

后量子区块链协议白皮书

具备密码敏捷能力的权益证明网络

第二版修订 2.2 后量子 PoS 与公开启动设计

2026 年 10 月 10 日

本文提出一套全新的后量子区块链协议设计，不以任何既有代码、测试网络或软件框架为前提。文中的“必须”表示拟议协议约束，“应”表示工程建议。安全性质须在列明的假设、精化证明和实现验证下成立；本文不是已部署网络的测试报告。

标准与研究资料核验截至 2026 年 10 月 10 日

摘要

本白皮书提出一个以标准化后量子密码为基础、采用加权拜占庭容错共识的权益证明网络。设计把交易授权、验证者投票、网络身份、共享密钥建立、状态承诺和升级授权作为分别审查的信任路径，并通过版本化对象、统一激活规则和可验证迁移连接这些路径。目标是在不创造新密码算法的前提下，为长期运行的公共账本建立明确的密码边界和可执行的演进机制。

基线配置采用 **ML-DSA-87** 处理账户与共识签名，使用 **48** 字节账户标识和 **64** 字节账本承诺，并为传输选择标准化的 **TLS** 混合密钥交换配置。账户身份与可轮换授权策略分离；交易绑定链标识、策略版本、序号与有效高度；验证者集合按预先承诺的边界交接。共识采用已有 **Tendermint** 研究所定义的锁定与投票机制，安全条件为相关集合的拜占庭投票权严格低于三分之一，提交证书覆盖严格超过三分之二的投票权。

协议将大签名的成本纳入独立的字节、验签、执行和状态增长预算，区分交易最终入块、业务执行成功及状态证明可验证的时间。治理通过延迟激活、权限分离和不可由普通参数提案取消的安全约束管理变化。白皮书同时给出经济守恒关系、轻客户端信任边界、密码迁移过程、实验口径和发布条件，以便第三方判断设计是否完整、实现是否一致、结果是否可复现。

经济设计采用最多 **1000** 万枚、**9** 位小数的累计发行上限。评审配置将 **75%** 用于面向公众的初始分配，**25%** 用于长期 **PoS** 安全发行；创始人、贡献者、顾问、机构与基金会的专属免费预留均为零，协议不设开发者手续费抽成。初始统一价格认购按公开成本预算封顶，超额按比例配售并退款；**BTC** 收款、受托与创世交付的风险单独披露。后续 **BTC** 换入属于市场交易，没有固定兑换率、**BTC** 储备或回兑承诺。发行曲线须同时接受稀释与验证者成本检验，不能据此承诺币价或收益。

本文引用标准机构与研究者的原始资料，其中包含大学研究成果。引用提供方法和参数依据，不表示相关作者或机构参与、审计或认可本协议。没有实测依据的吞吐量、收益率和安全认证不作为设计成果。

关键词 后量子密码 拜占庭容错 权益证明 密码敏捷 可验证状态

目录

01 设计目标与系统架构	4
02 量子威胁与安全目标	5
03 密码套件与编码	6
04 身份与密钥生命周期	8
05 协议对象与账本承诺	9
06 共识与最终性	11
07 状态机与交易生命周期	12
08 轻客户端与跨链边界	14
09 资源与性能经济模型	15
10 原生资产经济与治理	16
11 公开启动与 BTC 换入路径	21
12 密码演进与协议升级	23
13 验证计划与发布条件	24
14 研究路线与协议适用范围	26
附录 A 基线配置与参数注册	27
附录 B 安全主张与证明责任	28
附录 C 术语与符号	29
参考文献	30

01 设计目标与系统架构

1.1 协议要解决的问题

公共区块链需要在多年运行中维持授权、最终性和历史验证。公钥一旦进入账本或共识消息，就可能长期暴露。对椭圆曲线签名的依赖因此不能仅靠钱包升级消除，验证者、轻客户端、节点认证和软件发布根也必须具有迁移路径。本文将密码替换视为协议生命周期设计，并把每次替换的规则、成本和信任变化纳入同一系统模型。[1][2]

目标读者包括希望降低长期量子授权风险的 **BTC** 持有者。本协议提供独立的原生资产，用户可在了解新链共识、价格、流动性与交付风险后自愿参与。**BTC** 市值、持有人数量与历史信用不随兑换自动转移；本协议没有已承诺的交易所、流动性或机构采用。**Bitcoin** 的量子风险缓解与迁移提案仍在演进，其中 **BIP 360** 和 **BIP 361** 在核验时均为草案，不能假设 **Bitcoin** 必然无法升级。[28][29]

目标网络允许公开提交交易与独立运行全节点，以质押决定有限规模活跃验证者集合的投票权。初始应用层包括原生资产转移、质押委托、退出、授权策略更新和协议治理。通用智能合约、隐私交易和无需信任的外部桥不属于第一版执行环境；它们必须通过后续规范扩展各自的验证与资源边界。账户签名能力不自动赋予这些扩展安全性。

1.2 架构与责任划分

钱包构造确定编码的交易意图，并按账户策略签名；网络入口先限制长度和速率，再做授权及资源检查。提案者选择有序交易，验证者检查完整区块数据与应用有效性并执行共识。提交后，确定性状态机计算余额、质押、授权和治理状态；下一高度的最终区块头承诺本高度执行后的状态及收据。证明服务从这些承诺生成可独立验证的查询结果。每一层必须保留清楚的错误语义，而不是把“**RPC** 已接收”解释为“转账已成功”。

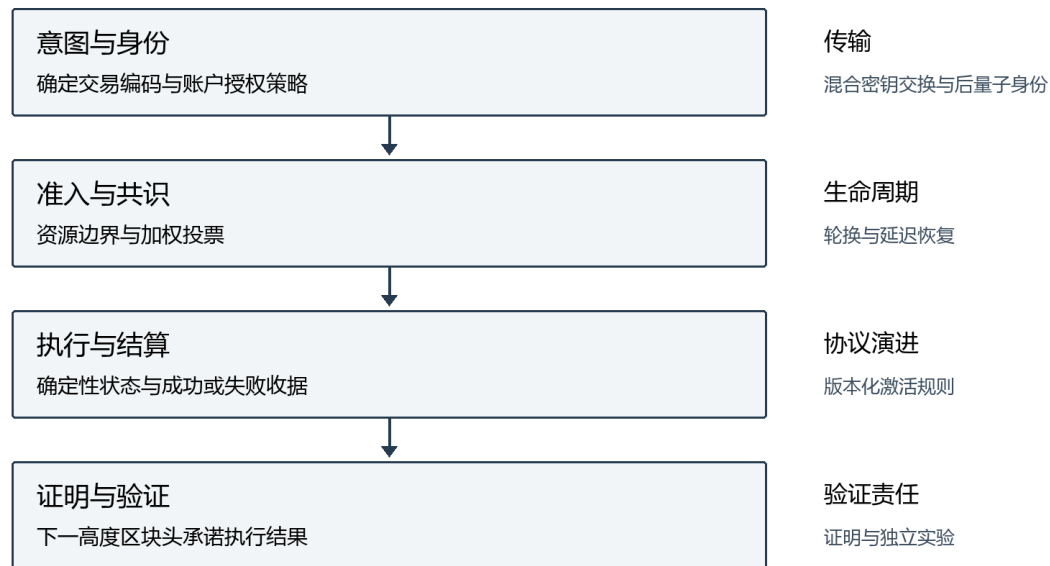


图 1 协议的主要信任路径。高度 h 的执行结果由高度 $h+1$ 的最终区块头承诺。

全节点自行验证共识和执行结果；验证者额外持有与质押身份绑定的共识密钥；轻客户端验证受信检查点之后的头链、集合变化与证明。节点的 TLS 身份证明连接对端，不能替代链上投票资格；共识签名证明验证者投票，不能证明交易业务成功；状态证明证明某个承诺下的值，不能证明远端服务持续可用。这样的责任划分允许每条路径单独更替算法并检验其影响。

1.3 设计原则与验收问题

安全优先级依次为授权不可绕过、共识状态一致、资产与费用守恒、故障可恢复，以及在明确条件下持续推进。性能优化必须保持这些不变量。每项重要设计都应回答四个问题：信任哪一种假设，承诺哪一种性质，如何观察反例，以及如何在升级后继续验证旧历史。白皮书提供协议骨架和论证依据；字节级规范、测试向量和精化证明构成实现前必须冻结的配套材料。

02 量子威胁与安全目标

2.1 威胁模型

协议面向长期公开的账本与开放网络。攻击者可以收集公钥、交易和握手记录，提交恶意消息，重放或篡改流量，并控制部分参与者；量子威胁模型进一步允许其使用未来的容错量子计算机。密钥设备被攻陷、随机源失效和验证者越过共识容错边界，分别属于实现、运维和共识风险，不能仅靠替换签名算法解决。

Shor 算法使整数分解与离散对数具有量子多项式时间算法，因此 RSA、传统有限域及椭圆曲线公钥机制不能承担长期后量子授权。Grover 算法则对非结构化搜索给出平方级查询加速；它不等同于 Shor 式结构性破解，也不能把查询次数直接换算为现实攻击时间。[1][3]

椭圆曲线量子资源研究表明，逻辑电路、纠错开销、物理错误率和允许攻击时长都会改变所需资源。资源估计不是量子破解年份的预测；协议不以某个确定的量子到来日期作为安全前提。网络机密性还需应对先收集密文、以后解密的风险，而公开账本本身不承诺交易隐私。[4][5]

2 2 分层安全目标

密码层要求未获授权者无法产生可接受的账户或共识签名，承诺能绑定唯一的规范化对象，通信同时提供密钥协商与身份认证，并使密钥和算法可以有序迁移。安全论证依赖所选算法的计算困难假设、正确的组合方式和实现条件；共识安全性、活性、状态执行正确性及治理权限仍需分别论证。

