



composable

I want to swap ETH for DOT



I want to send USDC to Cosmos Hub



Omar Zaki, Founder of Composable

# A Vertically Integrated Intent Supply Chain

Intents Day

I want to lend USDC



I want to borrow ETH



## Reintroducing Composable

Composable is the processing engine for user intentions in the digital world. The ability to transact from any chain, with any asset, and for any use case is a reality with Composable.

Our motto, "any money, any chain, anywhere," refers to our goal of enabling the use of any currency along any chain, within any application.

Composable, in short, is a co-processor of blockchains.

*picasso.*

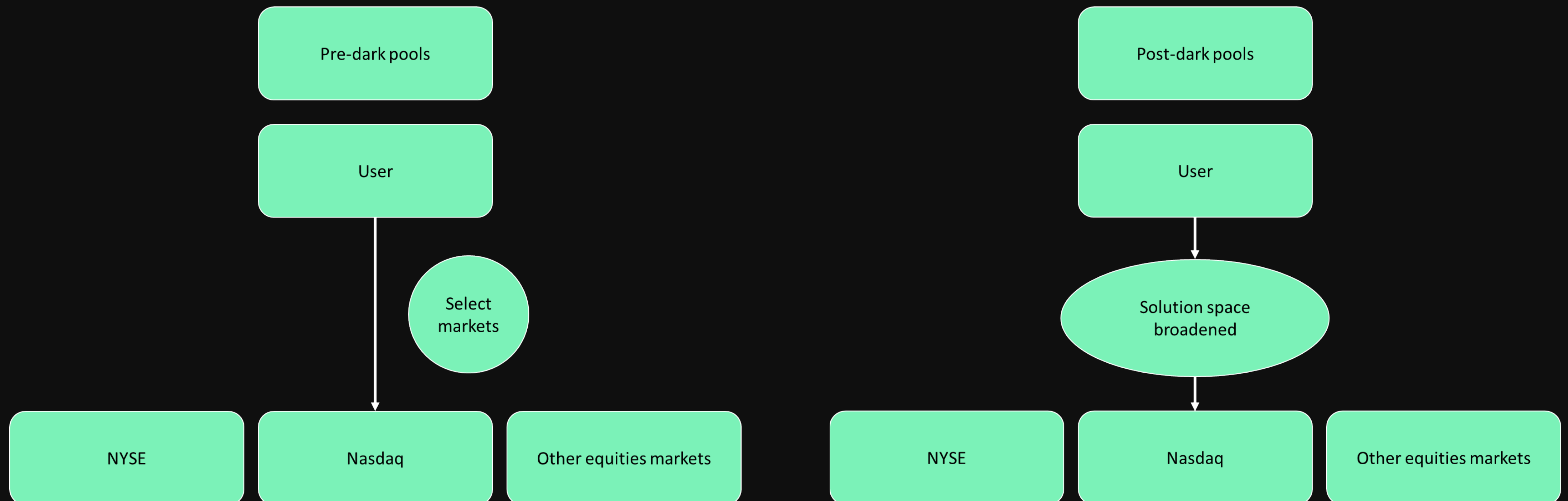
- Focus on Dotsama ecosystem
- Cross-chain DeFi
- Liquid Staking

 composable

- Focus on orderflow
- IBC everywhere
- Intent settlement
- Restaking

# Intents are Inherently Cross-Domain

Equities markets became more efficient with execution being broken across different markets.



# Blockchains are Inherently Trust-No-One Markets

Orders live on blocks that are publicly verifiable.

A supply chain forms around these orders.

- Users – submitting orders
- Protocols – serving as venues for orders
- Block builders – building blocks with orders
- Proposers – proposing blocks with orders
- Searchers – extracting MEV from the presence of these orders in pre-processed blocks

These distinct markets, though increasing the solution space for problems, do not actually communicate with each other.

There is thus a huge amount of potential loss due to lack of synchronicity between these markets.

## Equities:

- Stock trade -> dark pool -> multiple exchanges -> DTCC for settlement
- Execution cost:
  - Cost of trading in exchange + cost of settlement + repo cost
- Tools like Robinhood let you trade for free
  - Frontrunning revenue > execution cost

## Crypto:

- Order -> RPC -> Builder -> Network -> AMM
- Cost:
  - Execution cost + AMM fee + MEV cost

## How Can We Get Close?

There is no DTCC in crypto - so there is no credibly verifiable way to settle orders between chains, and also settle them at the same time.

