☰   Nesa   🔍

Robust Inference Committee Selection

A fair and secure method for selecting the inference committee is critical to maintaining the integrity and trustworthiness of our decentralized inference system.

To facilitate this, we incorporate VRF as the means for random yet deterministic committee selection, drawing inspiration from the organizational structure of duties within Ethereum 2.0 (ETH2).

The Role of VRF in Committee Selection

On Nesa each computational node is assigned a public-private key pair (pk, sk). These cryptographic keys serve as the node's identity and secure its participation in the network's inference processes. The nodes are responsible for executing AI tasks, and their 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 (sk) to invoke the VRF'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.

Transparent and Verifiable Committee Formation.

Thanks to the cryptographic guarantees of the VRF, the selection process is both unpredictable to prevent gaming the system and independently verifiable to ensure transparency. Every node in the network, alongside the governing smart contracts, can verify the validity of the VRF proof.

This serves as evidence that a node has been legitimately chosen to serve on the inference committee. If a node attempts to submit an inference result without a valid VRF proof or if it was not selected for the committee, the system is designed to enforce penalties akin to slashing in ETH2. This punitive measure serves as a deterrent against malicious behavior and safeguards the system's integrity by ensuring that only legitimately selected committee members can contribute to the inference process and be rewarded for their work.

Nesa has designed this VRF-based selection mechanism to instill confidence in the fairness and security of the committee formation process while upholding the decentralized nature of our network. By integrating such a robust selection protocol, we ensure that our system is resilient against manipulation and that the responsibilities of AI computation are distributed across a diverse set of participants, enhancing the overall reliability and credibility of the inference outcomes.

Previous
Bificurated Inference Ledgering - The Two-Phase Transaction

Next
Free-Riding Prevention

Last updated 1 month ago