KELYRIUM

네트워크 백서

기술 아키텍처 및 경제 사양 · V1.3

공동 창립자

Abraham Gómez
Gerardo Gómez

2026년 10월 23일

Kelyrium.org • Kelyrium.com

VERSION 1.3 | TECHNICAL DESIGN DRAFT

하나의 체인. 25개 네이티브 자산. 누구나 참여.

개정 기술 초안 | 2026년 10월 23일

Kelyrium.org • Kelyrium.com

초록

Kelyrium은 Bitcoin Core의 명칭만 바꾼 포크가 아니라 Rust로 독자 구현하는 오픈소스 독립형 레이어 1 작업증명(PoW) 네트워크 구상이다. 하나의 합의 기록이 네트워크 화폐 KELY와 각각 고유한 공급 상한을 지닌 24개의 Bitcoin World 네이티브 자산을 지원한다. 변경된 보상 설계에서는 유효한 블록 하나가 채굴될 때 25개 네이티브 자산의 보상을 모두 결정론적으로 발행한다.

이 프로토콜은 허가가 필요 없는 CPU/GPU 채굴, 사용자가 직접 관리하는 지갑, 자산 간 결제, 결정론적 EVM 스마트 계약, 사용자 발행 대체가능 토큰, NFT, 선택형 프라이버시 기능을 통합하는 것을 목표로 한다. 시드 서비스는 피어 검색만 돕고 잔액이나 합의 규칙을 바꿀 특별 권한이 없다.

본 백서는 현재 의도한 아키텍처를 설명하는 기술 초안이다. ‘ 계획 ’ 또는 ‘ 후보 ’ 로 표기한 기능은 이미 배포되었거나 보안 감사를 통과했다는 뜻이 아니다. 메인넷 매개변수와 보안성은 재현 가능한 실험과 독립 검토로 검증해야 한다.

1. 범위 및 사양 확정 상태

이 V1.3 문서는 25개 자산 네트워크의 초기 설계, 통화 매개변수, 보안 요구사항 및 엔지니어링 검증 기준을 정의한다. 독립적인 레이어1 설계 문서이며 계획된 기능이 구현되거나 감사를 마쳤다는 주장은 아니다.

목표 블록 간격은 30초이지만 실제 운영 성능이 입증된 것은 아니다. 채굴 보상 성숙 기간 120블록은 제안 상태다. 네트워크 직렬화 형식, 수수료 계수, 해시 알고리즘, 프라이버시 증명 체계 등 확정되지 않은 합의 매개변수를 구현자가 임의로 결정해서는 안 된다.

25개 프로토콜 네이티브 자산과 스마트 계약으로 만들 수 있는 수많은 토큰을 구분해야 한다. 계약 토큰은 각 계약의 규칙을 따르며 네이티브 자산 등록부 또는 공급 상한을 변경할 수 없다.

- 합의: 독립 PoW L1, CPU/GPU 이중 트랙 심사 중
- 목표 블록 간격: 30초, 세계 규모 성능 평가 필요
- 네이티브 자산: KELY와 Bitcoin World 24개, 총 25개
- 정밀도: 자산당 소수 12자리, 검사형 u128
- KELY 공급 한도: 21,000,000개(제네시스 630,000개 포함)
- 초기 보조금: 30초 블록당 2.425 KELY 제안
- 반감기: 4,200,000블록(약 4년, 정확한 총량 검증 필요)
- Coinbase 성숙: 120블록 제안, 미확정
- 기존 블록 바이트 예산: 192,000, 재검증 필요
- 계약: 결정론적 EVM, ERC - 20/721/1155 계획
- 프라이버시: 친화적 지갑, 향후 감사받은 선택형 차폐
- Gas: KELY 기본, 후원 결제 검토 중
- 업그레이드: 공개 KIP, 버전별 활성화, 관리자 우회 없음

- 메인넷 요건: 공개 테스트넷 최소 90일, 마지막 30일 안정 및 독립 검토

2. 단일 블록체인과 독립 검증

Kelyrium은 별도로 채굴되는 25개 체인이 아니라 하나의 P2P 원장과 하나의 전역 블록 이력으로 구성된다. 풀 노드는 작업증명, 자산별 잔액 보존, 서명과 지출 권한, 코인베이스 발행, 계약 상태 전환, 블록 커밋먼트를 독립적으로 검증한다. DNS 시드, 부트스트랩 노드, 채굴 풀, 지갑 서버, 블록 탐색기는 원장을 재작성할 특별 권한이 없다.

