Intent-based Architecture

Martinet Lee

Martinet Lee

Senior Research Engineer / Auditor

Head of Developer Relations

@ Quantstamp

Experience

Audited more than 50+ projects, from Defi, NFT, to Layer 1s including Yearn, ETH2, Avalanche.

Served as Audit PM and standardizing various processes that improves audit quality and communication with clients.

Quantstamp →

/Content

- Disclaimer
- Transactions
- What is an intent?
- Transaction v.s. Intent
- Who are working on intents?
- Generalized Intents
- Discussion

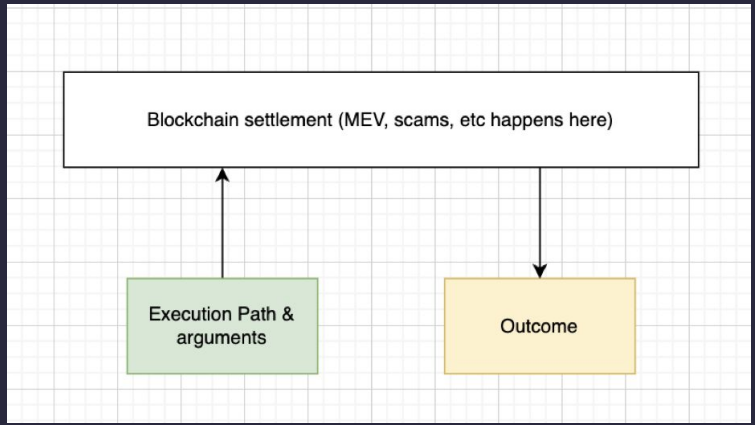
/ Disclaimer

- Intents is a very new field that made a little bit of sound - there’s no definitive answer yet. Lots of work are exploratory.
- Not an expert on intents
- This is essentially my study note and my take on intents

/ Transactions

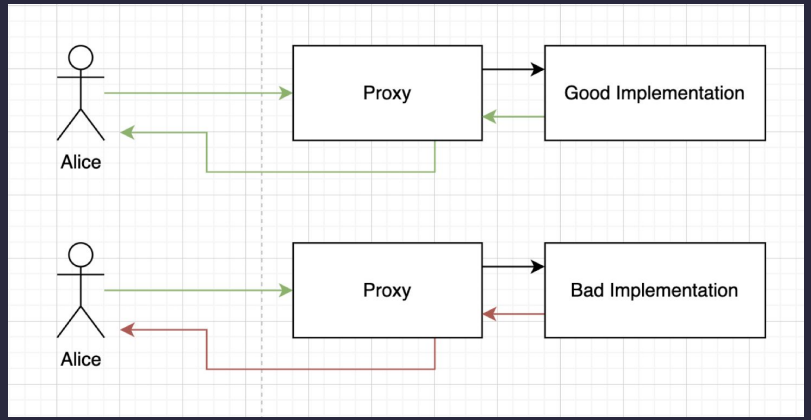
- “I am going to UniswapV2, 0×1234 USDC-WETH pool, provide 1900 USDC, with a slippage of 6%”
- Why not Sushiswap? Curve? The user has to think through this and decide for itself. What does it mean by slippage of 6%?
- The user has to know “HOW” exactly he/she wants to execute.

/ Transactions - User's UX Perspective



- TX will get executed, but not necessarily the expected outcome
- User has to specify the execution path and arguments

/ An example of unexpected outcome



- While Alice sends out the transaction, the proxy owner swaps out the underlying implementation.
- The smart contract takes the 1900 USDC but never returns the 1 ETH. Rugs Alice.

/ What is an intent?

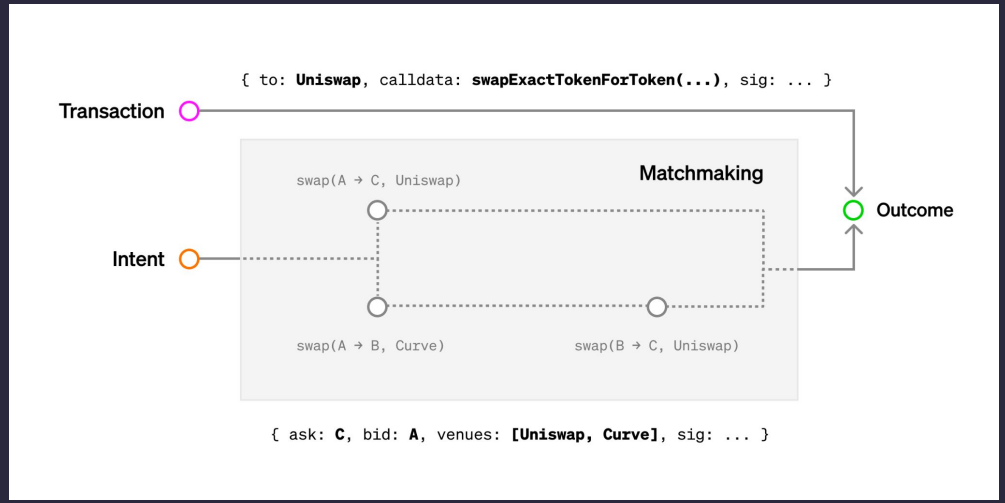
- “An intent is signed a set of declarative constraints which allow a user to outsource transaction creation to a third party without relinquishing full control to the transacting party.” – Quintus & Georgios, Paradigm

