Trading Challenge 技术与经济白皮书

全市场模拟交易竞技协议

TRADING CHALLENGE

技术架构 / 可验证结算 / 代币经济 / 风险边界

文档版本 v4.0 正式版
协议基线 Protocol v1 / Schema 1.0.0
发布日期 2026 年 8 月 12 日

文档定位

本白皮书聚焦 Trading Challenge 的协议设计、确定性赛事引擎、可验证结算、智能合约、安全边界和代币经济。运营增长机制不属于本文件范围。

所有参赛账户在同一赛事规则集下使用相同的初始资金、行情、成交规则和奖励公式。协议不设置账户身份层级或账户级收益加成；奖励只由公开的赛事参数、可验证赛果及协议级经济参数决定。

本文件构成 Trading Challenge Protocol v1 的正式技术与经济规范。主网合约地址、源码验证链接、审计报告、编译配置和部署交易哈希属于部署记录；部署记录不得改变本文件定义的供应上限、分配比例、安全不变量和参数硬边界。本文件不构成投资建议、收益承诺、代币价格承诺或任何金融产品要约。

目录

文档定位 2

第一部分：协议概览 5

1. 协议目标 . . . 5
2. 非目标与信任边界 . . . 5
3. 参与角色 . . . 5

第二部分：赛事协议 6

4. 赛事资产边界 . . . 6
5. 基础赛事模式 . . . 6
6. 奖池会计恒等式 . . . 6
7. 赛事状态机 . . . 7

第三部分：系统架构 8

8. 分层设计 . . . 8
9. 链下组件 . . . 8
10. 链上组件 . . . 8
11. 数据与隐私 . . . 8

第四部分：确定性赛事引擎 9

12. 规则集承诺 . . . 9
13. 指令接收与成交 . . . 9
14. 净值与排名 . . . 9
15. 市场边界条件 . . . 10

第五部分：行情与预言机 11

16. 两类价格系统 . . . 11
17. 赛事行情聚合 . . . 11
18. 经济参考价 . . . 11

第六部分：赛果证明与结算 12

19. 数据承诺 . . . 12
20. 验证与挑战 . . . 12
21. 领奖与退款 . . . 13

第七部分：智能合约 14

22. 合约模块 . . . 14
23. 部署与升级 . . . 14

第八部分：TC Token 经济模型 15

24. 基本信息 . . . 15

25. 创世分配与锁定 . . . 15
26. 协议费率与价值流 . . . 15
27. 单场经济示例 . . . 16
28. 生态赛事奖励释放 . . . 16
29. 收入驱动的回收与销毁 . . . 17
30. 供应量与流通量记账 . . . 18
31. 可持续性指标 . . . 19
32. 压力情景 . . . 19

第九部分：治理与权限 20

33. 渐进式治理 . . . 20
34. 财库纪律 . . . 20

第十部分：安全与运行保障 21

35. 威胁模型 . . . 21
36. 核心安全不变量 . . . 21
37. 工程验证 . . . 21
38. 性能与灾备目标 . . . 21

第十一部分：实施路线 22

39. 分阶段交付 . . . 22

第十二部分：风险与法律边界 23

40. 技术风险 . . . 23
41. 经济风险 . . . 23
42. 资产与对手方风险 . . . 23
43. 监管边界 . . . 23

附录 24

附录 A：初始参数表 . . . 24
附录 B：规则集最小字段 . . . 25
附录 C：链上事件最小集合 . . . 25
附录 D：公开验证材料 . . . 25

第一部分：协议概览

1. 协议目标

Trading Challenge 是基于真实市场行情运行的模拟交易竞技协议，覆盖数字资产、证券、期货、期权和差价合约等可获得合法行情授权的品类。参赛者不在赛事引擎内买卖真实金融资产，而是在统一的虚拟资金、时间窗口和成交模型下提交模拟交易指令，并按确定性规则竞争赛事奖池。

协议的目标是同时实现：

1. **公平执行**：同一赛事共享同一规则版本、规范化行情序列和成交模型；
2. **可复算**：在数据许可范围内，第三方可以从规则、行情和指令日志重放净值与排名；
3. **资产可审计**：链上报名资产、奖金、手续费、代币释放和销毁均可核验；
4. **经济可持续**：代币释放受外部收入和剩余奖励池双重约束，不依赖账户身份加成；
5. **故障可退出**：行情异常、结算争议、稳定币脱锚或服务中断时存在暂停、取消和退款路径。

2. 非目标与信任边界

协议不提供真实证券、期货、期权、外汇或差价合约的经纪、撮合、清算和交割。模拟竞技成绩不代表真实投资表现。

系统采用“链下高性能计算 + 链上资产与承诺”的混合架构。Protocol v1 不是完全无需信任的系统：赛事运营方负责接收指令和运行引擎，行情发布方负责数据签名，结果验证委员会负责复算与签名。链上合约约束资金流和最终化流程，但不能单独证明链下计算正确。数据承诺、回放数据包、5-of-7 验证签名和 72 小时挑战期共同约束链下信任边界。

3. 参与角色

角色	主要职责	关键限制
赛事运营方	发布规则、运行赛事、提交结果承诺	不能提取托管中的未结算奖池
行情发布方	聚合、规范化并签名行情	需满足来源数量、时效和偏差阈值
结果验证方	独立重放赛事并签署结果	达到 5-of-7 门槛后方可进入挑战期
托管与支付方	处理法币赛事的收付与对账	法币责任不由链上合约替代
链上合约	托管链上资产、记录状态、执行领取	不解释链下原始行情的商业授权
治理与安全多签	管理受限参数和应急暂停	不能覆盖已最终化赛果或突破供应上限

第二部分：赛事协议

4. 赛事资产边界

“USD 赛事”必须在下表前两种模式中二选一，不得混用；TC 赛事为独立模式：

模式	入场与奖金	结算保证	链上可见性
法币记账模式	由持牌支付或托管服务处理	依赖外部托管、对账和当地法律	仅可提交对账摘要与赛果承诺
稳定币模式	使用治理白名单内的链上稳定币	由 `EntryVault` 和结算合约约束	入场、退款、手续费和领奖全程可查
TC 模式	使用 TC 报名并以 TC 结算	由链上金库和结算合约约束	全程可查

Protocol v1 的链上稳定币赛事只开放 BNB Smart Chain 原生 USDC，其合约地址在部署记录中公布。以 3 个独立市场的 60 分钟中位 TWAP 计，连续 5 分钟偏离 1 USD 超过 2% 时停止新报名；偏离超过 5% 时取消尚未最终化的赛事并登记原额退款债权。固定金额赛事拒绝 fee-on-transfer、rebasing、回调型及余额可由管理员任意改变的代币；存款前后金库余额增量不等于报名金额时交易回滚。协议不以“USD”字样掩盖法币与稳定币在托管、赎回和对手方风险上的差异。

5. 基础赛事模式

模式	规模	基准时长	结算方式	特殊规则
Sit & Go	6 / 9 / 18	15 分钟	前三名 50% / 30% / 20%	满员后锁定规则并开赛
Scheduled	100	30 分钟	前三名 50% / 30% / 20%	固定时刻锁定报名
All-in	100	60 分钟	前三名 50% / 30% / 20%	至少交易 3 个品种；每品种仅允许一个方向性头寸
Battle Royale	100	40 分钟	Top 10：30% / 20% / 15% / 10% / 7% / 5% / 4% / 3% / 3% / 3%	第 10、20、30 分钟各淘汰末位 25 人；剩余 25 人完成终局