목표 블록 간격은 약 30초이며 초기 설계의 후보 직렬화 블록 크기 한도는 192,000바이트다. 국제적 전파 지연, 경쟁 블록 발생률, 체인 재구성, CPU/GPU 난이도, 저장 공간 및 대역폭 비용을 측정한 후 안전한 최종 설정을 선택해야 한다. 바이트 수뿐 아니라 계산 gas와 영구 상태 증가량도 한도를 두어야 한다.

피어 탐색은 복수의 독립 DNS · 부트스트랩 서비스, 캐시된 피어, 사용자가 지정한 노드로 제공해야 한다. 지역적으로 분산된 독립 운영 노드와 채굴자가 늘어날수록 프로젝트 소유 서버 의존도는 낮아져야 한다.

3. V1.3 최초 자산 목록 및 발행 정책

아래 표는 제네시스에 포함되는 전체 자산을 정의한다. 모든 자산은 국가 또는 지역, 참조 통화, 최대 공급량, 첫 에포크의 제안 보상을 명시한다. 25개 자산은 하나의 블록체인에서 발행된다. 통화 관련 이름은 법정화폐 연동, 준비금 보증 또는 상환 약속을 의미하지 않는다.

국가 / 지역	통화	자산	최대 공급량	초기 보상
글로벌 / Kelyrium 네트워크	Kelyrium	KELY	21,000,000	2.425
미국	US Dollar	BTC - USD	210,000,000	25
유로존	Euro	BTC - EURO	189,000,000	22.5
일본	Japanese Yen	BTC - YEN	2,100,000,000	250
중국	Chinese Yuan	BTC - YUAN	630,000,000	75
영국	British Pound	BTC - POUND	105,000,000	12.5
베트남	Vietnamese Đồng	BTC - VND	21,000,000,000	2500
멕시코	Mexican Peso	BTC - PESOM	420,000,000	50
태국	Thai Baht	BTC - BAHT	840,000,000	100
인도	Indian Rupee	BTC - RUPEE	1,050,000,000	125
대한민국	South Korean Won	BTC - WON	4,200,000,000	500
러시아	Russian Ruble	BTC - RUBLE	1,260,000,000	150
스위스	Swiss Franc	BTC - FRANC	84,000,000	10
튀르키예	Turkish Lira	BTC - LIRA	1,680,000,000	200
브라질	Brazilian Real	BTC - REAL	315,000,000	37.5
사우디아라비아	Saudi Riyal	BTC - RIYAL	168,000,000	20
아랍에미리트	UAE Dirham	BTC - DIRHAM	147,000,000	17.5
대만	New Taiwan Dollar	BTC - TWD	1,344,000,000	160
폴란드	Polish Złoty	BTC - ZLOTY	378,000,000	45
홍콩	Hong Kong Dollar	BTC - HKD	336,000,000	40
인도네시아	Indonesian Rupiah	BTC - RUPIAH	10,500,000,000	1250

국가 / 지역	통화	자산	최대 공급량	초기 보상
필리핀	Philippine Peso	BTC - PESOP	735,000,000	87.5
캐나다	Canadian Dollar	BTC - CAD	231,000,000	27.5
호주	Australian Dollar	BTC - AUD	294,000,000	35
싱가포르	Singapore Dollar	BTC - SGD	126,000,000	15

30초 목표 블록 간격, 4,200,000블록 반감기 및 25자산 동시 보상은 설계 매개변수다. 메인넷 전에 정수 기반 발행 일정과 모든 공급 상한을 검증해야 한다.

4. 발행, 제네시스 및 채굴 보상

모든 유효 블록에는 KELY와 24개 지역 자산의 결정론적 보상이 포함된다. 채굴자나 풀이 임의로 누락하거나 바꿀 수 없다.

