

FOLD v3: Return of the Relayoor

Content Disclaimer: No Financial Advice, for informational and educational purposes only.

[1]

- [ETH is the numinaire](#)
- [MEV Auction Platform](#)
- [New Block Structure](#)
- [Tokenising futures](#)
- [Tokenising futures](#)
- [New Block Structure](#)
- [Tokenising futures](#)
- [Tokenising futures](#)
- [Ensuring Orderly Market Operations](#)
- [Relay Service Protection](#)
- [Slashing Protection](#)
- [Relay Error Scenarios](#)
- [Relay Service Insurance Monitor](#)
- [Slashing Protection](#)
- [Relay Error Scenarios](#)
- [Relay Service Insurance Monitor](#)
- [Insurance Fee](#)
- [MEV Auction APY Gauges and mevETH Utility Token](#)
- [Summary](#)

Abstract

We introduce the reasoning behind not using ETH as the unit of account for providing network resource protection for the soon-to-be released MEV Auction Platform. We go into a high-level overview of the new MEV Auction platform, its benefits, and the needed protections to ensure LST (Liquid Staking Token) adoption. Furthermore, we then detail the differences between the originally proposed FOLD V2 protection proposal and the new V3 coverage proposal that utilizes FOLD as the underlying backstop asset and insurance collateral to be used in offering a Service-Level Agreement protection for Relay service disruptions for validators and LST node operators. We provide concluding remarks.

ETH is the numinaire

ETH as the shared unit of account only allows the network to price resources relative to each other and not in real terms based on the supply and demand for each resource. ETH being the native currency for the network is called the numinaire

[2]

We can further decompose this into two problems, coupled by the resource prices. One of these two problems is a simple one which can be easily solved on chain and represents the cost to the network for providing certain resources

, while the other is a maximal-utility problem that miners and users implicitly solve when creating and including transactions for a given block

. Correctly setting the resource prices aligns incentives such that the resource costs to the network are exactly balanced by the utility gained by the users and miners. This, in turn, leads to block allocations which solve the original 'ideal' problem, on average.

Why is this important? ETH being used for off-chain purposes such as what we propose would violate its properties as a numeraire as it has no way of being currently enshrined (i.e. enforcing at the protocol level) the proposed behaviour below. Additionally, adding FOLD for this usage does not compete with ETH for the proposed use case below as well as having other desirable properties for achieving the desired outcomes (e.g. Relay uptime, operational risk remuneration, etc) for ensuring relay adoption that will be required for the new MEV Auction Platform.

MEV Auction Platform

In a nutshell, it will differ from mev-boost in the following ways:

- It will split the block in two parts, which will be auctioned separately.
- It will implement a future market for blockspace.
- The mev-boost

API will be augmented by a new L2. No more custom APIs, JSON-RPC, etc.

Doing MEV will become as simple as using a dapp.

New Block Structure

We divide a block into two parts:

- One part, called a
- also referred to as above
- represents the top part of the blockspace. Economically, this is where competitive searchers want to place their transactions (e.g. for arbitrages etc.)
- The other part, called b
- also referred to as below
- represents the rest of the blockspace. Economically, this is where low-priority transactions - direct transfers, low volume swaps, some kind of intents, etc. - would go.

The rationale for this is simple: above

and below

represent two very different markets: The first serves strategic actors, whereas the second serves 'everyone else' - people not interested in speculation that just want to transact, e.g., to pay for stuff.

above

is a very time - sensitive kind of blockspace, as mev-rich transactions often come in last minute. As such, designing a futures market for above

is very hard, if not totally inappropriate.

On the other hand, below

is not very time sensitive, and designing a futures market for it is easier. The idea is this: Since we run our own validators, we will know 2 epochs in advance in which slots we will mint a block

. So, we can sell that blockspace about 2 epochs in advance, providing a futures market

for below

. We want users to be able to transact

, that is, to be able to resell the futures on a secondary market.