入场资产、入场金额、人数、市场范围、订单类型、批处理间隔、最大仓位、手续费模型、奖励曲线和异常处置均写入独立 `ruleset`。Scheduled 和 All-in 最低 50 人、最高 100 人，Battle Royale 必须满 100 人；不足最低人数即取消并按原资产退款。所有基础赛事使用 100,000 USD 虚拟初始权益、最大总杠杆 3 倍、单标的敞口不超过初始权益，同时持仓不超过 10 个标的。不同金额只是不同赛事配置，不形成账户等级或身份权益。

6. 奖池会计恒等式

对赛事 r 和报名资产 x，只按金库实际到账金额记账：

$$G_{r,x}=\sum_{i=1}^{n} e_{i,x}^{\text{received}}$$

$$\text{Fee}_{r,x}=\tau_r G_{r,x},\quad \text{Prize}_{r,x}=G_{r,x}-\text{Fee}_{r,x}+\text{Sponsor}_{r,x}$$

其中 $e_{i,x}^{\text{received}}$ 为单个实际到账入场金额，τ_r 为开赛前锁定的协议费率，$\text{Sponsor}_{r,x}$ 为已实际到账且与奖池同资产的额外赞助。跨资产赞助必须先完成可审计兑换，再以实际到账数量计入。`VaultBalance` 汇总该赛事在 `EntryVault`、分配器和 `UnclaimedPrizeVault` 的关联余额。奖金分配叶子必须满足：

$$\sum_i \text{AllocatedPayout}_{r,i,x}=\text{Prize}_{r,x}$$

同时：

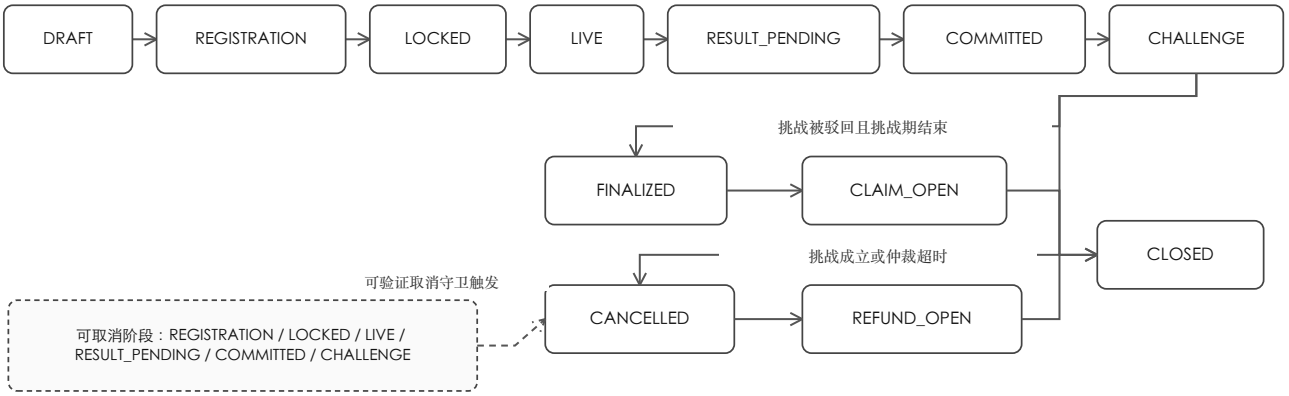
$$\text{Claimed}_{r,x}+\text{Unclaimed}_{r,x}=\sum_i \text{AllocatedPayout}_{r,i,x}$$

逐赛事、逐资产的全生命周期守恒为：

$$G_{r,x}+\text{Sponsor}_{r,x}=\text{VaultBalance}_{r,x}+\text{Claimed}_{r,x}+\text{Refunded}_{r,x}+\text{FeeWithdrawn}_{r,x}+\text{SponsorReturned}_{r,x}$$

协议费只能在赛事最终化后划出；取消赛事不计费。报名退款与奖金领取互斥。基础奖金领取窗口为 FINALIZED 后 180 个自然日；生态奖励领取窗口为分配器启用后 90 个自然日。舍入尾差和到期基础奖金进入按资产隔离的 UnclaimedPrizeVault，并在 30 日内注入下一场同资产公开赛事；30 日内无同类赛事时，按原报名实际到账比例退回参赛地址。生态 TC 奖励的尾差和未领取部分只返回 EmissionVault。

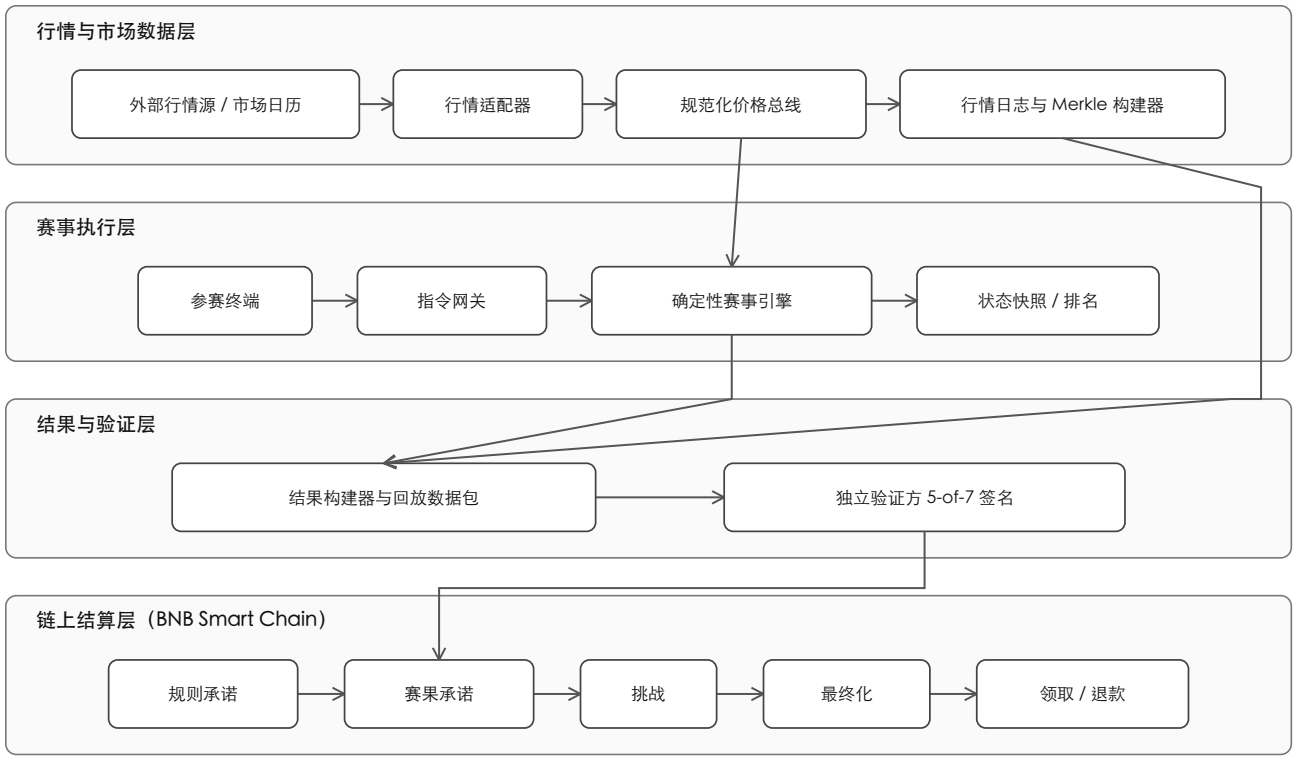
7. 赛事状态机



- LOCKED 后不得修改规则、参与名单、费率、验证方快照或奖励曲线；
- RESULT_PENDING 的结果提交硬上限为赛事结束后 2 小时，超时自动取消并退款；
- COMMITTED 仅代表结果取得门槛签名并已提交，不代表已经最终化；
- 挑战被驳回且挑战期结束后进入 FINALIZED；挑战成立时赛事直接取消并退款，不允许使用未在 LOCKED 时承诺的新验证集合重提结果；
- CLAIM_OPEN 与 REFUND_OPEN 互斥，领取和退款是逐地址累计状态，不是赛事级状态；
- FINALIZED 后结果根、领取人和金额不可覆盖。安全多签对单场领奖最多触发一次 24 小时暂停，必须给出链上原因；到期后任何地址均可恢复，暂停不得改变领取内容；
- 取消只能由规则集中可验证的守卫触发：报名不足、结果提交超时、承诺数据在 24 小时响应期内不可用、挑战成立或仲裁超时。管理员不得无条件取消；取消赛事不得转为协议收入，关闭前需满足退款负债归零以及未领取资产处置规则。

