LOTS Protocol - Smart Contracts Overview

This document provides a high-level overview of the two main smart contracts used in the LOTS Protocol:

1. LotsCycleManager
2. LotsMLInv (LOTS Token)

These contracts are deployed on the BNB Smart Chain and are designed to operate autonomously, securely, and transparently with no custodial control or financial guarantee.

1. LotsCycleManager

This is the core logic controller of LOTS. It manages:

- Ticket assignment and participant registration.
- Verification of registration before allowing randomness.
- Lifecycle control of each "cycle" (start, randomness, distribution, end).
- Payout distribution in tiers (first, second, silver, golden).
- Emission of events for transparency and indexing.
- VRF-based randomness using Chainlink VRF v2+.
- Signature validation using ECDSA and nonces.
- Access control with 'onlyOwner', 'onlyAllowed', and 'onlyDApp' modifiers.
- Geo-compliance and emergency pause options.

2. LotsMLInv (ERC-20 Token)

This contract:

- Implements a standard ERC-20 token with added burn and transfer rules.
- Includes `burnAllTickets()` and `burnTokens()` for token lifecycle control.
- Transfers LOTS reward balances with `transferFromLotsAccumulated()`.
- Supports the reset of sale cycles via `restartSale()`.

- Maintains a secure list of allowed caller contracts.

It does not collect user data or store any participant identity. All logic is governed on-chain.

Security & Audit Notes

- Both contracts follow OpenZeppelin standards.
- Chainlink VRF ensures verifiable randomness.
- Access to sensitive functions is limited by signature verification.
- No central authority can pause, reroute, or alter cycles post-deployment.