KELYRIUM

ネットワーク・ホワイトペーパー

技術アーキテクチャと経済仕様 · V1.3

共同創設者

Abraham Gómez
Gerardo Gómez

2026年10月23日

Kelyrium.org • Kelyrium.com

VERSION 1.3 | TECHNICAL DESIGN DRAFT

単一チェーン。25のネイティブ資産。許可不要の参加。

2026年10月23日 改訂技術草案

Kelyrium.org • Kelyrium.com

概要

Kelyriumは、Bitcoin Coreの名称変更やフォークではなく、Rustで独自に実装するオープンソースの独立したレイヤー1（L1）プルーフ・オブ・ワーク（PoW）ネットワーク構想である。単一のコンセンサス履歴が、基軸通貨KELYと、発行上限を個別に定めた24種類のBitcoin Worldネイティブ資産を支える。改訂された報酬設計では、有効なブロックの採掘ごとに25資産すべての決定論的な報酬を発行する。

本プロトコルは、許可不要のCPU/GPU採掘、利用者自身が管理するウォレット、資産間の決済、決定論的なEVMスマートコントラクト、利用者が作成する代替可能トークン、NFT、追加可能な任意のプライバシー機能を統合することを目指す。シードサービスはピア発見を助けるだけであり、残高やコンセンサスを変更する権限を持たない。

本書は現時点の設計を示す技術草案である。「計画」「候補」と表記した機能は実装済み・監査済みを意味しない。メインネットの最終パラメータと安全性は、再現可能な試験と独立した審査によって確認する。

1. 対象範囲と仕様の確定状況

本書V1.3は25資産ネットワークの初期設計、通貨パラメータ、セキュリティ要件および技術検証条件を定義する。独立したレイヤー1の設計文書であり、計画機能の実装・監査完了を保証しない。

目標ブロック時間は30秒であるが、本番環境での性能は未検証である。採掘報酬の成熟期間120ブロックは提案値であり確定値ではない。通信形式、手数料係数、ハッシュ方式、プライバシー証明など未確定の合意形成パラメータを、実装者が無断で決めてはならない。

25のプロトコル・ネイティブ資産と、スマートコントラクトで作成できる多数のトークンは区別される。契約トークンは独自のルールに従い、ネイティブ発行上限を変更できない。

- 合意形成：独立PoW L1（CPU/GPU二系統を審査中）
- 目標ブロック間隔：30秒（世界規模の性能検証待ち）
- ネイティブ資産：KELYと24種Bitcoin World、合計25種
- 精度：全資産12桁／検査付きu128保存
- KELY上限：21,000,000（ジェネシス630,000を含む）
- 初期補助金：30秒ブロックあたり2.425 KELY（提案）
- 半減期：4,200,000ブロック（約4年、厳密な総量検証待ち）
- Coinbase成熟期間：120ブロック案（未確定）
- 初期ブロック予算：192,000バイト（再測定が必要）
- 契約：決定論的EVM、ERC-20/721/1155を計画
- プライバシー：慎重な標準設定と将来の任意シールド
- Gas：KELY基本、スポンサー支払は提案段階
- 更新：公開KIPとバージョン化、管理者例外なし

- メインネット条件：90日以上の公開テストネット、最後30日安定・独立審査

2. 単一ブロックチェーンと独立検証

Kelyriumは25本の独立したチェーンではなく、1本のP2P台帳と単一のグローバルなブロック履歴からなる。フルノードはPoW、資産ごとの保存則、署名と所有権、報酬発行、契約状態遷移、ブロックのコミットメントを自ら検証する。DNSシード、ブートストラップノード、プール、ウォレットサーバー、エクスプローラーに台帳変更の特権はない。

30秒の目標ブロック間隔と、従来案である192,000バイトのブロック上限は、国際的な伝播遅延、競合ブロック、再編成、CPU/GPUの難易度調整、ストレージ・帯域・演算費用を測定して最終決定する。バイト数に加え、実行ガスと永続状態の増加量も制限する。

