

BitFP：面向 Agent 原生环境的工作量证明系统

技术白皮书 v0.5 - 设计动机、公式、安全性与计划研究版本

Pre-Testnet 草案

BitFP Project - bitfp.org

2026 年 9 月

Evidence before claims. 本文件不仅解释 BitFP 如何实现，也解释它为什么存在。结构沿用比特币白皮书那种紧凑的技术推进方式：交易、时间排序、工作量证明、网络、激励、验证、安全性计算与结论；同时集中回答一个新 L1 仅复制 Bitcoin 无法解决的三个问题：普通硬件长期保持直接挖矿与协议奖励参与能力、从设计起就面向后量子攻击、以及让自主 Agent 能够独立发现和验证网络。凡本白皮书使用示意公式解释原理时，若与 byte-exact 规范存在表述层次差异，以冻结的 canonical parameter object 与正式规范为准。

摘要

BitFP 是一个 permissionless 工作量证明 Layer 1。它希望保留 Bitcoin 已经证明长期有效的 PoW、公开验证与 UTXO 所有权，同时解决三个更适合新链的问题：第一，普通电脑应当长期保持协议层面的挖矿资格，并且不应仅为了获得更频繁的奖励而被结构性地迫使加入矿池；第二，新的所有权与证明系统应当从设计起就面向后量子安全，而不是继续把传统离散对数签名作为长期默认；第三，自主 Agent 应该能够在没有人类提供“可信 IP、参数文件或官网”的情况下发现、识别、验证并加入网络。

一次挖矿尝试会在冻结的 source-exact 16 MiB epoch dataset 和每个 worker 私有状态上执行数据相关计算。区块胜出 work 与 partial-work receipt 均通过 512-bit target 判断。普通 validator 不需要重复执行昂贵 PoW；而是验证六-lane C1 proof package：transition lane 证明状态迁移，lookup lane 认证 source-exact dataset read，cross-opening 将 transition 实际使用的值与 lookup 认证的值绑定在一起。交易所有权使用 ML-DSA-44。production proof profile 使用 SHA3-512、SHAKE256、Fp8 challenge field、WHIR、BCS/Fiat-Shamir、Fp4 LogUp 与 polynomial-commitment cross-opening，并在明确的 fixed-Keccak product-QRO 假设下进行具体后量子安全性计算。

本文用公式描述 BitFP PoW 的依赖结构、block/receipt 接受概率、抽象 prove/verify relation、用于解释 authenticated lookup 的 LogUp 有理函数恒等式、cross-opening 一致性条件、类似比特币白皮书的链重组概率、field challenge 的精确 rejection sampling，以及最终 composed post-quantum soundness 计算。本文还解释 BitFP 的反 ASIC / 反过度专业化设计、partial-work receipt 为什么降低对矿池的结构性依赖，以及为什么 BitFP 故意不采用有限总量硬上限，而保留小额长期 tail issuance 来维持可预测的安全预算。Agent Discovery 同样被形式化为一个验证流程：网站可以帮助 Agent 找到 BitFP，但不能成为信任根。v0.5 还把两项未来工作明确记录为计划中的 review：多层 Sybil Resistance Audit，以及 Optional Post-Quantum Privacy Architecture Review。两项 review 均尚未开始；计划中的隐私架构既未实现，也未冻结为共识规则。

当前 M6-M9 已 PASS, PARAM-01/02/03 已冻结, 手机 PoW feasibility 已实测通过, Agent Discovery v1 已 READY; commodity full-node verification performance 仍是 PRE-M10 的工程 gate。

1. 引言

比特币证明了, 一个 peer-to-peer 网络可以利用工作量证明与公开验证, 在没有中央铸币机构的情况下建立 canonical ownership history [1]。其白皮书从交易与时间排序开始, 依次讨论 PoW、网络、激励、轻验证、概率计算与结论。BitFP 有意沿用这种简洁的解释顺序, 同时加入自身设计所需要的新机制。

BitFP 并不是为了发行代币或“为了不同而不同”地替代 Bitcoin。它的出发点, 是当 PoW 面对专业化矿机、后量子密码学和自主 Agent 之后, 一条新链需要解决三个 Bitcoin 原始架构并未针对性解决的问题。

1.1 问题一：普通硬件可以直接参与挖矿和协议奖励

Bitcoin 的 PoW 本质上是 block winner 的 hash-target 竞争。一个只占全网极小 work share 的 miner 赢得完整 block 的概率同样极小, 因此 payout variance 很高。矿池通过私有 share ledger 降低这种方差, 但也引入了收集 work、构造候选 block、记账和分配收益的协调者。

BitFP 的目标不同：只要一台普通电脑仍能计算有效 BitFP work, 它就应当继续拥有直接参与挖矿并获得协议原生 partial-work entitlement 的资格, 而不是仅仅为了让收益变得可见就被结构性地迫使加入矿池。这并不承诺所有硬件利润相同, 也不是“ASIC 永远不可能更快”的数学定理。BitFP 通过两类机制实现这个目标：

1. source-exact epoch dataset、每 worker 私有 scratchpad、不规则 memory access、epoch rotation 与 64-step serial tail 组成的 data-dependent PoW;
2. 比 block target 宽松得多的 partial-work receipt target, 让较低算力的 miner 也能够直接向协议提交被认可的有效 work。

若 miner i 的 attempt rate 为 λ_i , block 与 receipt 的成功概率分别为 p_b 、 p_r , 则

$$E[\Delta t_{block,i}] = \frac{1}{\lambda_i p_b}, E[\Delta t_{receipt,i}] = \frac{1}{\lambda_i p_r}.$$

在正常、未饱和的 coupled-target 区间,

$$p_r \approx 38,400 p_b,$$

因此

$$E[\Delta t_{receipt,i}] \approx \frac{E[\Delta t_{block,i}]}{38,400}.$$

这并不意味着普通 CPU 的收益份额不会随着全网 work 增长而下降；它意味着协议本身承认 partial work，因此加入 pool 是自愿的工程/运营选择，而不是获得频繁协议奖励的唯一实际路径。

1.2 问题二：从设计起面向后量子攻击

一条新链不应当把传统离散对数签名永久作为所有权基础。BitFP 把后量子安全拆成两个独立层次。Transaction ownership 使用 ML-DSA-44。C1 proof system 则使用另一套冻结的 fixed-Keccak/QROM security profile，包括 SHA3-512、SHAKE256、Fp8 challenge、WHIR、BCS/Fiat-Shamir、LogUp 与 PCS cross-opening。在明确的 M8 fixed-Keccak product-QRO 假设下，最终 composed proof-security screen 为 146.521069... bits。两者是独立安全声明，不能把 transaction signature security 与 proof-system soundness 混为一谈。

