白皮书

Noticoin 协议、发行机制、钱包隐私、地图便笺与挖矿。

技术规范 · 1.0.0

Noticoin 是采用 RandomX 工作量证明、限制总发行量的网络，钱包内置地图。本规范涵盖共识、交易隐私、地图标记发布格式、付费便笺交付、运营方注册表、基金核算和矿池。各表区分共识参数及应用配置。时间与发行图表均注明模型假设。

01 共识与网络标识

02 工作量证明与区块验证

03 供应量与区块补贴

04 确认与可花费状态

05 钱包与交易隐私

06 地图记录格式与生命周期

07 运营方注册表与周期

08 地图记录与便笺交付

09 费用与基金

10 挖矿与矿池核算

11 验证与发布条件

12 实现与操作指南

01

共识与网络标识

Noticoin 源自 Monero v0.18.5.4，目标出块间隔为 45 秒。第 1 个区块使用协议版本 16 并验证 RandomX，版本 17 在高度 160 激活。P2P 握手检查网络标识。各网络分别使用自己的创世哈希、端口和地址前缀。

全新节点根据配置与创世区块确定网络标识。Levin 握手检查 16 字节网络 ID。地址前缀区分标准地址、集成地址和子地址。运营者可先将高度零的区块与清单核对，再使用节点验证付款。回归网络使用隔离数据，付款服务须显式启用才能接收。

网络	P2P	RPC	ZMQ	地址前缀
mainnet	19080	19081	19082	111 / 112 / 113
testnet	29080	29081	29082	114 / 115 / 116
stagenet	39080	39081	39082	117 / 118 / 119

标准 / 集成 / 子地址

Mainnet

创世哈希

`2784467d7c909874668b9f0accf533c63f77aad79a3b72bfc5b23ca09e3cb614`

P2P 网络标识

`305639f9810544e48197a8f69a0a6d19`

Testnet

创世哈希

`e2c8d4803df588a35e8289d2f939f3521ec92c43d4e8e453d05585917c205a90`

P2P 网络标识

`3946c278a80142618044dfa92619e1e7`

Stagenet

创世哈希

`090c1b22ef96a0d7e05d7ec6321ad3f61d4f36c90cce2ce573e3c4be19f8daef`

P2P 网络标识

`0205f90fad5c4d41a8ad3bf27b9c1f06`

02

工作量证明与区块验证

节点验证父区块、主版本、时间戳、工作量证明、交易及矿工奖励，并按累计难度比较竞争分支。RandomX 使用从链派生的种子对区块哈希输入求值。初始种子为创世哈希。默认种子周期为 2,048 个区块，滞后 64 个区块。

高度	主版本	范围
0	1	Genesis
1	16	RandomX · CLSAG · Bulletproofs+
160	17	6 区块

难度调整使用滞后 40 块后的历史记录，最多 1,920 条。先排序时间戳，在样本足够时裁去极值。所选区间的累计工作量乘以目标间隔，再除以至少一秒的经过时间，结果向上取整。历史记录至多一条时难度为一。时间戳规则另采用 160 块窗口，限制未来时间为两小时。

参数	值
RandomX 周期 / 滞后	2,048 / 64 区块
难度窗口 / 滞后 / 裁剪参数	1,920 / 40 / 160 区块
时间戳窗口 / 未来时间限制	160 区块 / 2 h

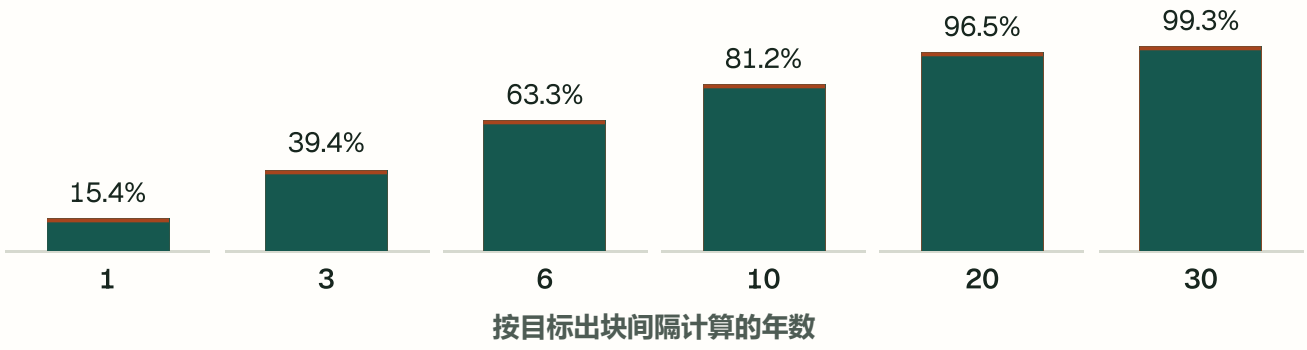
03

供应量与区块补贴

供应上限为 3.82 亿 Noticoin，精度为九位小数。创世区块将 17.592186044 Noticoin 计入不可花费的输出。发行达到上限后，矿工的链上收入来自交易手续费。