ピア発見には複数の独立DNSシード、既知ピア、利用者指定ノードを利用する。独立ノードと採掘者が増えるほど、プロジェクト運営の初期サーバーへの依存度を下げる。

3. V1.3 初期資産一覧と発行方針

以下の表は創世時点の全資産を定義する。各資産には対応する国・地域、参照通貨、供給上限、初期エポックの報酬案がある。25資産はすべて一つのブロックチェーン上で発行される。通貨名は法定通貨へのペッグや償還を意味しない。

国・地域	通貨	資産	最大供給量	初期報酬
グローバル／Kelyriumネットワーク	Kelyrium	KELY	21,000,000	2.425
米国	US Dollar	BTC-USD	210,000,000	25
ユーロ圏	Euro	BTC-EURO	189,000,000	22.5
日本	Japanese Yen	BTC-YEN	2,100,000,000	250
中国	Chinese Yuan	BTC-YUAN	630,000,000	75
英国	British Pound	BTC-POUND	105,000,000	12.5
ベトナム	Vietnamese Đồng	BTC-VND	21,000,000,000	2500
メキシコ	Mexican Peso	BTC-PESOM	420,000,000	50
タイ	Thai Baht	BTC-BAHT	840,000,000	100
インド	Indian Rupee	BTC-RUPEE	1,050,000,000	125
韓国	South Korean Won	BTC-WON	4,200,000,000	500
ロシア	Russian Ruble	BTC-RUBLE	1,260,000,000	150
スイス	Swiss Franc	BTC-FRANC	84,000,000	10
トルコ	Turkish Lira	BTC-LIRA	1,680,000,000	200
ブラジル	Brazilian Real	BTC-REAL	315,000,000	37.5
サウジアラビア	Saudi Riyal	BTC-RIYAL	168,000,000	20
アラブ首長国連邦	UAE Dirham	BTC-DIRHAM	147,000,000	17.5
台湾	New Taiwan Dollar	BTC-TWD	1,344,000,000	160
ポーランド	Polish Złoty	BTC-ZLOTY	378,000,000	45
香港	Hong Kong Dollar	BTC-HKD	336,000,000	40
インドネシア	Indonesian Rupiah	BTC-RUPIAH	10,500,000,000	1250

国・地域	通貨	資産	最大供給量	初期報酬
フィリピン	Philippine Peso	BTC-PESOP	735,000,000	87.5
カナダ	Canadian Dollar	BTC-CAD	231,000,000	27.5
オーストラリア	Australian Dollar	BTC-AUD	294,000,000	35
シンガポール	Singapore Dollar	BTC-SGD	126,000,000	15

目標ブロック時間30秒、半減期4,200,000ブロック、25資産同時報酬は設計上のパラメータである。メインネット開始前に供給上限を守る整数発行スケジュールを検証する必要がある。

4. 発行、ジェネシス、マイニング報酬

有効な各ブロックは、KELYと24のBitcoin World資産の計25資産からなる決定論的報酬セットを含む設計とする。従来の「採掘者が二次資産を1つ選ぶ方式」と、未請求枠を繰り越してまとめて受け取る仕組みは廃止する。発行額はプールや採掘者の好みではなく合意形成ルールが決める。

目標ブロック時間30秒、半減期4,200,000ブロック、25資産同時報酬は設計上のパラメータである。メインネット開始前に供給上限を守る整数発行スケジュールを検証する必要がある。

開示済みジェネシス割当630,000 KELYは上限21,000,000枚の3%であり、創設者向け210,000枚と運営向け420,000枚、計75のベスティング管理出力からなる。創設者分は初期条件で21,000枚、12か月目に31,500枚、13〜48か月目に4,375枚ずつ36回。運営分は初期63,000枚と1〜36か月に合計357,000枚の整数丸め配分である。いずれも上限内であり、所定の署名・時間条件に従う。

