Demystifying the Intent-Centric Thesis

Moulik Nagesh

Table of Contents

Key Takeaways **2**
The Intent-Centric Thesis **3**
Intents: The What, Why, and How 3
Intents vs. Transactions 4
The Role of Solvers 5
The Relevance of Account Abstraction 7
Market Landscape **8**
Use Cases 9
Ecosystem Mapping 10
Project Spotlight **11**
General Purpose 12
Anoma 12
SUAVE 16
Essential 17
Intent-Specific 18
UniswapX 18
CoW Swap 20
1inch Fusion 23
Outlook **24**
Opportunities and Risks 24
Adjacent Considerations 26
Closing Thoughts **27**
References **28**
Latest Binance Research Reports **29**
About Binance Research **30**
Resources **31**

1 Key Takeaways

- Current Web3 systems are complex and present barriers to entry, requiring users to navigate fragmented infrastructure. This often leads to suboptimal user experiences and vulnerabilities like MEV exploitation.

- Intents are signed messages that enable users to express their on-chain goals, while third-party solvers handle the technicalities, simplifying the process and enhancing user experiences. Intents are opening the door to new use cases.

- Solvers are pivotal for counterparty discovery, identifying and categorizing user intents to optimize the path for valid transactions. Their competition in a free market, based on price and credibility, incentivizes them to discover the most efficient execution path, ensuring maximum value for users.

- Account Abstraction serves as the gateway for intents, made possible by the validation logic within a smart contract wallet. However, it is primarily engineered for single-domain usage, lacking the capability to operate seamlessly across multiple chains.

- To handle more generalized, multi-domain intents, protocols like Anoma, SUAVE, and Essential are developing the requisite infrastructure for a dedicated intent layer. This includes the introduction of new intent languages and virtual machines.

- Leading applications are expanding their functionality by directly involving solvers. Various protocols are attending to specialized types of intents, including UniswapX, CoW Swap and 1inch Fusion.

- Improved composability among intent pools increases the matching opportunities for solvers, making it easier to bootstrap solver networks. Success in intent-centric networks hinges on aligning solver incentives with ideal user outcomes.

- Intent-centric setups encompass technical complexities that AI can effectively mitigate. AI's capabilities include interpreting natural language intent, goal deconstruction, and strategizing optimal transaction routes.

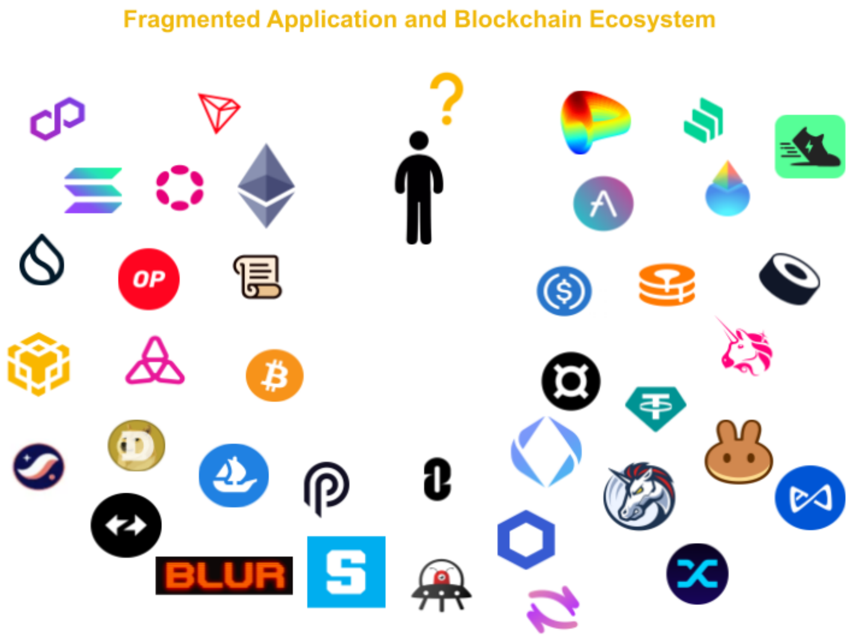
2 The Intent-Centric Thesis

Intents: The What, Why, and How

Intents[1] have recently gained prominence as a solution to the challenges encountered by users in the current Web3 paradigm. Today, while millions of users utilize blockchains to conduct transactions, there's a noticeable gap; among the total of 5.19B internet users[2], less than 100M possess blockchain wallets[3], the primary gateways to decentralized applications ("dApps"). What's hindering Web3 from broader adoption?

For starters, engaging with current Web3 systems can be a complex and time-consuming task, especially for those not well-versed with such technologies. These steep learning curves significantly heighten the entry barriers, deterring a large cohort of potential users from stepping into the ecosystem. **To interact with blockchains, users are required to navigate fragmented infrastructures to piece together an execution route**; this includes creating and signing transactions in a specific format, potentially using multiple applications and blockchains, and explicitly providing all information to reach a desired outcome. Such complexity often leads to a sub-optimal user experience ("UX"), is prone to errors, and paves the way for potential exploitation of MEV by more sophisticated actors.

Figure 1: The current order flow process in Web3 is fragmented



Source: Binance Research

As a result, intents emerged as a solution to overcome these challenges, with the aim of simplifying Web3 interactions for users. But what exactly are intents? **Intents are signed messages that enable users to express what they want to achieve on-chain, while third-party actors, known as solvers, handle the technical details to make it happen.** At their core, intents comprise a set of declarative constraints; users delegate transaction creation to solvers, who choose the best computational path on their behalf, all while retaining full control over their assets. In layman's terms, **intents allow users to focus on their end goals - the 'what' - without being bogged down by the specific steps - the 'how' - to realize those goals.**

Intent-centric solutions can be thought of as order flow abstraction. They pave the way for dApps to mirror the UX of conventional applications. **Users are no longer burdened by the complexities associated with blockchain interactions; instead, these are passed onto solvers**. This is particularly beneficial as the industry progresses toward a multi-Layer-2 ("L2"), multichain landscape. While Ethereum's rollup-centric roadmap solves for scalability, it introduces asynchronous states across a multitude of chains, in other words, it adds complexity to how information is processed and managed among these chains. This compromise adds challenges for users attempting to navigate this space. With intents, a substantial portion of the complexities associated with cross-chain liquidity, chain swapping, bridge selection and more are delegated to these backend solvers.

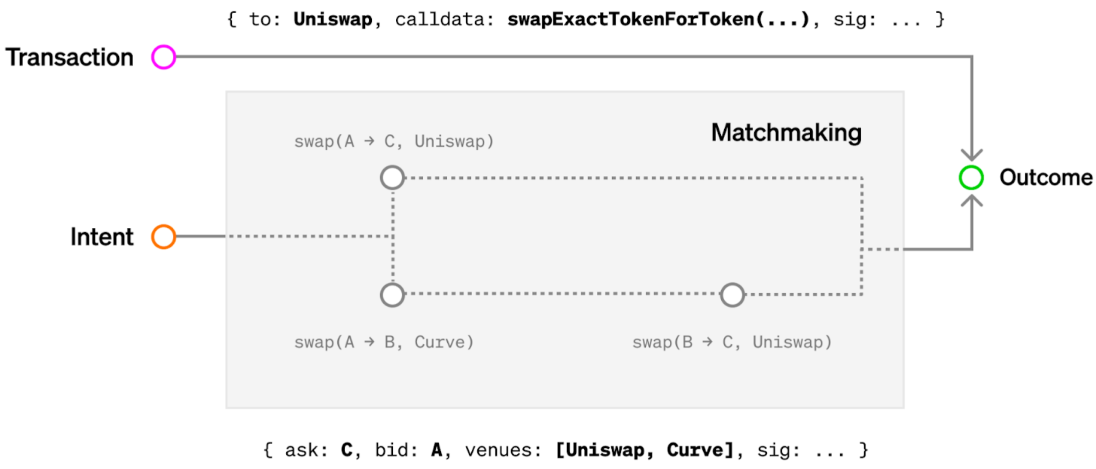
Ultimately, **intents are poised to transform the Web3 experience, transitioning it from a manual, step-by-step process to a more intuitive, outcome-focused approach**. They offer the prospect of smoother transactions, faster execution, and improved UX.

Intents vs. Transactions

The current transaction-based approach in Web3 leads to a sub-optimal user experience and a loss of efficiency, as users are compelled to make decisions without having sufficient access to information or employing sophisticated execution strategies. The inefficiency of transactions becomes glaringly apparent when one examines the steps required for a user to conduct transactions across two different blockchains. From connecting a wallet, switching networks, initiating a bridging method, to signing transactions, the process underscores significant pain points with the status quo.

In terms of definitions, a transaction is a highly specific action that a user wishes to perform, while an intent specifies what the user wishes to achieve within certain parameters. **When submitting a transaction, users specify the exact computational path; when submitting an intent, users specify the goal and some constraints, and a matchmaking process decides the computational path to be taken.** This system grants intents the versatility of multiple fulfillment avenues, in contrast to the rigid path set for transactions.

Figure 2: The shift from a transaction-based interaction to an intent-based approach removes additional barriers for users



Source: Paradigm

It is worthwhile to mention that the prevailing transaction-based approach also allows users to outsource transactions to a third party, typically applications. However, these applications often lack sufficient incentives to seek the optimal result for users. **The innovation of intents doesn't lie merely in delegating transaction creation to a third party, but to a network of specialized solvers ready to deliver superior outcomes**. This setup enhances execution efficiency as solvers possess the capability to assimilate extensive data from multiple chains, eliminating the need for repetitive user interactions.

