KELYRIUM

网络白皮书

技术架构与经济规范 · V1.3

联合创始人

Abraham Gómez
Gerardo Gómez

2026年10月23日

Kelyrium.org • Kelyrium.com

VERSION 1.3 | TECHNICAL DESIGN DRAFT

一条区块链。二十五种原生资产。开放参与。

更新技术草案 | 2026年10月23日

Kelyrium.org • Kelyrium.com

摘要

Kelyrium是一项独立、开源的Layer 1工作量证明（PoW）网络设计，采用原创Rust实现，并非将Bitcoin Core改名后分叉。网络通过单一共识历史支持基础资产KELY及24种分别设置固定供应上限的Bitcoin World原生资产。按照修订后的奖励模型，每个有效挖出的区块都将按确定性规则发行全部25种原生资产的奖励。

该协议旨在结合无需许可的CPU/GPU挖矿、自托管钱包、原生资产之间的结算、确定性EVM智能合约、用户发行的同质化代币、NFT以及可选隐私功能。种子服务只负责协助发现对等节点，不具有更改余额或共识规则的特权。

本白皮书说明目前计划采用的架构。标注为“计划中”或“候选”的功能不表示已经部署或通过安全审计。主网参数、形式安全性与运营准备情况仍须通过可复现的实验和独立审查确认。

1. 范围与规范状态

V1.3 文档定义25资产网络的初始设计、货币参数、安全要求和工程验证门槛。这是一项独立 Layer 1 设计，规划中的功能不代表已经部署或完成审计。

目标出块间隔为30秒，但尚未证明在生产环境中的表现。120个区块的coinbase奖励成熟期仍是建议值。对于网络线缆格式、费用系数、哈希算法和隐私证明系统等未定共识参数，实现者不得未经审核擅自确定。

必须区分25种协议原生资产与可由智能合约创建的潜在无限多种代币。合约代币遵从各自合约规则，不能更改原生货币登记表或原生供应上限。

- 共识：独立PoW L1，双CPU/GPU赛道仍在评审
- 目标区块间隔：30秒，待全球基准测试
- 原生资产：KELY加24种Bitcoin World，共25种
- 精度：每种资产12位小数，检查型u128存储
- KELY供应上限：21,000,000（包括630,000创世分配）
- 初始补贴：建议每30秒区块2.425 KELY
- 减半周期：4,200,000个区块（约4年，待总量验证）
- Coinbase成熟期：建议120个区块，未最终确定
- 原始区块字节预算：192,000字节，需重新测试
- 合约：确定性EVM，计划支持ERC-20/721/1155
- 隐私：隐私友好型钱包，未来可选审计过的屏蔽交易
- Gas：KELY基础支付，赞助交易仍是方案
- 升级：公开KIP，按版本激活，无管理者后门
- 主网门槛：至少90天公开测试网、最后30天稳定并接受独立审查

2. 单链架构与独立验证

Kelyrium只有一条点对点账本和一段全球区块历史，并非25条分别挖矿的链。完整节点独立验证工作量证明、每种资产的守恒、支出授权、coinbase发行、合约状态转换和区块承诺。DNS种子节点、引导节点、矿池、钱包服务器、区块浏览器都没有改写账本的特殊权限。

目标出块间隔为约30秒；原始方案的候选区块序列化大小上限为192,000字节。最终值必须通过跨地区传播时延、竞争区块、重组风险、CPU/GPU难度行为、节点的存储和带宽成本等基准测试确定。除字节大小外，还需限制计算Gas与永久状态增长。

节点发现应支持多个独立DNS/引导源、已缓存节点以及用户指定节点。随着全球独立完整节点和矿工的增加，网络对项目运营基础设施的依赖应逐步降低。

3. V1.3 创世资产目录与发行政策

下表规定创世时的完整资产名录。每项资产都有对应的国家或地区、参考货币、最大发行量以及首阶段拟定区块奖励。25项资产全部运行在同一条区块链上。货币名称不代表法币挂钩、储备担保或兑换承诺。

