LightDAO 白皮书 V2.4(2026-09-26 主网实况版)

> 本版在 V2.0 设计稿基础上,前置「主网部署实况」与「版本变更」,并附录已验证的链上参数。正文(第一~十二章)保持 V2.0 设计不变;凡与实况有偏差处,以本节前注与附录为准。

版本变更(V2.0 → V2.4)

- 2026-11-04 勘误（不改版本号，仍为 V2.4）：附录《主网已验证参数与地址》原写金库 `treasury_multisig` 为 5/7 多签，与正文 §7.2/§7.3/§8.1 的 3/5 冲突，也与链上实测冲突（`{"signers":{}}` 返回 5 个地址，不存在 7 名签名人）；已按正文统一为 3/5，并标明阈值本身不在合约查询接口内、只能由部署记录佐证。同节原写挖矿根为「5/7 验证者多签」，实测可证的只有阈值 5（115 笔 `submit_root` 事件 threshold 全部为 5，实际签名账户恰好 5 个），7 席授权是设计目标、当前无链上证据，已改为相应措辞。

1. **§4.5 Gas 经济:已主网部署并验证**。USD 锚定动态 min-gas-price 与 50% 销毁 / 30% 验证者 / 20% 金库分配于 2026-09-24 经治理提案(v2-lightfee)在高度 58627 上线,7 验证者协调切换、测试网端到端彩排后执行。主网实测:不足额 fee 被拒、足额 fee 按 50/30/20 精确分配。
2. **原生 denom 厘清**:质押/治理/Gas 均为 `ulight`(LIGHT,6 位小数,总供应 25 亿)。genesis 误配的 `stake` 通胀已于 2026-09-24 经治理提案归零(mint inflation=0),LIGHT 发行完全由 mining_reward 合约承担,杜绝双重发行;存量 stake 为待处置的遗留 denom(见附录 C)。
3. **§4.7 WebRTC 中继:已部署**。8 节点 coturn(TURN/STUN,TLS 证书 turn-*.lightdao.net)+ WSS 信令 + REST 临时凭证(HMAC-SHA1);客户端 P2P 数据通道互中继,中继字节计入 40% 带宽贡献;端到端实测经 TURN 中继传输成功。对称 NAT 走 TURN 兜底,失败降级纯验证模式(与 §4.7 一致)。
4. **§4.9 智能钱包:已上线**。Passkey/WebAuthn 无种子登录(PRF 派生密钥 + AES-GCM 密文存储,明文不落地)+ Shamir 3-of-5 社交恢复;助记词作为回退选项保留。
5. **§4.10 价格预言机:喂价已运行**。7 验证者 cron 轮值向 oracle_twap 提交 external_median(当前参考价 50000 = $0.05);链上 TWAP 待 LIGHT/USDC 流动性池建立后启用。v3 升级后 lightfee 直接读 external_median 转动态 min-gas。
6. **参数治理**:v3 升级将 lightfee 的 BurnPct/TreasuryPct/TransferUsd/StaticPrice/OracleContract 迁入链上 paramstore,治理参数提案可运行时调整,无需再协调升级。

主网部署实况(2026-09-26)

- 链 `lightdao-mainnet-1`,7 验证者(JP/KR/SG/US/HK/FR/UK)全部 BONDED、无 jailed;满足 §4.7「验证者<7 不得 TGE」的硬性底线

- 客户端 https://lightdao.net(PWA):Passkey 钱包 + 挖矿 + WebRTC 中继 + 领取,多语言(中/英/西)
- 挖矿闭环:浏览器贡献 → 网关每日定稿 → Merkle 根 5 签上链(阈值 5,链上可查) → 矿工凭 proof 领取;每日根持续提交
- 升级治理:v2-lightfee(已应用 @58627)、mint 归零(已应用)、v3-lightfee(全票通过,高度 118055 自动切换)
- 完整端点/合约地址/升级历史见仓库 `docs/MAINNET_STATUS.md`

LightDAO 白皮书 V2.0

全文核查校对优化版（国际网页端 · 数值审计 · 三方审计 · 经济模型优化版）

发布日期：2026年8月4日

核心原则：浏览器即节点，全民可参与，利润按规则共享

法律定位：LIGHT 及子代币定位为生态贡献积分与 SPV 收益分配请求权凭证，不属于证券或理财产品；具体法律属性以相关司法辖区的有效法律意见为准。

> 本文件为白皮书全文核查校对优化版本，不构成投资建议、证券发行文件、理财产品说明或任何形式的保本承诺。请在参与前咨询法律、税务及财务专业人士。

目录

- 前置声明
- 序章：三个人的故事
- 第一章：我们看到的真相
- 第二章：LightDAO 的回答
- 第三章：合规与法律隔离
- 第四章：技术架构
- 第五章：代币经济模型
- 第六章：治理机制
- 第七章：权力制衡与角色定义
- 第八章：信任与安全机制

- 第九章：投资运营与退出策略
- 第十章：路线图
- 第十一章：社区文化与开发者生态
- 第十二章：团队与顾问
- 第十三章：风险提示与免责声明
- 附录A：关键参数汇总表
- 附录B：数值推导与校验
- 附录C：审计修正日志
- 附录D：术语速查索引

执行摘要

LightDAO 是什么： 一个让全球普通人通过浏览器参与真实企业投资并分享利润的去中心化自治组织。用户无需购买矿机、无需具备技术背景、无需满足合格投资者门槛——只需一个浏览器和少量时间，即可贡献网络资源获得LIGHT代币奖励，并通过治理投票参与投资决策。

解决什么问题： 全球后50%人口（约40亿人）仅拥有2%的总财富（世界不平等实验室，2026）。优质资产（私募股权、风险投资）被合格投资者门槛（$20万年收入/$100万净资产）排斥在外。加密货币领域虽有"全民参与"叙事，但绝大多数代币最终归零（CoinGecko 2025：1,156万个代币死亡），DAO治理参与率仅约3-12%。

怎么解决： 双引擎模型——70%资金投向社区级刚性消费资产（现金流引擎），30%投向前沿科技（增长引擎）。投资通过开曼SPV执行，利润按链上规则分配：40%给子代币持有者、30%回金库再投资、20%回购LIGHT销毁、10%计提保险基金。

核心数据：

指标	数值
LIGHT总量	25亿枚，永不增发
投资金库	8.5亿枚（基准可部署≈$1亿）
挖矿产出	10亿枚，每2年减半
首纪元日释放	≈68.49万枚（10万矿工时人均6.51/天）
通缩底线	流通量≤10亿枚时永久停止销毁（基准情景第11-12年）

指标	数值
治理门槛	提案≥5,000 LIGHT；委员会≥50,000 LIGHT
技术栈	Cosmos SDK + Tendermint PoS + CosmWasm + PWA
验证者	初始21个（最低10），上限100
初始融资	荷兰式拍卖$1,500万 + Pre-TGE战略融资$225-375万

差异化： 目前唯一将"零门槛网页挖矿"与"合规SPV实体投资"结合的项目。不同于Pi Network（无实际效用）、Helium（需硬件$200+）、传统DAO（高门槛精英治理）。

路线图： 2026年Q4筹备 → 2027年Q1-Q2开发 → Q3审计测试 → Q4 TGE上线 → 2028年Q1种子用户 → Q2-Q3首笔投资 → Q4起规模化。

前置声明

这不是一份投资建议书

本白皮书所述"生态奖励""协议收入分配"均为协议内生机制产生的激励安排，不构成任何形式的证券发行、理财产品销售、保本承诺或投资建议。

LIGHT 及子代币不具有内在价值，价格可能归零。参与前，请自行咨询法律、税务及财务专业人士，并自行承担私钥保管、税务申报及参与行为的全部责任。

序章：三个人的故事

Maria 在马尼拉做外卖骑手，每天工作12小时，月收入约15,000菲律宾比索（约合270美元）。她想入股隔壁生意火爆的奶茶连锁品牌，对方却告诉她："最低投资额25,000美元起。"Maria 拿不出25,000美元。

Kwame 在拉各斯开网约车。他看好人工智能赛道，想投资一家做金融科技的小公司。机构告诉他："最低认购额100,000美元，锁定期5年。"Kwame 拿不出100,000美元。

Elena 是圣保罗的一位退休教师，每月养老金约3,000巴西雷亚尔（约合550美元）。她听说邻居的孩子在区块链公司工作赚了钱，但她看不懂白皮书，也不知道如何购买和配置专业矿机设备。

他们三个人，代表了全球绝大多数普通人：有判断力，也有参与意愿，却缺少低门槛、透明且可负担的参与通道。

LightDAO 正是为这些人设计的。一台能上网的设备、一个浏览器、一笔很小的资金，就可以参与生态建设；通过合规的 SPV 架构，用户还有机会间接接触优质企业的现金流分配，以及前沿科技项目的早期成长。

第一章：我们看到的真相

1.1 全球财富分配失衡

根据世界不平等实验室《2026年世界不平等报告》（World Inequality Report 2026，以下简称《报告》）：

数据	来源
全球最富有的0.001%人口（约6万人）拥有的财富，约为后50%人口（约40亿人）财富总和的3倍	世界不平等实验室，2026
全球前1%人口掌握23%的总收入和38%的总财富	世界不平等实验室，2026
全球前10%人口掌握53%的总收入和75%的总财富	世界不平等实验室，2026
全球后50%人口仅获得8%的总收入和2%的总财富	世界不平等实验室，2026

《报告》指出："全球不平等仍处于历史上的极端水平。不平等并非仅来自市场的自然运作，而是反映了政策选择、制度结构以及经济与政治权力的不平等分配。"

来源说明： 上述数据引自世界不平等实验室《2026年世界不平等报告》。该报告由 Lucas Chancel、Ricardo Gómez-Carrera、Rowaida Moshrif 与 Thomas Piketty 领衔编写（wid.world官网确认）。正式发布前，建议进一步标注报告中的具体图表编号，以降低二次转述可能产生的误差。

数据一致性校验： 上述比例与《2022年世界不平等报告》的结论（前10%拥有76%总财富、后50%拥有2%总财富）呈合理趋势延续，偏差幅度在统计学可接受范围内。

1.2 普通人被排除在优质资产之外

全球主要司法辖区对私募股权和风险投资设有严格的合格投资者门槛：

美国（SEC Regulation D, Rule 501, 17 CFR § 230.501）： 合格投资者（Accredited Investor）须满足以下条件之一——个人年收入不低于200,000美元（或与配偶合计不低于300,000美元）且连续两年达标；或净资产（不含主要住所）不低于1,000,000美元。

