NULVIA PROTOCOL · PRIVACY SETTLEMENT WHITEPAPER

隐私结算、隐匿质押与可验证邀请激励协议白皮书

NULVIA Protocol 致力于构建面向 Web3 资金流、质押参与和增长激励的隐私基础设施。协议以 BSC USDT 质押作为第一阶段入口，逐步演进至具备零知识证明、隐私池、查看密钥与链上可审计结算能力的隐私网络。

DOCUMENT VERSION	RELEASE DATE	NETWORK ENTRY
v1.2	2026-07-13	BSC USDT

00 / EXECUTIVE SUMMARY

执行摘要

公链透明性提高了资产可验证性，却同时放大了地址画像、交易路径追踪、持仓暴露和策略泄露等问题。对需要长期参与链上金融活动的用户而言，隐私不只是匿名需求，而是资产安全、商业竞争和合规披露之间的平衡能力。

NULVIA Protocol 的定位是“可验证的隐私结算与质押协议”。当前阶段通过 BSC USDT 质押合约、钱包连接、邀请关系绑定、返佣计算和链下索引数据库形成最小闭环；长期阶段将引入 zk-SNARK/PLONK、Merkle Root、Nullifier、Shielded Pool 和 Viewing Key，使用户可以在不公开完整交易信息的情况下证明状态有效。

用户入口	质押资产	单次范围
BSC	**USDT**	**50-100**

> **核心主张：**NULVIA 不把隐私与审计视为对立面。协议将交易默认隐私、收益可验证、关系可追溯和合规可选择披露放在同一个设计框架中。

当前阶段与长期阶段

阶段	重点	说明
Phase 1	BSC USDT 质押入口	完成钱包连接、USDT 授权、质押合约调用、邀请返佣与领取路径。
Phase 2	可验证索引层	将质押、邀请、返佣和领取事件形成可校验数据结构，支持链上事件与链下记录一致性核验。
Phase 3	隐私结算网络	引入隐私池、零知识证明、查看密钥和中继广播网络，降低地址与资金路径暴露。

01 / MARKET PROBLEM

市场问题与协议机会

传统公链将所有交易状态公开给全网验证者，这种透明性有利于验证，却不适合所有金融场景。地址聚类、交易图谱、资金来源推断和收益路径追踪已经成为链上数据分析的基础能力，普通用户和机构用户都面临隐私与安全压力。

主要痛点

痛点	影响	NULVIA 设计方向
地址画像	同一用户的多笔交易可能被聚类识别，形成完整资产画像。	使用隐形地址、隐私池与选择性披露降低默认暴露。
收益路径暴露	质押、返佣和领取行为会暴露参与规模与商业关系。	以索引层记录关系，以证明层保护长期结算隐私。
合规披露困难	完全匿名难以满足机构审计和风险控制要求。	引入 Viewing Key，让用户可向指定方披露必要信息。
增长激励不透明	邀请关系、返佣来源和领取记录容易产生争议。	以合约事件、数据库索引和后续 Merkle Root 共同核验。

设计原则

- **默认隐私**：长期目标中，地址、金额、收益路径不应默认暴露给公开观察者。
- **可验证**：质押、返佣、领取和销毁均应能够通过链上事件或证明系统核验。
- **可选择披露**：用户可以通过查看密钥向审计方披露特定交易，而不是公开全部历史。
- **最小信任**：资金流优先由智能合约执行，关键参数通过可审计规则约束。
- **分阶段演进**：先完成可运行的 BSC 入口，再迭代隐私证明与原生网络能力。

02 / SYSTEM ARCHITECTURE

系统架构与技术分层

NULVIA 采用分层架构，避免在早期阶段一次性构建过重的隐私链，同时保留未来向原生隐私结算层迁移的接口。当前架构由用户界面、钱包交互层、链上合约层、链下索引层和未来证明层组成。

层级	当前职责	未来扩展
用户界面层	展示协议说明、连接 BSC 钱包、发起 USDT 授权和质押调用。	支持多链入口、隐私证明生成提示、查看密钥管理。
钱包交互层	调用浏览器钱包 Provider，切换 BNB Smart Chain，提交交易签名。	兼容移动端钱包深链、WalletConnect 与更多 EVM 钱包。
合约执行层	处理 USDT 质押、推荐关系绑定、返佣留存和返佣领取。	引入 Merkle Root 奖励核验、隐私池存取款与可暂停升级策略。
索引数据层	记录钱包、质押地址、质押等级、邀请关系、返佣和领取哈希。	构建可重放索引器，保证链上事件和本地状态一致。
隐私证明层	当前为路线图能力。	使用 PLONK/zk-SNARK 证明余额、资格、Nullifier 和状态转换有效性。

