# KELYRIUM

## NETWORK WHITE PAPER

Technical architecture and economic specification · V1.3

CO-FOUNDERS

**Abraham Gómez**

**Gerardo Gómez**

23 October 2026

Kelyrium.org • Kelyrium.com

VERSION 1.3 | TECHNICAL DESIGN DRAFT

One chain. Twenty-five native assets. Open participation. Updated technical draft | 23 October 2026

Kelyrium.org • Kelyrium.com

## Abstract

Kelyrium is a proposed independent, open-source Layer 1 proof-of-work network built as an original Rust implementation, not a repackaged Bitcoin Core fork. A single consensus history supports KELY, the network currency, and 24 separately capped native Bitcoin World assets. Under the revised reward design, one valid mined block issues a deterministic reward allocation for all 25 native assets.

The protocol aims to combine permissionless CPU/GPU mining, locally controlled wallets, asset-to-asset settlement, deterministic EVM smart contracts, fungible user-created tokens, NFTs, and optional privacy capabilities. Seed services help participants find peers but have no privileged authority over balances or consensus.

This white paper sets out the current intended architecture. Features described as planned or candidates are not represented as deployed or security-audited. Mainnet parameters, security proofs and operational readiness must be established through reproducible experiments and independent review.

## 1. Scope and specification status

This V1.3 publication defines the initial 25-asset network design, monetary parameters, security requirements and engineering validation gates. The network is a proposed independent Layer 1; features described as planned are not claims of completed deployment or audit.

A 30-second target and the related subsidy/halving recalibration are the current protocol design direction, not a claim of demonstrated production performance. A 120-block coinbase maturity was recommended and remains provisional. Where precise wire formats, fee coefficients, hash algorithms or proof systems are unresolved, the implementer must not invent consensus values without review.

Kelyrium’s 25 protocol-native assets must not be confused with unlimited potential contract-created tokens. The latter follow their own contract rules and cannot alter the native monetary registry.

- Consensus: Independent PoW L1; CPU/GPU dual-track work under review
- Block interval: 30 seconds desired; world-scale benchmark pending
- Native assets: 25: KELY + 24 Bitcoin World
- Precision: 12 decimals per native asset; checked u128 storage
- KELY cap: 21,000,000 coins, including vested 630,000 genesis
- Initial KELY subsidy: 2.425 / 30-second block, proposed revised schedule
- Halving: 4,200,000 blocks (~4 years target), exact cap vectors pending
- Coinbase maturity: 120 blocks proposed; not final
- Baseline block-byte budget: 192,000 bytes; rebenchmark required
- Contracts: Deterministic EVM; ERC-20 / ERC-721 / ERC-1155 planned
- Privacy: Privacy-conscious wallet; future optional audited shielding

- Gas: KELY baseline; sponsored fee abstraction proposed
- Upgrades: Public KIPs, versioned activation; no admin override
- Mainnet gate: Public testnet ≥90 days; final ≥30 stable; independent review

## 2. One blockchain, independent validation

Kelyrium is one peer-to-peer ledger and one history of global blocks, rather than 25 independently mined chains. Full nodes independently verify proof of work, native asset conservation, spend authorization, coinbase issuance, contract-state transitions and block commitments. No DNS seed, bootstrap node, pool, wallet server or explorer has special authority to rewrite the ledger.

The desired aggregate block interval is approximately 30 seconds. Candidate serialized block budget from the original design is 192,000 bytes, including signatures and proofs; byte weight, computational gas and permanent storage also need explicit bounded budgets. Measured propagation, competing-block frequency, reorganization risk, CPU/GPU difficulty behavior and full-node cost determine the final safe operating point.

Peer discovery should work through multiple independent DNS/bootstrap sources, cached peers and user-specified nodes. The ecosystem should become less dependent on project-operated infrastructure as geographically diverse independently operated full nodes and miners join.

## 3. Initial V1.3 registry and monetary policy

The table below defines the complete initial registry. Each asset has an explicit country or region, currency inspiration, immutable maximum supply and candidate first-epoch reward. All 25 entries belong to one blockchain. The currency-themed names do not imply fiat pegs or redemption rights.

