEX experience, especially around better execution for traders, key components used in these systems are centralized and permissioned. Furthermore market makers that dominate these models tend to provide liquidity for a limited set of assets. Based on orderflow.art [45], 80% of the liquidity provided by Wintermute is for ETH-stable coin and BTC-stable coin pairs.

To recap, solver and RFQ models create an improvement over the current AMM design for takers but only for a select asset types.

Other improved AMM designs

In addition to Solver based hybrid DEX designs that leverage off-chain execution components in production, there has been several AMM models introduced by the community. These designs aim to improve the AMM experience for liquidity providers or traders by addressing LVR and adversarial transaction ordering methods.

McAMM

This new AMM design aims to capture LVR or CEX-DEX arbitrage and distribute that value back to liquidity providers [24]. Since CEX-DEX arbitrage is executed on the top of the block as the first transaction, this AMM design aims to sell the right to execute the first transaction in a given pool to a leader searcher

and distribute the proceeds to LPs. Given LVR comes at the expense of liquidity providers, this is a method to ensure liquidity providers capture the value lost to arbitrage. Based on this model, leader searcher is not charged any pool fees to ensure that they bring the price of the pool back to the market price and traders can only swap assets after the leader

searcher. However the model requires the bidder to approximate the MEV for the next block while bidding at the auction. This model introduces an application specific ordering logic, which also depends on a rational block builder with economic incentives: if the lead searchers TX is not the first one, all TXs in the block revert [30].

Diamond Protocol

Diamond protocol [25] is another design to capture LVR and re-distribute a portion of LVR to liquidity providers in the protocol. At the beginning of a block, arbitrageurs or block builders commit to a price for the end of the block. The final committed price is the Binance price in order to maximize LVR. By the end of the diamond block, the pool price must match the committed price in the beginning of the block. This is achieved by balancing token amounts between the diamond pool, the vault, which exists for each pool and the hedging contract, where block builders escrow funds [30].

Similar to mcAMM, the Diamond protocol auctions the right to capture top of the block arbitrage and proposes an application specific ordering that requires collaboration of block builders. Both mcAMM and Diamond protocol require competitive builders to ensure application specific ordering in Ethereum block building. The reliance on block builders and requirement of escrow, raise concerns about the long term viability of Diamond Protocol. Diamond protocol is currently built as a Uniswap V4 Hook [26].

Credible DEX design with verifiable ordering

This paper [27] enforces application specific transaction ordering rules to eliminate adversarial transaction ordering attacks . More specifically, during block building each buy order from a liquidity pool (asset pair) must be followed by a sell order. This approach ensures that builders cannot create sandwich attacks, which require at least 2 consecutive transaction in one direction during a front-run. Two orders in the same direction (buy/sell) can follow each other if and only if there are no orders in the opposite direction.

These three alternative AMM designs leverage application specific transaction ordering logic.

Dynamic fee AMMs

Given LVR increases at times of high volatility, volatility based proposals suggest increasing swap fees during times of high volatility. This is similar to market makers increasing the quoted bid and ask spread during times of higher volatility. Alex Nezbolin further suggests [28] that fees are adjusted to discriminate against toxic order flow, which is the main cause of LVR. Based on this method, when the price of an asset increases in block t,

the fee to buy the asset should increase in block t+1

while the fee to sell should decrease (while remaining positive). Another example to encourage non-toxic order flow is the recent fee agreement between Balancer and CowSwap. Balancer has been providing CoWSwap trades, which do not capture top-of-block LVR opportunities and therefore is deemed as non-toxic order-flow, discounted trading fees [29].

How can SUAVE applications (SUAPPs) help?