30초 목표 블록 간격, 4,200,000블록 반감기 및 25자산 동시 보상은 설계 매개변수다. 메인넷 전에 정수 기반 발행 일정과 모든 공급 상한을 검증해야 한다.

공개된 KELY 제네시스 할당량은 전체 2,100만 개의 3%인 630,000 KELY로 유지된다. 창립자용 210,000 KELY와 운영용 420,000 KELY가 75개의 베스팅 추적 출력에 배분된다. 창립자 몫은 초기 조건 충족 시 21,000, 12개월 차 31,500, 13~48개월 동안 월 4,375씩 36회다. 운영 몫은 초기 63,000과 1~36개월의 정수 분배 총 357,000이다. 모두 기존 발행 상한 안에 있으며 지정된 서명 · 시간 제약을 받는다.

보조 자산의 제네시스 잔액은 0으로 계획한다. 새 보상 바스켓은 각 자산의 불변 공급 상한을 검증해야 한다. 미세 단위 잔량, 보상 커밋먼트, 잠금 해제 조건, 깊은 재구성 처리 규칙을 확정해야 한다. 120블록(30초 목표 기준 약 60분) 코인베이스 성숙은 아직 후보이다.

5. 작업증명과 채굴 풀

CPU와 GPU의 두 PoW 트랙은 하나의 전역 체인을 연장하기 위해 경쟁한다. 트랙별 난이도는 독립적으로 관리하고 누적 작업량 비교 방식을 엄밀히 정의해야 한다. 초기 후보로 CPU yespower, GPU KawPow를 검토하고 Verthash와 비교했다. 어떤 방식도 ASIC 저항성을 보장하지 않으므로 최종 선택은 성능 · 보안 검토를 거친다.

사용자는 단독 채굴하거나 지갑에서 독립 운영 채굴 풀을 선택할 수 있다. 풀 목록에는 수수료, 지역, 지연 시간, 운영자, 공유 난이도, 지급 모델, 성숙 기간, 지급 기준, 성능을 보여야 한다. 해시레이트가 낮은 참여자도 블록을 직접 찾지 않아도 유효 공유 작업량으로 참여한다. 풀은 25개 자산의 보상 지분을 분배하며, 실제 유동성과 명확한 호가가 있을 때에만 선택 자산으로 교환한다.

공유 작업 조작, 블록 은폐, 오래된 작업, 체인 재구성, 보상 성숙, 풀 집중 문제를 방어해야 한다. 무허가 P2Pool 유사 설계도 연구 대상이다. 명목 해시레이트 외에 독립 노드 수, 채굴자 다양성, 풀 집중도를 주요 보안 지표로 삼는다.

6. 네이티브 원장과 자기 수탁

기본 원장은 자산별 보존 규칙을 갖춘 버전 관리형 다중 자산 UTXO 모델이다. 일반 지급은 입력 소유 권한을 인증하고 명시적 출력을 생성한다. 후보 스크립트에는 단일 키, 임계치 서명, 잠금 조건, 만료 시간 및 검증된 Schnorr 암호기술이 포함된다. 서명은 체인 도메인, 자산 ID, 금액, 수취 조건, 거래 문맥을 함께 묶어야 한다.

합의는 이중 지출, 입력 중복, 무효한 코인베이스, 비정규 인코딩, 오버플로와 언더플로를 거부한다. 재구성 시 UTXO · 발행 누계 · EVM 상태를 원자적으로 되돌리고 안전하게 다시 적용해야 한다.

지갑은 복수의 독립 신원, 복구 구문, 새 수신 주소를 관리하고 동일 앱에서 25개 네이티브 자산을 사용할 수 있어야 한다. 암호화 저장, 백업, 서명 미리보기, 코인 컨트롤이 필수다. 주소를 많이 만든다는 사실만으로 거래가 익명화되지는 않는다.