- “Intent specify desired outcomes/goals” – Uma Roy

/ Intent v.s. Transaction

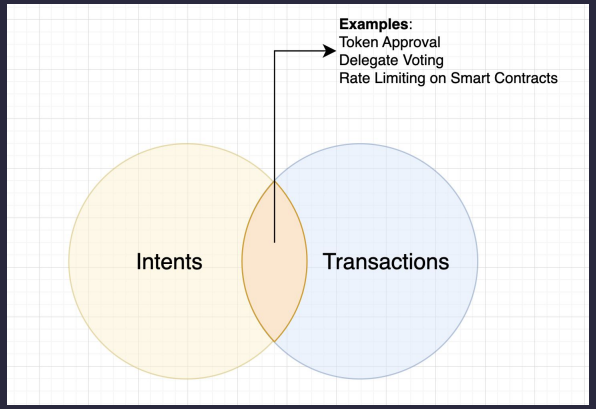
- Swaps
  - Transaction: Go to Uniswap Pool (0×1234), Swap 2000 USDC for at least 1 ETH.
  - Intent: I’m willing to give up to 2000 USDC for at least 1 ETH.
- Earning Yields
  - Transaction: Go to Compound ETH pool (0×abcd), deposit 1 ETH. (UI shows: 2% APY)
  - Intent: I’d like to lend out 1 ETH for 2% APY.

/ Intent - Paradigm's perspective



- Essentially, Paradigm is saying that Intent is one stage earlier than "transaction"
- There are other things being mentioned as intent too

/ Intent v.s. Transaction

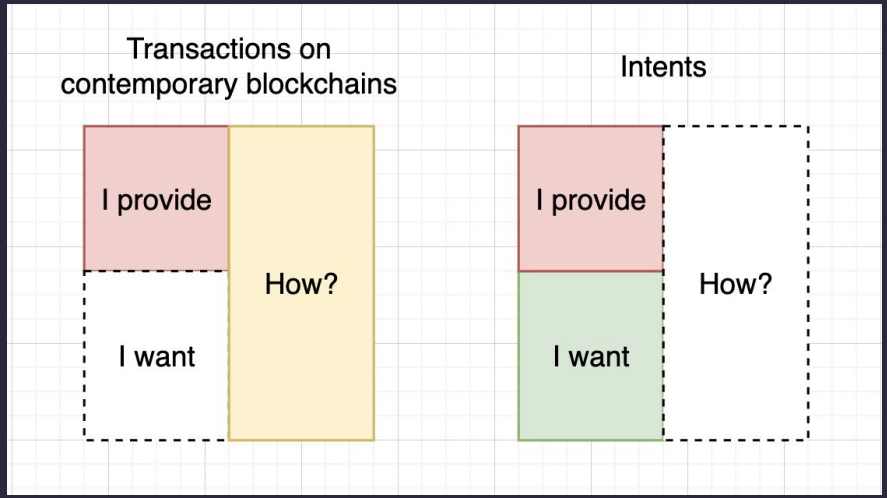


- Intents can be part of a transaction
- A transaction can also be purely intent
  - Mostly on smart contract wallet
  - Token contracts themselves can be viewed as a smart contract wallet

/ Intent v.s. Transaction

- Intent can be very specific too, and sometimes hard to distinguish from Transaction.
  - I only want to trade on Uniswap, Curve.
  - I only want to trade on this specific pool on Uniswap.
- Intent: focused on the result, may or may not be a transaction.

/ Intent - my view



- Intent is a design paradigm where applications, wallets, or even blockchains thinking about controlling the results.

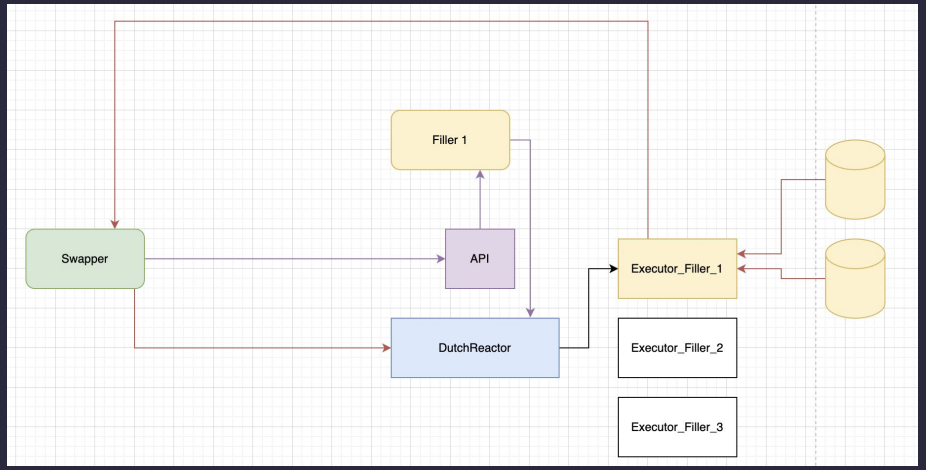
/ Who are working on intents?

- Intents are not new.
- Paradigm's view on the past intents:
  - Limit Orders: "100 X may be taken from my account if I receive at least 200 Y."
  - CowSwap-style Auctions
    - Same as limit orders but backend using a centralized service to improve efficiency
  - Gas Sponsorship
  - Delegation
  - Transaction Batching
  - Aggregators

/ Who were working on intents?