SUAVE chain has several features that are distinctly well-suited to address some of the inefficiencies with DEXs:

- Programmable privacy: Programmable privacy allows SUAPPs to compute on private data, which eliminates adversarial ordering attacks that cost users approximately $200mn a year [11] . Privacy eliminates information asymmetries that prevents traders from receiving best possible execution [31]. Privacy guarantees of Suave is provided by Kettles that run Trusted Execution Environments (TEEs).
- Credible, low cost computations: SUAPPs that run inside TEEs provide verifiable computation guarantees and are able to execute expensive computations like managing an order-book. Other techniques to achieve credibility involves duplicating computations or computing zero knowledge proofs; both of which increase the cost of computation.
- Low latency: SUAVE chain is aiming to target short block times (with initial targets set to 3 seconds) and instantaneous computations inside the Kettles, which are important to address LVR, a volatility driven value extraction method
- MEVM pre-compiles: Pre-compiles in SUAVE enable Kettles to access external data sources like Ethereum state or HTTP requests.

SUAVE architecture

SUAVE is an EVM based blockchain that leverages TEEs to provide private smart contracts (i.e. “programmable privacy”) and credible execution guarantees. SUAVE is designed as a generic blockchain to decentralize the block building process and address current trust assumptions in the MEV supply chain. SUAVE offers a flexible architecture for SUAPPs, which may choose to prioritize latency or security by varying communication among kettles.

[

image

1412×1088 100 KB

](https://collective.flashbots.net/uploads/default/original/2X/a/ac71083154f7eed26759f2fae285509e9111d755.jpeg)

Data propagation

In SUAVE, users or applications can either send requests directly to Kettles for low latency use-cases or post transactions on the SUAVE blockchain like a censorship resistant bulletin-board. Determined by the users, these transactions or requests have public and private inputs. Private inputs eliminate information asymmetries and eliminate trust requirements for private mempool operators. Kettles can read SUAVE blockchain state or use inputs they receive directly to run computations based on the SUAPP logic. The outputs of Kettle computations can be post on the SUAVE blockchain or other destinations like sharing directly with block builders. These outputs can be ordered transactions or transaction bundles which can be used to build Ethereum blocks. In other words, SUAPPs enable different block building and auction mechanisms to be programmed as smart contracts to drive better outcomes for the users.

Execution

SUAPP execution is enabled by Kettles

, network actors that run TEEs (Intel SGX) for credible and private computations. Privacy-preserving computation properties of SUAVE further protect users from informational asymmetries and adversarial transaction ordering (sandwich, frontrunning, backrunning) attacks.

SUAPP executions can either be handled by a single kettle or replicated across multiple kettles. Kettles can be designed as single off-chain co-processors (i.e. TEE-rollups [32] as proposed by A. Miller) with computational guarantees provided by the TEE. To be more specific, off-chain Kettle execution can be cheaply verified on chain, using remote attestation [47]. This design is suitable for low-latency use-cases like block building. Alternatively, SUAPP computations can be replicated by multiple Kettles, which would enable SUAVE validators to form consensus on Kettle computations. This model reduce reliance on TEEs for correctness and also provides stronger liveness and censorship guarantees seen in more traditional blockchain designs. The second approach is similar to the concept of privacy preserving smart contracts that was introduced by Ekiden [33] and built in production for the first time bySecret Network [34]. Different SUAPPs will have different security, liveness and latency trade-offs; therefore we are likely to see different execution models for SUAPPs. Kettles, which store their own private key inside the TEE, can sign transactions that emit bundles or transactions for Ethereum block production. Confidential computations that are run in Kettles can update public SUAVE chain state by emitting SUAVE transactions or directly share data with authorized parties such as block builders.

Written in Solidity, SUAPPs can trigger any arbitrary logic. In the case of block building, SUAPPs form and/or order transactions based on an auditable logic to create transaction bundles (partial blocks) that can be sent to external builders. These partial bundles can also be consolidated into full blocks on SUAVE, using a secondary SUAPP, to be sent to Ethereum proposers. SUAPPs can be used to order signed transactions like replicating existing searcher algorithms and allowing Ethereum dApps to auction their order flow. As a results, SUAPPs enable users and applications to know exactly how their transactions will be ordered. This is an extremely important feature that can enable application level transaction ordering logic proposed in improved AMM designs. Another use-case for SUAPPs is to build user-facing applications with specific execution logic that would take intents from Ethereum users, execute on SUAVE and settle on Ethereum. These applications can range from DeFi primitives to gaming.

