BLOCKLE PROTOCOL · WHITEPAPER

BLOCK: a post-quantum, universally merge-mined Layer 1

A proof-of-work blockchain secured by NIST post-quantum signatures, mined by every major ASIC algorithm at once, with native tokens, an on-chain AMM, shielded transfers, and a verifiable inference market.

AlienBeing LLC · blockle.org

Protocol v1 · This document describes the live mainnet protocol. It is technical documentation, not an offer to sell or solicitation to buy any asset.

1. Overview

Blockle is a layer-1 blockchain whose native coin is **BLOCK**. It is designed around two theses: that a chain settling value for decades must not rest on signatures a quantum computer can forge, and that proof-of-work security should draw on *all* of the world's mining hardware rather than a single algorithm's.

Every account and transaction is authenticated with **ML-DSA-44 (FIPS 204)**, NIST's standardized lattice signature scheme. Blocks are produced by a native proof-of-work and, equivalently, by merge-mining from any supported parent chain, so SHA-256, Scrypt, X11, Blake2b/Blake2s, Blake3, Eaglesong and kHeavyHash miners can all secure Blockle at no additional energy cost. On top of this base, Blockle provides a token standard (BLOCK-20), non-fungible tokens (BLOCK-721), a constant-product AMM built into consensus, optional shielded (zero-knowledge) transfers, and Blockle Intelligence — a market for AI inference settled in BLOCK.

2. Cryptographic foundation

ELEMENT	CONSTRUCTION
`Signatures`	ML-DSA-44 (FIPS 204), domain-separated with the context string `"BlklTxV1"`
`Addresses`	`blake2b_256("BlklAddr", pubkey)`, encoded bech32m as `block1…`
`Hashing`	Blake2b-256 (personalized) for txids, sighashes and Merkle nodes
`Block hash`	double-SHA-256 of the 140-byte header, compared little-endian
`Shielded field`	GF($2^{128}-45\cdot2^{40}+1$); Rescue-Prime note hashing; STARK proofs

Classical elliptic-curve signatures (secp256k1, ed25519) appear *only* at the edges, where Blockle interoperates with external chains through its multi-chain wallet. The Blockle consensus layer itself is post-quantum end to end.

3. Consensus and mining

Blockle targets a **600-second** block interval with per-block difficulty retargeting. The native proof-of-work is Equihash (200,9). The same header can instead carry an **auxiliary proof-of-work** (merge-mining): a miner on a parent chain commits Blockle's header hash into the parent coinbase and submits the parent's solved block as proof. Because the commitment is algorithm-agnostic, Blockle behaves as a **universal auxiliary chain** — a single pool can let SHA-256, Scrypt, X11, Blake2b, Blake2s, Blake3, Eaglesong or kHeavyHash hardware earn BLOCK while it mines its primary coin, with no extra electricity.

This diversifies the cost of attacking the chain across every major hardware ecosystem rather than concentrating it in one, and it lets Blockle bootstrap security from the existing global hashrate.

4. The BLOCK coin and monetary policy

- **Divisibility.** 1 BLOCK = 100,000,000 base units.
- **Issuance.** A Bitcoin-style schedule: the block subsidy halves every **210,000 blocks**, giving a hard-capped, disinflationary supply. No issuance is ever minted to pay fees, rewards, or ecosystem costs.
- **Premine.** A fixed **210,000 BLOCK** allocation exists at genesis for development and ecosystem funding; it is an allocation, not a mining reward, and is disclosed rather than hidden in the schedule.
- **Fees.** Transactions pay a fee in BLOCK; gas on contract actions is prepaid.

> Because supply is capped, BLOCK used across the ecosystem — fees on the AMM, tips and rewards in social features, bonds in the inference market — moves *circulating* coin between participants. Nothing is minted to subsidize it.

5. Tokens, NFTs and the native AMM

BLOCK-20 is Blockle's fungible-token standard; **BLOCK-721** is its NFT standard. Both are first-class consensus objects, not smart-contract conventions.

A **constant-product automated market maker** is built directly into consensus. Any BLOCK-20 token can seed a BLOCK-paired liquidity pool; swaps pay a **0.30%** fee to liquidity providers, and newly created positions carry a one-week LP lock. The AMM is fully **non-custodial**: trades are signed on the user's device and settle on-chain; Blockle never takes custody of trader funds or liquidity.

6. Shielded transfers

Blockle supports optional **hidden-amount** transfers. Value is committed inside zero-knowledge notes over a binary extension field, hashed with Rescue-Prime and proven with STARKs, so transferred amounts never appear on chain while remaining fully verifiable by every node. Users choose transparency per transaction.

7. Blockle Intelligence

Blockle Intelligence is a consensus-level market for AI inference, activated at a fixed block height. A fraction of each block's subsidy (configurable; currently 10%) is redirected from the proof-of-work coinbase into an **emission pool** — the total supply schedule is unchanged; this only re-targets part of each block's existing subsidy.

Participants register as **neurons** in task markets (**subnets**): miners serve inference, validators score it through a commit–reveal weight scheme and must prove liveness each epoch against a fresh on-chain beacon. Each epoch the pool is distributed to miners and validators by on-chain consensus over the revealed scores. Registration locks a BLOCK **bond** (recoverable by deregistering after a cooldown), aligning incentives and deterring sybil behavior. Inference is also purchasable per call — in BLOCK via the BLOCK-402 scripting standard, or in stablecoins via the x402 rail.

8. Wallets and interoperability

Blockle ships a browser extension, a desktop (Qt) wallet and a mobile wallet, each holding BLOCK and BLOCK-20/721 assets under post-quantum keys. From the same seed the wallet deterministically derives addresses on external chains (Bitcoin, Ethereum and EVM networks, Solana, Litecoin, Dogecoin) for a single-seed multi-chain experience; those external keys use each chain's native (classical) cryptography and never touch Blockle consensus. A wrapped-BLOCK bridge to external chains is specified and gated behind the applicable licensing.

9. Security and honesty principles

- **Post-quantum by default** — no consensus signature relies on classical ECC.
- **Height-activated upgrades** — protocol changes activate at published block heights, so every node upgrades in lockstep and old nodes fork off cleanly rather than silently diverging.
- **Non-custodial where it counts** — the wallet and the native AMM never take custody; keys are generated and sealed on the user's device.
- **No fabricated metrics** — displayed statistics come from live nodes; third-party or operator-reported figures are labeled as such.

© AlienBeing LLC. BLOCK and Blockle are products of AlienBeing LLC. This document is technical documentation describing the Blockle protocol as implemented. It is not investment advice and not an offer or solicitation. Protocol parameters cited (block time, halving interval, premine, AMM fee, intelligence α-split, activation heights) reflect the live mainnet configuration and may be changed only by published, height-activated consensus upgrades. blockle.org