本设计选择类别 5 的公钥参数，换取较高资源裕量并接受更大的带宽与存储成本。NIST 类别按规定攻击资源比较划分，不是整条链具有某个固定比特安全等级的保证；哈希原像、碰撞、签名伪造和协议攻击也不能用一个数字互换。采用 FIPS 算法不自动构成密码模块验证、第三方审计或完整协议安全证明。[6][7][8][9]

03 密码套件与编码

3 1 基线算法与成本

账户授权、共识投票与在线节点身份使用 ML-DSA-87，各角色使用独立密钥。账户标识采用 SHA3-384；交易、区块、状态与证据承诺采用 SHA3-512。基线不引入自定义签名聚合或格上门限签名；多方授权使用可独立验证的完整签名集合。[10][7]

用途	算法	标准编码长度
在线签名	ML-DSA-87	公钥 2592 B；展开私钥 4896 B；签名 4627 B
账户标识	SHA3-384	48 B
账本承诺	SHA3-512	64 B
传输 KEM 组件	ML-KEM-1024	公钥 1568 B；私钥 3168 B；密文 1568 B；共享秘密 32 B

用途	算法	标准编码长度
可选离线签名	SLH-DSA-SHAKE-256s	公钥 64 B；私钥 128 B；签名 29792 B

表 1 密码套件与编码。

表中三个公钥参数均属 NIST 类别 5。ML-DSA 的 32 B 密钥生成种子与 4896 B 展开私钥是不同存储形式；私钥备份必须标明格式、算法与版本。所有公钥、签名及 KEM 输入均按标准检查长度与编码，不接受预标准 Dilithium 或 Kyber 字节冒充 FIPS 对象。[6][7][8]

3 2 规范化与域分离

共识编码 C 即 ENC，采用 RFC 8949 第 4.2.1 节的受限确定 CBOR：仅使用按模式排列的确定长度数组、无符号整数与字节串，整数使用最短编码；禁止浮点数、不定长项、未知 tags 和非规范表示。集合语义数组按模式排序并拒绝重复；用途标签为 ASCII 字节串。账户交易签入版本、suite_id、auth_mode、G、auth_epoch、nonce 与有效期；投票按类型绑定集合 epoch、高度、轮次、步骤、区块及用于 BFT Time 的签名时间戳。解析器先检查长度、范围及数量上限，再验签。[11]

普通外层交易（含普通轮换）使用纯 ML-DSA 对完整 C(body) 签名，context 为 TX-v1；投票使用 VOTE-v1；独立的新键持有证明与密钥管理附属记录使用 KEY-v1，并绑定 G、账户、新策略摘要与生效高度。恢复专用封装使用 RECOVER-v1。以上 context 均为固定 ASCII 字节串，不另行发明预哈希签名变体。签名器默认采用 hedged 模式。哈希输入为含用途标签的 C 数组，Merkle 叶、内部节点和空树使用不同标签。[7]

3 3 传输配置与标准状态

节点传输指定 TLS 1.3、TLS_AES_256_GCM_SHA384 与 RFC 10024 的 SecP384r1MLKEM1024，严格沿用其密钥份额、组合顺序及 TLS 密钥计划，不能用 SHA3 替换握手内的 SHA384。该混合组已于 2026 年 8 月成为 Proposed Standard，但 IANA Recommended 为 N；它是本协议明确选择的配置，需要单独验证互操作性和资源成本。[12][13]

混合密钥协商不等于后量子身份认证。截止 2026-10-10，ML-DSA 的 X.509 编码已有 RFC 9881，TLS 用法仍为 draft-ietf-tls-mldsa-06。候选双向认证配置锁定该版本并以互操作测试及标准复核为发布门槛；TLS CertificateVerify 的 FIPS context 按草案置空，不能复用链上 context。协商失败时拒绝连接，禁止静默回退到经典认证；状态变更请求禁用 0-RTT。[14][15] 已知节点角色绑定的公钥必须来自独立可信配置或已验证的链上登记。允许自认证节点标识证明持钥，但它不赋予可信角色；若

使用 CA，完整认证签名路径及独立信任锚必须满足后量子身份配置，不得通过经典签名证书路径接受新的受信节点身份。

04 身份与密钥生命周期

4.1 稳定账户与授权策略

账户初始标识定义为 $A = \text{SHA3-384}(\text{C}([\text{ACCOUNT-v1}, G, P0]))$ ； $G = \text{SHA3-512}(\text{C}(\text{Genesis}))$ ，Genesis 不含派生字段 G。P0 是完整初始公钥策略，包含算法标识、公钥、授权阈值及启用的恢复配置。创建必须提供 P0 与相应持钥证明，重算 A 并检查策略合法性；同一 A 绑定不同 P0 时拒绝创建。账户状态保存当前 policy 与单调递增的 auth_epoch，轮换不改变 A。

账户密钥、验证者投票密钥、节点 TLS 身份和恢复密钥分离。多签按不同公钥计数，重复项不能增加权重；普通策略更新满足当前在线策略，恢复更新满足已登记恢复策略，两者都须证明新密钥持有者。auth_mode 在线编码为整数枚举 0（ordinary）或 1（recovery）。TLS 身份只认证通信对端，账户授权与验证者资格还须匹配链上策略和当前验证者集合。

4.2 生成保管与轮换

密钥生成使用满足所选参数要求的密码随机源；基线为独立角色生成独立随机种子，不把传统椭圆曲线 HD 派生直接套用到 ML-DSA。私钥采用加密、版本化备份并进行离线恢复演练，检查恢复公钥是否与登记值一致；日志、诊断接口与链上对象不得包含私钥或恢复种子。

轮换记录绑定旧 auth_epoch、新策略及生效高度；激活时再次匹配旧在线纪元并原子递增，此后旧纪元交易失效。待决恢复期间不得激活普通轮换，恢复成功后旧纪元预定轮换失效。历史策略保留用于验证已确认交易和共识证据，不能用轮换消除既有责任。KEM 临时密钥每次握手重新生成，用后尽快销毁；签名与解封装实现须处理侧信道、故障和秘密清除，并避免可观察的秘密相关分支。[9] 各高度先按确定规则处理到期恢复，再处理仍匹配旧纪元且未被冻结的普通轮换，然后执行该块交易。

4.3 可选离线恢复与密码迁移

账户可预先登记 SLH-DSA-SHAKE-256s 离线恢复公钥及 k-of-n 策略。恢复使用纯 SLH-DSA 与 RECOVER-v1，对完整 C(body) 收集 k 个不同完整签名，不需要旧在线签名；仅允许恢复、取消及已定义的恢复策略管理操作，禁止混入普通转账。公共 auth_epoch 与 nonce 在 recovery 模式分别匹配 recovery_epoch 与独立恢复序号；ordinary 模式匹配在线策略版本与在线序号。恢复绑定新策略及持钥证明，经过 D_recovery 后生效。未登记恢复的账户不存在协议级万能恢复钥。[8]

普通轮换不得改变已启用的恢复配置；恢复配置管理走 `recovery` 白名单并递增 `recovery_epoch`。独立恢复序号不随普通轮换重置。每账户最多一项待决恢复，期间锁定恢复策略，在取消或按请求到期激活前不得另行变更恢复公钥或阈值。提交与取消均消费下一恢复序号；取消签入待决请求摘要，解除冻结而不改在线策略。待决期间冻结普通在线授权的策略变更与扣款，恢复阈值已签的恢复费用及强制罚没照常处理。`D_recovery` 以区块数计，在确认时锁定，不能追溯缩短；自动激活不重复消费序号。成功后递增在线 `auth_epoch` 并解除冻结。恢复阈值拥有用户事先授予的最终替换权限。

算法标识、策略版本与生效高度由协议显式管理。新增套件先公布规范及测试向量，经治理确定迁移窗口，再停止旧套件的新授权；节点不得因未知算法而跳过验证。若旧算法已失去安全性，迁移不能仅依赖旧签名自证合法，必须采用事先授权的替代路径或按应急治理处理。该机制落实密码敏捷性，而不承诺自动修复未知密码分析突破。[2]

05 协议对象与账本承诺

5 1 确定编码与链标识

记 $C(x)$ 为 RFC 8949 第 4.2.1 节核心确定编码要求下的受限 CBOR 编码。共识对象采用定长数组、无符号整数与字节串；不允许浮点数、不定长项、重复映射键或未定义标签。所有用途标签均为规范固定的 ASCII 字节串。结构版本确定每个字段的位置与类型，未知版本或非最短整数编码必须拒绝。金额、序号和高度为 64 位无符号整数；中间计算使用足够宽度并在落盘前检查范围，不得溢出或回绕。[11]

创世清单包含协议版本、初始资产及授权记录、验证者集合、参数表、时间规则和治理权限。链标识 G 定义为该清单确定编码的 SHA3-512 摘要；清单本身不包含 G 或其他由 G 派生的字段，以避免自指。创世清单内的资产、权限和验证者引用使用清单索引或不依赖 G 的标签，不得引用尚未派生的账户标识。创世账户记录以初始策略和余额表示，账户标识在 G 确定后派生，再生成初始状态根。所有交易、投票、证明和升级对象都必须绑定 G ；网络显示名称相同不能替代链标识相同。创世还须绑定公开认购的最终接受额与分配清单、付款核验锚和初始自愿质押集合；清单仅引用不依赖 G 的初始策略与索引。

5 2 交易意图与授权封装

字段	类型	约束
<code>version</code> 、 <code>suite_id</code> 与 <code>chain_id</code>	整数与 64 字节	确定结构、密码配置及目标链

字段	类型	约束
expiry_height 与 sender_id	整数与 48 字节	限制有效高度并定位账户
auth_epoch 与 nonce	64 位整数	按 auth_mode 匹配相应策略版本及独立序号
fee_cap 与 compute_cap	64 位整数	限制费用加新增保证金的总扣款及执行预算
storage_cap 与 messages	整数与消息数组	限制新增状态及定义有序操作
tip	64 位整数	签名承诺的自愿小费，进入验证者奖励池；不保证优先纳入
auth_mode	模式整数	普通在线授权 = 0；已登记恢复授权 = 1