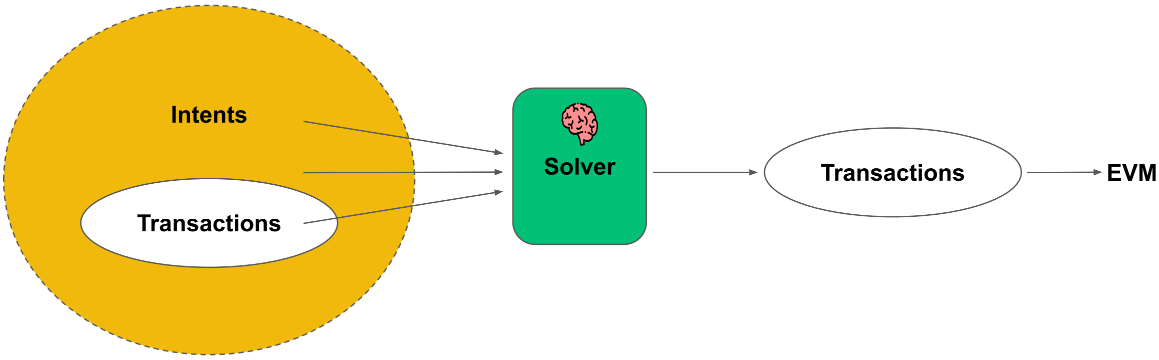
The Role of Solvers

Next, how exactly are intents executed? Here, the role of 'solvers' becomes crucial. **Intents with compatible preferences can be identified and matched** in many different, complex ways involving many independent counterparties. **Once a successful match is found, intents can settle on-chain** and be verified by the user. This process is referred to as **counterparty discovery** and it's performed by permissionless agents known as solvers, who run special algorithms. Put simply, **solvers can be thought of as on-chain smart assistants**.

Acting as intermediaries, solvers bridge the gap between user intents and blockchain execution, vying to offer the most favorable execution prices. **The solver presenting the most attractive execution price earns the right to execute the user's order.** As solvers have to compete on price and credibility in a free market, this competition incentivizes them to discover the best execution path and secure the best possible value for users. Solvers are able to match intents through one of the following channels:

- **Liquidity provision:** Solvers can act as the main counterparty by bringing their own liquidity to match trades.
- **Partial filling:** Multiple independent parties collectively buy a token being sold.
- **Direct coincidence of wants ("CoWs"):** Two intents can directly counter each other.
- **Ring trades:** Intent can be solved without direct CoWs. For example, three intents can produce a balanced transaction, even if no pairs of intents satisfy each other's preferences.

Figure 3: Solvers serve as coordinators, tasked with identifying user intents, categorizing them, and devising the optimal pathway to generate valid transactions



Source: Binance Research

Solvers are likely to assume specialized roles, and come in many different groups. For example, one solver might exclusively cater to matching trades on DEXes, while another might concentrate solely on NFTs. The following are some examples of what these distinctions may be.

- **Solver DAOs:** Solver DAOs are expected to act as generalized solvers, potentially fostering cross-ecosystem composability. Such DAOs may consist of solvers specialized for certain Layer-1 ("L1") ecosystems. Solver DAOs might even venture into private solving using trusted execution environments, where participants compete on skill - like optimizing routing solutions - while bidding in order flow auctions.
- **Application Specific Solvers:** Targeting specific sectors or verticals, these solvers specialize in certain applications, often without any overlap. This specialization allows them to refine their strategies, maximizing value extraction from tasks, whether in DeFi platforms or gaming applications.
- **Solver Funds:** These are specialized entities, distinct for a couple of reasons. Some solvers within this category might focus purely on routing solutions or

intent matching without maintaining any inventory. Others might both maintain inventory and act as market makers, thereby playing a dual role.

- **Individual Solvers:** Users or communities might occasionally solve their own intents by tapping into intent networks, operating solvers on nodes embedded in local devices.

Overall, the solver network is an important component of the intent-centric roadmap, utilizing off-chain infrastructure to improve on-chain UX.

The Relevance of Account Abstraction

While Account Abstraction ("AA") on its own is outside the purview of this report, ERC-4337 **provides wallets the capacity to serve as the gateway for intents**, made possible by the validation logic incorporated within a smart contract wallet. AA serves to enhance Externally Owned Accounts ("EOAs") by enabling their management through smart contract wallets, or alternatively, by allowing smart contracts to directly initiate transactions[4]. Users primarily utilizing EOAs can delegate their existing transaction-based workflows to solvers.

Hence, **AA is engineered to cater to 'specific intents'** and is often reduced to terms like 'gasless transactions' and 'seedless recovery'. It lowers the entry barriers to personal wallets and provides users with more user-friendly account systems. Yet, despite still being in early stages of adoption, the market's initial reception, as depicted in Figure 4, has been promising, with more innovation and development needed to fully realize its potential.

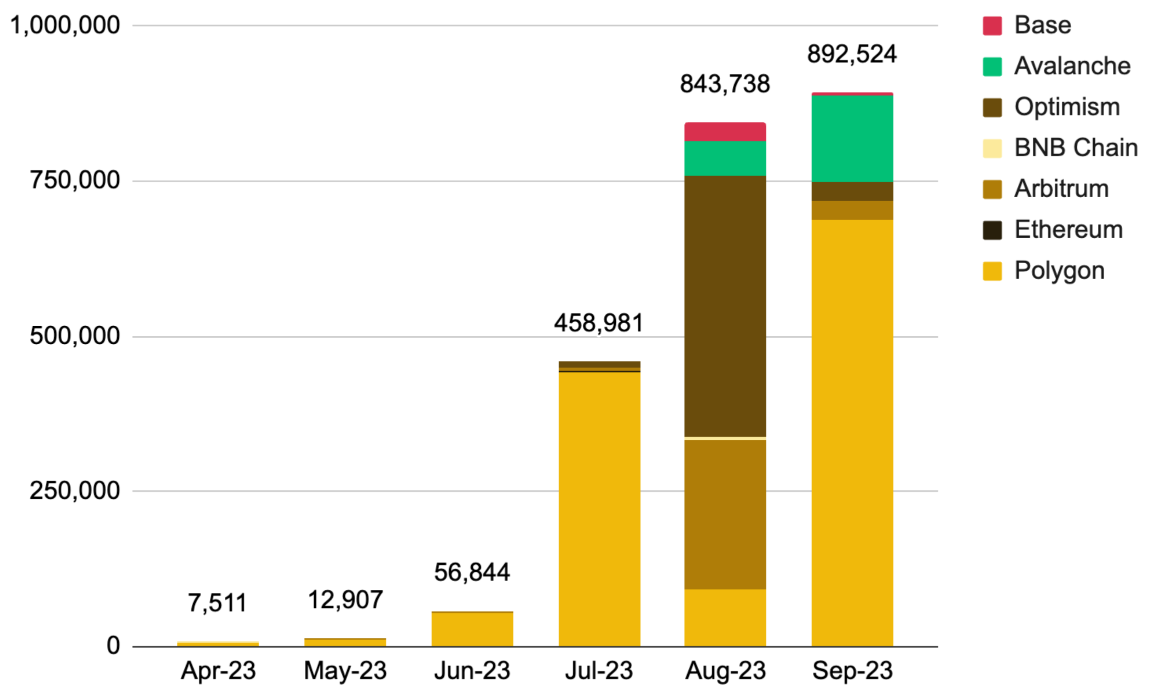
Intents simplify what users want to achieve, while Account Abstraction streamlines how it's accomplished

A notable limitation of AA is that it focuses solely on user accounts and is **primarily engineered for single-domain usage**, lacking the capability to operate seamlessly across multiple chains or support cross-chain paymasters. This constraint arises because ERC-4337, while proficient at enforcing a select number of intents within Ethereum's framework, **isn't designed as a generalized system for broader intent enforcement**. For example, AA still requires users to manually identify the most efficient route for order flows like swaps, bridging, or liquidity provisioning. **Intents aim to remove this discovery layer further, allowing users to specify only the starting and desired ending states**.

Therefore, simply addressing the UX issues through AA won't eliminate the entire spectrum of challenges faced by users today. Nonetheless, the recent upward trend in **AA adoption**

signals the market's appetite for products that enhance UX. By aligning with the capabilities of AA, intents are expected to further drive this adoption.

Figure 4: The month-on-month increase in ERC-4337 smart account transactions signifies broader adoption, highlighting the potential demand for related intent-centric products



Source: Dune Analytics (@niftytable), Binance Research, as of September 30, 2023

Ultimately, the true allure of AA resides in its architecture, which also transforms wallets into the entry point for intents, although its limitations become apparent when dealing with multi-domain scenarios - an issue the intent framework aims to address. If you're keen on delving deeper into AA, consider exploring our recent report: A Primer on Account Abstraction.

3 Market Landscape

Intents, in their most basic form, have been around for a while. Before the advent of Uniswap and Automated Market Makers ("AMMs"), several protocols had already embraced intent-based order books. Moreover, NFT marketplaces have been utilizing signed intents for listings and offers for a number of years. Another notable example is Decentralized Exchange ("DEX") aggregators. Here, users are solely focused on attaining the best execution, remaining indifferent to the specifics, such as the choice of DEX to be utilized.

More recently, platforms like CoW Swap and UniswapX have emerged, offering more advanced intent-based solutions for limit orders.

In the present market scenario, there are differences in how intents are perceived; some liken them to transactions ("txs"), while others view them as a contemporary form of limit orders. However, the architectural design for such intents is typically straightforward and single-purpose. Intents encompass far more than these classifications suggest, with a host of innovations yet to emerge.