7. 낮은 수수료, 자원 가격 및 가스 후원

KELY는 네트워크 수수료를 지불하는 기본 결제 자산이다. 전송 비용은 가능한 한 낮게 유지하되 무제한 자원 소모를 무료로 제공해서는 안 된다. 지속적 스팸 공격 비용과 일반 사용자 비용 사이의 균형이 중요하다.

단순 자산 이동에 불필요한 EVM 계산을 부과하지 않는다. 계약 실행, 영구 저장, 증명 검증, UTXO 생성, 데이터 사용량은 각 자원 비용에 따라 과금하고 혼잡 시 가격을 조절한다. 바이트, CPU, 메모리, 저장 공간, 상태 증가를 별도로 측정하고 상한을 둔다.

KELY가 없는 지갑을 위해 승인된 후원자가 KELY로 gas를 지급하고 사용자가 다른 지원 자산으로 상환하는 방식을 검토한다. 인증된 한도, 만료, 서명, 원자적 결제, 속도 제한, 명확한 시세가 필요하다. 합의가 KELY 이외의 자산을 gas로 직접 인정하는 방식은 아직 승인되지 않은 별도 결정이다.

8. 스마트 계약, 토큰 및 NFT

같은 레이어 1에서 결정론적 EVM 호환 실행 환경을 계획한다. 노드 RPC, 상태 커밋먼트, 영수증, gas 계량, 재구성 안전성이 실제로 구현된 범위에서 Solidity 및 호환 도구를 지원한다. ERC - 20 호환 대체가능 토큰 생성을 초기 목표로 하고 NFT용 ERC - 721 및 ERC - 1155도 포함한다.

무허가 계약 토큰은 25개 네이티브 자산 목록에 추가되지 않는다. 공급량, 발행 · 소각 권한, 소수점 자리, 업그레이드 권한은 공개된 계약에 따른다. 불변 계약과 권한을 공개하는 프록시형 업그레이드 계약이 공존할 수 있다. 지갑과 탐색기는 관리자 권한, 토큰 승인 위험, 검증되지 않은 코드를 경고해야 한다.

UTXO와 EVM 회계 경계에서는 네이티브 12자리와 EVM 단위의 정확한 정수 변환, gas 선납 · 환불, 원자적 결제, 상태 기록 상한, 결정론적 롤백이 필요하다. 계약은 PoW 발행 일정 이외에 KELY 또는 Bitcoin World 자산을 새로 만들 수 없다. 토큰 발행 UI와 NFT 마켓은 응용 서비스이며 가격 · 안전성 · 유동성을 보장하지 않는다.

9. 네이티브 거래소, 법정화폐 및 상호운용성

네이티브 분산형 거래소는 서명된 자기 수탁 P2P 주문을 사용하고 원자적 결제, 주문 취소, 만료, 안전한 입력 예약, 재생 공격 방지를 구현한다. 25개 자산은 모두 같은 체인에 있으므로 서로 교환하기 위해 외부 브리지가 필요하지 않다. 적정 유동성과 가격 제약이 있을 때 KELY 경유 경로를 사용할 수 있다.

새 사용자는 채굴 없이도 주소를 만들고 자산을 수령한다. 기존 보유자에게서 받거나 외부 거래소에 상장된 자산을 매수할 수 있다. 법정화폐 매수 기능에는 실제 결제 제공업체, 신원 · 규정 준수 요건, 진짜 시장 공급과 유동성이 필요하다. 국가 통화를 따온 이름만으로 법정통화를 네이티브 자산으로 자동 바꿀 수는 없다.

지갑에는 향후 Bitcoin, EVM 네트워크, Solana를 위한 모듈형 어댑터를 추가할 계획이다. 외부 체인 자산을 표시하거나 서명하는 것과 자산을 체인 간 안전하게 이동하는 것은 다르다. 브리지는 별도 신뢰 모델과 독립 감사를 요구하며 기본 출시 기능으로 간주하지 않는다.