表 2 交易主体的十三个固定字段。完整交易封装为 [body, authorization]，授权必须遵守账户当前策略。

普通交易以 pure ML-DSA 对 C(body) 签名并使用 TX-v1 context；已登记的恢复请求、取消及恢复配置管理使用恢复策略与 RECOVER-v1 context 下的 pure SLH-DSA，不要求旧在线密钥签名。到期激活按已提交请求自动生效，不重复消费恢复序号。auth_mode、suite_id 与全部主体字段都在签名范围内。auth_epoch 按模式解释为在线策略版本或恢复策略版本，nonce 分别使用独立的在线或恢复序号。恢复模式只允许规范列明的恢复操作。授权封装记录算法、键标识与签名，按相应策略排序且禁止同一键重复计数。策略解析使用该交易执行前的顺序状态；因此同块内轮换、恢复冻结与后续交易的顺序影响有效性。G、策略版本、序号与有效高度共同隔离重放。

意图标识为 SHA3-512(C([用途标签, body])), 用于识别同一已签业务意图；完整封装另有摘要，覆盖包括授权在内的全部字节。随机化签名可能使相同主体产生不同封装，因此区块交易根必须承诺完整封装，不能仅承诺意图标识。收据使用意图标识、高度和交易索引定位，并通过序号消费规则避免同一意图重复执行。

5.3 区块头与证明对象

区块头至少承诺版本、G、高度、epoch、父区块标识、当前及下一高度验证者集合根、上一高度提交证书根、当前完整交易封装根、上一高度收据根、上一高度执行后状态根、参数根和协议时间。上一提交证书在集合交接时仍按上一高度集合验证。集合叶项必须同时覆盖验证者身份、算法、公钥和投票权，排序与重复项拒绝规则保持确定。区块标识对完整确定编码区块头求 SHA3-512；共识投票另绑定 height、round、step 与该标识，不允许把同一签名解释为另一轮次或步骤。

next_validator_root 仅指下一高度的有效集合：epoch 内等于当前根，边界前最后一个高度才指新集

合；提前批准的未来集合另由状态承诺保存。用于 BFT Time 的 precommit 时间戳必须属于完整 C(vote) 签名和证书承诺，表示为自 Unix 纪元起的 UTC 毫秒整数；其他步骤的对应保留字段为零。

承诺树对空树、叶节点和内部节点使用不同用途标签，并承诺节点类型、子树长度和左右顺序，避免结构歧义。第一版采用版本化的稀疏 Merkle 状态树，以 512 位状态键路径定位；叶值承诺完整键、值和命名空间。证明必须携带树版本、键、值或不存在声明，以及由位图和兄弟摘要组成的路径，验证器限制最大路径深度和总字节数。具体节点编码与空子树常量必须随测试向量冻结；树版本改变属于协议升级。

索引服务可加速查询，但验证器只信任已最终提交的头、正确的集合证明及匹配的状态证明。区块交易根认证有序封装，不独立证明应用结果；收据必须覆盖状态码、实际收费、资源使用与事件摘要。对高度 h 执行后状态或收据的查询，应明确所用证明锚定于 $h+1$ 的最终头；高度 h 的交易封装成员证明可直接锚定于高度 h 的最终头，避免将未承诺的执行结果提前报告为可验证事实。

06 共识与最终性

6.1 基线与故障模型

本协议拟采用 Tendermint 风格的加权 BFT，以 Buchman、Kwon 与 Milosevic 2018 年论文 Algorithm 1 为共识精化起点，不提出新的共识算法。[16] 每个高度的验证者集合固定，总投票权为 W ，拜占庭投票权 B 必须满足 $B < W/3$ ；有效法定人数严格满足 $Q > 2W/3$ ，不能把恰好三分之二计作通过。权重运算须使用有界整数并检查溢出。

$$B < W/3 \quad Q > 2W/3$$

安全性还依赖签名与承诺安全、诚实节点执行锁定规则和确定性验证、故障恢复不丢失签名状态。活性采用部分同步模型：未知 GST 之后诚实节点间通信最终可靠且有界，并有足够诚实在线投票权与适当超时。[17] 网络分区可能使链停顿；协议不得因节点离线降低阈值。区块最终性不等于任意交易必被及时纳入。

6.2 投票、锁定与轮次推进

每轮包含 proposal、prevote 和 precommit，提议者按确定的加权轮转规则产生。节点保存 lockedValue/lockedRound 与 validValue/validRound。已锁定节点只可为相同区块投 prevote，或在核验提议所指历史轮次的同块 $> 2W/3$ prevote 证明后，按 $\text{validRound} \geq \text{lockedRound}$ 且

validRound < 当前轮的规则改投。当前轮形成同块 **prevote** 法定人数时锁定并 **precommit**；同高度同轮同块的 $>2W/3$ **precommit** 才构成提交证书。

上述历史 **prevote** 证明即本设计所称 **polka**。完整状态机必须保留基线算法的 **nil** 投票、超时与轮次追赶规则；超时本身不能清除锁定。投票签名绑定链标识、**epoch**、高度、轮次、步骤、区块标识及 **precommit** 时间戳，并采用 **ML-DSA-87** 用途隔离。锁定及有效轮次状态须持久保存或从不可回滚日志安全重建。签名器在发出签名前持久保存防双签记录；恢复或切换设备不得回滚该记录。[16]

6.3 Epoch 交接与资源约束

epoch 内冻结集合。下一集合清单包含规范排序的完整公钥、权重、算法版本及激活高度，并由旧集合提前最终承诺；公告提前量与 **epoch** 长度是链参数。截止高度前无有效清单则下一 **epoch** 继承当前集合，规则对所有节点一致。激活高度开始仅使用新集合；验证前一高度的证书仍使用旧集合。新节点负责提前同步，未就绪不得擅自改激活高度。每一集合都需满足故障假设，任意集合更替的正确性不能由单高度论文直接推出。

提交证书保留逐验证者 **ML-DSA-87** 签名，基线不假定可用的聚合签名。验证者数量、区块字节数、证书大小、待验签队列与每连接流量须设置协调限额，并测量多轮和恢复时的开销。上线前必须完成加权阈值、持久锁定、**epoch** 交接及密码替换的精细化论证、模型检查和故障测试；引用既有证明不代表本协议或实现已获证明，也不产生实测 **TPS**。

07 状态机与交易生命周期

7.1 确定性状态转换

状态机以相同初始状态和相同有序输入产生相同结果。[18] 交易采用规范编码，签名绑定协议版本、链标识、账户、策略版本、**nonce**、有效期、计算预算 **compute_cap**、存储预算 **storage_cap**、费用上限及完整业务消息；区块按确定顺序执行。交易与状态承诺使用 **SHA3-512**。整数宽度、舍入、错误码、资源计量及存储顺序必须由规范定义，执行不得读取本地墙钟、外部网络或未承诺的随机数。

时间输入仅取已按共识规则验证的区块 **time**。基线采用固定版本的 **BFT Time**：从前一高度提交证书的已签名时间戳按投票权重加权中位数，首块取 **Genesis** 时间；校验单调性并明确诚实时钟误差假设。[19] 用于此计算的前一提交证书数据须纳入区块承诺。此规则及轻客户端时间校验都需要独立测试。**precommit** 的 **UTC** 毫秒时间戳在投票签名范围内。中位数计算先按时间戳及验证者标识排序，取累计权重严格超过该证书总权重一半的首个时间戳；诚实签名者的时间戳须晚于上一块时间并满足已规定时钟误差界。

7.2 纳入、执行与失败语义

阶段	确定的含义
本地接收	检查格式、签名与资源限制；mempool 接收不构成承诺。
提议验证	按区块顺序检查授权、nonce、有效期与费用准备；无效交易使提议无效。
共识提交	完整有效区块取得提交证书，交易顺序最终确定。
执行结算	确定性执行，生成成功或失败收据，结算费用与 nonce。
结果证明	等待 $h+1$ 最终头承诺高度 h 的状态与收据。

表 3 状态机与交易生命周期。

提议验证必须按最终执行相同规则在隔离状态中顺序试执行，或执行可证明等价的验证，纳入前序交易的写集、失败回滚、费用、序号及策略变化，不发布外部效果。格式、授权、nonce 或费用准备无效的交易不能合法入块，不能向被冒用账户收费。合法纳入后发生业务失败或 out-of-gas 时，仅回滚业务写集，保留 nonce 消耗及已计量费用；每笔交易的多条业务消息一并成功或回滚。费用预留、价格、退款和 out-of-gas 上限须确定化，实际扣费不得超过签名授权的费用上限。执行失败时新增业务状态保证金 $D=0$ ，其预留全部退还；暂记的旧状态删除退款也回滚，只保留手续费 F 与相应序号消费。

7.3 结果承诺与数据可用性

Header _{h} 承诺当前完整交易 envelope 的 tx_root，以及 previous_state_root($S_{\{h-1\}}$) 与 previous_receipt_root($R_{\{h-1\}}$)。区块 h 最终提交后执行得到 S_h 、 R_h ，其根由 Header _{$\{h+1\}$} 最终承诺；空块也推进此过程。因此 h 的入块最终性与 $h+1$ 的结果证明可验证性必须在接口和钱包中分别呈现。收据固定包含意图标识、执行高度、交易索引、状态、资源使用、实际费用与事件摘要，不能把未承诺日志当作状态证明。

诚实验证者取得并验证完整区块后方可为其 prevote；基线不采用分片或数据可用性抽样。[20] 状态快照须以已最终承诺的根校验。区块、收据、证据和证明的保存期限、冗余服务及检索测试应公开，并覆盖信任期、解绑定期和证据提交窗口。一次签名证书不能保证历史数据永久可取；缺失数据时节点暂停相应验证，不推断业务成功。

