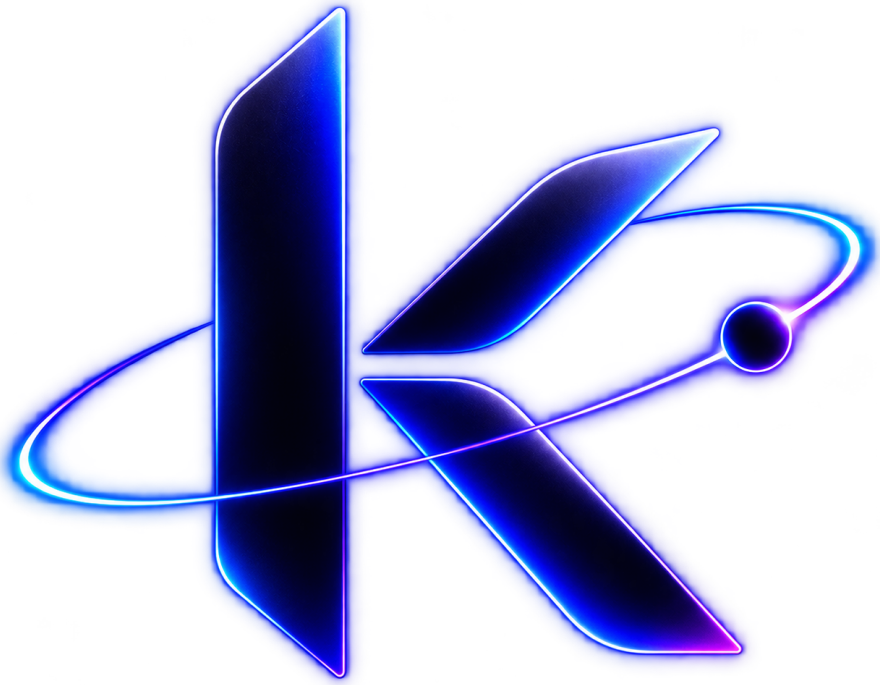

KELYRIUM

White Paper

One chain. A world of assets.

VERSION 1.0 / DRAFT 15 September 2026

KELY / Primary and gas asset Bitcoin World / 24 native assets

Abstract

Kelyrium is a proposed peer-to-peer proof-of-work network built around one independent Layer 1 blockchain. Its primary asset, KELY, has a nominal maximum supply of 21,000,000 coins. At genesis, the chain also defines Bitcoin World: 24 native BTC-* assets with distinct supply caps, shared validation, and no default promise of fiat backing or redemption.

Kelyrium is designed to bring payments, multi-asset ownership, permissionless mining, a self-custodial exchange, smart contracts and NFTs into one verifiable network. The project is being developed as a new Rust codebase that reuses audited cryptographic primitives. The design is deliberately published as a draft: several consensus-critical details still require exact specifications, cross-platform tests, adversarial evidence and independent review before mainnet.

1. The proposition

Most crypto products divide the experience between a base chain, a wallet, a mining client, a separate exchange, and application networks. Kelyrium proposes a unified path: run a node, validate the history, mine one of the network's reward paths, hold native assets, trade them directly, and use contracts or NFTs without custodial bridges.

The core proposition is narrow and testable: one peer-to-peer chain, a family of native assets, and a transparent path from local validation to application use. Kelyrium does not promise investment returns, stable prices, ASIC immunity, guaranteed liquidity or a mainnet date.

2. Network model

Kelyrium is a single proof-of-work blockchain. Full nodes independently validate blocks, transactions, asset conservation, contract execution and state commitments. Bootstrap seeds and DNS records are discovery aids; they do not have authority over balances or chain choice.

The target aggregate block rhythm is approximately 60 seconds. The current serialized block budget is 192,000 bytes, including proofs and signatures. These numbers are planning inputs and remain subject to implementation evidence, resource measurements and final consensus specification.

The protocol uses integer monetary accounting: 8 decimal places for KELY and every Bitcoin World asset, u64 stored amounts and checked u128 intermediates. Floating-point arithmetic is excluded from consensus. Native addresses are planned to use versioned Bech32m forms. Exact transaction and wire encodings remain open engineering work.

3. Bitcoin World

Bitcoin World is the collective name for 24 native assets defined by the Kelyrium blockchain. Each asset has a fixed protocol identifier and a distinct maximum supply. The names reference world currencies and regions as branding metadata; they are not ISO-issued currencies, claims on governments, or stablecoins by default.

The accepted registry includes BTC-USD, BTC-EURO, BTC-YEN, BTC-YUAN, BTC-POUND, BTC-VND, BTC-PESOM, BTC-BAHT, BTC-RUPEE, BTC-WON, BTC-RUBLE, BTC-FRANC, BTC-LIRA, BTC-REAL, BTC-RAND, BTC-DIRHAM, BTC-KRONA, BTC-KRONE, BTC-RINGGIT, BTC-RUPIAH, BTC-PESOP, BTC-CAD, BTC-AUD and BTC-SGD. All 24 definitions exist at genesis; all are eligible for ordinary block-one selection under the accepted design.