国家／地区	货币	资产	最大发行量	初始奖励
全球／Kelyrium网络	Kelyrium	KELY	21,000,000	2.425
美国	US Dollar	BTC-USD	210,000,000	25
欧元区	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
越南	Vietnamese Đ ồ ng	BTC-VND	21,000,000,000	2500
墨西哥	Mexican Peso	BTC-PESOM	420,000,000	50
泰国	Thai Baht	BTC-BAHT	840,000,000	100
印度	Indian Rupee	BTC-RUPEE	1,050,000,000	125
韩国	South Korean Won	BTC-WON	4,200,000,000	500
俄罗斯	Russian Ruble	BTC-RUBLE	1,260,000,000	150
瑞士	Swiss Franc	BTC-FRANC	84,000,000	10
土耳其	Turkish Lira	BTC-LIRA	1,680,000,000	200
巴西	Brazilian Real	BTC-REAL	315,000,000	37.5
沙特阿拉伯	Saudi Riyal	BTC-RIYAL	168,000,000	20
阿联酋	UAE Dirham	BTC-DIRHAM	147,000,000	17.5
台湾	New Taiwan Dollar	BTC-TWD	1,344,000,000	160
波兰	Polish Z ł oty	BTC-ZLOTY	378,000,000	45
香港	Hong Kong Dollar	BTC-HKD	336,000,000	40
印度尼西亚	Indonesian Rupiah	BTC-RUPIAH	10,500,000,000	1250
菲律宾	Philippine Peso	BTC-PESOP	735,000,000	87.5
加拿大	Canadian Dollar	BTC-CAD	231,000,000	27.5

国家／地区	货币	资产	最大发行量	初始奖励
澳大利亚	Australian Dollar	BTC-AUD	294,000,000	35
新加坡	Singapore Dollar	BTC-SGD	126,000,000	15

30秒目标出块时间、每4,200,000区块减半和25资产同步奖励是设计参数。主网上线前须验证整数发行规则及每项资产的供应上限。

4. 发行、创世分配与挖矿奖励

每个被网络接受的区块计划包含一个确定性的25资产奖励组合：KELY加24种Bitcoin World资产。原设计中矿工自主选择一种次级资产的机制及未领取奖励额度积累、补发的机制将被废除。发行规则由共识决定，而不是矿工、矿池经营者或资产持有人决定。

30秒目标出块时间、每4,200,000区块减半和25资产同步奖励是设计参数。主网上线前须验证整数发行规则及每项资产的供应上限。

已经披露的KELY创世分配仍为630,000枚（2,100万供应上限的3%），其中创始人210,000枚，运营420,000枚，共75个受归属条件管理的输出。创始人份额为初始可领取21,000枚、第12个月31,500枚、第13至48个月每月4,375枚，共36次。运营份额为初始63,000枚，随后第1至36个月按精确整数取整分配合计357,000枚。全部纳入供应上限，并受预定签名和时间限制。

次级资产的创世余额计划为零。新的奖励组合需要逐一验证每种资产的不可变发行上限。取整尾数、coinbase承诺、解锁条件和深度重组处理都需要明确共识定义。120个区块（30秒目标下约60分钟）的成熟期尚未正式确定。

5. 工作量证明与矿池

挖矿设计保留CPU与GPU两个PoW赛道，共同竞争延长唯一的全球链，分别调整难度，并定义可审查的累计工作量比较方式。原设计曾考虑CPU使用yespower、GPU使用KawPow，同时比较Verthash。任何候选算法都不能保证完全抗ASIC，最终算法与参数仍需工程评测和安全审查。

用户可独立挖矿，也可通过钱包选择独立运营的矿池。矿池目录应显示费用、地区、延迟、运营方、份额难度、分配模式、奖励成熟期、最低支付门槛和性能。低算力用户通过贡献有效矿池份额参与，而不必独立挖出区块。矿池可根据份额分配25资产奖励；只有具备真实流动性与明确报价时，才可选择兑换为指定资产。

矿池结算必须防范伪造份额、扣留区块、过期任务、链重组、奖励成熟问题和算力集中。无需许可的P2Pool式结构属于研究方向。网络安全不仅看名义算力，还取决于独立节点数量、矿工多样性和矿池集中度。

6. 原生账本与自托管

基础账本采用版本化多资产UTXO模型，强制遵守各资产的余额守恒。普通支付需要验证输入所有权并明确输出；候选授权条件包括单密钥、门限签名、时间锁、有效期及经过审查的Schnorr密码学。签名须绑定链域、资产标识、金额、接收条件和交易上下文。