- In-app intents
  - Uniswap (Slippage)
  - DAO Voting (Delegate)
  - Token Approval
- Intent specific applications
  - Opensea Seaport
  - Cowswap / UniswapX
  - Matcha
  - Genie

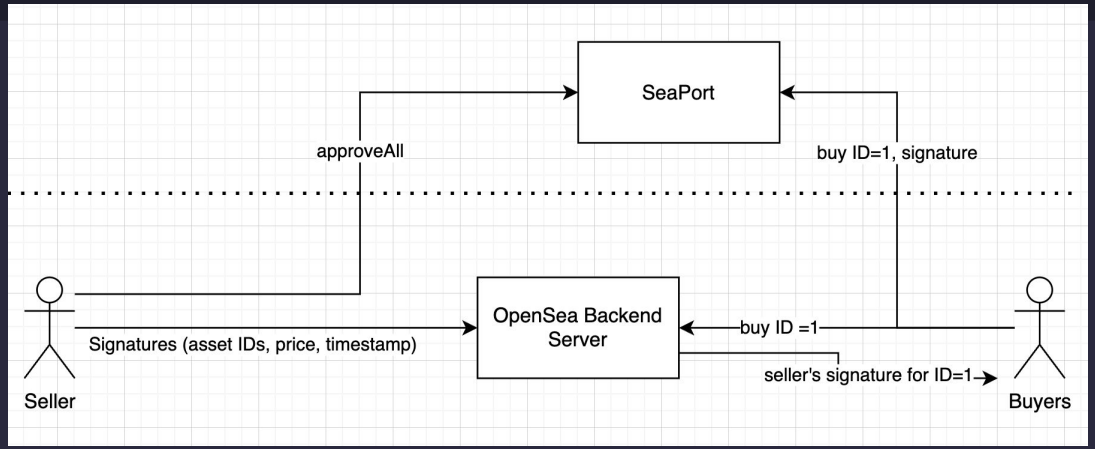
/ UniswapX



Setup: Swapper approves tokens to the Reactor

1. Swapper signs order, sends it to Uniswap centralized server
2. Filler gets order from Uniswap centralized server and matches order by sending a transaction
3. Condition set by the order is checked by the Reactor.

/ OpenSea Seaport



Setup:
Sellers send a transaction to approve all NFTs to Seaport contract.

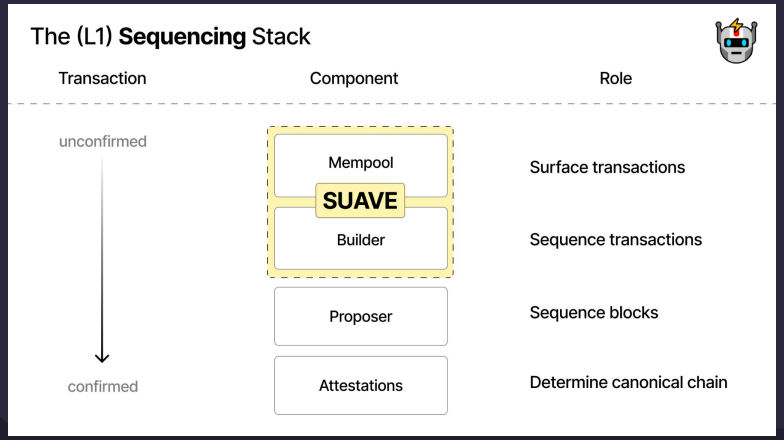
1. Seller sign an order, sends it to OpenSea centralized server
2. OpenSea displays the order on their UI, buyer sees and fetches seller’s signature from OpenSea centralized server.
3. Buyer sends out the transaction

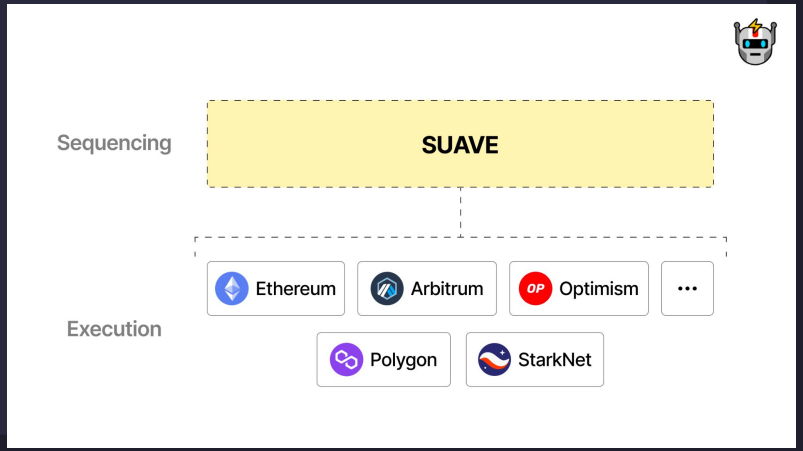
/ Who are working on general intents?

- Flashbot Suave
- Anoma
- ERC4337…(AA)?