So, how can we optimize the supply chain so that there is the remote possibility of facilitating this?

Introducing **Mantis**:

## Multichain Agnostic Normalized Trust-minimized Intent Settlement

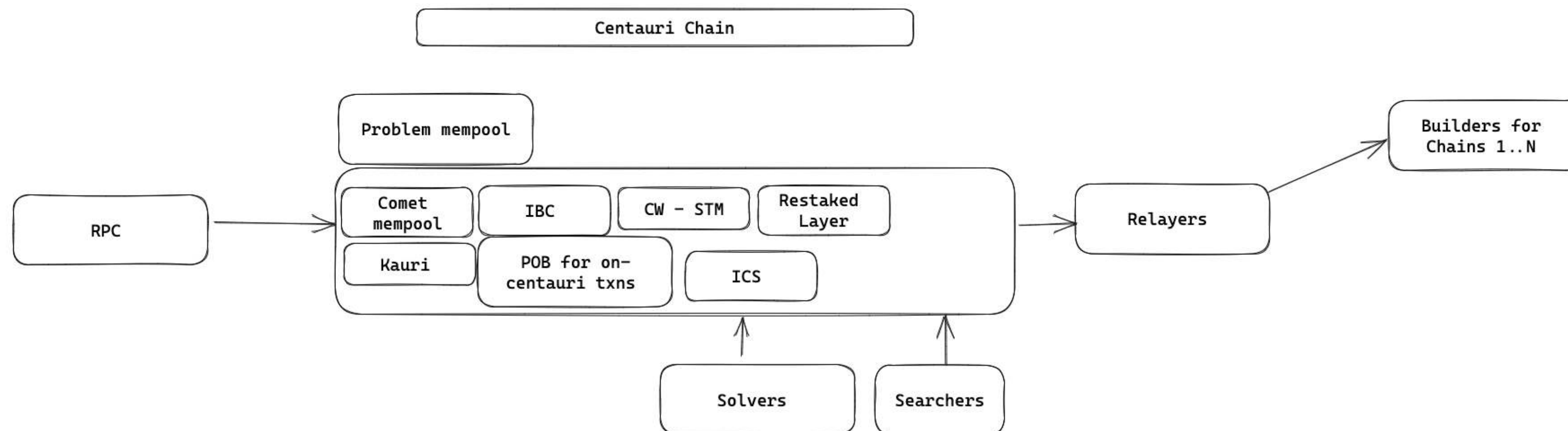
1. Cross-domain communication - IBC everywhere
2. Multi-domain auctions
3. Language for execution
4. Verifiable settlement



## Our Thesis:

Execution of transactions on the blockchain should be ecosystem agnostic, free, and private.