08 轻客户端与跨链边界

8.1 可信起点与长期离线

轻客户端以经独立渠道确认的链标识和可信检查点启动，检查点绑定高度、区块标识、时间及验证者集合承诺。仅由陌生服务器提供的自洽头链不能建立初始信任。信任期 T 必须小于解绑定期 U ，并为时钟误差、发现攻击和提交证据留出裕量。[21] 验证者退出后旧密钥仍可能签名，后量子算法不消除长程攻击与弱主观性。

超过信任期的客户端不得凭累计签名数量或最长历史自动恢复，应取得新的独立可信检查点。持续更新也要求信任期内相关集合满足规定的诚实假设；押金惩罚是一项激励和恢复机制，不能代替密码或协议假设。出现冲突的最终头时，客户端冻结受影响路径并保存可核验证据，恢复依据另行公布的治理程序。

8.2 头部验证与证明可获得性

基线采用逐高度验证：核验链标识、版本、父链接、时间、集合承诺，以及对应集合对同轮同块严格 $>2W/3$ 的签名；重复签名者不能重复计权。**epoch** 边界先验证旧集合最终承诺的清单，再切换验签集合。单凭新集合自签的证书不能证明其有权接任。跳跃或二分验证须另行规定可信集合的签名重叠与失败处理，不能从逐高度模式自行推导。[21]

业务验证还需交易、状态或收据的成员证明；不存在性必须使用已规定树结构的非成员证明。证明须绑定键、路径、根和执行高度， h 的状态与收据证明锚定 $h+1$ 最终头。头部有效与证明可获得是不同条件：服务器超时或拒绝提供证明只表示当前无法验证，不表示记录不存在。客户端可向多个独立服务请求同一承诺的证明。

8.3 跨链验证与升级边界

跨链为单独的安全协议，不因底层采用后量子签名而自动成立。接收链必须验证发送链最终头与其承诺下的业务证明，并绑定双方链标识、通道、包序号、接收方及超时条件，执行防重放与确定性确认。中继者仅传输数据，其签名不能替代源链证明。客户端过期、发现冲突或数据不可用时暂停相关跨链处理。[22]

双方需分别迁移账户授权、验证者证书、节点身份、传输认证及治理升级信任根，并明确 **ML-DSA-87**、**SHA3-512** 与证明编码的版本。**ICS-007** 提供信任期、集合更新和冲突冻结的参考，但现有

客户端不能被假定直接兼容本协议。[22] 更换算法、树结构、验证器或恢复检查点均须专门的升级证明和测试；跨链托管、经济安全及外部链失陷风险另行评估。

09 资源与性能经济模型

9.1 资源预算与解析场景

容量规划分别约束序列化字节、验签工作、执行计算和状态增长。ML-DSA-87 公钥为 2592 字节，签名为 4627 字节；交易若同时携带两者，仅这两项即为 7219 字节，尚未计入交易正文和编码开销。[7] 哈希承诺不能替代签名，公钥缓存也不能代替验证账户与公钥的绑定。标准 ML-DSA 未提供本协议可直接采用的聚合签名；并行或批量调度仍须保持每个签名的验证语义，任何减少密码学检查的方案均须单独证明与评审。

以下仅作未实测的解析场景：假设 100 个验证者、每 5 秒一块、每份提交证明包含 100 个签名，则原始签名为 462700 字节/块，每日 7995456000 字节，约 8.00 GB（十进制）。这不是带宽、存储或 TPS 承诺；实际提交门槛按严格超过三分之二的投票权计算，签名数不固定。公钥是否重复、提案传播、投票轮次、重传、区块索引和副本数须另行计量。

9.2 确定性计费与准入控制

拟议费用为 $F_i = [p_B B_i + p_V V_i + p_G G_i] + tip_i$ ； B 为完整交易封装的规范编码字节， V 为经校准的验签工作单位， G 为排除已计费验签工作的执行单位。 V 与 G 按确定性计量表累计，不以本机运行时间计费。价格由共同父状态确定，以公共分母 q 表示有理数，合计后统一向上取整；乘加须有界并检查溢出。交易主体签名覆盖 tip 与 fee_cap ； fee_cap 为支付人授权的最大协议扣款，覆盖手续费 F 与新增状态保证金 D 。协议先预留 fee_cap ，结算必须满足 $F + D \leq fee_cap$ ，并退还未用预留额；转账等业务金额在预留后另行检查可用余额。执行失败仍支付已消耗资源，应用写入回滚；通过认证并进入执行的交易消耗序号。解析或认证失败的交易不得进入区块。

$$F_i = \text{ceil} \left(p_B B_i + p_V V_i + p_G G_i \right) + tip_i$$

新增持久状态另锁定保证金 $D_i = p_S \cdot \sum_e \max(\Delta S_{i,e}, 0)$ ，逐条目计算正增量后求和，禁止用删除其他条目抵扣；计入托管余额而非手续费收入。状态条目记录付款归属，删除时只退还实际锁定额； $storage_cap$ 限制逐条目正增量之和，以字节计；保证金随费用共同受 fee_cap 约束，不另设保证金金额上限字段。相同区块内创建再删除状态，仍须支付字节和执行费用，不得以净增长为零免除计算与写入计量。区块须同时满足字节、验签、执行和状态增长上限；价格不能代替硬上限。未上链的恶

意输入无法靠链上收费约束，节点还须有长度检查、连接配额、有界队列与本地限流。费率与保证金参数须经成本测量冻结，不承诺其覆盖无限期归档。 p_S 限定为每字节的非负整数最小资产单位；退款始终以条目实际托管的整数额为准。失败交易不保留新增业务状态保证金，也不兑现暂记的旧状态删除退款。

10 原生资产经济与治理

10.1 设计目标与供给单位

经济模型服务于原生结算、资源付费、质押责任和协议维护。长期价值形成取决于用户是否持续购买这些服务，以及网络是否可靠、安全且便于集成。总量、单价与市值分别描述单位数量、市场成交价格 and 价格乘以供给的估值口径；把 1 亿枚改为 1000 万枚不会凭空增加网络价值。9 位小数保留小额结算能力，费用仍以整数最小单位计算。抗量子安全来自密码与协议，不来自某个发行数字。

本版采用累计发行硬上限 $S_{\max} = 10,000,000$ 枚；1 枚 = 10^9 原子单位，因此 $S_{\max} = 10^{16}$ 原子单位，小于 `uint64` 上限。累计发行计数 C_h 包括创世发行和此后所有新增发行，即使资产后来被销毁也不回减。现存总量 $M_h = C_h - B_h$ ，其中 B_h 为累计销毁量。任何发行均须同时满足已公开日程和 $C_h \leq S_{\max}$ ；销毁不产生再次发行权。普通治理不得提高上限、重置计数或从已铸造储备再记一次发行。

$$S_{\max} = 10^{16} \quad M_h = C_h - B_h \quad 0 \leq M_h \leq C_h \leq S_{\max}$$

本文保留单一原生资产用于手续费、质押与结算，并采用研究中可持续参与、去中心化、稳定性与可实施性的区分。[26] 75% 与 25% 是明确的评审配置，不是大学研究者证明的最优比例。其选择依据是：在 20 个参考年的曲线尺度下，将首参考年新增发行控制在创世分配的 2% 以内，同时在所比较的 5 个百分点梯度中尽量保留安全额度。2% 是本设计的偏好约束，不是价格稳定规律；验证者成本检验不通过时，必须重新评审参数并延后启动。

10.2 公开分配与零专属预留

用途	份额与数量	归属及约束
公开初始分配	75% 7,500,000 枚	仅在足额成交且发布条件满足时创世发行；全部映射到已验证的参与者后量子账户。
长期 PoS 安全发行	25% 2,500,000 枚	创世未发行；按高度进入独立奖励池。额度没有所有者、质押权或投票权。
创始人 贡献者 顾问 机构 基金会	0% 专属免费预留	无内部折价、保底配额或协议开发者抽成；参与公开认购须遵守相同规则。

表 4 公开分配与安全发行。零预留不等于无人集中持币，也不等于项目组织没有销售收入。

所有初始 750 万枚必须在创世清单中直接归属已完成公开分配的参与者，不设待售、待认领或项目方代持池。持有人可以自愿质押；未质押余额没有另设锁仓释放期。认购未足额、清算不能完整交付或发布条件未满足时，本配置整批取消并进入退款程序，不以少量参与者部分启动。不得把未售份额转入团队、金库或新增奖励额度。第 11 章定义公开启动与资金边界。

贡献者可以按同样条件购买、质押并获得履职奖励，也可以领取公开合同约定的研发服务报酬，但贡献者身份不产生代币发行权。研发资助与协议发行分开；启动前工作依靠已落实的前置资金，启动后预算支付、外部资助和自愿捐赠均须披露控制与关联关系。Bitcoin 白皮书的区块奖励没有开发者身份预留；Brink 的捐赠资助说明外部研发报酬与协议发行可以分离。[27][31]

10.3 长期发行与稀释口径

日程使用创世后已完成高度 h ，创世为 $h=0$ 。 H_{year} 是创世前根据测量冻结的正整数参考年高度跨度，不保证自然年历时。停链不推进高度，不按墙钟补发。令 $H_{\text{tau}}=20H_{\text{year}}$ ， $R=2.5 \times 10^{15}$ 原子单位，创世累计发行 $C_0=7.5 \times 10^{15}$ 。高度 $h \geq 1$ 的 I_h 只能发行一次并进入奖励池， $C_h=C_0+A(h)$ 。 H_{year} 的合法范围为 1 至 $\text{floor}((2^{64}-1)/20)$ 。乘法与 $h+H_{\text{tau}}$ 使用至少 128 位的检查运算。

$$A(h) = \text{floor}\left(\frac{R \cdot h}{h + H_{\text{tau}}}\right) \quad I_h = A(h) - A(h-1)$$