While numerous systems have emerged to serve the limit order use case, **the creation of more advanced intent-based tools paves the way for broader, general purpose architectures**. Notable examples of general purpose intent systems include Anoma and Flashbots' SUAVE. They aim to introduce an **intent layer, where users can broadcast signed intents to gossip nodes**. Intent-specific chains in these systems aim to bridge the gap between users who sign the intents and solvers who execute them across different networks. Ultimately, once the infrastructure is in place, these **general purpose solutions are set to enable more robust use cases for intent-specific applications**.

Use Cases

Intents serve as an excellent means to improve counterparty selection, automation, and to coordinate multi-party commitments. There are several intent-specific applications emerging today, unlocking a broad spectrum of industry use cases. A few notable examples are highlighted below[(5)].

- **Limit orders and batch auctions:** Limit orders function as partial transactions. Solvers compete to find the ideal combination of counterparties, potentially across multiple DEX pools, to secure the optimal routing and price for users.

- **Smart orders:** Users can define specific execution conditions for their swaps and use intents to place various bids customized to their needs.

- **Automated actions:** Automate the execution of various actions. For instance, users might choose to dollar-cost average into a token or auto-rebalance their portfolios, either within a set range or at a predetermined time.

- **Cross-chain bridging:** Bridging can pose a significant UX challenge for users. By specifying preferences and risk thresholds, users can delegate and let solvers handle the process.

- **Crowdfunding:** Using intents, users are able to conditionally pledge funds, committing only when a project hits predefined milestones. A case in point is GitCoin Matching Funds, where users pre-commit donations to winning projects, even before they're chosen.

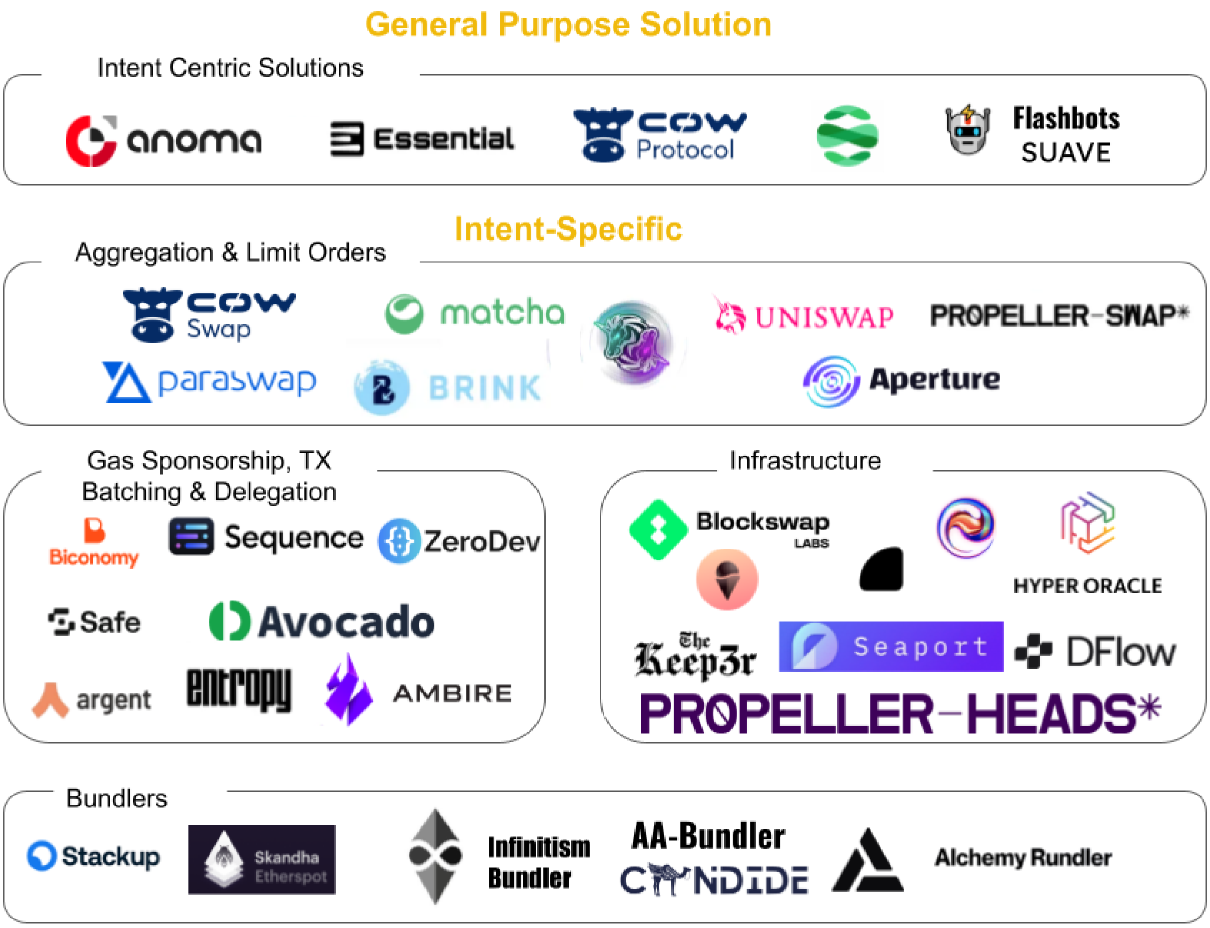
- **Peer-to-Peer ("P2P"):** By declaring intents, users can transact directly with others, eliminating the need for intermediaries and achieving better pricing. In the context of lending, lenders define their conditions, like desired collateral types and rates. Should a borrower repay early, and the lender wants to continue lending, solvers can match the lender with another suitable counterparty.

- **Security screening:** Utilize intents to restrict interactions to smart contracts that provide verifiable proofs, such as confirmation of approval by whitelisted audit teams.

Ecosystem Mapping

The diagram below only offers a general overview of projects exploring the world of intents. Though, it is important to recognize that there may be some intersections between categories, and the diagram below is simplified for clarity. In particular, the DeFi sector has observed growing adoption for intent-specific use cases. Going forward, we anticipate considerable shifts in the landscape, extending into other sub sectors as well.

Figure 5: Visual map of the different intent-centric projects and their categories



Source: Project Teams, Binance Research

4 Project Spotlight

Before diving further, it's worth highlighting that the intents sector can be broadly classified into two categories: general purpose infrastructure and intent-specific applications.

- **General Purpose:** More generalized intents require architecture tailored to optimize their use. Several protocols are developing this infrastructure, introducing components such as new intent languages and virtual machines ("VMs").

- **Intent-Specific:** Leading dApps that focus on specific types of intents are expanding their functionalities by directly involving solvers.

Given these distinctions, various protocols are attending to specialized types of intents. For example, swap-oriented intents are being catered to by platforms like UniswapX and CoW Swap. Single-domain or wallet-centric intents may be serviced by AA wallets or Essential-compatible dapps, while SUAVE and Anoma appear to be positioning themselves to manage generalized, multi-domain intents.

Figure 6: Comparative overview of general purpose and intent-specific solutions

Logo		Type	Solver Process	Solver Selection	Validation	Settlement
General Purpose						
	Anoma	Generalized Intents	Run algorithms, match intents, and propose to mempools	The first to complete task	Anoma VM	On-chain; Anoma protocols
	SUAVE	Multi-chain Intents	Off-chain computations, build and propose blocks to target chains	The first to complete task	Oracles and SUAVE validators	On-chain; SUAVE chain
	Essential	Intent-Centric Standard	Utilize on-chain and off-chain venues alongside DSL	Dutch auction	Core contract	On-chain
Intent-Specific						
	UniswapX	Limit Orders and Swaps	Combine on-chain and off-chain liquidity and run custom execution logic	Dutch auction	Reactor contract	On-chain
	CoW Swap	Limit Orders and Swaps	Identify CoWs and optimal routing	Batch auction	Smart contract	On-chain
	1inch Fusion	Limit Orders and Swaps	Identify matches and optimal routing	Dutch auction	Smart contract	On-chain

Source: Project Documentations, Binance Research

In the context of intent-specific applications, while solvers play a pivotal role, the absence of generalized intent solutions presents challenges. For instance, **one concern is the need to maintain separate infrastructures for off-chain solving and execution**. Though several teams are ambitiously tackling this, these undertakings typically necessitate multi-year roadmaps, which may impede innovations at the application level. By operating within custom, isolated off-chain networks, these protocols inadvertently forgo composability at the intent layer.

Notably, platforms like CoW Swap and 1inch Fusion, both serving in the DEX aggregator space, operate with distinct and non-intersecting intent pools. **Such compartmentalization means solvers lose out on potential aggregation and matching opportunities**. **This fragmentation also hinders the propagation of network effects**, which are important for the foundational growth of these ecosystems.

Intent-centric networks prosper when solvers engage in competitive resolution of intents, incentivized by fee accruals. The more intents that are circulated, the greater the incentive for new solvers to join, which is ultimately significant for enhancing the quality of intent execution. Therefore, this highlights the pressing need for a dedicated intent layer with the requisite infrastructure. Enter general purpose solutions like Anoma, designed to remove this burden and redirect application focus towards product-driven challenges. Nevertheless, the dynamics between general purpose and intent-specific solutions are likely to evolve going forward.

