公平挖矿 Fair 协议白皮书

2026 年 6 月 · 基于 BSC 主网已部署合约（当前活跃部署 Gen3）的技术修订版

目录

摘要

公平挖矿 Fair（Fair Mining，生态品牌 FairFi）是部署于 BNB Smart Chain（BSC）主网的应用层智能合约协议。协议以 FAIR 为挖矿产出通证，以 CBTC 为价值计量本位币，围绕 600 秒一个 epoch 的逻辑结算节拍，实现递减发行、存款再分配、三级推荐、质押分红、FOMO 奖池与惰性结算。

本文所称 epoch，是协议内部以 `block.timestamp` 划分的固定时间窗口，每个 epoch 长度为 600 秒。Fair 并非独立 L1，也不运行自有节点网络或自有共识协议。其交易排序、区块生产与终局性全部继承 BSC 的 Parlia PoSA 共识。协议自身只定义链上状态推进规则，即在 BSC 区块时间之上构造一个 10 分钟粒度的逻辑会计时钟。

FAIR 的理论供应硬顶为 21,000,000 枚，18 位小数。发行曲线参考比特币的递减货币政策：初始每 epoch 最多释放 50 FAIR，每 210,000 个 epoch 减半。若某个 epoch 无有效存款，则该 epoch 对应奖励不铸造，并计入放弃发行量，因此实际终态供应严格小于 21,000,000。FAIR 无预挖、无团队预留、无投资人份额、无基金会或国库分配，全部通过挖矿释放。FAIR 不承载治理投票权，其真实用途包括挖矿产出凭证、质押标的、分红资格门槛与复投介质。

协议存款本金以 CBTC 计价，存入后不可赎回。每笔有效存款被合约按固定比例拆分为三条现金流：15% 三级推荐奖励，45% 质押分红，40% FOMO 奖池。协议本身不保留手续费，不设置抽成，也不存在管理员可提取的协议收入。需要明确的是，这三条 CBTC 现金流属于参与者之间的再分配，协议不创造外生收益，个体期望收益可能为负。

Fair 的工程设计重点在于可验证规则、保守会计与受限治理。FAIRToken 的铸造权限永久绑定至 GameVault，setupAdmin 已在链上清零。GameVault 无 owner，仅设置 guardian 多签，用于暂停入口、管理有限配置与执行延迟变更。claim 类函数不受 pause 限制，用户在协议暂停时仍可提取已归属份额。该设计强化资金不可扣留属性，同时也削弱治理方在外部攻击场景下冻结提现的应急能力。

本文从技术架构、通证经济、安全模型、治理边界、路线图、合规风险与部署事实等方面，对 Fair 协议进行工程化描述。文中所有机制事实均以已部署合约及给定源码级调研材料为依据。

1. 引言

链上发行协议的核心问题并非只在于如何分配通证，而在于参与者能否独立验证分配规则、资金流向与权限边界。许多发行类项目依赖项目方口头承诺、可升级合约、隐藏手续费、预挖份额或链下分配表。此类设计在信息不对称环境下会放大逆向选择：诚实参与者无法区分规则是否真正固定，理性参与者则必须将管理员行为、隐含抽成和未来篡改纳入风险定价。

Fair 采用一种更受约束的应用层协议设计。其基本目标不是提供链下收益承诺，也不是构造独立共识网络，而是在 BSC 的 EVM 执行环境中，将发行曲线、存款拆分、分红条件、FOMO 触发规则与领取流程固化为可验证合约逻辑。协议的信任锚不建立在团队身份上，而建立在源码验证、不可逆放权与链上状态可复核之上。

Fair 的发射时间为 UTC 2026 年 6 月 3 日 10:18:00，即 UTC+8 2026 年 6 月 3 日 18:18:00，对应 `launchTime = 1780481880`。该时刻为 epoch 0 的起点。此后，协议以 600 秒为一个 epoch 推进内部会计状态。BSC 当前提供约 0.75 秒出块与快速终局性，Fair 在此基础上将约 800 个 BSC 区块聚合为一个逻辑结算窗口。

协议的关键资产为 FAIR 与 CBTC。FAIR 是挖矿产出通证，合约硬顶 21,000,000，18 位小数。CBTC 是协议的价值计量本位币，地址为 `0x18d0e455B3491E09210292d3953157A4Bf104444`，名称与符号均为「比特币」，18 位小数，固定供应 1,000,000,000。CBTC 不是币安官方 BTCB，后者地址为 `0x7130d2A12B9BCbFAe4f2634d864A1Ee1Ce3Ead9c`。GameVault 的 CBTC 地址为 immutable，不存在切换至 BTCB 或其他资产的开关。

本文使用「惰性结算」描述一种按需推进状态的会计方法：协议不依赖中心化 keeper 在每个 epoch 边界即时结算所有账户，而是在用户交互、主动 checkpoint 或领取函数中分页推进必要状态。该模型将全局结算成本摊销至多次调用，并通过 `maxEpochs` 参数限制单次交易的循环规模。

本文使用「X18 定点数」描述以 `1e18` 为缩放因子的整数定点会计表示。由于 Solidity 中整数除法向下取整，Fair 的挖矿、分红与 FOMO 会计均采用 floor 舍入，方向保守，即只可能少发，不会超发。舍入产生的 dust 会沉淀在合约中，无人可提取。

2. 问题陈述

链上公平发行协议面临三类问题。

第一类是规则可信度问题。若发行合约存在可变铸币权限、未披露预留、可升级逻辑或管理员可调比例，则参与者无法仅凭前端叙述判断未来供应和资金流向。即使初始承诺合理，管理员也可能在后续改变规则。此类风险在匿名团队项目中尤为重要，因为参与者难以依赖法律追索或声誉机制约束项目方行为。

第二类是会计可扩展性问题。许多链上博弈协议在结算时需要遍历大量用户或历史轮次。若每次全局结算复杂度随参与者数量线性或平方增长，协议在高参与度下会面临 gas DoS。FOMO 类协议尤其容易在末段触发交易拥堵，参与者为了抢占时序而集中提交交易，进一步放大 MEV 与排序风险。

第三类是资金流透明度问题。若存款进入不透明池、由链下规则再分配，或者合约允许管理员提取所谓运营费，参与者难以验证资金是否按规则流向推荐人、分红参与者与奖池。传统 FOMO3D 类机制提供了链上群体博弈先例，但也暴露出奖池触发、时序竞争与结算成本方面的工程缺陷。