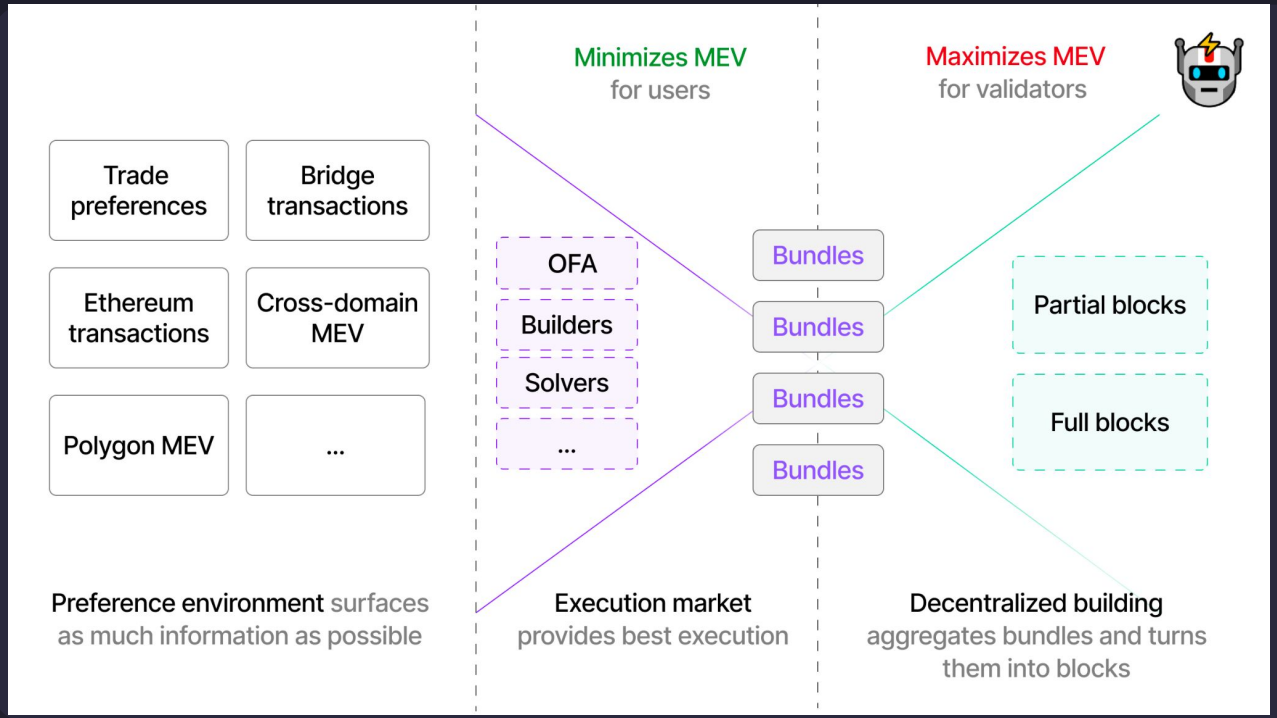
/ Flashbot Suave

- Details unclear yet
- Currently published contents are focused on “Cross-Domain” architecture rather than intent

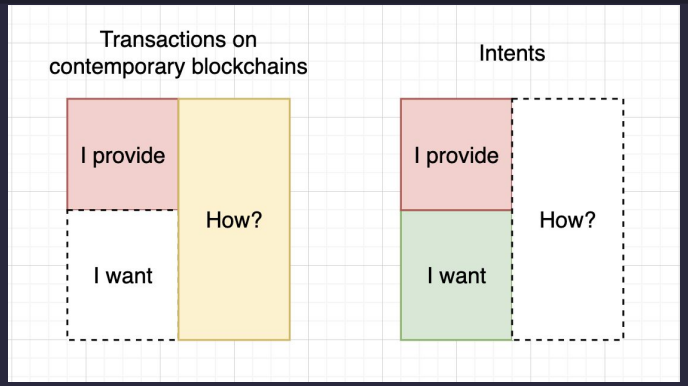




/ Flashbot Suave



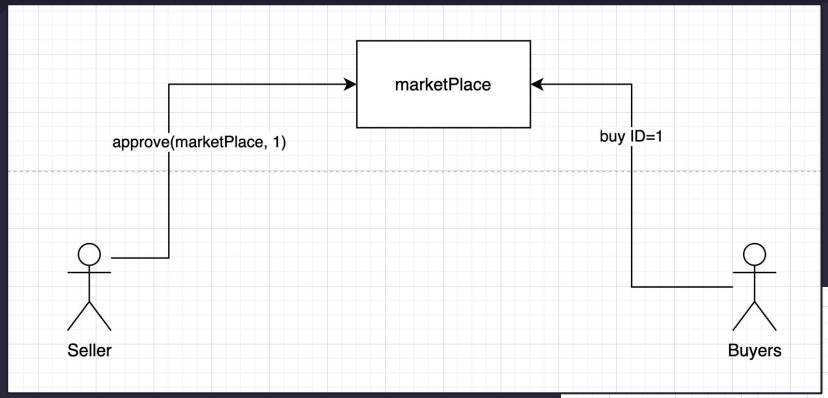
/ Anoma

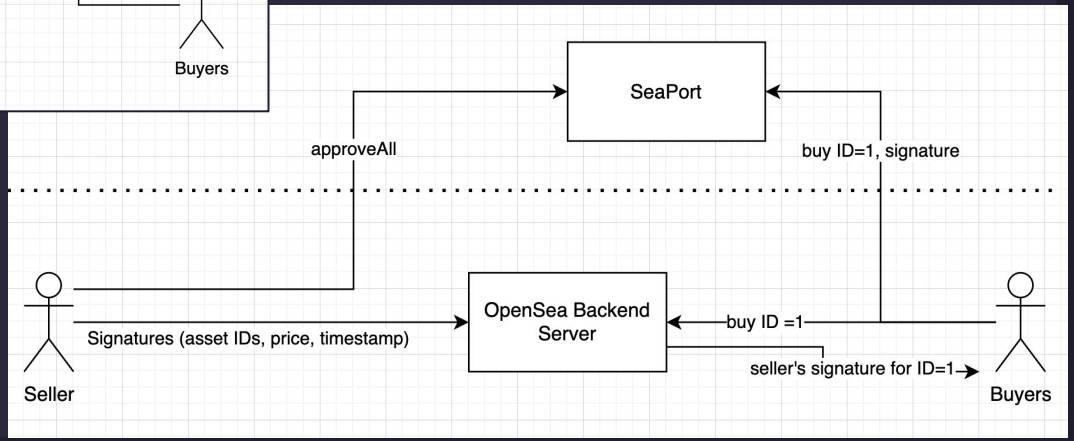


Why is there this Centralized party in lots of intent apps?