欧盟（MiFID II, 2014/65/EU, Annex II）： 专业投资者（Professional Investor）须满足以下条件中的至少两项——金融工具投资组合不低于500,000欧元；在金融行业担任专业职务不少于一年；执行大规模交易不少于每季10笔。

全球私募股权基金实务： 单只基金的最低认购额通常在250,000至1,000,000美元之间；监管规则普遍禁止"拆分份额、降低门槛、拼单代持"等规避行为。

资产类型	普通人能否参与	主要原因
未上市优质企业股权	通常不能	合格投资者门槛较高，例如美国要求净资产不低于100万美元或年收入不低于20万美元
风险投资（早期科技公司）	通常不能	主要面向合格投资者开放，单只基金投资金额通常不低于25万美元
上市公司股票	可以，但早期利润通常已被一级市场参与者获取	二级市场定价通常包含未来预期，投资者并不直接参与企业早期利润分配

1.3 加密货币领域的三大缺陷

缺陷一：失败率极高

根据 CoinGecko 2025年度统计报告，仅2025年一年就有约**1,156万个代币**归零或停止交易（含各链上长尾代币）。CoinGecko历史追踪的超过2,000万个代币中，绝大多数已处于"死亡"状态（无交易量、无开发活动、价格较历史高点下跌超过99%）。

与此同时，传统股票市场的失败率远低于加密货币。根据 Bessembinder（2018）发表于《Journal of Financial Economics》的论文《Do Stocks Outperform Treasury Bills?》对1926—2016年间美股全部个股的研究：

指标	数据	来源
创造全部净财富的股票占比	仅约4%（1,092只）	Bessembinder (2018), JFE 129(3):440-475
中位数个股终身回报	为负（跑输国库券）	Bessembinder (2018), JFE
约58%的美股终身表现	跑输同期国库券	Bessembinder (2018), JFE
2025年归零/停止交易的代币数量	≈1,156万个	CoinGecko 2025年度报告

对比结论： 加密货币领域的永久资本损失率远高于传统股票市场。美股中虽有约58%的个股跑输国债，但投资者仍可通过指数基金获得市场平均回报；而加密货币市场中，绝大多数代币的终局是归零，且缺乏类似"指数"的有效分散工具。

来源说明： Bessembinder, H. (2018). "Do Stocks Outperform Treasury Bills?" *Journal of Financial Economics*, 129(3), 440-475. Arizona State University. 该论文为金融学领域高被引文献（引用次数>2,000），数据覆盖1926—2016年CRSP数据库全部美股。CoinGecko数据来源于其2025年度代币存活状态统计报告（2026年1月发布），多家财经媒体（Sina Finance、Phemex、RBC Crypto）均有报道。

缺陷二：挖矿高度中心化

比特币挖矿已呈现较高集中度：

矿池	算力占比
Foundry USA	约30%
AntPool	约19%
ViaBTC	约14.5%
F2Pool	约10%
MARA Pool	约5%
前两大矿池合计	超过50%
前四大矿池合计	约75%

来源说明： 上述数据综合自2025年各月算力分布报告（CoinGradient 2025.3 "Foundry, Antpool, and Viabtc Dominate Bitcoin Mining"；HashrateIndex "Top 10 Bitcoin Mining Pools of 2025"）。不同数据源的具体数值可能存在小幅差异（通常在±2%以内），但"前四大矿池控制约75%算力"的结论在多个主流监测平台中均有体现。

缺陷三：DAO 治理参与率极低

数据	来源
多数 DAO 的投票参与率仅约3%—12%（中位数约6%）	DeepDAO (2025) 链上治理数据聚合；Boardroom DAO Governance Report (2024)
少数持币者控制绝大多数投票权（治理权力高度集中）	ACM (2024) "DAO Governance: Voting Power, Participation, and Controversy" DOI:10.1145/3777416

1.4 核心洞察

有判断力，却没有入场券；有眼光，却没有话语权；想参与，却被高门槛挡在门外。

第二章：LightDAO 的回答

2.1 核心定位

LightDAO 是一个以链上治理为核心、以合规 SPV 为投资执行载体的全民投资自治组织。通过一条专为轻量级网页节点设计的公链，全球用户仅需一个浏览器即可参与网络维护、治理投票，并按规则分享生态收益。

2.2 双引擎模型

引擎	投资方向	目标	收益特征
引擎一：现金流引擎（守）	社区级刚性消费服务资产	形成持续现金流，并按规则进行利润分配	追求相对稳定，但不承诺固定收益
引擎二：增长引擎（攻）	前沿科技公司	获取股权增值及退出回报	潜在弹性较高，同时可能面临亏损或退出失败

配置纪律： 原则上将70%资金配置于稳健现金流资产，将30%资金配置于高成长标的。

投资规模成长路径： 单笔投资规模随LIGHT价格和金库容量动态成长——启动期（LIGHT $0.02-$0.05）适配$255万-$637万的社区级小型资产；成长期（$0.05-$0.30）进入$637万-$3,825万的区域连锁和Seed-A轮（对标Lower Middle Market PE）；成熟期（$0.30-$1.00）达到$3,825万-$1.275亿的中端市场PE水平；规模期（$1.00+）可执行$1.275亿以上的大型收购和Pre-IPO投资。硬性约束：单笔不超过投资金库剩余量的15%（详见第九章）。

首个标的定位原则： 不预设具体企业名称，而是先确立筛选框架——优先选择社区级刚性消费服务资产，要求具备已验证的单店经济模型、稳定的现金流记录（过去3年 EBITDA margin 不低于10%，且年际波动率不高于15%）以及明确的区域扩张路径。具体标的由社区提案决定。

2.3 核心价值主张

浏览器即节点 ——不需要购买矿机，也不需要具备专业技术背景，访问官方网页平台即可参与网络贡献。

人人可参与 ——达到治理门槛后，持有小额 LIGHT 也可以参与投票，共同决定资金配置方向。

利润按规则共享 ——被投企业的经营利润、科技项目的退出回报，将按照链上规则和 SPV 安排进行分配。

2.4 口号

"你的浏览器，也可以成为连接优质资产的入口。"

2.5 竞品差异化分析

维度	Pi Network	Helium	传统DAO（MakerDAO等）	LightDAO
参与方式	手机APP点击	购买硬件热点（$200-$1000）	购买代币+链上操作	浏览器访问，零硬件成本
准入成本	零（但无实际效用）	高（硬件+安装）	中高（需购买治理代币）	零（浏览器即可）
代币总量	1000亿	2.23亿	各异	25亿
实际投资功能	无	无（仅网络覆盖）	有（但门槛极高）	有（SPV架构，全民可参与）
收益来源	不明确	网络使用费	协议费用	企业利润+退出回报+Gas费
法律隔离	无	无	部分有	开曼SPV+ZK-KYC
治理参与率	极低（无实质治理）	低	约6%	目标>15%（双维度投票+激励）

LightDAO 的核心差异： 它是目前唯一将"零门槛网页挖矿"与"合规SPV实体投资"结合的项目。用户不仅贡献网络资源获得代币奖励，还能通过治理投票直接参与真实企业的投资决策，并分享经营利润。

> **【本章术语】** **DAO**（Decentralized Autonomous Organization，去中心化自治组织）：通过智能合约编码治理规则、由代币持有者集体决策的组织形式，无传统公司层级结构。 **SPV**（Special Purpose Vehicle，特殊目的载体）：为特定交易或投资设立的独立法律实体（通常注册于开曼群岛），实现风险隔离——SPV的债务和法律责任不传导至DAO本体。 **DePIN**（Decentralized Physical Infrastructure Network，去中心化物理基础设施网络）：通过代币激励用户贡献物理资源（带宽、存储、算力、无线覆盖等）构建基础设施的网络模式。 **Lower Middle Market PE**（下游中端私募股权）：全球私募股权行业的一个细分市场，单笔交易规模通常为$1,000万—$1亿，标的企业EBITDA在$200万—$1,500万之间。

第三章：合规与法律隔离

3.1 SPV 法律隔离层

DAO 不直接持有任何实体企业股权。所有对外投资均通过设立于开曼群岛的特殊目的载体（SPV）执行。

设计要点	说明
SPV 章程	明确约定 SPV 的运营应遵循 DAO 的有效决议
子代币法律定义	子代币为"SPV 收益分配请求权凭证"，仅代表对未来现金流的分配资格
不附带股东权利	不附带公司治理权、清算优先权或任何股东权利
SPV 董事	由独立第三方担任；DAO 可通过有效决议更换董事
资金监管	银行账户由持牌托管机构监管，资金划转须通过多重签名及合规校验
SPV争议解决	SPV章程约定仲裁条款（SIAC或ICC），DAO可通过治理决议启动仲裁程序

3.2 可选验证与隐私保护

参与协议本身不需要任何身份证明。 访问网页、创建钱包、贡献资源、领取 LIGHT、发起与参与治理投票——全程无需上传证件，链上也不存储任何个人身份信息（PII）。

只有当用户**主动**使用受监管的第三方服务时，才会涉及该服务自身依法必须执行的核验，而这份核验由该服务方采集、承担与保管，LightDAO 不采集、不中转、也不存储任何资料：

场景	由谁执行核验	用户需要做什么
通过法币通道买入/卖出	持牌第三方（如 MoonPay、Ramp Network、Transak）	按该服务商自身要求完成其合规流程
兑换子代币（投资份额凭证）	视具体产品与其服务方要求	可以只做挖矿与治理，完全不涉及任何验证
提现到银行卡/本地支付	出金与支付服务商	按服务商要求完成其合规流程

核心原则：**默认零验证；验证只发生在用户主动跨入受监管服务的那一刻，且由该服务方承担。** 任何人不会因为"没做验证"而失去挖矿、持有、转账或投票的权利。

> 技术预留：若未来某类资产确需资质门槛，将以零知识证明（ZK）方式由用户自持凭证、链上只验证"是否满足"而不落任何身份信息——此项属于路线图，不是当前要求。

3.3 税务责任声明

协议不提供税务申报服务，所有生态奖励及相关收益的税务义务由用户自行承担。用户应遵循其税务居民所在地的相关法律法规。

3.4 用户准入：面向所有人开放

注册与参与不设门槛：不需要邮箱、手机号、社交账号或身份证明；一台能打开网页的设备就是全部条件。LightDAO **不主动限制任何国家或地区的用户参与，也不部署地理围栏。**