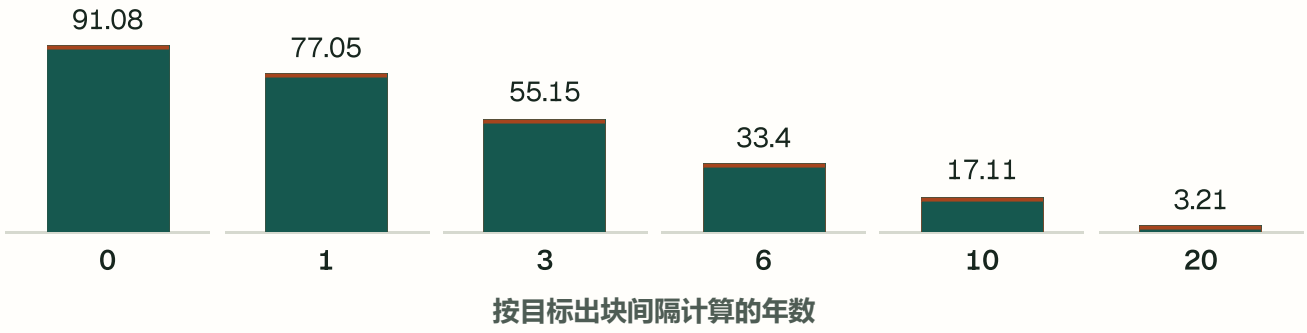
令 S 为累计发行的最小单位数，包含创世输出。达到上限时补贴为零，否则为 ceil((3820000000000000000 − S) / 4194304)。创世之后首块在无重量惩罚时，手续费前补贴为 91.075893023 Noticoin。区块重量介于有效参考重量与两倍参考重量之间时扣减补贴。手续费计算独立采用 0.3 Noticoin 的最低参考值。

累计发行量占上限比例



按每块 45 秒、每年 365.25 天估算。曲线采用完整补贴，暂略区块重量惩罚和最小单位取整。

区块补贴随时间变化模型



单位为每块 Noticoin，未计交易费、重量惩罚与最小单位取整。

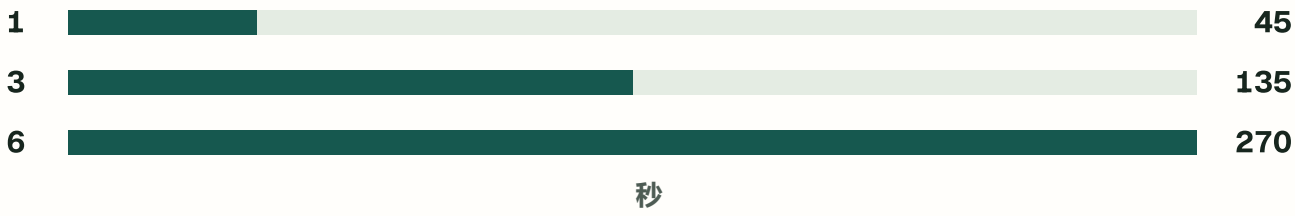
04

确认与可花费状态

从高度 160 起，普通输出获得六次确认后可花费。挖矿输出在 160 个区块后成熟。自动便笺交付核验三次确认及有效密钥份额。实际等待时间受上链、区块发现及链重组影响。