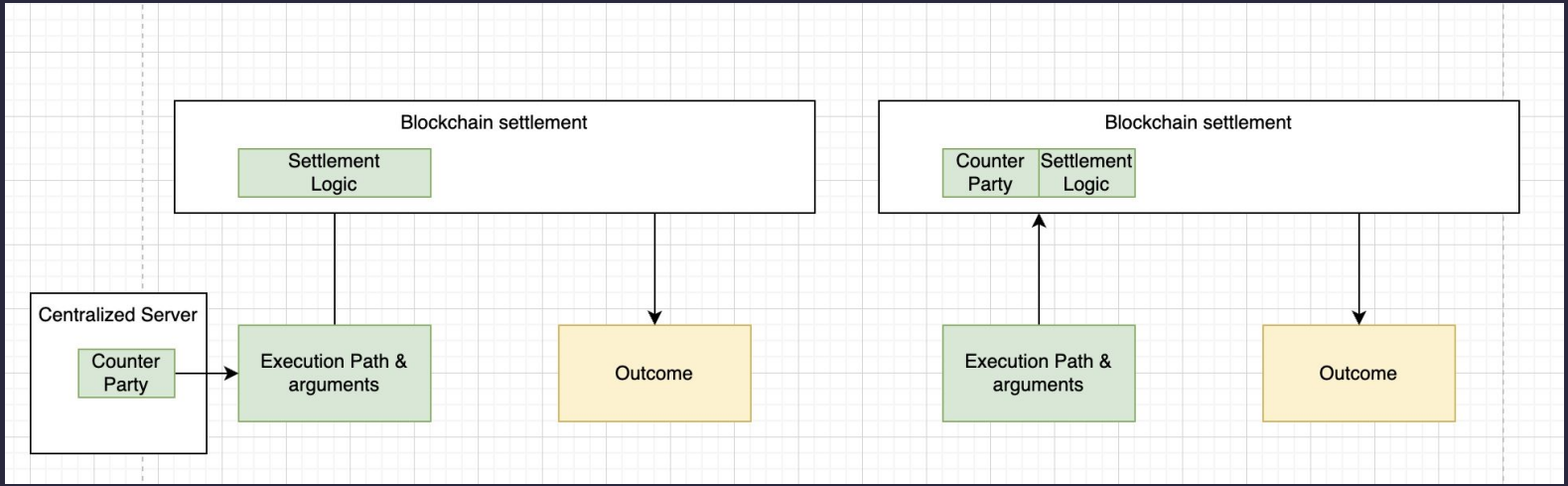
- One intent can be another intent's "How"
- For some applications, we need to know our "counterparty" to form a transaction ("Settlement" between parties)
- Posting intents on the blockchain is expensive (done before, not practical) - L2 alleviates this!

/ A review on NFT Market Places





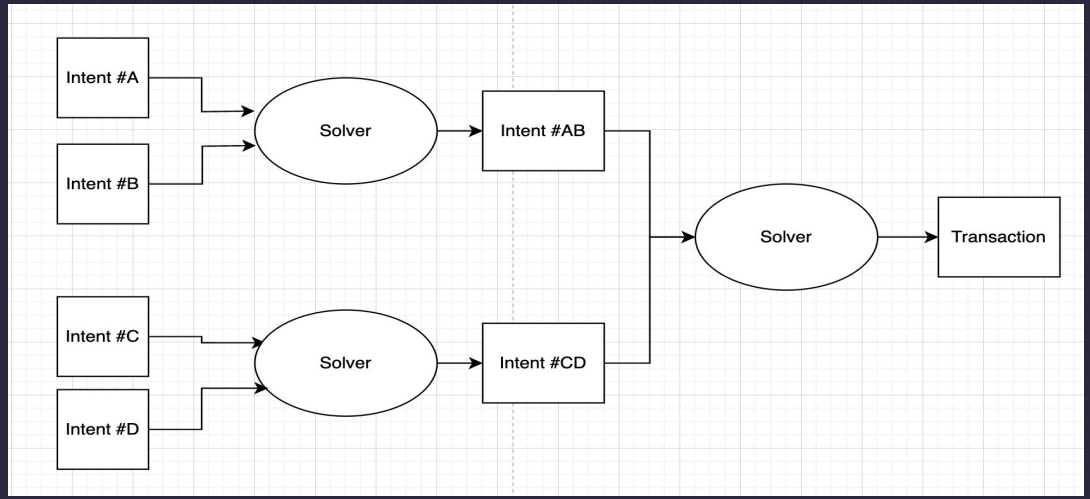
/ Counterparty discovery



- For lots of the apps that need counterparties, this is how they are done atm.

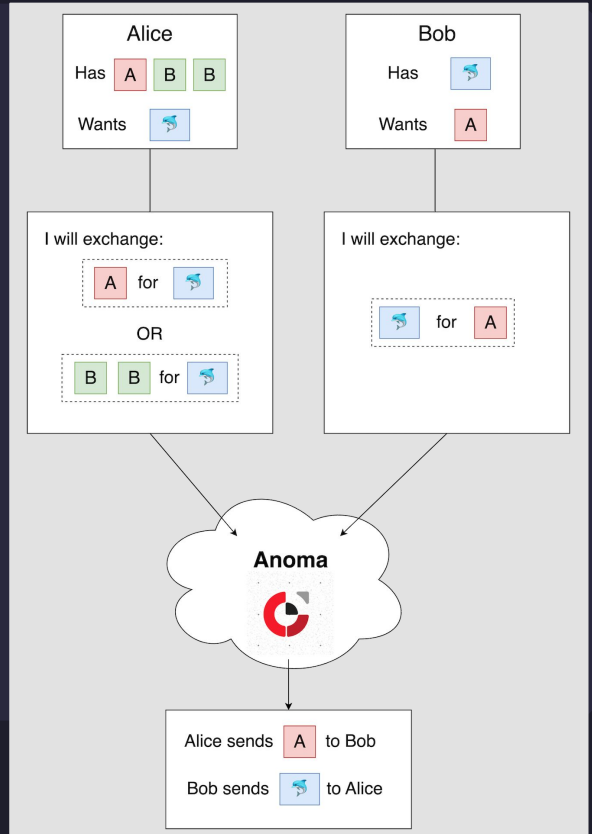
/ Anoma’s view - counterparty discovery

- Make counterparty discovery a decentralized game
- Allow parallel counterparty discovery: enabling partial intent solving

