承诺证明：一种以人为本的无许可共识资源

Homayoun Maleki 德乌斯托大学
DeustoTech 毕尔巴鄂，西班牙
h.maleki@deusto.es

Nekane Sainz
德乌斯托大学
DeustoTech
毕尔巴鄂，西班牙
nekane.sainz@deusto.es

Jon Legarda 德乌斯托大学
DeustoTech 毕尔巴鄂，西班牙
jlegarda@deusto.es

arXiv:2601.04813v1 [cs.DC] 8 Jan 2026

摘要

无许可共识协议需要一种稀缺资源来规范领导者选举并提供女巫攻击抵抗。现有范式——工作量证明（PoW）和权益证明（PoS）——通过可并行化资源来体现这种稀缺性，例如计算吞吐量或金融资本。一旦获得这些资源，便可将其划分给任意多个身份，而边际成本几乎为零。这意味着，在 PoW/PoS 风格的系统中，根本不可能实施线性女巫攻击成本。

我们提出承诺证明（*PoCmt*），这是一种以一种根本上不可并行化的资源为基础的共识原语：实时人类参与。每位验证者都维护一种可分解承诺状态，用以记录累积的人力投入、协议参与和在线可用性。参与度通过人类挑战预言机（HCO）来保障；该预言机会发布有时效性的、可由人类验证的任务，其解答与身份绑定，且必须在有限时间窗口内提交。因此，每个纪元可解答的挑战数量，天然受可用人类时间限制，与身份数量或资本无关。

在此模型下，维持 s 个活跃身份，每个人类时间窗口需要投入 $\Theta(s)$单位的人类时间。我们确立了一种明确的成本理论区分：任何权重资源可并行化的协议，其边际女巫攻击成本在渐近意义上都为零；而 PoCmt 则确保女巫攻击成本严格呈线性增长。基于加权骨干分析，我们证明，在部分同步条件下，PoCmt 能实现安全性、活性以及与承诺成比例的公平性；此外，若没有持续的线性人力投入，对抗方的承诺就无法超过诚实方的承诺。

我们还通过仿真补充分析，并将人类时间产能隔离为对抗方唯一的瓶颈。结果通过实证验证了承诺漂移不变量，表明仅增加身份数量或资本并不会增强影响力，并显示可用性衰减会抑制休眠或轮换的身份。综上，这些结果使 PoCmt 成为共识设计空间中的一个新方向，并将无许可安全性奠基于人类时间，而非计算或资本。

1 引言

开放网络中的无许可共识需要一种稀缺且可验证的资源，用于规范领导者选举并提供女巫攻击抵抗。经典范式将这种资源具体化为计算能力（工作量证明，PoW）[13] 或货币资本（权益证明，PoS）[7]。尽管这两种范式在实践中都取得了成功，但它们依赖的资源本质上都可并行化：一旦获得，算力或权益就能以可忽略的边际成本划分给任意多个身份。因此，PoW/PoS 系统无法强制实现线性女巫攻击成本：维持多个身份的成本渐近而言并不比维持一个身份高，而身份复制则成为对手放大的结构性途径。

超越可并行化资源。 本文探讨一种本质上截然不同的稀缺资源——它天生不可并行化，难以通过自动化实现，并与个体的人生轨迹紧密相连。我们的核心观察是，人类时间 和认知努力 恰好具备这些特性：每一单位可由人类验证的工作都必须由单个人完成，不能分割委托，也无法并行处理，除非增加在特定运行时段内积极参与的人数。

承诺证明（PoCmt）。 我们提出承诺证明（*PoCmt*），这是一种无许可共识原语，其验证者影响力源自实时、可由人类验证的参与 ，而非机器或资本。每个验证者都维护着一个三维承诺状态

$$S_v(t) = \big(H_v(t),\, P_v(t),\, U_v(t)\big),$$

该状态记录累积的人类参与、协议参与和在线可用性。这些组成部分按照确定性的增强、衰减和罚没规则演变，形成随时间变化的承诺分数，并直接决定领导者选举权重。

人力投入通过人类挑战预言机 （HCO）形式化，该预言机会发出与身份绑定的时限挑战，必须在有限的纪元内完成。关键在于，每个纪元内最多只能解决有限数量的挑战，与对手控制的身份数量无关。解决一个验证者的挑战并不会给另一个验证者带来任何优势，而自动化求解器成功的概率可以忽略不计。因此，在每个人类时间窗口内，维持 s 个活跃参与的身份必然需要 $\Theta(s)$ 单位的人类时间。