Fair 对上述问题的回应包含四个约束。

首先，FAIR 发行逻辑由合约固化，铸造权仅属于 GameVault，Token setupAdmin 在完成绑定后清零。其次，存款本金 100% 以固定比例再分配，协议零抽成。再次，挖矿与分红采用 O(1) 指数会计，历史结算采用 `maxEpochs` 分页，避免单次调用遍历不可控集合。最后，治理权限被限制在入口暂停、有限配置与延迟变更范围内，不能修改分配比例、不能动用用户应得份额、不能增发 FAIR。

这些约束并不消除所有风险。CBTC 的市场价值、初始分布与流动性并非 Fair 合约可控制事项；FOMO 机制仍具备时序博弈性质；Router 集成 DEX 时暴露于 MEV；匿名团队带来运营方不可追索风险。白皮书必须将这些风险纳入协议模型，而非将其视为外部噪声。

3. 解决方案概述

Fair 是一个由四个核心合约构成的 BSC 应用层协议：

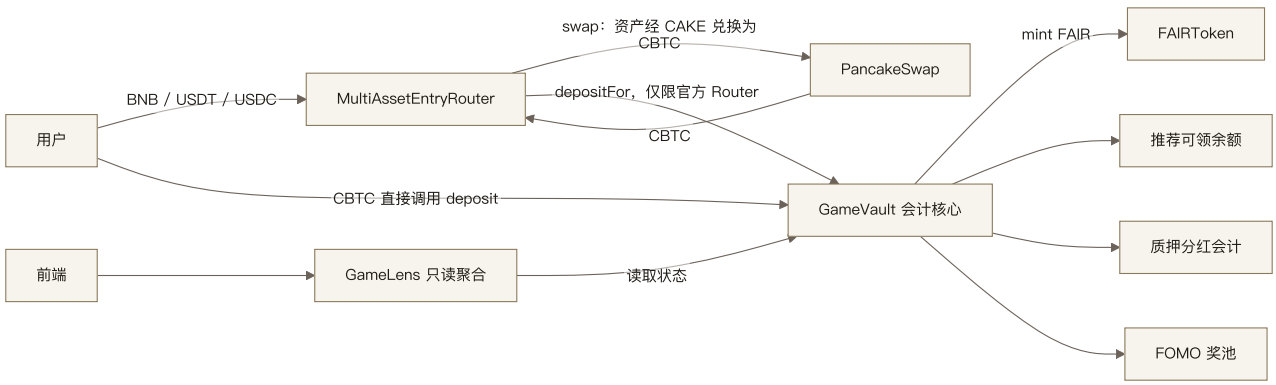

图 1 · 系统架构与合约拓扑

FAIRToken 负责 ERC20 通证表示与受限铸造。GameVault 是协议会计核心，管理 epoch 挖矿、存款拆分、推荐返佣、质押分红、FOMO 奖池和领取状态。GameLens 是无状态只读聚合层，面向前端提供 dashboard、排行榜与活动流。MultiAssetEntryRouter 是多资产入口，将 BNB、USDT、USDC 等资产经 PancakeSwap 路径兑换为 CBTC 后调用 GameVault 入金。用户也可以直接持有 CBTC 并调用 GameVault 的 `deposit`。

协议资金流如下：

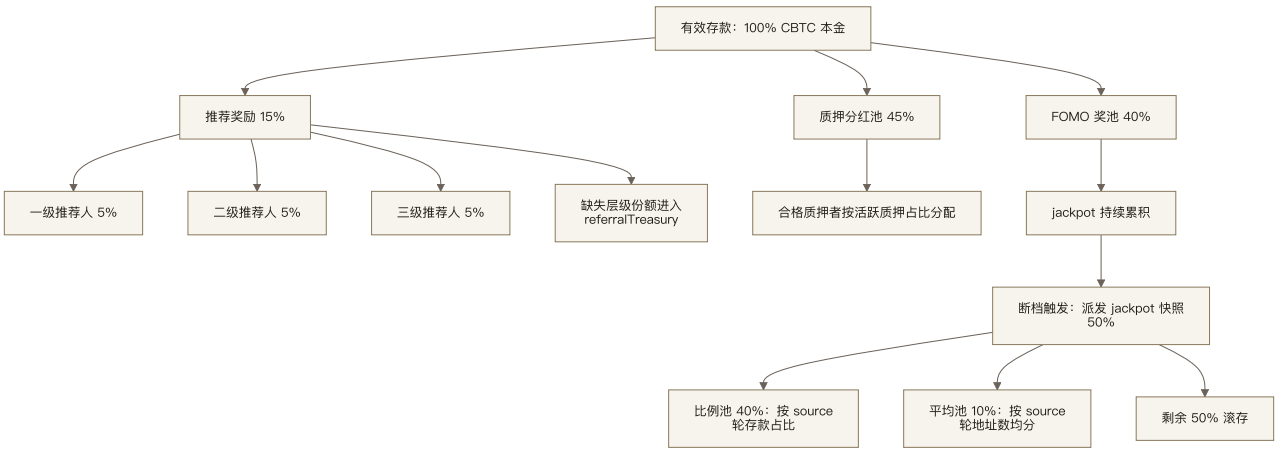

图 2 · 存款资金流拆分

每笔有效存款中的 15% 分配至三级推荐，每级 5%。缺失推荐层级对应份额不返还存款人，也不重分配给其他推荐人，而进入 referralTreasury。45% 进入质押分红逻辑；只有单地址活跃质押不少于 50 FAIR 的地址才计入合格分红地址，且全局合格地址数不少于 10 时新分红才释放。40% 进入 FOMO 奖池。

FOMO 状态机如下：

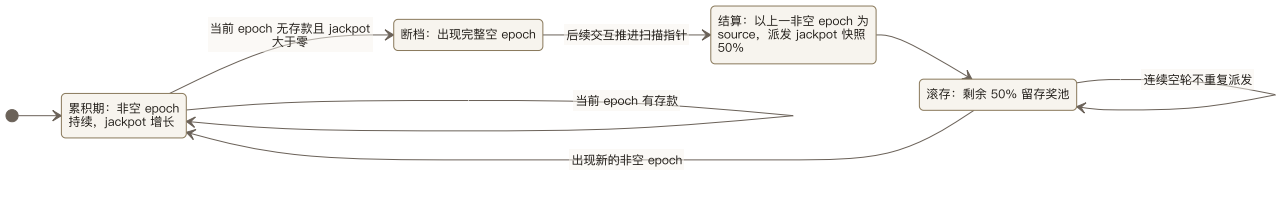

图 3 · FOMO 奖池状态机

若一个非空 epoch 之后出现空 epoch，则以上一个非空 epoch 为 source 触发 FOMO 结算。结算派发 jackpot 快照的 50%，其中 40% 按 source epoch 内用户存款占比分配，10% 按 source epoch 参与地址数平均分配，剩余 50% 滚存。连续空 epoch 只会派发一次，因为后续空轮自身不是有效 source。