第三部分：系统架构

8. 分层设计



9. 链下组件

1. **指令网关**：验证赛事状态、签名、nonce、速率和指令格式，分配单调递增接收序号；
2. **行情适配器**：连接获授权的数据源，统一时间戳、标的代码、精度和市场状态；
3. **确定性引擎**：以固定版本执行订单、持仓、费用、净值、淘汰和排名；
4. **事件日志**：追加写入，禁止原位修改；定期形成哈希链和 Merkle 根；
5. **结果构建器**：生成账户状态、排名、奖金叶子节点和内容寻址数据包；
6. **回放验证器**：从相同输入生成相同状态根，并对结果进行门槛签名；
7. **风控服务**：检测多账户、合谋、自动化滥用和异常指令，但不能静默改写赛果。

10. 链上组件

链上只承担低频、确定和具备资产约束价值的工作：规则版本承诺、链上报名资产托管、结果状态、Merkle 领奖、退款、TC 奖励释放、销毁、归属、财库和受限治理。高频行情与逐笔模拟成交不直接写入 BSC，以避免成本和确认延迟破坏实时赛事体验。

11. 数据与隐私

- 链上只使用钱包地址或带域隔离的伪匿名标识，不写入姓名、证件号、设备指纹或原始合规资料；
- 指令与行情数据使用规范化编码，并记录引擎版本、时区、精度和舍入模式；
- 规范化行情、指令、赛果和审计日志保存 7 年；法律要求更长期限时，只延长受影响地区的数据保存期；
- 行情授权允许时公开完整回放包；不允许公开时，由获授权的独立审计方复算并公开签名和审计结论。后一模式属于“受许可审计”，不得表述为完全公开验证。

第四部分：确定性赛事引擎

12. 规则集承诺

每场赛事在 LOCKED 前按 RFC 8785 JSON Canonicalization Scheme（JCS）把规则 JSON 编码为唯一 UTF-8 字节序列 `canonicalRulesetBytes`。整数必须位于实现共同支持的安全范围，涉及资产数量和价格的字段使用十进制定点整数字符串，禁止浮点数、重复键、NaN 和 Infinity。首先计算：

$$rulesetHash=keccak256(canonicalRulesetBytes)$$

再计算链上承诺：

$$H_{rules}=keccak256(abi.encode(RULESET_TYPEHASH,block.chainid,tournamentRegistry,protocolVersion,schemaVersion,roundId,engineCodeHash,rulesetHash))$$

`RULESET_TYPEHASH` 固定字段类型和顺序；`roundId` 为 `bytes32` 且在注册表内全局唯一；数量和价格使用 `uint256`，损益使用 `int256`，时间戳使用 `uint64`，任一越界规则集均拒绝注册。`engineCodeHash` 为可执行文件或容器镜像的内容摘要，不是可复用的版本字符串。链 ID、注册表和协议版本用于防跨链、跨合约和跨版本重放。规则集必须包含以下全部内容：

- 赛事开始、结束和淘汰检查点；
- 可交易标的、市场日历和合约乘数；
- 初始虚拟资金、杠杆、仓位与风险限制；
- 支持的订单类型、价格选择和成交优先级；
- 模拟手续费、滑点、精度和舍入；
- 行情异常、停牌、熔断、公司行动和取消规则；
- 排名、同分、奖励曲线和申诉时限。

13. 指令接收与成交

协议不使用无法验证的“所有人同时成交”表述。公平性由固定时间片和确定性价格规则实现：

1. 网关记录服务器接收时间与递增序号；
2. 有效指令进入规则集指定的批处理时间片；
3. 市价指令使用接收后首个满足新鲜度要求的规范化价格 tick；
4. 限价或止损指令按公开的穿价、触发和优先级规则执行；
5. 晚于时间片截止或发生行情断流的指令按规则拒绝，不得人工补单；
6. 所有接受、拒绝、成交和撤销事件进入不可变日志。

指令使用 EIP-712 会话密钥签名，绑定协议、chainId、网关、roundId、账户、指令类型、payloadHash、nonce、validAfter 和 deadline。nonce 严格递增，指令签名最长有效期为 30 秒；撤单与会话密钥轮换均产生事件。Protocol v1 的批处理时间片固定为 250 ms，网关每 30 秒向 BNB Smart Chain 提交追加日志根，使事后删除和重排可以被发现。该方案能审计已承诺日志，不能证明运营方从未丢弃到达网关之前的网络请求。

14. 净值与排名

账户 i 在时刻 t 的模拟净值定义为：

$$NV_i(t)=Cash_i(t)+\sum j=1mV_j(Position_{i,j}(t),Mark_j(t),FX_j(t))-AccruedLiabilities_i(t)$$

其中 V_j 是该品类的版本化估值函数，`Cash` 只包含已实际过账的现金变化，`AccruedLiabilities` 只包含尚未过账的费用和负债，避免重复扣费。规则集分别定义现货、期货、期权和 CFD 的权利金、合约乘数、变动保证金、融资费、强平、负价格和负净值处理。

基础排名指标为净值回报率：

$$R_i=(NV_i(T)-NV_i(0)) / (NV_i(0))$$

同分时依次比较：最终净值的未舍入整数值、每 1 秒采样计算的最大回撤（较小者优先）、有效指令数，最后比较 `keccak256(roundSeed, participantId)`。LOCKED 后立即请求 Chainlink VRF，等待 20 个区块确认；开赛前 2 分钟仍未取得 seed 时取消赛事并退款，不使用人工备用 seed。种子请求、结果和最终 seed 均进入数据承诺。

Battle Royale 在每个淘汰检查点生成独立状态根。被淘汰账户此后提交的指令必须被拒绝，不能仅在最终排名阶段补做淘汰。

15. 市场边界条件

引擎必须确定性处理负价格、空头、合约换月、时区和夏令时、停牌、熔断、拆股分红、期权到期、稳定币脱锚和终场无有效 tick 等边界。未在规则集中定义的事件不得由运营方临场裁量；应暂停受影响标的或取消赛事并退款。

第五部分：行情与预言机

16. 两类价格系统

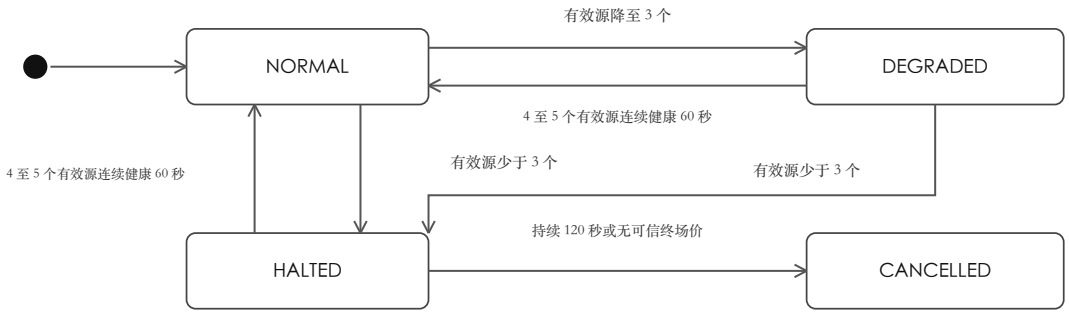
赛事行情与代币经济参考价用途不同，必须隔离：

系统	频率	用途	主要风险
赛事行情	亚秒至秒级	模拟成交、估值和排名	延迟、授权限制、单源异常
经济参考价	分钟至日级	限制回收执行规模、财库估值披露	DEX 操纵、低流动性、陈旧数据