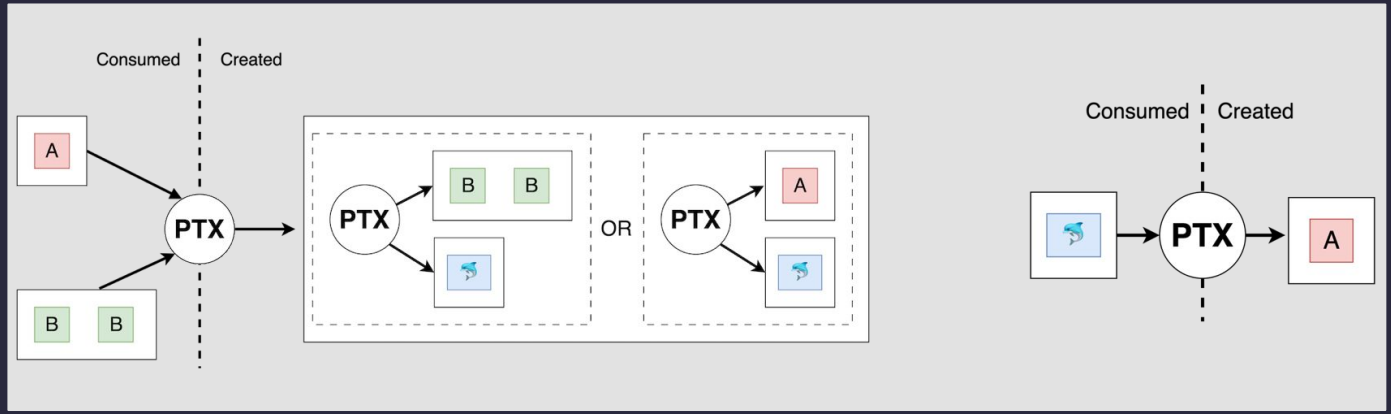


/ Anoma's approach to intents

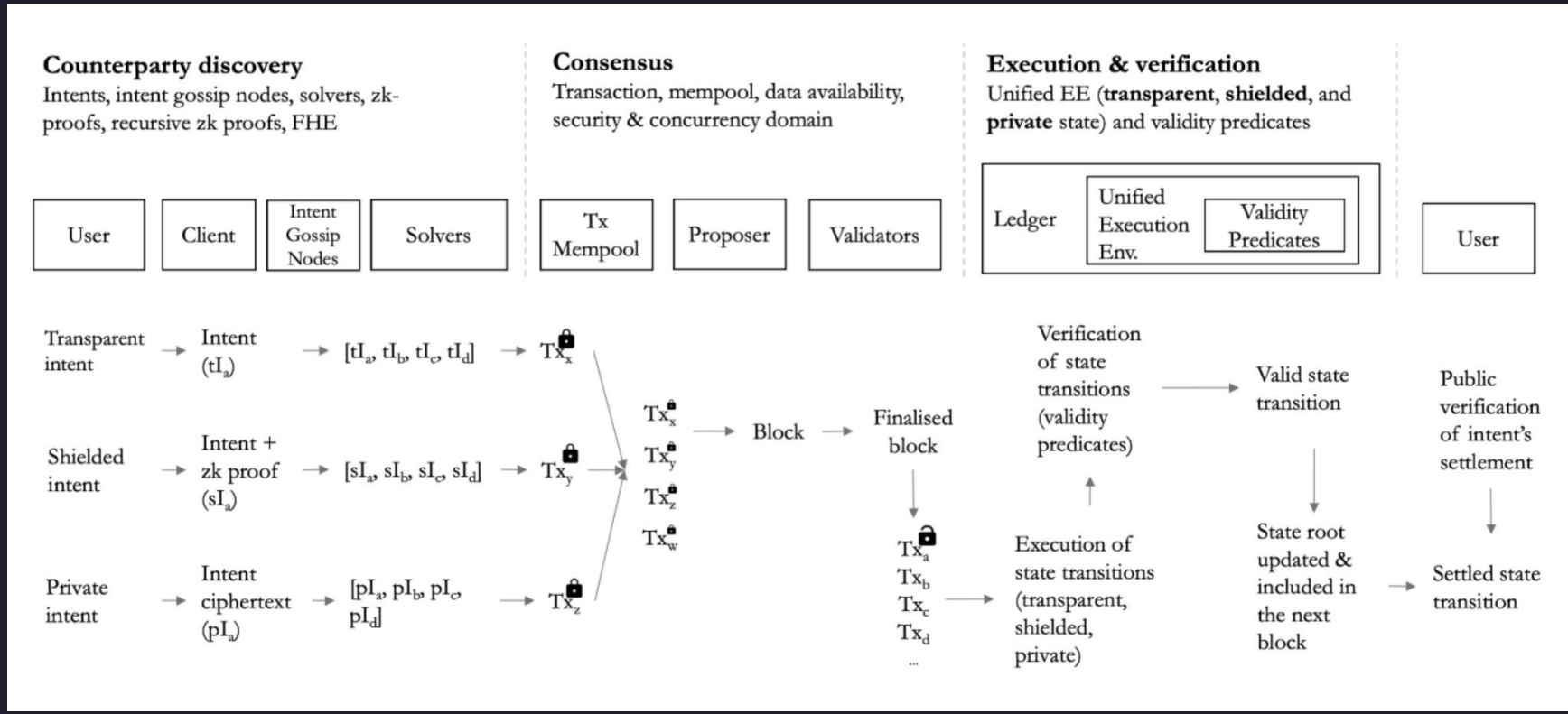
- Asset centric view
- Alice is willing to exchange either 2 B or 1 A for 1 Dolphin.
- Bob is willing to exchange 1 A for 1 Dolphin.



