



LAODENG UNIVERSE

LAODENG Universe 区块链白皮书

V5 去中心化动态难度与动态 Gas 技术规范

技术白皮书 1.0 | 2026 年 7 月

Chain ID 20260001 | Protocol V5 | Native Asset LDU



文件状态

本文件描述当前 V5 代码实现与协议目标，不构成投资、收益或法律承诺。项目尚未接受独立第三方安全审计。

目录

- 01 执行摘要
- 02 设计原则与系统边界
- 03 总体架构
- 04 工作量证明与动态难度
- 05 区块、状态与最终性
- 06 LDU 经济模型
- 07 动态 Gas 与费用分配
- 08 交易、EVM 与钱包兼容
- 09 网络、挖矿与同步
- 10 区块浏览器与可观测性
- 11 安全模型与部署要求
- 12 升级、治理、风险与路线图

网络参数速览

项目	LAODENG Universe	原生产产	LDU
协议版本	V5	Chain ID	20260001
小数位	18	目标出块	30 秒
最大供应	100,000,000 LDU	创世分配	100,000 LDU
挖矿额度	99,900,000 LDU	初始奖励	25 LDU
减半周期	2,000,000 块	难度周期	20 块
初始难度	226,000,000	区块 Gas 上限	30,000,000
创世基础费	1 Gwei	最低基础费	0.01 Gwei

01

执行摘要

LAODENG Universe 是一条 EVM 兼容工作量证明链。V5 将持续空块、链上可验证的动态难度、EIP-1559 风格动态 Gas、18 位资产精度和官方 LDUScan 区块浏览器整合为一个可独立运行的软件体系。

系统采用固定的共识规则与动态的运行参数。初始挖矿难度写入协议，随后每 20 个区块依据区块头时间戳确定性调整。任何完整节点都能重算预期难度并拒绝不符合规则的区块，因此调整过程不依赖中心化配置服务器。

项目的设计重点是可理解、可验证和可部署，而不是承诺商业回报。LDU 是链的原生 Gas 与价值计量单位，不是 ERC-20 合约代币。钱包直接通过 Chain ID 和 RPC 识别余额。

关键控制

- 完整节点独立验证区块头、PoW、状态根、交易根、收据根和累计难度。
- 协调节点可以只派发工作而不使用本机 CPU，手机和电脑矿工竞争同一高度。
- 浏览器直接读取 JSON-RPC，并用 SQLite 建立可重建索引。

02

设计原则与系统边界

协议优先采用整数运算和明确上限。余额、奖励、Gas 费用与供应量均以 10^{18} 最小单位存储，避免浮点舍入。共识字段进入区块头哈希，链身份由 Chain ID、协议版本和创世哈希共同约束。

去中心化在本项目中意味着多个完整节点可独立验证、同步和选择累计工作量更高的链；多个协调节点可并行服务矿工。单个网页、RPC 网关或矿池不是共识信任根。若某协调节点离线，矿工可以连接其他协调节点。

系统仍有明确边界：代码规模和测试覆盖不能替代第三方审计；公网 RPC、矿工端口和节点端口需要防火墙、限流、TLS 或 VPN；调试签名 APK 仅适合测试。

关键控制

- 确定性：相同父链与交易序列得到相同状态。
- 最小权限：主节点可禁用本机挖矿。
- 可恢复：浏览器索引可删除后从创世块重建。
- 兼容性：提供常用 Ethereum JSON-RPC 与 Type-2 交易字段。

03

总体架构

节点由共识执行层、状态数据库、交易池、PoW 调度器、完整节点网络和 JSON-RPC 服务组成。执行层基于 go-ethereum 的交易、状态与 EVM 组件，项目代码负责链参数、区块封装、奖励、Gas 分配、持久化和网络策略。

交易由钱包提交到 RPC，进入按账户 Nonce 管理的交易池。候选区块按有效优先费选择交易，执行后计算状态根、交易根、收据根、日志 Bloom 与 Gas 使用量，再为每个矿工绑定收款地址生成独立 PoW 工作。