唯一的外部约束来自第三方服务：如果某地法律对特定服务（例如法币出入金）另有要求，那部分服务由当地持牌机构在其侧依法执行，**不影响任何人使用链上功能**（挖矿、持有、转账、投票、提案）。

若某司法辖区未来出台明确禁止性法规，协议的应对顺序是：

1. 先保障已有用户的资产处置权不受影响——链上资产不可被冻结，任何人可随时转走自己的 LIGHT 与子代币；
2. 通过前端多入口（含 IPFS 镜像与社区镜像）保持可访问；
3. 最后才是在法律强制范围内调整**第三方服务**的可用范围。

一句话：**限制只可能落在服务上，不落在人身上。**

3.5 法币出入金与跨链通道

法币通道（第三方服务聚合）： 协议本身不运营法币出入金服务，但网页平台集成合规第三方通道（MoonPay、Ramp Network、Transak等），覆盖北美、欧洲、东南亚、拉美主要市场；本地P2P市场聚合覆盖非洲、南亚；出金支持GCash、M-Pesa、Pix、GrabPay等本地支付方式。

跨链桥与LIGHT获取渠道： TGE后在LightDAO链内置AMM交易；通过IBC与Cosmos生态互通；第6个月起规划wLIGHT（Ethereum/Solana）；第6个月起视合规情况申请CEX上市。跨链桥由独立第三方运营，桥上线前要求独立审计报告。

3.6 邀请机制合规声明（反MLM分析）

LightDAO的邀请激励为**单层分成**（仅直接邀请人获得被邀请人挖矿奖励的固定比例），不具备多层次营销（MLM）的核心特征：无多层级递归抽成；收益来源于协议预设代币释放而非新人本金；参与挖矿零成本无入门费。该结构更接近"开源项目贡献者推荐奖励"。正式运营前将聘请目标市场持牌律师出具专项合规意见。

【本章术语】 **KYC**（Know Your Customer，了解你的客户）：金融机构验证用户身份的合规流程，通常要求提交身份证件、地址证明等。 **ZK-KYC**（Zero-Knowledge KYC，零知识证明KYC）：用户无需向协议披露具体个人信息，仅通过密码学证明"我满足某条件"（如年龄≥18岁、非制裁国籍）的合规验证方式。链上不存储任何原始证件数据。 **PII**（Personally Identifiable Information，个人可识别信息）：可单独或组合识别特定自然人的数据，如姓名、身份证号、住址、生物特征等。 **Reg D / Reg S**（美国证券法D条例/S条例）：Reg D允许面向美国"合格投资者"私募发行而无需公开注册（Rule 501定义标准）；Reg S允许向美国境外人士出售证券而不触发美国注册要求。 **MiFID II**（欧盟金融工具市场指令II，2014/65/EU）：欧盟金融监管框架，其附件II定义了"专业投资者"认定标准（€500K金融工具组合、1年金融从业经验、每季10笔大规模交易，满足其二）。 **MLM**（Multi-Level Marketing，多层次营销）：通过多层级递归抽成（下线发展下线，上线层层抽佣）的商业模式。与单层推荐奖励有本质区别——LightDAO仅为单层（A邀请B，A从B处获得分成；B邀请C，A不从C处获得任何分成）。 **IBC**（Inter-Blockchain Communication，跨链通信协议）：Cosmos生态的原生跨链标准，允许不同区块链之间安全转移资产和消息，无需中心化中介。

第四章：技术架构

4.1 公链是什么

LightDAO 的公链可以理解为一个"规则透明且不可随意篡改的公共账本"：治理规则被写入代码，任何人的投票记录、资金流动和利润分配都可在链上查询和验证。

4.2 技术参数与选型论证

技术项	选型	选型依据
底层框架	Cosmos SDK	模块化架构，多条生产链验证
共识机制	Tendermint PoS	即时确定性；出块1.5—2秒；BFT容错≤1/3作恶
智能合约	CosmWasm	WebAssembly + Rust，编译时内存安全
跨链能力	IBC 协议	Cosmos原生跨链标准
前端交互	Progressive Web App (PWA)	浏览器运行，桌面/移动自适应，无需安装

4.3 轻量节点挖矿机制与激励模型

4.3.1 挖矿方式

用户通过浏览器访问官方网页平台，创建钱包，点击"开始挖矿"。挖矿过程中，用户通过浏览器贡献网络带宽（数据中继与验证）和本地计算资源（轻量级区块头验证），不依赖高能耗算力。

网页端技术实现： WebRTC数据通道P2P中继；Web Worker后台区块头验证；Service Worker离线缓存与心跳；WebSocket长连接。

移动端浏览器适配： 采用累计有效会话制（日满4小时=100%得分）；断线5分钟内重连不扣分；PWA安装用户获在线时长10%额外加成；委托在线机制（委托者70%/中继节点30%）。

4.3.2—4.3.3 激励方案与三引擎模型

采用"PoC贡献证明＋邀请裂变激励＋行为加成激励"三引擎模型。

4.3.4 贡献维度与权重

贡献维度	权重	测量方式
带宽中继贡献	40%	上传中继流量与验证数据量的比值
有效会话时长	30%	每日累计有效会话（满4小时=100%）
区块验证贡献	20%	有效验证的区块头数量与准确率
网络稳定性	10%	连接延迟、丢包率、响应时间

4.3.5 奖励计算公式

每日挖矿奖励 = BaseReward × 贡献权重得分 × (1 + 邀请加成) × (1 + 行为加成)

- BaseReward = 当日全网释放总量 ÷ 当日活跃矿工总数
- 邀请加成 = 被邀请人有效数量 × 1%（上限20%）
- 行为加成 = 投票参与5% + 内容贡献5% + 社区活跃5% + 节点验证质量5%（上限20%）
- 满加成系数 = (1+20%) × (1+20%) = 1.44倍

4.3.6 邀请裂变激励

层级	邀请有效人数	邀请分成比例	额外一次性奖励	治理权重加成
矿工	0人	—	基础挖矿奖励	无
布道者	不少于3人	10%	100枚 LIGHT	无

层级	邀请有效人数	邀请分成比例	额外一次性奖励	治理权重加成
大使	不少于10人	15%	500枚 LIGHT + 链上徽章	投票权重+5%
合伙人	不少于50人	20%	2,500枚 LIGHT + 链上徽章	投票权重+10%

治理权重加成与声誉加成（最高+30%）独立叠加，总上限+40%。邀请加成在20人时触顶（20×1%=20%）。

4.3.7 反作弊机制

浏览器环境完整性检测（Canvas/WebGL/WebRTC指纹）、数据包深度检测、IP聚类与行为模式分析、多维行为指纹（鼠标轨迹/键盘节奏/滚动行为）、邀请地址真实性校验。反女巫攻击成本：创建10,000独立指纹需$50,000-$200,000；检测率目标>90-95%。

4.4 LIGHT 代币功能矩阵

网络燃料（Gas费）、治理权（投票/提案/竞选）、质押绑定（保证金/竞选/验证者）、投资兑换（子代币）、生态激励（挖矿/邀请/行为）、未来扩展（dApp/NFT/跨链）。

4.5 Gas 费与交易费机制

设计原则： Gas 费以USD等值为锚定目标，实际收取的LIGHT数量由链上预言机（4.10节）每24小时自动换算。这确保无论LIGHT价格涨跌，用户的实际支付成本（以美元计）保持稳定，避免"币价涨100倍→转账费变成$10"或"币价跌90%→零成本刷票"的问题。

USD锚定Gas费目标：

交易类型	USD等值目标	LIGHT=$0.05时实收	LIGHT=$0.50时实收	设计意图
普通转账	$0.001	0.02 LIGHT	0.002 LIGHT	极低门槛，确保小额用户可自由转账
治理投票	$0.005	0.10 LIGHT	0.01 LIGHT	略高于转账，防止无成本刷票
提交提案	$0.10	2.0 LIGHT	0.2 LIGHT	配合保证金制度，增加提案严肃性
子代币兑换	$0.50	10.0 LIGHT	1.0 LIGHT	较高费用，匹配大额操作的严肃性
挖矿心跳上报	$0（免费）	0	0	挖矿贡献不收取Gas，确保零成本参与

动态换算规则：

- 实际Gas费（LIGHT）= USD目标 ÷ 预言机24h TWAP价格
- 每24小时（UTC 00:00区块）由oracle_twap合约自动更新换算比率
- 设置下限：任何交易类型的Gas费不低于0.001 LIGHT（防止价格为零时Gas归零）
- 设置上限：任何交易类型的Gas费不高于100 LIGHT（防止价格极低时Gas过高阻碍使用）
- USD目标值本身可通过微型提案（$100保证金）由治理调整

Gas 费分配规则：

去向	比例	作用
永久销毁	50%	持续通缩，减少流通供应
验证者奖励	30%	激励验证者维护网络安全和出块
生态金库	20%	补充开发者资助和社区运营资金

Gas 费通缩估算： 假设日均活跃交易10万笔、平均Gas费$0.005（以投票和转账为主），则日销毁USD等值 = 100,000 × $0.005 × 50% = $250/天。在LIGHT=$0.05时折合5,000 LIGHT/天≈182.5万/年；在LIGHT=$0.50时折合500 LIGHT/天≈18.25万/年。Gas费通缩的LIGHT数量随价格上升而减少（USD等值恒定），但其对价格的支撑作用通过"持续买压等价物"体现——每笔交易都在以固定USD速率销毁代币。

4.6 验证者体系

维度	验证者	轻节点（浏览器矿工）
职责	出块、共识、全节点	区块头验证、数据中继
质押	最低500,000枚 LIGHT	无
收益	Gas费30% + 日释放池5%	PoC挖矿奖励（日释放池95%）
数量	初始21，上限100	无上限
Slashing	双签罚没5%+禁入180天	无

分阶段启动（BFT容错：N≥3f+1）：

阶段	验证者数量	容错f	链停止条件	用户体验
测试网（TGE前3月）	7	2	3个同时离线	内测可容忍短暂中断

阶段	验证者数量	容错f	链停止条件	用户体验
主网TGE	最低10，目标21	3—6	4—7个同时离线	偶发中断（季度<1次）至流畅
第7月起开放竞选	21—100	6—33	7—34个同时离线	用户无感知

硬性底线：验证者<7个时TGE不得执行。 低于7个意味着f≤1，任何单点故障导致全链停摆，对非技术用户等同于"产品不可用"。

4.7 网络基础设施层

验证者节点分布式承载WebSocket接入网关（每验证者上限50,000连接）；P2P信令由验证者+社区中继节点提供；心跳Merkle聚合每区块仅提交Root哈希（O(1)链上开销）；前端通过IPFS+CDN分发。