一种新的女巫攻击抵抗机制。 PoCmt 在基于可并行化资源的共识协议与以人类时间为基础的共识协议之间，形成了成本理论上的区分。具体而言，我们证明：

- 任何权重资源可并行化的协议（例如哈希算力或权益）都存在零边际女巫攻击成本，因为身份可以在不额外消耗资源的情况下复制；
- PoCmt 强制实现线性女巫成本：要在T 个纪元内维持 s 个身份，需要投入 $\Theta(sT)$ 单位的人力，而且对手的承诺若想超过诚实方的承诺，就必须持续支付这一成本；
- 在标准部分同步假设下，PoCmt 中的承诺加权领导者选举满足骨干式安全性、活性和比例公平性。

人类时间为何重要。 传统上，人类参与仅作为一次性的身份门槛出现，例如验证码或人格证明仪式。PoCmt 将人类时间提升为持续、可量化且与共识息息相关的资源。这一转变从根本上改变了女巫攻击抵抗的格局：对抗方的影响力不再受硬件、资本或身份创建的限制，而是受持续的人力投入所限——这种资源既稀缺、具有经济价值，又天生不可并行化。

贡献。

- 我们提出 PoCmt，这是首个以不可并行化的人类时间为基础的共识原语，并通过可分解的承诺状态对其进行形式化。
- 我们定义了人类挑战预言机（HCO），用于刻画与身份绑定、抗人工智能的参与度，并明确纳入实时约束。
- 我们证明了成本理论上的区分：可并行化资源协议的边际女巫攻击成本为零，而 PoCmt 则要求对抗方付出 $\Theta(sT)$ 成本，才能在 T 个纪元内维持 s 个身份。
- 通过加权骨干分析，我们证明了在部分同步条件下的安全性、活性和公平性，并刻画了对抗方取得多数所需的人力投入。
- 我们展示了仿真结果：仿真将人类时间容量设为唯一的对抗方瓶颈，并以实证方式验证了承诺漂移、公平性，以及对休眠或轮换身份的抑制。

范围与激励机制。 我们的分析聚焦于在标准的诚实但参与假设下，将人类时间用作权重资源所带来的安全后果。对持续参与的激励机制进行建模——包括疲劳、流失、放弃和验证者替换——与成本理论上的区分正交；我们在第 8 节中明确将其作为部署限制加以讨论。

PoCmt 表明，无许可共识不必仅锚定于由机器主导的资源。通过以人类时间为安全基础，它在共识设计空间中确立了一个性质全新的位置，并拓展了抗女巫攻击区块链协议的理论基础。

2 背景与相关工作

女巫攻击抵抗与基于资源的共识。 女巫攻击——以可忽略的边际成本创建大量身份——是开放成员系统面临的根本障碍 [3]。无许可共识协议通过将影响力与一种假定稀缺的资源挂钩来应对这一挑战。在工作量证明（PoW）中，影响力与计算努力成正比 [13], ；而在权益证明（PoS）中，影响力则与锁定资本成正比。大量研究在骨干式框架及相关模型下形式化分析了此类协议的安全性与活性 [1, 7, 14], ，并研究了自私挖矿 [6] 、高出块率或分叉动态 [15] 等策略性偏离。经过严格分析的代表性 PoS 协议包括 Ouroboros [9], ；相关研究还考察了部分同步条件下的参与流失和“休眠”验证者 [14]。

PoW 和 PoS 共有一个根本局限：它们的权重资源——哈希算力和权益——在经济层面可并行拆分：一旦获取，就可以在几乎不增加边际成本的情况下拆分到任意多个身份之中。因此，这类系统无法实现线性女巫成本；这一现象已在我们的成本理论分析（第 5 节）中得到形式化论证。

为将 PoCmt 置于更广阔的背景中，表 1 根据底层资源的性质、其可并行化程度以及由此形成的女巫攻击成本特征，总结了既有的女巫攻击抵抗方法。值得注意的是，该表区分了共识加权资源 与身份或访问机制，并指出以往工作尚未将不可并行化的人力投入与持久且随时间演变的共识权重结合起来。

领导者选举、委员会与 *BFT* 最终性。 PoCmt 的协议层建立在领导者选举和最终性的标准原语之上。承诺加权抽签可通过可验证随机函数（VRF） [11] 实现，并用于抽选领导者和委员会，正如 Algorand [8, 10]等基于委员会的设计所采用的那样。对于确定性最终性，PoCmt 兼容经典和现代 BFT 协议，包括 PBFT [2] 和 HotStuff [17]。我们的贡献与这些协议机制正交：我们引入一种新的权重资源，并分析部分同步条件下由此产生的安全性和活性属性 [4]。

其他资源类别。 除计算和权益之外，还有若干提案将共识影响力与其他可由机器控制的资源挂钩，包括存储、带宽或可信硬件。空间证明和基于存储的方案依赖磁盘容量作为稀缺资源 [5],，而可信硬件方案则以对安全飞地或计时器的假设取代经济稀缺性。尽管这些设计改变了激励结构或能源成本，但其底层资源仍然可机器并行化，并可通过资本投资扩展。相比之下，PoCmt 针对的是一种稀缺类别，其限制因素是每个运行时段内的人类时间，而这一天然受限于积极参与的人数。

