PRO   MEV

Skip: Building Blocks in Cosmos

APR 27, 2023 • 22 Min Read

Ceteris

▶ Listen

The author of this report may personally hold material positions in ATOM, OSMO, ANOMA, ETH, SOL. The transparency... Show more

Appchains, Sovereign MEV, and Skip

MEV. Maximum extractable value. PBS. Order flow auctions. Shared sequencers. Cross-domain MEV. If you're keeping up with the discourse in crypto today, nearly every discussion involves these terms, and for good reason. MEV touches nearly every on-chain transaction, and the goal of protocols is to identify and extract it as efficiently and fairly as possible. Those protocols who are not able to capture the MEV they create will

In Ethereum, the MEV landscape is defined by Flashbots and PBS (proposer/builder separation). For a general purpose chain like Ethereum, building blocks is hard. Due to the size, variety, and complexity of transaction sets, the complex task of building blocks is outsourced to specialized parties called block builders. This has the benefit of keeping validator requirements low, but does not address the source of MEV itself and moves this centralizing factor to block builders instead. The supply chain also ends with the validator, which means the MEV goes to the current proposing validator (who has a single slot monopoly) instead of the entire Ethereum protocol (or the apps that create the MEV like Uniswap) itself.

The sovereign MEV thesis looks to address this shortcoming, taking the typical MEV supply chain one step further; why don't we end with the protocol instead of the validator, and allow the protocol to "internalize" the MEV it creates?
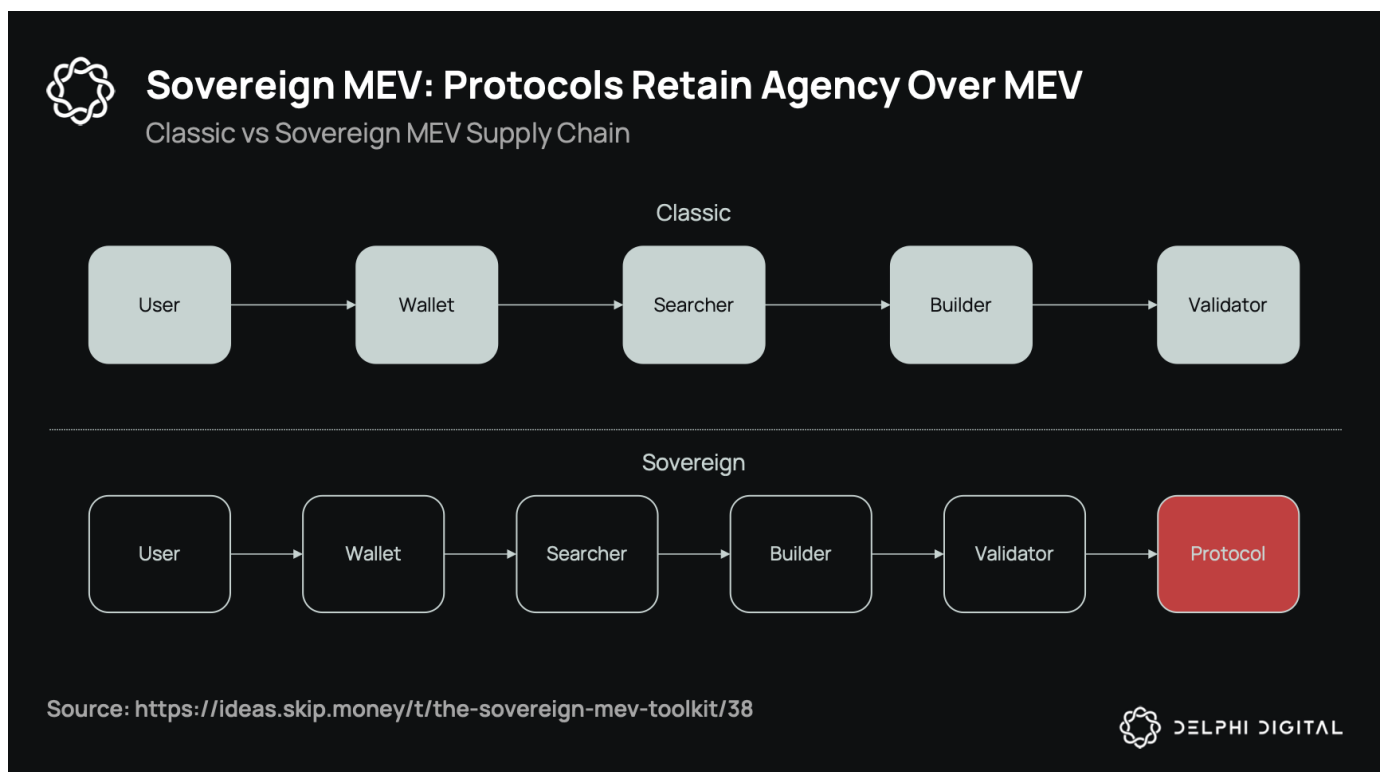
extracted, what is allowable, and where it accrues. Skip defines the sovereign MEV supply chain with three criteria:

1. **Community Determines Who Accrues MEV:** This can be LPs, stakers, end-users, validators, or even smart contract devs. Who should the chain prioritize and why? If you are an AMM chain like Osmosis, does it make more sense to prioritize stakers of OSMO or the LPs?

2. **Community Determination of Allowable In-Protocol MEV:** Cosmos communities DO NOT like front-running or sandwiching, so much so that Skip has made both of these activities essentially illegal by default. While validators can do whatever they want, with smaller validator sets in Cosmos they are more accountable. Reputations are important and delegators can freely move between validators more easily. This is fundamentally more challenging on Ethereum, not just because of the larger validator set, but because you cannot choose who you delegate to with liquid staking tokens like Lido (your stake is spread across Lido validators).

3. **Community Determination of How MEV Is Extracted:** Does extraction take place out-of-protocol? In-protocol? how democratic/accessible is it, and does a community prefer maximum decentralization over maximum efficiency?

Every appchain is different in its construction. Some strive for lower latency, others for privacy, some are orderbooks, others are AMMs. All of these generate MEV in different ways considering their design choices/tradeoffs, and thus protocols can create more tailored and granular solutions for how they build blocks. Compare this to a general purpose chain where you cannot get to this level of granularity considering all the diverse and competing activities. In short,

Of course, when we think of sovereign appchains, we think of Cosmos, and it's important to set this report up with a general framework for how the MEV landscape will look in the future and how Skip will play a part.

Breaking Down MEV in Cosmos

An ecosystem of diverse appchains has unique considerations. While the categories outlined below are applicable to every ecosystem, the way MEV will be handled in Cosmos differs mostly due to how chains customize and express their sovereignty. Total MEV can be split out into three categories: internal MEV, CeFi-DeFi MEV, and interchain MEV.

- **Internal MEV:** This is the MEV that happens on the appchain itself and is the most controllable or easiest to "internalize." An example here is the ProtoRev module Skip has developed for Osmosis which captures backrun MEV after every transaction. Appchains vary in how they intend to capture this, whether using frequent batch auctions (FBAs), privacy, out-of-protocol builders, in-protocol builders, multiple block proposers, and more. Internal MEV comes from ordering and is commonly referred to as atomic arb. Note that some of the designs/tactics in the chart below (green boxes) will also be used to mitigate the other categories of MEV (for example, protocol-owned builder, top-of-block, and orderflow auctions). We put them here because they are most effective with regards to internal MEV.
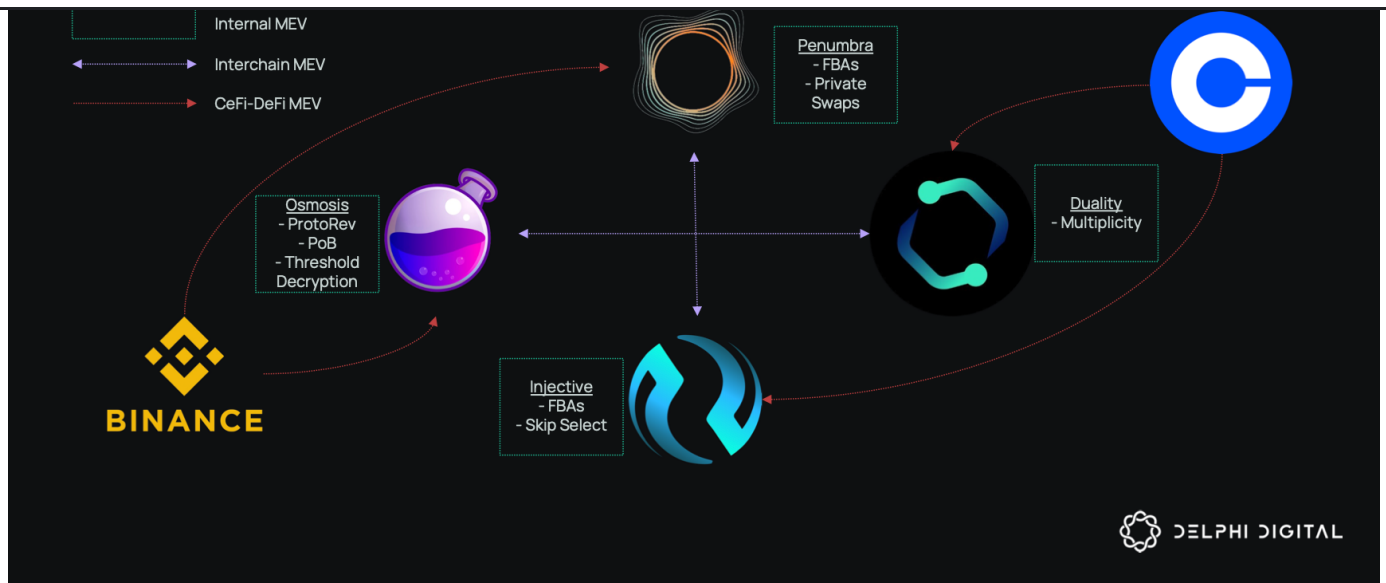
- **CeFi-DeFi MEV:** This is perhaps the biggest source of MEV. Stephane from frontier.tech and formerly Flashbots estimated $10B stat/$1B atomic on Ethereum as of May 2022 and more recently established a lower bound of $100M stat arb as of February 2023 (due to overall volume declines). Stat arb is MEV generated from information *invisible* to the blockchain, the most common being CeFi-DeFi arbitrages. Price discovery tends to occur on centralized exchanges, and thus the "true" price has been updated off-chain before on-chain pools are adjusted. Traders then arb the on-chain pools at their stale prices. The best way to visualize this is by estimating Uniswap LP markout. Markout is a measure of a trader's execution performance and fill quality. This is the value extracted from LPs as informed (i.e., toxic) flow arbs the pools. Uniswap LPs are by extension paying for a significant portion of Ethereum's security (thank you LPs, very cool!).