二次資産のジェネシス残高はゼロとする。各資産の発行上限、報酬シリアライズ、残余の最小単位、再編成、満期条件を厳格に検証する。120ブロック（30秒目標で約60分）のcoinbase成熟期間は未確定候補である。

5. プルーフ・オブ・ワークとマイニングプール

CPUとGPU用の2種類のPoWトラックが単一チェーンの次のブロックを競う構想である。難易度は別々に管理し、累積作業量を比較する方法を明文化する。旧評価案ではCPUにyespower、GPUにKawPowを使用しVerthashとも比較した。いずれもASIC耐性を保証しないため、最終アルゴリズムは安全性審査の対象となる。

利用者はソロ採掘または独立したプールをウォレット内から選択できる。プール一覧には手数料、地域、遅延、運営者、シェア難易度、支払方式、成熟時間、最低支払額、稼働状況を表示する。低ハッシュレートの参加者も有効シェアに応じて報酬を得られる。プールは25資産の報酬を分配し、流動性と正確な見積もりがある場合のみ任意で別資産に交換できる。

シェア偽造、ブロック隠し、古い作業、チェーン再編成、未成熟報酬、プール集中を評価する。P2Pool型の許可不要プールも研究課題とする。総ハッシュレートだけでなく独立ノード数と採掘者・プールの分散も重要である。

6. ネイティブ台帳と自己管理

基本台帳は、資産ごとの残高保存を行うバージョン付きマルチアセットUTXO方式である。通常の支払いでは入力の正当な支配者を署名で証明し、出力とその支出条件を明示する。単独署名、しきい値署名、ロック、期限、審査済みSchnorr方式などを検討する。署名にはチェーン識別子、資産ID、金額、受取条件、取引文脈を結び付ける。

二重支払い、入力の重複、違法な発行報酬、非正規エンコーディング、桁あふれ・負方向あふれを拒否する。再編成時にはUTXO、発行累計、EVM状態を原子的に巻き戻し、安全に再適用する。

ウォレットは独立した複数の識別子、リカバリーフレーズ、新しい受取アドレスを扱い、同じアプリで25資産を管理する。暗号化保存、バックアップ、署名前プレビュー、コインコントロールを重視する。アドレスを増やすだけでオンチェーン匿名性が保証されるわけではない。

7. 低手数料、資源価格、ガス代のスポンサー

KELYはネットワーク手数料の基本決済資産である。送金手数料は極力低く設計するが、ゼロコストで無制限に利用できるわけではない。手数料設計は攻撃者が大量の取引を送り付ける費用と、正当な利用者の費用のバランスを取る必要がある。

単純な資産送金に不要なEVM演算を要求しない。スマートコントラクトの演算、永続ストレージ、証明検証、UTXO生成、データ使用にはそれぞれ資源使用量に基づく料金を設定し、混雑時に調整する。バイト数、CPU、メモリ、ストレージ、状態の成長を独立して計測・制限する。

KELY残高がない利用者向けには、認証済みスポンサーがKELYで手数料を払い、利用者が別資産で償還する仕組みを検討する。期限、署名、利用上限、原子的な決済、レート制限、明示的見積もりが必須である。KELY以外をコンセンサスが直接gasとして受け入れる案は未承認の別仕様である。

8. スマートコントラクト、トークン、NFT

同じL1上に決定論的なEVM互換実行環境を予定する。RPC、状態コミットメント、レシート、ガス課金、再編成対応の実装が完了した範囲でSolidity等を使えるようにする。ERC-20互換の代替可能トークン作成をローンチ目標とし、NFT向けERC-721とERC-1155も対象とする。

コントラクトで作成されたトークンは25ネイティブ資産の登録簿には追加されない。発行・焼却権限、供給量、小数桁、アップグレード権限は公開された契約に従う。変更不能な契約と、権限を開示したプロキシによる更新可能契約を併存可能にする。ウォレットやエクスプローラーは危険な承認や管理者権限を警告する。

