Free-Riding Prevention

A potential vulnerability in any decentralized system is the risk of free-riding, where one party seeks to gain the outcomes of a shared effort without contributing its fair share of work. In the context of our decentralized inference system, this would manifest as a node waiting for others to submit inference results, then copying and submitting those results as their own, thereby conserving their computational resources illegitimately.

To mitigate this risk, we have designed a unique security mechanism that divides the second transaction phase into two distinct sub-phases, each with its transaction: the Commit phase and the Reveal phase.

The Commit Phase

In the Commit phase, nodes in the inference committee must submit a cryptographic commitment of their inference results. This commitment is a one-way hash of the result combined with a secret nonce, providing a way to lock in the result without exposing its content, i.e., H(m||r), where H is the hash function, m is the result, and r is a random nonce.

The commitment ensures that the node has performed the computation and is ready to reveal the valid result. This phase has a specified timeout limit within a fraction of the slot duration. Failure to submit a commitment within this window results in the node being ineligible to reveal its results and facing a penalty.

We list the detailed off-chain and on-chain algorithms for the commit phase

The Reveal Phase

Following the Commit phase, the Reveal phase allows nodes to disclose their previously committed results. Each node must reveal both the result m and the nonce r used in the commitment, allowing others to verify the hash against the commitment made in the previous phase. This phase also has a timeout limit, and failure to reveal on time, or a different result from what was committed, will result in punitive measures against the offending node.

The introduction of the Commit/Reveal scheme effectively prevents free-riding by ensuring that each node provides evidence of its contribution before any results are made public. This two-step process requires nodes to stake their claim on an outcome without knowledge of other nodes' work, thus ensuring that each node contributes independently.

By employing a cryptographic commitment scheme, we create a trustless environment where work cannot be copied, and honesty is enforced through the threat of penalties.

These penalties for non-compliance act as a strong deterrent against malicious activity, helping to maintain a fair and secure environment for all participants. The Commit/Reveal protocol guarantees that only nodes that genuinely perform the computations are rewarded, thereby upholding the integrity of the decentralized inference process and protecting the system from exploitation.

This careful orchestration of transactions and timings ensures that our network remains resilient, efficient, and free from the inefficiencies and unfair practices that free-riding would introduce.

We list the detailed off-chain and on-chain algorithms for the reveal phase.

Previous
Robust Inference Committee Selection

Next
Aggregation of Inference Results

Last updated 1 month ago