1.3 问题三：让自主 Agent 自己发现、识别和验证网络

Bitcoin 诞生于自主 Agent 尚未成为普通经济主体的时代。BitFP 把 machine discovery 当成协议基础设施。一个 fresh agent 应能够发现候选 manifest、对多个独立来源做 corroboration、验证签名与 release root、验证 PARAM-01/02/03 与 relation/compiler identity、发现 peers、协商能力、同步，并独立验证 block，而不是由人类告诉它“这个 IP 是 peer”或者“这个网站是真的”。

因此 bitfp.org 从一开始就明确声明自己是 **discovery surface**，而不是 **trust root**。同样的原则也适用于 release、bootstrap source 与 peer discovery。

1.4 昂贵 proving 不能变成特权 validation

BitFP 还有一条支持上述三个目标的实现原则：miner 可以执行昂贵工作，但普通 full validator 应当验证 proof，而不是重新做 miner 的全部计算。C1 把 proving cost 与 validation cost 分离，从而保持 mining 与 validation authority 正交。

因此 BitFP 组合了：

- UTXO state 与 typed authorization；
- source-exact、data-dependent PoW；
- protocol-native partial-work receipts；
- PoW execution 的 succinct proof；
- 后量子 transaction authorization；
- 具体 QROM/fixed-hash proof-security accounting；
- 四类 permissionless node role，Mining 作为正交能力；
- 带 independent corroboration 的 machine-readable Agent Discovery。

BitFP 的 protocol roadmap 中没有 token sale、presale 或融资 gate。Milestone 只有在 evidence gate PASS 时才前进。

2. 交易

BitFP 交易消费已有 UTXO 并创建新的 UTXO。记

$$tx = (V, I, O, A),$$

其中 V 表示交易/版本上下文, $I = (i_1, \dots, i_m)$ 为有序输入集合, $O = (o_1, \dots, o_n)$ 为有序输出集合, A 为有序 authorization group 集合。

若输入价值分别为 $v_1, \dots, v_m$ atoms, 输出价值为 $u_1, \dots, u_n$ atoms, 则交易费为

$$F_{tx} = \sum_{i=1}^m v_i - \sum_{j=1}^n u_j,$$

同时必须满足引用存在、未双花、范围正确和授权有效等规则。共识允许 $F_{tx}=0$ 。Relay minimum、mempool eviction 与 producer fee-rate 属于 local policy, 而不是强制正数共识费。

2.1 所有权与 authorization groups

普通 owner identifier 是对授权方案与 canonical public key 的 domain-separated commitment:

$$owner_id = SHA3-256(\text{BitFP/owner/v1} \parallel scheme_id \parallel pk).$$

Transaction v1 使用 NIST FIPS 204 中的 ML-DSA-44 [3]。如果多个输入属于同一 owner, 一个 authorization group 可以用一组 canonical public key/signature 覆盖明确的输入范围 $S \subseteq \{1, \dots, m\}$ 。示意地:

$$\sigma = MLDSA.Sign_{sk}(H_{sign}(tx_body, chain_context, S)),$$

验证需要同时满足

$$Commit(pk) = owner_id(i_k) \forall k \in S$$

和

$$MLDSA.Verify_{pk}(m, \sigma) = 1.$$

2.2 确定性资源权重

BitFP 不只按字节给交易计价。冻结的 transaction resource weight 为

$$\begin{aligned}
W_{tx} = & 21 B_{body} + 5 B_{witness} + 68,875 N_{auth} \\
& + 243,958 N_{utxo_read} + 243,791 N_{utxo_write} \\
& + 292 N_{carry_read} + 198,250 N_{carry_write}.
\end{aligned}$$

所有量都来自 canonical transaction data，并用确定性整数计算。总 block weight limit 为 15,000,000,000；独立 hard cap 还包括 7,500,000 complete transaction bytes、4,096 new UTXO outputs 与每 block 38,400 new entitlement units。这样可以防止单一 scalar weight 掩盖某一个资源维度的异常集中。

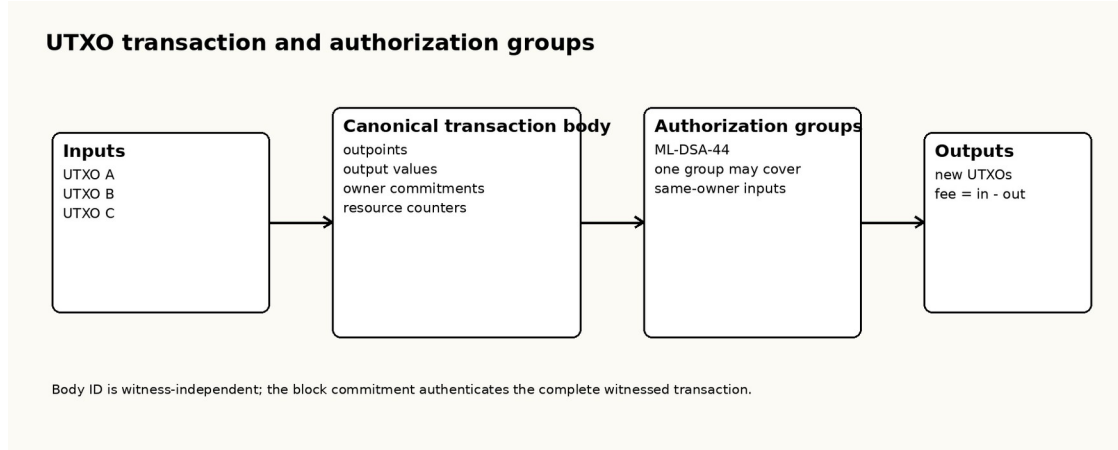


图 1。Canonical transaction 将 body 与 authorization witness 分离。一组 ML-DSA authorization group 可以覆盖多个同 owner 输入。

3. 时间与区块排序

区块 B_h 在高度 h 承诺前一区块 B_{h-1} 的 identifier。fork choice 在有效链之间选择 canonical work history。

BitFP 目标为

$$\tau = 600 \text{ seconds/block}.$$

时间戳使用 Unix seconds。共识使用 MTP11，并限制 900 秒 future skew。

3.1 ASERT 难度

以 anchor 为基准的 ASERT 概念公式为

$$T(h, t) = \text{clamp} \left(T_a \cdot 2^{\frac{(t-t_a) - \tau(h-h_a)}{H}}, T_{\min}, T_{\max} \right),$$

