Spinx: A Decentralized, Provably Fair Casino on Solana

Abstract

Online gambling today relies on centralized platforms that require players to trust custodians for fund safety and fair outcomes. Such systems are opaque, subject to manipulation, and vulnerable to custodial risk. Spinx proposes a fully decentralized PvP casino built on Solana, where outcomes are determined by verifiable randomness (VRF) and funds are held in program-owned vaults. This ensures that results are provably fair, transparent, and non-custodial.

1. Introduction

Conventional online casinos suffer from three critical flaws:

1. Custody of funds: Players must deposit into centralized wallets, exposing them to theft, insolvency, or frozen accounts.

2. Opaque randomness: The process of deciding outcomes is hidden, allowing potential manipulation.

3. Unverifiable execution: Players cannot independently confirm that games are executed as promised.

Spinx eliminates these flaws by decentralizing custody, randomness, and settlement.

2. System Overview

Spinx is deployed as a Solana program with the following properties:

- Non-custodial: Tokens are locked in program-derived accounts (vaults).

- Verifiable randomness: Game outcomes are based solely on ORAO's VRF, which produces randomness that is publicly verifiable on-chain.

- Automatic settlement: Payouts are executed directly by the smart contract.

- Public verifiability: All game states, vault balances, and randomness proofs are stored on-chain and visible via standard Solana explorers.

3. Coin Flip Game Mechanics

1. Challenge Creation

- A user initializes a CoinFlip account, escrowing tokens into a vault account derived by program seeds.

- The game remains open until an opponent joins.

2. Challenge Acceptance

- A second user joins by escrowing an equal amount of tokens.

- The program then issues a randomness request to ORAO VRF.

3. Randomness and Settlement

- Upon fulfillment, ORAO VRF writes randomness into the VRF account.

- The Spinx program consumes the randomness, applying randomness % 2 to determine the winner.

- The vault pays the winning player automatically.

4. Cancellation

- If no opponent joins, the creator can withdraw their tokens.

4. Verification Model

Each completed game can be independently verified by any user:

- Game Account (PDA): Stores creator, opponent, stakes, and VRF reference.

- Vault Account (PDA): Confirms tokens were locked during the game.

- VRF Request Account: Owned by the ORAO VRF program, containing the randomness value used.

- Deterministic Rule: Outcome = randomness % 2.

Verification requires no trust in Spinx or any operator—only in the cryptographic guarantees of VRF and Solana’s consensus.

5. Security Considerations

- Custody: Users never deposit to Spinx-controlled wallets; all funds are escrowed in PDAs derived by the program.

- Randomness integrity: Only ORAO’s VRF program can fulfill randomness requests; settlement validates the VRF account ownership and fulfillment status.

- Fair execution: Settlement logic is deterministic and idempotent, preventing double execution.

- Transparency: Users can reconstruct full game history from logs and accounts on-chain.

6. Conclusion

Spinx demonstrates that online gambling can operate without custodians, opaque logic, or unverifiable randomness. By combining Solana’s high-throughput blockchain with verifiable randomness, Spinx establishes a transparent, provably fair system for decentralized gaming.