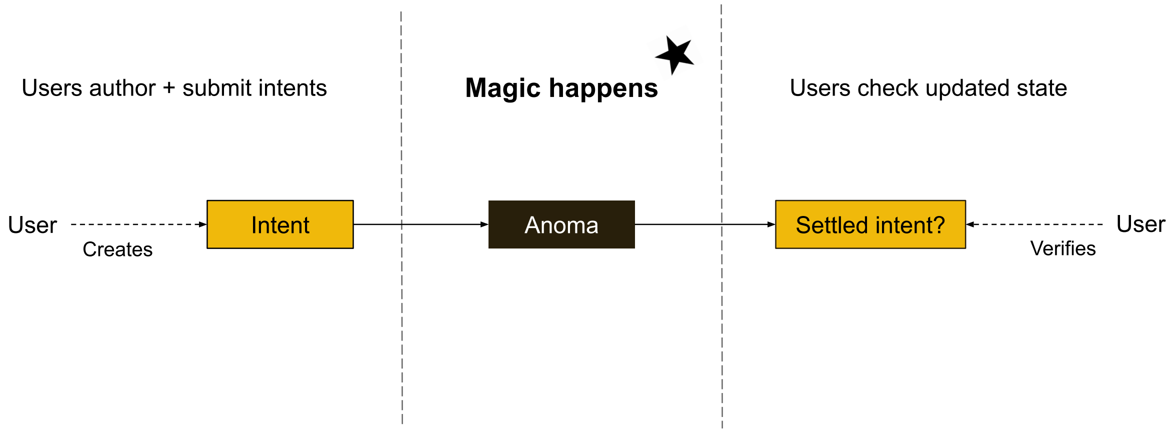
General Purpose

Anoma

Anoma serves as the unified intent-centric network. Their vision is to **build out a global intent network where nodes can observe and process intents across a wide range of use cases**[6]. Anoma utilizes intents to provide efficient and private means for counterparty discovery. In particular, Anoma facilitates declarative privacy, decentralized counterparty discovery, solving processes, and multi-chain atomic settlements.

Anoma positions itself as the base architecture deployable at any layer (L1, L2 etc.) rather than a function within a particular stack or layer. It is engineered so that anyone can create fractal instances of the protocols that collectively make up the Anoma ecosystem. This setup offers significant advantages in terms of flexibility and composability with each fractal instance.

Figure 7: Users can submit intents to the network, with Anoma handling both counterparty discovery and settlement

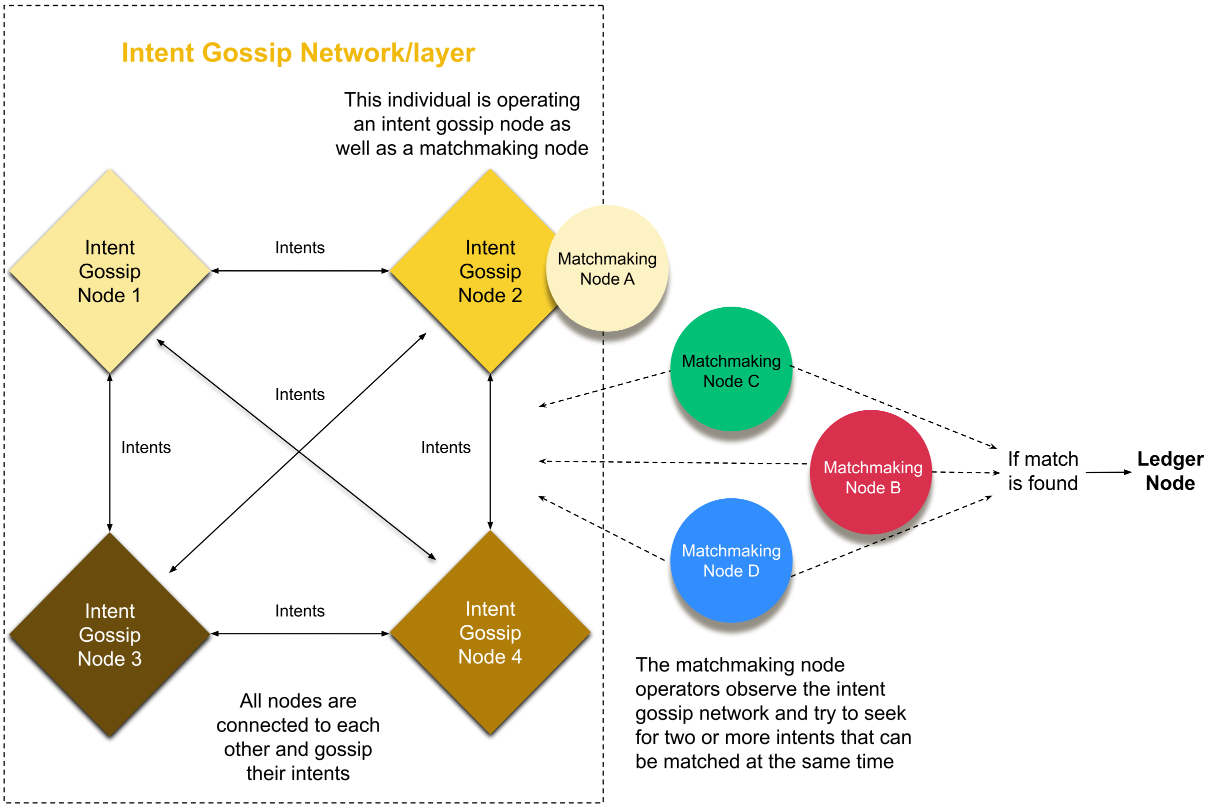


Source: Anoma Documentations, Binance Research

In Anoma's framework, users express their desired outcomes through intents, and the protocol generates signed partial transactions in response. User intents are then channeled to intent gossip nodes, forming permissionless intent pools. Much like the mempool, these pools function as a P2P networking layer filled with various user intents. Solvers enable counterparty discovery by sifting through these pools to identify matching intents, and when combined, they create transactions to fulfill the conditions of each respective user's intent. Solvers, being interoperable, operate over all fractal instances, allowing them to match intents across multiple chains.

Moreover, to improve efficiency, **Anoma's gossip layer employs path authentication**; in scenarios where the intent is complex and requires a series of matching, intermediate solvers and gossip nodes are tracked and rewarded for their participation. When a solver partially fulfills an intent, they can stake a claim on their efforts and share the partial intent with other solvers. Once matching intents are found, rewards are distributed to both solvers based on path authentication. This setup also aids solvers in maintaining local trust graphs for ongoing collaboration.

Figure 8: Intents are propagated via Anoma's intent gossip nodes, while matchmaking nodes employ solver algorithms to identify and match compatible intents



Source: Anoma Documentations, Binance Research

An essential aspect of Anoma is its modular and open-source architecture, available for developers to leverage in creating novel applications. As we will explore in the following sections, Anoma comprises several components in its technical stack. Developers have the flexibility to utilize the entire stack or select specific elements to address specific use cases, such as achieving counterparty discovery and solving.

Namada

Namada is the initial fractal instance of Anoma, dedicated to privacy at the settlement layer[7]. It acts as a testing ground for Anoma's multi-asset shielded pool ("MASP"). MASPs in Anoma utilizes zk-SNARKs, allowing all assets to share a common shielded pool, thereby enhancing the anonymity set for user. This, in turn, allows owners of these assets to form one big anonymity set contributing to each other's privacy.

Namada aims to be interoperable with Ethereum or any IBC-enabled blockchain, supporting both fungible and non-fungible tokens sent via a custom Ethereum bridge or through IBC. Privacy preserving asset transfers on Namada are enabled by MASPs, allowing assets like NFTs, ETH, DAI or any Namada-native assets to share the same shielded set, rendering them indistinguishable from outside observation. The protocol incentivizes users holding shielded assets as they essentially provide liquidity to aid the matchmaking of user-submitted intents.

Typhon

Typhon serves as the system responsible for storage, ordering and execution of transactions within Anoma; it plays a key role in areas related to consensus, gossip, parallel execution, and mempools. In particular, Anoma's consensus mechanism is based on Heterogeneous Paxos, which is designed to support atomic cross-chain transactions across its fractal instances(8). Put simply, it allows Anoma to execute intents across multiple chains simultaneously. At the core of this are base chains, which are the fractal instances of Anoma, and chimera chains that facilitate atomic transactions between base chains(9). Consequently, multiple base chains can connect to a chimera chain to achieve seamless interoperability.

Atomic cross-chain transactions often necessitate multiple rounds of consensus across chains, resulting in higher latency. However, Anoma's promotes parallel execution for unrelated states, diminishing the need for multiple consensus rounds, thereby mitigating latency issues. This opens the door for capabilities like cross-chain flash loans, atomic swaps, and other advanced functionalities. Anoma also employs a Narwhal-based mempool to ensure efficient transaction ordering. Ultimately, Typhon aims to make on-chain transactions faster, simpler, and improve the capabilities of applications interfacing across multiple overlapping instances.

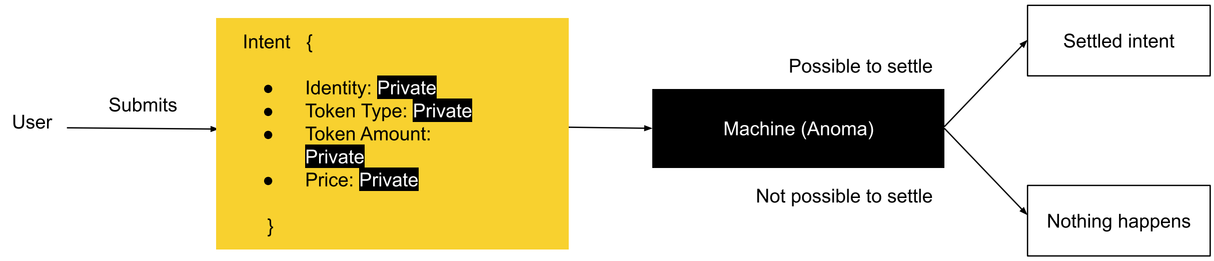
Taiga

Taiga, functioning as an execution environment, provides the tooling for privacy-preserving applications, fostering composable privacy(10). It ensures privacy through AA, allowing users to set their own privacy parameters. Intents can be categorized as public, shielded, or private. Given that solvers need to interpret intents to fulfill their roles, certain elements of an intent cannot be made wholly private. Applications built on Taiga maintain their state in the form of notes attributed to the application, with logic encapsulated through validity predicates, similar to smart contracts. These validity predicates serve as a form of AA, establishing the authorization logic.