Chainlink、Pyth 等网络不一定覆盖所有证券、期货、期权或差价合约。协议只在来源、授权、交易时段和精度均满足赛事规则时开放相关标的。

17. 赛事行情聚合

每个标的固定配置包含 5 个无共同上游的独立数据源、价格精度、交易状态和备用源。有效来源为 4 至 5 个时进入 NORMAL，3 个时进入 DEGRADED，少于 3 个时进入 HALTED；有效价格取规范化中位数。数字资产最大陈旧时间为 2 秒，股票、期货、外汇与 CFD 为 5 秒，期权为 10 秒；普通标的跨源偏差上限为 1%，期权为 2%。状态机如下：



- DEGRADED：3 个有效源仍满足安全门槛，赛事继续并公开标记；
- HALTED：停止接受受影响标的的新指令和结算；
- 恢复：4 个或 5 个有效源连续健康 60 秒后回到 NORMAL；
- CANCELLED：HALTED 持续 120 秒或无法形成可信终场价时，赛事取消并退款。

状态默认按标的管理；如果受影响标的仍有未平仓头寸且无法形成可信估值，则整场立即进入 HALTED。规则集必须定义存量头寸估值。所有源使用 UTC、单调序号和签名消息。服务器通过 NTP 加监控校时；节点时钟偏差超过 100 ms 时自动退出发布集合。

18. 经济参考价

经济模块使用版本化的“多市场 30 日中位 TWAP”。合格集合必须包含 3 个无共同上游的可提币市场；每个市场连续运营满 30 日，30 日中位日真实成交额不低于 50,000 USD，5 分钟 TWAP 样本在滚动 30 日内的覆盖率不低于 95%。先分别计算 TWAP，再取中位数。最新样本超过 15 分钟，或各市场中位价的最大偏差超过 10% 时，参考价失效，当期生态释放与回收执行均为 0，预算结转。参考价只用于执行限额和财务披露，不用于设定价格目标。

第六部分：赛果证明与结算

19. 数据承诺

单一“赛果哈希”只能证明某份结果曾被提交，不能证明结果正确。每场赛事分别构建：

- H_{market}：规范化行情事件根；
- $H_{commands}$：接受与拒绝的指令事件根；
- H_{state}：检查点账户状态根；
- H_{payout}：领奖叶子节点根；
- $H_{manifest}$：固定格式回放清单的摘要，清单包含各数据文件摘要。

总承诺绑定协议域、赛事和验证方集合：

$$H_{round}=keccak256(abi.encode(ROUND_TYPEHASH,block.chainid,resultRegistry,protocolVersion,schemaVersion,roundId,verifierSetId,engineCodeHash,H_{rules},H_{market},H_{commands},H_{state},H_{payout},H_{manifest}))$$

`H_manifest` 是固定格式回放清单的摘要，清单再记录可替换的 URI/CID 和每个文件摘要。所有 Merkle 树采用按 `leafIndex` 排序的 positional tree，左右节点不可交换；每树最多 1,048,576 个叶节点，`leafIndex` 使用 `uint32`，奇数层的最后节点与自身配对，空树根为 `keccak256(abi.encode(EMPTY_TREE_TYPEHASH, uint256(0)))`，不允许重复 `leafIndex`。禁止直接拼接可变长字段，禁止将原始账户资料写入哈希前像。编码规则、哈希算法和域分隔符必须版本化。

20. 验证与挑战

Protocol v1 采用“验证委员会认证 + 受许可仲裁”，不是链上欺诈证明。验证委员会由 7 个相互独立的实体组成，同一实际控制人最多 1 席，结果门槛为 5-of-7；仲裁委员会由与验证方无重叠的 3 席组成，裁决门槛为 2-of-3。验证集合和仲裁集合在 `LOCKED` 时快照。每名验证方锁定 50,000 USDC 保证金。结果签名采用 EIP-712：domain 固定 `name`、`version`、`chainId` 和 `ResultRegistry`，结构摘要为：

$$H_{struct}=keccak256(abi.encode(RESULT_ATTESTATION_TYPEHASH,roundId,H_{round},verifierSetId,deadline))$$

$$H_{attest}=keccak256(abi.encodePacked(hex"1901",domainSeparator,H_{struct}))$$

验证方对 H_{attest} 签名。每个签名地址只计一次，必须属于快照集合；合约拒绝零地址、不可恢复签名、ECDSA high-s 和无效 v 值。每个验证方下载同一回放包、运行固定引擎镜像并确认状态根；达到门槛后结果进入挑战期，而非立即生效。

挑战者提交保证金和以下任一类可受理证据：

1. 同一 `roundId` 的两份不同结果均取得门槛签名；
2. 回放清单中的文件摘要与已承诺 `H_manifest` 不一致或数据在响应期内不可获得；
3. 使用承诺的引擎和输入可重复生成与 `H_state` 或 `H_payout` 不同的结果，并由仲裁验证器确认；
4. 奖金叶子总额违反已承诺奖池或逐赛事资产守恒。

格式错误或无效 Merkle 路径在提交时直接拒绝，不视为挑战证据。结果进入 `COMMITTED` 后的挑战期为 72 小时，数据可用性请求和被挑战方的响应期均为 24 小时，响应期结束后的仲裁期为 48 小时；仲裁超时时赛事自动取消并退款。外部资产挑战保证金为奖池的 0.05%，最低 100 USD、最高 1,000 USD，以结算资产缴纳；TC 挑战保证金为奖池的 0.05%，最低 10,000 TC、最高 100,000 TC。挑战失败的保证金用于仲裁成本；挑战成功时全额退还保证金，并支付实际罚没额 10% 的奖励，奖励上限为 10,000 USD 等值，其余罚没资产进入风险准备金。重复签署冲突结果的验证方罚没 100% 保证金，签署经复算确认的错误结果罚没 20% 保证金，并移出验证集合；当前赛事直接取消退款。挑战被驳回且期限结束后最终化。Optimistic fraud proof 和 zkVM 执行证明不属于 Protocol v1 范围。

21. 领奖与退款

最终化后采用 Merkle pull-claim：

$$leaf_i = keccak256(abi.encode(PAYOUT_TYPEHASH, roundId, leafIndex, asset, recipient, amount))$$

合约验证证明、资产、金额、唯一 `leafIndex` 和领取 bitmap，防止跨赛事重放与重复领取。领取总额不得超过对应赛事金库余额。领取窗口结束后的基础奖金进入按资产隔离的 `UnclaimedPrizeVault`；生态奖励返回 `EmissionVault`，均不得由任意权限地址直接提取。

取消赛事按实际到账的原资产原额退款。退款窗口为 365 个自然日；到期未领取金额转入隔离退款金库，原参与者权利永久保留，不得转为协议收入。白名单排除转账税和 rebase 资产；若白名单稳定币在存续赛事中被发行方冻结，则停止该资产新赛事并取消存续赛事；退款债权按原额登记，发行方解除冻结后按登记地址退款。协议不执行代币替换、强制迁移或绕过发行方冻结。