The Kettles run MEVM, a fork of Geth's impementation of the EVM, which is extended with additional pre-compiles that provides flexibility to address MEV use-cases. More specifically application builders can perform off-chain queries (i.e. market price or computational outcome from another Kettle) and read Ethereum state using these pre-compiles in MEVM. These pre-compiles allow block builders and searchers to run computations that are very expensive in Solidity, such as simulating bundles of transactions and creating Ethereum transaction bundles (or partial / full Ethereum blocks). The ambition of the MEVM is to allow the current centralized MEV infrastructure to be expressed as smart contracts on a decentralized blockchain using these precompiles designed for the MEV supply chain. Furthermore, MEVM will run inside a trusted execution environment (TEE) and interact with confidential data store and confidential compute requests. Confidential data store allows Kettles to privately exchange data among themselves which is important for parallelized computations and forming consensus on confidential computations. This also allows for an encrypted state which enables access control use cases, such as NFT being only accessible to the buyer or a list of whitelisted addresses, to be built on SUAVE. Since MEVM provides credible and private computation guarantees and the ability to access off-chain data sources, it creates a new design space for decentralized applications as well besides decentralized block building.

How does SUAVE address DEX problems?

In the previous sections we have outlined problems for traders and liquidity providers in DEXs and provided an overview of SUAVE blockchain architecture and its unique features. In this section, we will explore how these features can help address specific problems with DEXs.

- Programmable privacy: Programmable privacy allows SUAVE applications (SUAPPs) to compute on private data, which in the context of DEXs, hide swap size and slippage limits. As a result, programmable privacy eliminates adversarial ordering attacks that extracts value from swappers. These attacks approximately cost 7-14bps based on Uniswap analysis on ETH-USDC and ETH-PEPE pairs. 7-14 bps lost on adversarial transaction ordering is a

significant cost item, as the total cost of a trade on Binance is 10bps. Furthermore programmable privacy enables effective (sealed-bid) on-chain auction designs, which is the backbone of any trade execution logic.

- Credible, low cost computations: SUAPPs that run inside Trusted Execution Environments (TEEs) provide verifiable computation guarantees and are able to handle expensive computations like running an order book and matching orders. Furthermore, SUAVE can minimize computational costs as execution would not have to be replicated across every node in the network. This is critical for seamless order placement. Coupled with orders that have expiry conditions, market-making on SUAVE can resemble market-making on a CLOB. One of the biggest reasons for LVR is high cost of active liquidity management in AMMs on Ethereum. Lowering costs and entry barriers to active liquidity provision would enable profitable LP'ing for retail, increase liquidity in DEXs and provide superior execution.

- Low latency: SUAVE is expected to have 3 second blocks. Shorter block times reduce losses to LVR, which is caused by block builders sniping passive liquidity. As shown in research [6], reduction of block times from 12 seconds to 3 seconds, halves the LVR losses for liquidity providers. Furthermore, the ability to run exchange logic inside the Kettle can significantly improve execution time and provide sub-second latency.

- Tight Ethereum coupling: Ability to access Ethereum state and post transactions on Ethereum allow SUAVE to become a low cost decentralized intent execution layer for Ethereum. Unlike roll-up based scaling which create liquidity silos that are detrimental to DeFi, Suave allows users to interact with liquidity on Ethereum.

- MEVM precompiles: These precompiles allow SUAVE to access off-chain data such as price oracles which are relevant for DeFi. Furthermore MEVM provides the ability to read Ethereum state via an Ethereum state through a light client integration, which can allow SUAPPs to tap into passive liquidity sources on Ethereum.

In addition to providing a unique feature set to solve problems faced by traders and liquidity providers in AMMs, SUAPPs can be used to implement DEX improvement areas discussed above in a more decentralized and trust minimizing way.

