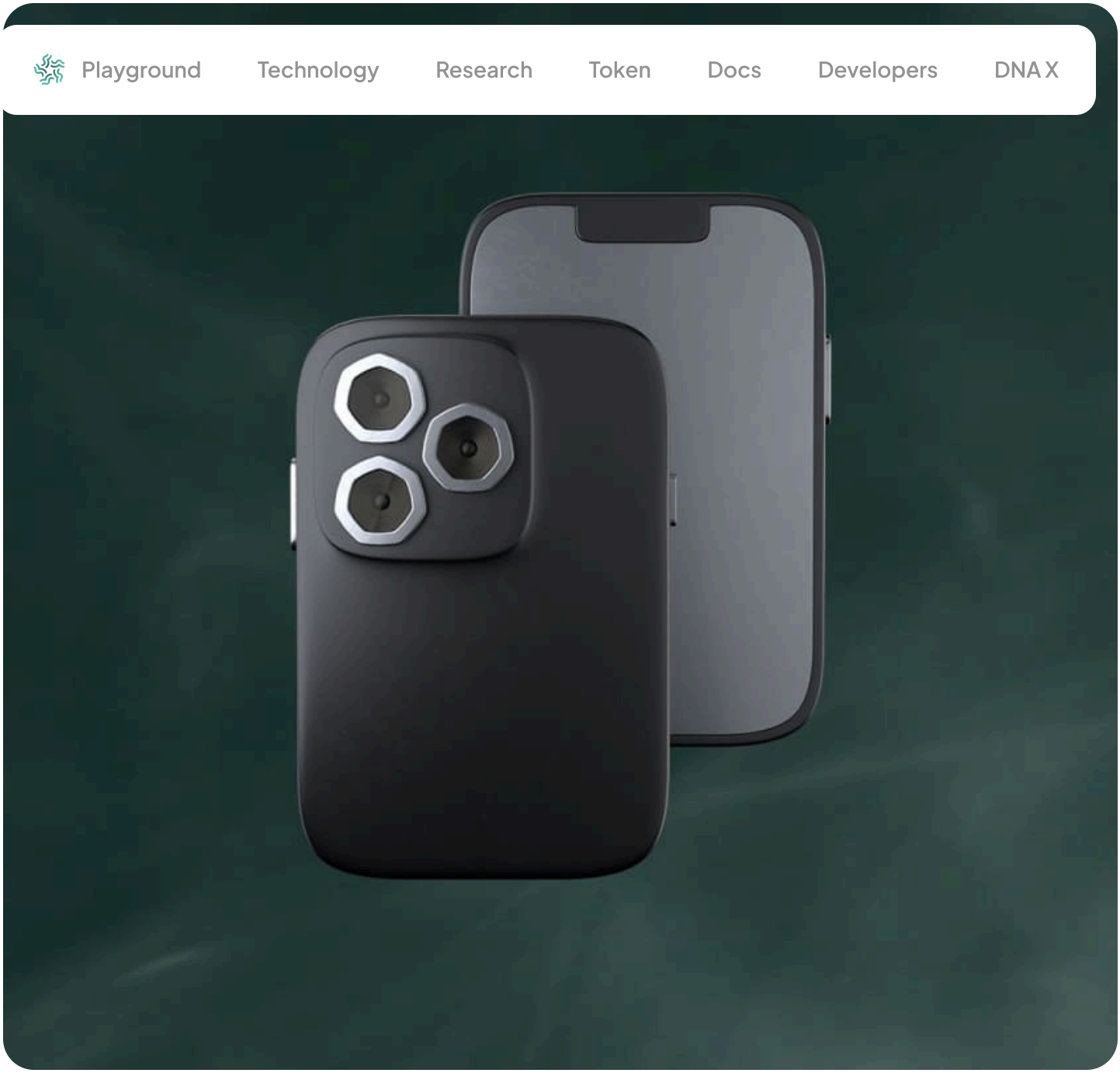

Decentralized Hardware

INFRASTRUCTURE

To address the challenges of privacy and verifiability, Nesa integrates a hardware-based solution, leveraging specialized hardware with enhanced security features for both CPU and GPU to fortify computation nodes. Some nodes in the network are designated as enhanced nodes equipped with Trusted Execution Environments (TEEs),which offer a secure enclave for processing sensitive data, protecting the user's input from exposure while still enabling computation.

Specialized Secure Hardware

To ensure that enhanced nodes with Trusted Execution Environments (TEEs) are trustworthy and properly configured, Nesa implements an attestation protocol similar to the decentralized trust mechanisms present in Chainlink's oracle network.

> This attestation process is critical as it not only provides the assurance that the TEE is genuine and secure but also serves as the initiation protocol for new nodes entering the system.

Besides the hardware requirement, Nesa relies on a threshold crypto system, because the user submits a request that is publicly accessible, hence the request should contain encrypted information that can be decrypted (in secure memory) by a randomly selected committee.