- *Note that calculating markout is complicated and more of an art than a science. For the definitive piece for those interested, I would refer to this deep-dive from CrocSwap (TL;DR: 0.05% fee*

CeFi-DeFi Arbitrage Costs Uni v3 LPs

Cumulative 1h Markout (w/Fees) for WETH/USDC v3 LP (source: Dune @wanxin / Ethereum Uniswap Markout)

♡ 2

- **Interchain MEV:** The last one here is interchain MEV, also known as "cross-domain" MEV. This one is a mix of both stat and arb. Today, blockchains do not see into each other and are siloed, so this mostly falls into the stat category. In the future, with more aware cross-domain builders like Suave, protocol-owned builders with Skip, cross-domain blockspace and orderflow markets with Skip and Mekatek, or Anoma's Chimera chains with their Typhon consensus, we can see this shift more towards atomic arb. This is both the most exciting and uncertain domain to explore, and in the long-run will likely be the

Now that we have a high-level understanding of the landscape, we can look to Skip's solutions and plans for the future. We start with their first product, the out-of-protocol builder known as Skip Select, or "MEV-Tendermint."

Out-of-Protocol Solutions: Skip Select

The simple explanation for Skip Select is that it's Flashbots for Cosmos chains. This is an off-chain builder that validators and searchers can opt-in to instead of relying solely on the public mempool. In Tendermint Core, transactions are ordered on a FIFO basis. This means that the gas fee one pays is irrelevant when it comes to a block's ordering, so searchers spam the network to win a latency race and get their transaction in first. Besides being demanding on validators, it also incentivizes colocation and decreases the geographic decentralization of the chain.

Skip Select (or MEV-Tendermint) is a side-car mempool and relay that allows searchers to send transactions with tips attached directly to the proposing validator. The process is:

1. Searchers send priority tx's with their tips

2. Sentinel relay filters the tx's and orders non-conflicting by highest tips

3. Proposing validator receives prioritized tx's from Sentinel and places at top-of-block

4. Proposing validator builds the rest of the block from public mempool
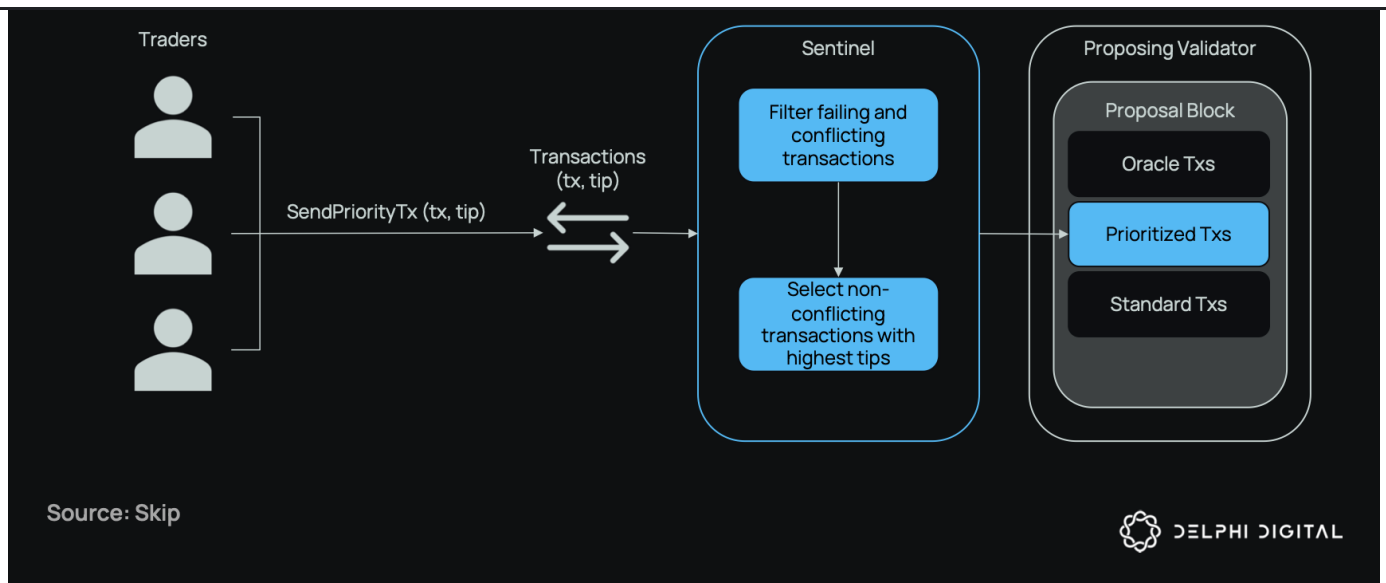
For searchers, this allows them to get top-of-block execution through bids instead of latency wars, keeps their trade private (to Sentinel) until landing on-chain, and protects them from wasting gas on failed MEV extraction attempts. For validators, they just run the software and receive the prioritized transactions with tips, and for the network it reduces the overall spam and failed transactions. Today, Skip claims over 300 searchers and some days with >100k bundles submitted.

Skip Select is opinionated when it comes to MEV, differing from Flashbots or Cosmos competitor Mekatek in that it distinguishes between "bad" and "good" MEV. The most notable is that it rejects frontruns or sandwich transactions by default. Why? Well, first of all, upon some analysis by the Skip team, they found very little evidence for front-running or sandwiching historically, mostly due to Tendermint's FIFO ordering, so they didn't want to make it *easier* for these "bad" MEV extraction techniques which weren't already prominent (note that even though Tendermint is FIFO, validators do not need to respect it and can order transactions in whatever order they want). Second, most Cosmos communities like Osmosis and Juno have taken a hard stance against "bad" MEV extraction and have outlined
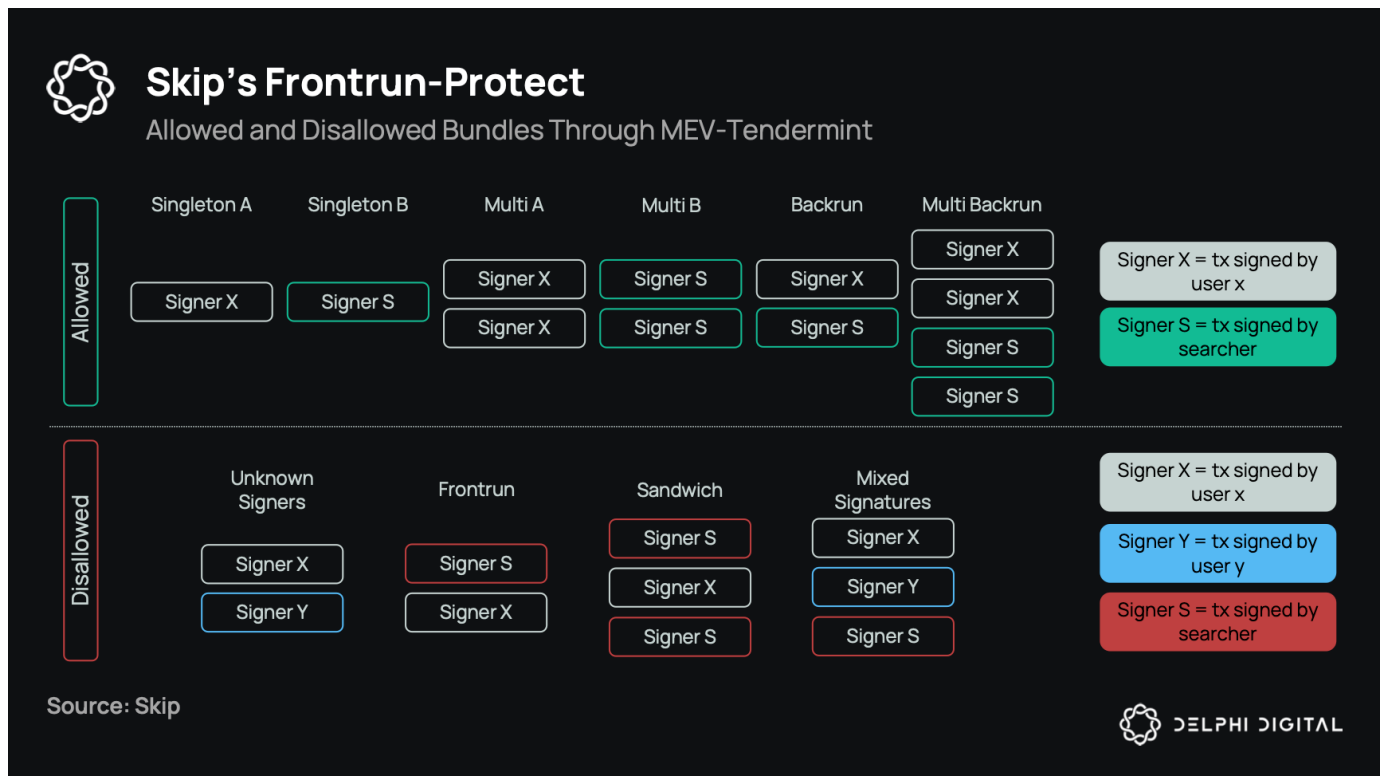
When opting to run Skip Select, validators have two choices to make:

1. Keep frontrun-protect on or turn it off. For the 4 networks Skip Select is running on (Juno, Evmos, Injective, and Terra), not one validator has turned this off.

2. What % split does the validator keep vs. returning to the network.

For the first point, social consensus is so far working in that no validator has chosen to accept "bad" MEV transactions through Skip. For the second, the profit split varies. Currently, the "network profit" split goes back to the entire network, but in the future it can go to stakers/delegators of the specific validator. Validators can choose to share more with delegators to earn a large share of stake. While it can be seen as beneficial to reward validators who "play by the protocol's rules" and share more of the pie, the tradeoff is that this can be a rather centralizing force and will

Validators Choose Profit Split

Top 15 Juno Skip Validators & Profit Split (source: Skip)

Validator Pro
Network Pro
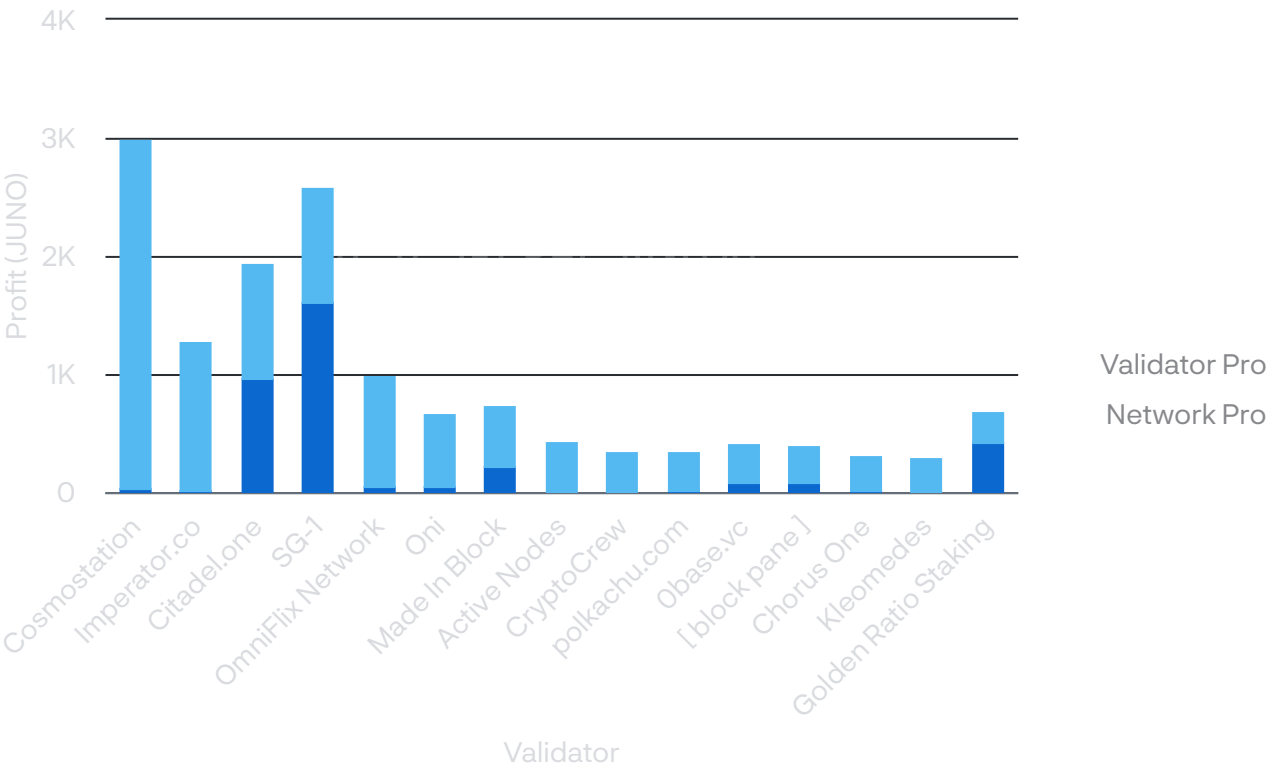
♡ 6

The challenge for Skip with the out-of-protocol builder is that it is only as effective as the number of validators who run it. When non-Skip validators are proposing blocks, searchers need to revert to spamming the chain for inclusion, as searchers will not get their bundles or auction bids through. While adoption has picked up, it's still not ideal at 25-50% of validators.
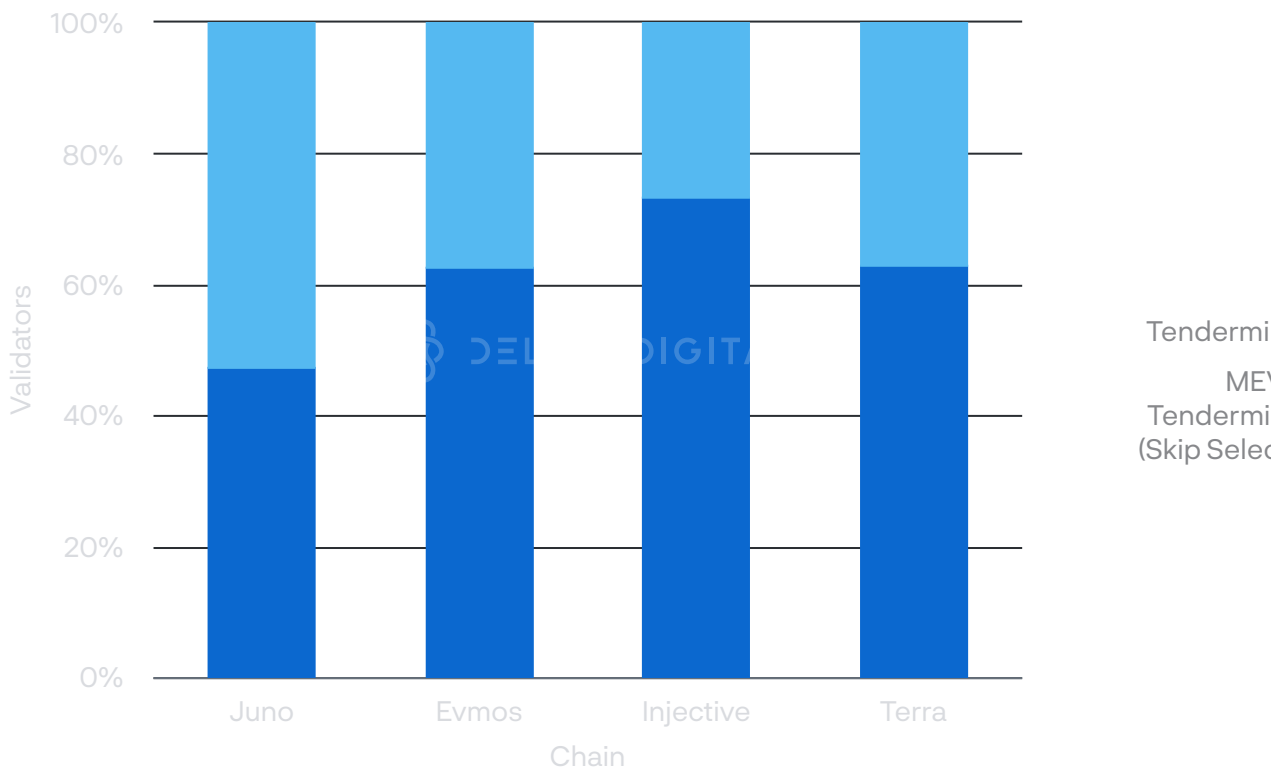
♡ 2

While Skip will continue to educate and onboard validators to Skip Select, in the long-run, they look to decommission it as they move all of the auction logic in-protocol instead. This takes us to our next section, moving from Skip's out-of-protocol solutions to their in-protocol ones. This is where the design space gets more exciting and where the "sovereign MEV" thesis starts to play out.

