A protocol built on evidence

Abstract

Project Boreal is a proposed independent proof-of-work payment blockchain. Its research goals are GPU-accessible mining, post-quantum transaction authorization and transparent supply rules. This document is a draft architecture, not an implemented or audited protocol. The working name and ticker are not cleared. No live network, asset sale, exchange listing or investment return exists.

The proposition

Use established cryptography for security; compete through measurable accessibility, maintainability and clear economics. NVIDIA is the first software target. Independent AMD implementations should be possible. Restricting the software vendor would concentrate participation without proving what hardware generated a share.

What exists today

A private concept website, this draft, proposed supply/accounting functions, original CUDA SHA-256 nonce-scanner source, an independent Python verifier and CPU reference tests. The scanner is a conventional baseline only. It is not the proposed final mining algorithm and does not connect to a chain or pool.

What remains unproven

There is no demonstrated advantage over existing projects, no cryptographic novelty claim, no measured GPU advantage, no ASIC-resistance evidence and no network-security result. A live cryptocurrency requires a substantial implementation, testing and independent review program.

Security starts with signatures

Transaction authorization

Propose ML-DSA-65 from NIST FIPS 204 through a maintained, reviewed implementation. Do not implement the signature primitive from scratch. Every signing message must bind network identifier, transaction version, all inputs and outputs, fee commitments, expiry policy if used and the signing context, with canonical byte serialization. Detailed wire formats and test vectors are required before interoperability.

Account and key design

Propose a UTXO ledger and versioned output types with a 512-bit hash commitment to the required public key and spending conditions. Keys and signatures are revealed when spending. Outputs must not offer a weaker legacy-signature bypass. Transaction IDs, Merkle commitments and proof-of-work hashing require separate specifications; a long digest alone is not a security proof.

Migration and recovery

Reserve explicit signature-scheme versioning. A future transition should require a reviewed consensus upgrade and a published migration window; there is no administrator key that can rewrite ownership. SLH-DSA is a possible future alternative, not an implemented fallback. Recovery and multisignature need independent designs; naive key or signature aggregation is not assumed.

Threat model

Post-quantum signatures address a particular attack surface. Compromised wallets, implementation bugs, key theft, network denial of service, majority hashpower, eclipse attacks, reorgs and quantum advantages against mining remain relevant. Larger keys/signatures affect bandwidth and validation. Key storage, entropy, replay separation and resource limits need testing. Describe the goal as post-quantum resistant, never absolutely quantum proof.

Mining for open participation

Research direction

Evaluate a memory-bandwidth-oriented workload with predictable VRAM use, integer operations, deterministic epoch data and no model downloads or floating-point dependence. An initial research target is compatibility with 8 GB GPUs; no dataset size or algorithm is locked. Benchmark at multiple memory sizes and compute intensities before selecting a candidate.

Why GPU only is not enforceable here

A valid computational result does not prove the model of device that generated it. CPUs, FPGAs and ASICs may compute the same function. Device attestation would add vendors and trust assumptions. Ethash is a useful caution: a memory-hard design intended to resist ASICs still acquired ASIC implementations. The credible objective is a measured GPU economic advantage, with uncertainty disclosed.

Verifier cost is a selection gate

Nodes must cheaply check submitted work without allocating the same large scratchpad for every malicious candidate. Measure verification time, memory, invalid-work rejection and worst-case peer load. Reject candidates with impractical verification, exploitable shortcuts, large time-memory tradeoffs or excessive consensus complexity. No invented "useful AI work" security claim is included.

Delivered NVIDIA baseline

The experimental CUDA scanner computes SHA-256(header32 || nonce_le64), checks a 1..32 leading-zero-bit target and reports the smallest valid nonce in a bounded batch. Python hashlib verifies a reported nonce independently. SHA-256 is deliberately a standard baseline and is ASIC-friendly. CPU tests exercise the shared hash function, not CUDA execution. No GPU hashrate, power draw or compatibility result is claimed.

Benchmark protocol

Test NVIDIA 5090 plus another architecture, an AMD GPU, a modern CPU and an explicit FPGA/ASIC cost model. Record source revision, driver/toolkit, power limit, measured wall power, kernel and end-to-end rates, thermal conditions, invalid shares and verification cost. Publish commands and raw results. Prevent pooled job reuse and stale work before a real mining release.

Supply: explicit, bounded, conditional

Proposed parameters

No premine, no founder allocation and no protocol developer tax are proposed. Block target: 60 seconds. One coin: 100,000,000 atoms. Reward at height h: floor(1,000,000,000 / 2^floor(h / 1,050,000)) atoms. Height zero is the first reward-bearing block in this proposal; any genesis container must be unspendable and non-issuing. These choices remain subject to founder review and modelling.