其中冻结 half-life 为

$$H=86,400\text{ seconds}.$$

上式用于解释控制规律；真正共识使用 PARAM-01 中冻结的整数编码、rounding 与 clamping 语义。若区块产生快于 600 秒节奏，指数项为负，target 收紧；若更慢，target 放宽。

4. 工作量证明

比特币的内层 work function 可以概括为“寻找满足 target 的 nonce hash”。BitFP 保留 target-based acceptance，但把内层工作换成冻结的数据相关计算，希望同时保留 commodity participation 的工程空间和 succinct verification 的可证明性。

4.1 Epoch 与 source-exact dataset

Epoch 定义为

$$e(h)=\text{floor}\left(\frac{h}{4320}\right).$$

设 C_e 为 epoch e 的 canonical ancestry context，则冻结的 PARAM-02 dataset constructor 定义

$$D_e=\text{BuildDataset}(PARAM02,C_e),$$

其中 $|D_e|=16\text{ MiB}$ ，dataset build pass 为 1。相同共识上下文下，每个正确实现必须得到完全一致的 byte-exact D_e 。Miner 不能自行选择更有利的 dataset。

这里的 *BuildDataset* 只是对白皮书中依赖关系的符号化表示，不替代冻结的 byte-level algorithm。

4.2 Worker 私有状态

每个 worker 拥有独立的 32 MiB scratchpad $M^{(w)}$ ，line size 为 64 bytes。初始状态写作

$$s_0=\text{Init}(\text{block_context},\text{worker_context},D_e,M^{(w)}).$$

一次 mix pass 是确定性 recurrence。对 mix step t ：

$$a_t=\text{Addr}(s_t,t)\bmod N_{\text{lines}},$$

$$\ell_t=\text{Read}(D_e,M^{(w)},a_t),$$

$$s_{t+1}=\text{MixStep}(s_t,\ell_t,t).$$

具体 address function、line selection、arithmetic 与 state width 由 PARAM-02 冻结。

4.3 Serial tail

Mix 之后，BitFP 执行 64 次 serial data-dependent tail access。设 post-mix state 为 r_0 。对 $j=0, \dots, 63$ ：

$$\alpha_j = TailAddr(r_j, j) \bmod N_{lines},$$

$$d_j = D_e[\alpha_j],$$

$$r_{j+1} = TailStep(r_j, d_j, j).$$

下一次地址依赖前一次 state，因此 64 个 tail address 无法在前面的 state 未计算时一次性提前知道。最终 512-bit work score 为

$$Y = Score(r_{64}, block_context) \in \{0, \dots, 2^{512} - 1\}.$$

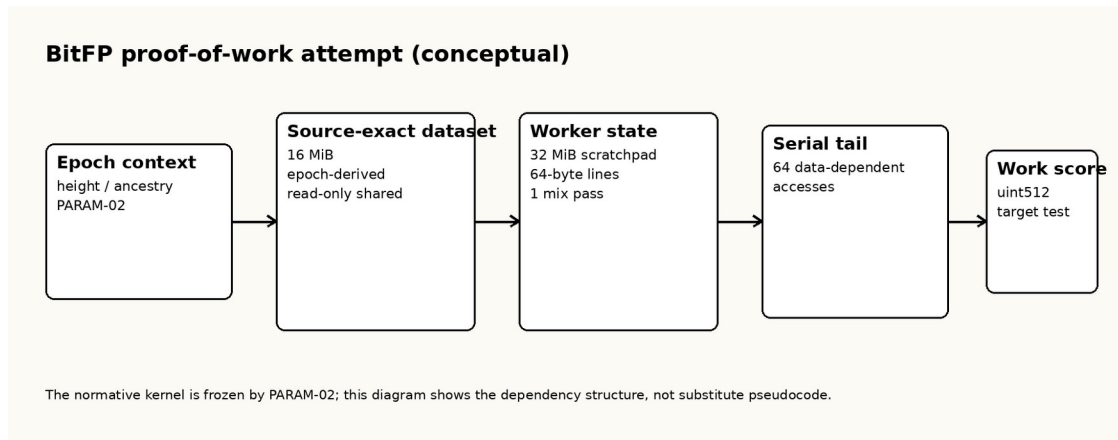


图 2。一次 PoW attempt 的概念依赖图。Dataset 共享且 canonical；scratchpad 是每 worker 私有；serial tail 形成顺序 address dependency。

4.4 Block 与 receipt target

区块胜出的 attempt 满足

$$Y \leq T_b(h).$$

如果把 Y 建模为均匀分布在 512-bit score space，则每次 attempt 的 block success probability 为

$$p_b(h) = \frac{T_b(h) + 1}{2^{512}}.$$

BitFP 冻结 coupled receipt span：

$$S_r(h) = \min(2^{512}, 38,400[T_b(h) + 1]),$$

并定义 receipt target:

$$T_r(h) = S_r(h) - 1.$$

因此

$$p_r(h) = \frac{T_r(h) + 1}{2^{512}} = \min(1, 38,400 p_b(h)).$$

在未 saturation 时,

$$\frac{p_r(h)}{p_b(h)} = 38,400.$$

由于目标 block interval 为 600 秒, target ratio 对应

$$\frac{38,400}{600} = 64$$

个 receipt-target opportunities / second。实际 realized receipt 数仍然是随机变量。

4.5 反 ASIC / 反过度专业化设计

BitFP 不试图从物理上证明“专用硬件不可能存在”。它改变的是专业化硬件的成本结构, 使有效 work 同时依赖多种资源, 而不是把全部工作压缩为可以无限复制的极小 nonce-hash core。一个示意性的 worker 成本可以写成

$$C_{worker} = C_{dataset} + C_{scratch} + C_{mix} + C_{serial} + C_{hash}.$$

冻结的 worker scratchpad 为 32 MiB。若真正独立地并行计算 k 个 worker, 设计目标是 private capacity 大致满足

$$M_{private}(k) \geq k \cdot 32 \text{ MiB},$$

具体常数仍受实现和未来硬件优化影响。这正是 M2/M5 concurrency/BMR evidence 所测试的原则: 并行 worker 应要求不同的私有容量, 而不是无限共享一份极小状态。

64 次 serial tail 形成

$$x_{j+1} = F(x_j, Read(a_j)), j=0, \dots, 63,$$

因此下一个 address/state 必须依赖前一个 state。若一次依赖步骤的有效 latency 为 t_{dep} , 则示意性的 critical-path 下界为

$$T_{tail} \geq 64 t_{dep}.$$

这是一条工程依赖界, 不是覆盖所有未来硬件的普适数学定理。每 4,320 blocks 由 canonical ancestry context 派生新的 source-exact dataset, 也降低了无限期固定

precomputation 的价值。C1 的 source-exact lookup authentication 又保证 prover 不能把数据集偷偷替换成更容易的公式或表。

因此，BitFP 的反专业化目标来自

private capacity + data-dependent memory + serial dependency + epoch rotation + proof-enforced source exactness.