核心结算流程如下：

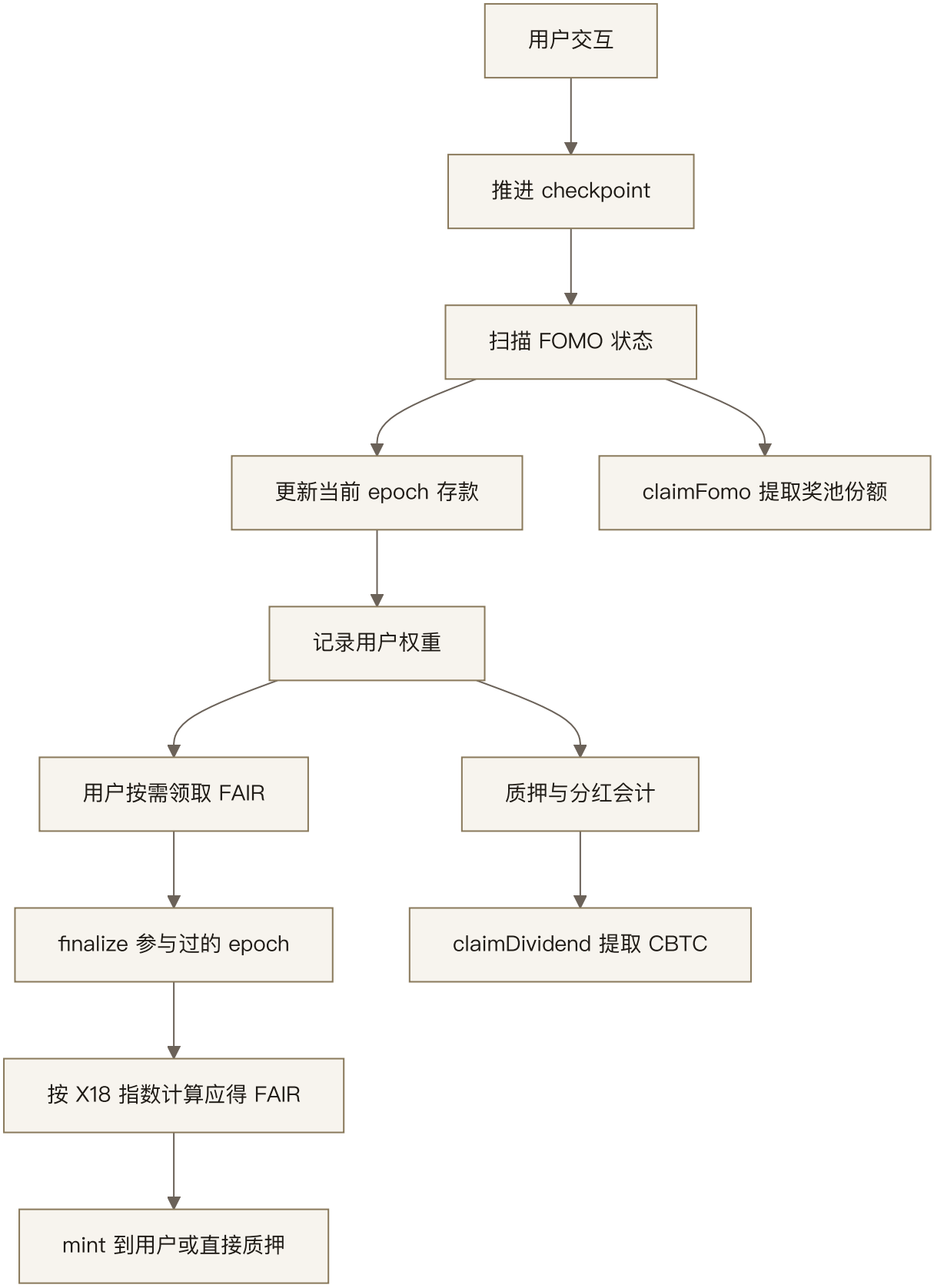
用户交互
推进 checkpoint
扫描 FOMO 状态
更新当前 epoch 存款
claimFomo 提取奖池份额
记录用户权重
用户按需领取 FAIR
质押与分红会计
finalize 参与过的 epoch
claimDividend 提取 CBTC
按 X18 指数计算应得 FAIR
mint 到用户或直接质押

图 4 · 核心结算流程

该方案的关键工程属性是最终一致性。协议不要求每个 epoch 边界立即完成全局结算。任何人可通过 `checkpoint(maxEpochs)` 或 `settleFomo(maxEpochs)` 推进状态；用户领取时也只结算自身真实参与过的 epoch。所有循环均受上限参数约束，避免不可控 gas 消耗。

4. 技术架构

4.1 网络与节点架构

Fair 部署于 BNB Smart Chain 主网，chainId 为 56。协议不运行独立节点，不维护 P2P 网络，不拥有独立区块生产者集合，也不定义自有共识规则。其可用性、交易排序、重组风险、区块时间与终局性均继承 BSC。

系统拓扑为单链四合约结构：

1. FAIRToken：ERC20 通证合约，18 位小数，`MAX_SUPPLY = 21,000,000 FAIR`。仅 GameVault 可 mint。setupAdmin 在绑定 vault 后自毁，链上已为 `0x0`。
2. GameVault：协议状态与资金核心，管理所有会计路径。无 owner，仅有 guardian 多签权限。
3. GameLens：只读聚合合约，不持有资金，不改变状态。
4. MultiAssetEntryRouter：多资产入口合约。其 owner 可调整 swap 路径、滑点与资产白名单，但 `setVault` 永久 revert，vault 地址不可更换。

外部依赖主要为 PancakeSwap。BNB、USDT、USDC 经预设路径兑换为 CBTC，路径形态为 `asset → CAKE → CBTC`。Router 默认滑点上限为 1000 bps，即 10%。用户若希望避免 DEX 路径带来的滑点与 MEV 暴露，可直接持 CBTC 调用 GameVault 的 `deposit(amount, referrer)`。