P2P网络：WebRTC ICE框架（STUN优先/TURN回退）；约70-80%用户可直连，20-30%对称NAT用户通过TURN中继；P2P失败时降级为"纯验证模式"。

性能规格：理论TPS 1,000-3,000；区块大小2MB（治理可调）；轻节点同步<30秒；百万节点心跳Merkle聚合<500ms。

4.8 贡献证明验证机制

三层验证架构：(1)验证者随机交叉抽样挑战（每10分钟5%节点，30秒响应时限）；(2)P2P对等体互证（8-16个对等体独立记录数据交换量，取中位数）；(3)Merkle聚合上链（每区块提交贡献得分Root，用户可通过Merkle Proof自查）。连续3次挑战失败→当日得分归零；7天内累计5次→触发反作弊审查。

4.9 钱包与密钥管理

三层架构：(1)内嵌智能钱包（Passkey/WebAuthn，无需助记词，目标80%+用户）；(2)社交恢复钱包（3-5恢复人，Shamir分片，2/3多数确认）；(3)自托管钱包（BIP-39助记词+硬件钱包兼容）。新用户前100笔交易Gas费由生态基金代付（Paymaster模式）。

4.10 价格预言机

链上TWAP（LIGHT/USDC池30天时间加权均价）为主价格源；3+外部DEX/CEX聚合为辅（验证者轮值提交，取中位数）；偏差>±15%触发异常标记；单区块偏离>5%不纳入TWAP（防闪电贷操纵）；外部预言机全部失效时回退至纯链上TWAP。

4.11 智能合约模块架构

10个核心合约：light_token、mining_reward、governance、treasury_multisig、subtoken_factory、oracle_twap、anti_fraud、validator_registry、vesting、insurance_fund。核心合约TGE前须完成形式化验证。

4.12 协议升级与链治理

四级升级：L1参数调整（治理投票24-72h）→L2合约迁移（重大提案+审计+72h延迟）→L3共识变更（66%通过+2/3验证者信号+7天分叉保护期）→L4紧急修复（影子委员会暂停+多签热修复+72h追认）。

> **【本章术语】** **Cosmos SDK**：模块化区块链开发框架，允许开发者像搭积木一样组装自定义公链，已有多条生产链（如Cosmos Hub、Osmosis）验证其成熟度。 **Tendermint PoS**（Proof of Stake，权益证明）：一种共识机制，验证者通过质押代币（而非算力竞争）获得出块权。提供"即时确定性"——区块一旦提交即不可回滚。 **BFT**（Byzantine Fault Tolerance，拜占庭容错）：分布式系统中容忍部分节点作恶或故障仍能正确达成共识的机制。Tendermint BFT可容忍不超过1/3的验证者同时作恶或离线。 **CosmWasm**：Cosmos生态的智能合约引擎，基于WebAssembly技术，支持使用Rust语言编写合约，具备编译时内存安全特性（防止常见漏洞如缓冲区溢出）。 **PWA**（Progressive Web App，渐进式Web应用）：基于浏览器运行但具备类原生应用体验的Web技术，支持离线缓存、推送通知、添加到主屏幕，无需通过应用商店下载安装。 **WebRTC / WebSocket**：两种浏览器实时通信技术。WebRTC用于P2P数据中继（节点间直接传输）；WebSocket用于维持客户端与验证者的长连接（心跳、奖励通知）。 **PoC**（Proof of Contribution，贡献证明）：LightDAO采用的激励机制，通过验证用户实际贡献的网络资源（带宽中继、区块验证、在线时长）发放奖励，而非依赖算力竞争或资本质押。 **Merkle Tree**（默克尔树）：一种哈希树数据结构，允许高效验证大量数据中某一特定条目的完整性。本白皮书中用于将百万级轻节点心跳聚合为单一Root哈希上链（O(1)存储开销）。 **Gas费**：区块链上执行交易或合约操作所需支付的手续费，用于补偿验证者的计算和存储资源。LightDAO的Gas费以USD等值锚定，由预言机每24小时自动换算为LIGHT数量。 **Slashing**（罚没）：验证者因作恶（如双重签名）或长期离线而被强制扣除部分质押代币的惩罚机制，是PoS网络安全性的经济保障。 **预言机**（Oracle）：将链下数据（如市场价格、天气、体育比分）安全传入链上智能合约的基础设施组件。LightDAO使用链上TWAP+多源聚合的混合预言机架构。 **TWAP**（Time-Weighted Average Price，时间加权平均价格）：将一段时间内每个区块的价格按时间等权平均，减少瞬时大额交易对价格参考的操纵影响。 **AMM**（Automated Market Maker，自动做市商）：去中心化交易协议，通过流动性池（而非订单簿）实现代币兑换，价格由池内资产比例按公式自动决定。 **DEX / CEX**：DEX（Decentralized Exchange，去中心化交易所）无需托管用户资产，通过智能合约点对点交易；CEX（Centralized Exchange，中心化交易所）由运营方托管资产并撮合交易。 **IPFS**（InterPlanetary File System，星际文件系统）：去中心化文件存储与分发协议，本白皮书中用于前端应用的抗审查托管（即使域名被封锁，用户仍可通过IPFS访问平台）。

第五章：代币经济模型

5.1 总量设计依据

LIGHT 总供应量：25亿枚（2,500,000,000），永不增发。

对标项目	总量	参与方式	与LightDAO可比性
Bitcoin	2,100万	PoW矿机	叙事参照，门槛远高
Helium (HNT)	2.23亿	硬件热点$200+	DePIN标杆，硬件限制规模
Filecoin (FIL)	20亿	存储硬件	量级最接近，同为"贡献资源换代币"
Kaspa (KAS)	287亿	PoW显卡	偏大，平滑递减有参考价值
Pi Network	1,000亿	手机点击	反面教材：总量过大→价值感知极低

选择25亿枚的核心理由：

1. **投资容量（首要约束）：** 金库8.5亿枚×基准价$0.15×75%利用率 = **$9,563万≈$1亿**可部署资本，达到Lower Middle Market PE最低可信门槛。学术依据：Cong, Li & Wang (2021) "Tokenomics: Dynamic Adoption and Valuation" (*Review of Financial Studies* 34(3):1105-1155, NBER w27222) 证明平台效用（投资回报→回购→价格支撑）是代币价值的根本驱动力，而非分发广度。
2. **网络引导：** 挖矿10亿枚，首纪元日释放68.49万枚，10万活跃矿工时人均6.51 LIGHT/天，保持"整数感知"。
3. **运营可行性：** 10%战略运营基金（2.5亿枚）解决TGE前开发/审计/法律资金缺口（$110-285万），纯社区模式无法覆盖此成本。
4. **通缩可行性：** 底线10亿枚在基准情景下第11-12年触及（较210亿方案的15年+缩短25-30%）。
5. **对标合理：** 与Filecoin（20亿）同一量级，后者为DePIN领域市值前五项目。

5.2 代币分配方案

分配类别	比例	数量	用途	释放方式
轻量节点挖矿	40%	10亿枚	奖励网络贡献者	每2年减半，按贡献实时释放
企业投资金库	34%	8.5亿枚	DAO治理下的投资执行（投资时销毁）	多签锁定，仅通过有效决议释放并销毁

分配类别	比例	数量	用途	释放方式
生态发展基金	16%	4亿枚	流动性、空投、开发者资助、社区运营	分阶段释放（见5.3节）
战略运营基金	10%	2.5亿枚	团队、审计、法律、基础设施、战略投资者	12月cliff + 36月线性（见5.X节）

行业对标（Tokenomics.net 2024-2025 cohort基准）： 社区/用户奖励20-35%（LightDAO: 40%挖矿+16%生态=56%，因无VC轮故偏高）；金库/储备15-25%（LightDAO: 34%，因承担投资功能）；团队/投资人15-45%（LightDAO: 10%，远低于行业，维持"全民DAO"叙事）。

5.3 生态发展基金释放计划

阶段	时间	比例	数量	用途
TGE	第0天	30%	1.2亿枚	DEX流动性（60%=7,200万）+ 种子空投（40%=4,800万）
线性释放期一	第1—12月	40%	1.6亿枚	每月1,333万枚：社区激励、市场推广、空投计划
线性释放期二	第13—24月	30%	1.2亿枚	每月1,000万枚：开发者资助、生态建设、储备

5.4 战略运营基金（2.5亿枚）

子类别	占比	数量	对象	释放规则
服务换代币	50%	1.25亿枚	开发公司、审计机构、律所、验证者运营商	12月cliff + 36月线性；以LIGHT支付服务费的30-50%
战略融资	30%	7,500万枚	2-3家DePIN/Cosmos生态基金或消费行业战略方	Pre-TGE以$0.03-$0.05出售（募集$225-375万）；12月cliff + 24月线性；单投资者≤总量2%
核心贡献者	20%	5,000万枚	3-5名发起人/核心建设者	12月cliff + 36月线性；按季度里程碑考核释放；任期内不得出售

战略投资者要求： 必须提供非资金贡献（deal flow、验证者服务、合规资源之一），纯财务投资者不接受。

监管合规： Pre-TGE sale采用Reg S（非美国投资者）+ Reg D Rule 506(c)（美国合格投资者）双轨豁免。

核心贡献者披露规则： 仅披露总额（5,000万枚=总量2%）和释放规则，不公开个人姓名和单人额度。角色类别公开：技术/投资/合规/社区。

5.5 挖矿产出与减半计划

推导： 2A = 10亿 → A = 5亿（第一纪元）。日释放 = 5亿÷730 = 684,932枚 ≈ 68.49万/天。每区块 = 684,932÷49,371 ≈ 13.87 LIGHT。

注意： 每区块奖励池为全网共享，其中5%划拨验证者（3.42万/天），95%分配轻节点矿工（65.07万/天）。

纪元	时间	产出总量	日释放量	每区块奖励池
第1纪元	0—24月	5亿枚	≈68.49万	≈13.87 LIGHT
第2纪元	25—48月	2.5亿枚	≈34.25万	≈6.93 LIGHT
第3纪元	49—72月	1.25亿枚	≈17.12万	≈3.47 LIGHT
第4纪元	73—96月	6,250万枚	≈8.56万	≈1.73 LIGHT
第5纪元	97—120月	3,125万枚	≈4.28万	≈0.87 LIGHT