第七部分：智能合约

22. 合约模块

模块	职责	关键不变量
TCToken	固定上限代币与销毁	部署后不可增发，供应量只因销毁下降
RulesetRegistry	登记规则版本和引擎摘要	已锁定赛事引用的版本不可变
TournamentRegistry	管理赛事状态机	不得跳过挑战期直接最终化
EntryVault	托管 TC 或白名单稳定币入场资产	未最终化前运营方不可提取奖池
ResultRegistry	保存数据根、验证签名和挑战状态	最终结果根不可覆盖
ClaimNullifierRegistry	跨分配器共享已领取 leaf bitmap	同一赛事同一 leafIndex 全版本只能领取一次
SettlementDistributor	Merkle 领奖和退款	累计领取不超过已拨付余额
RevenueAttestationRegistry	记录外部资产赛事的已结算净协议费证明	同一收入不得跨 epoch 重复计入
EmissionVault	锁定 4 亿枚生态奖励并按 epoch 释放	单期及累计释放不超过公式上限
CompetitionReserve	保存 TC 手续费回流部分	仅能实拨至公开 TC 赛事奖池
UnclaimedPrizeVault	按资产隔离保存过期基础奖金	只能按已锁定规则退回或进入同资产赛事
RecoveryVault	接收已兑换为链上资产的回收结果并执行销毁/POL 划拨	不直接执行法币交易，不根据涨跌改变预算比例
VestingVault	执行团队归属	不可提前解锁
TreasuryTimelock	协议财库支出	受预算上限、公告期和时间锁约束

Protocol v1 不部署账户激励、NFT 或独立游戏资产合约；这些资产不属于本版供应、奖励或治理模型。

23. 部署与升级

TCToken、VestingVault、每场 EntryVault 和已提交结果存储不可升级；RulesetRegistry、TournamentRegistry、ResultRegistry、RevenueAttestationRegistry、EmissionVault、RecoveryVault 和 TreasuryTimelock 采用版本化部署，旧实例不接受新业务。发现缺陷时停止新赛事进入旧版本并部署新实例，已锁定赛事仍按原规则结算；只有新赛事的注册表指针可由独立升级多签经时间锁更新。

任何版本迁移必须公开：源代码 commit、编译器版本、优化参数、字节码、状态迁移清单、审计结论和生效时间。迁移不能更改已最终化赛果、提前解锁归属资产或恢复已销毁 TC。领奖只允许 §7 所述的有界暂停；所有分配器共用不可升级的 ClaimNullifierRegistry。若领取合约自身失效，逃生合约必须保持同一 root/recipient/amount、相同领取截止和赛事余额上限，继续读取同一 nullifier，并在激活前永久关闭旧分配器，防止迁移后重复领取。

第八部分：TC Token 经济模型

24. 基本信息

项目	参数
名称	TC Token
符号	TC
网络	BNB Smart Chain
标准	BEP-20（ERC-20 兼容）
初始及最大供应量	1,000,000,000 TC
增发	不允许；创世时一次性铸造到各锁仓合约

TC 的协议用途限定为：TC 赛事入场与奖金结算、受限治理及协议流动性。Protocol v1 不承诺固定收益、存款利息、保本赎回或基于持有身份的奖励加成。

25. 创世分配与锁定

分配	数量	比例	初始约束
生态赛事奖励池	400,000,000	40%	锁入 `EmissionVault`，仅按 §28 公式释放
核心团队	300,000,000	30%	12 个月 cliff，随后 48 个月按秒线性归属
协议财库	200,000,000	20%	180,000,000 进入时间锁财库；20,000,000 用于 TGE 初始流动性
战略储备	100,000,000	10%	锁定至 2030-01-01，此后 36 个月按秒线性释放
合计	1,000,000,000	100%	不存在表外增发

战略储备只用于协议安全准备、验证网络抵押和 POL；每笔使用在执行前 30 日公开，未使用额度不得提前解锁。协议财库和战略储备的任何实际转出均形成可审计的流通变化。

创世铸造完成且 TGE 流动性尚未部署时，地址分类为：E=400,000,000、V=300,000,000、T=200,000,000、Z=100,000,000 TC，其余类别为零。TGE 初始流动性固定为 20,000,000 TC 与 200,000 USDC，初始池比例为 0.01 USDC/TC；TC 从 T 转入 AMM 后计入 U。200,000 USDC 由非奖池、非风险准备金的外部资金独立实缴。LP 头寸由 `TreasuryTimelock` 持有，初始 12 个月不得撤出；此后撤池需经过 30 日公示和 7 日时间锁。生态奖励、团队归属和财库支出分别披露，不把“已铸造但锁定”与“市场流通”混为一谈。

26. 协议费率与价值流

初始赛事协议费率为已确认入场金的 5%。费率写入每场规则集，`LOCKED` 后不可修改。治理只能在 3% 至 7% 的硬边界内调整尚未 `LOCKED` 的赛事费率，并在生效前公示 30 日。

对于法币模式，只有在赛事奖池负债已足额隔离后，协议费才能确认为毛协议费。支付、托管、税费、退款处理、拒付损失及其他直接结算成本必须先扣除：

$$\mathrm{NetFee}_e^{\mathrm{ext}}=\max(0,\mathrm{GrossFee}_e^{\mathrm{ext}}-\mathrm{Cost}_e^{\mathrm{direct}})$$

$$\mathrm{SettlementLoss}_e=\max(0,\mathrm{Cost}_e^{\mathrm{direct}}-\mathrm{GrossFee}_e^{\mathrm{ext}})$$

其中 $\mathrm{GrossFee}^{\mathrm{ext}}$ 为已结算且未退款赛事的毛协议费，$\mathrm{Cost}^{\mathrm{direct}}$ 仅包括逐笔可归属的支付、托管、税费、拒付和结算成本；固定行情、计算、研发和安全成本属于后续运营分配，不重复扣除。直接成本超过毛协议费时，差额作为 `SettlementLoss` 披露并由风险准备金补足，不能被 `max(0,...)` 隐去。取消赛事不产生协议费。稳定币模式的链上转账费若由参赛者自行承担，不重复计入直接成本；由协议代付时必须计入。回收、准备金与财库分配只以 $\mathrm{NetFee}^{\mathrm{ext}}$ 为基数，不能从奖金负债或尚未结算的收款中支付。

法币或稳定币赛事已结算净协议费的初始分配：

流向	比例	作用
基础设施与运营	45%	行情授权、计算、研发、安全审计、合规及支付/托管的固定供应商成本
TC 回收预算	30%	按 §29 的成交量上限执行公开回收
风险准备金	15%	拒付、结算损失、供应商中断和安全事件；不得承担正常取消退款或计作利润
协议财库收入	10%	形成可披露的协议盈余

TC 赛事协议费的初始分配：

流向	比例	作用
永久销毁	50%	直接调用 `burn`，降低总供应量
赛事储备	30%	锁定并用于未来公开 TC 赛事的附加奖池
协议财库	20%	用于经时间锁批准的协议支出

技术 API、白标赛事系统和品牌赛事等外部收入在扣除直接交付成本后，按独立财务报表披露，不并入赛事协议费释放口径。

风险准备金目标余额为 `max(250,000 USD, 90 × 3%)`。首场外部资产赛事开放报名前，必须由非奖池资产实缴不低于 250,000 USD。余额低于目标时，净协议费中原 15% 准备金份额与 10% 财库份额合并为 25% 补充准备金；余额低于 250,000 USD 时停止法币和稳定币新赛事，恢复至目标且连续保持 7 日后重开。准备金只能按已公开的结算损失或安全事件证明支取。正常取消赛事的退款始终来自隔离的报名资产，而非准备金。

27. 单场经济示例

在已确认入场金为 1,000,000 USD、费率为 5%、无额外赞助，且本例直接结算成本为 5,000 USD 的赛事周期中：

项目	金额
参赛奖金池	950,000 USD
毛协议费	50,000 USD
直接结算成本	-5,000 USD
可分配净协议费	45,000 USD
基础设施与运营	20,250 USD
TC 回收预算	13,500 USD
风险准备金	6,750 USD
协议财库收入	4,500 USD