基于身份和人在环机制的方法。 一条不同的研究路线通过约束或验证身份来寻求女巫攻击抵抗，而不是依据某种资源为身份赋予权重。基于图的防御机制利用社交网络结构 [18], ，而人格证明仪式则旨在通过不同的信任假设近似实现“一个人，一个身份” [12]。验证码等人工验证机制 [16] 利用认知难度差异，但被部署为一次性访问门槛。这些方法并未定义持久且随时间演化的共识权重，因此无法直接与领导者选举或骨干式安全性和活性分析相结合。

与 *PoCmt* 的关系。 PoCmt 在概念上不同于机器资源共识（PoW/PoS 及其变体）和以身份为核心的女巫攻击防御。它并不强制实行一人一身份，而是将人类参与度建模为一种稀缺、不可并行化且有时限的资源，必须持续补充。通过反复执行人类挑战预言机（HCO）任务和承诺状态演化，PoCmt 引入了一种数学定义的、以人为中心的加权信号，可直接整合

资源类型	可并行化	女巫攻击成本特征	代表性系统
计算能力	Yes	次线性／零边际成本	PoW（比特币）[13]
货币资本	Yes	次线性／零边际成本	PoS；Ouroboros [9]
存储／空间	Yes	次线性	SpaceMint [5]
可信硬件 / 计时器	Yes	次线性	PoET；基于 SGX 的设计
社会身份图	部分	有界（非经济型）	SybilGuard [18]
一次性人工验证	否（一次性）	固定设置成本	验证码 [16]；人格证明 [12]
人类时间（PoCmt）	**No**	**每个纪元线性增长**	**PoCmt（本文工作）**

表 1：女巫攻击抵抗机制分类。可并行化资源使身份复制成本低廉，因此其边际女巫攻击成本呈次线性或为零。身份与访问机制（例如验证码或人格证明）限制身份创建，但不定义持久共识权重。PoCmt 则独特地从一种不可并行化、受时间限制的人类资源中推导领导者选举权，从而确保每个活跃身份在每个纪元都承担线性女巫成本。

到标准的领导者选举和安全性分析中。据我们所知，先前的工作尚未提出一种正式的共识框架，在该框架中，每个纪元的人类时间是支配领导者选举权的根本稀缺资源。

3 模型与人类时间资源

我们介绍承诺证明（PoCmt）的形式化模型。其核心设计目标是将共识权重建立在不可并行化的人类时间资源之上，同时保留基于纪元的领导者选举和标准的主干式推理。

3.1 时间模型：纪元与人类响应窗口

PoCmt 将时间划分为两个相互耦合的层次。

共识纪元。协议以离散的共识纪元 $t = 0, 1, 2, \ldots$推进，每个纪元对应固定的挂钟时间长度 Δ_e（例如，几秒或几分钟）。领导者选举、区块提议和分叉选择均在这一时间尺度上执行。

人类时间窗口。人类可验证挑战以较粗粒度的人类时间窗口为尺度发布，并由 $d = 0, 1, 2, \ldots$进行索引（例如，按天计）。每个人类时间窗口跨越 Δ_h 个时间单位，包含 $E = \Delta_h/\Delta_e$ 个共识纪元。我们将 $d(t)$ 记作包含纪元 t 的人类时间窗口。

这种双时间尺度结构反映了实际运行情况：区块生产十分频繁，而人类参与的频率自然受到限制，通常每天只进行少数几次。

3.2 承诺状态与分数

每个验证者 v 都会维护一个承诺状态

$$S_v(t) = \big(H_v(t), P_v(t), U_v(t)\big),$$

其中：

- $H_v(t)$ 表示累积的人类参与，
- $P_v(t)$ 表示协议参与和诚实性，• $U_v(t)$ 表示在线可用性。

用于纪元 t 领导者选举的承诺分数为

$$CS_v(t) = \alpha H_v(t) + \beta P_v(t) + \gamma U_v(t),$$

对于固定的非负权重（α、 β、 γ）。

3.3 人类挑战预言机（HCO）

PoCmt 通过人类挑战预言机 （HCO）将人类时间建模为一种不可并行化资源。与按纪元运行的挑战机制不同，HCO 在每个人类时间窗口内只发起少量挑战。

挑战率与难度。 对于每个人类时间窗口 d，协议都会指定一个挑战率 $k(d) \in \mathbb{N}$。此参数用作窗口级别的难度 调节参数：预期每个验证者在时间窗口 d内最多解答 $k(d)$ 个挑战，以保持充分参与。