未取整的边际发行平滑递减，没有预定的减半跳变；整数逐高度增量可能相邻波动或为零。20 个参考年时发行安全额度的一半，并非补贴结束。任意有限高度均有 $A(h) < R$ ，残余原子单位可能永远不发行；1000 万是上限，不承诺最终补齐。销毁、罚没转移、奖励领取和委托都不得恢复已用额度。

参考年	累计安全发行	累计已发行 C
0	0.000	7,500,000.000
1	119,047.619	7,619,047.619
2	227,272.727	7,727,272.727
5	500,000.000	8,000,000.000
8	714,285.714	8,214,285.714
20	1,250,000.000	8,750,000.000
40	1,666,666.667	9,166,666.667
100	2,083,333.333	9,583,333.333

表 5 无销毁情景，单位为枚，显示值四舍五入至三位小数；协议计算始终在原子单位向下取整。创世分配全部交付，奖励池余额仍不必然进入市场流通。

首参考年新增为 119,047.619047619 枚，新增除以创世发行约为 1.587302%。不质押且余额不变的持有人，其占已发行供给的份额下降约 1.5625%，计算为 $1 - C_0/C_1$ ；这不是币价变化预测。口径必须分别报告累计发行、已分配余额、质押及退出中余额、奖励池与可转移余额。不能把最大总量当作分母，也不能通过预铸但不交付的库存压低公开的稀释率。

在相同曲线尺度下，首年新增与创世发行之比约为 $(1-g)/(21g)$ ，其中 g 是公开创世份额。2% 偏好对应 g 至少约 70.4225%；75% 是下表满足偏好的最小 5 个百分点梯度配置，且比 80% 配置多保留 25% 的安全额度。这个比较只解释选择过程，不证明真实用户偏好或安全预算充足。

公开与安全份额	首年安全发行 枚	首年发行增幅
40/60	285,714.286	7.142857%
60/40	190,476.190	3.174603%
70/30	142,857.143	2.040816%
75/25	119,047.619	1.587302%
80/20	95,238.095	1.190476%

表 6 分配敏感性，固定 1000 万上限与 20 个参考年曲线尺度。75 与 25 为评审配置，其他行仅作参考。

同一 250 万安全额度下，把曲线尺度改为 10、20、40 个参考年，首年新增分别约为 227,272.727、119,047.619、60,975.610 枚。较慢发行会降低早期验证收入，较快发行增加持有人稀释。生产 H_{year} 、资源容量与运行成本须一同校准，不能以少发币本身证明安全或增长。

10.4 手续费与安全奖励结算

第 9 章定义的全部手续费 F_i ，包括基础费与 tip_i ，初始均进入验证者奖励池；协议开发者抽成、公共金库手续费抽成与默认手续费销毁均为零。状态保证金 D 保持独立托管，不属于手续费。小费进入公共验证者奖励池，不根据当前未承诺的提案轮次指定个人收款者。公共研发支出使用第 11 章公开预算或外部自愿资助，不从共识手续费自动取得份额。

安全补贴进入奖励池后即属于已发行资产。奖励必须依据共同承诺的数据、固定集合与权重快照及可验证参与规则结算；禁止固定“每节点”奖励或依本地接收时间发放。第 h 高度执行不得依赖尚未被共同承诺的 h 高度提交证书。若使用上一高度证书，须绑定对应历史验证者集合，并证明提议者选择证书子集不能任意剥夺诚实参与者奖励；不能把“证书中恰好出现”直接等同于全部合格工作。参与证明、委托分账、佣金上限、罚没顺序与领取期限须在创世前完成字节级规范及偏置测试。

未赚取、舍入或到期未领取的份额留在专用奖励池，不能重新计作未发行额度，不能由后续参与者自动追溯补领，也不能普通治理改拨贡献者资金。池的再分配条件必须预先规范并保持可审计；仅本节函数产生新增发行。质押奖励取决于活跃权重、参与、实际手续费、补贴和佣金，不承诺固定 APR ，也不以增发维持目标币价。减少验证者手续费份额、引入销毁或改变本发行函数须作为经济规则的新版本重新审查安全预算，不能借普通预算转账实施。

仅持币不会自动取得安全奖励。持有人须登记后量子验证身份并自愿锁币，或按已冻结规则委托给验证者；委托费用、退出等待和罚没责任须事先说明。奖励由全节点根据固定权益快照、已承诺的履职证据和确定公式复算，不由项目方审批。若所有参与者履职相同，按有效权重分配的示例中，100 枚可分配奖励、全网 10,000 有效权重和个人 100 权重对应 1 枚；该示例不是固定收益承诺，也不是未冻结的生产结算规范。

10.5 资产守恒与验证者责任

每高度满足 $M_h = M_{(h-1)} + I_h - \text{burn}_h$ 。 M 为互斥的可转移余额、质押、退出中余额、状态保证金和协议池之和。可领取负债须由池资产足额覆盖，不能重复加到资产总量。转账、委托和罚没转移不创造资产；罚没销毁须单独记录。创世须冻结罚没比例、证据与退出窗口，以及每个池的授权和会计规则。

质押赋予投票权与可执行责任，不证明某个法币攻击成本，也不替代 BFT 假设。双签和缺席分别定义，网络分区不能自动认定为双签。按实际管理、密钥、资金、委托与共同故障域检查集中度；地址数量、节点数量和每地址限额都不证明独立控制。未发行额度没有质押权或投票权。团队按公开条件买到的币仍须按共同控制合并披露。

10 6 运营预算与采用条件

安全收入来自当期发行和实际手续费，按委托与佣金规则分配。必要的运营检查是：验证者扣除委托人分成后可留存的收入，在明确币价和费用情景下能否覆盖独立运营成本及风险补偿。它不是完整的攻击成本证明。第 20、40、100 个参考年的当年新增分别约为 32,051.282、14,124.294、3,501.401 枚；这些是相邻参考年累计整数发行之差，不是当年的固定质押 APR。

发布前须压力测试近零手续费、低需求、币价下降 80%、成本翻倍、委托集中与相关退出，并比较 70/30、75/25、80/20 及 10、20、40 个参考年曲线尺度。尚未有生产币价或真实运营数据，本版不声称 75/25 已满足该检验。若预算不足，应在创世前降低资源成本或公开修订经济配置，并延后启动；不能静默突破上限、补发内部额度或降低严格超过三分之二的提交阈值。

固定累计上限与趋零补贴要求长期有持续付费需求；不能同时保证固定供应、永久固定质押收益和不需要费用收入。采用指标包括扣除补贴与可识别自交易后的费用、成功结算、钱包与托管集成、独立活跃权重及运营净收入。安全算法、供应数字、免费认领和高名义收益都不自动带来买入需求。治理不设价格下限、保底回购或 BTC 固定兑换目标。

10 7 退出、证据与轻客户端信任

退出申请不得立即解除历史签名责任。以最后可归责签名为共同起点，设计须保证

$T_trust + T_check + T_report + T_process + \Delta_clock < T_slashable$ ；证据可提交期限和保存期限须覆盖对应检查、报告与处理窗口。退出资金在适用证据窗口内保持可罚没，及时提交的待决证据不得因退出到期而失效；责任结清后方可释放。高度期限与时间期限须同时建模，停链后的处理规则须明确。轻客户端信任过期须取得新的可信检查点，不得仅凭旧密钥签名延长信任。[21]

10 8 权限分离与安全边界

提案、投票、技术审查和延时执行分离；紧急权限仅能在预定范围及期限内暂停特定业务，须公开原因并自动到期，不得任意增发、没收余额或改写已最终确定的历史。普通参数治理不得解除严格超过三分之二提交门槛、完整验签、重放保护或密码算法最低要求。改变这些边界须作为新协议版本重新论证、审查和明确接受。算法替换需版本化注册、迁移窗口及降级拒绝规则。[2] 验证者独立性按管理权限、密钥控制、云平台及网络故障域评估，不能用节点数量代替。

11 公开启动与 BTC 换入路径

11.1 原生资产与兑换边界

本链采用 PoS，不以 PoW 分发作为启动前提。首批代币通过下述公开初始分配取得；上线后，新用户可向已有持有人按市场价格购买，再选择持有或质押。协议不保管所有市场交易中的 BTC，不为上线后市场交易设置固定 BTC 兑换率，不承诺上市或随时能成交，也不为原生币提供 BTC 储备和赎回债权。BTC 支付购买与后量子余额交付是不同链上的事件，不能描述为已实现的原子跨链兑换。

BTC 快照免费认领与本方案不同：领取人可以继续持有全部 BTC，因而不能称为资本迁移。按历史余额分配还会继承集中与托管控制，并面临遗失密钥、未认领与旧签名风险。[32] 本版不预留快照空投池。包装 BTC 也不改变 Bitcoin 链上抵押物的授权机制；本链的后量子签名不能替该抵押物提供保护。

11.2 统一价格与预算封顶

评审配置在一个充分预告的窗口内公开分配全部 750 万枚，建议参与窗口至少 30 日并留出至少 14 日清单复核期；实际 UTC 截止、确认锚与冲突处理在启动清单冻结。价格由公开审核的后续研发、审计、集成与基础服务成本预算形成，而非预测市值。用 L_BTC 表示本批次接受的 BTC 总额上限，以聪计； $J_0=7.5\times 10^{15}$ 为初始原子单位，公开统一价为 L_BTC/J_0 聪每原子单位。 L_BTC 数值须有实际预算依据，本白皮书不虚构该预算。

这是固定价格认购，不是价格发现拍卖。有效入金合计 D_BTC 低于 L_BTC 时整批取消。达到或超过时，先按入金比例向下取整并以最大余数、稳定订单标识打破并列，确定各订单接受聪 b_i ，保证总和为 L_BTC 且不超过各自入金；退款为入金减 b_i 。再按 b_i/L_BTC 分配 J_0 ，以同样的确定尾差规则完整分配原子单位； $b_i=0$ 的订单不获币并全额退款。统一价只受已披露的整数舍入误差影响。不得先到先得、内部折价或暗中保留份额；资金较多者仍可能取得更多，按地址限额不能消除拆分或共同控制。该尾差规则不抗拆单；须公开订单上限、最小申请额及相对尾差上界并测试，不能把单笔小于一聪误写为总体公平保证。