Maximum issuance

The headline ceiling is 21,000,000 coins. Integer truncation makes the actual schedule total 20,999,999.86350000 coins before burns. Halvings occur roughly every 1.997 years if the block target holds. Rewards become zero at epoch 30, roughly 60 years after launch at target speed. Time is illustrative; rewards are height based.

Fee burning

For each transaction fee f in atoms: burn floor(f / 4); pay f - floor(f / 4) to the miner. The rule removes burned atoms from spendable supply; it does not credit a secret or inaccessible address. For a valid block, coinbase may create no more than the subsidy plus miner fee portions. All arithmetic must be integer, bounded and checked. Tiny fees can round down to zero burn.

When is supply deflationary?

Change in outstanding protocol supply = new subsidy - fee burn. Supply declines only when burns exceed issuance. At the first reward rate, deflation needs more than 10 coins burned per block, equivalent to more than 40 coins in total fees when fees divide evenly by four. There is no immediate deflation guarantee. Lost keys do not count as protocol burns. A falling inflation rate is disinflation, not supply contraction.

Security budget and funding

Burning fees reduces miner revenue, and declining rewards increase reliance on transaction demand. Model low-fee and low-price periods, hash rental attacks and subsidy exhaustion. Sustained mining and unconditional early deflation can conflict. Founder funding and grants are possibilities; no committed funding exists. Any later treasury or allocation requires explicit disclosure and revised economics.

Consensus and delivery gates

Node architecture to build

A complete node needs deterministic parsing, transaction and script validation, bounded mempool, UTXO storage, block storage, coinbase maturity, timestamps, difficulty adjustment, peer discovery, chainwork fork choice and reorg handling. None is supplied in this starter. Select a mature permissively licensed base after assessing its cryptographic assumptions; a superficial Bitcoin fork is insufficient.

Consensus choices still open

Select and simulate difficulty adjustment under variable hashpower, define block-weight and signature-verification limits, bound timestamps and reorg work, choose coinbase maturity and deployment rules. A candidate 60-second block target must survive measured propagation tests. Do not advertise throughput, confirmations or finality before these experiments. Smart contracts, bridges and privacy systems are outside the initial payment-chain scope.

Gate 1 - reproducible research

Freeze a byte-level PoW candidate only after CPU/GPU vectors agree, verification costs are bounded, attack analysis is published and independent reviewers can reproduce claims. A candidate failing these tests must be redesigned or replaced, not marketed as finished.

Gate 2 - valueless testnet

Integrate node, wallet, NVIDIA miner and pool job protocol; add address checksums, network separation, reproducible builds, release signatures and update verification. Exercise partitions, reorgs, invalid signatures, coinbase inflation attempts, malformed blocks, equivocation and peer resource attacks. Testnet balances carry no promised mainnet conversion.

Gate 3 - launch decision

Commission independent cryptographic and consensus reviews, resolve critical findings, publish known risks and establish incident response. Decide fair-launch notice, seed-node operators, reproducible genesis and how development is funded. Mainnet launch, paid promotion and any asset sale require a separate decision based on the completed software and applicable professional advice. No dates or cost guarantees are set.

Positioning, evidence and sources

A distinctive project needs evidence

ML-DSA, fee burning and GPU-oriented mining are not unique individually. The research contribution should be a measured and reproducible balance of GPU economics, cheap verification and a maintainable post-quantum wallet. A competitor review and patent/name checks are still pending. "More advanced than all others" is not a defensible claim at this stage.

Launch copy - draft only

Project Boreal is researching GPU-favouring proof of work and post-quantum transaction signatures. Explore the draft design and experimental NVIDIA baseline. Research prototype. No live coin. No token sale. No investment returns promised.

Verification completed

The C++ host execution of the shared SHA-256 function matched Python hashlib for 66 deterministic input/nonce vectors. Unit checks also covered valid and invalid shares, no-solution reporting, halving boundaries, maximum issuance and fee conservation. CUDA compilation, GPU execution, blockchain consensus, signature integration, networking and security audit were not performed.

Primary technical references

[1] NIST FIPS 204, Module-Lattice-Based Digital Signature Standard (2024; current errata should be checked before integration). https://csrc.nist.gov/pubs/fips/204/final
[2] NIST FIPS 205, Stateless Hash-Based Digital Signature Standard (2024). https://csrc.nist.gov/pubs/fips/205/final
[3] Ethereum documentation, Ethash (historical). Documents the memory-hard design and later ASIC development. https://ethereum.org/developers/docs/consensus-mechanisms/pow/mining/mining-algorithms/ethash/
Sources consulted 8 November 2026. These standards and histories do not endorse or validate Project Boreal.

Status

Whitepaper v0.1 / 8 November 2026. Proposal and research starter only. All parameters may change before any testnet. No funds, keys or deposits should be entrusted to this software.