Ferveo

MEV arises from the transparency of transactions. If intents are made public prior to their execution, they become susceptible to MEV extraction. A key part of Anoma, Ferveo, employs Distributed Key Generation ("DKG") and Threshold Encryption, providing a solution for creating private mempools until the transaction order is confirmed(11). DKG generates a singular public key from distributed segments of a private key, termed as key shares. Upon submitting their intents, users have them signed with this public key, keeping them encrypted until they are ordered. Following the confirmation of the order, validators utilize threshold signatures to decrypt the transactions. This decryption mandates a two-thirds majority of validators, thereby offering cryptoeconomic guarantees of privacy.

Figure 9: Anoma employs DKG and Threshold Encryption to maintain the encryption of user intents until the transaction order is confirmed



Source: Anoma Documentations, Binance Research

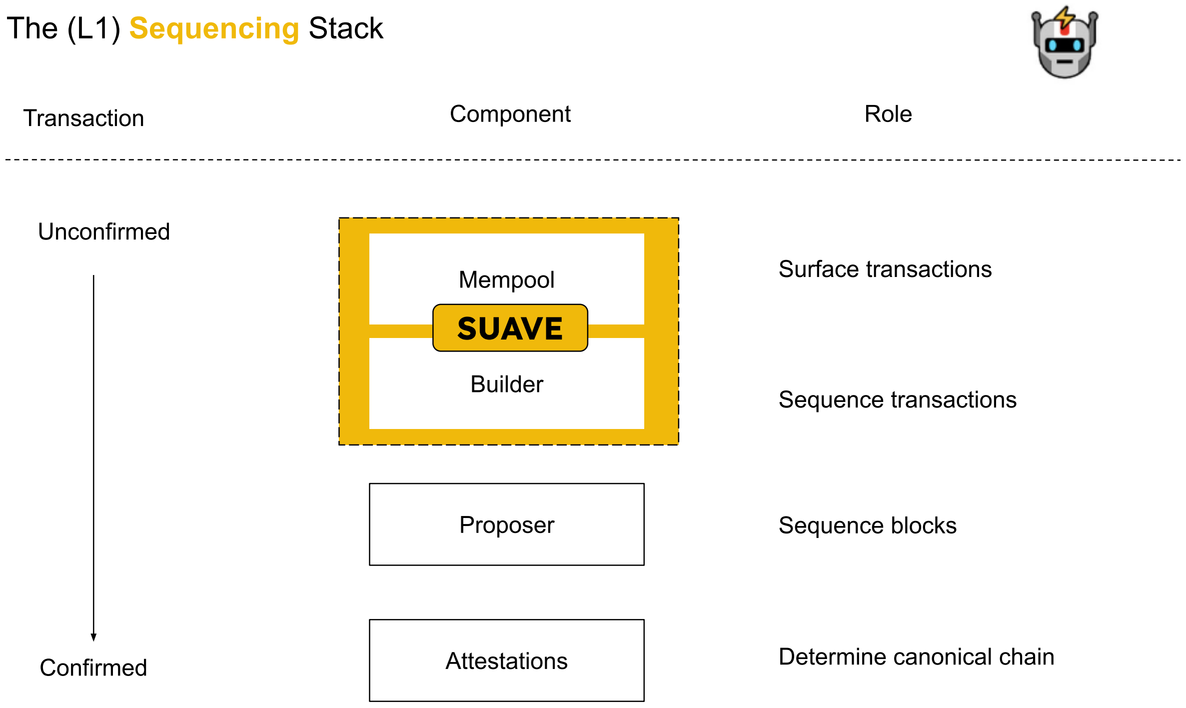
Ultimately, Anoma's introduction of intent-based architecture is exciting as it places user-centric design at the protocol's core, laying a strong foundation for other protocols to build upon. While the real-world implications for intents are still unfolding, it is anticipated that Anoma will play a key role in their adoption moving forward.

SUAVE

Flashbots' SUAVE, an acronym for Single Unifying Auction for Value Expression, strives to give more value for users whilst increasing decentralization in public blockchains[12]. Operating chain-agnostically, it acts as a standalone intermediary layer to facilitate intents. **SUAVE introduces MEVM**, a variant of Solidity, endowed with new precompiles for MEV use cases[13]. This adaptation enables developers to build MEV applications as smart contracts within an expressive, familiar and flexible programming environment, similar to the regular EVM.

By separating the roles of the mempool and block builder from existing blockchain structures, SUAVE introduces a **highly specialized, decentralized, plug-and-play alternative**. Its architectural framework is built around three primary elements: a memory pool where users express their preferences, an execution network where solvers compete to fulfill these preferences, and a block-building environment where solvers produce blocks, which can subsequently be accepted by other networks.

Figure 10: SUAVE separates the roles of the mempool and block builder from existing chains, offering a highly specialized plug-and-play alternative



Source: writings.flashbots.net, Binance Research

Sharing a common sequencing layer, SUAVE promotes decentralization, enables block builders to harness cross-domain MEV, allows validators to optimize their revenue, and ensures users enjoy superior transaction execution. This setup also assists to alleviate the centralizing effects of MEV. At its core, SUAVE revolves around preferences - messages signed by users to express their intents, facilitating both simple transfers and complex sequences across multiple blockchains. Overall, solvers compete to provide the best execution, capturing MEV and offering decentralized order flow value in the process. In essence, **SUAVE aims to become the universal mempool and block builder** for all blockchains.

Essential

Essential is focused on building a comprehensive suite of intent architecture solutions, encompassing three primary objectives: devising a domain-specific language ("DSL") for expressing intents, **establishing an Ethereum standard for intent-centric AA**, and developing a modular intent layer[14].

- **DSL:** For expressing intents, Essential utilizes a specialized DSL crafted in Rust. The DSL paves the way for standardized intent expression and solver-optimized resolution, thereby improving composability and fostering the growth of intent-based applications.

- **Intent-centric AA standard:** The intent-centric AA standard enables solvers to formulate valid transactions based on user intents.

- **Modular intent layer:** The modular intent layer lays the foundation for an intent-exclusive architecture, consolidated order flow, MEV resistance, and the potential for cross-chain intent execution. In short, this is Essential's protocol dedicated to handling intents.

In Essential's architecture, intents are not directly implemented. Instead, they are resolved, which then generates an execution trace of the resolved intent for on-chain execution. Unlike other solutions, Essential opts not to employ cryptographic execution for intent privacy; the underlying intent is recorded on-chain prior to decryption and execution. Moreover, Essential's consensus mechanism encourages solvers to compete on objective satisfaction, thereby competitively encouraging high satisfaction among end users.

Overall, a unified standard reduces the fragmentation problems caused by different intent types. It makes it easier for solvers to work with intent-enabled applications and for developers to adopt intent systems, while also preventing the need to build similar infrastructure several times.

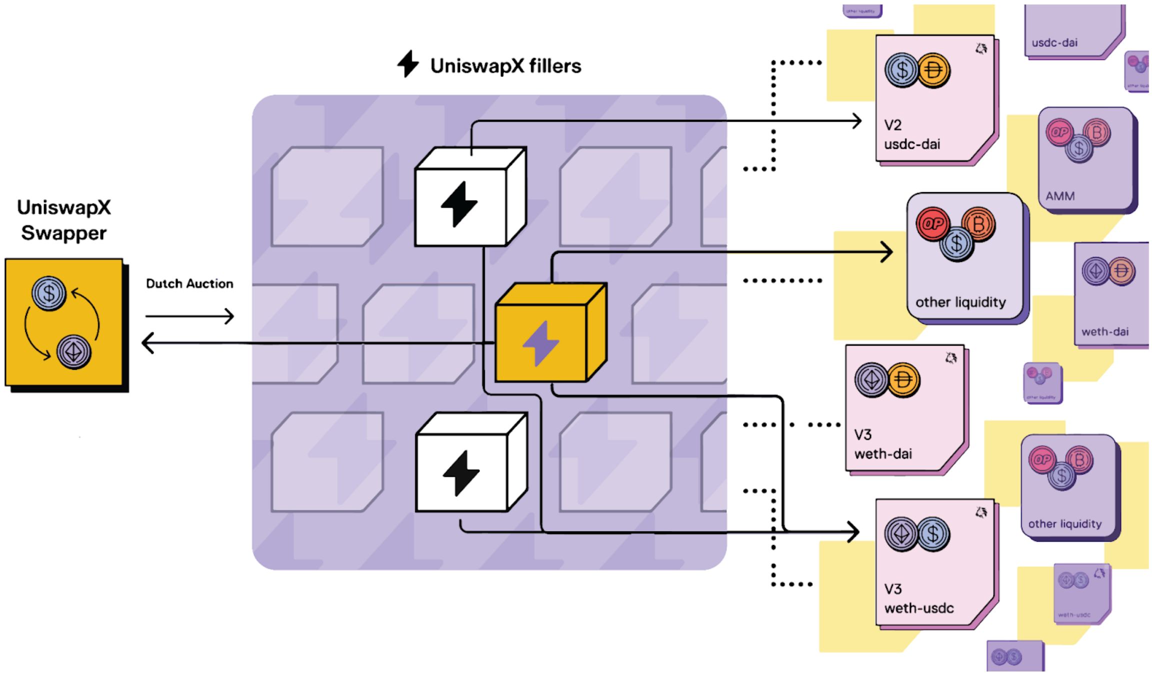
Intent-Specific

UniswapX

Uniswap's introduction of UniswapX this past July signaled a notable industry shift towards intent-specific applications[(15)]. Given that **UniswapX incorporates intents into one of DeFi's most prominent DEX, it stands as a resounding endorsement of the intent-centric thesis**. The platform operates as anticipated: users express their intents, which are then processed off-chain by specialized fillers - be they solvers, market makers, or searchers - before being settled on-chain. This approach diverges from Uniswap's Automated Market Maker ("AMM") model, where users interact directly with on-chain AMM pools. With UniswapX, users bypass AMMs altogether, directing their trades to fillers who employ both on-chain and off-chain strategies to compete in finalizing the transaction.