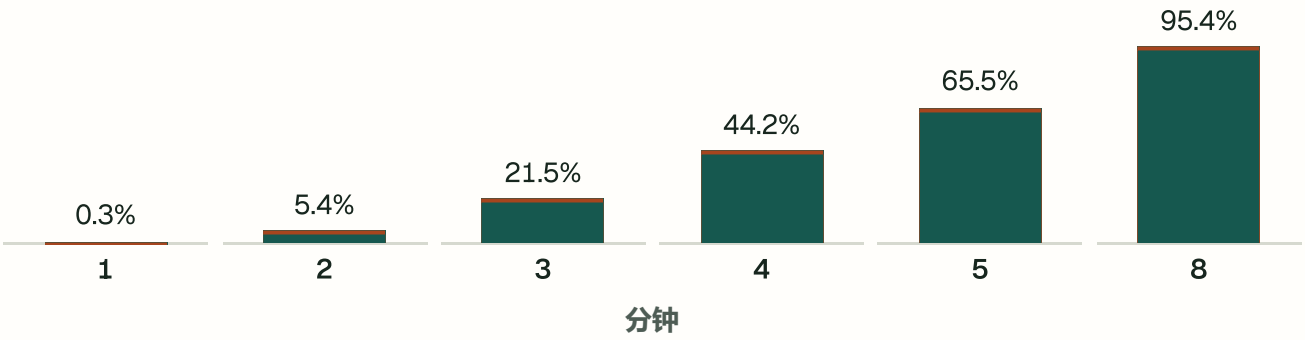
包含交易的区块计作第一次确认，内存池中的待处理交易有零次确认。版本 17 之前，普通输出的共识年龄为 27 块。高度规则按区块计数。模型设定交易进入到达的第一个区块，未纳入拥堵、难度变化及重组。

不同确认数的目标耗时



按 45 秒目标出块间隔计算。

六个区块到达的概率模型



泊松到达模型假设各次出块相互独立且均值稳定为 45 秒。图中显示指定时间内至少到达六个区块的概率。

05

钱包与交易隐私

RingCT 隐藏金额，一次性输出在链上隐藏收款地址。你可以为不同联系人创建子地址。

钱包使用私有查看密钥扫描输出，并以花费密钥材料签署交易。链上记录输出密钥、输入环、密钥镜像、承诺与证明。现行规则下普通 RingCT 输入使用一名真实成员和十五名诱饵。CLSAG 证明签名授权，密钥镜像阻止重复花费。Bulletproofs+ 验证金额范围。手续费与交易重量仍公开可见。

如需区分收款场景，可使用不同子地址。应分别备份恢复短语和私密标记或已购便笺所需的本地地图配置。链观察者能看到交易时间和结构，对等节点与服务可能看到部分连接元数据。

字段	范围
RingCT	机密金额承诺
CLSAG	可链接环授权
Bulletproofs+	金额范围有效性证明
公开交易数据	费用、重量、结构及时间

06

地图记录格式与生命周期

启用链上锚定时，钱包将签名的 118 字节记录写入 tx_extra 的 nonce，签名覆盖第 0 到 53 字节。地图在发布或撤回前核验签名和三次确认。公开记录锚定标记 ID 与作者密钥。期限、标题、坐标及密文由地图服务处理。免费发布或撤回向作者钱包自转一个最小单位并消耗网络手续费。

字节偏移	字段	值
0–4	魔数与版本	`4e544d5001`
5	操作	1 · 发布标记 2 · 撤回
6–21	无分隔符的标记 UUID	16 B
22–53	Ed25519 作者公钥	32 B
54–117	Ed25519 签名	64 B

公开便笺使用 AES-256-GCM，并随密文公开阅读密钥。共享标记保存在发送者钱包中，直到用 RSA-OAEP 与 SHA-256 为指定接收者打包。接收钱包在本地打开包。Atlas 分开保存瓦片和便笺，发布标记无需更改地图瓦片。

07

运营方注册表与周期

运营方在签名交易记录中公告网络、到期高度、Ed25519 身份、RSA-3072 加密密钥和 HTTPS 入口。节点根据周期边界前六块为止的规范链生成名单。按交易手续费排序，随后按签名身份升序排列。加密密钥及入口去重。名单至少需要三项，便笺交付需要严格多数。

参数	公开网络	Regtest
周期长度	40	10
最长注册期限	240	30
截止深度	6	6
高度 200 前 / 起的名单上限	3 / 10	3 / 10

购买使用发布所在区块对应的名单。更新后的名单适用于未来发布，待交付购买仍需可访问原有份额。选择证明注册及链上位置。运营方独立性与密钥保管是单独的运维假设。原运营方在线不足时，自动交付可能停滞。

`get_note_operator_roster · NOTI_NOTE_REGISTRY=1`

08

地图记录与便笺交付

发布者的钱包先用 AES-256-GCM 加密便笺，再将其发送到地图服务器。

地图服务器保存便笺的加密文本。区块链记录便笺的发布和付款交易。

付费版由卖家设定价格及 1 至 100 份的数量限制。钱包为每份生成不同的卖家子地址并发布签名报价。买家预留一份并向该地址付款。运营方验证付款证明、订单绑定及三次确认，再返回面向买家加密的份额。买家在本地重建 AES 密钥。启用运营方交付后，卖家发布后可以离线。