Solver and RFQ model

Current off-chain order matching model, that is used by CowSwap, 1inch Fusion and Uniswap, which are maintained by solver that are permissioned and whitelisted by DEX operators, can be built as SUAPPs. Privacy preserving and trusted computation guarantees of SUAVE eliminate the need for DEX operators to run permissioned access systems. Currently CowSwap solver auction is run centrally by the CowSwap protocol. CowSwap solvers are required to stake funds which would be slashed if they deviate from the rules of the solver competitions. These deviations that are detected by social consensus and governance rules [18]. The entire CowSwap solver process can be coded into SUAPP execution logic: the introduction of privacy preserving and credible computations eliminate the need for these centralized structures and high barriers of entry. As a result, SUAPPs can ensure censorship resistance and increase competition, which will provide better execution for end users. Finally SUAPPs would also enable platform decentralization, which is important given the legal uncertainties surrounding DeFi.

Application specific transaction ordering models

In the earlier section, we also introduced application specific transaction ordering proposals for DEXs to address LVR and adversarial transaction ordering. These models require buy-in from builders and proposers on Ethereum or more realistically adjustments to the current application logic. Recent innovations like Uniswap Hooks [35], provide application level ordering or execution logic without requiring protocol level changes. However these hooks require dedicated liquidity pools and have the risk of siloing liquidity. As a results, these adjustments may come at the expense of users as fragmented liquidity will increase price slippage. Given that SUAVE is a system to help block production on Ethereum, SUAPPs can execute logic that allows application specific ordering and send these partial blocks to block builders (which may also be implemented as contracts in the MEVM) as bundles rather than requiring them to be ordered a certain way by the block builders. Uniswap community can vote to send all Uniswap user transactions to a SUAPP with ordering properties to eliminate LVR, rather than creating different hooks that would fragment liquidity and increase the cost of trading.

SuaveDEX

In addition to the proposed improvements, SUAVE can enable an intent-based DEX, in which orders execute on SUAVE and settle on Ethereum or other EVM chains. The order execution can involve frequent batch auctions or an order-book model with a matching engine executing on SUAVE. Privacy preserving computation properties of SUAVE protect user transactions from attacks and allow credible and efficient (sealed-bid) auctions or order execution to be performed on each SUAVE block. These bundled transactions can be sent to block builders and later settle on Ethereum.

[

image

1400×816 192 KB

](https://collective.flashbots.net/uploads/default/original/2X/9/9f864f3519ebbadcdbbea1f454ba7ec365212af4.jpeg)

SuaveDEX contract receives intents from users and liquidity providers, who provide spending permissions (deposits) to the SuaveDEX contract on Ethereum. SuaveDEX contract on the SUAVE:

- acts as a private order-book for taker and maker orders and;
- checks user balances and permissions to ensure only valid orders are in the order-book leveraging the built-in Ethereum light node in Kettles
- runs trade execution logic every SUAVE block (planned to be 3 seconds) or instantaneously inside a kettle. Matched transactions and the status of the orderbook can be posted on the SUAVE chain.
- consolidates matched transactions from SuaveDEX before each Ethereum block and pass a single Ethereum transaction to block builders via a relay to ensure SuaveDEX transactions are included in the next Ethereum block. Users can also opt into delayed settlement on Ethereum, as opposed to immediate settlement, which would allow executed SuaveDEX transactions to be further bundled to provide better post-execution anonymity.

SuaveDEX singleton contract on Ethereum manages user spending permissions, account balances and signature verifications. Similar to EntryPoint

contract in ERC-4773 or Permit2

function used by UniswapX, the contract ensures users have sufficient funds to trade, relevant signatures from the maker, taker and the SUAPP (Kettle) is provided, after which the contract enables movement of funds between takers and makers. This contract also collects trading fees from makers and takers. SuaveDEX can also use a deposit contract on Ethereum to provide a TEE-roll up app-chain like construct.

How else SUAVE can help with DeFi?

In addition to create an improved DEX design, SUAVE can enable an auction protocol that helps existing DeFi application to run more effective auctions. Auctions are one of the most important building blocks in DeFi. While blockchain based auctions have been a promising alternative to electronic auctions, as they can replace the requirement for an auctioneer to be trustworthy and correctly run the auction, with smart contracts that would guarantee correctness of execution. However, blockchain based auctions fail to scale linearly with increasing number of participants and cause network congestion, increased fees and slower transaction times [36]. Auctions also require bid privacy to prevent bidder collusion and maximize the payment to the seller.