UniswapX employs Dutch auctions to process intents, starting at a high price that incrementally drops until a participant deems it profitable and fills an order. This structure, in a competitive marketplace, aids in reducing slippage, creating a more favorable setting for order flow auctions. Participants have diverse avenues to execute swaps: through Uniswap, Balancer, or Curve pools, aggregators, or even leveraging their own inventory while hedging on centralized platforms. **Remarkably, a user can interface with Uniswap's front-end and have their transaction processed using entirely off-chain liquidity sourced from centralized exchanges ("CEXes")**. This aspect, to some degree, positions Uniswap as a gateway to CEX liquidity.

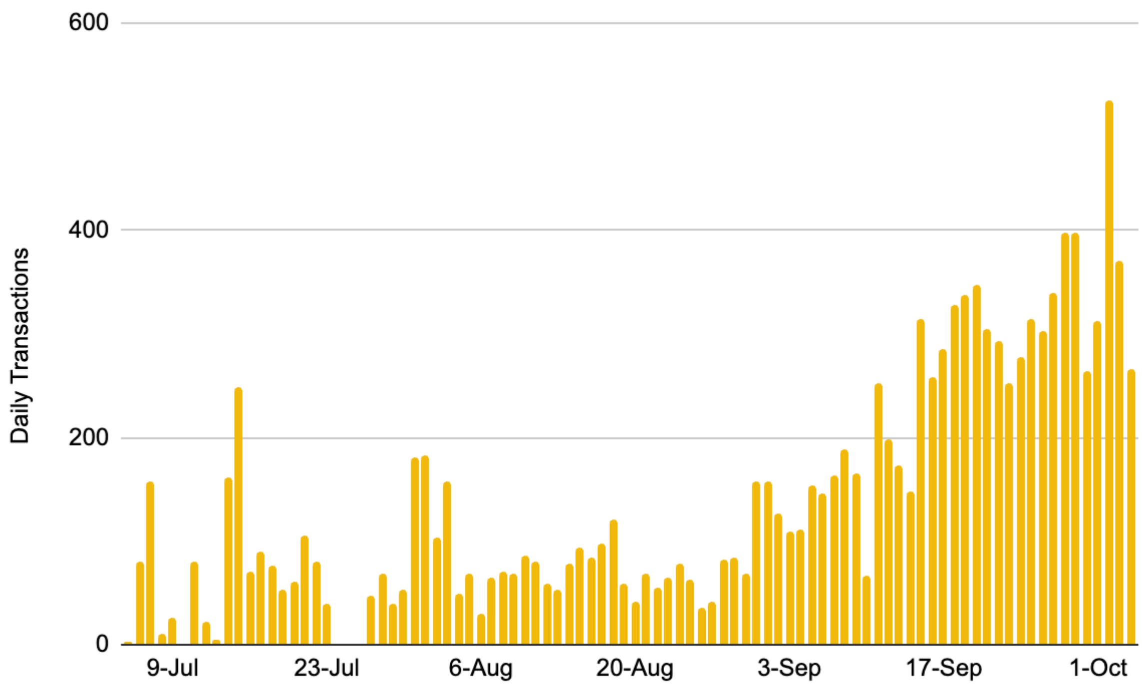
Figure 11: Swappers generate signed orders, specifying the intents of their swap, and fillers employ competitive strategies to satisfy these orders



Source: Uniswap Blog, Binance Research

Beyond standard UX improvements, **UniswapX brings forth additional cross-chain benefits**. Users will no longer have to navigate the multi-step operations required to swap assets between chains. Moreover, in many traditional cross-chain bridge designs, funds reside in the bridge contract, which is often highly susceptible to hacker breaches. Yet, with the advent of UniswapX, the only funds at risk are the 'swaps in transit' or active exchanges. By limiting exposure solely to the transit period of the exchange, it markedly reduces the amount of funds at risk in the event of an attack. Given that September was recently identified as 2023's most significant month for crypto exploits[16], this advancement is certainly welcomed. Ultimately, this development represents a significant leap in the cross-chain domain.

Figure 12: The daily number of transactions on UniswapX has been trending upward



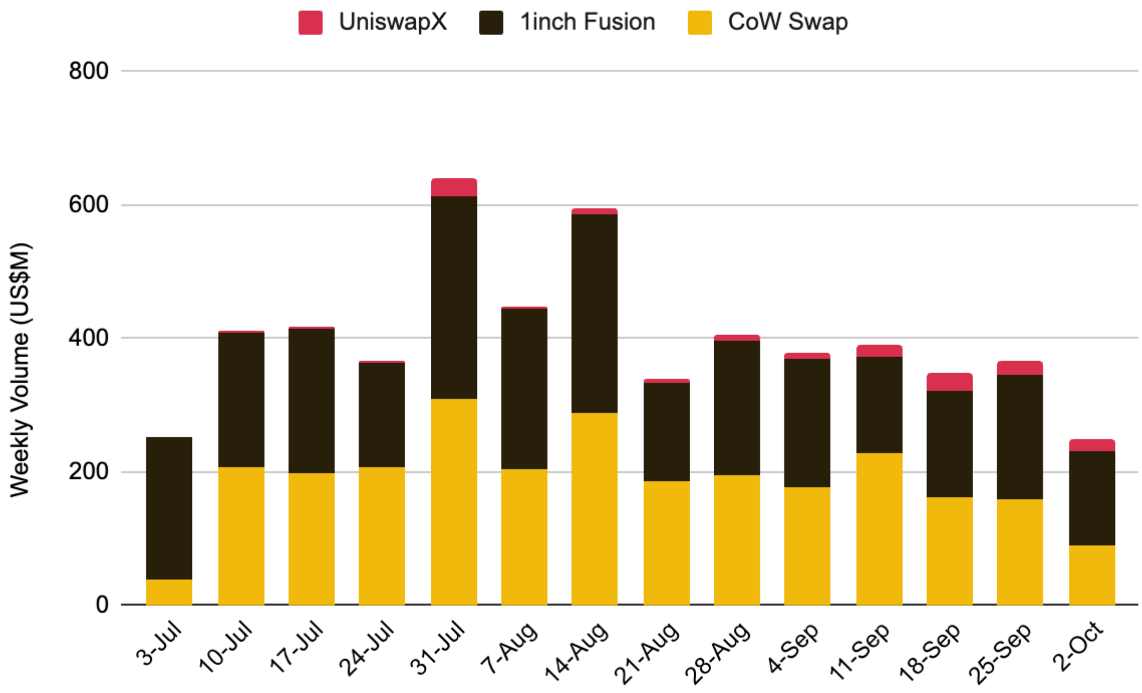
Source: Dune Analytics (@cryptokoryo), Binance Research, as of 5 October, 2023

Following the introduction of Uniswap V4's **hooks**[(17)] - a feature allowing developers to effortlessly integrate their capabilities with existing liquidity pools - the spotlight has turned toward improving on-chain trading experiences. Specifically, through UniswapX, Uniswap is optimizing cross-chain interconnectivity, and streamlining both efficiency and UX. Ultimately, improving on-chain trading experience is pivotal in bridging the gap between DEX and CEX trading volumes, and the role of intents may be key in achieving this parity.

CoW Swap

With over US$28B in cumulative trading volumes to date[(18)], **CoW Swap pioneered one of the early implementations of intent-specific trading dApps**, enabling peer-to-peer settlement orders powered by the CoW protocol[(19)]. Compared to its peers, this trading volume is certainly high; however it's probable that UniswapX hasn't fully tapped into its potential due to its recent launch.

Figure 13: While their trading volume has shown volatility, CoW Swap's weekly figures have typically surpassed US$200M



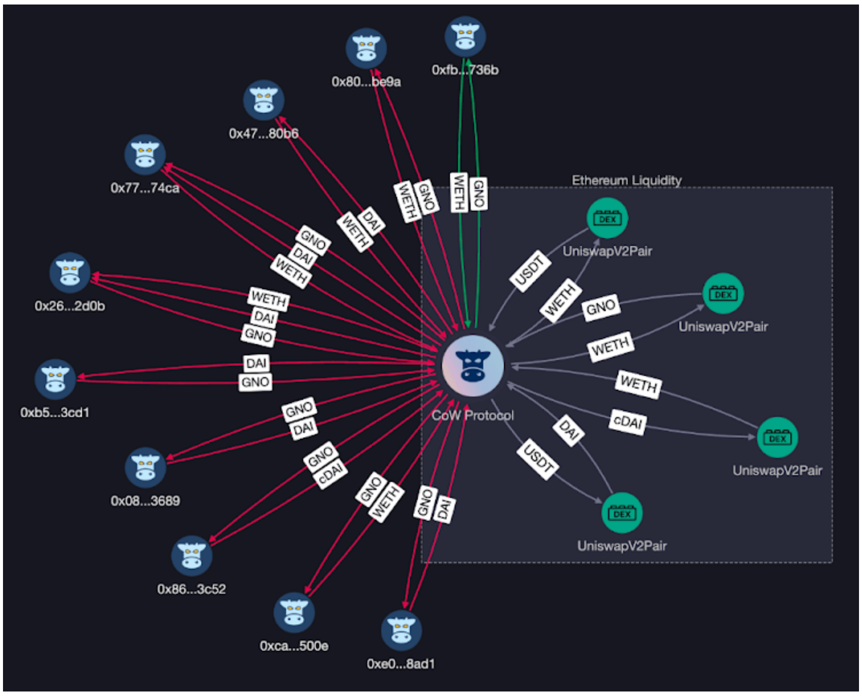
Source: Dune Analytics (@cowprotocol, @1inch), Binance Research, as of 5 October, 2023

The protocol utilizes batch auctions[20], where a competitive marketplace of solvers compete to secure the most optimal batch through their individual strategies. CoW Swap incentivizes solvers to match buy and sell orders, batching them together to execute at the best possible price. Solvers in CoW Swap face a clear-cut situation: they either have the best batch or they don't, with no middle ground for sharing. They can execute these orders against each other off-chain, taking advantage of CoWs. **CoWs are simply instances where two or more traders directly swap assets without the need for on-chain liquidity**, thereby removing the need for liquidity provider fees[21].