成功证明返回协调节点后，节点复算哈希和目标，提交状态并广播完整区块。其他节点从共同祖先重放区块，按照累计总难度选择规范链。

关键控制

- 钱包 / 应用 → HTTPS RPC → 交易池
- 交易池 → EVM 执行 → 候选区块
- 协调节点 → 手机与电脑矿工 → 有效 PoW
- 完整节点网络 → 校验、同步、重组
- JSON-RPC → FastAPI 浏览器 → SQLite 索引

04

工作量证明与动态难度

V5 允许包含零笔交易的区块持续产生。空块使相邻区块时间具有共识意义，从而能够在不依赖链外挖矿计时的情况下调整难度。初始难度为 226,000,000，目标平均出块时间为 30 秒。PoW 结果服从随机分布，单块可能显著快于或慢于目标。

每当父区块高度为 20 的倍数时，下一块使用新难度。周期两端各选取 3 个区块时间戳并取中位数，以降低单个边界时间戳的影响。有效测量区间为 18 个区块间隔，目标时间为 $18 \times 30 = 540$ 秒。

计算公式为 $\text{newDifficulty} = \text{oldDifficulty} \times \text{expectedTime} / \text{actualTime}$ 。结果使用整数除法，并限制在旧难度的 0.5 倍至 2 倍之间，最后执行最低难度 1,024。新难度进入区块头、PoW 目标和累计总难度。

每个新区块时间戳必须大于过去 11 块的中位时间，并且不得领先验证节点当前时间超过 120 秒。该约束与边界中位数共同降低矿工操纵时间以改变难度的空间。

关键控制

- 首次调整后的难度从区块 #21 生效。
- 后续调整从 #41、#61、#81 等高度生效。
- 单周期算力大幅变化不会让难度瞬间超过 2 倍或低于一半。
- 规范链由累计工作量优先，工作量相同使用确定性哈希规则打破平局。

05

区块、状态与最终性

区块头承诺协议版本、Chain ID、父哈希、高度、时间戳、矿工、Gas 上限、Gas 使用量、基础费、状态根、交易根、收据根、日志 Bloom、难度、累计难度和 Nonce。任何字段变化都会改变区块哈希。

账户状态以 256 位整数表示余额和 EVM Gas 存储。交易执行产生收据、状态码、日志和合约地址。失败交易不转移调用价值，但仍根据实际使用扣费。状态只有在 PoW 成功并完成数据库提交后才成为规范状态。

PoW 链没有绝对即时最终性。应用应根据价值选择确认数，并理解短分叉可能重组。节点限制自动重组深度为 128 块，孤块中的仍有效交易可返回交易池。

关键控制

- 区块根与 Bloom 可检测交易、收据或日志篡改。
- 持久化加载会重新检查链身份、父子关系、动态基础费、动态难度和累计难度。
- 状态数据库提交失败时回滚候选区块和交易池。

06

LDU 经济模型

LDU 使用 18 位小数, $1 \text{ LDU} = 10^{18}$ 个最小单位。最大累计发行量为 100,000,000 LDU, 其中创世测试分配 100,000 LDU, 占 0.1%; 挖矿可发行额度为 99,900,000 LDU, 占 99.9%。创世块自身奖励为 0。

普通区块初始奖励为 25 LDU, 每 2,000,000 个区块减半。按 30 秒平均出块计算, 每轮约 60,000,000 秒, 即约 694.44 天或 1.90 年。奖励完全使用整数最小单位计算, 最终趋近于零。

当挖矿累计发行达到 99,900,000 LDU, 或累计发行达到 100,000,000 LDU 时, 增发奖励永久归零。矿工仍可获得交易优先费。基础费销毁会降低当前流通供应量, 但不会重新打开已经使用的挖矿发行额度。

