About Spinx

1. Introduction

Spinx is a decentralized peer-to-peer (PvP) casino platform on the Solana blockchain.
The first game is Coin Flip, where two users stake SPX tokens and a winner is chosen using verifiable randomness (VRF) provided by the official ORAO VRF program.

Spinx is:
- Non-custodial: funds are never held by Spinx.
- Provably fair: outcomes are verifiable on-chain.
- Transparent: all state and results can be inspected with standard Solana explorers.

2. Key Principles

- Non-custodial: Tokens are locked in program-derived vaults until settlement or cancellation.
- Provably fair: Outcomes are based solely on ORAO VRF. Randomness and results are publicly verifiable.
- Automatic settlement: The program pays the winner directly, without human intervention.
- Open verifiability: Game state, vault balances, and VRF requests are all on-chain.

3. SPX-Only Participation & SOL Requirement

Challenges on Spinx can only be created and joined with SPX tokens.
Users must also hold a small amount of SOL to pay network transaction fees and the VRF request cost.

This design concentrates platform utility into SPX: if demand for the platform grows, participation requires SPX, aligning utility with token holders.

⚠️ No outcomes or returns are guaranteed. SPX is a utility token, not investment advice.

4. How Spinx Works

4.1 Create a Challenge
A user creates a coin flip challenge by staking SPX tokens. The tokens are moved into a program-derived vault account (PDA).
A protocol fee of 0.005 SOL is charged at creation. The challenge stays open until someone joins or the creator cancels.

4.2 Accept a Challenge

Another user joins by staking an equal amount of SPX tokens. A protocol fee of 0.005 SOL is charged at acceptance.
The program submits a request to ORAO VRF to obtain the random value that will decide the outcome.

4.3 Settlement (Verifiable Randomness)
ORAO VRF fulfills the request and writes randomness to a request account. The Spinx program computes the outcome deterministically:
randomness % 2 → 0 = Heads, 1 = Tails. The vault balance is automatically transferred to the winner's wallet.

4.4 Cancellation
If no opponent joins, the creator can cancel and withdraw their SPX tokens from the vault.

5. Verification (On-Chain Proofs)

Every game can be independently verified by anyone:
- Game Account (PDA): On-chain record of participants, stakes, status, and VRF request reference.
- Vault Account (PDA): Escrow holding the staked SPX tokens while the game is active.
- VRF Request Account: Owned by the ORAO VRF program, contains the randomness used.

Spinx provides direct explorer links to these accounts so users can confirm staking, randomness, and settlement independently.

6. User Experience

- Active Listings: Shows open challenges. Each listing displays the creator's wallet and a link to the vault PDA so users can confirm tokens are staked.
- Completed Challenges: Available via filters. Each entry includes links to the Game PDA, Vault PDA, and VRF request (randomness proof).
- Profile Dashboard:
  - Shows SPX and SOL balances.
  - Displays live challenges created by the user (with cancel option).
  - Provides history of created/joined challenges with win/loss results and verification links.

7. Fees

- 0.005 SOL fee on challenge creation.
- 0.005 SOL fee on challenge acceptance.
- Users must also pay normal Solana network fees and the VRF request cost in SOL.

Keep a small amount of SOL in your wallet at all times.

8. Security Model

- Non-custodial: Spinx never controls user private keys or wallets.
- Escrow: SPX tokens are locked in vault PDAs; payouts are executed by the program.
- Randomness integrity: Only the official ORAO VRF program can fulfill randomness requests.
- Determinism: Settlement runs once per game and uses a simple, auditable rule.
- Transparency: All state is on-chain and can be reconstructed from accounts and logs.

9. Open Source & Verification

Spinx smart contracts are open-sourced.

- The GitHub repository (link to GitHub repo) contains source code, documentation, and build artifacts.
- Anyone can review the code and verify deployed binaries by rebuilding and comparing hashes with the on-chain program.

10. Getting Started

1. Connect a compatible Solana wallet (e.g., Phantom, Solflare).
2. Ensure you have:
   - SPX tokens (to create or join challenges).
   - A small amount of SOL (for network and VRF costs).
3. Create a challenge or join one from the Active Listings.
4. After settlement, use the provided links (Game PDA, Vault PDA, VRF request) to verify fairness.

11. Disclaimers

Spinx is a decentralized application.

- Users are responsible for complying with local laws and age restrictions.
- Gambling carries financial risk — only stake what you can afford to lose.
- SPX is a utility token used for platform participation. No outcomes, profits, or returns are guaranteed.