Dutch auctions, which is also known as a descending auction, have been seeing increased adoption in DeFi. In a dutch auction, the price gradually decreases until a buyer submits the winning bid. Dutch auctions can reduce congestion and scaling issues associated with blockchain auctions. However Dutch auctions do not guarantee that the seller maximizes the payout. Since the transaction mempool is public in blockchains, Alice, an adversarial bidder, who values the auction more than any other bidder can withhold her bid, observe the mempool to see when Bob, the next highest bidder sends his bid and front-run Bob's transaction. This may allow Alice, the adversarial bidder to pay less than what she would have in a sealed bid auction and reduces the profit of the auctioneer.

Privacy-preserving computational guarantees of SUAVE enable efficient and credible auctions, which are the building block of any trade execution method. Blockchains are able to solve for credible auctioneer problem via smart contracts. Coupled with privacy preserving execution properties of SUAVE, it's possible to run sealed bid auctions, which may maximize auctioneer welfare as well. SUAPP based auctions will also have significant cost and user experience benefits, compared to commit-reveal based auctions that depend on deferred revelation of bids to ensure incentive compatibility of actors and the credibility of the auctioneer [37].

Auctions are already widely used in most popular DeFi protocols:

Auctions in collateralized stable coins

Collateralized stable coin projects like MakerDAO and Reflexer (a fork of Maker) use auctions for vault liquidations when collateral in the vault is no longer able to sustain collateralization ratio. Both of these protocols use a two phased auction mechanism; i) first an ascending auction to determine how much stable coin is required to achieve target colletalization rate and ii) a descending auction to determine the minimum amount of collateral to be taken out in exchange for provided stable coin.

MakerDAO has two additional auction mechanisms; surplus auction and debt auction. When the system surplus from stability fees go above a certain level, the system auctions surplus DAI in exchange of MKR. This is an ascending auction where highest bidder of MKR receive the allocated DAI in the auction. Debt auction on the other hand is used when the system has bad debt that cannot be covered by the stability pool DAI. In this case, the system auctions newly minted MKR in exchange for DAI. This is also a descending auction where bidders are accepting decreasing amounts of MKR for a given amount of DAI to recapitalize the system. Given MKR's reliance on USDC as a collateral, there has been fewer liquidations in the recent months compared to the early days of MKR [38].

All of these auctions can be executed on SUAVE as single-phase sealed bid auctions, which would; i) eliminate the two step process required in collateral auctions, ii) eliminate possible collusion opportunities in Surplus auctions, iii) create cheaper auctions that do not result in network congestion and high transaction fees.

In addition to liquidations in collateralized stable coins, auctions are used in NFT sales, options pricing (Ribbon Finance) and

finally bond issuance (FRAX). Option and derivatives pricing is an interesting use-case for auctions; given that no accepted industry standard exists to price options and derivatives, auctions are very beneficial for price discovery. Of these auction models, NFT sales and options pricing depend on centralized auctions [39]. Frax Bond (FXB) token is a zero-coupon bond that converts to FRAX stable coin at maturity. The rate of the FXB discount (or the effective interest rate) is determined based on a Dutch auction, similar to price determination in government treasuries [40].

Conclusion

The exploration of the application design space on SUAVE in Decentralized Finance (DeFi), underscores its potential to significantly create value for blockchain applications. This study has identified that SUAVE, with its advanced features such as programmable privacy, fast finality, and an efficient execution framework with validity guarantees, is well-positioned to address several critical challenges currently faced by Decentralized Exchanges (DEXs), the most used decentralized applications. Notably, SUAVE's design can reduce the cost of on-chain trading by providing effective solutions to pervasive issues in the AMM-based DEXs, such as front-running and the Loss-Versus-Rebalancing (LVR) problems for traders and liquidity providers respectively. Furthermore, SUAVE holds the potential to revolutionize the mechanisms of DeFi auctions, providing a more efficient and value maximizing auctions in collateral liquidations and price discovery processes, initially for digital assets, and potentially extending to Real World Assets (RWAs) in the future.