对于每个验证者 v和索引 $j \in \{1, \ldots, k(d)\}$，预言机都会输出一个新的挑战

$$\chi_{v,d,j} \leftarrow \mathrm{HCO}(v, d, j).$$

预言机假设。 HCO 满足以下性质。

(H1) 时间限制下的人类优势。对于部署的 d 操作难度为 d的挑战族，诚实的人类可在 Δ_{resp} 内以高概率解答，而任何可行的自动化求解器成功的概率至多为 $\varepsilon(d)$，其中 $\varepsilon(d)$ 足够小，以满足安全要求。**(H2) 身份绑定**。 每个挑战都绑定到 (v, d, j)；解答无法在不同验证者或挑战索引之间重复使用。**(H3) 实时约束**。 解答必须在较短的响应窗口 Δ_{resp}内提交，以防止预计算和长期囤积。**(H4) 人类时间并行性上界**。 单个人类在每个人类时间窗口内最多可解答 $\tau_h = O(1)$ 个挑战，不受其控制的身份数量影响。如果攻击者雇用 m 个人类，则一个时间窗口内可解答的挑战总数至多为 $m \cdot \tau_h$。

在本文余下部分，我们将对抗方人类时间容量定义为 $M = m \cdot \tau_h$，表示每个时间窗口内可解决的挑战总数。所有界限均相对于 M 给出。

并行性上界。 如果对手控制 s 个身份并雇用m 名人类，那么在任意时间窗口 d内解决的挑战总数至多为 $m \cdot \tau_h$。因此，要以难度 $k(d)$维持 s个身份，就需要

$$m \geq \Omega\left(\frac{s \cdot k(d)}{\tau_h}\right),$$

确立身份数量上的线性女巫成本。

设想中的挑战有哪些类型？ HCO 是一种理想化原语，但预期的具体实现更接近受速率限制、与身份绑定的活性和注意力测试，而非一次性的账户创建验证码。具体而言，挑战可以实现为交互式微任务，要求 (i) 人类在短时间内实时响应，(ii) 与验证者密钥及当前窗口标识符绑定，(iii) 能够公开验证格式正确的响应记录。示例包括带有随机提示、限时完成的感知／匹配任务，或随机性在窗口边界生成、从而防止预计算的轻量级交互式协议。在实际部署中，这类挑战可以通过轻客户端（由用户界面引导）作答，并通过与验证者密钥和窗口标识符绑定的可公开验证的记录进行验证。

为何这一假设可与共识机制分离。我们的协议和证明将 HCO 视为不可并行化性的来源：只要具体实现保留分析中用到的两项性质——身份绑定（H2）和每个时间窗口内每人的解题速率上界（H4）——任何实现方式都可以接受。我们强调，PoCmt 并不要求人类具有全局唯一性（不同于 Proof-of-Personhood）；它只要求每个新增的活跃身份都需要额外的同期人力投入，而这正是定理 5.3 背后的核心障碍。

分析所用的最简 *HCO* 接口。形式上，我们的安全性论证仅依赖 HCO 的以下两项性质：(i) 在每个时间窗口使用新鲜随机性的情况下，不同身份之间不可重复使用（H2）；(ii) 每个时间窗口内每人的解题速率上界（H4）。只要这两项保证成立，其他方面（任务格式、用户体验、交付渠道和验证基础设施）都与共识层无关。这样一来，共识证明便不依赖于任何特定的类似验证码的实现。

人机差距假设。 PoCmt 的安全性依赖于这样一类任务的存在：在有限时间窗口内，人类相较于自动化求解器仍保有不可忽略的优势。与密码学困难性假设一样，这种差距被视为一种建模假设，而非永久保证。关键在于，PoCmt 不要求任务在全球范围内或无限期地仅由人类完成：只要在每个运行时段内，存在一类挑战，其自动化成功概率相对于人类实时表现始终足够低即可。我们在第 8 节将这一假设在自动化不断进步下长期易受冲击的问题，作为一项明确的局限性重新讨论。

分析所需的最小假设。 重要的是，PoCmt 的安全性证明仅依赖于 HCO 的两项性质：(i)身份绑定，防止解决方案在不同身份之间重复使用或转移；(ii) 对每个时间窗口内每个人可解决挑战数量的速率上限 。除这些性质外，不对挑战的语义内容作任何假设。任何满足这些约束的构造，都能保留第 5 节和第 6 节中的所有定理。

3.4 承诺动态

承诺按照以下规则确定性地演变。

人类参与（时间窗口加成）。设 $x_v(d) \in \{0、\ldots\ldots、 k(d)\}$ 为验证者 v 在人工时间窗口 d内解决的挑战数量。在时间窗口 d 和 d+1的边界处，

$$H_v(d{+}1) = H_v(d) + \kappa_h \cdot x_v(d).$$

在一个时间窗口内， $H_v(t)$保持不变。

可用性更新。 在每个共识纪元 t，

$$U_v(t{+}1) = \begin{cases} U_v(t) + \kappa_u, & \text{if } v \text{ is online,} \\ U_v(t)e^{-\lambda}, & \text{if } v \text{ is offline,} \end{cases}$$

