LAODENG
UNIVERSE

LAODENG Universe Blockchain Whitepaper

V5 Decentralized Difficulty Retargeting and Dynamic Gas Specification

Technical Whitepaper 1.0 | July 2026

Chain ID 20260001 | Protocol V5 | Native Asset LDU

DOCUMENT STATUS

This document describes the current V5 implementation and protocol objectives. It is not investment, return, or legal advice. The project has not completed an independent third-party security audit.

Contents

NETWORK AT A GLANCE

Project	LAODENG Universe	Native asset	LDU
Protocol	V5	Chain ID	20260001
Decimals	18	Block target	30 seconds
Maximum supply	100,000,000 LDU	Genesis allocation	100,000 LDU
Mining allocation	99,900,000 LDU	Initial reward	25 LDU
Halving interval	2,000,000 blocks	Retarget interval	20 blocks
Initial difficulty	226,000,000	Block gas limit	30,000,000
Genesis base fee	1 Gwei	Minimum base fee	0.01 Gwei

01

Executive Summary

LAODENG Universe is an EVM-compatible proof-of-work blockchain. V5 combines continuous empty blocks, consensus-verifiable difficulty retargeting, EIP-1559-style dynamic gas, 18-decimal asset accounting, full-node synchronization, and the official LDUScan explorer.

The protocol separates fixed rules from dynamic operating values. Initial difficulty is a protocol parameter; every 20 blocks, all full nodes deterministically derive the next difficulty from committed block timestamps. A block carrying an unexpected difficulty is invalid, so no central configuration service controls retargeting.

LDU is the native asset used for gas and value transfer. It is not an ERC-20 token and requires no token contract address. The project prioritizes inspectability and practical deployment, and makes no promise of market value or financial return.

KEY CONTROLS

- Independent validation of PoW, state, transaction, receipt, gas, and cumulative-work commitments.
- Coordinator-only nodes can dispatch work without consuming local CPU.
- The explorer consumes JSON-RPC data and maintains a disposable SQLite query index.

02

Design Principles and Scope

Consensus accounting uses integers throughout. Balances, rewards, fees, burns, and supply are represented in 10^18 base units. Protocol version, Chain ID, and genesis hash jointly identify the network, while committed roots make state transitions auditable.

Decentralization means that multiple full nodes can independently verify, synchronize, and select the valid chain with the greatest cumulative work. Multiple coordinators may serve miners in parallel. A website, RPC gateway, or individual mining coordinator is not a consensus trust anchor.

The boundaries are explicit. Internal testing does not replace an external audit; public RPC and peer interfaces require firewalling, rate limits, TLS, or VPN controls; and every public APK must be signed with the project's long-lived release identity.

KEY CONTROLS

- Determinism: identical parent state and transactions produce identical commitments.
- Least privilege: a coordinator can disable local CPU mining.
- Recoverability: the explorer index can be rebuilt from genesis.
- Compatibility: common Ethereum JSON-RPC methods and Type-2 fee fields are supported.

03

System Architecture

A node contains consensus execution, an EVM state database, transaction pool, PoW scheduler, full-node networking, persistence, and JSON-RPC. go-ethereum components provide transaction, state, and EVM primitives; LAODENG code defines chain identity, block construction, rewards, fee distribution, network policy, and validation rules.

Wallet transactions enter the RPC and are queued by sender nonce. Executable account heads are prioritized by effective tip. Execution produces state, transaction, receipt, and log commitments. The candidate header is then bound to each miner payout address before PoW work is distributed.

The coordinator recomputes every submitted proof and commits state only after a valid result. Peers replay blocks from a common ancestor and compare cumulative work before adopting a branch. This separates mining work distribution from consensus validation.

KEY CONTROLS

- Wallet/application -> HTTPS RPC -> transaction pool
- Transaction pool -> EVM execution -> candidate block
- Coordinator -> mobile and desktop miners -> valid PoW
- Full-node network -> validate, synchronize, reorganize
- JSON-RPC -> FastAPI explorer -> SQLite index

04

Proof of Work and Difficulty Retargeting

V5 continuously produces blocks, including blocks with zero transactions. This gives inter-block timestamps consensus meaning and allows retargeting without trusting off-chain mining-duration reports. Initial difficulty is 226,000,000 and the long-run target is 30 seconds per block. Individual solve times remain random.

When the parent height is a multiple of 20, the next block begins a new difficulty epoch. Three timestamps are sampled at each epoch boundary and reduced to a median. The measurement spans 18 block intervals, with an expected duration of 18 x 30 = 540 seconds.