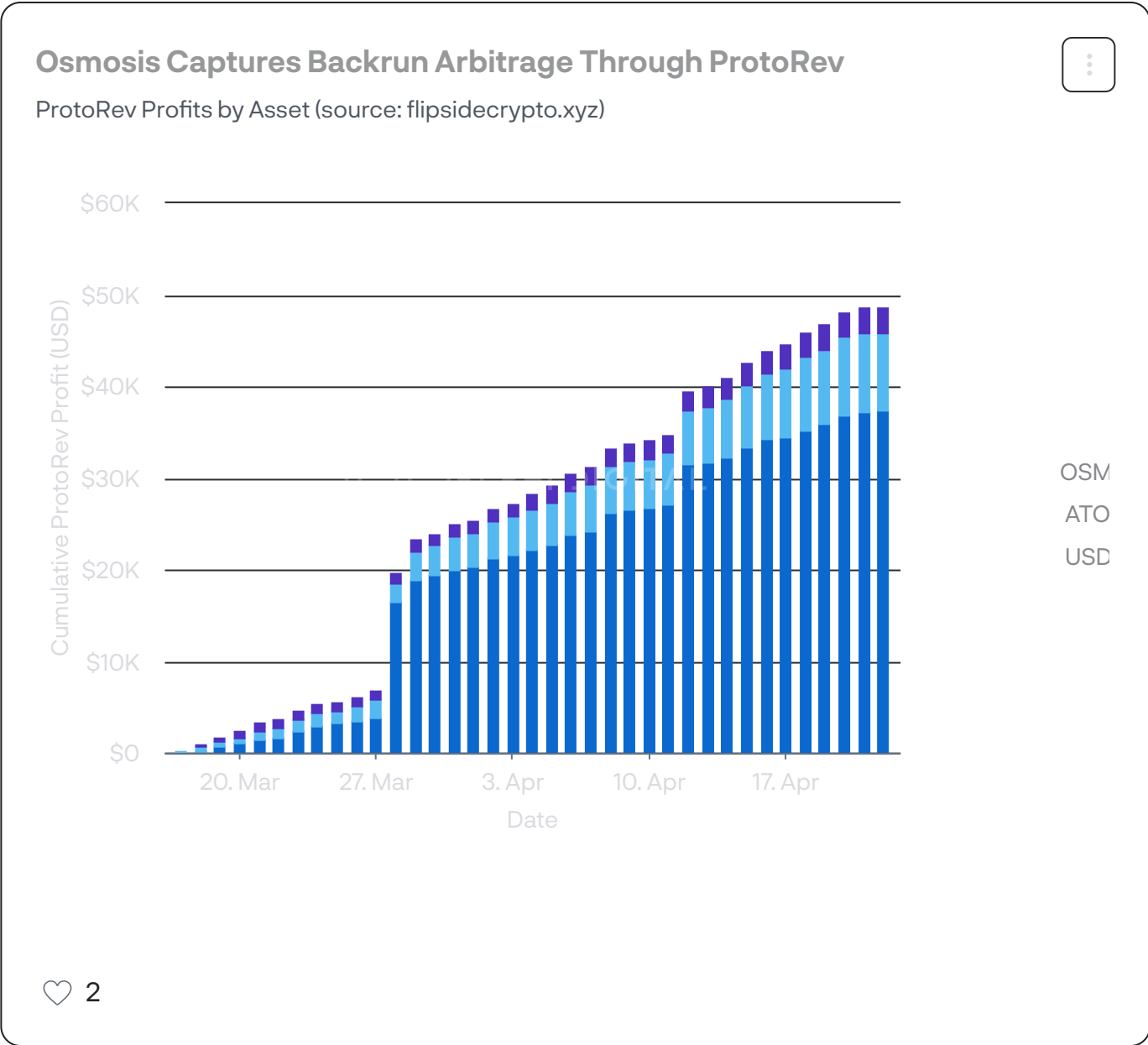# In-Protocol Solutions: Osmosis' ProtoRev Module

Skip team took a look at backrun MEV (and made a dashboard) on Osmosis and uncovered ~$7M in backrunning profit from searchers all-time. During the height of Osmosis activity with Terra, this amounted to ~$2.5M from 01/01/22-05/08/22, or ~$20k/day, and $2M over the 2-3 day depeg period.

Backrunning is when liquidity pools become imbalanced, and as a result, a risk-free profit opens up. Historically, this was all done by searchers playing latency games to get first in line, a direct MEV extraction from users and the protocol to searchers. With ProtoRev, the protocol does this themself and gains a unique advantage over searchers, as not only are ProtoRev transactions prioritized, but the protocol has the ability to flash mint whatever tokens necessary to complete the backrun (can mint OSMO, ATOM, USDC, etc.). The graphic below depicts the ProtoRev flow, starting with the protocol minting the token in step 1 and finishing with burning the minted amount and sending the rest to the treasury in step 5.

ProtoRev Flash Mints & Burns Tokens to Backrun
ProtoRev Example

ProtoRev Module

1 Flash Mint 100 OSMO

Swap 100 OSMO for 7 ATOM (OSMO/ATOM Pool)

2

3 Swap 7 ATOM for 75 USDC (USDC/ATOM Pool)

Burn 100 OSMO

5 Profit 5 OSMO

4 Swap 75 USDC for 105 OSMO (USDC/OSMO Pool)

Osmosis Treasury

Source: Skip, Osmosis

DELPHI DIGITAL
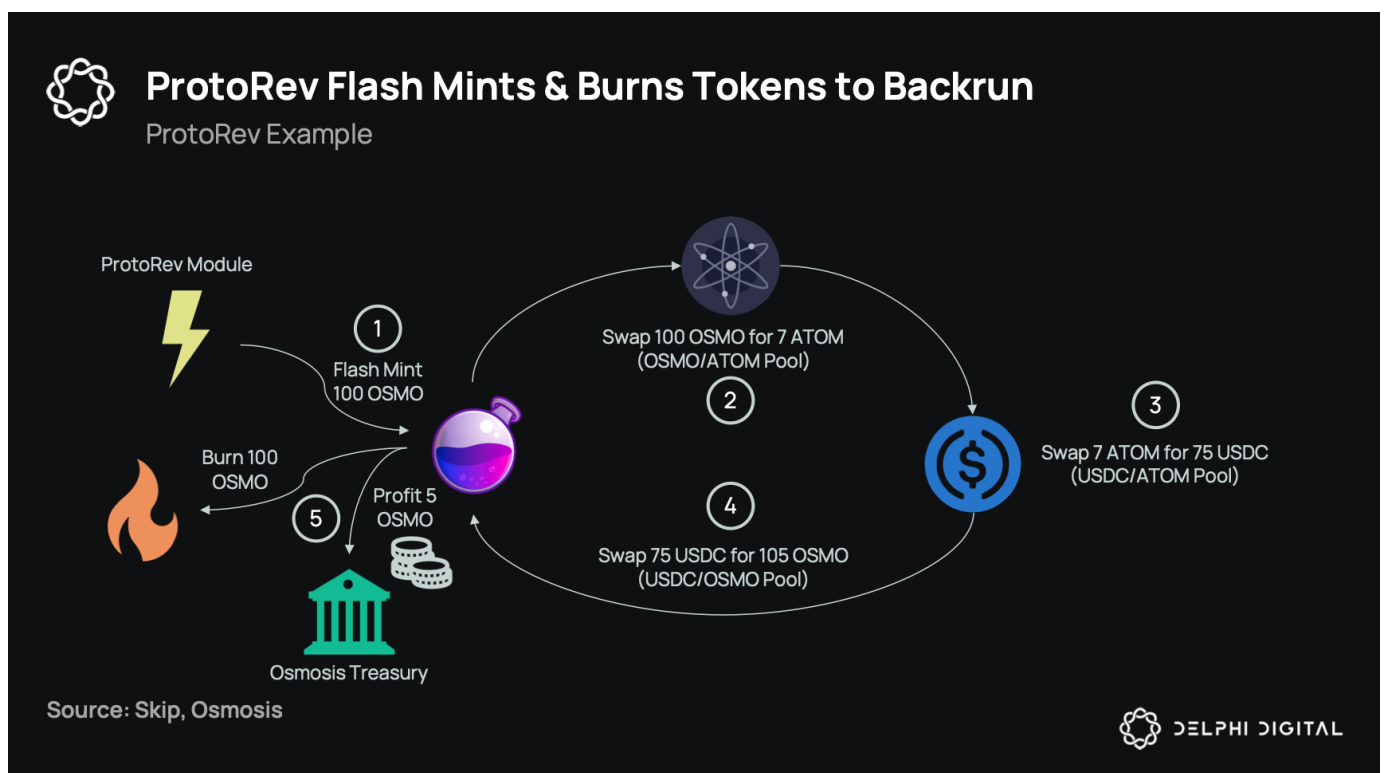
instead of relying on outside parties. Value that would have left Osmosis now stays in, and there has been no material change in performance with the added compute and transactions from the module. With USDC coming to Cosmos and numerous chains launching, Osmosis is prepared to benefit from the potentially higher volumes this time vs. in the past. For their efforts, Skip is receiving 20% of profits in year 1, 10% in year 2, and 5% after.