10. 공개 검증성과 단계적 선택형 프라이버시

Kelyrium의 기본 방향은 지갑에서 프라이버시 친화적인 동작을 기본으로 하면서, 향후 Zcash와 유사한 선택형 차폐 송금과 명시적 공개 · 투명 모드를 제공하는 것이다. 초기 지갑 보호에는 로컬 키 보관, 암호화 백업, 코인 컨트롤, 주소 교체, 최소한의 텔레메트리 및 Tor/I2P 전송 선택권이 있다. 이러한 조치만으로 공개 금액이나 거래 상대방을 암호학적으로 숨길 수는 없다.

진정한 선택형 차폐는 각 자산의 보존 및 발행 상한을 모든 검증 노드가 확인하면서 필요한 거래 정보를 보호해야 한다. 커밋먼트, nullifier, 영지식 잔액 증명, 조회 · 공개 키, 증명 검증 비용, 안전한 복구를 검토한다. 최종 증명 체계, 지원 자산 작업, 지갑 스캔 방식, 적용 일정은 미결정이며 전문 감사가 필요하다.

일반 EVM 활동, 투명한 교환, 채굴 보상 출력, 차폐 · 투명 영역 사이의 이동은 메타데이터를 드러낼 수 있다. 지갑은 이 한계를 설명해야 한다. 블록 탐색기는 전체 합의 데이터, 자산별 발행량, 트랜잭션 커밋먼트, 공개 계약 정보를 표시해야 하며 숨겨진 정보를 표시할 수 있다고 주장해서는 안 된다. 수탁형 믹서나 임의 동결을 위한 관리자 키는 핵심 구조에 포함하지 않는다.

11. 보안, 스팸 방어 및 운영 복원력

합의 보호에는 한도가 있는 정규 블록 · 거래 형식, 자산별 불변 조건, 검사형 정수 연산, 서명과 증명의 도메인 분리, 블록당 계산 · 저장 상한, 결정론적 gas, 코인베이스 성숙 기간, 재구성 시 완전한 롤백이 포함된다.

경제 보호에는 0보다 큰 자원 비례 수수료, 수요에 맞춘 가격, UTXO 생성 비용, dust 방지 정책, 영구 저장 비용이 필요하다. 공격자가 수백만 건의 저렴한 송금을 제출하거나 UTXO를 대량 생산하고 계약 상태를 팽창시키거나 혼잡을 조작하는 시나리오를 검증한다. 노드별 로컬 멤풀 릴레이 정책과 합의 유효성 규칙은 분리한다.

P2P 및 RPC 계층은 수신 바이트, CPU, 메모리, 연결 수, 미처리 요청, 큐 길이, 메시지 크기, 고비용 과거 기록 조회를 독립적으로 제한한다. 비싼 암호 검증 전에 값싼 형식 검사를 수행한다. 피어 다양화, eclipse/Sybil 공격 방어를 시험하며 공유 네트워크의 정당한 사용자를 일괄 차단하지 않도록 한다.

응용 보호에는 안전한 지갑 서명과 피싱 경고, 계약 동작 시뮬레이션, 업그레이드 관리자 공개, 후원 한도와 인증 서명, 풀 공유 작업 검증, 외부 체인 어댑터 격리, 영지식 증명 검증 비용 통제가 있다. 모든 미래 취약점을 막는 방어는 없으므로 퍼징, 공격 시뮬레이션, 재현 빌드, 독립 감사, 보안 신고와 사고 대응이 필수다.

12. 업그레이드, 호환성 및 거버넌스

합의 및 네트워크 요소에는 명확한 버전을 지정한다. 변경 사항은 공개 Kelyrium Improvement Proposal(KIP), 참조 사양, 테스트 벡터, 독립 검토, 테스트넷 활성화 및 사전 공지된 릴리스 절차를 따른다. 네트워크 기능 협상은 호환되는 전송 기능만 정하며 현재 유효한 합의 규칙을 노드마다 다르게 정하는 것을 허용하지 않는다.

지갑 앱, 인덱서, 채굴 클라이언트, 외부 네트워크 어댑터는 호환성을 유지하며 별도로 업데이트할 수 있다. 계약 개발자는 불변 계약 또는 업그레이드 권한을 공개한 프록시를 선택할 수 있고 다중 서명 · 타임락을 권장한다. 지갑 소프트웨어 관리자나 계약 관리자는 네이티브 공급 상한을 바꾸거나 임의로 사용자 자산을 몰수할 수 없다.

