Whitepaper

Limit Blockchain - Redefining the Foundation of Digital Trust

Overview

Limit Blockchain is designed to be a self-contained, secure, and future-forward decentralized network.

Inspired by fundamental blockchain principles, it introduces a unique structural and cryptographic approach to on-chain identity, supply, and block generation.

Total Supply

- Fixed Total Supply: 20,820,080 LIMIT
- No inflation, minting, or additional issuance
- This supply model emphasizes scarcity, transparency, and long-term sustainability

Address Generation Logic

1. Standard Private Key Format (Up to 256-bit)

- Traditional private key -> Public key -> Address
- Utilizes standard elliptic curve cryptography (secp256k1) and hashing (SHA-256)
- All addresses will begin with a unique Base58 prefix derived from: 030808

2. Extended Private Key Format (256-bit to 512-bit)

- Input private key (up to 512-bit) -> SHA-256 hash -> Used to derive public key -> Address
- This method ensures a valid 256-bit cryptographic key is always generated from higher entropy
- High entropy allows for near-infinite keyspace - ensuring address uniqueness remains intact even under extended range use

- Enables broader identity flexibility and longer cryptographic lifespans

Mining & Reward Mechanism

- Block Reward: 100 LIMIT tokens per mined block
- Halving Schedule: Every 1 year (365 days), reward halves
- Dynamic Difficulty Adjustment:
  - If more blocks are mined than previous day -> difficulty increases by 1%
  - If fewer blocks mined -> difficulty remains constant
- This system balances adaptability with resistance to manipulation

Security & Identity Principles

- High-bit cryptographic identity support (up to 512-bit key entropy)
- Cold wallet and offline key generation encouraged
- No reserve address systems, no central ownership, and no redistribution structure
- Each address is self-sovereign and can independently mine, transact, and store

Vision Statement

Limit Blockchain is more than a digital currency - it's a new model of identity, scarcity, and control.

It is built for resilience, flexibility, and transparency.

By leveraging deeper cryptographic layers and respecting the boundaries of finite supply, Limit sets a

new standard in decentralized digital architecture.