Additionally, we can extend this MEV Auction to external validators that exclusively use the new Manifold Relay

. Validators using the new Manifold Relay only need to change their currently configured relay's to use just Manifold's, with a backup relay endpoint also pre-configured to use Manifolds failover endpoint.

Economically, splitting the block in two parts makes sense as it fractures a market where different use cases are conflated: In a nutshell, currently builders have problems serving 'common people's needs' in Ethereum as they have to compete with

ultra-optimized searchers like Beaverbuild. On the other hand, strategic searchers like Beaverbuild often have to fill the block with 'strategically irrelevant txs' as they have to purchase more blockspace than they need.

It is clear that this homogenization is forced: Different players that want to do different things have to compete for the same thing. Fracturing the block solves this.

The newest breakthrough is that it blurs the differences between on-chain and off-chain infrastructure.

In a nutshell, we would like to spawn a centralized L2 where our sequencer is directly interfaced with our relayer.

The reason for doing this is that we want to give future purchasers the ability to transact. What if I buy a future, and then I find out that I do not have enough order flow to fill my calls? Clearly, I would like to resell it on some secondary market.

This secondary market will be detailed in a separate post. This is planned for v0.2 of the MEV Auction platform.

Tokenising futures

The easiest way to achieve this is by representing futures as tokens. These tokens are peculiar in that they allow the owner to do some operations like submitting transactions to be included in the b

block they refer to.

The standard we considered for tokenizing futures is ERC-1155

for the following reasons:

- Futures for different slots are not fungible.

As an extreme case, notice that an unused future for an already minted slot is worthless, whereas a future for a slot that still has to come certainly has value!

- Futures within the same slot are fungible.

This will be clarified below

, but if you suppose multiple futures can refer to the below

of the same slot, then they should be vastly interchangeable. This is because b

is not as sensible to ordering as a

is.

Ensuring Orderly Market Operations

Now that we have explained the high-level overview of the new MEV Auction platform, we can see that the relay provides a crucial service in both facilitating the auction and carrying the results of the auction. Without the Relay endpoint, buyers of the call options would not have a way of ensuring the execution of their position on the chain without also directly integrating with a supporting block builder. In this way, the Relay also acts as a sort of Sequencer's private mempool, providing a way for Searchers (or any user really) to bypass the need of directly submitting to a block builder if they wish.

This presents an obstacle however in trying to get external LST's to adopt the new MEV Auction platform without also exposing them to additional risk of using the new Manifold Relay as their exclusive relay endpoint.

Relay Service Protection

How can we protect validators that are participating in the new MEV Auction from faulty relay behaviour? Moreover, how do we prevent/remediate prolonged service outages, such as continuous slots with errors due to faulty relay behaviour?

Slashing Protection

The original FOLD Slashing Protection proposal was aimed directly at providing validator coverage from slashing. However, that implementation proposal had a few assumptions that made it difficult to scale. The assumptions such as:

- Manifold would have to run the validators to ensure operational standards
- Manifold could not extend coverage to anything other than validator protocol behaviour, meaning only attestation rewards were possible to provide coverage over.

This results in a situation in which:

- Manifold could only cover the validators it operationally ran.
- Manifold was unable to cover the downside risk that other LST Service Providers would potentially incur by exclusively running the new Manifold Relay.
- Manifold would only be able to cover situations that resulted in an undesirable slashing event, as opposed to a more broad service outage event.
- Call Market Options for future slots would be at risk of being un-executable due to service outage.

Relay Error Scenarios

There's several relay error scenarios:

1. Payload withholding: The relay doesn't release the payload and the proposer must forfeit the slot.
2. Incorrect payload:
 - a. Incorrect value: The final amount paid by the builder to the proposer was different to the amount claimed in the BuilderBid
 - b. Invalid block: Invalid data and/or Invalid fields.

Relay Service Insurance Monitor

Once a proposer calls submitBlindedBlock

to a relay (with a signed header), it depends on the relay to release the block to be able to propose anything^[3]

We use this interaction mechanism to provide a slashing protection mechanism from the relay itself, extending it to the validator set that is also participating in the new MEV Auction platform. This effectively provides the slashing protection that would result from a relay error, as well as additional protections and coverage to ensure relay adoption from other LST's for the new MEV Auction platform, without also exposing them to additional downside risk of the relay service going down.