합의 업그레이드는 호환성, 활성화 높이, 잠재적 체인 분기, 복구 · 롤백 계획, 다자간 릴리스 절차를 밝혀야 한다. 시드 서버에는 네트워크 관리 특권이 없다.

13. 구현 계획과 메인넷 기준

단계 A — 사양과 회계: 기존 경제 일정, 소스 코드, 12자리 수정 사항을 대조하고 자산 ID, 제네시스 및 베스팅, 보상 벡터, 블록 · 거래 형식, 수수료 단위, 다국어 구현 공통 테스트 벡터를 확정한다.

단계 B — 합의 프로토타입: CPU/GPU 채굴과 난이도 회복, 다중 자산 UTXO 회계, 결정론적 EVM, 25개 보상 직렬화, 공급 불변 조건, 재구성 및 30초 · 60초에서의 풀 노드 성능을 벤치마크한다.

단계 C — 사용자 소프트웨어: Windows/Linux 지갑과 Ubuntu 헤드리스 CLI 노드, 독립 풀 연동, 검증 가능한 블록 탐색기, 서명 주문 거래소, 네이티브 자산 송금, 계약 토큰 발행 및 NFT 기능을 구현한다. 고급 차폐, 법정화폐 사업자, 외부 체인 브리지는 별도 심사 단계가 필요할 수 있다.

단계 D — 공개 테스트넷 및 독립 검토: 재현 가능한 소스를 공개하고 최소 90일간 공개 테스트넷을 운영한다. 마지막 30일은 안정 상태여야 하며 공격 실험을 수행한다. 독립 평가자가 합의, 암호기술, 통화 발행, EVM 동작 및 결함 수정 사항을 검증한다. 문서화된 수용 기준 전에는 메인넷을 출시하지 않고 날짜나 시장 가격도 보장하지 않는다.

14. 한계와 연구 과제

핵심 기술 위험은 두 알고리즘의 누적 작업량 규칙, 25개 보상 바스켓과 UTXO 상태 증가, UTXO/EVM 통합, 계약 gas 및 영구 상태의 경제성, 강력한 선택형 차폐 증명, 지갑 복구, 풀 신뢰, 외부 체인 상호운용성이다. 30초 블록과 저렴한 수수료는 측정 가능한 상충관계를 동반하며 자동으로 확장성을 뜻하지 않는다.

초기 일회용 Rust 실험은 11개 교차 플랫폼 테스트로 발행 및 베스팅 산술을 검증했을 뿐, 완성된 암호학, 안전한 네트워킹, EVM 적합성, 차폐 거래, 채굴 수익성, 감사 완료 지갑 또는 메인넷 준비를 입증하지 않았다. 향후 홍보 주장보다 검증 가능한 구현 증거를 우선해야 한다.

참고 문헌 및 문서 이력

Kelyrium Network, 《White Paper 1.0 Draft》(2026년 9월 15일); 《Consolidated Architecture & Design Decision Record V1.2》(2026년 10월 23일); 《Master Implementation Prompt for Claude/Astra/Codex V1.2》(2026년 10월 23일).

기술 선례: 《Bitcoin: A Peer-to-Peer Electronic Cash System》, Ethereum gas 및 EVM 문서, ERC-20 · ERC-721 · ERC-1155 사양, P2P 채굴 및 지갑 보안 연구. 이 문헌은 설계 참고 자료이며 어떤 제휴 관계도 의미하지 않는다.

저작권 및 저자

Copyright © 2026 Abraham Gómez and Gerardo Gómez. All rights reserved.
Kelyrium Network White Paper · V1.3 · 2026년 10월 23일.

이 문서는 기술 검토와 토론을 위한 것이다. 출처를 명시한 인용이나 공유 허용은 Kelyrium 상표, 아트워크 및 별도로 보호되는 자료의 사용 허가가 아니다. 공개되는 오픈소스 소프트웨어 구성 요소는 각각 공표된 라이선스를 따른다.