关键控制

- 余额示例: 创世 100,000 - 转账 1 - Gas + 区块奖励 25 = 约 100,024 LDU, 具体值取决于 Gas。
- 持续空块也获得区块奖励, 因此减半按真实区块高度推进。
- 白皮书不对 LDU 市价、流动性或收益作任何保证。

07

动态 Gas 与费用分配

每个区块 Gas 上限为 30,000,000，目标使用量为 15,000,000。基础费根据父区块利用率调整：高于目标时上升，低于目标时下降，每块最大变化 12.5%。创世基础费为 1 Gwei，最低基础费为 0.01 Gwei，用于避免安静网络降至零费用。

Type-2 交易的实际单价为 $\min(\text{maxFeePerGas}, \text{baseFeePerGas} + \text{maxPriorityFeePerGas})$ 。Legacy 与 Type-1 交易使用 gasPrice，并要求 gasPrice 至少覆盖当前基础费。基础费从供应中永久销毁，优先费支付给实际出块地址。

交易池支持跨多个区块排队、账户 Nonce 顺序和同 Nonce 替换。不同账户的可执行队首交易按照有效优先费排序；替换交易要求费用至少提高 10%。余额预检使用费用上限，执行结算使用实际 Gas 和实际价格。

关键控制

- $\text{eth_gasPrice} = \text{下一块基础费} + \text{建议优先费}$ 。
- $\text{eth_maxPriorityFeePerGas}$ 使用近期非零小费中位数，无历史时为 0.1 Gwei。
- eth_feeHistory 返回真实基础费、Gas 利用率和按 Gas 加权的小费百分位。

08

交易、EVM 与钱包兼容

链接受带 Chain ID 20260001 的签名交易，验证签名恢复地址、Nonce、余额、内在 Gas、费用上限和交易大小。支持普通转账、合约创建、合约调用、事件日志、访问列表和 EIP-1559 Type-2 费用字段。

LDU 是原生币，因此 MetaMask、Binance Wallet 等 EVM 钱包添加自定义网络后会直接显示 LDU 余额，不需要代币合约地址。钱包展示精度为 18 位，前端必须使用 BigInt 或可靠大数库。

RPC 实现常用账户、区块、交易、收据、日志、调用、Gas 估算和费用接口。兼容性目标是支持常见钱包和开发流程，而不是声称与任意 Ethereum 客户端的每个调试或管理接口完全等价。

关键控制

- 网络名称：LAODENG Universe。
- 货币符号：LDU。
- Chain ID：20260001，十六进制 0x13524a1。
- RPC 应通过 HTTPS 暴露给公网钱包。

09

网络、挖矿与同步

完整节点使用独立的 V5 点对点协议交换身份、定位器、区块和累计难度。握手校验协议版本、Chain ID 和创世哈希，防止不同网络互连。节点从共同祖先请求有限批次区块，验证后才更新规范链。

矿工协议由协调节点派发绑定收款地址的工作。绑定可以阻止矿工截取其他地址的有效证明并更改收款地址。客户端支持多个协调节点和重连退避；CPU 线程可限制为 1。手机端显示连接、工作、成功区块、奖励地址和历史统计。

协调主节点可使用 coordinator-only 模式，不参与本机哈希竞争，但仍验证结果、提交区块并广播。真正的抗单点运行需要部署多个完整节点和多个协调入口，矿工配置多个地址。

关键控制

- node.laodeng.org:30304：完整节点 P2P。
- mine.laodeng.org:30303：矿工协调协议。
- https://rpc.laodeng.org：受限钱包/DApp RPC。
- https://scan.laodeng.org：官方 LDUScan。

区块浏览器与可观测性

浏览器后端使用 FastAPI，通过 JSON-RPC 读取真实区块、交易、收据和余额，不解析终端日志。SQLite 仅作为可重建的查询索引，用于区块列表、地址累计值和余额变动明细。RPC 断开时网页保留最后同步数据并显示离线原因。