GameVault 的 CBTC 地址为 immutable，因此协议价值本位币不可替换。该设计降低后门风险，但也将协议永久绑定至 CBTC 的市场与合约属性。

4.2 共识机制

Fair 自身不存在共识机制。作为 BSC 上的智能合约系统，Fair 的执行结果由 BSC Parlia PoSA 共识确认。Parlia PoSA 结合权益授权与验证者轮换机制，BSC 提供约 0.75 秒出块和快速终局性。Fair 合约不参与验证者选择，不影响区块排序规则，也无法改变底层链终局性。

协议自身定义的是逻辑时钟：

`currentEpoch = floor((block.timestamp − launchTime) / 600)`

其中 `launchTime = 1780481880`，epoch 长度为 600 秒。一个 epoch 约对应 800 个 BSC 区块，但实际区块数会随区块时间波动而变化。epoch 边界由 `block.timestamp` 判定，因此验证者在边界附近存在极小的时间戳选择空间。由于 epoch 粒度为 10 分钟，该影响通常小于秒级链上游戏中的时间戳风险，但在 FOMO 边界时仍应纳入威胁模型。

状态推进遵循按需原则。deposit 会顺带推进有限步 checkpoint 与 FOMO 扫描；任何人可主动调用 checkpoint 或 settleFomo；claimFair 会按用户真实参与历史 finalize 对应 epoch。协议不依赖中心化 keeper，keeper 只可作为可用性辅助，而非安全必要条件。

4.3 数据模型、状态机与执行环境

Fair 的执行环境为 EVM，合约语言为 Solidity ^0.8.24。四合约均无外部库依赖，ERC20 与 safeTransfer 由项目自实现。Solidity ^0.8 系列内置整数溢出检查，降低传统算术溢出风险。

epoch 数据模型包含：

1. epoch 总存款量。
2. 用户在该 epoch 的存款量。
3. epoch 是否已 finalized。
4. rewardPerShareX18。
5. FOMO source 状态、奖池快照、已领取标记。

挖矿会计使用 X18 定点数：

$$rewardPerShareX18 = floor(epochReward \times 1e18 / epochTotalDeposit)$$

用户应得 FAIR：

$$userFair = floor(userDeposit \times rewardPerShareX18 / 1e18)$$

当 epoch 无存款时，奖励不铸造，计入 `forfeitedFair`。当 epoch 有存款时，所有用户可领取量之和不超过该轮理论释放量。由于两次 floor 舍入，微小 dust 会残留在合约会计中，不会导致超发。

分红使用 MasterChef 式累积指数：

$$accDividendPerShareX18 \mathrel{+}= floor(distributable \times 1e18 / totalActiveStake)$$

用户可领取分红：

$$pending = floor(userStake \times accDividendPerShareX18 / 1e18) - rewardDebt$$

每次 stake、unstake 或 claim 后更新 rewardDebt，使用户只领取增量分红。该模型避免遍历所有质押者，单用户操作为 O(1)。

舍入方向在挖矿、分红、FOMO 中保持一致：全部向下取整。该策略牺牲少量精确性，换取偿付安全，即合约不会因累计四舍五入而超发或透支。

4.4 关键子系统

存款拆分

每笔有效 CBTC 存款要求不低于 0.1 CBTC。存入后本金不可赎回，立即按固定比例拆分：

去向	比例	说明
三级推荐	15%	每级 5%，缺失层级进入 referralTreasury
质押分红	45%	分配给合格 FAIR 质押者
FOMO 奖池	40%	进入 jackpot，等待断档触发
协议抽成	0%	无协议手续费与管理员抽成

本金不可赎回是协议定义的一部分。存款不是可撤回存款账户，而是消费性参与行为，换取当前 epoch 的 FAIR 挖矿权重及相关博弈暴露。

三级推荐

推荐关系在用户首次入金时绑定。用户可显式指定 referrer；若未指定，则使用 fallbackReferrer。通过 fallbackReferrer 绑定的用户拥有 48 小时改绑窗口，且仅可改绑一次。系统包含 2–3 层防环校验，禁止形成短环推荐关系。

下线每次有效入金时，一级、二级、三级推荐人各获得 5% CBTC 可领取余额。缺失层级对应份额进入 referralTreasury，初始指向 guardian 多签。该设计使每笔入金的推荐流出恒定为 15%，避免因推荐链缺失改变其他资金池比例。

质押分红

FAIR 持有人可 stake FAIR 获取 45% 存款流对应的 CBTC 分红。单笔质押不少于 50 FAIR。单地址活跃质押不少于 50 FAIR 才计入合格分红地址；全局合格地址不少于 10 个时，新分红才释放。若合格地址数跌回 10 个以下，新分红暂停累积，条件恢复后继续。

解押采用两步流程：先 requestUnstake，再等待 24 小时冷却，之后 claimUnstaked。冷却期内可 cancelUnstake。部分解押要求取出量与剩余活跃质押均不少于 50 FAIR；当活跃质押低于门槛时，只允许全额解押。

FOMO 奖池

FOMO 奖池接收每笔有效存款的 40%。当一个非空 epoch 之后出现空 epoch 时，以上一个非空 epoch 为 source 触发结算。结算派发 jackpot 快照的 50%，其中 40% 按该 source epoch 内用户存款占比分配，10% 按参与地址数平均分配，剩余 50% 滚存至后续奖池。

FOMO 设计同时包含比例激励与参与人数激励。比例池奖励较大存款权重，平均池则为小额参与者保留固定份额暴露。但该机制无法消除边界补单、阻止断档与大资金占优等博弈行为。

惰性结算

惰性结算是 Fair 的核心可扩展性机制。协议不在每个 epoch 结束时遍历所有用户，而是通过以下路径推进状态：

1. deposit 顺带推进有限步 checkpoint 与 FOMO 扫描。
2. 任何人可调用 `checkpoint(maxEpochs)`。
3. 任何人可调用 `settleFomo(maxEpochs)`。
4. 用户 claimFair 时只 finalize 自己参与过的 epoch。
5. claimFomo 只领取已结算且用户有份额的 source epoch。

claimFair 不设最低领取数量门槛；claimFairAndStake 要求单次领取量不少于 50 FAIR，并将其直接转为立即生效的活跃质押。所有循环均受 `maxEpochs` 上限约束，使调用者可控制 gas 风险。其代价是 FOMO 结算可能晚于实际 epoch 边界，需要等待后续交互推进扫描指针。账目仍保持最终一致。