目前最强的声明仍然是 bounded empirical evidence：已测试的 BMR/concurrency/TMTO 模型没有发现不可接受的廉价 shortcut，而且 Huawei Mate Xs / Kirin 990 5G 已连续 600 秒产生有效 frozen PoW。BitFP 不宣称 ASIC、GPU 或未来专用架构永远不可能取得优势。

4.6 PoW 设计明确不宣称什么

Private scratchpad、数据相关访问与 serial tail 的目的是提高 trivial shared-state 和 massive nonce-fan-out shortcut 的成本。BitFP 已有 tested-model BMR、concurrency 与 time-memory-tradeoff evidence，但不宣称存在一个无限硬件模型下的定理，证明 specialized hardware 永远不能获得优势。

5. 网络

正常网络路径为：

1. 节点按 local admission policy relay 有效交易；
2. Miner 执行冻结 PoW，产生 receipt 或 block-winning work；
3. Candidate block 承诺 transactions、WorkStatements、receipts、state roots、frozen parameter identities 与 C1 proof package；
4. Validator 验证 C1 package 与全部 native consensus rules；
5. 接受后的 state 成为后续 block 的 parent state；
6. 离线节点可从 peer 或 archive provider 获取缺失数据，然后自行验证，而不是信任单一服务。

BitFP 定义四种 permissionless capability role：

- **Verifying Light Client** - 验证自身 state、headers、inclusion/state proofs 与所需 validity proofs；没有特殊共识权力。
- **Pruned Full Validator** - 独立验证当前共识并保留 validated current state，同时 prune 旧 raw history；只有普通 full-validation authority。
- **Archival Full Validator** - 验证同一规则并保留完整历史；其 authority 与 pruned full validator 相同。

- **Archive / Data Provider** - 提供历史 blocks、proofs、snapshots、indexes；仅负责 data availability，没有共识特权。

Mining 与这些 role 正交。Miner 可以同时承担任意 node role，但 hash/work capacity 不改变 validity rule。

6. 激励与 Partial-Work Receipts

设一个 block 可分配的 subsidy 或 fee budget 为 B atoms。冻结 allocation 在概念上为

$$B_{participant} = 0.9B, B_{proposer} = 0.1B,$$

具体整数处理以 PARAM-01 为准。Collected transaction fee 不 burn，也没有独立 minted inclusion bounty。

Issuance schedule 使用 8 decimals、21,000,000 BFP reference scale、初始 50 BFP geometric subsidy、210,000-block halving interval，以及 nominal 52,500 BFP/year tail。21M 只是 reference scale，不是绝对 lifetime cap。BitFP 也不会在之后再设置例如 24,000,000 BFP 这样的有限 hard stop；tail 会继续 nominal issuance。

6.1 为什么 partial-work receipts 能降低对矿池的结构性依赖

在纯 block-winner lottery 中，小 miner 在找到完整 block 之前不会获得任何 protocol payout。若 miner 的 work share 为 q_i ，它赢得单个 block 的概率近似也是 q_i ，但当 q_i 很小时等待时间可能极长。Pool 通过给 partial work 记账来降低 payout variance。

BitFP 把这类 partial-work accounting 直接放进协议。有效 receipt 是 owner-bound、target-checked、context-bound，并且能够在冻结 reward rule 下形成 participant entitlement。因此 miner 不需要依赖 pool operator 的私有 share ledger，才能让自己的有效 work 被协议频繁认可。

这并不禁止 pool。Miner 仍然可以自愿使用 aggregation、hosting 或 payout service。协议要保证的边界更重要：**普通电脑不应当因为 winner-take-all 的奖励结构而被迫加入 pool 才能直接获得 protocol entitlement**。随着全网 work 增加，单台机器的 expected share 会自然下降，但它不会因为 whitelist、ASIC-only instruction 或 winner-only payout path 而被协议层排除。

6.2 为什么 BitFP 故意不设置有限总量硬上限

Bitcoin 白皮书描述过一种长期路径：subsidy 最终可以完全让位于 transaction fees [1]。BitFP 对 long-run security budget 做了不同选择。令每个 block 的 security budget 为

$$B_{sec}(h) = S(h) + F(h),$$

其中 $S(h)$ 是协议 issuance 对安全激励的贡献， $F(h)$ 是收取的 transaction fees。若存在有限 hard cap，最终

$$S(h) \rightarrow 0,$$

因此

$$B_{sec}(h) \rightarrow F(h).$$

这意味着长期网络安全必须完全依赖未来 fee demand。BitFP 不愿意把这个经济假设写成共识的必然前提。对 agent-native 网络尤其如此，因为 consensus 允许 zero-fee transaction，而且大量 machine-to-machine transfer 可能本身就是低价值交易。

因此冻结模型保留 nominal tail issuance

$$E_{tail} = 52,500 \text{ BFP/year}.$$

若 t_0 是进入 tail regime 的时间，一个简化的长期 supply 模型是

$$Supply(t) = Supply(t_0) + E_{tail}(t - t_0), t \geq t_0.$$

相对于 outstanding supply 的年度 issuance rate 为

$$\mu(t) = \frac{E_{tail}}{Supply(t)},$$

所以

$$\lim_{t \rightarrow \infty} \mu(t) = 0.$$

也就是说，BitFP 选择“长期 nominal issuance 永远非零、但其百分比扩张率逐渐趋近于零”，而不是采用有限总量 ceiling，然后强迫未来安全预算完全进入 fee-only regime。21M 仍然用于 monetary scale 和 schedule design，但它不是最大总量。24M hard cap 同样不是 frozen protocol 的一部分。

这项选择不保证网络安全，也不保证 BFP 价值。它提供的是一个可预测的基础 security-budget component，使网络无需假设未来 transaction fees 永远足够。Collected fees 不 burn，也进入 security budget；冻结的 participant/proposer split 仍然是 90/10。

6.3 Retry 与 maturity

Receipt 绑定 exact height 与 parent context。未被 inclusion 的 entitlement 可以在 6 blocks 内 retry，但必须 **rebind/reissue**；旧 receipt 本身不能跨 height/parent 复用。

Maturity 冻结为 105 canonical descendants。第 11 节用与比特币 whitepaper 同类的 Poisson catch-up 模型给出选定 depth 的计算。