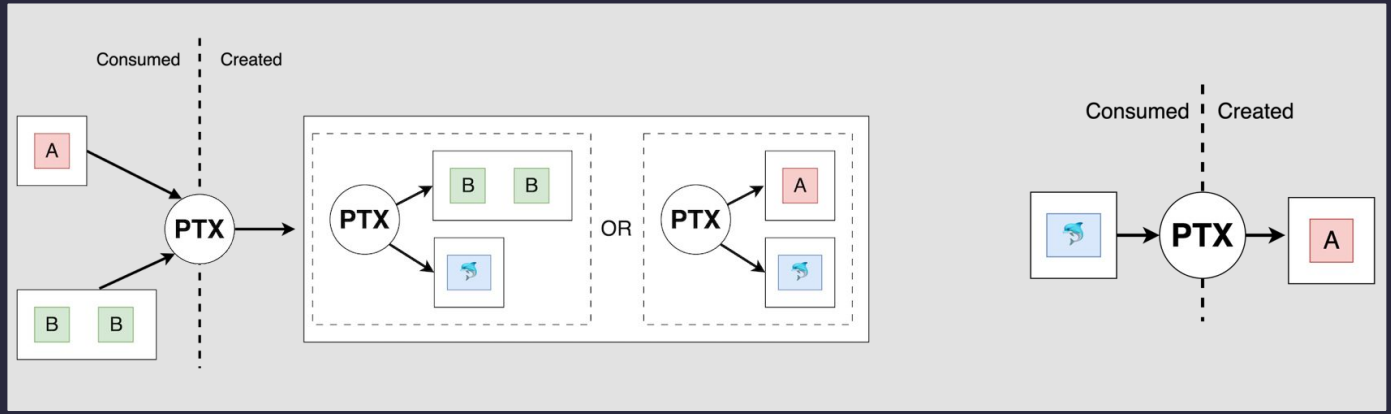
/ Anoma’s approach to intents



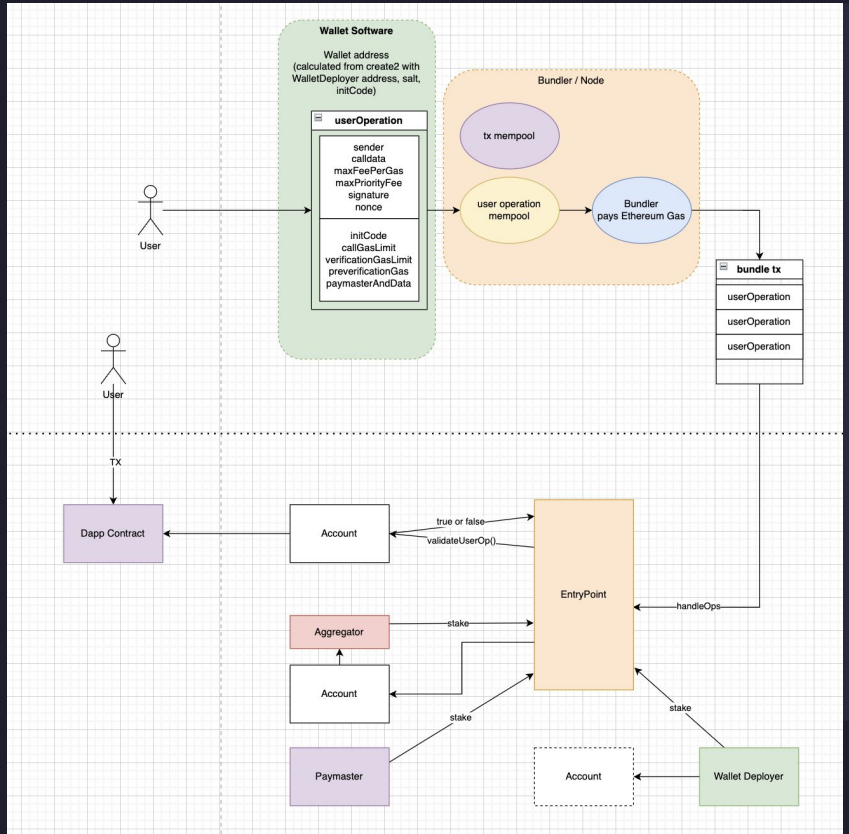
/ Anoma's approach to intents



/ Anoma’s approach to intents



/ What does EIP-4337 has to do with intents?



EIP-4337 encoded the commonly used intents into the smart contract wallet specification.

- Gas Payment
- Hooks for verifying
  - Can potentially add logic to do more general intents, e.g. access control

However:

- It's only on one chain (Cannot cross domain)

/ “Intent” needs an executor

- Someone needs to be aware of the intents and incentivized to execute the intent.
- Who is this person? Trusted or not trusted? Permissioned or Permissionless?
  - Limit Orders ⇒ The other matching party will send the tx
  - Gas Sponsorship ⇒ Relayer
  - Delegation ⇒ Delegate will vote (send tx)
  - Aggregators ⇒ the aggregators will send the tx
- How do we deal with this in a generalized intent?