校验： 5+2.5+1.25+0.625+0.3125+⋯ = 5×2 = 10亿 ✓。97%在前10年完成。

5.6 用户收益参考模型

网络规模	人均日收益	月收益	年收益	满加成(1.44x)月收益
1万矿工（种子期）	≈65.07	≈1,952	≈23,751	≈2,811
10万矿工（成长期）	≈6.51	≈195.2	≈2,375	≈281.1
100万矿工（规模期）	≈0.65	≈19.5	≈237.5	≈28.1

合伙人级（50邀请，20%分成，满加成）：

网络规模	自身(含加成)	邀请分成	日综合	月综合
1万矿工	≈93.7	≈650.7	≈744.4	≈22,332
10万矿工	≈9.37	≈65.07	≈74.44	≈2,233
100万矿工	≈0.94	≈6.51	≈7.45	≈223.4

5.7 空投增长计划

经济模型： 空投总预算 = 目标触达用户 × 人均空投 × (1+浪费率) = 100,000 × 150 LIGHT × 1.3 ≈ 1,950万枚（获取类）+ 3,550万枚（生态类）= **5,500万枚**（占生态基金4亿的13.75%）。

空投类型	触发条件	单次额度	预算
首挖空投	首次完成4小时有效挖矿	50 LIGHT	1,500万枚
地理扩张	目标市场用户完成ZK-KYC	100 LIGHT	1,000万枚
Learn-to-Earn	完成教育模块+测验	30 LIGHT	600万枚
治理首投	首次参与投票	20 LIGHT	300万枚
流动性提供	LP注入≥$50锁仓30天	200 LIGHT	1,000万枚
内容创作	经社区验证的教程/翻译	50-200 LIGHT	600万枚
合作渠道	通过合作方注册+首挖	80 LIGHT	500万枚

CAC验证： 5,500万枚×$0.03 = $165万 ÷ 30,000留存活跃矿工 = **$55/人**（行业区间$50-200，处于低端）。学术依据：Zheng (2023) "Operation Dumbo Drop: To Airdrop or Not to Airdrop for Initial Coin Offering Success?" 证明活动绑定型空投留存率为纯空投的3-5倍。

防滥用： 唯一浏览器指纹+ZK-KYC；每类每地址限领1次；30天锁定期；领取后30天无链上活动自动回收。

5.8 双引擎飞轮与资金池

飞轮：投票→金库LIGHT销毁→USDC支付→利润回流→回购销毁→价格支撑→更多用户。

双轨制：稳定金库（USDC，利润截留）+ 弹性金库（LIGHT层，投资时销毁不流入市场）。回购采用TWAP拆单，单笔≤日均交易量5%。

5.9 子代币发行与交易

发行总量=投资金额÷$1；兑换价以30天VWAP为基准；兑换所得LIGHT全部销毁；分配50%赞成者/30%空投/20%运营储备（锁仓6月）。单地址分红上限15%。子代币在链内AMM交易，发行后30天锁定期，退出后标记"已清算"下架。

5.10 初始流动性与价格发现

TGE（Token Generation Event，代币生成事件）安排：

项目	方案
初始流动性池	从生态发展基金TGE释放的1.2亿枚中，划拨7,200万枚（60%）注入DEX流动性池
配对资产	USDC（主池）、USDT（辅池）
空投	剩余4,800万枚（40%）用于种子用户空投（见5.7节空投计划）
上线交易所	TGE后首先上线去中心化交易所（如Osmosis、JunoSwap）；第6个月起视合规情况申请中心化交易所上市

荷兰式拍卖（Dutch Auction）详细机制：

荷兰式拍卖是一种"价格由高至低递减"的定价方式。与英式拍卖（价格由低至高竞价）相反，荷兰式拍卖中卖方设定一个起始高价，价格随时间自动下降，直到买方在某个价格点提交认购。第一个使总认购额达到目标的价格即为最终开盘价。

为什么选择荷兰式拍卖而非固定价格或英式拍卖：

定价方式	优点	缺点	适用性
固定价格预售	简单	定价主观，过高则卖不出，过低则被机器人抢购	不适合（无价格发现功能）
英式拍卖（竞价）	价格发现充分	大额买家可策略性等待、抬价；gas war	不适合（链上gas war排斥小额用户）
荷兰式拍卖	**自动价格发现；无需竞价（无gas war）；大小买家平等参与；防机器人（价格递减机制天然抑制抢跑）**	需要合理设定起始价和递减速率	**最适合（公平+高效+防操纵）**

LightDAO荷兰式拍卖具体参数：

参数	设定	说明
拍卖标的	LIGHT代币（从生态基金TGE释放的7,200万枚中划拨）	拍卖所得USDC注入稳定金库
目标募集额	**$1,500万 USDC**	$500万→稳定金库最低储备；$1,000万→初始投资资本
起始价	$0.20/LIGHT	高于预期均衡价，确保不会"秒光"

参数	设定	说明
递减速率	每小时下降5%	从$0.20起，约48小时后降至$0.017（若无人认购）
最低保留价	$0.01/LIGHT	若降至保留价仍未达目标，拍卖延期24小时或调整标的数量
认购方式	用户提交"我愿意以当前价格购买X USDC等值的LIGHT"	无需竞价，系统按最终统一价格结算（多退少不补）
单用户上限	不超过目标募集额的5%（即$75万）	防止单一买家垄断初始筹码
KYC要求	增强验证（税务居民身份）	合规要求

拍卖结果的资金去向：

```
用户认购总额 $1,500万 USDC
    ├── $500万 → 稳定金库（最低储备，覆盖运营+应急）
    └── $1,000万 → 初始投资资本（稳定金库中可部署部分）

拍卖售出的LIGHT → 买家钱包（进入流通）
未售出的LIGHT（若有）→ 注入DEX流动性池
```

价格发现保护期： TGE后前72小时设价格波动熔断——若DEX交易价格较拍卖开盘价偏离超过±50%，暂停子代币兑换功能（不影响挖矿和转账），防止极端投机行为干扰生态启动。72小时后熔断自动解除。

为什么$1,500万而非更低： 初始投资资本$1,000万需支撑首年3-5笔投资（单笔$200-500万，见9.1节启动期规模）。若仅募集$500万（全部作为储备），则首年无任何可部署投资资本，飞轮无法启动。$1,500万 = 储备$500万 + 投资$1,000万，是"安全底线"与"飞轮启动"的最小可行平衡。

5.11 通缩机制与底线

流通量 = 挖矿释放 + 生态释放 + 战略基金已释放 − 兑换销毁 − Gas销毁 − 回购销毁。 投资金库8.5亿枚从未进入流通。流通量理论上限 = 10+4+2.5 = **16.5亿枚**。

触发条件	系统行为
流通量≤15亿枚	减速信号（极端低销毁情景）
流通量≤12亿枚	预警公示，暂停主动销毁（基准情景约第8年）

触发条件	系统行为
流通量≤10亿枚	硬停止，所有销毁永久关闭（基准情景约第11-12年）

5.12 价格稳定机制（防死亡螺旋）

核心原则： LightDAO 不干预日常市场价格发现。协议仅在极端下跌情形下调整自身参数，以降低陷入"死亡螺旋"的风险。

分级逻辑： 在不同波动环境中，同等跌幅所代表的异常程度不同。低波动市场中的大幅下跌属于更强的异常信号，需要更高强度的干预；高波动市场中的大幅下跌相对常见，可采用较轻干预。因此，干预强度与信号的异常程度正相关，而非仅取决于跌幅的绝对值。

机制全流程表：

市场状态	30日历史波动率	触发条件	信号等级	触发后执行	恢复条件
低波动	≤30%	连续5日累计跌幅≥40%	I级	挖矿产出降至50%；销毁比例由20%提升至35%；风险参数调整公示期由72h缩短至12h；影子委员会进入激活状态（仅可依法行使临时暂停权）	价格站上30日均线，且较触发价反弹≥80%，并连续保持10日
中波动	30%—60%	连续7日累计跌幅≥50%	II级	挖矿产出降至50%；销毁比例由20%提升至30%；公示期缩短至24h；影子委员会进入激活状态	价格站上30日均线，且较触发价反弹≥60%，并连续保持7日
高波动	60%—100%	连续10日累计跌幅≥55%	III级	挖矿产出降至75%；销毁比例由20%提升至25%；公示期缩短至48h；影子委员会进入待命状态	价格站上30日均线，且较触发价反弹≥40%，并连续保持5日
极端波动	>100%	连续10日累计跌幅≥65%	III级	按高波动状态的III级措施执行	按高波动状态的III级恢复条件执行

排除条件： 仅当同期比特币跌幅低于 LIGHT 跌幅的50%时，上述机制方可触发，以排除系统性市场崩盘情形（即：若BTC同期也暴跌，则属于市场整体事件，不单独对LIGHT启动干预）。

恢复逻辑说明： 反弹要求与持续时间随异常等级递减：I级要求最高反弹幅度（80%）和最长确认时间（10日），III级要求相对较低（40%/5日）。该安排符合"异常信号越强、干预越强、恢复确认越严格"的递进逻辑。

波动率与价格数据来源： 30日历史波动率和累计跌幅均由链上价格预言机（见4.10节）提供，以每日UTC 00:00区块的TWAP快照为计算基准，不依赖任何外部数据源。

5.13 收益可持续性压力测试

压力情景	假设条件	协议应对	最坏结果
全部投资失败	所有被投企业亏损或退出失败	保险基金（利润10%计提）覆盖部分损失；稳定金库储备（≥$800万）维持运营；暂停新投资直至社区重新评估	子代币持有者无法获得分红；LIGHT价格承压但不归零（挖矿和治理功能持续运行）
市场暴跌80%	LIGHT价格较峰值下跌80%	触发防死亡螺旋机制（II级或III级）；挖矿产出削减50-75%；销毁比例提升；影子委员会可暂停高危操作	用户收益缩水但网络持续运行；恢复条件达成后机制自动解除
主要市场监管禁令	某大国全面禁止加密资产	前端切换 IPFS 镜像保持可访问；链上资产与已有用户权益不受影响；仅在法律强制范围内调整第三方服务可用性；SPV在开曼群岛运营不受单一国家管辖	该区域用户增长停滞；全球其他区域不受影响
用户大规模流失	活跃矿工下降超70%	BaseReward自动重新分配（分母缩小→留存用户人均收益上升）；邀请激励加权吸引回流；治理门槛临时下调（5.14节动态机制）	网络安全性下降但不会停链（Tendermint BFT容忍<1/3验证者离线）
智能合约重大漏洞	核心合约被发现可利用漏洞	多签紧急暂停资金流出（72小时时间锁提供响应窗口）；发起备用合约迁移投票（L4级紧急修复，见4.12节）；保险基金覆盖用户损失	部分资金可能受损；迁移完成后恢复正常运营

