CIP: title: Reduced bonding requirements author: fleupold status: Draft created: 2024-05-13

Simple Summary

In order to become a solver on CoW Protocol, parties have to be vouched for by a so-called bonding pool, as specified in CIP-7. These pools provide significant guarantees ($500k in stables and 1.5M COW) to the protocol and may get slashed by CoW DAO in case of misbehavior by one of its associated solvers.

While there are 20 solver solving on CoW Protocol today, there are only two bonding pools covering those solvers:

1. A Gnosis DAO sponsored bonding pool (vouching for 6 solvers)
2. A CoW DAO sponsored bonding pool (vouching for 14 solvers)

Gnosis DAO is currently not accepting new external solvers to join and CoW DAO's bonding pool poses some requirements and limitations under which solvers have to operate.

The goal of this proposal is to introduce a new type of setup with reduced bonding requirements which will incentivize more solvers to become bonded using their own resources, while maintaining existing security guarantees and allowing solvers to have more control over aspects of the competition they currently lack.

In this new setup solvers can get the right to manage their settlement submission private keys without passing any due diligence checks, thus providing a more permissionless experience while remaining capital efficient.

Motivation

The goal of this proposal is to foster decentralization, accelerate CoW DAO's ability to deploy on new networks, improve the reliability of service while allowing for competition and innovation on more advanced aspects of the auction (ie. solution settlement).

Let's revisit CoW Protocol's off-chain architecture:

[

1600×830 113 KB

](https://europe1.discourse-cdn.com/business20/uploads/cow/original/2X/6/6155d766ebc353e8c42bf0a2798f5bf48e9542c7.png)

The core protocol consists of the orderbook (which quotes and receives signed orders from users) as well as the autopilot, which prepares auction instances and facilitates the competition evaluation process.

External solvers then can conceptually be split in two parts:

1. The solver engine, whose task it is to compute the optimal solution to the batch auction instance at hand.
2. The driver, which

a. pre-processes the auction (potentially filtering orders and fetching extra liquidity)

b. posts the winning solution back to the autopilot, and if selected, encodes and executes the settlement on-chain

It is important to note that the driver requires access to the private key with which solutions can be submitted on-chain.

Let's now look at the possible attacks a solver can perform:

1. Losing settlement contract's internal token balances through e.g. settling trades with excessive slippage, setting bad allowances on an external protocol, etc.
2. Submitting a settlement for an auction they didn't win or which doesn't match the settlement they proposed during the auction

While the risk of 1. is manageable by doing frequent withdrawals of buffers and "only" affects DAO resources (no user funds are at risk), 2. could potentially lead to users being systematically executed at their limit price (rather than at the fair uniform clearing price).

The damage that can be inflicted in this case depends on the limit prices (or surplus) as well as the number of trades that are exploited until the solver is deny-listed and has no strict upper bound.

Because of that, CoW DAO bonded solvers have so far not had access to their own private keys. Running their own driver

would require them to create their own “full” bonding pool. Due to the large amount of capital required for that, this proposition hasn’t found any traction so far.

This proposal introduces reduced bonding requirements with which solvers are able to run their own driver while maintaining reasonable security guarantees for the protocol and its users. As mentioned above the benefit of doing this are manifold:

Foster Decentralization & Improve Reliability

CoW DAO believes that permissionless innovation will outcompete gated and permissioned systems in the long run. Reducing capital requirements reduces the barrier to entry for new solvers. It also removes centralization points, which have been partially responsible for outages and downtimes in the past. We believe that heterogeneous implementations of the liquidity indexing, order filtering and solution submission logic will make the protocol more robust against single points of failure.

Accelerate Scaling

CoW Protocol is currently only deployed on Mainnet and Gnosis Chain. Given the amount of off-chain infrastructure that currently needs to be deployed and maintained by the development team in order to add a new network, there is a limit to how fast we can expand the protocol to more chains.

Having fully co-located driver/solver-engines would simplify this work tremendously and only require a sufficient number of solvers to signal their willingness to support that chain.

