How It Works

Every coin flip on Spinx is provably fair and can be verified directly on the Solana blockchain.

Game Account (PDA)

The on-chain record of the flip. It shows who created the challenge, who joined, how much was staked, and the linked VRF request.

Vault Account (PDA)

The escrow account that holds the staked tokens. You can confirm that the tokens were locked before the game and released only after settlement.

Randomness Proof (VRF)

A request handled by the official ORAO VRF program. When fulfilled, it contains the random number used to decide the flip.

- You can check that the account is owned by the ORAO VRF program (so no one else could have generated it).

- The random value stored here is the one our contract used.

- Rule: randomness % 2 $\rightarrow$ 0 = Heads, 1 = Tails.

Together, these three links let anyone confirm:

1. Tokens were really staked.

2. The result was decided by ORAO's verifiable randomness.

3. The winner was paid out automatically by the contract.