Osmosis Captures Backrun Arbitrage Through ProtoRev

ProtoRev Profits by Asset (source: flipsidecrypto.xyz)

♡ 2

execution path on-chain. Ideally, and where Skip would like to head eventually, is solving most of this matching further up the stack, with orderflow auctions and matching user intents. Instead of each user executing their trades one by one and opening up a small backrun after each trade, you match these trade preferences before executing instead (i.e., if user A wants to trade X for Y and user B Y for X, we can match these intents instead of having both execute on-chain and being backrun by the protocol).

ProtoRev Backruns Nearly Every Transaction

Osmosis Dex Swaps Split PR/No PR (source: flipsidecrypto.xyz)
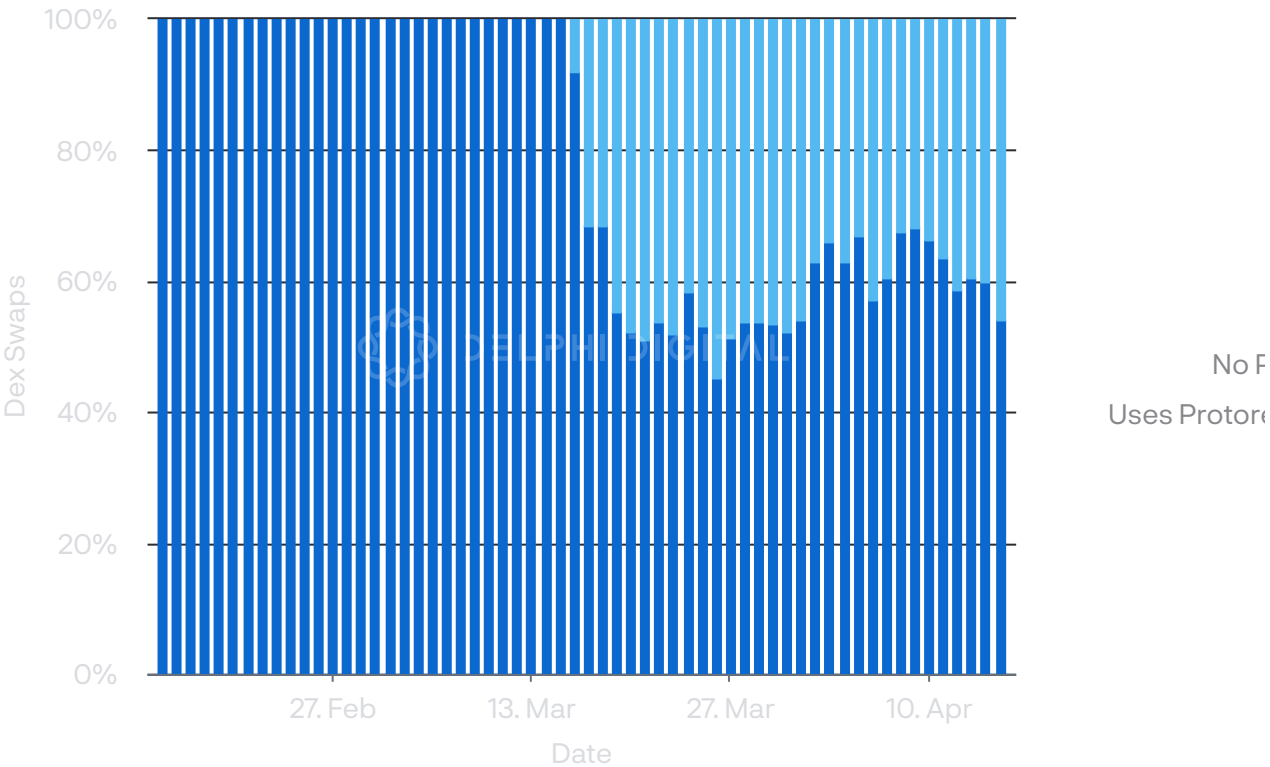
♡ 1

active ones, especially Secret more recently with the launch of their Shade DEX and stablecoin "Silk." Filtering by recent Osmosis backrun MEV will tell you which tokens are being bought or sold in larger than usual size.

SCRT and JUNO Create Most Backrun MEV

ProtoRev Profit by Route (source: https://osmosis-skip-protorev-dashboard.vercel.app/
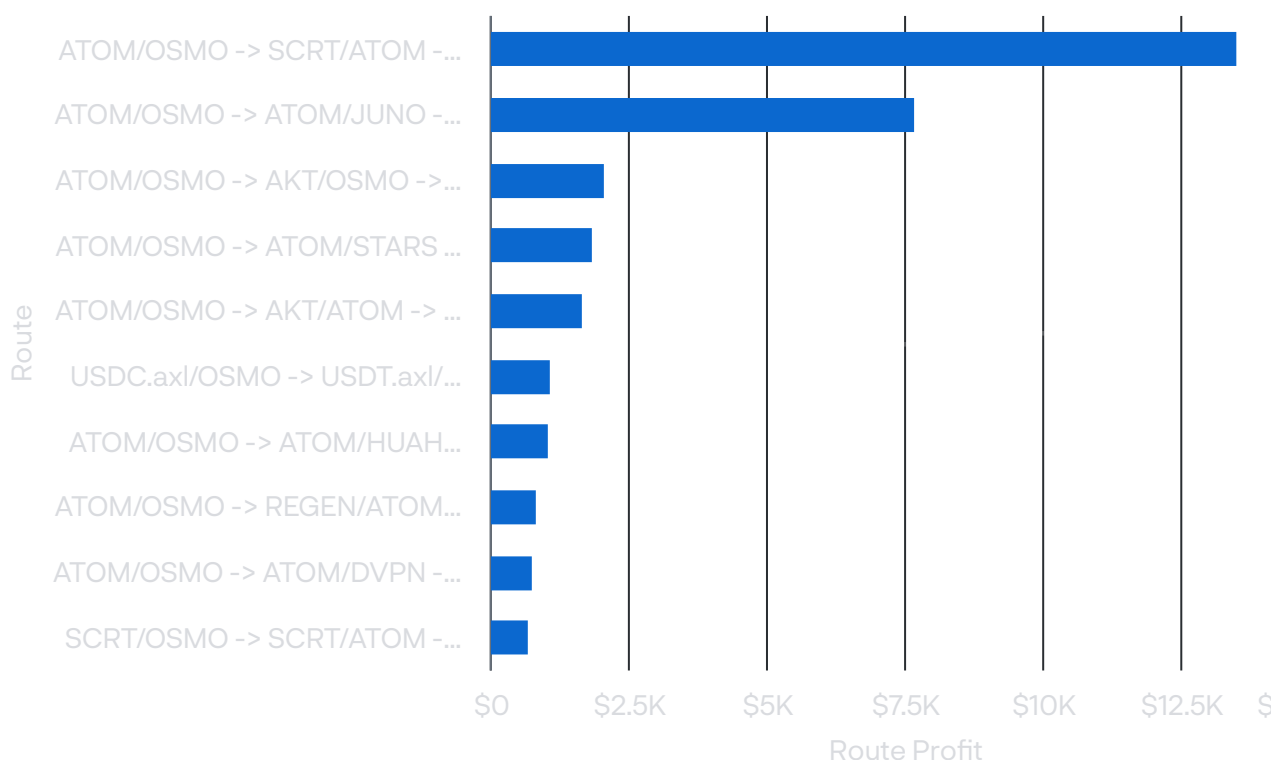
Interestingly enough, even though Osmosis doesn't have a lot of stablecoin liquidity, stablecoin routes make up nearly 1/3 of the ProtoRev module's backruns but only 8% of profit. Most of these are small arbs for immaterial amounts (the top route that arbs Axelar's USDC against Gravity's USDC has done 2k trades for a measly $58 profit).

