基于0G AI的预测市场聚合交易终端Demo技术方案 (v3 - 修正版)

1. 项目概述

根据您的最新反馈，我们对方案进行了关键修正。本项目旨在设计并实现一个基于0G测试网的预测市场聚合交易终端Demo。该终端的核心特点是**“链下数据 + 链上交易”**的混合架构，其核心逻辑已修正为：

1. **市场数据源**: 预测市场事件的数据（如问题、结束时间、解析结果）**完全从Polymarket API中只读获取**。
2. **链上交易逻辑**: 0G测试网上的智能合约**不再创建市场**，而是作为一个纯粹的交易层，负责处理用户资金、订单簿管理和交易撮合。市场的唯一标识符直接使用Polymarket的市场ID。

2. 修正后的系统架构

系统架构简化为链下服务和更精简的链上合约两部分。`MarketFactory.sol` 和 `PredictionMarket.sol` 合约被移除。

系统架构图 (v3)

mermaid

3. 简化后的0G链上智能合约设计

链上部分被大大简化，仅需两个核心合约：

合约名称	文件名	主要职责
Demo USDC Token	`DemoUSDC.sol`	- (职责不变) 实现一个标准的ERC20代币，作为系统内的计价和结算资产。 - 提供 `mint` 功能，方便用户在测试网获取初始资金。

交易中心合约	`TradingHub.sol`	- **唯一的核心交易合约**，处理所有逻辑。 - **资金库**: 管理所有用户的 `DemoUSDC` 存款。 - **订单簿**: 通过 `mapping(bytes32 => OrderBook)` 结构管理**所有外部市场**的订单。 `bytes32` 是Polymarket的市场ID。 - **结果代币**: 合约本身可作为ERC1155的实现，为每个市场的“是/否”结果动态生成和管理代币。 `tokenId` 可以是 `keccak256(abi.encodePacked(marketId, outcome))` 。

- **订单撮合**: 撮合对手方订单，并转移 `DemoUSDC` 和结果代币。
- **市场解析**: 包含一个受信任的 `resolveMarket(bytes32 marketId, uint8 winningOutcome)` 函数，由后端服务（作为预言机）调用，以标记一个市场的最终结果。
- **结算**: 允许用户在市场解析后，将获胜的结果代币兑换回 `DemoUSDC` 。 |

4. 修正后的核心交易流程

流程 1: 用户充值 (不变)

用户通过 `mint` 获取测试币，然后 `approve` 并 `deposit` 到 `TradingHub.sol` 合约。

流程 2: 市场同步 (后端驱动，无链上创建)

1. **同步事件**: 后端服务持续监控Polymarket的 `/events` API。
2. **前端展示**: 当获取到新的市场数据时，后端将其推送给前端界面进行展示。**此过程不与0G链发生任何交互。**

流程 3: 下单与撮合 (基于外部市场ID)

1. **用户下单**: 用户在前端选择一个Polymarket市场，输入价格和数量。前端调用 `TradingHub.sol` 的 `placeOrder(bytes32 marketId, ...)` 函数，其中 `marketId` 是Polymarket的市场ID。
2. **订单处理**: `TradingHub` 合约使用 `marketId` 作为key，在该市场的链上订单簿中进行查找和撮合。所有逻辑与之前类似，但操作对象从 `address` 变为了 `bytes32` 。

流程 4: 市场解析与结算 (后端驱动解析)

1. **监控结果**: 后端服务监控Polymarket，当一个市场被Polymarket官方解析后，获取其最终结果。
2. **结果上链**: 后端服务（作为预言机）调用 `TradingHub.sol` 的 `resolveMarket(bytes32 marketId, uint8 winningOutcome)` 函数，将Polymarket的官方结果记录到0G链上。
3. **用户赎回**: 用户调用 `redeem(bytes32 marketId)` 函数，将获胜的结果代币换回 `USDC` 。

5. AI分析与技术选型 (不变)

AI分析流程、技术选型与v2版本保持一致，作为链下服务为用户的链上交易提供决策支持。

6. 总结

此v3修正方案准确反映了“数据源与交易层分离”的核心思想，大大简化了链上合约的复杂性，使其更易于实现和审计。链上部分现在只专注于最核心的金融操作（记账、撮合、结算），而将市场状态的管理完全交给了外部数据源，这更符合一个聚合交易终端的定位。