首页展示区块高度、供应量、累计销毁、挖矿发行、奖励、减半倒计时、平均出块时间、当前难度和下次难度调整。详情页区分创世分配、转账、Gas 扣款、区块奖励、优先费收入与基础费销毁。

金额从 RPC 整数转换为 18 位 LDU，最多显示 18 位小数并去除无意义末尾零。中英文界面默认跟随系统语言，支持手动切换和深色、浅色主题。

关键控制

- 索引数据库不是共识数据源。
- 索引不一致时可删除并从区块 0 重建。
- 服务端限制请求大小、分页数量与访问频率。

11

安全模型与部署要求

主要威胁包括私钥泄露、RPC

滥用、交易池垃圾、时间戳操纵、低算力重组、恶意矿工结果、数据库损坏和依赖漏洞。V5 使用 Chain ID 签名隔离、费用下限、消息大小限制、连接限额、PoW

复算、时间戳约束、累计难度分叉选择和原子持久化降低风险。

服务器应将 RPC 绑定到本机或私网，通过 TLS 反向代理发布所需方法，启用防火墙、速率限制和访问日志。管理密钥不得放入源码、压缩包、网页目录或命令历史。节点数据与密钥应分开备份，并定期执行恢复演练。

公网矿工端口和节点端口应只在确有需要时开放。个人部署优先使用 VPN。Windows EXE 与 Android Release APK 均提供 SHA-256 校验；Android 正式版使用长期保管的独立发布证书签名，并应固定核验其证书指纹。

关键控制

- 当前版本已通过项目内单元、集成、静态与实际挖矿测试。
- 当前版本没有第三方审计结论。
- 运营者必须监控高度停滞、同高度分叉、异常难度、RPC 错误率、磁盘空间和节点时间。

12

升级、治理、风险与路线图

V5 是不兼容 V4 的共识版本，使用新的创世哈希和 `data/laodeng-v5-mainnet` 数据目录。协议版本、创世参数或共识公式变化必须形成新版本和明确激活计划，不能由单个节点静默修改。

项目治理以代码、参数文件、发行哈希和公开说明为准。建议发行时固定源码归档、Windows EXE、APK 签名证书指纹、白皮书版本和创世哈希。升级前应在独立测试网运行，并保留数据库备份与回退说明。

关键风险包括初期算力集中、协调入口集中、PoW 能耗、出块随机性、软件缺陷、钱包兼容差异和监管不确定性。未来工作可包括可复现构建、模糊测试、更多异构节点、硬件钱包测试、监控面板和外部安全复核。

关键控制

- 该路线图是工程方向，不构成时间或交付承诺。
- 任何公开主网都应先进行多节点长时间测试。
- 协议安全取决于软件正确性、诚实算力、运维安全与用户密钥管理的共同作用。

A

附录：正式参数与参考资料

项目	LAODENG Universe	原生产产	LDU
协议版本	V5	Chain ID	20260001
小数位	18	目标出块	30 秒
最大供应	100,000,000 LDU	创世分配	100,000 LDU
挖矿额度	99,900,000 LDU	初始奖励	25 LDU
减半周期	2,000,000 块	难度周期	20 块
初始难度	226,000,000	区块 Gas 上限	30,000,000
创世基础费	1 Gwei	最低基础费	0.01 Gwei

参考资料

- EIP-1559: Fee market change for ETH 1.0 chain - <https://eips.ethereum.org/EIPS/eip-1559>
- Ethereum JSON-RPC API - <https://ethereum.org/developers/apis/json-rpc/>
- go-ethereum source and documentation - <https://geth.ethereum.org/>
- LAODENG Universe V5 chain specification - config/chain-spec-v5-mainnet.json

正式创世哈希

0x00ec8452119c4bbb0f7f4d31948546ded651fae41e44f05e4a67943d77a3faa3

若本白皮书与已发行源码或链参数文件不一致，以对应版本源码和 chain-spec-v5-mainnet.json 为准。