



Playground

Technology

Research

Token

Docs

Developers

DNAX



# Trustless AI Oracle

ARTIFICIAL INTELLIGENCE

As a trustless AI oracle network, a critical step in Nesa's decentralized inference system

[Playground](#)[Technology](#)[Research](#)[Token](#)[Docs](#)[Developers](#)[DNAX](#)

default majority vote strategy within a smart contract.

# Oracle Aggregation of Inference Results

Any submitted result that does not align with the majority is flagged as faulty. The node responsible for a faulty result is subject to a penalty. This could manifest as a loss of a security deposit (slashing), a reduction in reputation score, or both.

This majority vote strategy ensures that the aggregated result reflects the consensus of the committee, thereby reducing the likelihood of erroneous outcomes due to individual node failures or malicious behavior.

Once the official result is determined and faulty nodes are penalized, the smart contract finalizes the result and triggers the appropriate reward distribution to the nodes that contributed to the majority result. Rewards are allocated as per the pre-defined incentive structure as dictated in the smart contract, balancing the costs incurred by nodes and incentivizing continued honest participation in the system. The oracle reports the decision back to the network.

Customized aggregation strategies are also offered by Nesa and can range from simple methods like majority voting or averaging to more complex techniques such as averaging with outlier removal. This is helpful when certain use cases may demand more tailored approaches.

The AIVM implements the following verification methods to ensure reporting is accurate

[Playground](#)[Technology](#)[Research](#)[Token](#)[Docs](#)[Developers](#)[DNAX](#)

expected range of results. b) Publicly Checkable Proof: Similar to approaches used in academic works like TownCrier, the model owner can require nodes to produce zero-knowledge proofs or leverage trusted hardware attestations to publicly verify the correctness of their computations. c) Outlier Quota and Proof Submission: Each node is assigned an outlier quota, limiting the number of times it can deviate from the consensus results before it is required to submit a proof of computation. If a node exceeds its quota, it must provide such proof to maintain its standing in the network and avoid penalties.



[Playground](#)

[Technology](#)

[Research](#)

[Token](#)

[Docs](#)

[Developers](#)

[DNAX](#)

[COPYRIGHT 2024 NESA FOUNDATION](#) [GITHUB](#)

[CAREERS](#)

[TEAM](#)

[TERMS](#)

[PRIVACY](#)

[CONTACT](#)