专业术语

术语	说明
Commitment	承诺值。将资产票据、随机数和用户密钥组合后生成的哈希，用于隐藏原始数据。
Nullifier	防双花标识。证明某张票据已被使用，同时不暴露票据本身。
Merkle Tree	用根哈希压缩大量状态记录，使链上验证只需要短路径证明。
PLONK	通用零知识证明系统，适合构建可复用的状态转换电路。
Viewing Key	查看密钥。允许用户向指定方披露局部交易信息，用于审计或合规证明。
Shielded Pool	隐私池。资产进入池后，公开链上只保留承诺和证明，减少地址与金额关联。

03 / PRIVACY DESIGN

隐私协议设计

NULVIA 的隐私设计围绕“资产状态不可见、状态转换可验证、防双花可检测、合规披露可授权”四个目标展开。早期 BSC 质押入口不声称已经实现完整隐私链能力，而是为后续证明层积累用户路径、数据结构和资金流模型。

隐私状态转换模型

1. 用户生成私有票据，包含资产金额、随机数和接收密钥。
2. 系统将票据哈希为 Commitment，并写入 Merkle Tree。
3. 用户花费票据时生成 Nullifier，证明票据存在且未被花费。
4. 零知识证明验证输入有效、金额守恒和输出 Commitment 正确。
5. 链上只公开 Root、Nullifier、输出 Commitment 和证明结果。

交易广播隐私

在未来网络中，NULVIA 将研究 Dandelion++ 与加密中继的组合方案。交易先进入低可见度的中继阶段，再扩散到公开网络，从而降低交易内容与发起 IP、钱包环境之间的直接关联。

选择性合规

隐私不等于不可审计。Viewing Key 模型允许用户在必要时对特定交易、特定时间窗口或特定资金路径进行选择性披露。该机制适合机构审计、税务申报、风险核验和合规调查，同时避免把全部链上历史暴露给公开观察者。

> 完整隐私池、零知识证明电路和中继网络属于后续路线图能力。正式上线前需要完成电路安全审计、性能测试、可信设置流程说明和跨司法辖区合规评估。

04 / STAKING CONTRACT

BSC USDT 质押合约模型

第一阶段合约采用 BSC USDT 作为质押资产。用户先授权 USDT，再调用 NULVIA 质押合约。该模型让早期协议可以在成熟 EVM 环境中验证资金流、邀请关系、返佣领取和用户体验。

核心参数

参数	数值	说明
质押资产	USDT on BSC	BSC 主网 USDT 地址为 `0x55d398326f99059fF775485246999027B3197955`。
单次最小质押	50 USDT	低于该数量的交易会被合约拒绝。
单次最大质押	100 USDT	高于该数量的交易会被合约拒绝。
一级邀请返佣	40%	直接邀请人按被邀请人实际质押额获得待领取 USDT。
二级邀请返佣	10%	上级邀请链第二层按同笔质押额获得待领取 USDT。

合约接口

接口	Selector	用途
`stake(uint256,address)`	`0x7acb7757`	提交质押金额和一级推荐人地址。
`claimReferralRewards()`	`0x05eaab4b`	领取当前钱包地址的待领取邀请返佣。

资金流说明

- 无邀请关系：用户质押的 USDT 全额进入协议 Treasury。
- 一级邀请关系：40% 留在合约内作为一级邀请人待领取返佣，60% 进入协议 Treasury。
- 二级邀请关系：一级 40%、二级 10% 留在合约内，剩余 50% 进入协议 Treasury。
- 领取返佣：邀请人调用领取接口，合约将 USDT 自动转入该邀请人的钱包地址。

安全基线

合约安全

- `SafeERC20` 提升 ERC20 调用兼容性。
- `ReentrancyGuard` 降低重入风险。
- `Pausable` 支持异常情况下暂停交互。
- `Ownable` 限定关键配置权限。

上线要求

- 完成第三方安全审计。
- 完成 BscScan 源码验证。
- Treasury 建议使用多签钱包。
- 部署后公开合约地址与 ABI。

05 / INCENTIVE DESIGN

邀请激励与增长机制

NULVIA 的邀请机制用于把早期网络增长与实际质押行为绑定。系统不因单纯连接钱包产生奖励，只有被邀请钱包完成有效 USDT 质押后，邀请人和二级上级才会获得对应返佣。

层级	比例	触发条件	结算方式
Tier 1	40%	直接被邀请钱包完成 50-100 USDT 质押。	合约留存待领取 USDT，邀请人自行领取。
Tier 2	10%	一级下级继续邀请的新钱包完成有效质押。	合约留存待领取 USDT，二级上级自行领取。

关系绑定原则

- 每个钱包地址拥有唯一邀请码和专属邀请链接。
- 推荐关系以首次有效绑定为准，避免后续频繁更改造成争议。
- 返佣以实际质押金额为基准，不以页面输入或口头承诺为准。
- 领取记录应保留交易哈希，方便用户核验。

可验证增长

邀请激励的价值不在于制造短期拉新，而在于把真实资金行为、关系归属和奖励结算进行结构化记录。未来版本可将邀请与返佣数据批量生成 Merkle Root，由用户通过 Merkle Proof 验证自己的奖励资格。