共识拒绝双重支付、重复输入、非法coinbase奖励、非规范编码以及整数上溢或下溢。发生链重组时，UTXO、发行累计和EVM状态必须原子回滚，并安全重新执行。

钱包应支持多套独立身份、助记恢复密钥及新的收款地址，在同一应用管理全部25种原生资产。重点是加密存储、备份、签名预览与UTXO选择控制。拥有多个地址不等于交易自动匿名。

7. 低费用、资源定价与Gas赞助

KELY是协议网络费用的主要结算资产。普通转账应尽量低廉，但不能允许无限制的零成本资源消耗。手续费机制必须平衡普通用户成本与攻击者持续制造拥堵的经济成本。

简单资产转账不应执行不必要的EVM代码。合约执行、永久状态写入、证明验证、UTXO创建和数据占用都应按照资源使用计费，并根据需求调节。字节、CPU、内存、存储和状态增长分别计量并设置上限。

如果钱包没有KELY余额，可以研究由获授权的赞助者支付KELY，用户再以另一种支持的资产偿付的设计。此流程必须具备鉴权配额、到期时间、原子结算、签名、频率限制及明确报价。直接让共识接受非KELY Gas仍是另一项尚未批准的决定。

8. 智能合约、代币与NFT

Kelyrium计划在同一L1中加入确定性的EVM兼容执行环境。只有在节点RPC、状态承诺、收据、Gas核算及重组安全性真正实现后，才可声明支持Solidity和相关工具。ERC-20兼容同质化代币的部署是明确的启动目标，ERC-721和ERC-1155用于NFT及收藏品。

无需许可创建的合约代币不计入25种共识原生资产。其供应、铸造/销毁权限、小数位数及升级权限取决于公开的智能合约。不可变合约与具有透明管理权限的代理升级合约可以并存。钱包和浏览器应提示升级控制者、代币授权风险及未经验证的代码。

UTXO与EVM之间必须明确12位原生单位与EVM单位的精确整数换算、Gas预付/退款、原子结算、状态写入限制及确定性回滚。合约不得绕开PoW发行表额外生成KELY或Bitcoin
World资产。代币创建界面和NFT市场属于应用功能，不保证代币价值或流动性。

9. 原生交易所、法币入口与互操作

计划中的去中心化交易所使用签名的自托管P2P订单，实现原生资产的原子结算、撤单、过期控制、安全输入预留以及重放保护。25种资产共用一条链，因此彼此交换无需外部跨链桥。在流动性、限价及安全原子执行允许的条件下，可经由KELY路由交易。

新用户无需挖矿即可生成地址并接收资产。也可以从其他持有者、已上线的外部市场获取资产。法币购买入口需要真正的支付合作方、有效的流动性与供应、以及适用情况下的身份和合规控制。原生资产不会因为名字类似某国货币就自动与该货币兑换。

钱包计划逐步增加模块化Bitcoin、EVM网络和Solana适配器。显示外部链余额或为该链签名，与安全地跨链转移价值并非同一能力。跨链桥有独立信任模型和审计要求，并非默认启动功能。

10. 公共可验证性与分阶段可选隐私

Kelyrium的隐私路线是默认采用保护隐私的合理钱包行为，未来提供可选的类似Zcash的屏蔽转账模式，并保留明确的透明/公开模式。初期钱包保护包括本地密钥保管、加密备份、UTXO控制、地址轮换、最小遥测及可选Tor/I2P网络传输。这些措施本身并不会以密码学方式隐藏公开交易的金额或对手方。

真正的可选屏蔽交易必须在隐藏合适交易细节的同时，让每个验证节点核查各资产守恒与发行上限。研究范围包括承诺、nullifier、零知识余额证明、查看/披露密钥、证明验证计费及安全恢复。证明系统、支持的资产操作、钱包扫描设计与上线计划尚未确定，需要专项安全审计。

普通EVM活动、透明兑换、矿工奖励输出以及透明与屏蔽域之间的转移可能泄露元数据。钱包必须说明这些边界。公开区块浏览器应展示共识数据、各资产已发行量、交易承诺和公开合约信息，但不得声称能读取真正隐藏的信息。核心架构不包含托管混币器或可任意冻结资金的管理员密钥。

11. 安全、反垃圾交易与运营韧性

共识层防护包括：有界且规范化的区块与交易编码、每资产供应不变量、检查型整数运算、签名和证明的域分离、区块级计算与存储限额、确定性Gas、coinbase成熟和重组时完整可逆的执行。