5.14 代际平衡机制

治理门槛动态调整：每新增100万累计活跃矿工，提案门槛自动下调5%（下限2,500 LIGHT）。

【本章术语】 **TGE**（Token Generation Event，代币生成事件）：代币首次通过智能合约创建并分发的时点，通常伴随初始流动性池建立、荷兰式拍卖定价和首次公开交易。类似于传统金融中的IPO，但不涉及证券交易所上市。 **减半**（Halving）：挖矿产出每隔固定周期（LightDAO为2年/730天）自动减少50%的机制。目的是制造渐进稀缺性——随着时间推移，新增供应越来越少，若需求不减则价格获得支撑。比特币采用每4年减半。 **金库**（Treasury）：由多签合约锁定的代币储备，仅可通过治理决议释放。LightDAO设有两类金库：投资金库（持有LIGHT，投资执行时销毁）和稳定金库（持有USDC，用于支付投资对价和运营开支）。 **通缩**（Deflation）：代币总供应量或流通量持续减少的过程。LightDAO通过四种机制实现通缩：投资执行销毁、子代币兑换销毁、Gas费销毁（50%）、利润回购销毁。 **死亡螺旋**（Death Spiral）：代币价格下跌→矿工收益缩水→矿工退出→网络安全性/贡献度下降→信心进一步丧失→价格继续下跌的恶性循环。第5.12节的分级干预机制专为阻断此循环而设计。 **子代币**（Sub-token）：每完成一次企业投资后按规则发行的SPV收益分配请求权凭证（如收购咖啡品牌→CAFE代币）。持有子代币=持有对未来利润的分配资格，不代表股东权利或公司治理权。 **LP**（Liquidity Provider，流动性提供者）：向DEX流动性池注入等值两种资产（如LIGHT+USDC）的参与者，赚取交易手续费作为回报。LP是DEX正常运行的基础。 **VWAP**（Volume-Weighted Average Price，成交量加权平均价格）：将一段时间内的价格按每笔交易的成交量加权平均，反映真实市场成交成本。LightDAO用30天VWAP作为子代币兑换的定价基准。 **CAC**（Customer Acquisition Cost，用户获取成本）：获取一个有效活跃用户的平均成本。LightDAO空投计划的目标CAC为$55/留存活跃矿工（行业区间$50-200）。 **wLIGHT**（Wrapped LIGHT，封装LIGHT）：通过跨链桥在Ethereum或Solana上发行的LIGHT等价代币，由桥合约锁定等量原生LIGHT作为1:1储备。目的是让非Cosmos生态用户也能获取和持有LIGHT。 **荷兰式拍卖**（Dutch Auction）：一种"价格由高至低递减"的定价方式。卖方设定起始高价，价格随时间自动下降，直到买方在某个价格点提交认购。第一个使总认购额达到目标的价格即为最终成交价。优点是无需竞价（无gas war）、大小买家平等、天然防机器人抢跑。

第六章：治理机制

6.1 双维度投票模型

持币权重（含声誉+层级加成，总上限+40%）+ 地址数量（1地址=1票，关联地址合并）。投票权90天有效，5枚LIGHT转账可激活。声誉加成：持币满1年+15次有效投票→最高+30%。

6.2 动态通过率

最低通过率＝50%＋（50%－实际投票率）。投票率≥50%时简单多数。

6.3 提案参数

类型	保证金	持币投票率	地址投票率	通过率	执行延迟
微型	$100	≥15%	≥20%	动态≥55%	24h
收购型	$500	≥25%	≥30%	动态≥60%	72h
风投型	$500	≥35%	≥40%	动态≥60%	72h
重大	$1,000	≥45%	≥50%	动态≥66%	72h
紧急	$2,000	≥50%	≥60%	≥75%	非资金6h/高危1h；资金操作仍受72h时间锁

6.4 提案生命周期

提交资格：≥5,000枚LIGHT + 连续质押30天 + 保证金。公示72h（修订≤2次）。投票7日（快速通道48h，≤50万USDC）。否决冷却90天。生效延迟24h。

门槛说明： 5,000枚在种子期（1万矿工）≈77天基础产出；合伙人级≈7天。治理第7月激活，早期用户有充足积累时间。

6.5 投票激励

参与有基础激励（均分），判断正确有额外加成（押注池50%）。押注区间5—500 LIGHT。抑制羊群效应：反对者即使"站错队"仍获基础激励。

6.6 成败奖惩

善意失败：退50%保证金+30天冷却。恶意失败（造假/重复）：全额没收+永久禁止。造假举证：封顶5,000 LIGHT，成立奖40%罚没金+500 LIGHT。

6.7 财务透明

链上实时仪表盘+季度财务报告+年度独立审计（TGE前须完成首次审计）+投资标的即时披露。

第七章：权力制衡与角色定义

7.1 初始监护人

权限仅限文档/格式/官网信息。任期≤24月。须指定备选监护人（连续30天无法签名→自动接管）。同时失能→48h紧急投票指定临时管理人。

7.2 权力转移路线图

阶段	时间	权限	投资审批
创世期	0—6月	监护人（非资金类）	监护人+社区多签3/5
过渡期	7—12月	监护人+核心贡献者联名	同上+核心贡献者
成熟期	13—24月	治理委员会3/5	常规双维度投票
自治期	25月+	全体持有者	同成熟期

7.3 治理委员会

五人分权（轮值主席/财务/技术/社区/密钥），季度轮换，任期6月可连任1次。竞选质押50,000 LIGHT + 100地址联名。决策≥3人且覆盖≥3职位。

门槛说明： 50,000枚在种子期≈合伙人67天（2.2月）；成长期≈672天（22月）。委员会第13月首选举，早期合伙人可达。

7.4 影子委员会

仅限"违法/制裁/重大欺诈"临时暂停。72h内须全体追认（反对>60%→解除）。连续2次被否决→自动弹劾解散。

7.5—7.6 竞选验证与密钥预案

SimHash>80%取消资格；AI内容须补充说明；缺席质询扣20%得票。密钥分片备份+季度健康检查+7天公示判定+投票更换。

第八章：信任与安全机制

8.1 五大安全机制

时间锁72h（紧急提案不可豁免资金操作）；多签3/5；季度轮换≤2届；造假罚没100%；全交易上链。

8.2 保险基金

成功投资利润的**10%**计提。理赔须独立报告+DAO 66%赞成+单次≤池20%。补充来源：造假罚没金的30%。定位"部分缓冲"非全额保障。

8.3 极端预案

监管黑天鹅→IPFS+移除管理员权限；欺诈→影子委员会暂停（72h追认）+保险基金+SPV仲裁；死亡螺旋→5.12节机制；合约漏洞→多签暂停+迁移投票；验证者集体作恶→BFT容忍<1/3，超过则链暂停+紧急投票迁移。

第九章：投资运营与退出策略

9.1 投资标的筛选与规模

投资规模分阶段成长轨迹（公式：金库剩余×15%×LIGHT价格）：

阶段	LIGHT价格	金库初始期单笔上限	适配标的	行业对标
启动期(Y1-2)	$0.02—$0.05	$255万—$637万	单店/小型连锁、天使轮	微型PE
成长期(Y3-5)	$0.05—$0.30	$637万—$3,825万	区域连锁30-200店、Seed-A轮	Lower Middle Market PE
成熟期(Y5-8)	$0.30—$1.00	$3,825万—$1.275亿	跨国连锁/中型科技、B-C轮	Middle Market PE
规模期(Y8+)	$1.00+	$1.275亿+	大型收购、Pre-IPO	大型PE/成长期VC

9.2 投资决策流程

项目发现（≥5,000 LIGHT）→独立尽调→72h公示→双维度投票→24/72h执行。

9.3 退出与利润分配

年度分红：**40%**子代币持有者 / **30%**稳定金库 / **20%**回购LIGHT销毁 / **10%**保险基金。 退出收益：**70%**稳定金库 / **30%**回购销毁。

9.4 投资纪律

规则	内容
单笔销毁上限	金库剩余×15%（初始8.5亿×15%=1.275亿枚）
单一标的	≤金库总价值25%
行业集中	≤组合40%
地域集中	≤组合30%
稳定金库储备	TGE时$500万（拍卖），第24月前达$800万
冷静期	连续2次失败→180天

金库容量： 8.5亿枚×$0.10=$8,500万（初始总容量）；×$0.30=$2.55亿；×$1.00=$8.5亿。15%单笔上限使投资节奏与价格正相关。

> **【本章术语】 EBITDA**（Earnings Before Interest, Taxes, Depreciation and Amortization，息税折旧摊销前利润）：衡量企业核心经营盈利能力的指标，排除了财务结构（利息）、税务政策（税）、会计选择（折旧/摊销）的干扰，便于跨企业、跨行业比较。EBITDA margin = EBITDA ÷ 营业收入。 **DCF**（Discounted Cash Flow，现金流折现法）：将企业未来预期现金流按一定折现率换算为当前价值的估值方法。适用于现金流稳定的成熟企业（如消费连锁），不适用于尚无盈利的早期科技公司。 **IPO**（Initial Public Offering，首次公开募股）：企业首次在证券交易所公开发行股票并上市交易。对LightDAO而言，被投企业IPO是增长引擎标的的主要退出路径之一。 **Pre-IPO**：企业在正式上市前的最后一轮私募融资，通常估值已接近上市后水平，风险低于早期轮次但回报倍数也较低。 **TWAP执行**（Time-Weighted Average Price Execution）：将大额回购订单拆分为多笔小额订单，在一段时间内均匀执行，以避免单笔大单对市场价格造成冲击。LightDAO规定单笔回购不超过日均交易量的5%。