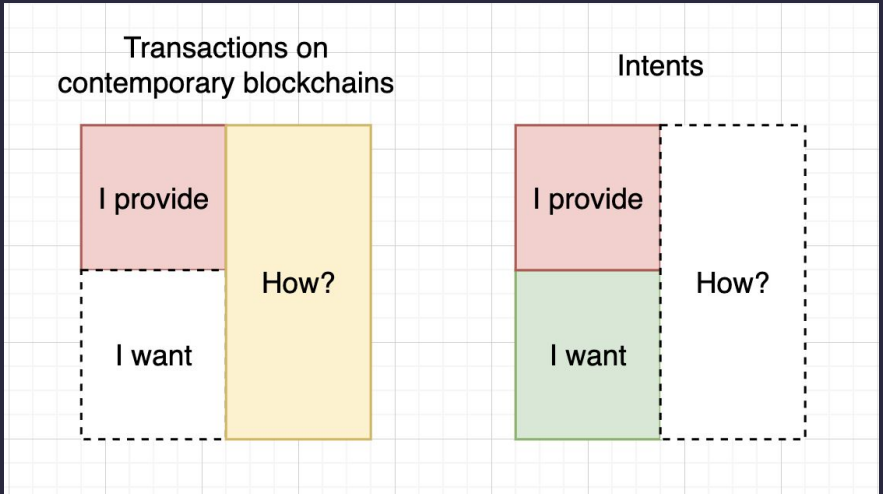
/ Permissionless Executors

- Executors should not be able to change user intents
- Executors are incentivized to execute intents
- Executors cannot be attacked by executing intents
  - Limit work for validating intents
  - Intents need to be limited in functionalities. e.g. cannot be non-deterministic.
  - Cannot easily and cheaply cancel intent

/ Intent Challenges & Risks

- Order flow monopoly
- Trust
- Opacity

/ Intent - my view (reiterate)



- Intent is a design paradigm where applications, wallets, or even blockchains thinking about controlling the results.

/ Intent - my view (cont.)

- Anoma’s view is pretty great except that it does not capture “long-term” intents, e.g.
  - Delegate
  - Infinite Approve
  - Access Control
  - Rate-limiting on smart contract wallets
- Let’s discuss about some interesting short term intent!

/ Swapping Intents

- Let’s say current ETH price is 1890
- Intent
  - Offer 1900 USDC
  - Receive 1 ETH

- Swap fee + Gas fee = 10 USDC

/ Swapping Intents without gas fees

- Let’s say current ETH price is 1890
- Intent
  - Offer 1890 USDC
  - Receive 1 ETH

- Any takers?

/ Bridge user intents

- Intent
  - Offer 100k USDC on Arbitrum
  - Receive 99.9k USDC on Polygon

- Requirement: Cross-domain

/ Bridging liquidity intents

- Intent
  - Offer 100k USDC on Polygon
  - Receive 100.1k USDC on Arbitrum

- Requirement: Cross-domain

/ ONLY UP intent

- Intent
  - Offer 1,000,000 USDC
  - Receive 1,003,000 USDC

- Any takers?

/ Intents that just do transfer...?

- Intent
  - Offer 1,000,000 USDC from Address A
  - Receive 1,000,000 USDC to Address B

- What is this meaningless intent?

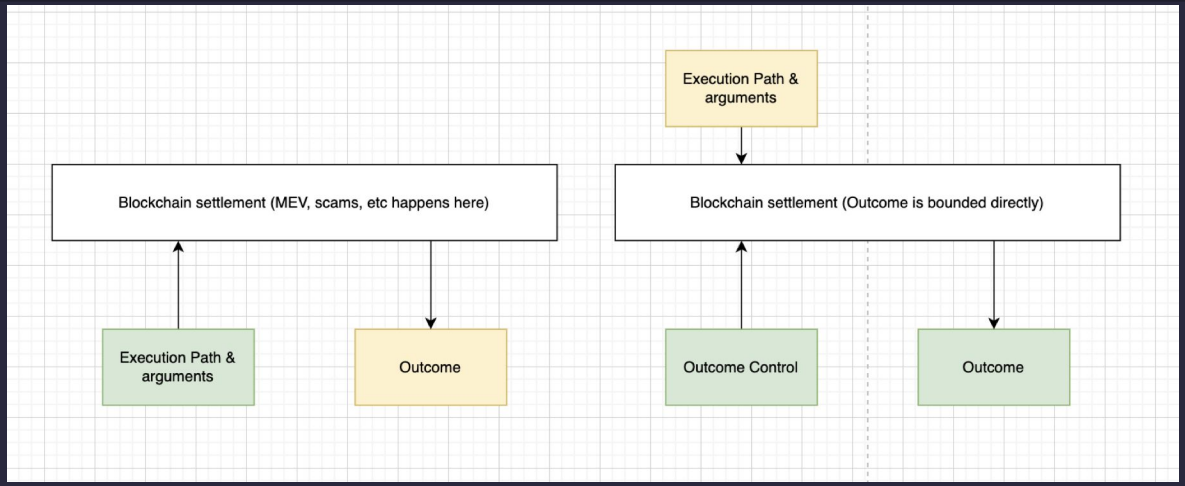
/ Intents can be more complicated

- Define resource offered
- Define resource received
- Define the mechanism between resource offered and resource received, it can even be time-dependent and access controlled.
  - Think about UniswapX, dutch auction!

/ Intents improve UX and security

- How do you get scammed?
- UX for bridging (credit: Uma Roy)
  - User needs to bridge
  - Google for a bridge
  - Send a transaction that sends the funds to the “bridge”
  - Pray that it will come up on the other chain.

/ Contemporary TXs v.s. Intent aware design



- TX will get executed, not necessarily the expected outcome
- Intent may not be executed if the outcome control just doesn’t make sense
- Intent can be on different levels - “blockchain”, “wallets”, “apps”.

/THAT'S A WRAP!  (mic drop)