多资产入口

MultiAssetEntryRouter 支持 BNB、USDT、USDC、CBTC 四种前端入口。除 CBTC 直接入金外，其他资产通过 PancakeSwap 预设路径（asset → CAKE → CBTC）兑换为 CBTC 后调用 vault.depositFor；GameVault 的 depositFor 仅接受当前 depositRouter 调用。GameVault 在入金路径上使用 balanceBefore 与 balanceAfter 实测到账，以兼容转账税资产或实际到账偏差，并以独立会计余额隔离直接向合约打款对记账的干扰。因此参与资格与分配基于有效到账数量，而非前端输入面板的理论值。

Router owner 可调整 swap 路径、滑点和资产白名单。当前 owner 与 guardian 为同一多签。该权限可用于维护流动性路径，也可能在恶意或错误配置下使用户遭受不利兑换。因此直接 CBTC 入金是规避 Router 风险的路径。

4.5 可扩展性、性能与资源模型

Fair 的核心状态更新以 O(1) 为目标。挖矿采用 epoch 级 rewardPerShareX18，分红采用全局 accDividendPerShareX18 与 rewardDebt。用户 stake、claimDividend、claimReferral、claimUnstaked 等操作不需要遍历其他用户。

历史 epoch 处理无法完全 O(1)，因为用户可能跨多个 epoch 参与。协议通过 `maxEpochs` 分页限制单次处理数量，使复杂度为 O(k)，其中 k 由调用者选择。该策略防止历史积压导致某个领取函数永久不可执行。

FOMO 扫描同样使用分页。连续空轮不会重复派发，因为只有非空 source 可触发结算。deposit 顺带推进少量状态，有助于在正常交互中逐步消化历史任务。

GameLens 是只读层，面向前端展示 dashboard、排行榜与活动流。其资金安全风险较低，因为不持有资产、不写状态。但排行榜存在 $O(n^2)$ 全量遍历局限，当参与者达到数千级时，链上只读调用可能超时或前端不

可用。该问题不影响 GameVault 的资金安全，但会影响用户体验。合理缓解方式是引入链下索引服务。该索引服务如未来建设，应被视为可用性层，而非结算权威。

4.6 密码学、安全模型与威胁分析

Fair 使用 EVM 标准密码学假设，包括账户签名、交易哈希、区块确认与 BSC 共识安全。协议不引入额外零知识证明、门限签名或自有密码原语。

技术威胁模型包括以下方面。

重入面：GameVault.deposit 无 nonReentrant，依赖 CBTC 为无转账回调的标准 ERC20。当前 CBTC 已验证无 hook、无税、无黑名单、无交易限额，且 vault 的 CBTC 地址 immutable，因此该假设对当前绑定代币恒定成立。然而这仍是隐式依赖。合约整体基本遵循 CEI，即先更新状态再执行外部转账，并使用 safeTransfer 封装。

MEV 与 DEX 风险：Router 多跳路径可能遭受三明治攻击，默认 10% 滑点上限较宽。攻击者可在用户 swap 前后操纵价格，使用户以不利价格换入 CBTC。缓解方式包括用户直接 CBTC 入金、Router owner 调低滑点、前端基于池深动态报价，以及用户自行设置更严格交易参数。

时间戳依赖：epoch 边界由 `block.timestamp` 判断。BSC 验证者在区块时间戳上存在有限选择空间，因此 FOMO 边界处可能出现细微时序影响。由于 epoch 为 600 秒，单区块时间戳扰动通常不改变长期发行节奏，但在临界交易排序中可能影响某笔交易归属。

会计自洽性：FAIR 发行由 `epochReward` 与 `MAX_SUPPLY` 双重约束。空轮不铸造，已铸造量不会超过理论上限。挖矿、分红与 FOMO 均使用 floor 舍入，任何用户可领合计不超过对应池余额。dust 沉淀方向安全，但会降低完全分配精度。

权限边界：guardian 不能转移用户已归属资金，不能修改分配比例，不能增发 FAIR。其主要风险在于暂停新入口、调整 fallbackReferrer、调整 referralTreasury、调整 depositRouter，以及作为 Router owner 修改兑换路径和滑点。治理权不是零风险，但其可作恶范围受到合约结构限制。

5. 通证经济模型

5.1 通证用途

FAIR 是协议的挖矿产出通证，18 位小数。其用途限于协议内真实功能，不包含治理投票权。

用途	机制	说明
挖矿产出凭证	按 epoch 内存款占比分配	用户通过有效 CBTC 存款获得当前 epoch 的 FAIR 权重
质押标的	stake FAIR	质押者获得 45% 存款流对应的 CBTC 分红
分红资格门槛	活跃质押不少于 50 FAIR	低于门槛不计入合格分红地址
复投介质	claimFairAndStake	单次领取不少于 50 FAIR 时可直接转为活跃质押
治理权	无	FAIR 不承载代币投票，治理主体为 guardian 多签

FAIR 的市场价格由二级市场决定。协议不承诺回购、不承诺收益率、不承诺价格稳定，也不将 FAIR 设计为对外生现金流的法律索取权。协议内 CBTC 分红来自后续参与者存款再分配，不构成外部经营收益。

5.2 供应机制与货币政策

FAIR 固定供应硬顶为 21,000,000。每个 epoch 最多释放量为：

`epochReward(e) = 50 FAIR >> floor(e / 210000)`

右移实现按 wei 级整数减半。理论几何级数为：

`210000 × 50 × (1 + 1/2 + 1/4 + ...) = 21,000,000`

合约层还设置 `MAX_SUPPLY` 硬顶作为双保险。若某 epoch 无人存款，该轮奖励不 mint，并计入 forfeitedFair。因此 21,000,000 是理论上限，不是最终必然供应量。

阶段	epoch 区间	每 epoch 释放	阶段释放上限	累计上限与占比	大致日历区间
1	0–209,999	50 FAIR	10,500,000 FAIR	10,500,000，50%	2026 年 6 月至 2030 年 5 月
2	210,000–419,999	25 FAIR	5,250,000 FAIR	15,750,000，75%	2030 年 5 月至 2034 年 5 月
3	420,000–629,999	12.5 FAIR	2,625,000 FAIR	18,375,000，87.5%	2034 年 5 月至 2038 年 5 月
4	630,000–839,999	6.25 FAIR	1,312,500 FAIR	19,687,500，93.75%	2038 年 5 月至 2042 年 5 月
n	依此类推	50 × 2^(1−n) FAIR	21M × 2^(−n) FAIR	21M × (1 − 2^(−n))	每约 3.995 年一阶段

该货币政策的机制含义是前期发行较高，随后边际发行持续下降。早期参与者承受较高不确定性与较高博弈波动，同时获得较高单位 epoch 发行暴露。后期参与者面对更稀缺的新增供应，但协议能否维持分红与奖池规模取决于持续存款需求，而非发行曲线本身。