The deterministic formula is newDifficulty = oldDifficulty x expectedTime / actualTime. Integer division is used. The result is clamped to 0.5x through 2x of the previous difficulty and then to a protocol floor of 1,024. Difficulty is committed in the header and cumulative-work calculation.

A new timestamp must exceed the median time of the previous 11 blocks and cannot exceed validator wall time by more than 120 seconds. These checks and median boundary samples reduce the effect of a single manipulated timestamp.

KEY CONTROLS

- The first retarget applies to block 21.
- Later retargets apply to blocks 41, 61, 81, and so on.
- Abrupt hash-rate changes are absorbed over bounded epochs.
- The canonical chain maximizes cumulative work, with deterministic tie-breaking.

05

Blocks, State, and Finality

The block header commits protocol version, Chain ID, parent hash, height, timestamp, miner, gas limit and usage, base fee, state root, transaction root, receipt root, logs bloom, difficulty, cumulative difficulty, and nonce. Altering any committed field changes the block hash.

Account balances and EVM storage use 256-bit integers. Transaction execution creates status, logs, receipts, and contract addresses. A failed call does not apply its requested value transfer, but still pays for gas actually consumed. State becomes canonical only after proof verification and database commit.

PoW finality is probabilistic. Applications should select confirmation depth according to value and threat model. Nodes limit automatic reorganizations to 128 blocks, and valid transactions from orphaned blocks may return to the pool.

KEY CONTROLS

- Commitment roots detect transaction, receipt, log, or state tampering.
- Startup revalidates identity, linkage, base fee, difficulty, and cumulative work.
- Persistence failures roll back candidate state and restore transactions.

06

LDU Monetary Policy

LDU uses 18 decimals: 1 LDU equals 10^18 base units. Maximum cumulative issuance is 100,000,000 LDU. The genesis test allocation is 100,000 LDU, or 0.1 percent; mining may issue at most 99,900,000 LDU, or 99.9 percent. The genesis block reward is zero.

The initial ordinary block reward is 25 LDU and halves every 2,000,000 blocks. At the 30-second target, one epoch is approximately 60,000,000 seconds, 694.44 days, or 1.90 years. Rewards are computed exclusively in integer base units and eventually converge to zero.

Issuance permanently stops when mining issuance reaches 99,900,000 LDU or cumulative issuance reaches 100,000,000 LDU. Miners may still collect priority fees. Base-fee burning reduces circulating supply but never recreates spent mining issuance capacity.

KEY CONTROLS

- Continuous empty blocks receive the protocol reward.
- Halving therefore advances with real block height.
- No statement in this paper guarantees price, liquidity, or mining profitability.

07

Dynamic Gas and Fee Distribution

The block gas limit is 30,000,000 and the target is 15,000,000. Base fee rises above target utilization and falls below it, with a maximum 12.5 percent change per block. Genesis base fee is 1 Gwei and the anti-spam floor is 0.01 Gwei.

For Type-2 transactions, effective gas price is min(maxFeePerGas, baseFeePerGas + maxPriorityFeePerGas). Legacy and Type-1 transactions use gasPrice and must cover base fee. Base fee is permanently burned; the priority component is paid to the successful block miner.

The pool spans multiple blocks, preserves sender nonce order, prioritizes executable account heads by effective tip, and requires a 10 percent fee bump for same-nonce replacement. Admission reserves fee cap while execution settles actual gas at the effective price.

KEY CONTROLS

- eth_gasPrice returns next base fee plus a priority-fee suggestion.
- eth_maxPriorityFeePerGas uses recent non-zero median tips, defaulting to 0.1 Gwei.
- eth_feeHistory reports real base fees, utilization, and gas-weighted tip percentiles.

08

Transactions, EVM, and Wallets

Signed transactions must target Chain ID 20260001. Validation covers recovered sender, nonce, balance, intrinsic gas, fee caps, transaction size, and supported type. Transfers, contract creation, contract calls, logs, access lists, and EIP-1559 Type-2 fee fields are supported.

Because LDU is native currency, MetaMask and other EVM wallets display it immediately after a custom network is added. No token contract is required. User interfaces must use BigInt or a reliable arbitrary-precision library for 18-decimal values.

The RPC implements common account, block, transaction, receipt, log, call, gas-estimation, and fee methods. Compatibility targets normal wallet and development workflows and does not claim parity with every Ethereum administrative or debugging API.

KEY CONTROLS

- Network name: LAODENG Universe.
- Currency symbol: LDU.
- Chain ID: 20260001, hexadecimal 0x13524a1.
- Public wallet access should use an HTTPS RPC endpoint.