| Country / Region | Currency | Asset | Maximum supply | Initial reward |
|---|---|---|---|---|
| Global / Kelyrium Network | Kelyrium | KELY | 21,000,000 | 2.425 |
| United States | US Dollar | BTC-USD | 210,000,000 | 25 |
| Eurozone | Euro | BTC-EURO | 189,000,000 | 22.5 |
| Japan | Japanese Yen | BTC-YEN | 2,100,000,000 | 250 |
| China | Chinese Yuan | BTC-YUAN | 630,000,000 | 75 |
| United Kingdom | British Pound | BTC-POUND | 105,000,000 | 12.5 |
| Vietnam | Vietnamese Đồng | BTC-VND | 21,000,000,000 | 2500 |
| Mexico | Mexican Peso | BTC-PESOM | 420,000,000 | 50 |
| Thailand | Thai Baht | BTC-BAHT | 840,000,000 | 100 |
| India | Indian Rupee | BTC-RUPEE | 1,050,000,000 | 125 |
| South Korea | South Korean Won | BTC-WON | 4,200,000,000 | 500 |
| Russia | Russian Ruble | BTC-RUBLE | 1,260,000,000 | 150 |
| Switzerland | Swiss Franc | BTC-FRANC | 84,000,000 | 10 |
| Turkey | Turkish Lira | BTC-LIRA | 1,680,000,000 | 200 |
| Brazil | Brazilian Real | BTC-REAL | 315,000,000 | 37.5 |
| Saudi Arabia | Saudi Riyal | BTC-RIYAL | 168,000,000 | 20 |

| Country / Region | Currency | Asset | Maximum supply | Initial reward |
|---|---|---|---|---|
| United Arab Emirates | UAE Dirham | BTC-DIRHAM | 147,000,000 | 17.5 |
| Taiwan | New Taiwan Dollar | BTC-TWD | 1,344,000,000 | 160 |
| Poland | Polish Złoty | BTC-ZLOTY | 378,000,000 | 45 |
| Hong Kong | Hong Kong Dollar | BTC-HKD | 336,000,000 | 40 |
| Indonesia | Indonesian Rupiah | BTC-RUPIAH | 10,500,000,000 | 1250 |
| Philippines | Philippine Peso | BTC-PESOP | 735,000,000 | 87.5 |
| Canada | Canadian Dollar | BTC-CAD | 231,000,000 | 27.5 |
| Australia | Australian Dollar | BTC-AUD | 294,000,000 | 35 |
| Singapore | Singapore Dollar | BTC-SGD | 126,000,000 | 15 |

The 30-second target block interval, 4,200,000-block halving epoch and 25-asset reward vector are design parameters. Exact integer subsidy schedules must be validated against each supply ceiling before mainnet.

## 4. Issuance, genesis and miner rewards

Each valid block includes the deterministic reward basket for KELY and all 24 regional assets. Miners and pools cannot substitute or omit rewards.

The 30-second target block interval, 4,200,000-block halving epoch and 25-asset reward vector are design parameters. Exact integer subsidy schedules must be validated against each supply ceiling before mainnet. The first-epoch KELY reward candidate is 2.425 KELY per valid block; exact lifetime totals and reward rounding require consensus test vectors.

The original disclosed KELY genesis allocation remains 630,000 KELY (3% of the 21-million cap), comprising 210,000 KELY for the founder and 420,000 KELY for operations, across 75 vesting-tracked outputs. Founder vesting provides 21,000 KELY at initial eligibility, 31,500 at month 12 and 36 monthly installments of 4,375 in months 13–48. Operations has 63,000 initially and 36 exact integer-rounded installments totaling 357,000 during months 1–36. All allocations are inside the cap and subject to their predetermined signature/time restrictions.

Zero secondary-asset genesis balances are planned. The proposed new reward basket must be checked independently against each asset’s immutable supply cap. Integer rounding, residual base units, coinbase commitments, unlock conditions and deep-reorg behavior remain subject to exact consensus definitions. Coinbase maturity of 120 blocks (~60 minutes at 30-second target) is a candidate, not yet a frozen rule.

## 5. Proof of work and mining pools

The mining design retains two CPU and GPU proof-of-work tracks competing to extend one global chain, each with independent difficulty accounting and a formally defined cumulative-work comparison. The original candidate evaluation used yespower for CPU and KawPow with Verthash comparison for GPU. None of those algorithms is guaranteed ASIC-proof, and algorithm/parameter choice remains an engineering and security-review decision.

Users should be able to solo mine or select independently operated pools inside the wallet. The directory should show fees, geographic region, latency, operator, share difficulty, payout model, maturity, threshold and performance. Low-hashrate workers contribute pool shares rather than requiring a solo block discovery. Pools may distribute earned portions of the 25-asset basket; optional conversion to one chosen payout asset is available only when independent liquidity and clear quotes exist.

Pool accounting must withstand manipulated shares, withholding, stale work, reorganization, reward maturity and concentrated pool ownership. Permissionless or P2Pool-like arrangements are research goals. More nominal hashrate is not enough: independent node count, miner diversity and pool concentration are essential security metrics.

## 6. Native ledger and self-custody

The baseline ledger is a versioned multi-asset UTXO model with per-asset balance conservation. Ordinary payments use authenticated input ownership and explicit outputs; candidate scripts include single-key and threshold authorization, lock conditions, expirations and reviewed Schnorr cryptography. Signatures bind the chain domain, asset identifiers, amounts, recipient conditions and transaction context.