## Our Architecture:



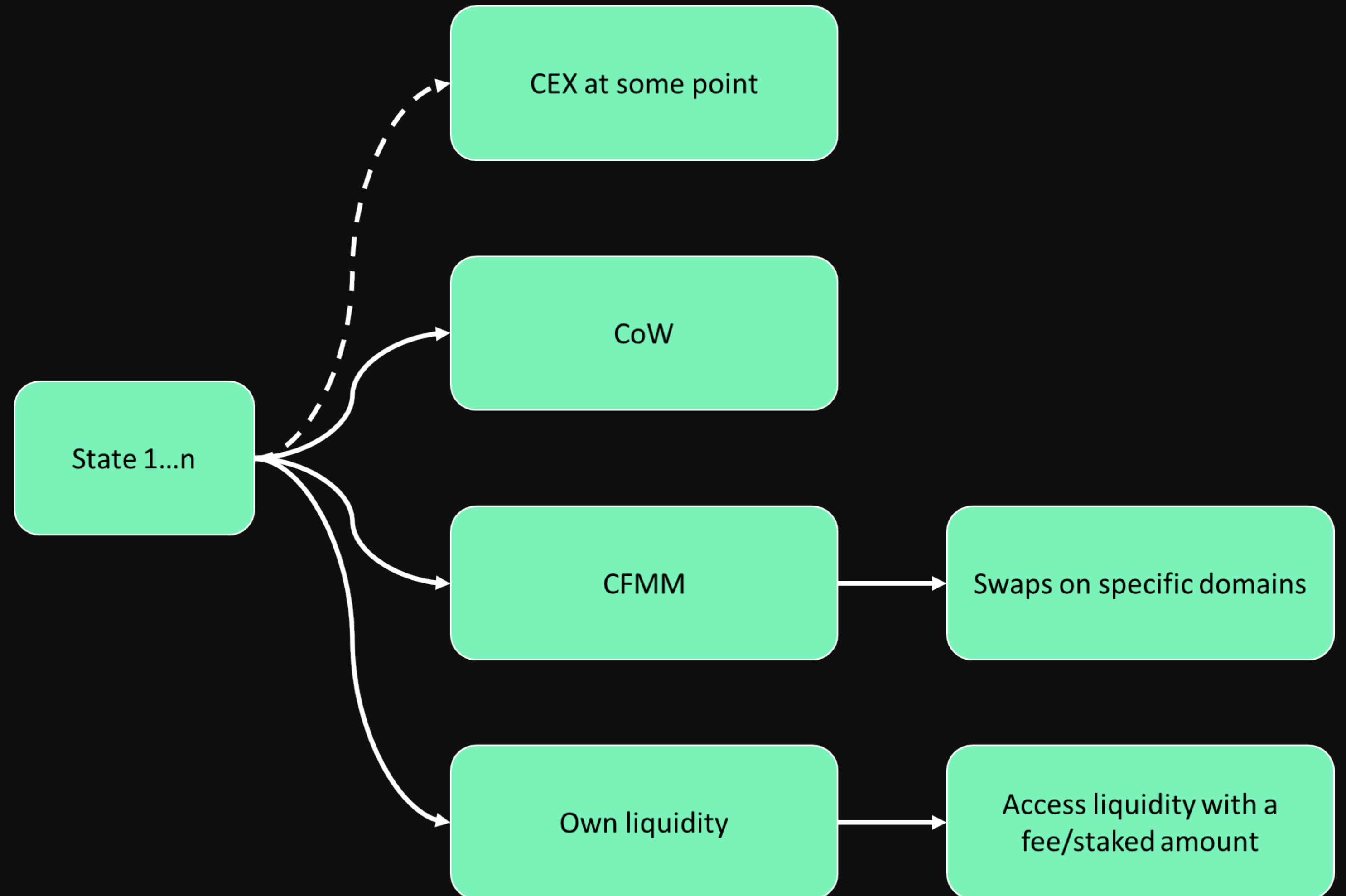
## User Specifies Problem:

User transaction intents involve the following:

- Format: I want to [function] [asset 1]...[asset n] for [asset 2]...[asset m]
- This involves solving a path between:
  - State 1 = [Token ID][Chain ID][Amount]1...n assets
  - State 2= Token ID and Chain ID are variable
- Beginning and destination chain/location(s) may also be specified by the user
- The user will also set limits for buy and sell orders
- Funds moved to virtual Wallet