11.3 收款 订单与创世映射

付款前，订单必须绑定 `launch_id`、`batch_id`、唯一 `nonce`、后量子公钥及持钥证明、用户明确选择的 BTC 退款脚本和条款版本。实际入金以收款 `outpoint`、金额、Bitcoin 确认锚和去重记录核实。BIP 322 消息签名不证明某人发送过历史交易，也不永久证明资金控制，不能替代入金记录。[30] 不要求提交助记词或私钥，退款不能默认发回输入地址，因为输入可能来自交易所、多方或找零结构。

公开可重算数据必须生成一致的接受额、退款额、参与者余额、授权策略和创世分配根。参与者确认目的账户并单独选择质押、委托或保持可转移余额；不能将购买等同于强制委托给团队验证者。创世清单包含完整初始权益集合、共识公钥与真实控制关系披露。两个独立实现必须重算相同结果；无法验证或完整交付则不启动。认购阶段绑定初始授权策略与不依赖 **G** 的索引；最终 **G** 确定后再派生账户标识，避免创世循环定义。

11.4 BTC 受托与研发资金

销售收入不是代币抵押储备。启动清单必须列明接收组织、受托人、签名门限、收款脚本描述符、预算项目、受益人与关联方、里程碑、费用来源及剩余资金处置。项目组织或开发服务提供者可能获得收入；零团队代币预留不能被宣传为零经济利益。共同控制与实际报酬须持续披露，且资金管理不赋予本链铸币、改账或冻结用户余额的权限。

本方案依赖受托资金保管。**Bitcoin** 脚本不会自行判断本链是否正确启动，受托人仍可能合谋、失联或错误放款；多签不消除该信任边界。募集本金在启动成功条件满足前不得用于支出，前置开发与审计依靠独立前置资金。成功后按已公布里程碑分批释放，未用款的退款或其他处置不得事后改变。未经预算、托管、争议处理与责任条款冻结，不得开始收款。

11.5 失败退款与交付顺序

启动清单须将入金、清算、异议、分配确认、首批最终区块、资金释放和失败退款写成完整状态机，定义截止冲突、深度重组与停链处理。同一订单不能同时取得有效交付和有效失败退款。成功标准必须包含可独立核验的创世与最终性证据；这些证据供受托流程核验，不意味着 **Bitcoin** 自动强制执行跨链成功条件。启动前只有条件性分配凭证，不是可转移主网余额。达到已冻结的成功标准后进入运行阶段；之后停链或价格变化不重新触发初始认购本金退款。

若整批失败，应退还已到账本金；原始发送交易的矿工费不是到账本金。退款矿工费须由另行预存的费用准备金承担；若采用扣费退款，项目、计算方式和上限必须在付款前明示，不得同时宣称无条件全额退款。本版不设隐含扣费。退款准备金、超额退款、尘埃限制和受托人故障都必须实测；准备金不足或无法兑现承诺时不得进入募集。

11.6 PoS 启动与量子风险窗口

足额认购不证明有足够安全权益。主网须单独核验实际自愿锁定的权益、验证密钥、委托与运营准备，并审查共同控制、托管和故障域。在相关集合拜占庭权重严格低于三分之一的假设下，仍需严格

超过三分之二权重提交；仅有少量同一控制者的地址不满足分散的启动目标。独立性审查不能证明没有隐蔽合谋，阈值也不能因人少而降低。[32]

BTC 入金和兑换的 Bitcoin 一侧仍依赖当时的 Bitcoin 授权安全。BIP 360 的 P2MR 草案仅缓解长暴露风险，本身不提供完整短暴露防护；BIP 361 迁移草案也不等于已部署的升级。[28][29] 若已出现可破坏相关旧签名的量子攻击，必须停止接受依赖这些授权的新入金并启动已公布的暂停与退款程序。不能把本方案宣传为危机发生后仍可无风险抢救 BTC 的通道。执行退款仍取决于当时 Bitcoin 的安全、可用性及受托资金可支配性。

12 密码演进与协议升级

12.1 版本化能力与确定激活

协议维护独立的结构版本、密码套件版本、账户策略版本、状态树版本和传输配置版本。算法标识必须对应完整参数集与编码，不能只写“后量子签名”。升级提案承诺新规范摘要、激活高度、允许的旧对象验证窗口、迁移计划和资源上限。治理通过并不立即改变有效性规则；所有诚实节点按同一已提交高度激活，不依据本地安装时间决定协议版本。[2]

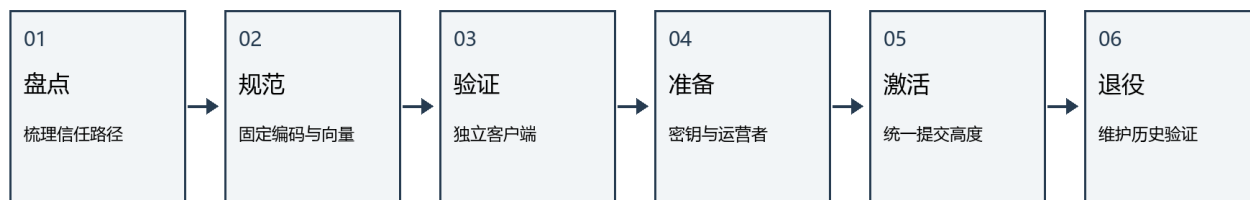


图 2 协议演进顺序。每一步均有可检查的输入、产物与拒绝条件。

迁移依次完成密码资产清单、字节级规范及向量、双实现验证、账户与验证者准备、确定激活、旧授权退役和历史验证维护。兼容期可同时识别旧、新格式，但任何特定高度的授权规则必须唯一。双签过渡若采用 AND 组合，必须两份签名均通过；将其改成 OR 会引入较弱算法可单独授权的路径，必须被视为不同安全设计。基线不要求常规交易叠加经典签名。

12.2 账户与验证者迁移

普通账户轮换以现行有效在线策略授权新策略，并提升 `auth_epoch`；事务对新策略摘要和生效高度作出签名承诺。已登记的延迟恢复策略可在原密钥失效时按其原定权限操作。若某类签名已被攻击者

实际伪造，事后继续用该类签名证明所有权无法恢复失去的信任。因此，应在风险暴露前完成恢复登记与迁移，而不是依赖治理人员临时判断资产归属。

验证者密钥替换必须绑定同一质押身份、激活边界与新集合承诺，旧密钥不得在边界后继续获得新高度投票资格。签名器的防双签状态随密钥和高度迁移；恢复备份不能让两个设备同时签署冲突消息。轻客户端同时更新集合、算法白名单和历史验证规则，不允许出现全节点可验证而客户端无法验证的静默分裂。

12.3 紧急处置与历史完整性

紧急暂停权限必须预先列明对象、最长持续时间和恢复程序，限于停止指定危险操作或进入只读模式，不能伪造用户授权或改写已最终提交的历史。若模型假设已被破坏，社会协调恢复必须以独立说明记录受影响高度、检查点、资产处理规则和分歧，而不能继续使用“原链无条件安全”的表述。任何恢复都必须保留证据以便事后审查。

归档节点保留必要旧算法验证器、版本说明和承诺数据，但“能够解析旧签名”与“旧签名仍具有当前安全性”不同。长期历史可信度来自及时接受的检查点、当时有效的共识证据及明确的迁移链条。协议应公开每次退役决定及其影响，使审查者能够识别依赖已失效假设的历史区段。

13 验证计划与发布条件

13.1 协议模型与实现验证

每次候选发布固定协议版本、威胁模型、源码与构建摘要。形式化模型检查加权法定人数交集、锁定规则、验证者变更、账户轮换、重放保护及资产守恒；活性须声明部分同步和足够诚实在线投票权假设。模型检查与证明的结论限于其模型及假设，不能自动归于实现。^[23]至少两套独立实现进行编码、状态转移和密码验证差分；使用标准测试向量，模糊测试畸形长度、非规范编码、整数边界、未知版本与错误签名，并保留最小失败样例。

故障试验覆盖延迟、丢包、分区、时钟偏差、崩溃重启、数据库恢复和签名器防双签状态恢复，并覆盖密钥轮换、过期检查点及伪造快照。按投票权分别配置离线和恶意比例；低于安全阈值时检验不分叉，在不具备足够在线法定人数时检验安全停顿，恢复同步后检验恢复进展。接近或超过拜占庭阈值的试验用于呈现保证边界，不声称协议仍保持无条件安全。

13 2 可复核的性能测量

借鉴 BLOCKBENCH 的分层评估方法，分别测量密码、网络、执行和存储，再测端到端表现。[24] 报告硬件、软件版本、地理分布、运营控制域、负载组成、预热及测量区间。成功 TPS 为区间内最终确定且执行成功的交易数除以秒数；已最终确定的失败交易 TPS 另列，同时报告提交率、准入率、超时和积压。延迟从首次提交至最终确定，报告 p50/p95/p99 及超时比例，失败交易单列；不得静默删除超时。开放与闭环负载分开，跨机器时间戳说明校时误差，原始数据和脚本可复核。 本协议在 h+1 区块头承诺 h 后的执行状态与收据，故分别报告 h 的入块最终确定时延，以及获得 h+1 承诺和有效证明的状态可验证时延；收到 RPC 成功响应不能替代任一指标。

$$TPS_{success} = N_{finalized, success} / \Delta t$$

13 3 逐级发布门槛

阶段	必须完成的证据
协议冻结	编码与状态规则完整；模型假设、Genesis 参数及迁移路径可审查；不得留有影响互操作性的未决项。
独立测试网	由独立控制域运营；差分、向量、模糊与故障测试通过；发布失败结果、恢复记录及完整测量方法。
生产候选	独立密码与协议评审完成，阻断项已修复并复核；依赖锁定、SBOM、可复现构建、签名发布及密钥恢复演练完成。
上线放行	满足预先公布的资源、时延和恢复目标；TLS 认证候选规范完成定版及互操作验证；重大未决风险有明确处理结论。