Increase Competition

Solvers already compete on liquidity as well as optimal matching strategies in order to give users the best deal possible. However, we believe that there is significant room for additional innovation when it comes to things like prioritizing which orders to include in the search, how to encode settlements in the most gas efficient way and also how to make sure a winning settlement gets included on-chain quickly and efficiently. For instance, solvers could wrap the settlement transaction in a transaction bundle containing other public mempool transactions, which are ordered in a way to give users even better execution (ie. by including non CoW Protocol trades in the opposite direction first).

Specification

Introduce a new reduced bonding requirement with a minimal initial deposit of (rationale for these amounts can be found in the section below):

- $50k in yield bearing stable coins or ETH
- 500k COW

And a target deposit of:

- $100k in yield bearing stable coins or ETH
- 1M COW

The right to iterate on the set of eligible tokens (as well as define conversion rates for non stable tokens) shall be granted to the development team.

Solvers that have provided the minimal initial deposit of $50k/500k COW are required to submit their solutions via the MEV Blocker RPC and have any refunds as well as 50% of their COW rewards go towards increasing the size of the bond until the target is reached. Solvers have to reach the target deposit within 1 year.

Solvers that have provided the minimal initial deposit of $50k/500k COW are allowed to submit solutions from their own submission account provided they can provide a signature which will be given out by the autopilot attesting to the fact their solver indeed won the competition.

For this, the development team will build and deploy a settlement contract facade, which itself can get allow-listed as a solver on the main settlement contract (GPv2Settlement). The facade will take the calldata required to call settle

on the main contract as well as a signature.

It then checks the following things:

1. The signature is indeed authored from the autopilot
2. The signature has been granted to the msg.sender

3. The signature attests to certain aspects of the settle

payload (ie. orders that are included, clearing prices, a subset of pre/post interactions)

and then forwards the call to the main settlement contract.

[

1600×805 106 KB

](https://europe1.discourse-cdn.com/business20/uploads/cow/original/2X/3/3ca82bcd5a74181c80c210069524e12d496372b8.png)

To further decentralize the system, such an “attestation” model could also be adopted by other independent parties that provide the “full bonding pool” (not just CoW DAO) and would like to define custom requirements for the participants of their pool.

Transition Period

We believe that building, auditing and testing the required on-chain verifier and off-chain signature logic may require a few weeks of development work. At the same time we would like to start testing co-located driver/solver-engines as soon as possible to identify other challenges and make progress toward co-located launches on L2s.

We therefore suggest that existing solvers, that have been part of the CoW DAO bonding pool for more than 6 months, and that pledge the initial minimal bonding requirements are allowed to run in co-located mode even before the autopilot signing has been implemented. They will be required to transition to signature provided settlements as soon as the system is ready.

Work to build a robust circuit breaker which can deny-list solvers in case of detected misbehavior has already started and is a requirement for the transition period.

Rationale

The introduction of the signature verifying contract allows the protocol to limit the damage a misbehaving solver can have on users (e.g. settling their order out of competition at limit price) by attesting to certain key aspects of the competition, while still giving solvers freedom to manage solution submission and other crucial aspects of running the driver.

The reduced bonding requirements are still large enough to cover any damages for misbehaviors described in point 1 above (loss of settlement contract funds) given the current withdrawal frequency of accrued funds. Misbehaviours of type 2 (settling out of competition) are mitigated by introducing the required attestation from the autopilot which will only be given out to the winning solver. The COW portion of the bond ensures continued incentive alignment between solvers and the DAO.

At the cost of extra settlement overhead (gas for signature verification and extra call), these reduced requirements keeps the DAO’s risk exposure neutral to the current status quo, while giving solvers additional incentive to work towards creating their own bonding pools.

The transition period makes sure we can move fast with already well established solvers to identify technical requirements beyond the ones already mentioned in this proposal. This will accelerate the speed with which CoW Protocol can be deployed to other chains.