5.3 分配、发行与锁仓安排

FAIR 无预挖、无团队预留、无投资人份额、无基金会或国库分配。全部 FAIR 通过 GameVault 按 epoch 规则 mint。

分配类别	数量上限	占理论总量	锁仓安排	释放方式
挖矿产出	⩽ 21,000,000 FAIR	⩽ 100%	无统一锁仓	按 epoch 存款权重释放
团队	0 FAIR	0%	不适用	不适用
投资人	0 FAIR	0%	不适用	不适用
基金会或国库	0 FAIR	0%	不适用	不适用
空投	0 FAIR	0%	不适用	不适用
空轮放弃量	不铸造	不计入流通	不适用	计入 forfeitedFair

CBTC 现金流分配如下：

CBTC 去向	比例	受益方	是否可由治理调整
三级推荐	15%	最多三层推荐人或 referralTreasury	分配比例不可调
质押分红	45%	合格 FAIR 质押者	分配比例不可调
FOMO 奖池	40%	FOMO source epoch 参与者	分配比例不可调
协议手续费	0%	无	不适用

锁仓设计方面，FAIR 本身没有团队锁仓，因为没有团队份额。质押 FAIR 属于用户主动选择的协议状态，解押需 24 小时冷却。该冷却并非发行锁仓，而是质押分红系统的退出规则。

5.4 激励机制与机制设计

Fair 的激励结构由四组参与者构成：存款挖矿者、推荐人、质押者、FOMO 参与者。单个地址可以同时扮演多个角色。

存款挖矿者用 CBTC 本金换取 FAIR 发行份额和 FOMO source 暴露。其策略变量包括存款规模、存款时点、是否直接使用 CBTC、是否绑定推荐链、是否参与 FOMO 边界博弈。由于 epoch 内 FAIR 发行固定，单个 epoch 中用户收益份额与其存款占比相关。若其他存款增加，既稀释 FAIR 份额，也增加 FOMO 与分红资金池。

推荐人获得下线每次存款的固定 5% 层级奖励。该机制为网络扩散提供直接激励，但也会引入拉新导向。存款人的推荐支出恒定为 15%，绑定与否不改变其自身成本；绑定只决定该份额流向其推荐网络还是 referralTreasury。防环校验减少自循环套利，但不能消除多地址策略。

质押者通过锁定 FAIR 获得 45% CBTC 分红。分红门槛要求单地址活跃质押不少于 50 FAIR，且全局合格地址不少于 10 个。这降低了极小额地址制造状态噪声的动机，并要求分红系统具备最低参与广度。质押者承担 FAIR 市场价格波动和 24 小时解押冷却风险。分红来自新存款，若后续参与下降，分红也会下降。

FOMO 参与者在断档前最后一个非空 epoch 中获得 jackpot 快照一半的分配权。比例池鼓励较大存款，平均池鼓励地址参与。该机制天然存在边界博弈：大资金可在临近 epoch 结束时补单，阻止空轮出现，并使自身成为下一次 source 的主要受益者。该行为不是合约漏洞，而是机制设计中的可预期策略空间。

从激励相容性角度，Fair 的主要优点在于规则可验证、比例固定、管理员无法事后改变支付函数。其主要局限在于整体资金流为零和再分配，协议不产生外部收入。理性参与者的期望收益取决于相对入场时点、后续参与流量、CBTC 市场价格、FAIR 市场价格、推荐网络与 FOMO 时序。

5.5 价值捕获、销毁机制与长期可持续性

Fair 的价值捕获不是协议抽成模型，而是质押分红模型。FAIR 持有者若选择质押，且满足分红资格，可获得后续存款流中 45% 的 CBTC 分红。因此 FAIR 的协议内功能价值来自其对分红资格的控制，而非治理权或手续费索取权。

协议不存在主动回购机制，也不存在明确的 FAIR 销毁机制。供应减少主要来自两类方向安全的非发行或沉淀：空 epoch 奖励不铸造，floor 舍入 dust 留在合约中。FOMO 未领取份额、Router 多转差额等也可能沉淀在 vault 中，无人可提。此类沉淀不是价值捕获收入，因为治理方和协议账户均不能提取。

长期可持续性取决于三项条件。

第一，CBTC 需要具备持续可用的市场流动性与稳定的合约属性。合约层已验证 CBTC 固定供应、owner 已 renounce、无税、无黑名单、无交易限额，但初始分布与流动性深度属于外部市场假设。

第二，FAIR 的质押需求需要与分红预期形成相对平衡。若后续存款减少，质押分红下降，可能削弱 FAIR 的协议内需求。发行减半只能降低新增供应，不能单独创造收入。

第三，FOMO 奖池需要足够透明且可领取。惰性结算降低 gas 风险，但用户仍需等待状态推进。若前端或索引可用性不足，用户体验可能下降，但链上 claim 路径仍存在。

安全预算方面，Fair 不以协议收入支付验证者或节点，因为底层安全由 BSC 提供。其安全预算表现为参与者愿意为 BSC gas、DEX 滑点和时间成本支付的总成本。若 BSC 安全性或可用性下降，Fair 无独立机制抵御该系统性风险。

6. 治理机制

Fair 采用弱治理与不可逆放权结合的模型。治理主体为 2/3 Gnosis Safe v1.4.1 多签，地址为 `0xed12F10f0Ba076658c97B632a0a8D1B6871EF28d`。多签包含 3 名签名人，阈值为 2。

guardian 可以执行的操作包括：

权限	说明	风险边界
pause 与 unpause	暂停或恢复 deposit、stake、bind 等入口	claim 类函数不受影响
管理 keeper	增删辅助推进状态的 keeper	不影响任何人主动推进状态的能力
修改 fallbackReferrer	调整兜底推荐人	影响未指定推荐人的新用户
修改 referralTreasury	调整缺失层级推荐份额接收方	可能截留缺级推荐分成
修改 depositRouter	调整官方 Router 地址	不影响用户直接 CBTC deposit
两步转移 guardian	schedule 后 24 小时 accept	可中途取消

guardian 不能执行的操作包括：

禁止事项	合约边界
动用用户本金或已归属 claim 份额	无对应提取路径
修改 15% / 45% / 40% 分配比例	比例固化
增发 FAIR	Token 铸造权仅属于 GameVault，且受 MAX_SUPPLY 限制
修改 FAIR 发行曲线	发行逻辑固化
冻结 claim 类函数	claim 不受 pause 限制

launch 后所有配置变更需 24 小时 timelock。`freezeKeepers` 与 `freezeFallbackReferrer` 可不可逆冻结相应配置。该设计为参与者提供观察窗口，降低突发治理变更风险。