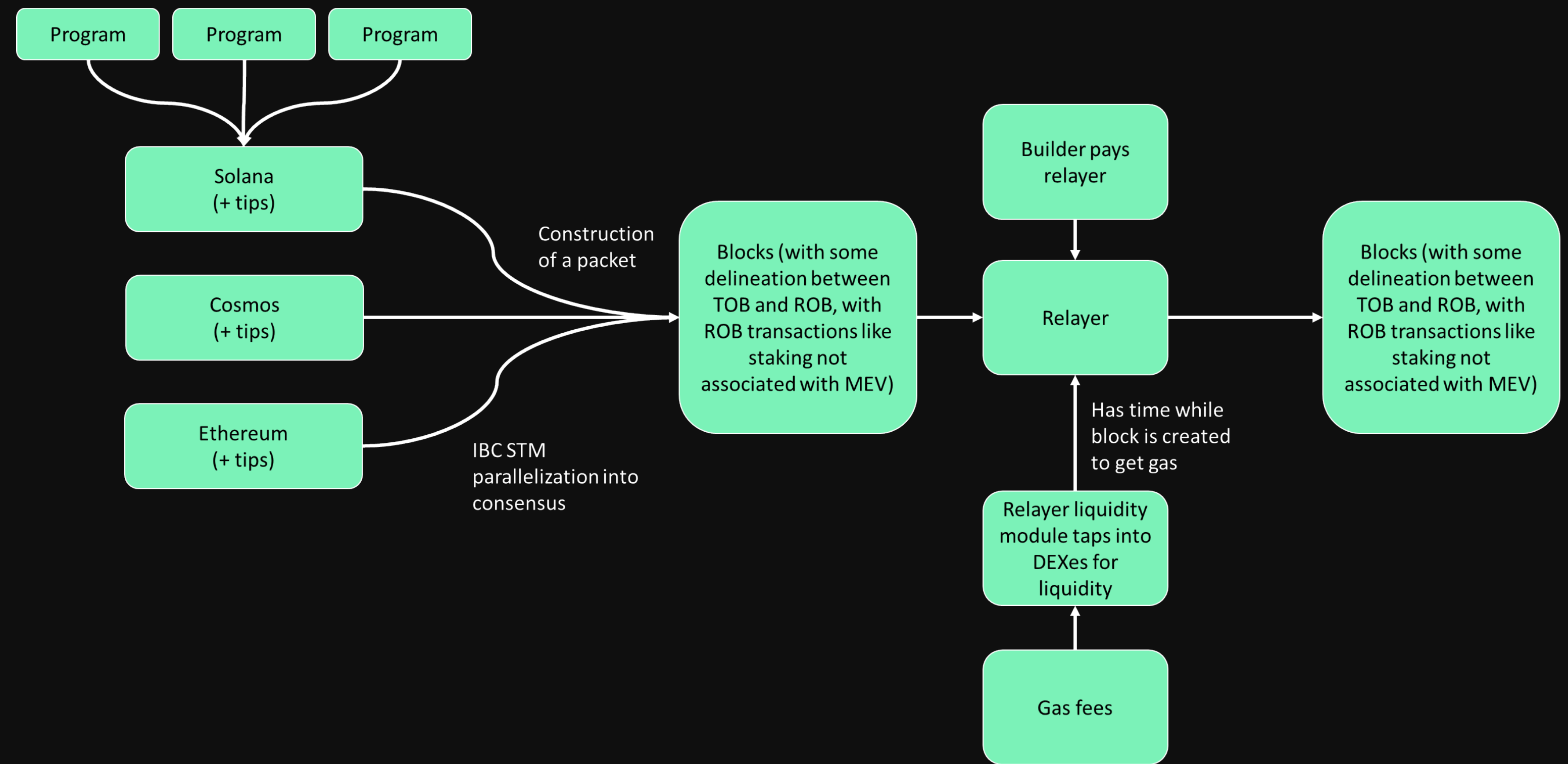
## Allowable Solutions:

- Coincidence of Wants (CoWs)
- Constant Function Market Makers (CFMMs)
- Market makers' own liquidity
- Protocol bidding (protocols can bid for routing orderflow to their respective locations)



# Multi-Domain Auction:

- Scored based on volume cleared
- Solutions are screened for MEV
  - Multiple solutions then bundled into a block for a specific domain
- Searchers tip in the asset associated with each domain and provide conditioning via smart contract.
- Finalized blocks embedded with validity predicates and sent to builders (builder module on Cosmos, Jito builders on Solana)