对于参数 $\kappa_u > 0$ 和 $\lambda > 0$。

参与和罚没。 如果 v 在纪元 t遵循协议，

$$P_v(t{+}1) = P_v(t) + \kappa_p.$$

如果 v 双重签名或违反协议规则，

$$P_v(t{+}1) = \delta\, P_v(t), \quad 0 < \delta < 1.$$

分数重新计算。 应用所有更新后，承诺分数将重新计算为

$$CS_v(t{+}1) = \alpha H_v(t{+}1) + \beta P_v(t{+}1) + \gamma U_v(t{+}1).$$

这种动态机制清晰地区分了人力投入、协议行为和可用性，同时生成一个随时间变化的权重，供共识协议使用。

参与假设与激励机制（范围）。 我们的核心定理遵循标准的“诚实但参与”假设：诚实验证者会继续执行协议，并在需要时提供规定的人类参与。我们不会在安全性证明中对效用、疲劳、流失或验证者替换建模，因为成本理论上的区分取决于人类时间的不可并行化 特性，而非任何特定的奖励机制。因此，激励机制和持续投入方面的考量被视为正交的部署问题，并在第 8 节中作为局限性和设计空间明确讨论。

4 PoCmt共识协议

现在我们来介绍 PoCmt 共识协议。PoCmt 将基于人类时间的承诺资源整合进无许可共识机制，同时保持与经典的领导者选举、链增长和最终性框架兼容。PoCmt 的一个关键设计特点是采用两个相互耦合的时间尺度运行：较频繁的共识纪元 和较粗粒度的人类响应窗口，具体形式化定义见第3节。

4.1 双时间尺度执行模型

时间被划分为离散的共识纪元 $t = 0$，1，2，……，用于驱动领导者选举、区块提议和消息交换。与此同时，时间被划分为人类时间窗口 $d = 0$，1，2，……，每个窗口涵盖多个纪元（例如一天）。

验证者 $v, S_v(t) = (H_v(t)\ P_v(t)\ U_v(t))$ 的承诺状态在两个时间尺度上演化：

- **人类参与** H_v仅在人工窗口边界更新，其依据是在该时间窗口内发布的人类挑战预言机（HCO）挑战的解决情况。

• **参与** P_v 和**可用性** U_v 在每个纪元更新一次，反映协议行为和在线状态。

在给定的人类时间窗口内，人类参与度成分 H_v 保持不变。因此，承诺分数在各纪元间平滑变化，确保人类时间作为一种持续且缓慢变化的资源发挥作用，而非每纪元一次的信号。

4.2 协议概述

PoCmt 通过重复执行一系列窗口级操作和纪元级操作来运行。

窗口级操作。在每个人类时间窗口d开始时：

(1) HCO 向每个验证者 v 发出 $k(d)$ 个新的身份绑定挑战 $\{\chi_{v,d,j}\}_{j=1}^{k(d)}$。(2) 验证者在预言机指定的实时响应窗口内提交解答。(3) 记录每个验证者 v 成功解决的挑战数量 $x_v(d) \in \{0,\dots,k(d)\}$。(4) 在窗口边界处，人类参与度状态更新如下

$$H_v(d{+}1) = H_v(d) + \kappa_h \cdot x_v(d).$$

纪元级操作。 对于当前人类时间窗口内的每个共识纪元 t：

(1) 验证者交换共识消息，并参与区块提议与验证。(2) 参与度评分 $P_v(t)$ 会更新；双重签名或其他协议违规行为会触发罚没。(3) 观察在线状态；可用性分数 $U_v(t)$ 会增加或衰减。(4) 承诺分数

$$CS_v(t) = \alpha H_v(d(t)) + \beta P_v(t) + \gamma U_v(t)$$

会重新计算。
(5) 使用承诺加权随机性执行领导者（以及可选的委员会）选举。

这种分离确保人类时间会在多个纪元中持续影响共识权重，而快速时间尺度的动态则保障安全性与活性。

4.3 基于承诺的领导者选举

PoCmt 假设可以访问公共随机源，该随机源通过可验证随机函数（VRF）、阈值随机性或外部信标链实现。

每个验证者 v 持有一个 VRF 密钥 sk_v，并计算

$$r_v(t) = \mathsf{VRF}(\mathrm{sk}_v,\ t \,\|\, \mathsf{rand}(t)).$$

如果满足以下条件，验证者 v 就有资格在纪元 t 中提议区块

$$r_v(t) < \tau_v(t), \qquad \tau_v(t) = \Theta \cdot \frac{CS_v(t)}{\sum_{u \in V(t)} CS_u(t)},$$