Router 具有独立 owner，当前与 guardian 同地址。Router owner 可调整 swap 路径、滑点和资产白名单。该权限不属于 GameVault 核心会计，但会影响通过多资产入口参与的用户。因此治理风险评估必须同时覆盖 guardian 与 Router owner。

FAIR 不承载治理权，协议未采用代币投票。可治理范围本身已被压缩至少量运营参数，发行与分配规则不依赖任何投票流程。该结构降低了治理捕获与买票风险，但也意味着普通 FAIR 持有人不能通过链上投票改变协议配置。

7. 应用场景与实际用途

Fair 的实际用途可以分为四类。

第一，链上可验证发行。参与者可在 BSC 上独立核查 FAIR 发行曲线、每 epoch 存款权重、空轮放弃量、铸造记录与总供应。相较于链下分配表，合约发行降低了人工裁量空间。

第二，质押分红。FAIR 持有人可将 FAIR 质押为活跃 stake，满足门槛后参与 CBTC 分红。分红来自每笔新存款的 45%，而非外部经营收益。

第三，推荐网络激励。推荐人可获得下线存款流中的固定层级奖励。该机制适合链上社区传播，但也要求用户理解推荐奖励来自存款本金再分配。

第四，FOMO 群体博弈。参与者可围绕 epoch 断档条件进行策略博弈，并在 source epoch 中获得 jackpot 暴露。该机制具有显著的博弈性与风险性，不应被描述为稳定收益工具。

前端显示的年化收益率、预估分红、排行榜与活动流均为辅助展示。最终权益以主网合约状态与链上记录为准。

8. 实施路线图

Fair 已完成 BSC 主网部署，当前活跃部署为第三代（Gen3），此前两代部署已废弃；本文全部地址均指当前活跃部署。四合约源码均已在 BscScan 验证，链上交叉引用已验证一致。launchTime 已固定为 UTC 2026 年 6 月 3 日 10:18:00。

阶段	状态	技术里程碑
主网部署	已完成	FAIRToken、GameVault、GameLens、MultiAssetEntryRouter 部署于 BSC 主网
权限绑定	已完成	FAIRToken vault 绑定完成，setupAdmin 清零
发行启动	已完成	epoch 0 于 2026 年 6 月 3 日启动
第一发行阶段	进行中	epoch 0–209,999，每 epoch 最多 50 FAIR，预计至 2030 年 5 月
第二发行阶段	由减半曲线决定	epoch 210,000–419,999，每 epoch 最多 25 FAIR
后续发行阶段	由减半曲线决定	每约 3.995 年减半一次，理论供应逐步趋近 21M
链下索引层	规划中	缓解 GameLens 排行榜 $O(n^2)$ 只读调用局限
审计与形式化验证	规划中	引入第三方审计、关键不变量验证与公开报告
生态层工具	假设	可包括数据看板、风险提示、Router 报价优化与 FOMO 状态可视化

路线图中的发行阶段由合约曲线决定，不依赖团队主观安排。生态层规划若无已部署事实，应被视为规划中或假设，不构成承诺。

9. 安全、审计与形式化验证

截至本文撰写，协议未公布正式第三方审计机构报告。已有独立源码级评审与 Slither 静态分析结果显示，101 个 detector 产生 68 条结果，均为信息级，未发现 reentrancy、arbitrary-send、unchecked-transfer 级别问题。该结论支持「合约内部会计自洽、无直接盗取资金路径」的判断，但不能替代正式审计。

建议的形式化验证重点包括：

不变量	描述
FAIR 供应上限	任意状态下 totalSupply 不超过 21,000,000 FAIR
单 epoch 不超发	同一 epoch 所有用户领取合计不超过该 epoch reward
空轮不铸造	无存款 epoch 对应 reward 不 mint
CBTC 拆分守恒	每笔有效存款按 15% / 45% / 40% 进入对应会计路径
分红不透支	所有 pending dividend 合计不超过已分配分红余额
FOMO 不重领	同一 source epoch 同一用户不可重复领取
claim 不受 pause 影响	pause 状态下已归属 claim 路径仍可执行
guardian 权限边界	guardian 无法修改发行曲线、分配比例或铸造权限

安全评估还应覆盖 Router 层。尽管 GameVault 允许直接 CBTC 入金，前端用户可能主要依赖多资产入口。Router 的 swap 路径、滑点、资产白名单与 PancakeSwap 池深均会影响实际入金数量。形式化验证不能替代对外部 DEX 流动性和 MEV 风险的运行时监控。

10. 法律、监管与合规考量

Fair 包含挖矿发行、质押分红、推荐奖励与 FOMO 奖池机制。在多数司法辖区，此类机制可能涉及博彩、证券、集资、传销式激励或消费者保护相关法规的不确定性。协议为不可升级应用层合约，无 KYC、无地域屏蔽能力，也无链上身份识别流程。参与者需自行判断其所在司法辖区的合规责任。

FAIR 不承载治理权，不代表公司股权、债权或收益保证。CBTC 分红来自其他参与者存款再分配，不是经营利润分配。尽管如此，市场宣传、用户预期与二级市场交易仍可能触发不同法域下的监管分析。白皮书不构成法律意见、投资建议或收益承诺。

团队为匿名或化名团队。匿名并不必然意味着合约不可信，但会削弱传统法律追索、声誉约束与持续运营责任。Fair 的可信度主要来自链上可验证代码、权限收缩和不可逆放权。用户不应将团队身份背书作为主要信任来源。