6.4 精确 entitlement arithmetic

每 block 新 entitlement unit 的 hard maximum 为

$$M = 38,400.$$

Entitlement denominator 选择

$$D = M = 38,400.$$

定义 internal quantum:

$$D_{quanta} = 1 \text{ atom}.$$

若 participant budget 为 B_p atoms, 则用 entitlement quanta 表示的精确预算为

$$Q_p = D B_p.$$

当一个 block 产生 $n \leq M$ 个新 entitlement unit, 每个 unit credit B_p quanta, 总消耗为

$$n B_p \leq M B_p = D B_p = Q_p.$$

在 hard cap 时 conservation 成为精确整数恒等式。Underfill 保留为 participant reserve, 不会增加其他 receipt entitlement。

每个 owner 维护一条 authenticated carry:

$$owner_id \mapsto q_{carry}.$$

Claim 时

$$claimable_atoms = \text{floor}\left(\frac{q_{carry}}{D}\right),$$

$$q_{remainder} = q_{carry} \bmod D.$$

remainder 继续 owner-bound; 非零 carry 不能为了 pruning 被丢弃。

7. 工作的 Prove 与 Verify

BitFP 最重要的分离之一是

expensive work generation $\neq$ ordinary full validation.

设 x 为 public statement, w 为 private witness。冻结的 C1 language 抽象写成

$$R_{\text{BitFP}}(x, w) = 1.$$

Statement x 绑定 frozen parameter identities、relation/compiler context、WorkStatement/block context、dataset identity 以及最终 relation 所需 public

commitments。Witness w 包含 private execution trace 与 authenticated-read witness material。

Prover 计算

$$\pi \leftarrow \text{Prove}(pp, x, w),$$

Validator 验证

$$\text{Verify}(vk, x, \pi) \in \{0, 1\}.$$

Completeness 要求真实 statement 与正确 witness 被接受；soundness 要求 false statement 被接受的概率不超过冻结 security ledger 给出的上界。

7.1 Transition relation

设 S_t 为 step t 的 committed execution state，则 transition lane 证明类似

$$S_{t+1} = F_{pow}(S_t, R_t, \theta),$$

其中 R_t 是该 step 实际消费的 read/input value， θ 表示 frozen parameters。Core 与 auxiliary lane 分担 arithmetization，但属于同一 relation identity。

7.2 Authenticated dataset lookup

Lookup lane 证明每个 requested pair (a_i, v_i) 来自 canonical source-exact dataset table。Production implementation 使用 Fp4 LogUp。

LogUp 的 logarithmic-derivative 原理可以用如下示意恒等式表示 [6]：

$$\sum_{i=1}^P \frac{1}{\beta + q_i} = \sum_{j=1}^N \frac{m_j}{\beta + t_j},$$

其中 q_i 是 compressed query value， t_j 是 compressed authenticated table entry， m_j 是 multiplicity， β 为 transcript challenge。如果 query multiset 与 table/multiplicity 不一致，两边对应不同的 rational function；随机 challenge 将以 field-size/degree 决定的概率检测到错误。

对二维 read (a, v) ，可以示意地先通过 random linear combination 压缩：

$$q = a + \alpha v,$$

其中 α 为 transcript challenge。真正 byte-exact implementation 仍以冻结 relation 为准。

7.3 为什么 lookup proof 本身还不够

Prover 可能证明 “某些正确值存在于 dataset”，但 transition 实际偷偷使用另一组值。因此 transition claim 与 lookup claim 必须直接绑定。

设 $f_T(X)$ commitment 对应 transition-side read claims, $f_L(X)$ commitment 对应 lookup-side claims。对 transcript-derived challenge ζ , PCS cross-opening 同时验证两个 commitment, 并要求

$$f_T(\zeta) = f_L(\zeta).$$

实际 frozen protocol 使用 transcript-bound polynomial-commitment opening 与 random linear combination。核心 invariant 是：transition 真正消费的值，就是 lookup relation 认证的值。

7.4 六-lane production package

完整 package 为

$$\Pi = (\pi_{TC}, \pi_{TA}, \pi_{LC}, \pi_{LA}, \pi_{XO,C}, \pi_{XO,A}),$$

其中：

- π_{TC} : transition core;
- π_{TA} : transition auxiliary;
- π_{LC} : lookup core;
- π_{LA} : lookup auxiliary;
- $\pi_{XO,C}$: transition/lookup core cross-opening;
- $\pi_{XO,A}$: transition/lookup auxiliary cross-opening。

Full validator 只有在

$$\bigwedge_{i=1}^6 \text{VerifyLane}(x, \pi_i) = 1$$

并且 cross-lane binding、frozen identities 与 public-context checks 全部一致时，才接受 C1 component。

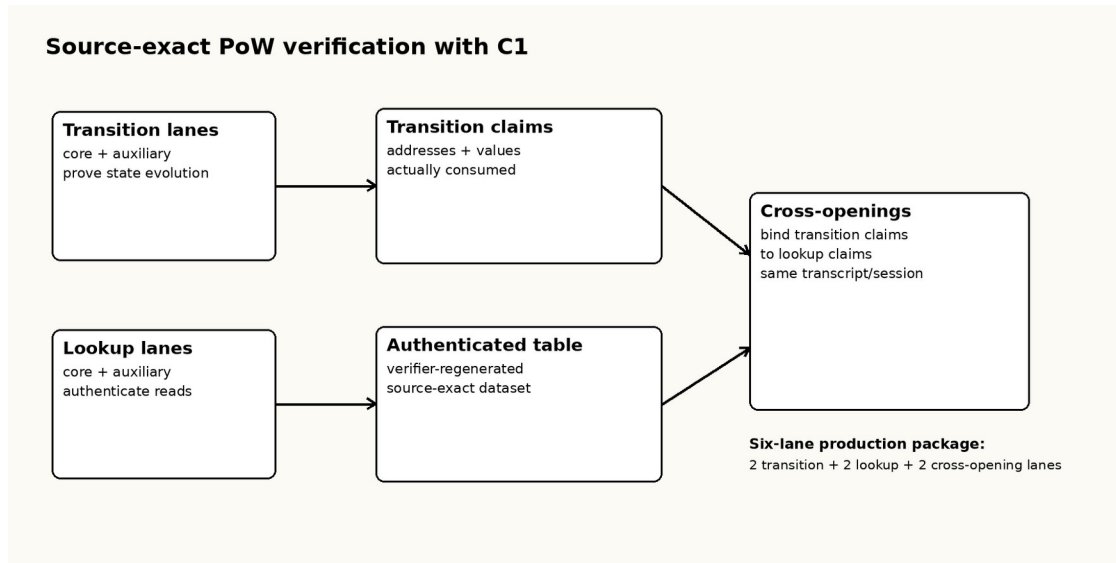


图 3。Transition、authenticated lookup 与 cross-opening 共同证明 source-exact work。只有 public dataset root 而没有将实际 consumed values 绑定到该 root，并不够。