Source: https://osmosis-skip-protorev-dashboard.vercel.app/
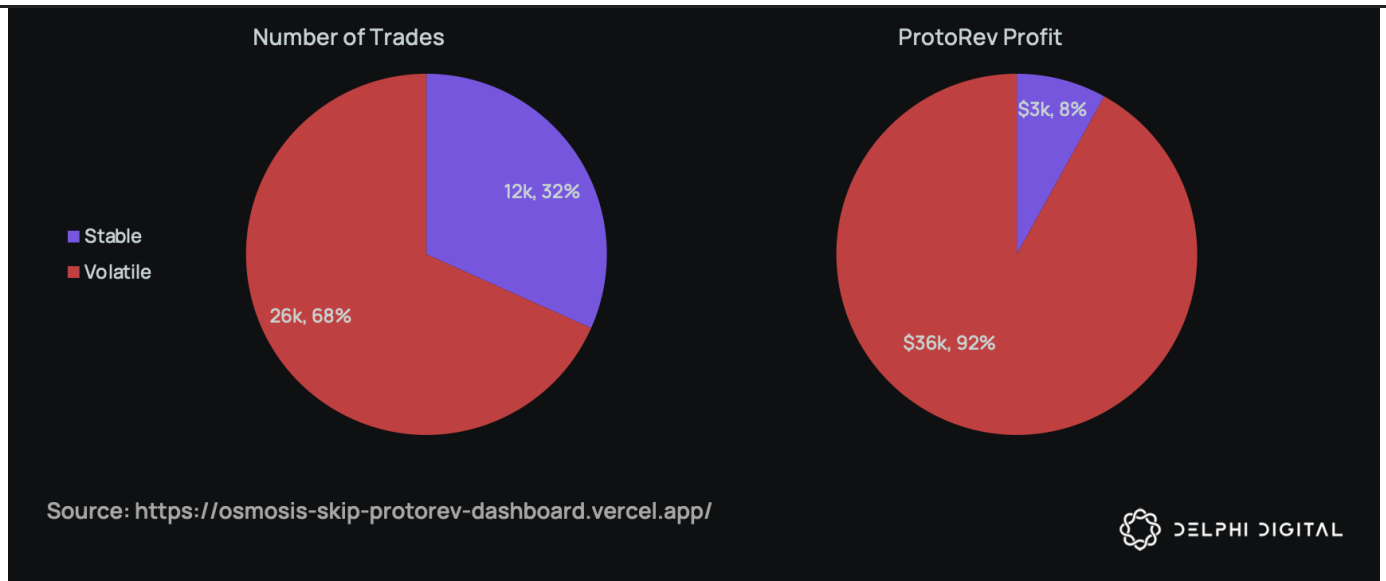
ProtoRev is a cool first proof-of-concept for in-protocol MEV extraction, but it's limited to a fairly simple and inefficient arb. Where the design space *really* starts to open up is through leveraging ABCI++ and moving the block builder in-protocol. This is where appchains can truly start creating custom, granular solutions around block building and MEV extraction.

Taking In-Protocol Further With ABCI++ and x/builder

ABCI++

We talked about ABCI++ a few times in our Sei report, but as a refresher, ABCI++ is the evolution of ABCI that allows every step of consensus to be programmable, creating a tighter connection between the app and consensus layer. With ABCI, the app has no say in block building, and would receive a "black box" of transactions from Tendermint/Comet and execute them. ABCI++ invites the app into the box.

Source: Skip, CometBFT
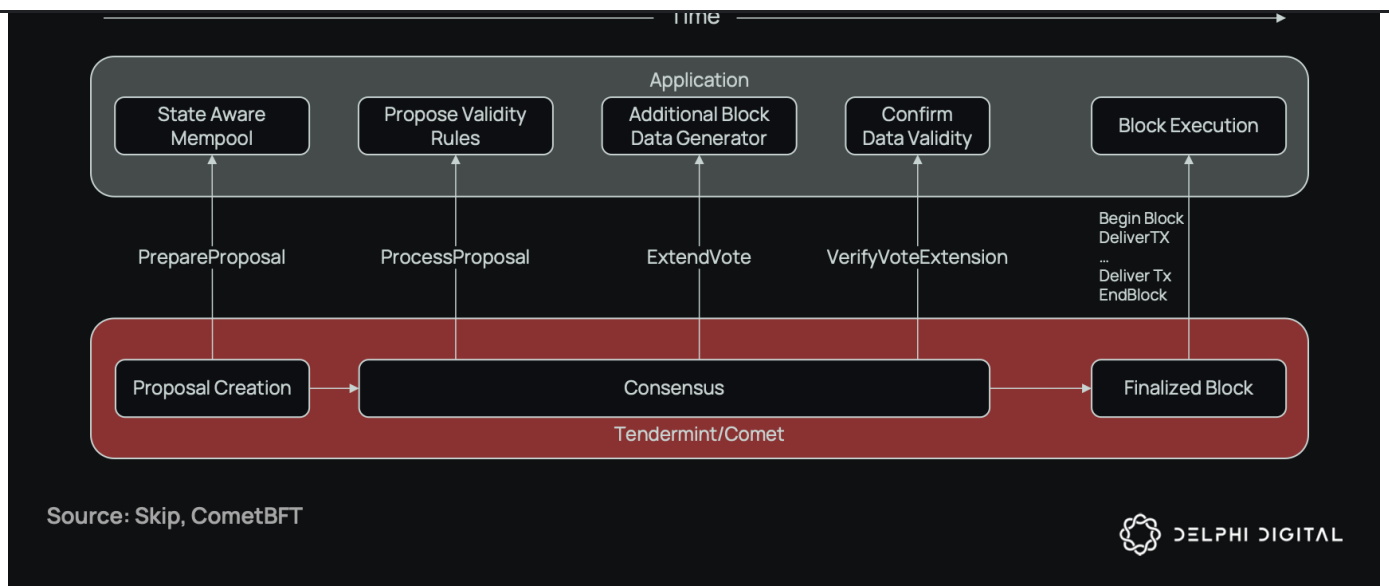
There are a few new steps added which enable the protocol-owned builder. Note that only PrepareProposal and ProcessProposal are live in the current Cosmos SDK build.

- **PrepareProposal:** Proposer asks the app what transactions it should include and in what order. The mempool here is actually *expecting* bundles, with two-dimensional transaction ordering for both bundles and top-of-block auctions.

- **ProcessProposal:** CometBFT asks the app how it should vote on the block proposed. Does it satisfy the validity rules? For example, the block proposal has, at most, one MsgAuctionBid (top-of-block auction) transaction, transactions are ordered by declining gas price, and no more than some max amount has been withdrawn over bridges (i.e., IBC). If any of these conditions fail, honest validators will reject the block proposal.

- **ExtendVote & VerifyVoteExtension:** Non-proposing validators have an opportunity to contribute other transactions or data. With *vote extensions,* validators can agree on things like oracle prices or use

Skip leverages ABCI++ for their new module x/builder, taking their out-of-protocol builder Sentinel and putting it in-protocol.

x/builder: Moving Sentinel In-Protocol With ABCI++

By moving the builder in-protocol, applications and developers retain full control and gain the ability to enforce more expressive preferences in how blocks are built and MEV is redistributed. It is also fully open source and transparent, so you do not need to trust the auctioneer (Skip) to run a fair auction. With the off-chain builder, validators don't see exactly how the auction is done and put trust in Skip to run it fairly. When it's in-protocol, this trust in Skip is removed, and validators can confirm that blocks are being built to the protocols' specifications and rules in a fully transparent way. Searchers still submit transactions the same way and governance can enforce MEV redistribution in consensus. Compare this to outsourcing block-building, where you cannot guarantee it is done exactly to your specifications, and external parties cannot be trusted to act for the benefit of the chain long-term.

Some of the features you can add to the builder are things mentioned before like top-of-block auctions and bundled transactions, but also consensus-enforced fee markets with consensus-forced ordering (instead of FIFO), app-aware fee markets to dynamically adjust gas prices depending on their importance to the app, top-of-contract auctions (allowing individual smart contracts to have their own top-of-block type auctions), and more advanced ideas like multiple block proposers and threshold decryption (will go into both below).
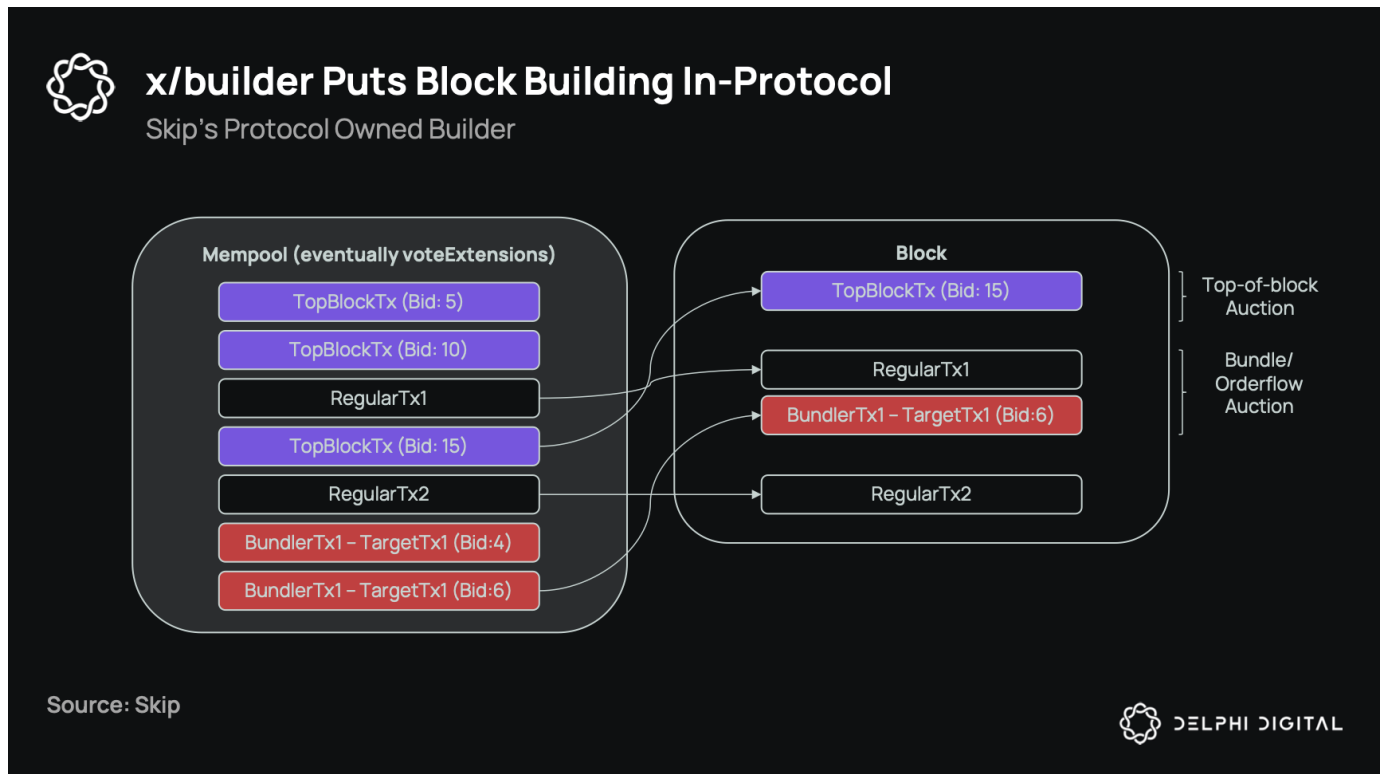
But to reiterate, with the out-of-protocol builder, the non-proposing validators would not see this level of granularity around the mempool, as it is entirely off-chain. All they would see is if the proposing validator proposed a valid block or not and accept or reject it. With the PoB, they can verify that the auction was run fairly and that the block was built to the protocol's specifications and rules. v1 of x/builder will take this functionality and apply it to contracts as well, along with more customizable fee markets to do things like transaction or MEV burning.