其中，Θ 的取值应使每个纪元中合格领导者的预期数量接近 1。

由于 H_v 仅在人工窗口边界处发生变化，因此在每个时间窗口内，领导者选举概率呈分段常数。这避免了由自动化驱动的影响力快速放大并直接实现了承诺比例抽样，这是引理 6.7 中公平性分析的基础。

可选的委员会组建。 PoCmt 还可以使用相同的 VRF 输出抽选委员会，以用于 BFT 式共识。每个验证者均以独立概率被选中

$$p_v(t) = c \cdot \frac{CS_v(t)}{\sum_{u \in V(t)} CS_u(t)},$$

其中，参数 c 用于控制委员会规模。这使 PoCmt 兼容 HotStuff 或 Algorand 式的最终性机制。

4.4 区块提议与验证

如果 ℓ_t 在纪元 t中被选为领导者，则它会提出一个包含以下内容的区块 B_t：

- 父哈希，
- 纪元编号 t，
- 交易集合，
- VRF 资格证明，
- 领导者签名，
- 与近期承诺更新相关的可选证据（例如，窗口级 HCO 解答记录）。

收到 B_t 后，验证者会执行以下检查：

(1) 验证可验证随机函数证明和领导者签名，(2) 检查与本地分叉选择的一致性，(3) 验证交易并检测双重签名，(4) 验证包含的任何承诺相关证据。

未通过任何一项检查的区块都会被拒绝，而有效的罚没证明则会被传播。

罚没条件。 如果验证者满足以下条件，则可被罚没：

- 在同一纪元生成冲突区块，
- 提交无效的可验证随机函数证明，• 伪造或歪曲承诺相关状态。

罚没会施加乘数惩罚 $P_v \leftarrow \delta P_v$，并以 $0 < \delta < 1$ 为乘数，从而降低对抗权重，同时不抹去历史人工参与度。

4.5 分叉选择与可选最终性

PoCmt 支持两种部署配置 .

加权最长链规则。 验证者会选择使.....最大化的链

$$W(\text{chain}) = \sum_{B \in \text{chain}} CS_{\text{leader}(B)}(t_B),$$

其中 t_B 表示提出区块 B 的纪元。在加权诚实多数的情况下，诚实链的预期增长速度更快，满足骨干式链增长的要求。

可选的 *BFT* 式最终性。 PoCmt 可以整合类似 HotStuff 的最终性组件，验证者根据 $CS_v(t)$ 按比例赋予权重，对区块进行投票。当某个区块获得超过总承诺权重 2/3 的支持后，即可最终确定；在部分同步条件下，这将带来确定性最终性。

4.6 纪元和时间窗口时间线摘要

PoCmt 的执行过程可概括如下。

人类时间窗口 d:

(1) HCO 向每位验证者发出 $k(d)$ 挑战 $\{\chi_{v,\,d,\,j}\}$。(2) 验证者解答挑战，并在窗口边界更新 H_v。

窗口 d内的每个纪元 t:

(1) 交换共识消息；更新 $P_v(t)$。(2) 应用在线/离线状态；更新 $U_v(t)$。(3) 重新计算承诺分数 $CS_v(t)$。(4) 通过可验证随机函数选举领导者（以及可选的委员会）。(5) 领导者提出 B_t；验证者进行验证并更新分叉。(6) 传播并应用罚没证明。

至此，PoCmt 共识协议的描述完毕。

5 成本理论分析与女巫攻击抵抗

本节将 PoCmt 背后的成本模型形式化，并确立其核心保证：若要长期维持 s 个对抗方身份，就需要线性的人力时间投入，且与资本、硬件或网络带宽无关。我们还将证明，在影响力完全源自计算或权益等可并行化 资源的协议中，这一性质无法实现。

与经典模型的一个关键区别在于，PoCmt 中的人类参与以较粗粒度的人类时间窗口 为尺度演进（第3.1节），而共识执行则发生在细粒度的纪元中。因此，我们按每个时间窗口衡量对抗成本，并根据第 3.4 节中的承诺分数动态关系，将其转换为长期影响力。

5.1 对抗性投入模型

考虑一个控制着 A 个 s 身份的对手。每个对抗方身份 $a \in A$ 都维护一个承诺状态 S_a（t） =（H_a（t） P_a（t） U_a（t））,其定义见第3节。维持非平凡的承诺需要三种性质各异的资源:

- **人类时间成本 c_h：** 在每个人类时间窗口内解决 HCO 挑战 d，以增加（或维持增长） H_a。
- **协议/可用性成本c_P：** 保持节点在线并参与消息传递，以防止 U_a 衰减并积累 P_a。
- **罚没风险 c_s：** 因双重签名、无效行为或协调失败而导致参与度评分预期损失。