While the promise of SUAVE in propelling a new wave of growth and innovation in DeFi is clear, it will be interesting to observe whether incumbent Ethereum applications will integrate SUAVE into their products and to see how transaction bundles made in SUAVE will impact the block-building supply chain in the early days. Moving forward, it's important to concentrate efforts to foster collaborative relationships within the DeFi community, incubate and support new players to build native SUAPPs and continue the momentum of research and development to optimize SUAVE's capabilities in sync with the dynamic needs of DeFi as well as block building. By targeting fundamental issues around privacy, efficiency and provability of transaction executions, SUAVE will provide significant benefits to blockchain applications.

In conclusion, SUAVE represents a pivotal advancement in the ongoing evolution of blockchain applications. Its successful integration will pave the way for a new era of adoption in blockchain applications and specifically DeFi.

Thanks to @Quintus @sarah.allen @dmarz @halo3mic for their feedback

References

[1] DeFiLlama, "Total Value Locked All Chains", DeFiLlama, 2024. [Online]. Available: https://defillama.com/chains. [Accessed: Jan. 05, 2024].

[2] Dune Analytics, "Ethereum Overview Recent TX," Dune Analytics, 2023. [Online]. Available: https://dune.com/queries/1109717/1895686. [Accessed: Nov. 24, 2023].

[3] Nansen, "Multichain ETH," Nansen, 2023. [Online]. Available: https://pro.nansen.ai/multichain/eth. [Accessed: Jan. 9, 2024].

[4] D. Robinson, "Uniswap V3," presented at the Stanford Blockchain Conference, Palo Alto, CA, USA, Aug. 29, 2022. [Online]. Available: https://www.youtube.com/watch?v=rbcGjQgbksk&t=1924s. [Accessed: January 17, 2024].

[5] [3] Nansen, "Gas Tracker," Nansen, 2023. [Online]. Available: https://pro.nansen.ai/gas-tracker. [Accessed: Jan. 8, 2024].

[6] J. Milionis, C. Moallemi, T. Roughgarden and A. Zhang, "Automated Market Making and Loss-Versus-Rebalancing,". arXiv:2208.06046 ,

1. [Online]. Available: https://arxiv.org/pdf/2208.06046.pdf

[7] The Block, "Decentralized Finance (DeFi) / DEX (Non-Custodial)," The Block, 2023. [Online]. Available:DeFi Exchange Data and Charts for DEXs, AMMs and Swaps. [Accessed: Jan. 04, 2024].

[8] The Block, "DEX to CEX Spot Trading Volume," The Block, 2023. [Online]. Available: DeFi Exchange Data and Charts for DEXs, AMMs and Swaps. [Accessed: Jan. 04, 2024].

[9] Uniswap, "Uniswap Pools," Uniswap Info, 2023. [Online]. Available:Uniswap Info. [Accessed: Dec. 12, 2023].

[10] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach and A Juels, "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges," arXiv:1904.05234,

1. [Online]. Available: [1904.05234] Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges

[11] EigenPhi, "Ethereum Sandwich," EigenPhi, 2023. [Online]. Available:Sandwich Overview | EigenPhi. [Accessed: Dec. 24, 2023].

[12] A. Adams, B. Chan, S. Markovich and X. Wan, "The Costs of Swapping on the Uniswap Protocol," arXiv:2309.13648v1

, 2023. [Online]. Available: https://arxiv.org/pdf/2309.13648.pdf

[13] 0x, “Measuring the Impact of Hidden DEX Costs,” 0x, 2023. [Online]. Available: Measuring the impact of hidden DEX costs. [Accessed: Dec. 10, 2023].

[14] W. Warren, “Once MEV bots are ubiquitous…,” Twitter, 17-Jun-2021. [Online]. Available: https://twitter.com/willwarren/status/1405355903138680840. [Accessed: Dec. 10, 2023].