第十章：路线图

阶段	时间	核心目标	关键里程碑	前置条件
筹备期	2026年Q4	法律实体+团队+资金到位	开曼/BVI实体注册完成；技术合伙人或开发团队签约；战略投资者意向确认（2-3家）；启动资金≥$15万到位	创始人确定身份公开方式；完成BP和Pitch Deck
开发期	2027年Q1—Q2	核心系统开发	10个智能合约模块开发完成；PWA前端开发完成；7个验证者测试网部署；内部Alpha测试通过	开发团队到位；需求文档（技术Spec）定稿
审计与测试期	2027年Q3	安全性与合规性验证	独立安全审计报告发布（≥1家顶级机构）；法律合规意见书发布（MLM+证券法）；5万并发压力测试通过；反作弊系统误报率<2%；治理投票演练完成	合约开发冻结（Code Freeze）；审计费用到位
TGE与主网上线	2027年Q4	代币发行+网络启动	荷兰式拍卖完成（目标$1,500万）；主网上线（≥10验证者）；挖矿平台公开开放；DEX流动性池建立；种子空投发放	审计通过；验证者≥7（硬性底线）；拍卖合约部署
信仰构建期	2028年Q1（TGE后第1-3月）	3—5万种子用户	活跃矿工突破3万；首次治理投票演练；社区多语言频道建立（英/中/西/葡/菲）；首份月度社区报告发布	TGE完成；社区运营团队到位
价值锚定期	2028年Q2—Q3（TGE后第4-9月）	首笔投资+过渡期治理	首个投资提案通过（第4-6月内适用创世期多签审批；第7月起适用过渡期联名审批）；首笔SPV交割完成；验证者开放竞选（第7月起）；首份季度财务报告发布	稳定金库USDC≥$500万；投资标的尽调完成
治理成熟期	2028年Q4—2029年Q1（TGE后第10-15月）	委员会选举+去中心化过渡	治理委员会首次选举（第13月）；进入成熟期（委员会3/5决策）；wLIGHT跨链桥上线；CEX上市申请提交；开发者资助计划启动	活跃矿工≥10万；≥100个地址联名候选人
生态扩张期	2029年Q2起（TGE后第16月+）	规模化复制	活跃矿工突破20—50万；完成2—3笔投资；首笔利润回流验证；LIGHT回购销毁启动	治理委员会运转正常；投资模式已验证
成熟运营期	2029年Q4起（TGE后第25月+）	飞轮自转+完全自治	进入自治期（全体持有者重大提案）；投资组合累计部署≥$3,000万；通缩数据公开可验证	治理完全去中心化

路线图设计原则：

- **审计先于TGE：** 绝不在未完成独立安全审计的情况下发行代币。这是用户资金安全的基本保障。
- **验证者先于用户：** 主网上线时验证者≥10个（BFT容错f≥3），确保网络不会因单点故障停摆。

- **投资先于扩张：** 首笔投资成功并产生可验证的利润回流后，方进入规模化扩张。避免"先圈人后找项目"的本末倒置。
- **时间缓冲：** 每个阶段预留20-30%时间缓冲。技术开发、审计修复、法律流程均可能超预期，路线图不应是"最乐观情景"。

与白皮书发布日（2026年8月4日）的关系： 白皮书于2026年8月发布，作为项目愿景和技术设计的公开声明。实际执行从2026年Q4开始（筹备期），TGE目标为2027年Q4。白皮书发布与TGE之间约14个月的间隔用于团队组建、开发、审计和合规准备。

第十一章：社区文化与开发者生态

11.1 四条价值观

- **透明优于完美** ——有瑕疵的公开，胜过完美的隐藏。所有金库流动、投资决策、治理投票永久上链可查。
- **渐进优于激进** ——小步快跑，持续迭代。首笔投资从$200-500万起步，验证模式后再扩大规模。
- **责任优于权利** ——权力与义务对等。治理委员会成员须质押50,000 LIGHT并公开施政纲领，失职则罚没。
- **多元优于同质** ——不同声音是系统的免疫力。双维度投票（持币+地址）确保巨鲸和散户都有话语权。

11.2 陪审团制度

维度	规则
组成	随机抽取12名持有≥10,000枚LIGHT且无违规记录的用户
任期	30天，届满后重新随机抽取
职责	审理反作弊处罚申诉、提案造假指控、社区争议
流程	被处罚用户可在72小时内提交证据；陪审团须在48小时内作出裁决
裁决标准	12人中≥8人（2/3多数）同意方可维持或撤销处罚
回避	与当事方存在邀请关系或同一IP段的陪审员自动替换
报酬	任期内每日获得5 LIGHT的陪审服务补贴（从生态基金列支）

11.3 开发者生态计划

模块	内容	资金来源	申请方式
开发者资助（Grants）	面向在LightDAO链上构建dApp、工具、基础设施的团队，单个资助$5—50万等值LIGHT	生态发展基金（线性释放期二）	提交提案→技术审核官评估→治理投票（微型提案流程）
SDK与API	提供JavaScript/TypeScript SDK、REST API、WebSocket接口，降低第三方开发门槛	技术审核官主导开发	开源，GitHub公开
黑客松	每季度举办一次线上黑客松，奖金池$10万等值LIGHT	生态发展基金	公开报名，无门槛
漏洞赏金（Bug Bounty）	核心合约漏洞赏金计划，单个有效漏洞奖励$1,000—$50,000（按严重度分级）	保险基金 + 生态发展基金	通过Immunefi或自建平台提交
CosmWasm合约市场	鼓励第三方部署智能合约，Gas费收入的20%回流生态金库支持开发者	Gas费分配（见4.5节）	自动，无需申请

11.4 多语言与本地化策略

维度	规划
平台语言	首发支持英语、中文、西班牙语、葡萄牙语、菲律宾语；第6个月起增加法语、阿拉伯语、斯瓦希里语、印尼语
治理语言	提案和竞选纲领接受任何语言提交，系统提供机器翻译+社区人工校对
社区运营	按语言设立独立社区频道（Discord/Telegram），各频道配备本地化社区联络志愿者
文档翻译	白皮书及核心文档由社区翻译志愿者完成，翻译贡献计入"内容贡献"行为加成（5%）
本地化资助	生态发展基金中预留10%（4,000万枚）专项用于本地化社区建设和翻译激励

第十二章：团队与顾问

12.1 核心角色定义

角色	职责	背景要求	披露方式
初始监护人/项目发起人	部署初始合约、维护文档、协调早期运营	区块链行业≥3年经验，有智能合约部署或DeFi协议运营记录	TGE前公开真实身份或提供第三方身份验证报告（如公证人签名+链上消息验证）
技术负责人	合约架构设计、开发团队管理、审计对接	Cosmos SDK/CosmWasm开发经验，有生产链部署记录	同上
投资负责人	标的筛选、尽调协调、SPV设立、退出管理	私募股权/风险投资行业经验，有已完成退出案例	同上
合规顾问	法律架构设计、监管对接、MLM合规意见	持有美国/欧盟/开曼执业资格的律师	公开律所名称（个人姓名除非本人同意否则不公开）

12.2 顾问委员会

- 由3—5名独立顾问组成，涵盖：DePIN技术、跨境投资合规、社区运营、消费行业；
- 顾问以LIGHT代币形式获得咨询报酬（从战略运营基金"服务换代币"部分列支），锁仓12个月；
- 顾问名单在TGE前公开，并接受社区质询（去中心化文字质询会，见7.5节）；
- 顾问不得同时担任治理委员会成员（利益冲突隔离）。

12.3 团队承诺与约束

约束	规则
代币锁仓	核心团队持有的LIGHT（含战略运营基金分配）须锁仓12个月，解锁后线性释放36个月
出售限制	初始监护人在任期内（≤24个月）不得出售通过任何渠道获得的LIGHT（含空投、奖励、薪酬）
利益冲突	团队成员的利益冲突须在任命时完整披露（是否持有其他DAO代币、是否与潜在投资标的存在关联）
未披露后果	未披露利益冲突一经查实，永久禁止参与治理，已解锁代币的50%罚没至保险基金

约束	规则
替换机制	核心角色离职或失能时，由治理委员会（成立前由初始监护人+备选监护人）指定继任者，须经社区公示72小时无异议

12.4 核心贡献者薪酬（战略运营基金20%部分）

- 总额：5,000万枚LIGHT（占总量2%）
- 覆盖人数：3—5人
- 释放规则：12月cliff + 36月线性（即第13个月起每月释放约115.7万枚）
- 里程碑绑定：每季度由治理委员会（成立前由初始监护人+独立第三方）确认里程碑达成后方可释放当季额度
- 披露规则：仅披露总额和释放规则，不公开个人姓名和单人额度（保护隐私，同时通过链上多签地址可验证总额不超发）

第十三章：风险提示与免责声明

13.1 风险提示

风险类型	说明	缓解措施
市场风险	LIGHT价格可能出现大幅波动，历史价格不代表未来表现。TGE初期流动性有限，价格可能剧烈波动	荷兰式拍卖公平定价；TGE后72小时±50%熔断；防死亡螺旋四级干预机制
项目风险	投资标的可能亏损，风投项目可能失败，本金可能全部损失。PE/VC行业历史平均失败率约50-70%（单笔）	双引擎分散（70%现金流+30%增长）；单一标的≤25%；行业≤40%；地域≤30%；保险基金10%计提
技术风险	智能合约可能存在未被发现的漏洞；浏览器兼容性可能影响挖矿体验；跨链桥可能被攻击	TGE前独立审计+形式化验证；Bug Bounty $1K-$50K；72小时时间锁；多签暂停机制
监管风险	各国及地区监管政策可能发生变化，可能导致部分功能受限或特定区域用户无法参与	开曼 SPV 架构；默认零验证（核验由持牌第三方在其服务侧承担）；前端 IPFS 镜像抗审查；不面向特定国家营销
流动性风险	子代币在早期可能缺乏足够交易深度；LIGHT在TGE初期可能面临抛售压力	子代币AMM初始流动性（发行量6%）；30天转让锁定期；团队/投资者12月cliff+36月线性

风险类型	说明	缓解措施
稀释风险	随活跃矿工增长，人均挖矿收益将自然稀释（BaseReward分母增大）	设计意图：早期参与者承担更高风险获得更高回报；后期用户可通过邀请分成加速积累；治理门槛动态下调
运营风险	被投企业经营管理可能不达预期；SPV运营依赖第三方董事；投资团队可能流失	SPV章程约束+独立董事；DAO可投票更换董事；SIAC/ICC仲裁条款；关键人保险（探索中）
跨链桥风险	wLIGHT跨链桥由第三方运营，桥合约漏洞可能导致资产损失（历史上跨链桥是最大单点损失来源）	桥上线前独立审计；桥接资产不超过总供应量5%；风险披露；用户可选择仅使用原生链
验证者风险	验证者集体离线或作恶可能导致链暂停出块，所有用户操作（挖矿、投票、转账）暂时不可用	Tendermint BFT容忍<1/3作恶；验证者≥21个（f=6）；Slashing惩罚；紧急迁移投票机制