表 7 验证计划与发布条件。

供应链与发布流程以 SSDF 组织可追溯证据。[25] 引用研究、通过测试向量或使用标准算法不构成审计、认证或研究机构背书。上述表格是须完成的条件，性能结果、外部评审结论和生产就绪声明只能在相应证据公开后填写。

经济发布条件包括：独立复算累计上限和发行表；验证奖励池与领取债权不重复计数、销毁不补发行额度、未发行额度无投票权且无内部预留；验证整数边界、证据去重和证书选择偏置；披露分发受益人与关联控制；完成低手续费及低价格下的运营预算分析。模型曲线可由整数算术复算，不表示需求、运营盈利或未来币价已经验证。

13.4 公开启动的发布条件

公开启动发布材料必须包含实际成本预算与 BTC 上限、固定认购价、参与窗口、受托与退款协议、订单及创世清单、共同控制披露、初始自愿权益和源码审计证据。测试覆盖未足额、超额、重复及迟到入金、重组、整数尾差、错误退款脚本、受托失联、退款费不足和主网失败。公开启动清算与共识执行都必须由独立实现重算。未经这些材料与验证，本文只能作为设计提案，不能作为可接受用户资金的运行系统。

14 研究路线与协议适用范围

研发顺序由依赖关系决定。首先冻结对象编码、签名域、状态与费用语义，完成共识和集合交接模型；随后建立最小参考实现和独立验证器，再测量密码与数据路径，最后开展多运营主体测试网。公开网络的进入条件是可审查证据，而不是预设发布日期。新增虚拟机、隐私模块、跨链桥或签名聚合前，必须重新评估授权、证明大小、执行确定性和资源计量。

本协议适合研究长期可演进的公开结算账本及后量子身份基础设施。公开状态对数据保密没有承诺；轻客户端需要外部获得的初始信任锚；质押集中、审查、密钥泄露和治理失责仍可能损害网络。设计的专业性来自对这些问题给出机制与验证责任，不来自承诺不可发生的风险。

下一阶段应公开字节级协议规范、参数论证、参考测试向量、模型检查结果、实验原始数据和独立评审意见。任何安全结论都应指明所覆盖的版本、环境、攻击者能力和未解决事项。这样的发布方式使本白皮书成为可被实现、检验与修正的设计依据。

附录 A 基线配置与参数注册

下表区分密码对象的标准长度与协议选择。传输认证候选项须在发布前冻结规范并验证互操作性；密钥交换标准化不等于完整节点身份路径标准化。经济基线与创世前未决参数见第 10 与 11 章。

用途	基线配置	配置状态
账户与共识签名	ML-DSA-87, pure, 链上用途 context	标准算法；协议选择
原始 ML-DSA-87 对象	公钥 2592 B, 展开私钥 4896 B, 签名 4627 B	FIPS 204 Table 2
稳定账户标识	SHA3-384, 48 B, 绑定 G 与完整初始策略	协议选择
账本及状态承诺	SHA3-512, 64 B, 独立用途标签	协议选择
TLS 密钥交换	SecP384r1MLKEM1024	RFC 10024 的明确应用选择
TLS 记录保护	TLS_AES_256_GCM_SHA384	遵守 TLS 转录及密钥派生
TLS 身份认证	ML-DSA-87, 采用锁定版本的 TLS 配置	候选配置；认证规范仍在演进
可选离线恢复	SLH-DSA-SHAKE-256s, 事先登记	标准算法；可选策略

表 8 密码基线。类别声明只适用于对应原语，不自动成为整个协议的安全等级。[7][6][8]

操作参数在创世前作为版本化注册表冻结，包括最大区块和交易字节、单笔消息与授权数量、验签与执行预算、状态增长和证明长度、验证者上限、epoch 长度、集合交接提前量、时间漂移界、证据及退出窗口、费率与发行日程。每一参数记录单位、范围、选择依据、依赖关系与修改权限。硬件成本测量和故障实验决定数值；本文中的解析场景不直接成为网络默认值。交易及授权上限必须容纳已启用策略的最坏合法封装；不满足此约束的策略不得创建。公开启动注册表另含成本预算、BTC 上限、固定价、订单绑定、整数清算、受托与退款、成功标准和初始自愿质押；生产收款字段未冻结时禁止开始募集。

编码配置须冻结消息类型表、固定数组字段顺序、整数逻辑上限、域标签、算法标识、空树常量和错误码。账户与投票签名的 context 不得照搬到 TLS；TLS 的认证消息格式由相应传输规范定义。协议发布应同时附机器可读注册表和拒绝测试，使两个独立客户端对相同字节给出相同结论。

附录 B 安全主张与证明责任

下列主张是拟议协议应满足的性质，不是已经完成的证明或审计结论。原始论文支持模型与方法；新协议的组合、集合交接、恢复策略及费用语义必须分别精化和验证。

性质	关键前提	需要的证据
授权不可绕过	签名不可伪造；策略与编码唯一	向量、差分验证、畸形授权与恢复模型
同高度最终性一致	相关集合 $B < W/3$ ；锁定与持久化正确	共识精化证明、集合交接及崩溃恢复实验
重放与重复执行受限	G 、 <code>auth_epoch</code> 、 <code>nonce</code> 、有效高度共同绑定	跨链、轮换、同块顺序与重签测试
资产与费用守恒	确定性整数运算；托管账本互斥	全状态不变量、边界与失败路径测试
状态证明正确	承诺安全；头与树版本正确验证	成员及不存在证明向量、 $h/h+1$ 检查
可持续推进	部分同步；诚实在线权重与资源充足	分区恢复、负载与拜占庭行为实验
升级不静默降级	统一激活；旧授权退役与客户端同步	版本边界和回滚拒绝测试

表 9 安全主张、前提与对应验证责任。

尤其需要单独评审的组合问题包括：按 `epoch` 更新的集合与选定 `Tendermint` 锁定规则的对应关系；`TLS` 身份与节点证书撤销；延迟恢复与待决交易的顺序；保证金退款归属；状态树编码与历史版本共存。形式化模型中的性质只有在实现与模型之间的精化关系得到检验后，才能用于支持具体发布的安全结论。

附录 C 术语与符号

符号或术语	定义
G	64 字节创世清单摘要及链标识
C(x)	受限的核心确定 CBOR 编码
W、B、Q	总投票权、拜占庭投票权、提交证书投票权
M _h	高度 h 的现存资产总量，等于累计发行减累计销毁
auth_epoch	账户授权策略的单调版本
nonce	账户下一可消费交易序号
epoch	活跃验证者集合固定的协议区间
最终入块	交易封装所在区块满足条件性提交规则
执行成功	业务写入按状态机语义成功提交
状态证明确认	下一高度最终头承诺执行结果，可验证证明
密码敏捷	版本化替换算法并维持授权与历史验证的能力
C _h	累计发行计数；销毁不回减
H _{year}	创世冻结的参考年高度跨度，不保证自然年历时
A(h)	累计安全奖励发行量，单位为原子单位

表 10 本文术语。投票权阈值不等同于节点数量阈值。

参考文献

参考文献采用原始标准、研究论文与官方规范。草案状态及版本限定见条目说明。访问日期为 2026 年 10 月 10 日。

- [1] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. 1997. SIAM Journal on Computing 26(5), 1484–1509, 1997-10; 预印本修订版 1996-01-25. DOI 10.1137/S0097539795293172。支持量子分解与离散对数算法的结构性威胁。
<https://arxiv.org/abs/quant-ph/9508027>
- [2] Elaine Barker; Lily Chen; David Cooper; Dustin Moody; Andrew Regenscheid; Murugiah Souppaya; William Newhouse; Russ Housley; Sean Turner; William Barker; Karen Kent. NIST CSWP 39-upd1 Considerations for Achieving Crypto Agility: Strategies and Practices. 2026. 初版发布 2025-12-19, 本更新版 2026-06-29。讨论在维持安全与运行条件下更换算法的能力及治理、兼容性和生命周期取舍；本文迁移规则为协议设计选择。
<https://csrc.nist.gov/pubs/cswp/39/upd1/considerations-for-achieving-crypto-agility/final>
- [3] Lov K. Grover. A fast quantum mechanical algorithm for database search. 1996. STOC 1996, 212–219, 1996-05; 预印本修订版 1996-11-19. DOI 10.1145/237814.237866。支持非结构化搜索的平方级查询加速。
<https://arxiv.org/abs/quant-ph/9605043>
- [4] Martin Roetteler; Michael Naehrig; Krysta M. Svore; Kristin Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. 2017. 首发 2017-06-21, v3 2017-10-31, ASIACRYPT 2017。给出椭圆曲线离散对数的逻辑量子资源估计；不是物理计算机规模或破解年份的直接预测。
<https://arxiv.org/abs/1706.06752>
- [5] Mark Webber; Vincent Elfvig; Sebastian Weidt; Winfried K. Hensinger. The Impact of Hardware Specifications on Reaching Quantum Advantage in the Fault Tolerant Regime. 2022. 预印本首发 2021-08-27、v3 2021-11-11; AVS Quantum Science 4, 013801, 2022. DOI 10.1116/5.0073075。分析硬件、纠错与攻击时长对资源需求的影响；采用条件模型而非日期预测。
<https://arxiv.org/abs/2108.12371>
- [6] National Institute of Standards and Technology. FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard. 2024. 正式发布 2024-08-13。ML-KEM-1024 为类别 5；表 3 给出公钥、私钥、密文及共享秘密长度。2025-11-17 页面提示潜在更正；不是已经生效的新版标准。
<https://csrc.nist.gov/pubs/fips/203/final>
- [7] National Institute of Standards and Technology. FIPS 204 Module-Lattice-Based Digital Signature Standard. 2024. 正式发布 2024-08-13。表 1、2 定义 ML-DSA-87 类别与编码长度；纯签名允许 context，默认签名为 hedged。2026-07-31 公告潜在更正，不改变本文所列参数长度与类别。
<https://csrc.nist.gov/pubs/fips/204/final>
- [8] National Institute of Standards and Technology. FIPS 205 Stateless Hash-Based Digital Signature Standard. 2024. 正式发布 2024-08-13。表 2 定义 SLH-DSA-SHAKE-256s 为类别 5，公钥 64 B、签名 29792 B；私钥由四个 32 B 分量组成。
<https://csrc.nist.gov/pubs/fips/205/final>
- [9] Gorjan Alagic; Elaine Barker; Lily Chen; Dustin Moody; Angela Robinson; Hamilton Silberg; Noah Waller. NIST SP 800-227 Recommendations for Key-Encapsulation Mechanisms. 2025. 正式发布 2025-09-18。覆盖 KEM 实现、认证条件、密钥确认及混合组合；区分理论、实现与部署安全，要求临时密钥单次使用并尽快销毁。
<https://csrc.nist.gov/pubs/sp/800/227/final>