Consensus must reject double spends, repeated inputs, invalid coinbase rewards, noncanonical encodings, overflow and underflow. Reorganizations atomically roll back UTXO, issuance and smart-contract state. The precise format for efficiently distributing 25 rewards in every block requires a canonical design: 25 distinct UTXOs per block could create approximately 26.28 million reward UTXOs yearly at a 30-second interval, before those outputs are spent.

Wallets can manage multiple independent identities, recovery phrases and fresh receiving addresses. Each wallet may hold all 25 native assets; there is no need for 25 separate chains or wallet installations. Address separation alone does not guarantee anonymity.

## 7. Low fees, resource pricing and gas sponsorship

KELY is the protocol’s principal settlement asset for network fees, and the baseline directs transaction fees to the winning miner without a mandated burn. The project aims for extremely low costs for ordinary native transfers, but no fixed lifetime fee or guaranteed number of transactions per KELY is asserted. Fees must reflect scarce resources and market conditions.

Transfers should avoid unnecessary EVM computation. Contract execution, durable storage writes, new UTXOs, signatures, network bytes and optional privacy-proof verification must be metered separately with deterministic rules and bounded block budgets. Congestion adjustment and minimum economic fees should raise the cost of saturating limited capacity while keeping ordinary use affordable when demand is low.

A KELY-empty wallet can potentially transact through an authorized fee sponsor paying KELY and receiving a separately agreed reimbursement in another supported asset. Such sponsorship requires authenticated quotas, expiration, atomic settlement, rate limits and clear quotes. Direct consensus recognition of non-KELY gas remains a distinct unapproved design decision.

## 8. Smart contracts, tokens and NFTs

Kelyrium plans a deterministic EVM-compatible execution environment on the same Layer 1. Solidity and compatible tooling can be used where node RPC, state commitments, receipts, gas accounting and reorganization-safe contract execution have actually been implemented. ERC-20-compatible fungible token creation is an explicit launch goal; ERC-721 and ERC-1155 support are included for NFTs and other collectibles.

Permissionless contract tokens are not added to the native 25-asset consensus list. Their supplies, mint/burn permissions, decimals and upgrade privileges derive from published contract rules. Immutable contracts and explicitly upgradeable proxy designs may coexist; wallet and explorer interfaces should warn about upgrade controllers, token allowances and unverifiable code.

The UTXO-to-EVM accounting boundary requires exact 12-decimal-to-EVM denomination conversions, gas prepayment/refunds, atomic settlement, bounded state writes and deterministic reversion behavior. Contracts may not create native KELY or Bitcoin World supply outside the PoW schedule. A token-launch interface and NFT market are application features; neither guarantees asset safety, price or liquidity.

## 9. Native exchange, fiat access and interoperability

The intended decentralized exchange uses signed, self-custodial peer-to-peer orders with atomic native-asset settlement, cancellation, expiry, safe input reservations and replay protection. All 25 native assets share one chain, so swaps among them require no external bridge. Efficient routing through KELY may be used where liquidity, price limits and safe atomic execution permit it.

A new user can generate an address and receive funds without mining. Mining is optional; users may receive assets, acquire them from holders, or buy on an external exchange if listed. A wallet-integrated fiat buy flow requires an independently supported payment partner, identity/compliance controls where applicable, genuine market supply and liquidity. It cannot automatically convert national fiat to a newly invented native asset.

The wallet is planned to support modular Bitcoin, EVM and Solana network adapters over time. Displaying or signing for external chains is different from safely bridging asset value between chains. Cross-chain bridges require distinct trust models and independent audits and are not implicit launch features.

## 10. Public verifiability and staged optional privacy

Kelyrium’s privacy direction is privacy-conscious by default, with an optional future Zcash-like shielded transfer mode and an explicit transparent/public mode. Early wallet protections include local key custody, encrypted backups, coin control, address rotation, minimal telemetry and optional privacy-preserving transports such as Tor or I2P. Those measures do not cryptographically conceal public amounts or counterparties.

True optional shielding must protect appropriate transaction details while allowing every validating node to verify conservation and capped issuance for each native asset. Candidate work includes commitments, nullifiers, zero-knowledge balance proofs, viewing/disclosure keys, proof metering and safe recovery. The exact proving system, supported asset operations, wallet scan model and rollout schedule are unselected and require specialized audits.

Ordinary EVM activity, transparent asset swaps, reward outputs and movements between shielded and transparent domains can reveal metadata. The wallet must communicate these limits. The public block explorer should expose global consensus data, per-asset circulating issuance, transaction commitments and visible contract details without promising to reveal information that a future cryptographic shield properly hides. No custodial mixer or privileged chain-freezing key is part of the core architecture.