经济层防护包括：非零资源加权手续费、需求驱动定价、UTXO创建成本、dust阈值政策及永久存储收费。模拟攻击者提交数百万笔廉价转账、大量创建UTXO、逼迫合约状态膨胀及操纵拥堵的场景。必须区分各节点的本地内存池/转发策略和共识有效性规则。

P2P及RPC层面分别限制传输字节、CPU、内存、连接数、未完成请求、队列深度、消息大小和高成本历史查询。先进行低成本格式检查，再执行昂贵密码学运算。通过多个发现方式、对外连接分散和测试抵御eclipse/Sybil攻击；防护也不应无差别排斥共享网络上的正常用户。

应用层防护包括钱包安全签名与钓鱼警告、合约交互模拟、升级权限披露、赞助额度与授权签名、矿池份额核验、隔离外部链适配器、限制零知识证明验证资源。没有任何方案能彻底消除未来漏洞；必须进行模糊测试、攻击模拟、可复现构建、独立审计、漏洞披露与事件响应。

12. 升级、兼容性与治理

共识和网络组件拥有明确版本号。升级通过公开的Kelyrium Improvement Proposal（KIP）、参考规范、测试向量、独立评审、测试网上的激活验证以及公开通知的软件发布流程实施。节点之间的能力协商只涉及兼容的网络功能，不允许各节点自行选择不同的有效共识规则。

钱包、索引服务、挖矿客户端和网络适配器可以在兼容条件下独立更新。智能合约开发者可选择不可变合约或明确披露升级权的代理合约，并采用多重签名及时间锁。钱包软件更新者或合约管理员不能随意修改原生资产上限或没收他人资产。

影响共识的升级必须明确兼容性、激活高度、潜在链分叉、恢复方案及多方发布程序。项目运行的种子服务器并非具有治理特权的网络管理者。

13. 实施路线与主网上线标准

阶段A——规范和会计：核对旧经济发行规则、源码及12位小数修订，确定资产ID、创世区块与归属规则、奖励向量、交易与区块编码、手续费单位，以及跨语言的完整测试向量。

阶段B——共识原型：测试CPU/GPU算法及难度恢复，多资产UTXO会计、确定性EVM、25资产奖励序列化、供应不变量、区块重组，以及30秒和60秒方案中的节点性能。

阶段C——用户软件：交付Windows/Linux钱包、Ubuntu无界面CLI节点、独立矿池集成、可验证区块浏览器、签名订单交易所、原生资产转账、合约代币部署与NFT功能。强屏蔽交易、法币合作方和外部链桥可在独立阶段实施。

阶段D——公开测试网与审计：发布可复现的源代码，运行至少90天公开测试网，最后30天须保持稳定，完成对抗性测试，并由独立评审人员审核共识、密码学、货币发行、EVM行为及问题修复。只有达到书面验收标准才启动主网，不保证具体发布日期或资产价格。

14. 局限与研究议题

主要技术风险包括：双算法累计工作量计算、25资产奖励组合及UTXO状态增长、UTXO/EVM整合、合约Gas与永久存储经济性、强可选屏蔽证明、钱包恢复、矿池信任风险和外部链互操作。30秒区块和低费用均存在可测量的成本权衡，不代表自动拥有更高扩展性。

早期一次性Rust实验以11项跨平台测试验证发行和归属计算，但未证明密码学完整性、P2P安全、EVM兼容性、屏蔽转账、矿工盈利性、已审计钱包或主网准备就绪。未来的技术主张应以可复核的实现证据为基础。

参考资料与文档沿革

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》（2026年10月23日）。

公共技术先例：《Bitcoin: A Peer-to-Peer Electronic Cash System》；Ethereum Gas与EVM文档；ERC-20、ERC-721、ERC-1155标准；相关点对点挖矿和钱包安全研究。所引资料仅作为技术背景，并不代表任何合作或隶属关系。

版权与作者

Copyright © 2026 Abraham Gómez and Gerardo Gómez. All rights reserved.

本文件仅供技术审查和讨论。允许注明出处引用或分享，并不授予使用Kelyrium商标、艺术作品或其他独立受保护材料的许可。未来公开的软件组件将分别遵守其正式发布的开源许可证。