我们强调，c_P 和 c_s 可以由机器和资本承担，而 c_h 则不可避免地依赖人类认知努力。

窗口级核算。 设 $k(d)$为时间窗口 d中的挑战率（“难度”）（第 3.3 节）。设 $x_a(d) \in \{0,\dots,k(d)\}$为身份 a在时间窗口 d 内提交的有效解数量。根据第 3.4 节中的更新规则，随着$H_a(d+1) = H_a(d) + \kappa_h x_a(d)$，人类参与度会提高。因此，任何试图维持大量且参与度不断增长的身份的做法，都必须在每个时间窗口内持续提交大量有效解。

人类时间硬约束。 根据 HCO 假设（第 3.3 节），挑战与身份绑定且有时限，单个人类在每个时间窗口内最多可解决 $\tau_h = O(1)$ 个挑战。如果对手雇用 m 个人类，那么它在时间窗口 d内最多可解决 $m \cdot \tau_h$ 个挑战。

由此得到 PoCmt 背后的核心约束：

人类时间的可并行化程度，不会超过一个时间窗口内参与的人数。

5.2 PoCmt 中的线性女巫成本

现在，我们将线性人类时间壁垒形式化，并将其与承诺加权领导者选举下持续的对手影响力联系起来。

引理 5.1（时间窗口层面的线性人类时间需求）。固定一个人类时间窗口 d，其挑战率为 $k(d)$。对于任何维持 s 个身份、并在时间窗口 d 内总共提交了 $X(d) = \sum_{a \in A} x_a(d)$ 个有效 *HCO* 解答的对手，所需的人类时间满足

$$X(d) \;\le\; m \cdot \tau_h,$$

其中，m 是对手可用的人数。特别是，要让所有 s 个身份都达到 $x_a(d) \ge 1$（所有身份均有实质性参与），需要 $m = \Omega(s/\tau_h)$；要让所有身份都达到 $x_a(d) = k(d)$，则需要 $m = \Omega(sk(d)/\tau_h)$。

证明思路。根据 (H2) 身份绑定，解答不能在不同身份或挑战索引之间重复使用。根据 (H3)，响应窗口可防止预计算或囤积。根据 (H4)，每个人在每个时间窗口内最多能解决 τ_h 个挑战。因此，m 人在该时间窗口内最多能解决 $m\tau_h$ 个挑战，由此可得上述界限。□

引理 5.1 仅涉及每个时间窗口内的可行参与度。现在我们将其与对抗方相对于诚实验证者的承诺增长联系起来。

诚实方的增长基线。 在诚实但参与的假设下，诚实验证者会解决挑战，并以很高的概率保持在线，因此其承诺会单调增长：H 在窗口边界处增加，而 P 和 U 通常会随纪元推进而增加（第 3.4 节）。

对抗性不对称。 如果对手身份跳过 HCO 解答，其 H_a 会在窗口边界处停滞。如果它们离线，U_a 会呈指数衰减；如果它们行为不端，P_a 会受到乘法式削减。因此，若没有充足的人类时间容量，大型女巫集合中必然会有许多身份无法积累参与度，也无法维持较高的承诺分数。

引理 5.2（次线性人类时间意味着对抗方权重有界）。如果一个控制 s 个身份的对手每个时间窗口拥有 $m = o(s)$ 的人类时间容量（等价地，每个时间窗口解决 $m\tau_h = o(s)$ 个挑战），那么对抗方总承诺权重无法渐近地追上诚实方总权重。具体而言，对于足够长的时间，

$$W_A(t) \ll W_H(t),$$

其中，$W_A(t) = \sum_{a \in A} CS_a(t)$和 $W_H(t)$以类似方式定义。

证明概要。根据 $m = o(s)$，引理 5.1 表明，在每个时间窗口内，能够获得哪怕恒定数量有效解的身份，其比例也会趋于零。这些身份的 H_a停滞不前，并且由于可用性衰减和／或罚没风险，无法在总体上维持较高的 $CS_a(t)$。与此同时，诚实身份不断累积参与度并维持参与度／可用性，因此 $W_H(t)$

以严格更高的有效速率增长。这会形成持续的差距，因此 $W_A(t) \ll W_H(t)$ 渐近成立。□

现在陈述主要的成本理论结果。

定理 5.3（PoCmt 实现线性女巫成本）。要在W个人类响应窗口内持续维持s个具有实质性承诺的对手身份，需要

$$\Omega(sW)$$

单位的人力时间投入（等价地，$\Omega(s)$每个时间窗口）。因此：（*i*）*PoCmt* 渐近抗女巫攻击；（*ii*）资本、硬件和带宽无法替代人类参与；（*iii*）在 *PoW/PoS* 中有效的身份放大策略在此并不适用。

证明概要。根据引理 5.1，要维持s个身份的参与度，每个时间窗口需要解决 $\Omega(s)$ 个挑战，因此每个时间窗口需要投入 $\Omega(s)$ 人类时间。引理 5.2 表明，次线性容量会使对抗权重落后于诚实权重，从而无法持续施加影响。对W个时间窗口求和，得到总计 $\Omega(sW)$ 人类时间。□