v2 and v3 are when we get into more granular things, but won't be enabled until vote extensions are live. The first of these is multiplicity, based off of a research paper from Duality that moves chains away from leader-based PoS. In leader-based PoS (the way every chain works today), the current block proposer chosen for a slot has a complete monopoly for that moment in time. You can read the paper for a more in-depth explanation,

send their own transactions/bundles as well and will not sign the proposer's block if they are not included. The costs for the colluding bidder to bribe multiple validators (vs. only the proposing one) is too high to be feasible. This idea has surfaced before, by Anatoly to build into Solana.
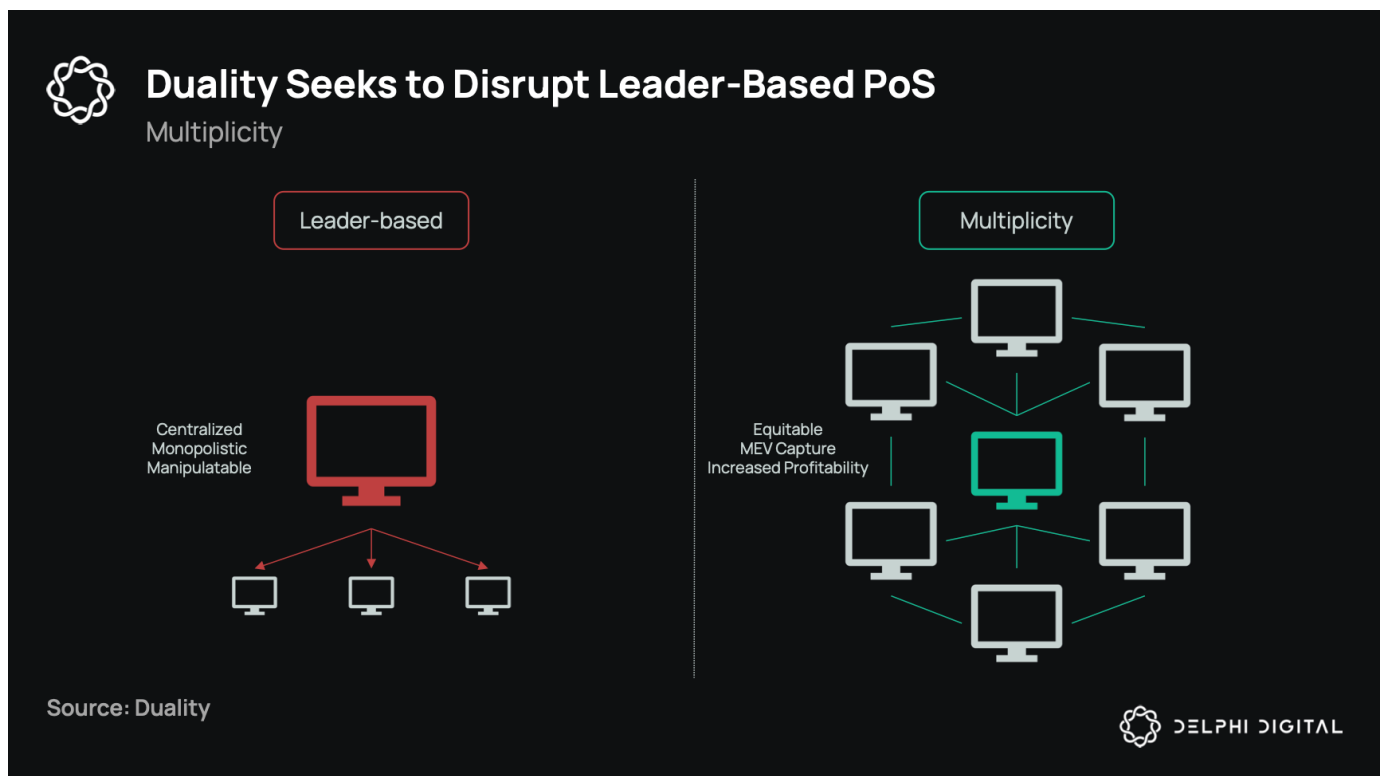
In v3, they aim to have support for threshold decryption. This is actually the origin of ABCI++'s development, as Osmosis wanted to add mempool privacy, something you cannot do with ABCI. Under this architecture, validators must commit to a set of transactions *before* information about them is known, and since Osmosis wants a top-of-block auction, they can't use an off-chain option like Skip Select because the ordering comes *after* inclusion.

Decrypting is done on-chain and requires validators to agree (with vote extensions) so you can't use an off-chain mempool and builder. Validators

been decrypted. Once decrypted, the block would run the auction for top-of-block and sort transactions by any other protocol rules that are enforced (e.g., by declining gas price). Crucially, since transactions have already been committed to, validators cannot insert new ones and will build the block with those committed.

In summary, the PoB is a way for appchains to exhibit their preferences for how blocks are built and how internal MEV is extracted, but it isn't limited to just mitigating internal MEV — it can help with external as well.

Interchain MEV: Solutions & Challenges

Cross-domain MEV is the new game in town. In Ethereum, discussions have mostly centered around SUAVE and/or shared sequencers. With SUAVE, you have this builder with a global view of many chains who builds blocks for all of them. This is centralizing by nature but with the goal of SUAVE itself being a decentralized block builder in the long-run (tbd). In the case of shared sequencers, they can give atomic *inclusion* but not *execution*, and again will have to deal with the likelihood of a centralized builder (whether SUAVE or otherwise) to build blocks for all chains using the shared sequencer.

With Cosmos, since there is little MEV on every chain, utilizing a global builder (i.e., PBS) would be undesirable. With the low MEV amounts, it's not practical for someone to build the infrastructure to be a builder on a single chain, they would want to build on *all* chains for it to be worthwhile. This could very quickly lead to a single builder with a monopoly building blocks on all chains. With PoB's, you do not get a global "interchain builder" and