Secondary supply is accrued per global block and may be claimed by a selected reward asset within published limits. Unclaimed allowance is retained; actual issuance is tracked permanently. Burns do not create new allowance, and the chain does not mint secondary assets through an administrator or an asset owner.

4. KELY monetary policy

KELY has a nominal cap of 21,000,000 whole coins, represented as 2,100,000,000,000,000 base units. Ordinary mining begins with a 4.85 KELY subsidy for the first 2,100,000 global blocks and halves by epoch. Integer halving leaves a calculated mining total of 20,369,999.769 KELY; with the premine, the planned issuance is 20,999,999.769 KELY, leaving 0.231 KELY below the nominal cap. There is no tail emission or catch-up subsidy in the accepted model.

Transaction fees are paid in KELY and go to the miner. No protocol fee burn or treasury diversion is currently selected. Fees and gas prices are consensus work items, not fixed dollar prices.

5. Disclosed premine and vesting

The design includes a 3% KELY genesis allocation: 630,000 KELY inside the cap. It is disclosed as 75 separately tracked allocation outputs. The founder allocation is 210,000 KELY and the operations allocation is 420,000 KELY.

The founder receives 21,000 KELY at the initial spend height, a 31,500 KELY cliff at calendar month 12, and 36 monthly installments of 4,375 KELY during months 13 through 48. Operations receives 63,000 KELY initially and 36 exact integer-rounded installments totaling 357,000 KELY during months 1 through 36. Thus 84,000 KELY is initially available; all remaining outputs are locked.

Unlocks use a reproducible UTC calendar anchor and the parent median clock, with the destination date clamped to the last valid day of its month. A parent median at or after the unlock timestamp is required, along with the relevant signatures. The schedule is not an administrator-controlled withdrawal key. Mainnet genesis keys, final serialization and custody procedures remain to be specified and reviewed.

6. Mining

Kelyrium aims to support both CPU and GPU miners. The selected direction is two independent difficulty tracks with a cumulative chain-work formula that accounts for the required target. Either class may find the next block; strict alternation is not used. If one class loses participation, the surviving class should preserve liveness at approximately its own track's interval. If both classes disappear, the network stops honestly.

The initial CPU evaluation uses yespower 1.0 with an 8 MiB parameter candidate. The initial GPU evaluation considers KawPow with Verthash as a comparator. These are evaluation candidates, not frozen production algorithms. Difficulty recovery, work normalization, proof domains, timestamp admission, parameters and licenses require a written experiment specification and adversarial testing.

Miners may select a secondary asset for a winning block while receiving the KELY subsidy and eligible fees. A block claims at most one selected secondary reward. Wallet scheduling and non-custodial P2P pooling are planned conveniences; they do not create guaranteed earnings.

7. Transactions and self-custody

The baseline ledger is a versioned multi-asset UTXO model with explicit per-asset conservation. Ordinary templates support single-key and threshold spends, Schnorr signatures from reviewed libraries, expiry and optional lock conditions. Signatures bind the network domain, transaction contents, asset identifiers, amounts, recipients, conditions and input positions. Duplicate inputs, noncanonical encodings, unknown templates and mutated signed fields must be rejected.

The built-in exchange is planned as a hybrid P2P signed-order system. Quotes are relayed without a central matching authority; settlement is atomic on chain. A sequential partial-fill baseline reserves inputs before a signature leaves the wallet, and a crash-safe wallet must retain pending order and signature state. There is no custodial operator balance or guaranteed liquidity.

8. Smart contracts and NFTs

Smart contracts and NFTs are required at initial mainnet launch. The selected direction is deterministic EVM execution integrated into the same Kelyrium Layer 1, with KELY as the gas asset. ERC-721 and ERC-1155 behavior is planned for the initial NFT surface: minting, ownership, transfers, balances and wallet/explorer visibility.

Remix can be used as a client through a future Ethereum-compatible JSON-RPC endpoint. It will compile Solidity, submit deployment and call transactions, and read contracts by address and ABI. Remix is not a privileged injector; the node must implement contract creation, execution, gas accounting, state roots, receipts and reorg-safe rollback before Remix interoperability is real.

The contract path must specify the relationship between UTXO and account state, atomic conservation, 8-decimal KELY and EVM denomination, gas prepayment, refunds, failed-call behavior, code and storage limits, concurrency, state growth and RPC bounds. NFT metadata is expected to be off-chain and bounded; availability and mutable content cannot be guaranteed by the chain. No contract may mint native KELY or Bitcoin World assets.

9. The Kelyrium wallet, exchange and app surfaces

The Kelyrium wallet is the primary user client, not a custodial account. It is planned as a desktop application for Windows and Linux with a matching headless CLI for Ubuntu nodes. The wallet creates and imports keys, derives fresh receiving addresses, displays spendable and locked balances for all 25 native assets, tracks confirmations, and exports encrypted backups. Private keys remain local; seed nodes, explorers and RPC endpoints are replaceable discovery and data conveniences.