[15] E. Chen, A. Toberoff, S. Srinivasan and A. Chiplunkar, “A Tale of Two Arbitrages,” Frontier, 2023. [Online]. Available: A Tale of Two Arbitrages. [Accessed: Oct. 13, 2023].

[16] 0xfbifemboy, CrocSwap, “Usage of Markout to Calculate LP Profitability in Uniswap V3,” Medium, [Online]. Available: Usage of Markout to Calculate LP Profitability in Uniswap V3 | by CrocSwap | Medium [Accessed: Nov. 15, 2023].

[17] According to Titan CEO, Kubi Mensah [17], Uniswap - Binance arbitrage accounts for approximately 60% of MEV on Ethereum.

K. Mensah, “MEV: Fractalization of Block Building | Pragma Istanbul 2023,” [Online]. Available: https://www.youtube.com/watch?v=SUeBGrBiu7M. [Accessed: Nov. 25, 2023].

[18] CoW Protocol, “CoW Protocol Documentation,” [Online]. Available: https://docs.cow.fi/. [Accessed: Oct. 21, 2023].

[19] Uniswap, “Uniswap V3 Overview,” Uniswap Documentation, [Online]. Available: Overview | Uniswap. [Accessed: Oct. 22, 2023].

[20] 1inch Network, “Introduction to Fusion Swap,” 1inch Documentation, [Online]. Available: Introduction | 1inch Network. [Accessed: Oct. 22, 2023].

[21] 0x, “About the RFQ System,” 0x Swap API Documentation, [Online]. Available: About the RFQ System | 0x Docs [Accessed: Nov. 4, 2023].

[22] Hashflow, “Hashflow Documentation,” Hashflow Docs, [Online]. Available: What is Hashflow? - Hashflow. [Accessed: Oct. 24, 2023].

[23] DFlow, “Introduction to DFlow,” DFlow Documentation, [Online]. Available: Overview. [Accessed: Oct. 24, 2023].

[24] Josojo, “MEV-Capturing AMM (McAMM),” Ethereum Research Forum, 10-Aug-2022. [Online]. Available: MEV capturing AMM (McAMM) - #6 by fleupold - Applications - Ethereum Research. [Accessed: Oct. 27, 2023].

[25] C. McMenamin, V. Daza and B. Mazorra. An Automated Market Maker Minimizing Loss-Versus-Rebalancing arXiv:2210.10601.

November, 2023.

[26] ArrakisFinance, “Code Walkthrough for Minimize LVR Hook Proof of Concept,” GitHub, 2023. [Online]. Available: minimize-lvr-hook-poc/documentation/code-walkthrough.md at main · ArrakisFinance/minimize-lvr-hook-poc · GitHub [Accessed: Dec. 3, 2024].

[27] M. Ferreira and D. Parkes, “Credible Decentralized Exchange Design via Verifiable Sequencing Rules,” arXiv:2209.15569,

1. [Online]. Available: https://arxiv.org/pdf/2209.15569.pdf

[28] A, Nezlobin, “So it begins…,” Twitter, 15-Feb-2023. [Online]. Available: https://twitter.com/0x94305/status/1674857993740111872. [Accessed: Nov. 12, 2023].

[29] Snapshot, “Proposal: Lowering Trading Fees on Select Balancer Pools,” Balancer, 2023. [Online]. Available: Snapshot. [Accessed: Dec. 1, 2023].

[30] 0xKeyu, “Ending LP’s Losing Game: Exploring the Loss-Versus-Rebalancing (LVR) Problem and its Solutions,” Mirror, 2023. [Online]. Available: Ending LP's Losing Game: Exploring the Loss-Versus-Rebalancing (… — 0xKeyu [Accessed: Nov. 13, 2023].

[31] P. Daian and A. Miller, “SUAVE Explained with Phil Daian and Andrew Miller,” in Bankless

, Bankless, [Online]. Available: 198 - SUAVE Explained with Phil Daian & Andrew Miller | Bankless [Accessed: Dec. 2, 2023].