Solvers have flexibility in their strategy, drawing from various liquidity sources - be it on-chain liquidity pools, flash loans, or even private order flows, although the latter isn't ideal. If more liquidity is needed, the remaining portion of a trade can be processed by finding the most efficient route via on-chain liquidity pools. Instead of having liquidity providers on the platform, **CoW Swap integrates with existing on-chain liquidity, and can further tap into liquidity from other AMMs where required**. At present, CoW Swap is capable of settling orders on platforms like Uniswap, Sushiswap, 1inch, and Paraswap, and executes user transactions through signed messages.

CoW Swap also facilitates multidimensional swaps involving three or more asset trades. In other words, CoWs can be found in a minimum of three different tokens. Although these trades don't offset each other directly, the idea is that liquidity is shared across several trades, and when executed collectively, they achieve an overall balance. This alleviates concerns around fragmented liquidity. The protocol is able to match several token pairs in the same batch and avoid having to interact with multiple AMM pools, saving on gas and settling at a uniform price. Ultimately, the standout feature of CoW Swap is the protocol's idea behind CoWs.

Figure 14: Several matching intents reduces the need for on-chain AMMs, as demonstrated by this CoW where 12 swaps effectively shared liquidity

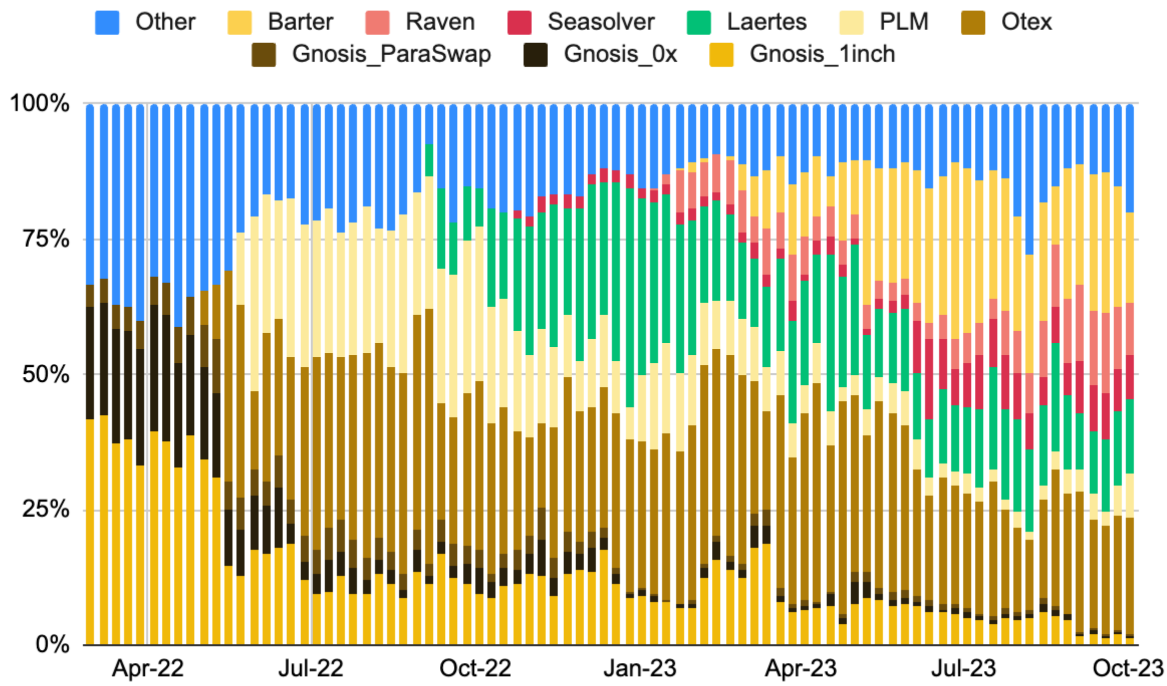


Source: CoW Protocol Documentations

While CoWs demonstrate the advantages of using intents, CoW Swap faces challenges given that it operates in an ecosystem that is not inherently designed for intents. In particular, Ethereum doesn't fully cater to the intent structure, pushing CoW Swap to establish and maintain its separate off-chain framework. Its scope is further confined, as it taps into the intents of only its direct users. As a result, the limited access to broader intent mempools has curtailed the frequency of CoWs on CoW Swap.

Nevertheless, CoW Swap's progress with intents is evident. In its early days, CoW Swap mainly saw batches won by DEX aggregators such as 1inch, facilitated by CoW Swap's integrated 1inch API. **Over time, as specialized solvers like Barter, Otex and Laertes came on board, the role of 1inch and other aggregators began to lessen**. This shift highlights solvers' increasing efficiency in maximizing value and optimizing batched orders. Additionally, CoW Swap has recently introduced **CoW Hooks**[22], enabling users to perform custom-coded DeFi actions like trading, bridging, staking, depositing, and more. **This addition enhances composability, which is fundamental to the effectiveness of intents,** further abstracting complexities for users.

Figure 15: Solvers are rising in prominence on CoW Swap, with DEX Aggregators seeing a diminishing market share



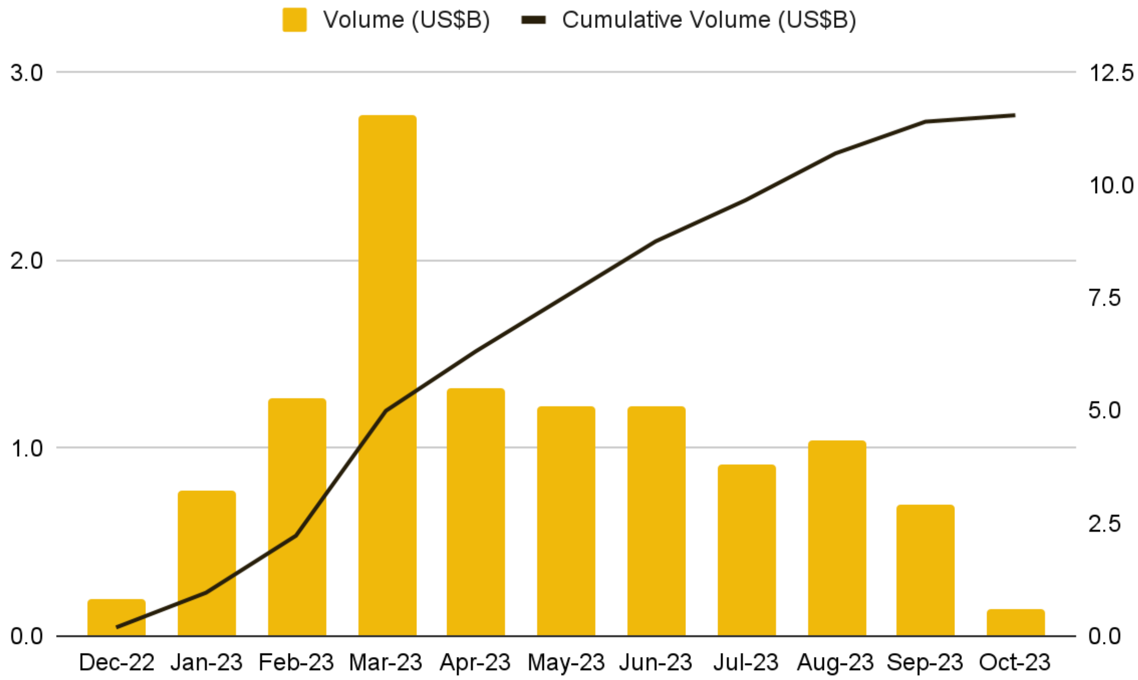
Source: Dune Analytics (@cowprotocol), Binance Research, as of 4 October, 2023

1inch Fusion

1inch's response to the emergence of intents was the introduction of 1inch Fusion, in many ways paralleling CoW Swap's off-chain order matching approach[23]. **While CoW Swap employs batch auctions, 1inch Fusion distinguishes itself by using Dutch auctions**; though, its operational mechanics bear resemblance to that of UniswapX[24]. Within Fusion's ecosystem, users, acting as makers, submit off-chain orders, or intents. These are then available to solvers who engage in the Dutch auction process. 1inch assists users by auto-generating intents based on their DEX aggregator's pricing, though users maintain the flexibility to customize or choose different order parameters. Notably, like CoW Swap, direct matching between intents can bypass the need of utilizing traditional liquidity pools.