# Composable VM: Each Solution is Turned into a Program

```
message Instruction {
  oneof instruction {
    Transfer transfer = 1;
    Send send = 2;
    Spawn spawn = 3;
    Call call = 4;
    AbortProgram abort = 5;
    DropContext drop = 6;
  }
}

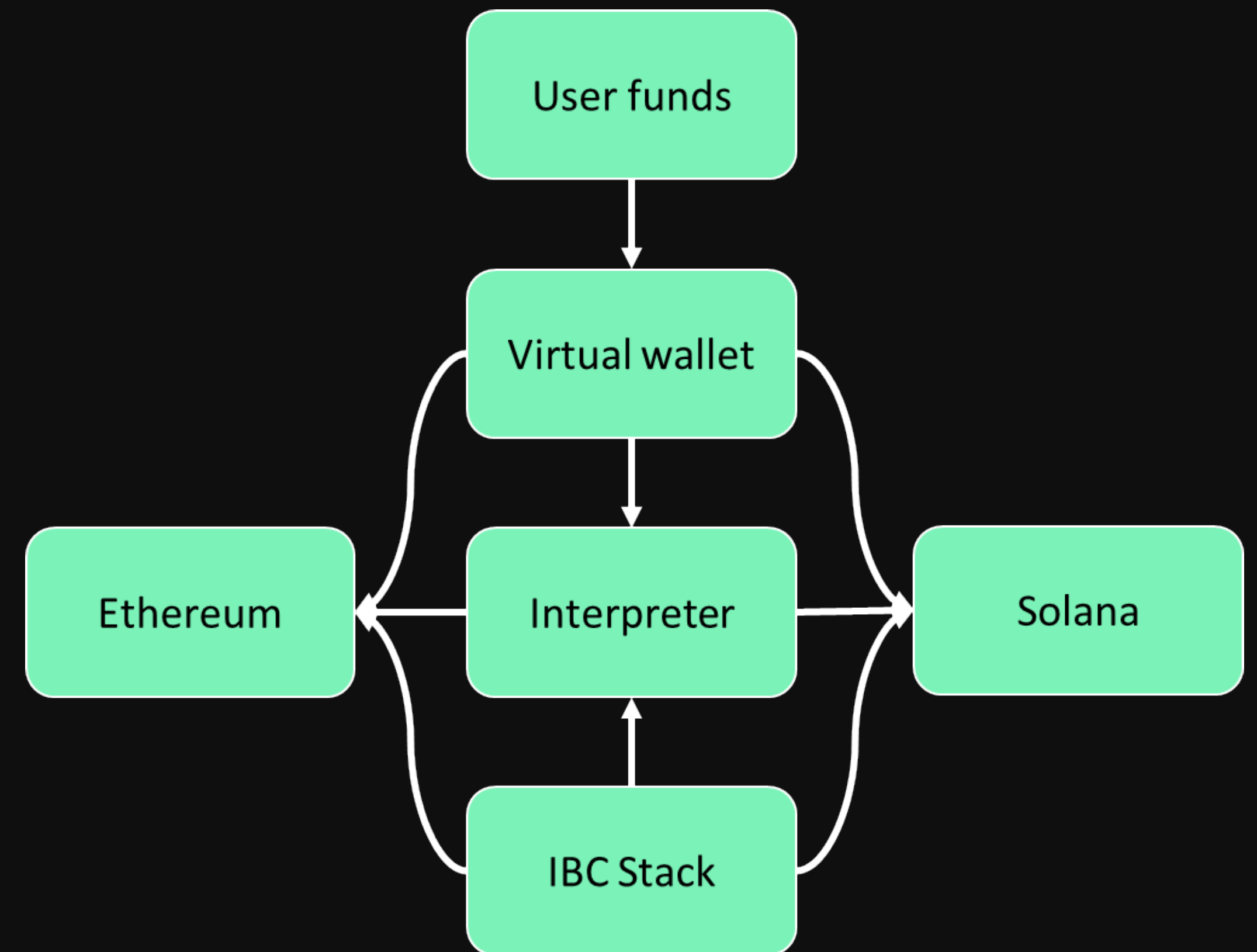
message InstructionResult {
  Instruction executed_instruction = 1;
  bool success = 2;
  bytes outcome = 3;
}
```



# Constructing a Program

When the best solution is found, it is turned into a CVM program:

- Specifies which hops need to happen
- Specifies which calls to virtual wallet need to occur
- If a solution has multiple hops - routed back to Centauri chain
- Ex. Transferring to a CEX
  - Problem defined as location to send funds to
  - User funds transferred to VW
  - CVM instruction set defines the necessary hops to the required network able to accept the assets
  - Transfers occur over IBC