[32] A. Miller, N. Jean-Louis, Y. Li, S. Bellemare, G. Arrouye, J. Austgen, B. Akintade, A. Seira, D and Z. Wu, “TEE Rollups: Fixing Access Patterns in TEE-Based Smart Contracts with Off-Chain Computing,” Medium, 2023. [Online]. Available: TEE Rollups: Fixing Access Patterns in TEE-based Smart Contracts with Off-chain Computing | by Decentralized Systems Lab | Medium. [Accessed: Sept. 27, 2023].

[33] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson,

A. Juels, A. Miller and D. Song, “[Ekiden: A Platform for Confidentiality-Preserving,

Trustworthy, and Performant Smart Contracts](https://www.notion.so/SUAVE-s-Potential-in-DeFi-A-focus-on-decentralized-exchanges-DEX-and-auction-mechanisms-1487c4855212453bb8f0d05648e03bd2?pvs=21),” arXiv:1804.05141v7,

1. [Online]. Available: https://arxiv.org/pdf/1804.05141.pdf

[34] Secret Network Documentation, “Secret Network Overview,” Secret Network Documentation, 2023. [Online]. Available: Secret Network Overview | Secret Network. [Accessed: Jan. 9, 2024].

[35] H. Adams, “Uniswap V4,” Uniswap Blog, 2023. [Online]. Available:Our Vision for Uniswap v4. [Accessed: Nov. 12, 2024].

[36] M. Minaei, V. Le, R. Kumaresan, A. Beams, P. Moreno-Sanchez, Y. Yang, S. Raghuraman, P. Chatzigiannis and M. Zamani, “Scalable Offchain Auctions”, Cryptology ePrint Archive, Report 2023/1454

, 2023. [Online]. Available: https://eprint.iacr.org/2023/1454.pdf

[37] T. Chitra, M. V. X. Ferreira and K. Kulkarni, “Credible, Optimal Auctions via Blockchains,” Cryptology ePrint Archive, Report 2023/114

, 2023. [Online]. Available: https://eprint.iacr.org/2023/114.pdf

[38] [1] MakerDAO, “The Auctions of the Maker Protocol,” MakerDAO Documentation, 2023. [Online]. Available:The Auctions of the Maker Protocol | Maker Protocol Technical Docs. [Accessed: Oct. 24, 2023].

[39] Ribbon Finance, “Theta Vault Auctions,” Ribbon Finance Documentation, 2023. [Online]. Available:Auctions | Ribbon Finance. [Accessed: Oct. 25, 2023].

[40] Frax Finance, “FRAX V3 FXBs,” Frax Finance Documentation, 2023. [Online]. Available:FXBs | English | Frax ¤ Finance. [Accessed: Oct. 25, 2023].

[41] U.S. Department of Justice, “Justice Department Sues Google for Monopolizing Digital Advertising Technologies,” U.S. Department of Justice, [Online]. Available: Office of Public Affairs | Justice Department Sues Google for Monopolizing Digital Advertising Technologies | United States Department of Justice. [Accessed: Dec. 13,2023].

[42]

B. Caparros, A. Chaudhary and O. Klein, “Blockchain scaling and liquidity concentration on

decentralized exchanges,” arXiv, [Online]. Available: https://arxiv.org/pdf/2306.17742.pdf. [Accessed: Nov. 17, 2023].

[43] Snapshot, “CIP-7: Allowing External Solvers,” CowDAO, [Online]. Available:Snapshot. [Accessed: Jan. 22, 2024].

[44]

A Lu, “Illuminate the Order Flow,” Flashbots Writings, [Online]. Available:Illuminating Ethereum's Order Flow Landscape | Flashbots. [Accessed: Insert Jan. 21, 2024].

[45] “Orderflow Visualization,” Orderflow.art, [Online]. Available: Link. [Accessed: Jan. 23, 2024].

[46] “Builders - Rated Network,” Rated Network, [Online]. Available:Builder Landscape | Ethereum Mainnet. [Accessed: Jan. 23, 2024].

[47] “Demystifying Remote Attestation by Taking It On-Chain,” Collective, Flashbots, [Online]. Available: Demystifying remote attestation by taking it on-chain - #2 by socrates1024. [Accessed: Jan. 21, 2023].