Since its December 2022 launch, **Fusion has experienced no shortage of volume, benefiting greatly from its foundation on the 1inch protocol and its substantial user base**. The parallels between 1inch Fusion and CoW Swap have led to shared solver networks between them, which is a natural and economically beneficial overlap for the ecosystem. As the focus on intent-centric solutions grows, solvers are expected to compete expansively across various protocols and networks.

Figure 16: Since its inception, Fusion has maintained steady monthly transaction volumes, now contributing on average over US$1B to 1inch



Source: Dune Analytics (@1inch), Binance Research, as of 4 October, 2023

5 Outlook

Opportunities and Risks

Predominantly, poor UX has been a deterrent in the broader adoption of decentralized products, often tilting the scale in favor of centralized solutions among users. However, with the right execution, the concept of intents harbors the potential to pivot this trend towards a more user-friendly decentralized landscape. In this on-going debate, innovations like SUAVE and Anoma are driving a paradigm shift. **They ensure that in the domain of swaps, staking, and other DeFi activities, the user's intent is not merely recognized but also realized to its fullest value**. By focusing on outcomes rather than processes, **intents possess several opportunities**, some of which we have outlined below.

- **Enhanced UX:** By streamlining the UX, intents eliminate the necessity for users to navigate through complex transaction parameters. Instead of maneuvering across fragmented Web3 infrastructure, users are only required to express their desires, leaving the rest for solvers to handle. This user-centric approach paves the way for increased adoption.

- **Mitigated MEV exposure:** By abstracting away specific transaction details, intents diminish the likelihood of front-running and other MEV extraction strategies, thereby promoting a more equitable environment to transact in.
- **Increased competitiveness:** The competition among solvers incentivizes them to provide the most favorable execution prices, enabling users to optimize their returns and minimize slippage.
- **Higher composability:** Composability refers to the ease at which various protocols or dApps can integrate and build upon one another. User intents create a new avenue for systems to be tailored for enhanced compatibility. For instance, solvers can be utilized to expand functionality and emulate atomicity across chains by executing intents.
- **Gas efficiency:** Instead of multiple individual transactions, intents can be batched into a single transaction, reducing gas fees and making transactions more cost-effective.
- **Improved privacy and security:** In an intent-centric model, users only need to express their end goal, sidestepping the need to outline each intermediate step. This reliance on fewer steps typically makes transactions safer and mitigates exposure to users' strategies or preferences.

While intents bring forth substantial advantages, there are challenges that persist. Concerns surrounding centralization, privacy, and robustness against MEV strategies must be adequately addressed. A longstanding consideration is **finding the appropriate balance between efficiency, decentralization, and privacy**. Similar to how other network participants in sequencers and searchers have leaned towards efficiency, the involvement of off-chain actors in intent-centric systems may introduce a potential centralizing effect.

Yet, this off-chain approach offers a silver lining, particularly in the form of computational efficiency compared to standard transactions. Such a trade-off might be favorable in the short term, provided that it doesn’t impact the decentralization of validation and there's a strategy to alleviate major centralization risks going forward. The following are **some key points for consideration**.

- **Striking a balance between solver efficiency and user privacy:** The more information that solvers possess, the more effectively they can fulfill an intent. However, sharing more information comes at the expense of user privacy, paving the way for issues related to MEV. Striking the right balance with privacy features to support intents will be crucial.

- **Centralization risks:** The emergence of a few dominant players skilled in processing complex user intents may lead to centralization. Just as we've observed with private mempools and order flows, these entities may attract a larger share of intent orders due to their underlying efficiencies. Such centralization might not always align with the users' best interests.

- **Technical barriers:** Establishing an intent-centric model can be a relatively complex task. It demands a thorough understanding of user desires, along with the capability to navigate the extensive blockchain landscape and employ advanced algorithms to efficiently execute intents.

Adjacent Considerations

Ensuring adequate solver incentives

Intent-centric platforms face hurdles in efficiently engaging solvers to address user demands. In the short term, low volumes may deter optimal incentive structures, potentially hindering solver efficiency. However, as the space gains traction, increased competition is expected to naturally realign solver incentives to where they should be.

In all intent-based systems, **solvers require incentives to cover their operational costs** and secure a profit - they are typically profit-driven entities inclined toward short-term strategies. To earn these incentives, solvers compete with other solvers as well as with generalized MEV bots. Solvers are essentially part of the MEV ecosystem, as they strive to extract maximum value from every intent they execute. **Optimal solver incentive designs align solver incentives with ideal user outcomes**, ensuring that increased MEV for solvers translates to faster and improved execution for users. For instance, solver fees might be determined based on the tokens involved in the intent the user aims to execute. Permitting solvers to stake a claim on a portion of the fees and pass on their partial solutions to others within a shared framework is also beneficial. Therefore, incorporating solver incentives is a crucial aspect of intent-centric architectures.

To further foster a synergy of incentives between users and solvers, reputation-based systems could be instituted. Such systems would nurture trust with users through consistent engagement and the establishment of accountability. Given that users delegate search tasks to solvers, the latter are held accountable and, over time, build a reputation for reliability. Users, in turn, can delegate the enforcement of rules to the chain, proposers, or validators, thus ensuring a structured, trustworthy framework within which solvers operate.

Potential interplays with AI

The potential integration of advanced AI could positively impact the intent-centric approach. **Intent-centric setups involve various technicalities, and AI has the potential**

to help obscure these complexities. Whether it's through interpreting natural language inputs of intent, breaking down goals, or strategizing the optimal route to execute transactions, AI stands as a powerful tool. On the other side, in scenarios where user intent is complex or inaccurately expressed, solvers may struggle to comprehend and devise optimal solutions. **By analyzing the user's transaction request and data, AI can assist in bridging this gap**.

However, incorporating AI into the process from intent to execution is likely to involve multiple parties, bringing about security challenges. Providers of intent-centric protocols must establish deterrents and penalties for malicious behavior to maintain a secure third-party execution layer. Additionally, enhancing technical security to prevent vulnerabilities will be crucial to safeguarding user rights. **The combination of AI with intent-centric protocols is certainly promising but remains an open research area**.

6 Closing Thoughts

As Web3 technology advances towards mass adoption, it becomes imperative to empower users to navigate the complexities of the ecosystem on their own. Against this backdrop, intent-centric architectures emerge as a promising solution, signifying a progressive shift in Web3 interactions. While still in the exploratory phase, intents hold the potential to enhance Web3 UX and facilitate the onboarding of the next wave of users.

At the core, intents aim to abstract as much as possible from the user, all while preserving decentralization, and improving transactional efficiency and expressiveness. Central to this is enhancing the interoperable UX to a point where bridging complexities between different blockchain ecosystems become something of the past for users. By shifting from an imperative to a declarative paradigm, users are empowered to state their intentions while leaving the complexities of execution to solvers. Solver networks, alongside interplays with mechanisms like AA and bridging, will play pivotal roles in realizing the practical applications of intents.

Several intent-specific applications are already in existence, with the trend poised to persist. As the blockchain ecosystem continues to mature, the widespread adoption of intents holds the potential to reshape how users engage with dApps going forward.

References

1. https://www.paradigm.xyz/2023/06/intents
2. https://www.statista.com/statistics/617136/digital-population-worldwide/
3. https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/
4. https://www.erc4337.io/
5. https://www.propellerheads.xyz/blog/intents-and-where-to-find-them
6. https://anoma.net/
7. https://docs.namada.net/
8. https://anoma.net/blog/heterogeneous-paxos-and-multi-chain-atomic-commits
9. https://anoma.net/blog/chimera-chains
10. https://www.youtube.com/watch?v=72VsJj_c99M
11. https://anoma.net/blog/ferveo-cryptography-overview
12. https://writings.flashbots.net/the-future-of-mev-is-suave/
13. https://writings.flashbots.net/mevm-suave-centauri-and-beyond
14. https://blog.essential.builders/introducing-essential/
15. https://docs.uniswap.org/contracts/uniswapx/overview
16. https://cointelegraph.com/news/crypto-exploits-top-for-crypto-exploits-in-2023-certi-k
17. https://blog.uniswap.org/uniswap-v4
18. https://dune.com/cowprotocol/cowswap
19. https://docs.cow.fi/overview/introduction
20. https://docs.cow.fi/overview/batch-auctions
21. https://docs.cow.fi/overview/coincidence-of-wants
22. https://docs.cow.fi/overview/cow-hooks
23. https://1inch.io/fusion/
24. https://docs.1inch.io/docs/fusion-swap/introduction

Latest Binance Research Reports

Monthly Market Insights: October 2023

A summary of the most important market developments, interesting charts and upcoming events

Oracle-Less: Challenging the Status Quo

An exploration of oracle-less protocols

The OP Stack: What's New?

A look at the growing OP Stack ecosystem

Navigating Crypto: Industry Map

An overview of different verticals in crypto

About Binance Research

Binance Research is the research arm of Binance, the world's leading cryptocurrency exchange. The team is committed to delivering objective, independent, and comprehensive analysis and aims to be the thought leader in the crypto space. Our analysts publish insightful thought pieces regularly on topics related but not limited to the crypto ecosystem, blockchain technologies, and the latest market themes.

Moulik Nagesh

Macro Researcher

Moulik is a Macro Researcher at Binance, having been involved in the cryptocurrency space since 2017. Prior to joining Binance, he had experience spanning cross-functional roles in Web3 and Silicon Valley-based tech companies. With a background in co-founding start-ups and a BSc in Economics from the London School of Economics & Political Science ("LSE"), Moulik brings a comprehensive perspective to the industry.

Resources

Read more **here**

Share your feedback **here**