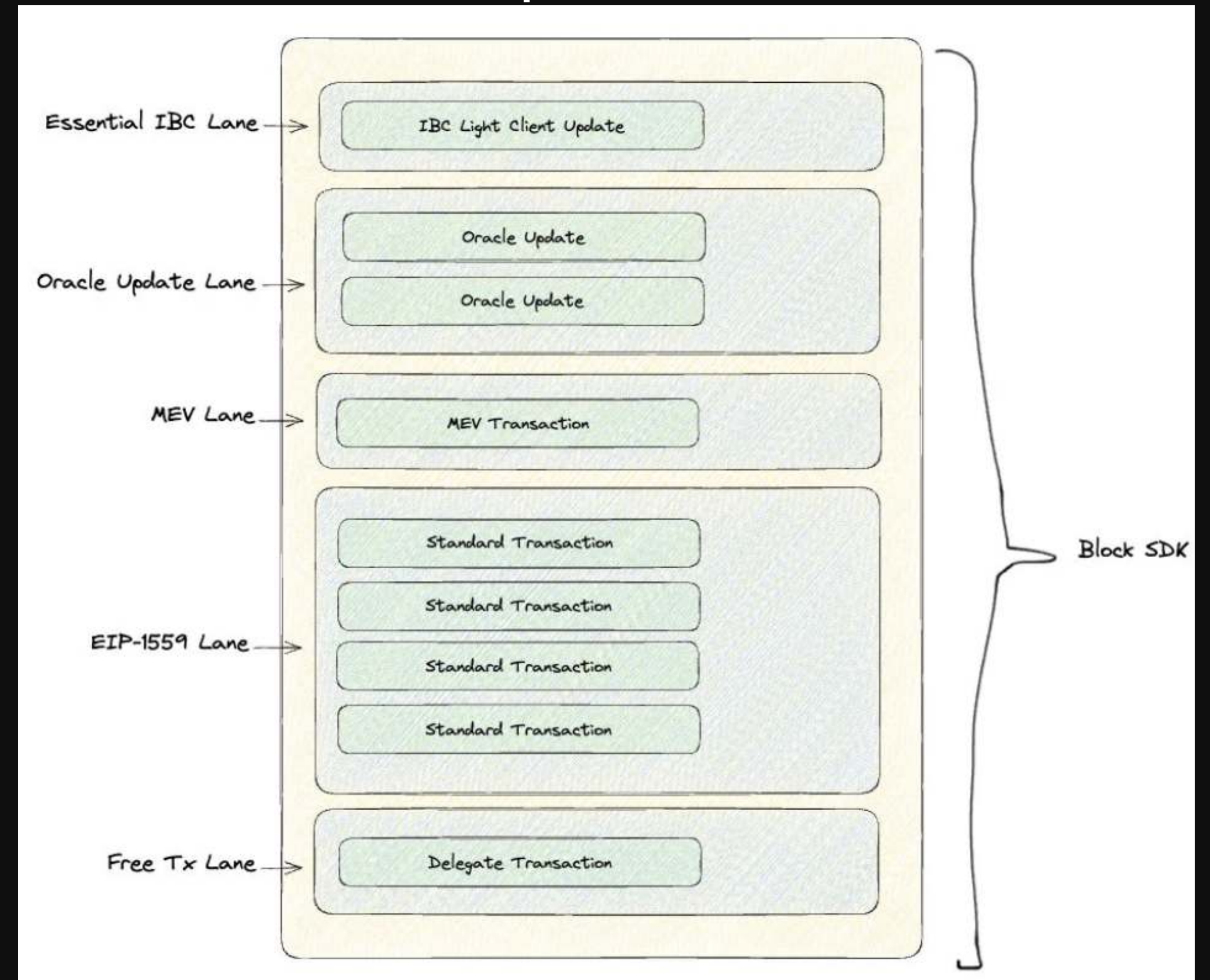
# Cross-Domain Transactions Must be Partial Block Aware

To improve cross-domain censorship-resistance and enforce searcher conditioning for cross-domain transactions, partial block auctions are a must.

