Model Inference Querying

On Nesa, each computational node is assigned a public-private key pair, serving as their identity to secure its participation in the network's inference processes. Node selection is organized using a framework of slots and epochs, similar to how validators' attestation duties are arranged in ETH2. At the onset of each slot, the highest-priority inference request in the queue is identified. Each node then utilizes its private key to invoke the VRF's (Verifiable Random Function's) evaluate function, generating a random number unique to that node but consistent across evaluations. This random number is used to determine the node's eligibility to be part of the inference committee for that particular slot.

Free-riding Prevention during Inference

To mitigate risk, Nesa has designed a security measure that divides the second transaction phase into two distinct subphases. 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 with-out exposing its content.

> Free-riding is a potential vulnerability of decentralized systems where one party seeks to gain the outcomes of a shared effort without contributing its fair share of work.

In the Reveal phase, nodes are permitted to disclose their previously committed results. Each node must reveal both the result and the nonce 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 revealing a different result from what was committed, will result in punitive measures against the offending node. In this