1. Whenever mev-boost calls submitBlindedBlock to a relay, it also sends a request to the RSIM (Relay Service Insurance Monitor), including the SignedBuilderBid, the relay it originated from, and the submitBlindedBlock body.

1. The RSIM will also request the payload from the relay.

Thus, the RSIM can check:

- a. whether the payload is withheld
- b. whether the block matches the bid

If there is any problem, the relay's health check is being updated in the RSIM, and propagated to all connected proposers (via the registry). If the relay behaves incorrectly, all connected proposers can ignore the faulty relay for some time and revert to querying the other 'vanilla' relays.

This works as the auction platform is backwards compatible with mev-boost

.

Insurance Fee

APY is denominated in ETH, as it is earned by execution rewards

A 2.5% Fee on the gross APY earned by the MEV Auction platform is charged. The fee is distributed in three ways:

- A portion of the fee is re-invested back into the new mevETH Utility Token, in which Protocol Owned Validators are purchased in exchange for newly minted Utility Token positions representing the corresponding purchase.
- A portion of the fee is paid to lent/staked 80/20 ETH/FOLD or STABLECOIN/FOLD LP positions^[2:1]
- A fix portion goes to FOLD buybacks.

MEV Auction APY Gauges and mevETH Utility Token

The mevETH Utility Token earns the net APY earned by the MEV Auction platform, representing the surplus yield left after paying validators and the insurance fee. As an example, let's say the platform generates 0.7% additional APY, after the Insurance fee we would have 0.35% APY, with 0.1% going to validator APY and the remainder 0.25% APY going to mevETH Utility Token Gauges. The gauges are controlled by the Utility Token. Gauges are Protocol owned Validator

s, Protocol owned Liquidity

, and Protocol owned Treasury

. Gauges control how much and where these flows end up.

The Protocol Owned Validator Set

is agnostic to the underlying LST operator so long as certain criteria are met, such as multiple node operator support. This means, for example, stFRAX v2 can be used so long as Manifold Finance is the node operator for that validator set. The mevETH Utility Token can include LST's other than mevETH, which means participating LST's in the new MEV Auction Platform can reinvest their additional APY earned back into the platform, further providing positive feedback into the Protocol Owned Validator Set

flywheel.

Summary

The new Relay Service Insurance Monitor can observe any relay problem a validator could experience, and can tell all the other connected validators about problems with the relay. Thus, if the new relay causes a problem with one validator, all the other connected validators would immediately know, and would revert to using the normal MEV Boost Relays. This provides the needed downside risk protection for ensuring that the new MEV Auction Platform can be adopted by other LST's, such as FRAX[3:1]

, without placing the risk of adoption and risk of operational issue back on the adopting LST.

This provides a scalable way of providing protection for adopting the new MEV Auction Platform for LST's while minimizing the risk of adoption and maximizing the APY earned by adopting it for participating LST's.

The new V3 Coverage system provides a way for the protocol to approximate a fee proportional to the value of the transaction for providing and ensuring Relay service performance and outage compensation to validators, and surplus accrual is distributed to its respective token holders. The insurance coverage is proportional to the transactional value of the new MEV Auction platform for all participating validators, regardless of the underlying LST that the validator is operating under.

This makes the new FOLD coverage protocol (formerly known as FOLD v2) incentive aligned to protect at a minimum the proportional value of the transactions that the new MEV Auction platform facilitates.[4]

Protocol activity → token value

1. [legal/active/disclaimer/CONTENT_DISCLAIMER.txt at master · manifoldfinance/legal · GitHub](#)↵
2. LP Position should approximate ETH price volatility.↵ ↵
3. <https://frax.com> ↵ ↵
4. The new mevETH Utility Token can be utilized by participating LST's and thus is unable to facilitate this use case for the protection of the relay, Additionally FOLD is a fully diluted and fixed-supply token. ↵