在总入场金为 1,000,000 TC 的赛事周期中，协议费为 50,000 TC，其中 25,000 TC 销毁、15,000 TC 进入赛事储备、10,000 TC 进入时间锁财库，奖金池为 950,000 TC。

以上仅演示会计流向，不代表预计流水、利润、买入价格或代币价值。

28. 生态赛事奖励释放

奖励 epoch 固定为 UTC 自然月，不可治理修改。epoch 开始时对奖励池余额和参数做快照，并预留本期预算，避免先领取者改变后领取者的释放系数。

定义：

- E_e：epoch e 开始时 `EmissionVault` 可用余额；
- E_0=400,000,000 TC；
- q：单期生态池释放率上限，初始为 1%，合约硬上限为 1%；

- α：预铸 TC 排放参考价值相对净协议费的上限比例，初始为 20%；该比例不预留或支出外部资产；
- F_{e-1}^{ext}：上一期已清算、扣除直接成本后的外部资产赛事净协议费，按统一记账单位计量；
- F_e^{target}：最近 6 个完整 UTC 自然月的已最终化净协议费中位数，包含零收入月；偶数样本取中间两项算术平均值。`F_target_floor` 固定为每个 UTC 自然月 100,000 USD，计算值不得低于该下限；
- g_e：外部经济活动系数。
- P_e^{ref}：以 F^{ext} 同一记账单位表示的合格市场 30 日中位 TWAP，且必须大于零；若不可用则本期释放为零。

$$g_e=\min(1,(F_{e-1}^{ext}) / (F_e^{target})),F_e^{target}>0$$

$$A_e=\lfloor \min(qE_e g_e,(\alpha F_{e-1}^{ext}) / (P_e^{ref})) \rfloor$$

只有实际清算、未退款且扣除直接成本后的法币或稳定币赛事净协议费计入 F^{ext}；TC 循环报名、财库赞助和未到账承诺不计入。多币种金额按结算时的可审计记账价值转换为同一单位；脱锚资产在恢复可靠定价前不计入。TGE 后未形成完整 30 日合格价格数据时，生态释放为零。

稳定币赛事的 `EntryVault` 事件只能直接证明实际到账和链上毛协议费；由协议承担的链下直接成本仍需审计证明。法币赛事由托管方对账摘要、独立审计签名和运营方签名共同形成门槛证明，提交至 `RevenueAttestationRegistry`，并经过与赛果相同的公示和挑战期。证明至少包含 epoch、币种、毛协议费、退款、拒付、直接成本、净协议费及源文件摘要；同一赛事 ID 只能计入一次。该机制属于受许可财务证明，不等同于无需信任的链上收入。

即使外部活动持续达到目标且收入价值上限不构成约束，前 n 期累计释放仍不超过：

$$\text{Released}_n \le E_0(1-(1-q)^n)$$

按 q=1% 逐期向下取整计算，60 期累计释放上限为 181,137,323 TC，即初始生态池的约 45.284%；实际值因收入价值上限、活动系数、退款和舍入只会更低。有限整数精度下不存在数学意义上的“永久非零”：当余额低于最小可分配阈值时，剩余 dust 按合约规则销毁，不得转入团队或财库。

每月 1 日 00:00 UTC 对生态池余额和参数快照，上一月收入证明提交截止时间为 5 日 23:59 UTC，10 日 00:00 UTC 固化当期预算；尚未最终化的收入顺延至下一期。每期预算按已最终化赛事产生的外部协议费权重分配到赛事，再按开赛前公开的排名曲线分配：

$$A_r=A_e(\text{NetFee}_r^{ext}) / (\sum_{j\in R_e}\text{NetFee}_j^{ext}),A_{r,i}=A_r(w_{rank(i)}) / (\sum_k w_{rank(k)})$$

R_e 只包含在上一 epoch 截止前完成赛果最终化、收入证明最终化、未退款且净协议费为正的赛事，与 A_e 使用同一收入集合。规则集注册时必须满足至少一个排名权重为正，即 $\sum_k w_{rank(k)}>0$。集合为空时 $A_e=0$，不预留预算。迟延证明进入下一期；之后发生拒付时先冲减下一期 F^{ext}，不足部分计入 `SettlementLoss`，不向已领取账户追缴。w_{rank} 只由开赛前锁定的排名奖励曲线决定，不接受账户属性、持币数量或 NFT 加成。预算从 `EmissionVault` 拨至逐期分配器；实际领取进入流通，过期未领取和尾差原路返回。最小奖励叶为 0.000001 TC；`EmissionVault` 总余额低于 1 TC 时全额销毁。计算使用定点整数、全精度 `mulDiv` 和统一向下舍入。

α 是预铸代币的排放估值护栏，不是外部资产现金预算；因此 45%/30%/15%/10% 的净协议费分配仍合计 100%。月度面板必须披露 TC / NetFee^{ext}，避免把现金分配和代币转移混为同一资产。

29. 收入驱动的回收与销毁

外部资产赛事已结算净协议费的 30% 进入回收预算。预算比例不随 TC 涨跌改变，避免把协议变成价格干预器。实际回收量按成交回报记账，不用理论点价反推。每个 epoch 的最大执行金额为：

$$X_e=\min(B_e,\lambda V_e^{30d})$$

其中 B_e 为已到账且未使用的回收预算，V_e^{30d} 为以同一记账资产计量、跨合格市场去重后的 30 日中位日成交额，λ 初始为 5%。X_e 是整个 epoch 的总上限，不是每日额度；另设单日 1%、单市场 0.5%、最大价格影响 1% 和最大滑点 1% 的初始上限。关联交易、可疑刷量和共享同一上游的重复市场不计入成交额。预算不失效但累计余额不放宽执行上限。执行采用分时成交和多市场报价；任一价格、深度或分歧阈值失效时，当期剩余执行上限置为 0，预算结转下期。每期公开实际投入、成交 TC 数量、成交量加权均价、滑点和交易哈希。

实际回收的 R_e^{TC} 枚 TC 按以下比例处理：

$$D_e^{buyback}=\rho_e R_e^{TC},Target_e^{POL}=(1-\rho_e)R_e^{TC}$$

$$0.70\le\rho_e\le1,qquad0\le ActualTransfer_e^{POL}\le Target_e^{POL}$$

初始 $\rho_e=0.70$；$D_e^{buyback}$ 永久销毁，剩余部分是目标 POL 数量。回收完成后 24 小时内销毁 70%；POL 份额按执行时 TWAP 做 50:50 市值配对，且必须在 30 日内取得协议财库独立批准和实拨的稳定币；届满仍未配对的 TC 全部销毁，不得单边投入市场。配对资产不占用已经执行完毕的回收预算。LP token 或集中流动性头寸由 `TreasuryTimelock` 持有，撤池需时间锁；地址、配对资产来源、头寸区间、手续费收入和无常损失逐期披露。AMM 池内 TC 归入公开流通余额，不作为长期锁定扣减。