06 / TOKEN & BURN

代币模型与销毁计划

NULVIA 代币用于承载协议治理、生态激励、节点协作和长期价值捕获。当前白皮书不对二级市场价格、固定收益或回报率作任何承诺，代币模型应以正式发行文件和链上治理结果为准。

发行总量与区域额度

全区总发行量	亚洲区额度	亚洲区目标融资
100,000,000	**25,000,000**	**$375,0000**
NULVIA / 100%	NULVIA / 25%	亚洲区指定融资目标

本轮代币单价为 **$0.015**，亚洲区指定目标融资规模为 **$375,0000**，预期全流通估值（FDV）指定为 **$15,000,000**。

代币用途

用途	说明
协议治理	参与参数调整、费用分配、升级提案和生态预算治理。
节点激励	为证明服务、中继服务、索引服务和生态贡献提供激励。
生态增长	支持开发者、合作方、早期社区和协议集成。
安全储备	用于审计、漏洞赏金、应急响应和长期基础设施成本。

销毁计划

> NULVIA 计划采用季度回购销毁机制，将协议真实收入的一部分转化为长期通缩压力。销毁规模与协议真实收入挂钩，长期年度目标为流通量的 1%-2%，具体节奏以主网上线后的治理规则和公开披露为准。

- 销毁来源：协议手续费净收入、机构结算服务费、验证者罚没收入中的约定比例。
- 销毁频率：建议按季度执行，特殊情况下可由治理提案调整。
- 销毁验证：每次销毁应公开 Burn Address、交易哈希、数量和来源说明。
- 目标约束：销毁规模应与真实收入挂钩，避免脱离协议基本面的叙事化销毁。

07 / ROADMAP

两年路线图

NULVIA 的路线图采用“可运行产品优先、隐私能力逐步增强”的策略。每一阶段都应有明确验收标准，避免只停留在概念叙事。

周期	目标	验收标准	状态
0-6 个月	完成 BSC USDT 质押入口与邀请返佣闭环。	用户可连接钱包、质押、形成邀请返佣并完成领取。	开发中
6-12 个月	完成合约审计、主网部署和链上事件索引。	审计报告、合约验证、多签 Treasury、稳定事件索引器。	待启动
12-18 个月	推出隐私证明原型与 Merkle 奖励核验。	Commitment、Nullifier、Merkle Proof、Viewing Key 原型可测试。	规划中
18-24 个月	构建隐私结算网络与节点协作模型。	中继网络、证明服务、节点激励和治理流程形成公开规范。	规划中

关键里程碑

- 发布正式合约地址、ABI、部署交易和源码验证链接。
- 完成安全审计，并对发现问题进行修复和复审。
- 建立链上事件索引器，支持质押和返佣数据重放核验。
- 发布隐私证明技术规格，包括电路输入、约束、证明成本和安全假设。
- 发布 Viewing Key 与选择性披露流程。

08 / SECURITY & COMPLIANCE

安全、合规与风险控制

NULVIA 的长期价值依赖安全与合规边界。隐私协议尤其需要清晰说明：哪些数据默认不可见，哪些数据可由用户授权披露，哪些行为会被合约规则拒绝，哪些风险由用户自行承担。

安全要求

类别	要求
智能合约	审计、单元测试、主网小额试运行、暂停机制、多签 Treasury、公开验证。
密钥安全	部署私钥隔离保存，生产密钥不进入源码或前端文件。
数据一致性	链上事件和索引数据需可重放、可核验、可恢复。
隐私证明	电路审计、可信设置说明、证明生成性能测试和异常案例覆盖。

合规边界

- NULVIA 不应被设计为规避合法监管审查的工具。
- 协议应提供用户授权的选择性披露能力。
- 不同地区对质押、返佣、代币发行和隐私工具的监管差异较大，正式运营前应取得法律意见。
- 对外材料必须避免收益承诺、保本承诺和误导性投资表述。

09 / DISCLAIMER

免责声明

本白皮书仅用于说明 NULVIA Protocol 的产品方向、技术设计、经济模型和路线图，不构成投资建议、法律建议、财务建议、募资文件或证券发行说明。

加密资产、智能合约、链上质押和隐私协议均存在高风险。任何参与者都应独立评估风险，包括但不限于合约漏洞、市场波动、流动性不足、监管变化、第三方钱包或 RPC 服务故障、数据同步失败以及不可预见的技术缺陷。

本文所述路线图、参数、比例、销毁计划和功能边界可能在主网上线前后根据安全审计、治理决议、法律意见和市场环境进行调整。NULVIA 不对任何固定收益、价格表现或业务结果作承诺。

> 正式运营前，协议应完成合约审计、法务审查、公开风险披露、密钥托管方案和生产监控方案。未完成上述步骤时，不建议进行大规模真实资金运营。

结语

NULVIA 的第一阶段重点是以可验证的 BSC USDT 质押合约建立真实资金流闭环，再逐步扩展至隐私证明、隐私结算和选择性合规披露。只有当安全、合规与可验证性同时成立时，隐私金融基础设施才具备长期生命力。