09

Networking, Mining, and Synchronization

The V5 full-node protocol exchanges identity, locators, blocks, and cumulative difficulty. Handshake validation covers protocol version, Chain ID, and genesis hash. Nodes request bounded batches from a common ancestor and apply full validation before changing canonical state.

Coordinators distribute work bound to each authenticated payout address, preventing a miner from changing the recipient on another miner's proof. Clients support multiple coordinators, retry backoff, and configurable CPU worker count. Mobile clients report work, successful blocks, payout address, and income history.

Coordinator-only mode disables local hashing while retaining proof validation, state commit, and broadcasting. Removing single-point dependency requires multiple full nodes and coordinator endpoints, with miners configured for more than one address.

KEY CONTROLS

- node.laodeng.org:30304: full-node P2P.
- mine.laodeng.org:30303: mining coordinator protocol.
- https://rpc.laodeng.org: restricted wallet/DApp RPC.
- https://scan.laodeng.org: official LDUScan.

10

Explorer and Observability

The FastAPI explorer reads blocks, transactions, receipts, and balances through JSON-RPC rather than terminal logs. SQLite is a rebuildable query index for lists, address aggregates, and balance-change history. When RPC is offline, the service retains its last synchronized view and presents a clear error.

The home page reports height, supply, burned base fees, mining issuance, reward, halving estimate, average block time, current difficulty, and next retarget. Detail pages distinguish genesis allocation, transfers, gas debits, rewards, priority income, and base-fee burn.

RPC integers are formatted as 18-decimal LDU with insignificant trailing zeros removed. The interface follows system language by default, supports Chinese and English, and provides light and dark themes.

KEY CONTROLS

- The SQLite index is not a consensus source.
- It can be deleted and rebuilt from block zero.
- The service bounds request size, page size, and request rate.

11

Security and Deployment

Threats include key compromise, RPC abuse, mempool spam, timestamp manipulation, low-hash-rate reorganizations, invalid miner submissions, database corruption, and dependency vulnerabilities. V5 mitigations include replay-protected signatures, fee floors, message limits, connection quotas, proof recomputation, timestamp rules, cumulative-work selection, and atomic persistence.

Production servers should bind RPC to loopback or a private interface and publish only required methods through a TLS reverse proxy with firewall and rate limits. Administrative keys must never enter source code, release archives, web roots, or shell history. Backups should separate keys from chain data and be recovery-tested.

Peer and mining ports should be public only when required; a VPN is preferred for personal deployment. Windows and Android release artifacts include SHA-256 checksums. The Android Release APK is signed with the project's long-lived private release identity, whose certificate fingerprint should be pinned and verified before distribution.

KEY CONTROLS

- Internal unit, integration, static, and real-mining tests have passed.
- No independent third-party audit has been completed.
- Operators should alert on stalled height, competing tips, abnormal difficulty, RPC failures, disk pressure, and clock drift.

12

Upgrades, Governance, Risks, and Roadmap

V5 is consensus-incompatible with V4 and uses a new genesis hash and data/laodeng-v5-mainnet directory. Changes to protocol version, genesis parameters, or consensus formulas require a new release and explicit activation plan; a single node cannot silently redefine validity.

Release governance should pin a source archive, executable hashes, APK certificate fingerprint, whitepaper version, and genesis hash. Upgrades should first run on an isolated test network, with database backup and rollback instructions prepared before activation.

Material risks include early hash-rate concentration, coordinator concentration, PoW energy use, stochastic block times, software defects, wallet differences, and regulatory uncertainty. Future engineering may add reproducible builds, fuzzing, heterogeneous nodes, hardware-wallet testing, monitoring dashboards, and external review.

KEY CONTROLS

- The roadmap is directional and not a delivery commitment.
- A public network should complete sustained multi-node testing before material use.
- Security is the combined result of software correctness, honest work, operations, and user key management.

A

Appendix: Canonical Parameters and References

Project	LAODENG Universe	Native asset	LDU
Protocol	V5	Chain ID	20260001
Decimals	18	Block target	30 seconds
Maximum supply	100,000,000 LDU	Genesis allocation	100,000 LDU
Mining allocation	99,900,000 LDU	Initial reward	25 LDU
Halving interval	2,000,000 blocks	Retarget interval	20 blocks
Initial difficulty	226,000,000	Block gas limit	30,000,000
Genesis base fee	1 Gwei	Minimum base fee	0.01 Gwei

References

- 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

Canonical genesis hash

0x00ec8452119c4bbb0f7f4d31948546ded651fae41e44f05e4a67943d77a3faa3

This whitepaper is subordinate to the released source code and chain specification in any case of inconsistency.