回收金库状态为：

$$H_{e+1}=H_e+R_e^{TC}-D_e^{buyback}-ActualTransfer_e^{POL}$$

所有销毁和 POL 划拨在同一期完成时 H_{e+1} 仅保留历史未处置余额；否则余额继续公开并受相同规则约束。

TC 赛事另产生直接销毁：

$$D_e^{game}=0.50Fee_e^{TC}$$

总销毁包括回收销毁、TC 赛事费销毁、生态池最终 dust 销毁及可验证的其他自愿销毁：

$$D_e=D_e^{buyback}+D_e^{game}+D_e^{dust}+D_e^{other}$$

回收与销毁是收入和使用量驱动的供应管理机制，不构成价格底线或升值保证。

30. 供应量与流通量记账

由于 TC 在创世时一次性铸造，生态奖励释放不是“新增铸币”。总供应量只因销毁变化：

$$TotalSupply_{e+1}=TotalSupply_e-D_e$$

协议按互斥的实际地址类别做逐期对账。定义 E,V,T,Z,H,R,C,U,O 分别为生态奖励金库、团队归属金库、协议财库、战略储备、回收金库、TC 赛事储备、赛事与分配托管金库（包括未最终化、待领取和待退款余额）、其余公开流通地址（包括 AMM 池）和已登记的其他托管地址，则每期结束必须满足：

$$E_e+V_e+T_e+Z_e+H_e+R_e+C_e+U_e+O_e=TotalSupply_e$$

销毁地址不计入余额，每个持币地址只能归入一个类别，跨类别转移不能改变等式总额。`SettlementDistributor`、`EntryVault`、逐期奖励分配器和 `CompetitionReserve` 分别进入 C 或 R；协议持有的 LP token 不是 TC，不能加入等式，AMM 合约持有的全部 TC 统一归入 U。创世区块和每个 epoch 均发布地址到类别的映射及余额快照。

“估算流通量”采用广义口径：外部地址与 AMM 池余额、团队已归属但未领取数量、已最终化可领取余额均计入流通；未归属、时间锁财库、战略储备、回收金库和未最终化托管不计入。即：

$$Circulating_e=U_e+V_e^{vested_unclaimed}+C_e^{claimable}+O_e^{circulating}$$

月度报表同时披露链上实际领取量。相比单一余额递推，协议采用钱包向量转移表作为权威账本：

事件	转出	转入/销毁
生态预算预留	E	C；过期未领从 C 返回 E
团队到期归属	无实际钱包转移	增加 $V^{vested_unclaimed}$ 并计入广义流通
团队领取	V	U；广义流通总额不因此改变
财库或储备支出	T/Z	U 或指定托管类别
外部市场回收	U	H
回收销毁	H	销毁并同步减少 `TotalSupply`
POL 入池	H	U 中的 AMM 合约地址

事件	转出	转入/销毁
TC 赛事报名	U	C 中的 `EntryVault`
TC 赛事储备实拨	R	C，作为不计费的赞助奖池
其他 TC 赞助实拨	U/T	C，作为不计费的赞助奖池
TC 赛事最终化	C	仅报名金 G 的 2.5% 销毁、1.5% 转 R、1% 转 T；0.95G+Sponsor 留在 C 待领
TC 奖金领取	C	U；广义流通总额不因此改变
TC 赛事取消	C	报名金 G 退回参赛地址 U；赞助按来源退回 R/T/U；不计费、不销毁

财务面板必须展示逐钱包的期初余额、流入、流出和期末余额，以及总供应、累计销毁、已解锁、实际领取和估算流通量。任何无法归类的余额差异都应阻止该期经济报表最终化。

31. 可持续性指标

协议不以单一市值预测证明经济可持续性，而持续披露以下可复算指标：

指标	公式或口径	含义
奖池偿付率	可用奖池资产 / 已确认奖金负债	必须始终不低于 100%
现金运营覆盖率	外部净收入 / 现金运营支出	衡量协议是否依赖储备续航
净流通变化	释放 + 解锁 + 财库支出 - 销毁 - 净锁定	衡量实际供给压力
已执行回收覆盖率	实际回收外部资产 / 实际领取 TC 的参考价值	使用实际成交与领取数据
实际销毁覆盖率	当期销毁 TC / 当期进入广义流通的 TC	只比较代币数量，不暗示价格支撑
流动性冲击率	计划交易额 / 30 日中位日成交额	限制协议自身造成的滑点
财库续航	可用外部资产 / 月均现金支出	衡量低收入情景下的生存期

此前版本的五年市值、净销毁和流通拐点结果不适用于本版参数。本版不发布确定性五年市值或价格预测；经济可持续性只按 §31 指标和 §32 压力情景评估。代币价格作为压力测试输入，不由流水乘以估值系数直接推导。

32. 压力情景

情景	机制反应	仍然存在的风险
外部赛事收入下降	g_e 自动下降，生态释放同步收缩	运营收入和财库续航恶化
TC 价格快速下跌	回收预算比例不变，执行仍受成交量上限约束	同额预算可能买到更多 TC，但不能保证价格恢复
市场流动性枯竭	回收暂停或减速，预算留存	退出滑点、价格发现失真
团队集中解锁	按既定归属进入流通披露	协议不会自动扩大买盘对冲卖压
稳定币脱锚	停止新报名，按规则暂停、换源或退款	托管方、桥和发行方可能无法足额兑付
行情或验证方失效	赛事进入暂停、挑战或取消	长时间中断会降低赛事可用性

第九部分：治理与权限

33. 渐进式治理

受控主网上线后前 24 个月由职责公开的多签和时间锁执行受限操作：应急暂停使用 3-of-5，升级与财库使用 5-of-7，与结果验证委员会不得重叠。第 25 个月启用 TC 投票治理，多签只保留单次最长 24 小时的应急暂停权。治理权不等同于对公司股权、利润或托管资产的所有权。

类别	可治理事项	不可治理事项
赛事参数	新标的、新规则版本、未锁定赛事费率（3% 至 7%）	修改已锁定赛事规则或最终赛果
经济参数	未锁定赛事费率、回收执行上限、财库预算	增发 TC、突破释放硬上限、提前团队归属、恢复已销毁 TC
技术参数	验证方集合、挑战期、外围模块版本	绕过奖池偿付、重复领取或退款不变量
应急操作	暂停新报名、结果提交、最终化；按 §7 有界暂停领奖	延长领奖暂停、修改已最终化领取内容、将参赛奖池划入运营账户

普通变更经过 7 天讨论和 48 小时时间锁；影响费率、释放或财库的大项经过 30 日公示和 7 日时间锁。q 只能下调、α 可在 0 至 20% 内调整、净协议费回收预算可在 0 至 30% 内调整、回收后销毁比例可在 70% 至 100% 内调整；任何下调的现金分配比例只能增加风险准备金，不能自动转为财库收入。F^{target} 由历史中位数计算，不能投票指定。投票使用历史快照，防止闪电贷临时取得权重。验证方、暂停方、升级方、财库执行方和结果发布方必须使用不同角色与密钥。

34. 财库纪律

- 所有财库地址、余额、归属合约和 POL 地址公开；
- 普通支出在滚动 30 日内的 TC 金额不超过期初 TC 财库余额 0.5%，外部资产金额不超过期初外部资产余额 10%；
- 超过普通支出上限的战略支出必须取得 5-of-7 通过，并执行 30 日公示加 7 日时间锁；单一提案不得超过对应资产期初余额 2%；
- 风险准备金与参赛奖池隔离，不得合并记账；
- 月度报告披露外部资产收入、运营支出、回收预算、实际成交、销毁交易和流通变化。

第十部分：安全与运行保障

35. 威胁模型

协议重点防护：合约重入与重复领取、异常 ERC-20、签名重放、验证方串谋、赛果覆盖、预言机操纵、行情数据不可用、多账户与同局合谋、密钥失陷、治理攻击、链重组、RPC 中断、稳定币脱锚和外部托管违约。

链下风险评分只用于触发审查、限制或申诉，不直接秘密改变排名。确认作弊必须形成可审计的规则命中记录；被冻结方可在通知后 72 小时内申诉，仲裁方在申诉截止后 7 日内作出链上终局决定。

36. 核心安全不变量

1. 单场实际到账报名款与赞助款始终等于金库余额、累计领取、累计退款、已划协议费和已退赞助之和；
2. 奖金领取路径与退款路径互斥，二者累计均不得突破对应负债；
3. 已最终化结果根不可修改；
4. 同一领奖叶子只能消费一次；
5. 单期生态释放不超过 qE_e，累计释放不超过奖励池初始余额；
6. 总供应量只可因销毁下降；
7. 团队代币不得早于归属合约释放；
8. 暂停权限不能把参赛资产转移给权限持有人，也不能在有界暂停到期后阻止领取。