UTXOとEVMの境界には、12桁とEVM単位の厳密な整数換算、ガスの前払いと返金、原子的決済、状態書込み上限、決定論的な失敗時巻戻しが必要である。契約はPoWの発行スケジュールを超えてネイティブ資産を生成できない。NFT市場とトークン発行画面はアプリ機能であり、資産の価値や安全性を保証しない。

9. ネイティブ取引所、法定通貨、相互運用性

分散型取引所は、署名済みの自己管理P2P注文、期限、取消し、入力予約、リプレイ防止、原子的ネイティブ資産決済を基本とする。25資産は同じチェーン上にあるため、資産間スワップに外部ブリッジは不要である。流動性と価格制限が許す場合にKELYを中継した経路も利用できる。

新規利用者は採掘しなくてもアドレスを作り、資産を受け取れる。法定通貨で購入するには、上場市場・実際の流動性・外部支払事業者、および適用法に応じた本人確認・コンプライアンスが必要になる。名称だけで国の通貨とネイティブ資産を自動交換できるわけではない。

将来のウォレットにはBitcoin、EVM系、Solana用のモジュール式アダプターを想定する。外部チェーン残高の表示・署名と、チェーン間で安全に資産を移すことは異なる。ブリッジには別個の信頼モデルと独立監査が必要で、初期リリースの必須機能ではない。

10. 公開検証性と段階的な任意プライバシー

基本方針はプライバシーに配慮したウォレットを標準とし、将来はZcash型に似た任意の暗号学的シールド送金と明示的な公開・透明モードを用意することである。当初の対策には鍵のローカル保管、暗号化バックアップ、UTXOコントロール、アドレス更新、テレメトリー最小化、Tor/I2P等の任意の匿名化トランスポートを含める。これらだけで公開額や相手先が暗号学的に隠れるわけではない。

真のシールド方式では、各資産の発行上限と残高保存をすべてのノードが検証できるまま、必要な取引詳細を秘匿する。コミットメント、nullifier、ゼロ知識残高証明、閲覧鍵、証明検証コスト、鍵回復を研究する。証明系、資産ごとの対応範囲、ウォレット走査、導入時期は未確定で、専門監査が必要である。

公開EVM操作、透明スワップ、報酬出力、公開・シールド領域間の移動はメタデータを漏らし得る。ウォレットは制約を説明する。公開エクスプローラーはブロック、各資産の発行量、公開契約情報と必要なコミットメントを表示する。管理者が他人の資産を凍結する鍵や、保管型ミキサーを基本設計に含めない。

11. セキュリティ、スパム対策、運用耐性

コンセンサス層は、正規かつ有界なブロック・取引形式、資産保存則、チェック付き整数演算、署名・証明のドメイン分離、実行・ストレージ上限、決定論的gas、coinbase成熟、再編成時の完全な巻戻しを強制する。

経済的対策として、ゼロではない資源比例手数料、需要に応じた価格、UTXO生成の費用、dust防止方針、永続状態への課金を設ける。大量の安価な転送、UTXOの水増し、契約状態の無限増加、混雑操作を模擬試験する。ノードのローカルなメモリプール・中継ポリシーと全ノードが守るコンセンサスの有効性規則を分離する。

P2P/RPCでは受信バイト数、CPU、メモリ、接続数、処理待ち、要求キュー、メッセージ容量、高コストの履歴検索を個別に制限する。高価な暗号処理の前に不正形式を安価に拒否する。ピアの多様化とeclipse/Sybil攻撃耐性を検証し、共有回線の正当利用者を一律排除しない。

アプリ側では署名前確認、フィッシング警告、コントラクト呼出しシミュレーション、変更可能な管理権限の開示、スポンサーの署名・上限、プールのシェア検証、クロスチェーン機能の隔離、ゼロ知識証明処理の制限を行う。万能の防御は存在せず、ファジング、攻撃シミュレーション、再現可能ビルド、独立監査、脆弱性報告と事故対応が必要である。