11. 风险与缓解措施

风险	描述	缓解措施或权衡
CBTC 外部依赖	协议全部价值计量依赖 CBTC。CBTC 合约层固定供应、已弃权、无税、无黑名单，但初始分布、持仓集中度和流动性深度由发行方与市场决定	用户需独立核查 CBTC 分布与流动性。合约无法保护 CBTC 市场价格
零和博弈	三条 CBTC 现金流为参与者之间再分配，协议不创造外生收益，本金不可赎回	前端与文档应明确本金为消费性参与，预估收益不构成承诺
FOMO 时序博弈	大资金可在 epoch 边界补单阻止断档，并使自己成为下一次 source 主要受益者	属于机制固有策略空间。600 秒粒度降低秒级操纵敏感度，但不能消除
时间戳依赖	epoch 边界由 `block.timestamp` 判定，验证者在临界点有有限操纵空间	依赖 BSC 共识约束。用户应理解临界交易存在归属不确定性
DEX MEV	Router 默认滑点 10%，多跳路径增加三明治攻击暴露	用户可直接 CBTC 入金。owner 可调低滑点，前端可动态报价
条件性重入假设	GameVault.deposit 无 nonReentrant，依赖 CBTC 无回调	当前 immutable CBTC 已验证无 hook。仍建议未来审计重点覆盖
治理单点	guardian 可暂停入口、调整 referralTreasury、调整 Router 等	guardian 不能动本金、不能改比例、不能增发。配置变更有 24 小时 timelock
无冻结提现能力	claim 不受 pause 限制，强化不可扣留属性	若发生外部攻击，治理方无法阻止资金流出。这是有意权衡
GameLens 可用性	排行榜 $O(n^2)$ 全量遍历，大规模参与时可能超时	不影响资金安全。可通过链下索引缓解
dust 沉淀	floor 舍入、未领取 FOMO、Router 多转差额可能永久沉淀	方向安全，只少发不超发。无人可提取
审计状态	未公布正式第三方审计报告	已有源码级评审和 Slither 信息级结果，但仍需正式审计
团队匿名	运营方不可追索风险较高	信任锚转向代码验证、权限边界和链上事实
监管不确定性	博弈与奖池机制可能触及多法域监管	用户自行承担合规判断。协议无 KYC 与地域屏蔽

风险缓解不等同于风险消除。Fair 的设计优先保证合约规则不可随意篡改和已归属资金可领取，但这也减少了治理方在极端事件中的干预能力。

12. 结论

Fair 是一个部署于 BSC 的应用层智能合约协议，其核心设计是将发行、分配、分红、FOMO 与领取路径固化在链上，以减少预挖、隐藏抽成、任意改规则和资金流不透明等问题。协议不运行独立共识，不构造自有节点网络，而是在 BSC Parlia PoSA 共识提供的执行环境中，以 600 秒 epoch 实现逻辑结算。

FAIR 的货币政策具有明确硬顶和递减发行规则。空轮不铸造使实际供应低于理论上限。CBTC 本金按 15% 推荐、45% 分红、40% FOMO 奖池进行 100% 再分配，协议零抽成。O(1) 指数会计与 `maxEpochs` 分页降低了链上结算的 gas 风险。不可逆放权和弱治理限制了管理员可作恶范围。

同时，Fair 仍具有显著风险。CBTC 是项目生态自行发行的本位币，其市场价值和流动性是协议最重要的外部依赖。FOMO 机制具有固有时序博弈。Router 暴露于 DEX MEV。团队匿名与监管不确定性也需要被严肃对待。Fair 的合理评估方式应基于合约事实、会计不变量、权限边界、外部依赖与参与者博弈，而非基于收益承诺或叙事预期。

参考文献

1. Satoshi Nakamoto《Bitcoin: A Peer-to-Peer Electronic Cash System》，2008。
2. Ethereum Improvement Proposals《EIP-20: Token Standard》。
3. BNB Chain 官方文档《Parlia Consensus》：PoSA 共识机制。
4. SushiSwap MasterChef 合约：accumulated reward per share 与 rewardDebt 奖励会计模式。
5. FOMO3D（2018）：链上群体博弈与奖池机制先例。
6. Safe（原 Gnosis Safe）v1.4.1 多签合约与文档。
7. Solidity 官方文档（^0.8 系列）：整数溢出检查与 EVM 执行语义。
8. PancakeSwap 官方文档：AMM 与多跳 swap 路由执行模型。
9. BscScan：本协议全部已验证源码与 BSC 主网链上合约状态（参见附录地址表）。

附录

术语表

术语	定义
Fair	公平挖矿 Fair 协议，部署于 BSC 的应用层智能合约系统
FairFi	Fair 生态品牌
FAIR	协议挖矿产出通证，18 位小数，理论硬顶 21,000,000
CBTC	协议价值计量本位币，项目生态自行发行，不是币安官方 BTCB
epoch	协议内部 600 秒逻辑结算窗口
FOMO	以空 epoch 作为触发条件的奖池博弈机制
jackpot	FOMO 奖池余额或结算快照
X18 定点数	以 `1e18` 为缩放因子的整数定点会计表示
惰性结算	按需推进状态、分页处理历史任务的结算方式
rewardPerShareX18	挖矿 epoch 中每单位存款对应的 FAIR 奖励指数
accDividendPerShareX18	分红系统中每单位活跃质押对应的累计 CBTC 分红指数
rewardDebt	MasterChef 式会计中用于记录用户已结算分红基线的变量
guardian	协议有限治理多签，不是 FAIR 持有人投票机制
referralTreasury	缺失推荐层级对应 5% 份额的接收地址
dust	floor 舍入或多转差额造成的微小沉淀余额

关键参数总表

参数	值
部署链	BNB Smart Chain 主网
chainId	56
launchTime	1780481880
发射时间	UTC 2026 年 6 月 3 日 10:18:00，UTC+8 18:18:00
epoch 时长	600 秒
初始每轮释放	50 FAIR
减半周期	210,000 epoch，约 3.995 年
FAIR 理论上限	21,000,000
FAIR 小数位	18
最小存款	0.1 CBTC
推荐分成	每级 5%，共 3 级，合计 15%
分红占比	45%
FOMO 占比	40%
协议抽成	0%
分红资格	单地址活跃质押 ≥ 50 FAIR
分红启动条件	全局合格地址 ≥ 10 个
解押冷却	24 小时
推荐改绑窗口	48 小时，仅兜底绑定，限一次
治理 timelock	24 小时
FOMO 单次派发	jackpot 的 50%
FOMO 派发结构	40% 按存款占比，10% 按地址平均，50% 滚存
Router 默认滑点上限	1000 bps，即 10%
CBTC 供应	1,000,000,000
CBTC 小数位	18

链上部署地址表

合约或角色	地址
FAIRToken	`0xCAc6D8EC6D05fBCb7065edcfb7897a1633993876`
GameVault	`0x0375f966b518713FC4Ab89c3ABc6BA063376BC4A`
GameLens	`0xFA0AA68ffc7F98F5Dce6d72Ad5ca05911e7Af661`
MultiAssetEntryRouter	`0x3f8e213e5aEcd400C868765f1559968dB2c4F741`
CBTC	`0x18d0e455B3491E09210292d3953157A4Bf104444`
guardian 多签	`0xed12F10f0Ba076658c97B632a0a8D1B6871EF28d`
币安官方 BTCB，非本协议本位币	`0x7130d2A12B9BCbFAe4f2634d864A1Ee1Ce3Ead9c`