付费便笺交付顺序

签名报价	预留一份	核验付款	交付密钥份额	本地解密

成交后服务提供 24 小时取回窗口。阅读副本在本地归档后，可从已购便笺再次打开，直至删除本地副本。售罄或过期条目从公开地图移除。系统控制交付流程。读者打开后可保存或分享内容。

09

费用与基金

发布费用收至专用基金钱包的子地址。独立桥接服务验证节点及钱包标识、高度和到账金额。网站以快照显示余额、可用余额及六次确认后的历史，链接交易哈希并可公布支出金额与用途。基金报告省略单笔收入金额及付款者地址。矿工所得网络手续费独立计算。

按操作划分费用

操作	值	收款方
公开标记、7 天、标准图标	网络手续费	矿工
付费便笺发布、7 天	0.2 Noticoin	基金
发布 30 天	0.6 Noticoin	基金
钻石图标	0.1 Noticoin	基金
秘密便笺	由作者设定	作者
支持捐赠的标记	由发送方选择	作者

发布费和图标费合并为一笔款项支付给基金。发送方另付网络手续费，由矿工获得。

10

挖矿与矿池核算

两种 Stratum 模式均采用 RandomX。联合模式按最近 128 份份额的工作量分配符合条件的收益。单独模式的区块直接支付给矿工。矿池算力基于十分钟内接受的份额；全网算力按难度除以目标出块间隔估算。查询个人统计需要完整地址。

Stratum 作业包含哈希输入、种子哈希、高度、份额目标及作业 ID。份额满足份额目标。区块候选还满足网络难度，由矿池提交给节点。联合账本保存与规范链候选绑定的最近 128 份份额分配。奖励在 160 块后成熟，联合结算扣除付款手续费。单独模式下，节点为提交者地址构建矿工交易。

面板基于 600 秒内接受的工作量，启动阶段窗口较短。每 30 秒采样两种模式的算力和网络难度，一个进程最多保留 240 个样本。重启会清空图表样本。份额与付款账本独立持久化。公开面板提供聚合数据，个人查找需要完整地址。

参数	值
PPLNS	128
算力统计窗口	600 s
图表采样间隔及样本上限	30 s · 240
奖励成熟期	160 区块

11

验证与发布条件

开发记录使用真实节点与钱包二进制及隔离数据。固定难度回归网络可复现交易和核算状态变化。公开部署还需验证独立对等节点、持续算力及网络中断恢复。

验证项	已记录覆盖
共识与网络标识	三个网络隔离运行的创世区块和首个 RandomX 区块
确认与可花费状态	激活后钱包中继、对等节点可见性及六次确认花费
地图记录格式与生命周期	作者撤回、付费交付及份数限制、直接捐赠与基金到账
挖矿与矿池核算	接受 Shared 和 Solo 区块、账本重启和确认结算

`verify-first-blocks.mjs` · `verify-economy.mjs` · `verify-note-registry.mjs` · `verify-offline-release.mjs` · `pool/tests/integration.mjs`

发布准备

12

实现与操作指南

Windows 命令行套件包含 START-NODE.cmd。启动节点，核验链标识，完成同步后再查看余额。管理 RPC 应绑定可信接口。各网络使用独立的数据目录和钱包文件。核验发行包校验和，将恢复短语与钱包文件分开保存。

公开部署应为每个付款组件设定预期网络并核对高度零哈希。钱包 RPC 经认证且仅在回环接口。地图有需要时，通过 HTTPS 暴露受限桥接服务。收款钱包和账单数据库一起备份。保护运营方密钥，并保留仍需取回的交付份额。测试与公开服务使用独立目录。

组件	运维接口
Daemon RPC	链标识、高度及挖矿模板 `get_info, get_block_header_by_height, get_block_template`
Wallet RPC	余额、地址与转账证明 `get_balance, get_address, check_tx_proof`
运营方注册表与周期	包含签名身份与交付密钥的周期名单 `get_note_operator_roster`
Bridge	受限付款核验与子地址分配
Pool HTTP	聚合统计及按地址 POST 查询 `GET /api/stats · POST /api/miner`

- 网络清单 (/assets/noticoin-network.json)
- 桌面钱包指南 (/zh/guide.html) · 运行节点 (/zh/guide-node.html) · CLI 与钱包 RPC (/zh/guide-cli.html)
- 地图与标记 (/zh/map.html) · 付款 (/zh/payments.html) · Noticoin 隐私说明 (/zh/privacy.html)
- 挖矿与矿池 (/zh/mining.html) · 基金报告 (/zh/fund.html)