The wallet home screen is designed around four actions: receive, send, mine and build. Send flow includes fee and gas estimation, coin and asset selection, change review, transaction simulation, expiry and explicit signing. A transaction activity view shows inputs, outputs, asset identifiers, lock state, confirmation depth and reorganization status. A recovery mode can restore a wallet from an approved seed backup without trusting a hosted service.

The exchange surface is a self-custodial P2P order book. A user creates a signed quote, chooses the asset pair and amount, and reserves the exact UTXOs before the signature is released. The wallet relays quotes, verifies counterparty signatures and settles accepted trades atomically on chain. There is no operator balance,

withdrawal queue or promise of liquidity. The planned marketplace uses the same signing and settlement path for NFT listings, offers and transfers, with creator royalties and metadata rules treated as explicit contract policy rather than hidden platform behavior.

Messaging is an optional privacy-aware peer channel attached to a wallet identity, with transport encryption, anti-spam limits and no custody of funds. Users can share quotes, contract addresses, NFT previews and payment requests, while the chain remains the source of truth for settlement. Full messaging and marketplace UX follows protocol validation; the launch requirement is that wallet signing, NFT ownership, transfer and explorer visibility are independently verifiable.

10. Privacy and user experience

The safer privacy direction includes coin control, fresh receiving addresses, Tor/I2P transport and relay privacy. Custodial mixers are not part of the core design. A desktop wallet/node is planned for Windows and Linux, with Ubuntu headless CLI nodes as the first integration target. Mobile and advanced privacy features follow later validation.

The wallet is intended to expose balances, node state, mining choice and schedule, transaction simulation, contract signing, NFT ownership and exchange reservations without hiding independent verification. Seed nodes, explorers and RPC services must be optional conveniences rather than trust anchors.

11. Launch and governance

Development is intended to move from private draft preparation to a public protocol and source repository before the counted public testnet. Releases should be reproducible, signed by multiple independent builders and approvers, and accompanied by security disclosures. Governance is public review and voluntary signaling; no hidden admin key or consensus backdoor is planned.

Mainnet requires at least a 90-day public testnet with a final 30-day stable period, including contract and NFT workloads, plus independent protocol/economic review, implementation audit and remediation verification. Multi-person release and treasury custody remain required even though the founder is currently the sole available signer. Founder-only testing cannot satisfy independent review or mainnet custody gates.

12. Current validation evidence

The first disposable Rust experiment, V0-E01, validates issuance and vesting arithmetic. It checks all accepted asset caps, integer halving totals, secondary allowance boundaries, the 75-output allocation schedule, calendar month clamping, lock eligibility, ordinary maturity, overflow rejection and synthetic branch replay. The same 11 tests pass in debug and release on Windows and Ubuntu 22.04 under WSL2.

This evidence does not establish secure cryptography, production serialization, node storage, EVM correctness, mining security, pool fairness, wallet recovery, throughput, launch readiness or a completed audit. Every remaining consensus area requires its own written experiment specification before implementation.

13. Roadmap

1. Complete cross-platform economic vectors and canonical transaction/genesis specifications.

2. Specify and validate UTXO signatures, block commitments and reorganization behavior.

3. Specify EVM revision, gas/resource model, state/receipt commitments and ERC-721/1155 conformance.

4. Complete dual-PoW work accounting and difficulty experiments on Windows and Linux hardware.

5. Build a local multi-node Ubuntu CLI network, then verify Windows compatibility.

6. Add wallet, scheduler, self-custodial DEX, P2P pool coordination and NFT UX.

7. Publish the coherent source, run the public testnet, complete independent review and decide mainnet readiness.

14. Risks and open work

The largest risks are the complexity of combining UTXO and account execution, deterministic EVM resource accounting, dual-algorithm chain work, state growth, pool coordination, wallet recovery and limited project resources. A compiled prototype does not resolve these risks. Parameters marked candidate or provisional remain open until evidence and review support them.

Kelyrium is a work in progress. This document describes the current design direction and accepted economic choices; it is not an offer, a promise of value, a guarantee of performance or a substitute for source review.

References

• Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

• Ethereum Foundation, *Gas and fees*, https://ethereum.org/developers/docs/gas/

• Ethereum Improvement Proposal 721, *Non-Fungible Token Standard*, https://eips.ethereum.org/EIPS/eip-721

• Ethereum Improvement Proposal 1155, *Multi Token Standard*, https://eips.ethereum.org/EIPS/eip-1155

• Remix documentation, *Deploy & Run*, https://remix-ide.readthedocs.io/en/latest/run.html

• Kelyrium project specifications: KELYRIUM-MASTER-SPEC.md, ARCHITECTURE.md, ASSET-SUPPLY-PROPOSAL.md, SECONDARY-PAYOUT-PROPOSAL.md, BLOCKER-RESOLUTION-PROPOSAL.md and VALIDATION-PHASE-PLAN.md