12. アップグレード、互換性、ガバナンス

コンセンサスとネットワーク仕様には明確なバージョンを設ける。変更は公開Kelyrium Improvement Proposal（KIP）、参照仕様、テストベクトル、独立審査、テストネット導入、周知された更新期間を経て実施する。ピア同士が対応ネットワーク機能を交渉しても、現在有効なコンセンサス規則を勝手に変えてよいわけではない。

ウォレット、インデクサー、採掘ソフト、外部ネットワークアダプターは互換性を保ちつつ独立更新できる。スマートコントラクトは不変形式または権限を開示した更新可能プロキシを選べる。後者ではマルチシグとタイムロックを推奨する。ウォレット更新権限や契約管理者はネイティブ資産の上限変更や恣意的な資産没収をできない。

コンセンサス変更では互換性、発動高度、チェーン分岐リスク、巻戻し・復旧、多者によるリリース手順を明示する。シードサーバーはネットワークの管理者ではない。

13. 実装工程とメインネット基準

段階A：仕様・会計。既存の経済規則とソース、12桁改訂を照合し、資産ID、ジェネシス、ベスティング、報酬ベクトル、ブロック・取引形式、gas単位、言語横断テストベクトルを定義する。

段階B：コンセンサス試作。CPU/GPU採掘と難易度回復、マルチアセットUTXO、決定論的EVM、25報酬のシリアル化、発行上限、再編成、30秒・60秒条件でのノード費用を測定する。

段階C：利用者向けソフト。Windows/Linuxウォレット、Ubuntu用ヘッドレスCLIノード、独立プール統合、検証可能なエクスプローラー、署名注文の取引所、ネイティブ送金、トークン生成、NFT機能を実装する。強いシールド、法定通貨事業者、外部ブリッジは個別の審査段階で追加する可能性がある。

段階D：公開テストネットと独立審査。再現可能なソースを公開し、少なくとも90日間の公開テストネットを実施し、最後の30日間は安定稼働を条件とする。攻撃テストを行い、コンセンサス、暗号、発行、EVM、修正の妥当性を独立審査にかける。受入条件を満たすまでメインネットを開始しない。開始日や市場価格を保証しない。

14. 限界と研究課題

主要リスクはCPU/GPU二重方式の累積作業量、25資産報酬とUTXO状態の肥大化、UTXO/EVM統合、gasと永続状態の価格、強力な任意シールド証明、ウォレット復元、プールの信頼問題、外部チェーン相互運用性である。30秒ブロックと低手数料には測定すべき代償があり、自動的に高いスケーラビリティを意味しない。

当初の使い捨てRust実験は11件のクロスプラットフォーム試験で発行・ベスティング計算を確認したにとどまる。完成した暗号方式、安全なP2P、EVM適合性、シールド送金、採掘収益性、監査済みウォレット、メインネット安全性を証明したものではない。将来の説明は設計意図ではなく確認可能な実装証拠に基づく。

参考文献と文書の沿革

Kelyrium Network『White Paper 1.0 Draft』（2026年9月15日）、『Consolidated Architecture & Design Decision Record V1.2』（2026年10月23日）、『Master Implementation Prompt for Claude/Astra/Codex V1.2』（同日）。

技術的な先行資料：『Bitcoin: A Peer-to-Peer Electronic Cash System』、EthereumのgasとEVMの資料、ERC-20・ERC-721・ERC-1155規格、P2P採掘・ウォレットセキュリティ研究。これらは設計参考資料であり、提携関係を意味しない。

著作権と著作者

Copyright © 2026 Abraham Gómez and Gerardo Gómez. All rights reserved.
Ｋｅｌｙｒｉｕｍ　Ｎｅｔｗｏｒｋ　Ｗｈｉｔｅ　Ｐａｐｅｒ　・　Ｖ１．３　・　２０２６年１０月２３日．

本書は技術的検討と議論のために提供される。出典を明記した引用・共有を許可することは、Kelyriumの商標、アートワーク、その他独立して保護される素材の利用許諾を意味しない。公開されるオープンソースソフトウェアの利用条件は、それぞれの正式ライセンスに従う。