We see examples of this in Cosmos, but Ethereum requires additional work regarding commitments to allow for a differentiation between TOB and ROB



## Skip "Lanes"



# Redefining Commitments – Towards a New Relay

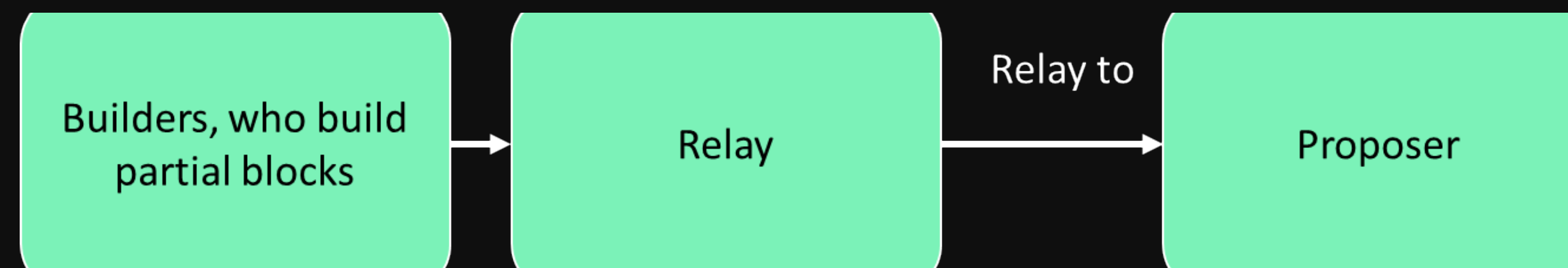
Restaking is a monetary layer for trust. This can be used to create commitments. Composable will offer a restaked layer via its consumer chain + EigenLayer connectivity.

Currently:

- Builders commit to building the best block possible
- Relays propose the “best” block

Initially:

- Searchers commit to building the best blocks for themselves
- Builders commit to building the best partial block (they can be specialized)
- Relay + proposers are committed to broadcasting a full block based on these partial components
- Proposers and builders are both staking assets in the restaked layer

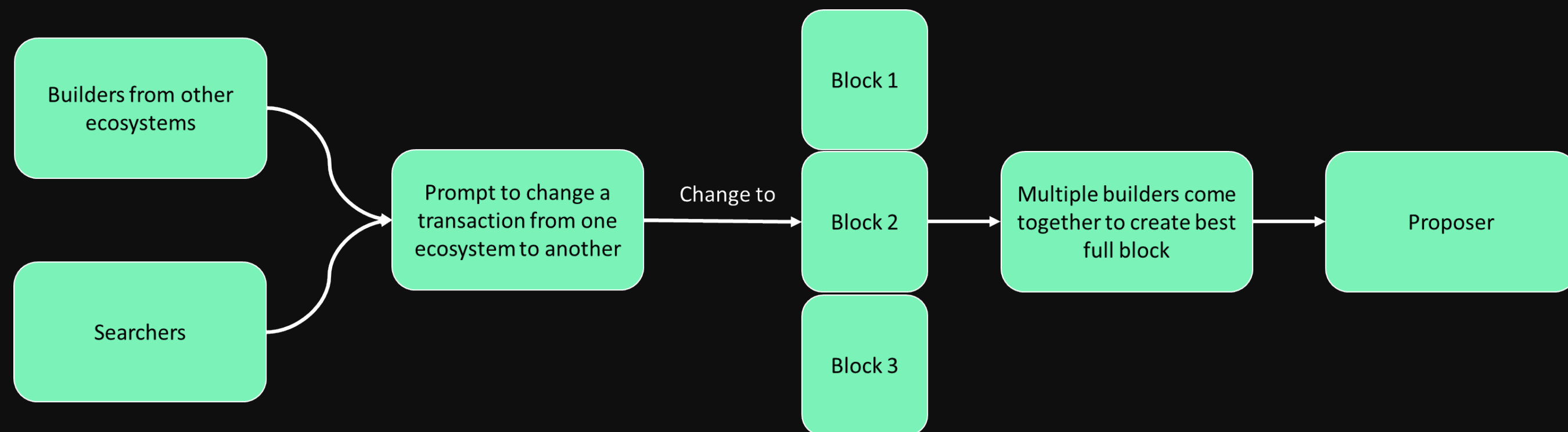




# Towards a No-Builder Future: Domain Exchange

Builders or searchers can pay to change a transaction or a set for execution to another domain, with proof that execution is the same, otherwise, slashed.