Interchain Scheduler idea from the ATOM 2.0 whitepaper or Chimera chains from Anoma to commit to atomic cross-chain blocks.
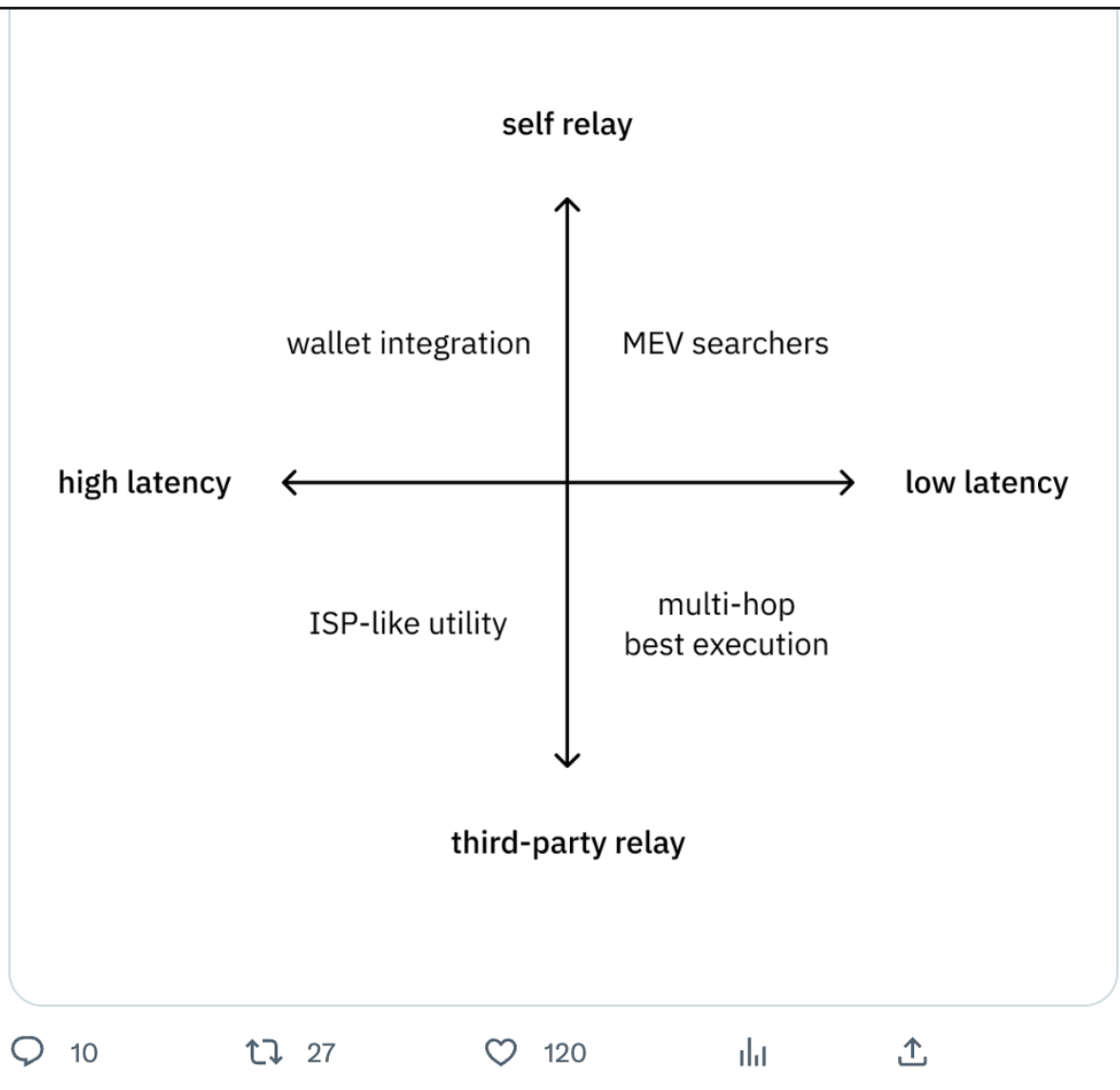
Near-Term: Relayer Incentivization & OFAs

Relayers are perhaps one of the more forgotten pieces of the Cosmos economy, yet they sit in a critical position. Relayers are the ones to send IBC packets (cross-chain messages) to one chain from another and are relied upon for liveness. As it stands today, this is a thankless job that relayers are not compensated for, but relayers receive useful information, especially when it comes to cross-chain swaps. To enable a more efficient market here, Skip, along with Mekatek and Composable, have collaborated on a cross-domain order flow market. By rewarding relayers with a portion of MEV, they are incentivized to relay both quickly and with the most competitive bid. The way it will work is as follows:

1. User submits cross-domain swap on Picasso (a Kusama parachain)

2. Swap is routed through XCVM (Composable's cross-chain VM) to their Hyperspace relayer

3. Relayer routes swap to Osmosis

4. Osmosis completes swap and backruns transaction

5. PoB sends some of the MEV to the relayer

Source: Skip, Mekatek, Composable Finance
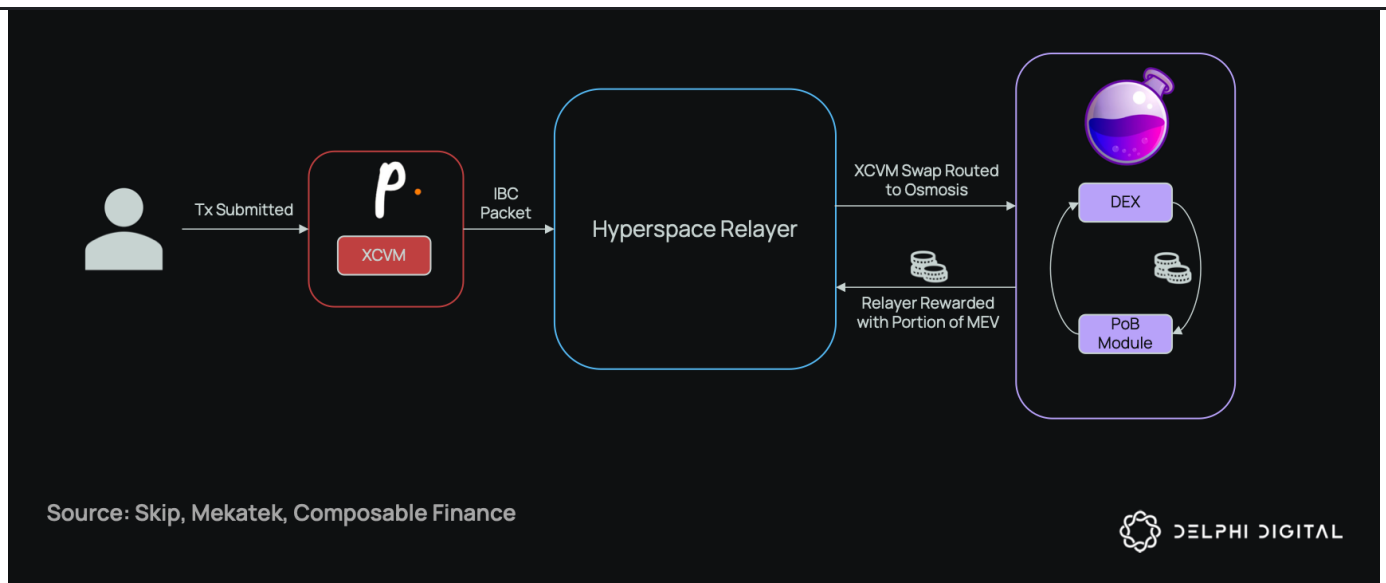
This architecture can be taken further, with relayers competing in top-of-block auctions or bundled transaction bids by sending cross-chain flow directly to the PoB. Sam Hart, who newly joined Skip from the ICF, has thought about the relay market before and how its future will evolve. MEV solves the majority of the relayer incentivization problem, there's just not a lot of it right now.

```
                            self relay
                                ↑
                                |
       wallet integration       |        MEV searchers
                                |
                                |
high latency  ←─────────────────┼─────────────────→  low latency
                                |
                                |
          ISP-like utility      |      multi-hop
                                |    best execution
                                |
                                ↓
                         third-party relay
```

💬 10   ⟲ 27   ♡ 120   ▫ili   ⬆

While the first relayer OFA collaboration is actually with a non-Cosmos chain, it is something you can expect to see become more built out in the Cosmos stack in the near-future.

Medium to Longer-Term: Blockspace Futures, Typhon, and Chimera Chains

In the medium to long-term, we can see things like cross-chain coordination with PoBs to agree on blocks. One idea is to do a version of the Interchain Scheduler from the ATOM 2.0 whitepaper. Chains could

incoming transactions from foreign chains.

In the longer-term, something utilizing Anoma's Chimera chains with their Typhon consensus could also make sense here. We won't go super into the details, but Chimera chains take advantage of the fact that there is large validator overlap between blockchains. We can use this overlap to get strong guarantees around cross-chain execution by having two separate chains commit to a joint-block for cross-chain atomic execution. This is essentially dynamic sharding, as both chains A and B would recognize this block on chain "AB" as their canonical, and then continue building blocks on their own chains independently after. A joint protocol-owned builder could be used here to satisfy both chains' rules, although more research will be needed.

Conclusion

If there's anything I would like the reader to take away from this piece it's this: **There is no single solution for MEV, and every appchain gets to create their own path, with full customization on how they build blocks and distribute MEV.** It's the idea of fine-tuned, granular local consensus vs. generalized, uncontrollable global consensus. When your chain specializes in a certain subset of tasks, it is much easier to create enforceable rules specifically tailored towards them. You do not need to outsource block building to a third party who will not build blocks specifically to your protocol's desires.

MEV throughout Cosmos is immaterial right now, but that is expected to change over the coming years as the ecosystem starts to grow. As value

Does your application control how its blocks are built?

Special thanks to Jose Villacrez for designing the cover image for this report and to Can Gurel and Brian McRae for editing.

Ceteris

Readers also enjoyed

	NFTs	May 15, 2023
	NFT Debrief - May 2023	
	By Yun Heng Lin	

	AMM	Mar 23, 2023
	Trader Joe's Novel Take on Concentrated Liquidity	
	By Joo Kian	

	NFTs	Mar 20, 2023
	NFT Debrief - March 2023	
	By Yun Heng Lin	

	Liquid Staking	Mar 08, 2023
	Brace Yourselves, Shanghai Is Coming	
	By Ceteris	

Delphi Shop   Research Plans   Research   Ventures   Labs   Analysts   Transparency