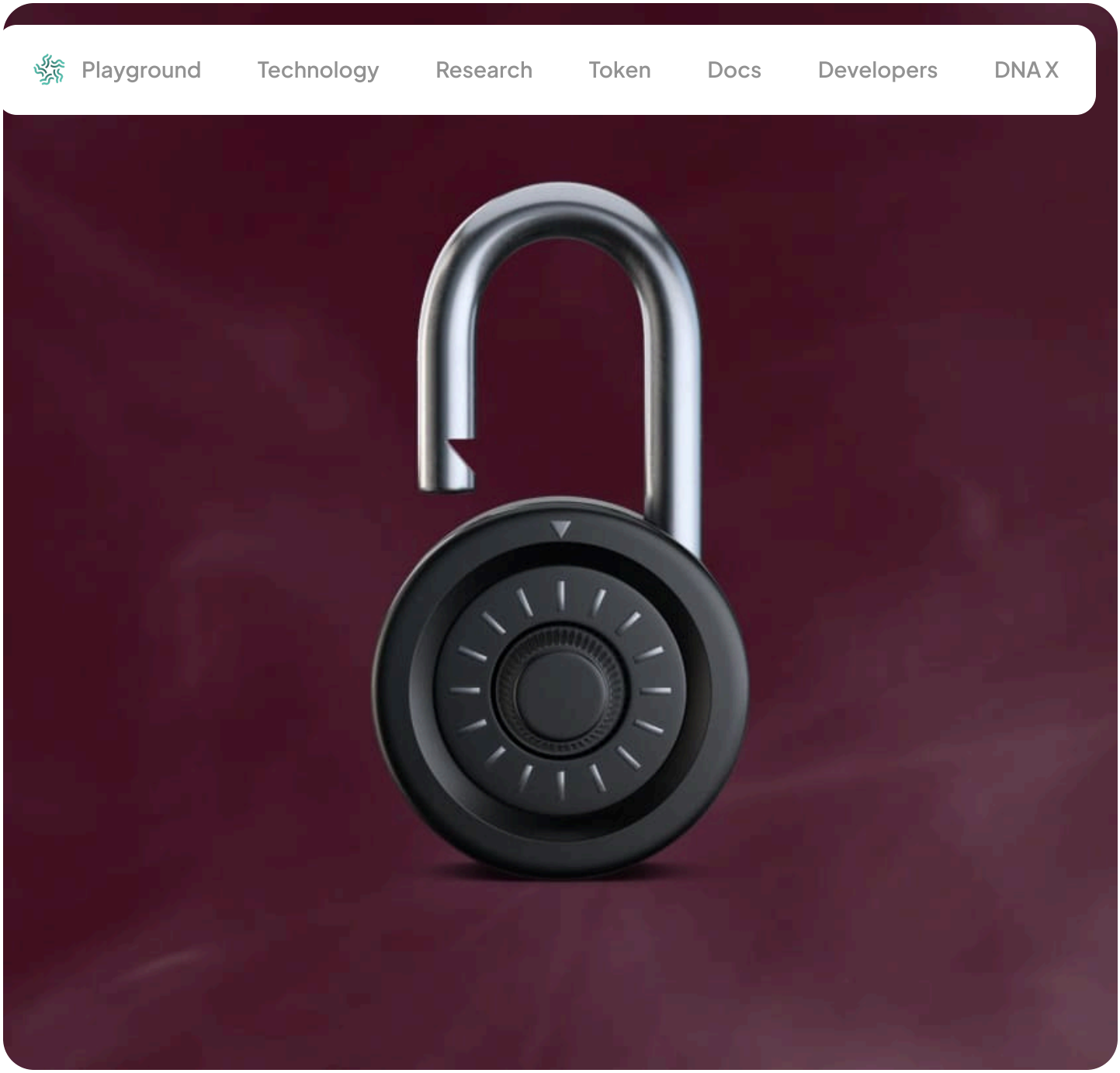

Cryptographic Privacy

CRYPTOGRAPHY

Nesa's cryptography-based design allows users to encode their sensitive input data into a

When nodes receive their respective shares, they perform computations on this fragmented data without the ability to reconstruct the original input individually.

ZK Proof Engine with VRF

Through this process, nodes collaboratively engage in the computation of the AI inference task using an SMPC protocol, where each node contributes its computational power while the data remains distributed and confidential.

> ZK Proof is implemented when Nesa needs to verify that nodes have correctly performed their part of the secure multi-party computation without revealing the underlying data or model parameters.

Nesa strategically incorporates ZKP-based verifiable computation for use cases where the model complexity and inference task size allow for the practical application of these advanced, albeit computationally heavy, cryptographic methods. This selective integration ensures that Nesa continues to offer enhanced privacy and verifiable computation where feasible, without disproportionately affecting the system's overall throughput and performance.