## 11. Security, anti-spam and operational resilience

Consensus defenses: bounded, canonical block and transaction formats; per-asset invariants; checked monetary arithmetic; signature and proof domain separation; block-wide compute/storage ceilings; deterministic gas; coinbase maturity; and fully reversible execution during reorganizations.

Economic defenses: nonzero resource-weighted fees, demand-sensitive pricing, UTXO creation economics, anti-dust policy and durable-state charges. Spam models must account for attackers submitting millions of cheap transfers, hoarding UTXOs, forcing contract storage growth or manipulating congestion. Local mempool relay rules must be distinguished from validity rules accepted by consensus.

P2P and RPC defenses: independently bounded bytes, CPU, memory, connection counts, in-flight requests, queue depth, message size and expensive historical queries; inexpensive rejection of malformed traffic before expensive cryptography; multiple discovery mechanisms and tested eclipse/Sybil resistance. Peer mitigation must avoid systematically excluding honest users on shared networks.

Application-layer defenses: safe wallet signing and phishing warnings; simulated contract interactions; disclosure of upgradeable contract authorities; sponsor quotas and signature authorization; validated pool shares and transparent payout accounting; isolated external-chain adapters; audited zero-knowledge verification budgets. No protection prevents all future vulnerabilities; deployments require fuzzing, simulations, reproducible builds, independent audits, security disclosure and incident-response procedures.

## 12. Upgrades, compatibility and governance

Consensus and network components have explicit versions. Proposed changes proceed through public Kelyrium Improvement Proposals (KIPs), reference specifications, test vectors, independent review, testnet activation and publicly communicated release windows. Protocol capability negotiation may select compatible networking features but may not allow peers to invent different active consensus validity rules.

Wallet applications, indexers, mining clients and network adapters may update independently when compatible. On-chain application developers may choose immutable contracts or transparent proxies with disclosed upgrade rights, multisignature controls and timelocks. Neither wallet updates nor contract upgrade administrators can change the native monetary caps or arbitrarily confiscate user assets.

Consensus upgrades must clearly identify compatibility, activation height, potential chain split, rollback/recovery arrangements and multi-party release procedures. Project-operated seed servers do not vote as network administrators.

## 13. Implementation path and mainnet criteria

Phase A — specification and accounting: reconcile original economic schedules, source code and the approved 12-decimal amendment; define canonical asset IDs, genesis and vesting, reward vector, block/transaction formats, fee units and full cross-language test vectors.

Phase B — consensus prototypes: benchmark CPU/GPU mining and difficulty recovery, multi-asset UTXO accounting, deterministic EVM execution, 25-reward serialization, supply invariants, chain reorganizations and sustainable full-node performance at 30-second and 60-second alternatives.

Phase C — user software: deliver Windows/Linux wallet and Ubuntu headless CLI nodes, independent pool integration, a verifiable explorer, signed-order exchange, native asset transfers, contract token deployment and NFT behavior. Advanced shielding, fiat providers and external-chain bridges may require separate gated phases.

Phase D — open testnet and independent review: publish reproducible source, run at least 90 days of public testnet, require the final 30 days to be stable, evaluate adversarial attacks and have independent reviewers verify consensus, cryptography, monetary issuance, EVM behavior and remediation. Launch mainnet only after documented acceptance; no date or price is guaranteed.

## 14. Limitations and research agenda

The largest technical risks remain secure dual-algorithm cumulative-work rules, reward-basket/UTXO state growth, precise UTXO/EVM integration, contract gas and persistent-state economics, strong optional shielded proofs, wallet recovery, mining pool trust and external interoperability. Thirty-second blocks and low fees create measurable tradeoffs rather than automatic scalability.

The original disposable Rust experiment validated issuance and vesting arithmetic with 11 cross-platform tests; it did not establish finished cryptography, secure networking, EVM conformance, shielded transfers, miner profitability, audited wallet behavior or mainnet readiness. Future claims should refer to verifiable implementation evidence rather than design intent.

## References and document lineage

Kelyrium Network, White Paper 1.0 Draft (15 September 2026); Kelyrium Consolidated Architecture & Design Decision Record V1.2 (23 October 2026); Kelyrium Master Implementation Prompt for Claude/Astra/Codex V1.2 (23 October 2026).

Public technical precedents: Bitcoin: A Peer-to-Peer Electronic Cash System; Ethereum gas and EVM documentation; ERC-20, ERC-721 and ERC-1155 specifications; established peer-to-peer mining and wallet security research. These references are design context, not claims of affiliation.

## Copyright and authorship

Copyright © 2026 Abraham Gómez and Gerardo Gómez. All rights reserved.
Kelyrium Network White Paper, updated technical draft dated 23 October 2026.

This document is provided for technical review and discussion. Permission to quote or share this white paper with attribution does not confer a license to use Kelyrium trademarks, artwork or other separately protected materials. Open-source software components, when released, will be governed by their respective published licenses.