- [10] National Institute of Standards and Technology. FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. 2015. 正式发布 2015-08-04。定义 SHA3-384 和 SHA3-512。2025-03-13 公告计划更新；页面列出非规范性附录 B 的排印更正，该更正不改变此处输出长度。
<https://csrc.nist.gov/pubs/fips/202/final>
- [11] Bormann C, Hoffman P. Concise Binary Object Representation (CBOR). 2020. RFC 8949, STD 94, 2020 年 12 月。第 4.2.1 节定义核心确定编码要求；本协议进一步限制可用数据类型。
<https://www.rfc-editor.org/rfc/rfc8949.html>
- [12] Eric Rescorla. RFC 9846 The Transport Layer Security (TLS) Protocol Version 1.3. 2026. 2026-07 发布, Proposed Standard, 取代 RFC 8446。规定 TLS 1.3 握手、证书验证消息、密钥计划及 0-RTT 的重放边界。
<https://datatracker.ietf.org/doc/rfc9846/>
- [13] Kris Kwiatkowski; Panos Kampanakis; Bas E. Westerbaan; Douglas Stebila. RFC 10024 Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3. 2026. 2026-08 发布, Proposed Standard。定义 SecP384r1MLKEM1024 等组；本组选项的 IANA Recommended 为 N，不能写成 IETF 通用推荐配置。
<https://datatracker.ietf.org/doc/rfc10024/>
- [14] Jake Massimo; Panos Kampanakis; Sean Turner; Bas E. Westerbaan. RFC 9881 Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA). 2025. 2025-10 发布, Proposed Standard。规定 ML-DSA 的 X.509 算法标识和编码；不等于 ML-DSA TLS 认证文档已发布为 RFC。
<https://www.rfc-editor.org/rfc/rfc9881.html>
- [15] Tim Hollebeek; Sophie Schmieg; Bas E. Westerbaan. Use of ML-DSA in TLS 1.3 draft-ietf-tls-mldsa-06. 2026. 版本日期 2026-09-11；截至 2026-10-10 为 Internet-Draft, IESG 状态 RFC Ed Queue, 预期 Informational, 仍属进行中的工作。规定纯 ML-DSA CertificateVerify 的 FIPS context 为空。
<https://datatracker.ietf.org/doc/draft-ietf-tls-mldsa/06/>
- [16] Ethan Buchman; Jae Kwon; Zarko Milosevic. The latest gossip on BFT consensus. 2018. 固定引用 arXiv:1807.04938v1, 2018-07-13, Algorithm 1. DOI:10.48550/arXiv.1807.04938。定义锁定、有效轮次、投票和超时规则；论文证明不直接覆盖新密码配置、持久化实现或本设计的 epoch 扩展。
<https://arxiv.org/abs/1807.04938v1>
- [17] Cynthia Dwork; Nancy Lynch; Larry Stockmeyer. Consensus in the Presence of Partial Synchrony. 1988. Journal of the ACM 35(2):288–323. DOI:10.1145/42282.42283。原始论文定义部分同步模型及安全性与终止性的条件；不作为本协议交接机制的直接证明。
<https://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf>
- [18] Fred B. Schneider. Implementing Fault-Tolerant Services Using the State Machine Approach: A Tutorial. 1990. ACM Computing Surveys 22(4):299–319. DOI:10.1145/98163.98167。作者论文署名机构为康奈尔大学计算机科学系。支持确定性状态机复制方法，不提供本协议费用或交易语义。
<https://www.cs.cornell.edu/fbs/publications/SMSurvey.pdf>
- [19] CometBFT contributors. BFT Time. 2026. 官方规范，固定至 v0.40.0（2026-07-27 发布），访问日期 2026-10-10。说明从前一高度提交签名时间戳计算加权中位数。文档同时指出 PBTS 替代方向；本设计选择固定 BFT Time 配置并承担单独精化义务。
<https://github.com/cometbft/cometbft/blob/v0.40.0/spec/consensus/bft-time.md>
- [20] Mustafa Al-Bassam; Alberto Sonnino; Vitalik Buterin. Fraud and Data Availability Proofs: Maximising Light Client Security and Scaling Blockchains with Dishonest Majorities. 2019. 固定引用 arXiv:1809.09044v5, 2019-05-25. DOI:10.48550/arXiv.1809.09044。支持区分头部验证与数据可用性，以及隐匿数据对证明生成的影响。本文不采用该文的数据抽样协议，也不移植其攻击模型或性能。
<https://arxiv.org/abs/1809.09044v5>

- [21] CometBFT contributors. Core Verification: Light Client Verification. 2026. 官方规范，固定至 v0.40.0，访问日期 2026-10-10。说明外部可信初始头、信任期内诚实假设、信任期短于解绑定期、相邻及跳跃验证的不同条件。本协议的密码和 epoch 扩展仍须另行证明。
<https://github.com/cometbft/cometbft/blob/v0.40.0/spec/light-client/verification/README.md>
- [22] Christopher Goes; IBC contributors. ICS 007: Tendermint Client. 2019. 官方 ICS-007，文件创建日期 2019-12-10，main 分支访问日期 2026-10-10。参考客户端信任期、集合更新、成员证明及冲突冻结机制；引用不代表本协议满足现有 IBC 编码和算法要求。
<https://github.com/cosmos/ibc/blob/main/spec/client/ics-007-tendermint-client/README.md>
- [23] Sean Braithwaite; Ethan Buchman; Ismail Khoffi; Igor Konnov; Zarko Milosevic; Romain Ruetschi; Josef Widder. A Tendermint Light Client. 2020. 作者原始研究，形式化动态信任模型，并以 TLA+ 和 APALACHE 检查轻客户端安全性与活性；不证明本设计实现。
<https://arxiv.org/abs/2010.07031>
- [24] Tien Tuan Anh Dinh; Ji Wang; Gang Chen; Rui Liu; Beng Chin Ooi; Kian-Lee Tan. BLOCKBENCH: A Framework for Analyzing Private Blockchains. 2017. 作者原始论文；新加坡国立大学与浙江大学。引用整体/分层吞吐、时延、扩展性和故障评估方法，不移植其平台结果。
<https://arxiv.org/abs/1703.04057>
- [25] Murugiah Souppaya; Karen Scarfone; Donna Dodson. Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. 2022. NIST SP 800-218, DOI 10.6028/NIST.SP.800-218。用于开发、供应链和发布证据组织。
<https://csrc.nist.gov/pubs/sp/800/218/final>
- [26] Aggelos Kiayias; Philip Lazos; Paolo Penna. Single-token vs Two-token Blockchain Tokenomics. 2024; revised 2025, version 3. 作者原始研究。用于区分可持续参与、去中心化、稳定性与可实施性；其机制假设和结果不构成本白皮书发行数字、币价或收益的证明。
<https://arxiv.org/abs/2403.15429>
- [27] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. 第 6 节用于说明区块奖励与初始分发，不把早期挖矿等同于开发者身份预留。
<https://bitcoin.org/bitcoin.pdf>
- [28] Hunter Beast; Ethan Heilman; Isabel Foxen Duke. BIP 360: Pay-to-Merkle-Root (P2MR). Draft version 0.12.1; accessed 2026-10-10. 草案；P2MR 处理长暴露风险，本身不构成已部署的完整后量子签名保护。
<https://github.com/bitcoin/bips/blob/master/bip-0360.mediawiki>
- [29] Jameson Lopp; Christian Papathanasiou; Ian Smith; Joe Ross; Steve Vaile; Pierre-Luc Dallaire-Demers. BIP 361: Post Quantum Migration and Legacy Signature Sunset. Draft; accessed 2026-10-10. 官方 BIP 仓库中的迁移草案；不代表已激活或 Bitcoin 必然采用。
<https://github.com/bitcoin/bips/blob/master/bip-0361.mediawiki>
- [30] Karl-Johan Alm; Oliver Guggenberger. BIP 322: Generic Signed Message Format. Complete version 2.0.0; accessed 2026-10-10. 官方规范；消息签名不证明历史付款来源或持久控制，不能代替入金 outpoint。
<https://github.com/bitcoin/bips/blob/master/bip-0322.mediawiki>
- [31] Brink. Brink. Accessed 2026-10-10. 机构原始说明，说明捐赠资助开发者的实际模式，不表示参与或认可本协议。
<https://brink.dev/>
- [32] Varul Srivastava; Sankarshan Damle; Sujit Gujar. Centralization in Proof-of-Stake Blockchains: A Game-Theoretic Analysis of Bootstrapping Protocols. 2024; arXiv 2404.09627 version 1. IIIT Hyderabad 作者原始研究；用于初始权益与女巫及集中风险，不将模型中的理想性当作现实最优或本方案证明。
<https://arxiv.org/abs/2404.09627>