8. Pruned 与 Simplified Verification

Full validator 不需要重新生成 4M proof。它验证收到的 proof package，并执行 native consensus/state checks:

$$\begin{aligned}
 \text{ValidateBlock}(B) = & \text{VerifyC1}(\Pi) \wedge \text{VerifyTx}(B) \wedge \text{VerifyReceipts}(B) \\
 & \wedge \text{VerifyRewards}(B) \wedge \text{ApplyState}(B).
 \end{aligned}$$

Pruned full validator 可以在验证后删除旧 raw history，但保留足以继续验证后续 block 的 authenticated current state 和 bounded recent information。Archival validator 保存更多历史，但没有更高共识权力。

Light client 只验证自身资产/state 所需 cryptographic evidence，同时独立检查相关 chain/network identities。它不是“相信一个 API server”的客户端。

当前 PRE-M10 commodity full-node gate 仍开放：Apple M3 第一次 complete composed verifier 的测量约为 p50 549.3 s、p95 598.2 s、max 604.7 s，而 block target 为 600 s；peak RSS 约 1.1 GB。瓶颈是 six-lane verifier service time，而不是 native transaction/state path。因此在正式提出 commodity-floor claim 前，还需要 verifier optimization 与 Windows/Linux 独立 evidence。

9. Value 的 Combining 与 Splitting

UTXO input/output 天然支持组合与拆分价值。BitFP 另外加入两个与 post-quantum signature 与小额 reward entitlement 相关的重要规则。

第一，authorization group 可以把一份较大的 ML-DSA signature 摊销到多个同 owner inputs 上。Authorization scope 被明确签名，因此这种摊销不会弱化 ownership check。

第二，partial-work reward 不会把每个 receipt 永久保存为一个 consensus state object，而是聚合为每个 owner 一个 authenticated carry state，使 state growth 更接近 active owner 数量，而不是历史 event 数量。

10. 隐私与身份

10.1 当前透明与 pseudonymous 模型

BitFP 不被描述为 privacy coin。Owner commitment 在授权发生前隐藏 raw public key，但 transaction graph 仍可能暴露关联；multi-input authorization group 更会明确证明其覆盖输入具有共同授权。

共识中的身份是 cryptographic identity，而不是组织身份。网站、公司、miner、archive provider 或高性能机器都没有能力把 invalid bytes 变成 valid consensus data。

10.2 当前 Sybil-resistance 原则与计划审计

BitFP 不使用 one-identity-one-vote 共识。创建更多 protocol identity 本身不会产生 validity authority、chain work、block probability、receipt entitlement 或 reward；mining influence 与 partial-work receipt 都必须由有效 PoW work 支撑。Mining identity 可以低成本创建并保持 pseudonymous，因此观测到的 active mining identity 数量不等于独立人类或机器数量。一个 operator 可以控制多个 identity，一个 identity 也可以代表多台机器。

这些性质是当前设计约束，不是整个系统已完成 Sybil-resistance 证明。BitFP Sybil Resistance Audit v0.1 状态为 PLANNED / NOT_STARTED。计划范围包括：在总物理 work 相同时的 economic identity splitting；P2P Sybil、eclipse 与 network partition 压力；大规模自主 Agent identity；diagnostics/maintenance report flooding、clustering、deduplication 与 AI cost amplification；以及公开 mining breadth/concentration 指标的稳健性。BitFP 当前不宣称已经被证明为 Sybil-proof。

10.3 计划中的 Optional Post-Quantum Privacy 协议研究

BitFP 当前使用透明、pseudonymous 的交易。协议级 shielded transaction 当前尚未实现。计划中的 Optional Post-Quantum Privacy Architecture Review v0.1 将比较：

- Candidate A: transparent-only baseline；
- Candidate B: transparent UTXO + optional post-quantum shielded pool + selective disclosure；
- Candidate C: private-by-default 或 mandatory privacy。

待评估的设计目标是：默认公开，可选隐私，全程面向后量子安全。研究范围包括 shielded note、note commitment、nullifier、authenticated shielded state、double-spend prevention、value conservation、zero-knowledge requirements、post-quantum recipient encryption、selective view/audit capability、metadata 与 linkage leakage、anonymity-set behavior、agent-native wallet interface、fee 与 transaction weight、proof/prover/verifier cost、mobile verification、commodity full-node 资源，以及任何 proposal 会影响的 M6/M7/M8 interface。

目前没有选择 PQ KEM、commitment construction、note format、privacy relation、selective-disclosure key model 或 anonymity guarantee。当前没有 shielded pool、hidden-value transaction、hidden sender/recipient protocol、finalized post-quantum privacy construction 或 finalized anonymity guarantee。架构仍须经过正式 review 与人类协议决策。如果 privacy 被纳入初始协议，M10 必须继续被阻塞，直到所有受影响的 frozen interface 都被明确 version、amend 并重新验证；如果 privacy 被 deferred，则当前透明协议仍是唯一真实 baseline。

11. 安全性计算

比特币白皮书用公式分析攻击者从区块差距中追赶 honest chain 的概率。BitFP 保留这类链重组分析，并加入 proof-system 的具体安全性计算。

11.1 链追赶概率

设 honest work fraction 为

$$p=1-q,$$

其中 q 是 adversarial work fraction。若 $q \geq p$ ，最终 catch-up probability 为 1。若 $q < p$ ，当 honest chain 领先 z 个 blocks 时，比特币白皮书用 mean 为 [1]

$$\lambda = z \frac{q}{p}$$

的 Poisson distribution 建模 attacker progress。Catch-up probability 为

$$P_{catch}(z, q) = 1 - \sum_{k=0}^z \frac{e^{-\lambda} \lambda^k}{k!} \left[1 - \left(\frac{q}{p} \right)^{z-k} \right].$$

BitFP receipt/reward maturity policy 使用 modeled bound

$$q \leq 1/3$$

以及 target

$$P_{catch} \leq 10^{-9}.$$

当 $q=1/3$:

- Depth $z=104$ 时, $P_{catch}=1.06480248 \times 10^{-9}$, 未达到选择的 target。
- Depth $z=105$ 时, $P_{catch}=8.77327768 \times 10^{-10}$, 达到 target。

因此 104 未达目标, 105 PASS。Containing block 记为 depth zero, 所以 maturity 定义为 105 canonical descendants。