If we believe searchers to be the “smartest entity” eventually they should be able build blocks collaboratively and send them directly to proposers, without builders.



## What this means for the protocol:

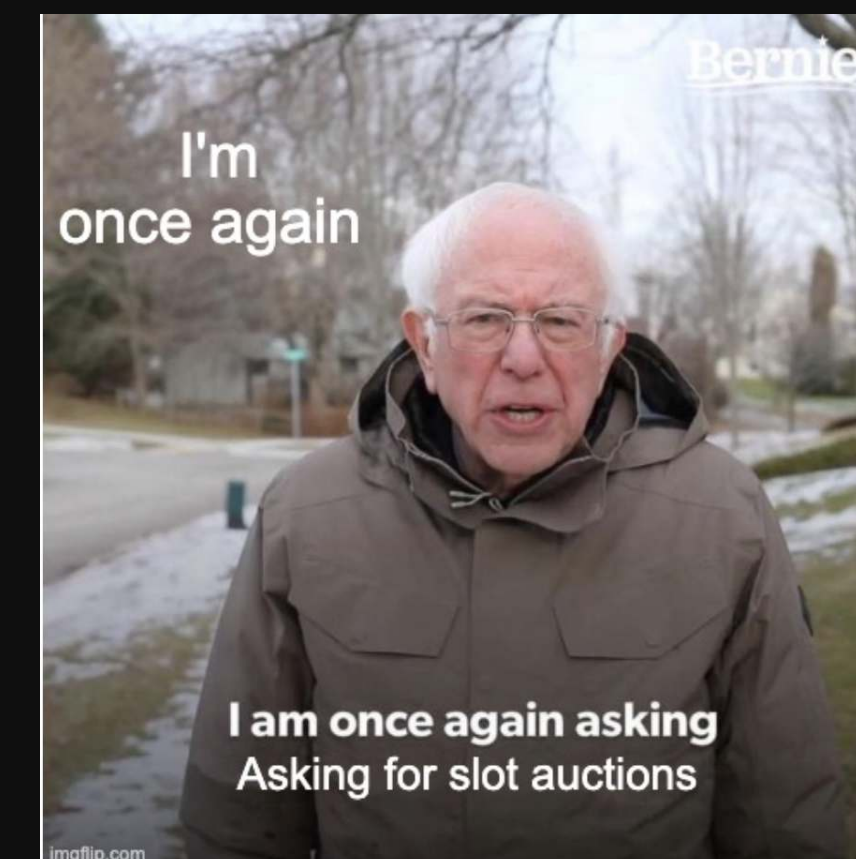
Making protocols interested in offering better execution by allowing the ability to guarantee the same execution while waiting for a ROB transaction vs a TOB transaction.

## Extensions: Mempool Matching + Pre-Reserving Blockspace

Eventually, instead of transactions being routed through Centauri, solvers can match mempool "intents" across different chains to allow for settlement. This requires coordination between solvers, and searchers viewing mempools of multiple chains.

Pre-confirmations offer us the first examples of pre-reserved block auctions.

With things like Skip's lanes, we can have solvers begin to offer atomicity through blockspace reservations, but pre-confirmations allow a market to form around builders, and later proposers.



## Next Steps

Modeling the value of cross-domain orderflow via MEV-Share w/RIG

- Utilizing ETH-IBC
- Evaluating the value of revenue back to Relayers

Open sourcing Solver

- Sept 2023


v0 of Intent Supply Chain

Open Sourcing Relay w/ Collaboration with EigenLayer

I want to swap ETH for DOT 

I want to send USDC to Cosmos Hub 

# Questions?

I want to lend USDC 

I want to borrow ETH 

## References & Resources

1. IBC Protocol: <https://ibcprotocol.org/>
2. The Centauri Bridge: <https://app.trustless.zone/>
3. The Centralizing Effects of Private Order Flow on Proposer-Builder Separation: <https://arxiv.org/pdf/2305.19150.pdf>
4. Decentralizing the Builder Role: <https://joncharbonneau.substack.com/p/decentralizing-the-builder-role>
5. Composable: <https://www.composable.finance/>
  - a. Composable Documentation: <https://docs.composable.finance/>