13.2 免责声明

- LIGHT 及子代币不是证券，不具有内在价值，价格可能归零。本白皮书不构成任何形式的证券发行文件、投资要约或投资建议。
- 协议收入分配取决于底层资产的实际经营表现，历史数据不代表未来收益。任何关于投资回报的描述均为前瞻性估计，非承诺。
- 用户须自行承担私钥丢失、泄露导致的全部损失，协议不提供找回服务。使用第一层（Passkey）或第二层（社交恢复）钱包可降低此风险，但不消除。
- 本协议面向全球用户（受限于适用法律法规），用户应自行确认其所在司法辖区对加密资产、DAO组织及SPV收益凭证的法律态度，并确保参与行为合法合规。
- 本白皮书中的前瞻性陈述（包括路线图、收益模型、通缩估算、投资规模预测）均为基于当前假设的预测，实际结果可能因市场、技术、监管、团队执行等因素而重大偏离。
- 邀请激励为单层分成机制，不构成多层次营销或金字塔计划。但用户仍应自行确认其所在司法辖区对推荐奖励的法律态度。
- 参与LightDAO生态的最低年龄为18岁（或所在司法辖区的法定成年年龄，以较高者为准）。未成年人不得参与挖矿、治理或投资。

附录A：关键参数汇总表

类别	参数	数值
发行	总量	25亿枚，永不增发

类别	参数	数值
发行	挖矿	40% = 10亿枚
发行	投资金库	34% = 8.5亿枚
发行	生态基金	16% = 4亿枚
发行	战略运营	10% = 2.5亿枚（服务50%/融资30%/贡献者20%）
发行	减半周期	每2年
发行	第一纪元日释放	≈68.49万枚（矿工95%=65.07万，验证者5%=3.42万）
发行	每区块奖励池	≈13.87 LIGHT
挖矿	贡献权重	带宽40%/会话30%/验证20%/稳定10%
挖矿	满加成	1.44倍
邀请	布道者/大使/合伙人	3人10%+100L / 10人15%+500L+5% / 50人20%+2500L+10%
行为	四项×5%	上限20%
Gas费	定价机制	USD等值锚定，每24h由预言机自动换算为LIGHT数量
Gas费	普通转账	$0.001等值（@$0.05时=0.02 LIGHT）
Gas费	治理投票	$0.005等值（@$0.05时=0.10 LIGHT）
Gas费	分配规则	50%销毁 / 30%验证者 / 20%生态金库
通缩	减速/预警/底线	≤15亿/≤12亿/≤10亿（流通量）
通缩	理论上限	16.5亿（10+4+2.5，金库8.5亿永不流通）
治理	提案门槛	≥5,000 LIGHT + 30天质押
治理	委员会质押	50,000 LIGHT + 100地址
治理	陪审团	10,000 LIGHT
治理	押注	5—500 LIGHT
治理	声誉加成	1年+15次投票→+30%（总上限+40%）
投资	单笔上限	金库剩余×15%（初始1.275亿枚）

类别	参数	数值
投资	基准可部署	8.5亿×$0.15×75% = $9,563万≈$1亿
投资	利润分配(年度)	40/30/20/10
投资	利润分配(退出)	70/30
拍卖	目标	$1,500万（$500万储备+$1,000万投资资本）
储备	稳定金库	TGE $500万→第24月$800万
保险	计提	利润10%
空投	总预算	5,500万枚（生态基金13.75%），CAC≈$55/留存用户
验证者	初始/上限	21（最低10）/ 100
验证者	最低质押	500,000 LIGHT
验证者	TGE硬性底线	≥7个，否则不得上线

附录B：数值推导与校验

B.1 挖矿产出

2A=10亿→A=5亿。日释放=5亿÷730=684,932≈68.49万。矿工池=684,932×95%=650,685≈65.07万。验证者=684,932×5%=34,247≈3.42万。每区块=684,932÷49,371≈13.87。校验：684,932×730=499,999,960≈5亿✓

B.2 治理门槛可达性

10万矿工基准（6.51/天，合伙人74.44/天）：提案5,000→768天/67天；委员会50,000→7,684天(21年)/672天(22月)；陪审团10,000→1,537天(4.2年)/134天(4.5月)；押注500→77天/6.7天。

种子期（1万矿工，65.07/天，合伙人744.4/天）：提案→77天(2.5月)/6.7天；委员会→768天(25月)/67天(2.2月)；陪审团→154天(5月)/13.4天。

B.3 通缩时间线

流通量=挖矿+生态+战略(vested)−兑换−Gas−回购。金库8.5亿永不流通。

年	累计挖矿	生态	战略	兑换	Gas	回购	流通量
1	2.50	2.80	0	0	0.01	0	≈5.29
2	5.00	4.00	0.83	0.05	0.02	0	≈9.76
3	6.25	4.00	1.67	0.20	0.03	0.05	≈11.64
4	7.50	4.00	2.50	0.45	0.04	0.20	≈13.31(峰值)
5	8.13	4.00	2.50	0.80	0.05	0.50	≈13.28
6	8.75	4.00	2.50	1.20	0.06	0.90	≈13.09
7	9.06	4.00	2.50	1.60	0.07	1.40	≈12.49
8	9.38	4.00	2.50	2.00	0.08	1.90	≈11.89
9	9.53	4.00	2.50	2.40	0.09	2.30	≈11.24
10	9.69	4.00	2.50	2.80	0.10	2.70	≈10.59
11	9.77	4.00	2.50	3.10	0.11	3.00	≈10.06
12	9.84	4.00	2.50	3.40	0.12	3.30	≈9.52

结论：峰值Y4≈13.31亿；预警线12亿约Y8触及；底线10亿约Y11-12触及；减速线15亿仅极端低销毁情景。

附录C：审计修正日志（累计36项）

含原22项（L1-5, A1-4, D1-4, M1-8, G1-3）+ 技术架构7项（T1-7）+ 本轮经济模型优化7项：

编号	修正
E-1	总量21亿→25亿（投资容量约束驱动）
E-2	分配50/30/20→40/34/16/10（新增战略运营基金10%）
E-3	荷兰拍卖$1,000万→$1,500万（初始投资资本$500万→$1,000万）
E-4	新增5.7节空投增长计划（5,500万枚，CAC $55/人）

编号	修正
E-5	验证者分阶段启动（测试网7→TGE最低10/目标21→开放100）
E-6	通缩触发线调整（14/12/10→15/12/10，适配16.5亿流通上限）
E-7	外部引用全部替换为可验证来源（移除不可验证SSRN论文）

附录D：术语速查索引

各术语的完整解释已标注于其首次出现章节末尾的【本章术语】注释块中。本索引按字母顺序列出所有术语及其所在章节，便于快速定位。

术语	定义所在章节
AMM（自动做市商）	第四章
BFT（拜占庭容错）	第四章
CAC（用户获取成本）	第五章
CEX（中心化交易所）	第四章
Cosmos SDK	第四章
CosmWasm	第四章
DAO（去中心化自治组织）	第二章
DCF（现金流折现法）	第九章
DePIN（去中心化物理基础设施网络）	第二章
DEX（去中心化交易所）	第四章
EBITDA（息税折旧摊销前利润）	第九章
Gas费	第四章
IBC（跨链通信协议）	第三章
IPFS（星际文件系统）	第四章

术语	定义所在章节
KYC（了解你的客户）	第三章
LIGHT（原生代币）	第四章
LP（流动性提供者）	第五章
Lower Middle Market PE（下游中端私募股权）	第二章
Merkle Tree（默克尔树）	第四章
MiFID II（欧盟金融工具市场指令II）	第三章
MLM（多层次营销）	第三章
PII（个人可识别信息）	第三章
PoC（贡献证明）	第四章
PoS（权益证明）	第四章
PoW（工作量证明）	第四章
Pre-IPO	第九章
PWA（渐进式Web应用）	第四章
Reg D / Reg S（美国证券法D/S条例）	第三章
Slashing（罚没）	第四章
SPV（特殊目的载体）	第二章
TGE（代币生成事件）	第五章
TWAP（时间加权平均价格）	第四章
TWAP执行（回购拆单）	第九章
VWAP（成交量加权平均价格）	第五章
wLIGHT（封装LIGHT）	第五章
ZK-KYC（零知识证明KYC）	第三章
子代币（Sub-token）	第五章

术语	定义所在章节
死亡螺旋（Death Spiral）	第五章
减半（Halving）	第五章
金库（Treasury）	第五章
荷兰式拍卖（Dutch Auction）	第五章
预言机（Oracle）	第四章

白皮书全文完

版权说明： 本文档为开源社区文档，可自由转载，但须保留完整内容。

附录:主网已验证参数与地址(V2.4 实况)

A. §4.5 Gas 经济实测参数

- min-gas-price 公式:`(TransferUsdTarget / UsdPerLight) × 10^6 / RefTransferGas`;当前 TransferUsdTarget=$0.001、UsdPerLight=$0.05、RefTransferGas=100000 → **0.2 ulight/gas**
- 分配实测(总 fee 300000 ulight):销毁 150000(50%)/ 金库 60000(20%)/ 验证者 90000(30%),精确匹配
- 销毁地址:`wasm1aeaty43lrlt9rmkyxujkkfuddnsfye6az4htcu`(确定性死地址)
- 金库:`treasury_multisig` 合约(3/5 多签;链上 `signers` 查询返回 5 名签名人,阈值本身不在查询接口内)

B. 核心合约地址

见仓库 `docs/MAINNET_STATUS.md`(light_token / mining_reward / governance / treasury_multisig / oracle_twap / vesting 等 10 合约)。

C. 遗留 denom(stake)处置

genesis 误配 mint_denom=stake 已归零停止增发;存量 stake(约 2.56e11 微单位)为无用途遗留,处置方案(兑换/销毁)待治理提案,不影响 ulight 经济模型。

D. §4.4 vesting 实况

vault 250,000,000 LIGHT,3 个独立 schedule:75M(cliff 0)/ 100M(cliff 1 年)/ 75M(cliff 2 年),已上链。

E. 安全实践

- 主网升级为 x/upgrade 治理 + 全节点同块高协调 + auto-swap 看门狗,测试网端到端彩排后执行
- Passkey 种子仅密文存储;Shamir 分片本地不保存
- 合约挖矿根提交阈值 5(链上每笔 `submit_root` 事件实测 threshold=5;当前 5 个授权账户在签,7 席为设计目标);反女巫/反作弊见 §4.8