11.2 精确 field challenge sampling

Production profile 使用 SHAKE256 派生 Fp8 challenge, 并使用 exact rejection sampling, 而不是简单 modulo reduction。

令

$$N = p^8, Q = 2^{512},$$

定义

$$L = \text{floor}\left(\frac{Q}{N}\right)N.$$

均匀抽取满足 $0 \leq X < Q$ 的 512-bit integer X 。只有当

$$X < L$$

时接受, 并输出

$$c = X \bmod N.$$

每个 residue 在 accepted range 中恰好有 $\text{floor}(Q/N)$ 个 preimages, 因此在接受条件下 c 对 field representation 是精确 uniform。Reject 时按冻结 domain/counter 规则重新抽样。

11.3 LogUp false identity 的概率直觉

如果 LogUp rational identity 两边不相等, 清除 denominator 后得到非零 polynomial $g(\beta)$ 。若其 degree 至多为 d , field 为 F , 则随机 challenge 错误通过的概率至多为

$$\Pr[g(\beta)=0] \leq \frac{d}{|F|}.$$

冻结 M8 ledger 执行的是实际 protocol-specific union accounting; 其 Fp4 LogUp screen 约为 220 bits。

11.4 Fixed-Keccak 假设

Proof reduction 在 random/product-oracle model 中推理，而实际 implementation 使用固定 FIPS 202 Keccak constructions [2]。BitFP 因此明确声明一个假设，而不是说 “Keccak 被证明是 random oracle”：

M8-FIXED-KECCAK-PRODUCT-QRO-Q64-ADV160-V1

该假设把相关 distinguishing/forgery contribution 限制为

$$\epsilon_K \leq 2^{-160}$$

并限制 adversarial quantum query budget

$$q_{QRO} \leq 2^{64}.$$

11.5 Composed post-quantum soundness

记主要 failure term:

- ϵ_{CMS} : four-session CMS19/product-QRO;
- ϵ_{LU} : Fp4 LogUp union;
- ϵ_{PCS} : PCS cross-opening;
- ϵ_K : fixed-Keccak instantiation。

保守 composition 为

$$\epsilon_{total} \leq \epsilon_{CMS} + \epsilon_{LU} + \epsilon_{PCS} + \epsilon_K.$$

定义 concrete security bits:

$$b_{sec} = -\log_2(\epsilon_{total}).$$

冻结 ledger 中展示的 component strength 为:

- Four-session CMS19/product-QRO: **146.521195714087 bits**。
- Fp4 LogUp union screen: **219.999977986389 bits**。
- PCS cross-opening screen: **234.977632186972 bits**。
- Fixed-Keccak instantiation assumption: **160 bits**。

使用内部 full-precision term，冻结 M8 composed result 为

$$b_{sec} = 146.521069347829899925285615048305 \text{ bits}$$

高于选择的 post-quantum target:

$$146.5210693478 - 128 \approx 18.5211 \text{ bits}.$$

Displayed term 中 dominant contribution 是 CMS19/product-QRO, 因此仅提高已经更强的 LogUp 或 PCS margin, 并不会显著提高最终 composed total。

11.6 Production proof evidence

最终 M9 package 使用

$$N_T = N_L = 4,194,304$$

条 transition 与 lookup rows。六-lane production package 通过 native 与 independent verification, 认证 1,048,656 reads、覆盖 257,387 个 distinct dataset address, 拒绝 29 个 production tamper case, 并通过 Receipt/BlockCandidate binding。

这些属于 frozen relation 的 implementation evidence, 不替代上面的 security assumptions。

12. Agent Discovery 作为验证协议

对 Agent-native chain, discovery 不能等同于 DNS lookup。设 m 为从某个 source 得到的 candidate network manifest。Agent 只有在类似下列 predicate 为真时才应接受:

$$\begin{aligned} \text{AcceptManifest}(m) = & \text{ValidSyntax}(m) \wedge \text{Fresh}(m) \wedge \text{SignaturesValid}(m) \\ & \wedge \text{RootsValid}(m) \wedge \text{Corroborated}(m) \wedge \text{ConsensusIDsMatch}(m). \end{aligned}$$

Corroboration 明确要求多来源。bitfp.org 可以帮助 Agent 找 candidate facts, 但不能单独使这些 facts 成为 authoritative。

目标 discovery flow:

discover candidate sources

- > corroborate independent origins
- > verify signatures / release roots
- > verify network + genesis identity
- > verify PARAM-01 / PARAM-02 / PARAM-03
- > verify relation + compiler identity
- > discover peers
- > negotiate capabilities
- > choose node role
- > sync
- > independently verify blocks

Canonical public discovery entry:

GET https://bitfp.org/.well-known/bitfp.json

并且 endpoint 明确声明网站不是 root of trust。

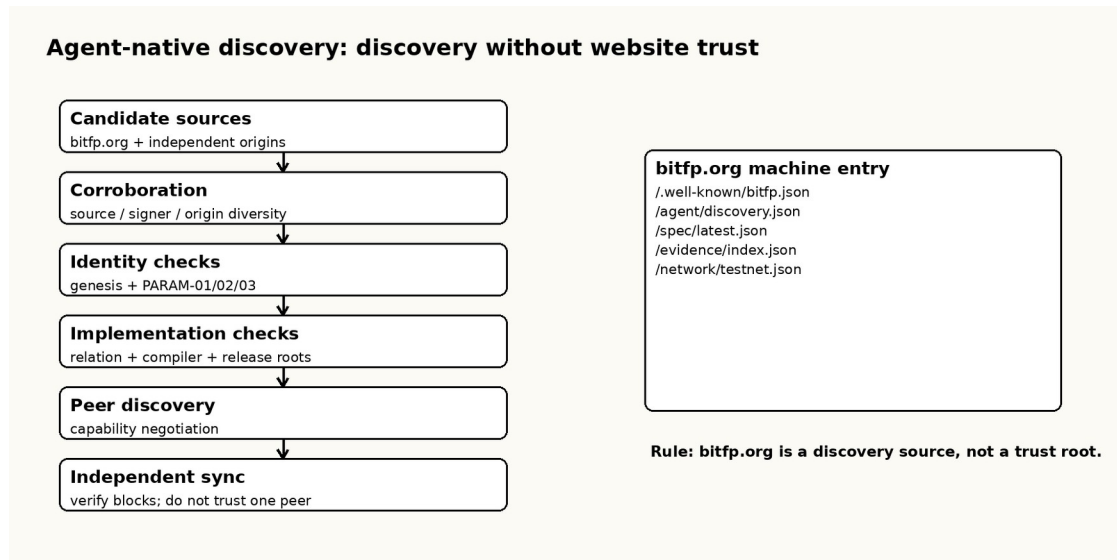


图 4。Discovery 是 verification graph；website 只是其中一个输入。

13. 实现状态与明确 Non-Claims

当前：

- M6/G6: PASS - PARAM-01 与 PARAM-02 frozen;
- M7/G7: PASS - final source-exact C1 relation frozen;
- M8/G8: PASS - fixed-Keccak/QROM/PQ128 closure, PARAM-03 frozen;
- M9/G9: PASS - production 4M six-lane package 与 Receipt/BlockCandidate PASS;
- Huawei Mate Xs mobile PoW: PASS;
- Agent Discovery v1 architecture: READY;
- commodity full-node scaling: IN PROGRESS / PRE-M10 gate;
- BitFP Sybil Resistance Audit v0.1: PLANNED / NOT_STARTED;
- Optional Post-Quantum Privacy Architecture Review v0.1: PLANNED / NOT_STARTED / NOT_IMPLEMENTED / NOT_CONSENSUS_FROZEN;
 - M10 integrated testnet: NOT STARTED;
 - mainnet: NOT LIVE.

BitFP 当前不宣称：

- specialized hardware 永远不能比 commodity hardware 更快；
 - Keccak 被证明等价于 random oracle；
 - 整个系统具有 unconditional quantum safety；
 - 手机挖矿已经证明经济竞争力；
 - production-independent bootstrap 已完成；
 - 在 PRE-M10 service-time gate PASS 前，commodity full validation 已经完成。
- multi-layer Sybil audit 已经 PASS；
 - BitFP 已被证明为 Sybil-proof；
 - 当前已经存在 shielded、hidden-value、hidden-sender、hidden-recipient 或 finalized post-quantum privacy 功能。

14. 结论

BitFP 遵循让 Bitcoin 白皮书长期耐读的同一条基本推理链：定义 ownership，定义时间排序，定义 work，定义网络行为，定义激励，再量化相关攻击概率。它保留 Bitcoin 最核心的思想——用可验证的 proof 替代制度性 trust——但围绕三个新的问题重新设计协议。

第一，挖矿不能在协议结构上把普通电脑排除在外。BitFP 因此组合 source-exact data-dependent workload、每 worker 私有 memory、serial dependency、epoch rotation 与 protocol-native partial-work receipt。它不保证不同硬件效率相同，也不宣称 ASIC 不可能存在；它要保留的是一条直接路径：只要一台机器能够产生有效 work，就可以直接参与，而不需要仅为了获得奖励认可就被迫进入矿池。

第二，一条新链应当从一开始就面对后量子威胁。Ownership 使用 ML-DSA-44。C1 proof system 另行冻结 fixed-Keccak/QROM security profile，在明确假设下 composed screen 为 146.521 bits。两层安全性有意分开，不能混为一个模糊的“量子安全”口号。

第三，自主 Agent 应当能够自己发现和验证网络。BitFP 把 consensus identity、manifest、node capability、release root 与 evidence 做成 machine-readable，同时拒绝把 bitfp.org 或任何单一 origin 变成 trust root。

经济模型服务于同一个长期目标。21M 是 reference scale，而不是 terminal hard cap；BitFP 也不会之后设置 24M hard ceiling。Nominal 52,500 BFP/year tail 为 security budget 保留可预测的 issuance component，同时随着 supply 增长，其百分比扩张率逐渐趋近于零。这是一个明确取舍：与其强制未来网络安全完全依赖 transaction-fee demand，BitFP 更愿意接受很小、长期存在的 nominal issuance。

技术上，work function 不是单次 nonce hash，而是冻结的 source-exact、data-dependent computation，包含 worker 私有状态和 serial tail。Block 与 receipt threshold 仍然是普通的 512-bit target test，因此成功概率可以明确写出。昂贵 work 不由 validator 重做，而被表示为 relation $R_{\text{BitFP}}(x, w)$ ，并由六个 coupled lane 证明。LogUp 认证 source-exact dataset read，PCS cross-opening 则把这些 value 与真正消费它们的 transition 绑定。Receipt maturity 使用 Bitcoin 风格 Poisson catch-up calculation 推导。

当前剩余 PRE-M10 challenge 主要是工程问题而不是概念问题：native full-node six-lane verifier 必须在 commodity hardware 上获得足够的 service-time headroom。BitFP 不会在 measurement evidence 真正 PASS 之前宣称这个 gate 已完成。

PRE-M10 roadmap 现在把两项需要 human review 的研究 gate 排在 physical commodity-machine closure 与 external evidence 之后：正式 Sybil Resistance Audit 与 Optional Post-Quantum Privacy Architecture Review。把它们记录到 roadmap，不等于已经增加 privacy 功能、冻结 privacy semantics，或重新打开 frozen M6/M7/M8 protocol；它只是确保这些未决问题在任何 M10 authorization decision 之前被清楚呈现。

References

- [1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.
<https://bitcoin.org/bitcoin.pdf>
- [2] National Institute of Standards and Technology, *FIPS 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, 2015.
<https://doi.org/10.6028/NIST.FIPS.202>
- [3] National Institute of Standards and Technology, *FIPS 204: Module-Lattice-Based Digital Signature Standard*, 2024. <https://doi.org/10.6028/NIST.FIPS.204>
- [4] A. Chiesa, P. Manohar, N. Spooner, *Succinct Arguments in the Quantum Random Oracle Model*, TCC 2019 / Cryptology ePrint 2019/834.
- [5] G. Arnon, A. Chiesa, G. Fenzi, E. Yogev, *WHIR: Reed-Solomon Proximity Testing with Super-Fast Verification*, Cryptology ePrint 2024/1586.
- [6] U. Haboeck, *Multivariate Lookups Based on Logarithmic Derivatives*, Cryptology ePrint 2022/1530.
- [7] BitFP Project, *BitFP M6 Consensus Parameter Specification v1* and M6.2 freeze audit.
- [8] BitFP Project, *BitFP M7 Final C1 Relation v1* and G7 source-exact dataset-authentication evidence.
- [9] BitFP Project, *BitFP M8 Fixed-Keccak / QROM Security v1*, PARAM-03 specification, and G8 security-closure audit.

[10] BitFP Project, *M9 G9 Production 4M Closure Audit*.

[11] BitFP Project, *BitFP Agent Discovery v1* and PRE-M10 readiness audits.

文档状态： Pre-Testnet Draft v0.5。

Canonical public discovery surface： <https://bitfp.org/>

Mainnet： 未上线。

Public testnet： 本草案发布时尚未上线。