37. 工程验证

- 合约单元测试、属性测试、模糊测试和主网分叉测试；
- 引擎 golden fixtures：同一输入在不同机器和版本生成相同状态根；
- 行情断流、乱序、重复、跳变和时钟偏移故障注入；
- 领奖、退款、取消、重组和异常代币的端到端演练；
- 主网上线前完成两次独立合约审计和一次独立赛事引擎审计；
- 审计 commit、修复记录、部署字节码和验证源码公开；
- 上线后运行漏洞赏金和链上监控，热密钥每 90 日轮换，安全事件 24×7 值班。

38. 性能与灾备目标

Protocol v1 的受控主网验收 SLA 固定为：行情端到端延迟 p95 不超过 500 ms、p99 不超过 1 s；指令确认 p95 不超过 200 ms、p99 不超过 500 ms；单赛事持续吞吐不低于 5,000 指令/秒；赛果发布 p95 不超过赛事结束后 15 分钟，硬上限 2 小时；完整回放耗时不超过原赛事时长的 50%；月度可用性不低于 99.95%；已承诺日志 RPO=0，未承诺日志 RPO 不超过 30 秒，RTO 不超过 15 分钟。

赛事事件日志在 3 个可用区同步复制，关键状态采用追加写和每 30 秒快照。灾备切换不得重置接收序号或生成两个有效结果根；无法保证单一确定结果时，必须取消受影响赛事并退款。

第十一部分：实施路线

39. 分阶段交付

阶段	技术交付	验证门槛
Phase 0：2026-09-30	规则 schema、引擎 fixtures、经济参数文件、威胁模型	规范测试向量 100% 通过
Phase 1：2026-12-31	TC/USDC 金库、赛事状态机、Merkle 领奖、回放工具	测试网连续 100 场赛事，零个未解决 Critical/High 缺陷
Phase 2：2027-03-31	固定供应、归属、时间锁、5-of-7 验证、数据面板	两家独立审计零个未解决 Critical/High；以 1,000,000 USD 资金上限运行 90 日
Phase 3：2027-09-30	验证节点扩展、技术 API、白标赛事、公开回放索引	独立复算成功率不低于 99%，月度可用性不低于 99.95%
Phase 4：2028-06-30	证明系统研究实现与 TC 投票治理演练	证明系统完成独立审计，单场证明成本不超过奖池 0.5%

每一阶段必须同时满足表中日期和验收门槛；未满足验收门槛时不得进入下一阶段。

第十二部分：风险与法律边界

40. 技术风险

智能合约、赛事引擎、验证器、预言机、RPC、密钥管理和数据存储均可能出现漏洞或中断。审计和形式化不变量能够降低但不能消除风险。混合架构在 v1 仍依赖运营方和验证方诚实执行。

41. 经济风险

TC 可能缺乏需求、流动性不足、价格剧烈波动或归零。销毁、回收、POL 和释放衰减均不保证价格上涨。外部赛事收入下降会同步降低回收预算和奖励释放，也可能使现金运营无法覆盖成本。团队、财库或战略储备释放会增加流通压力。

42. 资产与对手方风险

稳定币可能脱锚、冻结或无法赎回；支付、托管、行情和云服务商可能违约或中断；链上资产与法币资产的法律追索路径不同。协议只能约束其控制范围内的链上合约，不能以链上哈希替代外部托管责任。

43. 监管边界

不同司法辖区可能把技能型赛事、付费奖池、加密资产、回收操作或治理代币作不同认定。任何地区上线前均需完成当地法律分析、年龄和地域限制、制裁筛查、税务、数据保护、广告及消费者保护评估。白皮书中的技术分类不是监管机构的法律结论。

附录

附录 A：初始参数表

参数	初始值	硬边界或说明
赛事协议费率 τ	5%	新赛事可在 3% 至 7% 内治理调整
生态池初始余额 E_0	400,000,000 TC	不可补铸
epoch 时长	UTC 自然月	不可治理修改
单期释放率 q	1%	只能下调，合约硬上限 1%
奖励价值上限 α	净协议费的 20%	以 30 日中位 TWAP 换算
`F_target_floor`	100,000 USD / UTC 自然月	不可治理
回收预算占外部协议费	30%	变更需 30 天公告
回收执行量上限 λ	30 日中位日成交额的 5%	行情异常时为 0
单日 / 单市场回收上限	日成交额 1% / 0.5%	最大价格影响与滑点均为 1%
回收后销毁比例 ρ	初始 70%	可在 70% 至 100% 内治理调整，其余为目标 POL
TC 赛事费销毁比例	50%	链上自动执行
风险准备金目标	max(250,000 USD, 近 90 日入场金的 3%)	低于 250,000 USD 时停止外部资产新赛事
团队归属	12 + 48 个月	不可提前释放
普通变更时间锁	48 小时	重大经济变更另加 30 天公告
验证委员会	5-of-7	同一实际控制人最多 1 席
挑战 / 响应 / 仲裁	72 / 24 / 48 小时	仲裁超时自动取消退款
基础奖金 / 生态奖励领取	180 / 90 自然日	未领取资产按 §6 和 §21 处置
行情源 / quorum	5 个 / 3 个	4-5 源为 NORMAL，3 源为 DEGRADED
批处理 / 日志承诺	250 ms / 30 秒	Protocol v1 固定值
TGE 初始流动性	20,000,000 TC + 200,000 USDC	初始池比例 0.01 USDC/TC
战略储备	锁定至 2030-01-01	之后 36 个月按秒线性释放

附录 A 与正文共同构成 Protocol v1 的参数基线；部署记录只填写链上地址、交易哈希、审计版本和编译信息，不改变本表参数。

附录 B：规则集最小字段

```
protocolVersion / schemaVersion
engineCodeHash / rulesetHash
roundId
entryAsset / entryAmount / feeRate
registrationStart / lockTime / startTime / endTime
instrumentSet / marketCalendar / pricePrecision
initialEquity / leverageLimit / positionLimit
orderTypes / batchInterval / fillModel / costModel
oracleSources / quorum / staleThreshold / deviationThreshold
rankingFormula / tieBreakers / eliminationCheckpoints
payoutCurve / challengePeriod / claimWindow
verifierSetId / verifierThreshold / arbitrationRules
logCommitInterval / roundSeedPolicy
haltPolicy / cancelPolicy / refundPolicy
```

附录 C：链上事件最小集合

```
RulesetRegistered
TournamentCreated
EntryDeposited
TournamentLocked
TournamentStarted
CommandLogRootCommitted
ResultCommitted
ResultChallenged
ChallengeResolved
ResultFinalized
TournamentCancelled
ClaimPauseTriggered
ClaimPauseReleased
RewardClaimed
EntryRefunded
EmissionReserved
EmissionReturned
RevenueAttestationSubmitted
RevenueAttestationChallenged
RevenueAttestationFinalized
TokenRecovered
TokenBurned
POLFunded
ReserveFunded
UnclaimedPrizeTransferred
VestingClaimed
TreasuryOperationQueued
TreasuryOperationExecuted
```

附录 D：公开验证材料

每次主网版本必须公开以下全部材料：合约地址与源码验证链接、代码 commit、编译配置、审计报告、管理员与多签地址、时间锁参数、代币分配地址、归属计划、赛事引擎镜像摘要、规则 schema、回放工具、经济参数 JSON、月度资产与供应报表。

Trading Challenge 技术与经济白皮书 v4.0 正式版 · 本文件不构成投资建议、收益承诺或任何金融产品要约。