备注：外包与协调。PoCmt 不会阻止对手通过雇用许多人类来外包 HCO 解答，也不会强制实行一人一身份。这些行为为模型所允许，并不与定理 5.3 相矛盾。相反，它们阐明了安全态势：PoCmt 将对手的扩张方式从可由机器并行化的资源（资本/硬件复用）转向明确的劳动力容量。协调可以汇聚人力投入，但无法压缩或将其在多个身份之间倍增；影响力仍与每个时间窗口内的同期人力时间成正比。

5.3 可并行化资源协议中线性女巫攻击成本的不可能性

我们将 PoCmt 与影响力源于可并行化资源的协议进行对比，例如计算能力或权益。

资源可并行化协议。令 R 表示对手拥有的总资源。这类协议满足：

(1) 可加性： 影响力仅取决于总资源 $R_{\text{tot}} = \sum_i R_i$，而非身份数量。**(2) 可分割性：** R 可以忽略不计的成本任意拆分到多个身份中。**(3) 单调性：** 影响力随 R 增加而不减。

这些假设涵盖了 PoW、PoS 及相关设计。

引理 5.4（零边际女巫攻击成本）。 在任何资源可并行化协议中，拥有资源 R 的对手都可以创建 s 个身份，并以 $C(R)$ 的成本获得相同的总影响力，且成本与 s 无关。因此，边际女巫攻击成本渐近趋于零。

证明。根据可分割性，将 R 拆分到 s 个身份上。根据可加性，总影响力保持不变。创建身份的成本远低于获取 R 的成本，因此成本仅取决于 R，而与 s 无关。□

推论5.5（PoW/PoS 中线性女巫攻击成本的不可能性）。任何仅基于可并行化资源的协议都无法强制实现线性女巫攻击成本。具体而言，在 *PoW* 和 *PoS* 中，增加身份的边际成本渐近趋近于零。

这确立了鲜明的成本理论上的区分：PoCmt 不属于可并行化资源协议这一类，并实现了 PoW/PoS 式系统中可证明无法实现的特性。

6 PoCmt 的安全性分析

本节论证，在第3节的模型以及第 3.3 节的人类时间约束下，PoCmt 满足骨干式安全属性。一个关键的细微之处在于双时间尺度结构：人类参与度 H_v 按较粗粒度的 人类时间窗口 时间尺度更新，而共识则以细粒度的纪元推进。因此，我们的论证结合了：（i）由当前承诺权重决定的逐纪元领导者选举概率；以及（ii）诚实方与对抗方总权重在窗口尺度上的 漂移。

假设、范围与稳健性。PoCmt 在标准的部分同步假设（第 4 节）下运行，并要求验证者维持相对稳定的连接性，以保持可用性评分 $U_v(t)$。网络访问持续不佳的验证者，即使出于诚实意图，也可能遭遇可用性衰减。这一局限并非 PoCmt 独有：基于领导者和委员会的协议，在根本上都依赖 GST 后及时的消息交换。重要的是，在 PoCmt 中，可用性是一种软性加权信号，而非正确性条件：暂时不可用会降低未来影响力，但不会使过去的区块失效、触发罚没或造成安全性违规。因此，连接性主要影响相对权重和活性界限，而非协议正确性。

最后，我们的结果依赖于人类挑战预言机这一假设：对于某些限时任务，人类仍然比自动化求解器更具优势（第 3.3 节）。与密码学困难性假设一样，这一差距被视为一种建模原语：PoCmt 要求在有限的运行时限内存在实际的人机差距，而非绝对或永久性的保证。

6.1 加权诚实多数与漂移不变量

设 $CS_v(t)$ 为在纪元 t 进行领导者选举时使用的承诺分数，并定义诚实方权重与对抗方权重的总和：

$$W_H(t) = \sum_{v \in H} CS_v(t), \qquad W_A(t) = \sum_{a \in A} CS_a(t), \qquad W_{\text{tot}}(t) = W_H(t) + W_A(t).$$

定义 *6.1*（加权诚实多数）。如果存在 $\rho < 1/2$，使得对于所有纪元 t，PoCmt 满足加权诚实多数，则：

$$W_A(t) \le \rho \cdot W_{\text{tot}}(t).$$

定义 6.1 是承诺加权领导者选举倾向于诚实参与者的标准条件。该条件在 PoCmt 中保持稳定的核心原因在于成本理论：对抗权重无法扩张而不付出每个时间窗口线性的人类时间成本（定理 5.3），而诚实验证者则会在正常运行期间持续累积参与度、参与和可用性（第 3.4 节）。

引理 6.2（承诺漂移不变量（窗口尺度））。假设 *GST* 之后，诚实验证者 *(i)* 在 *HCO* 挑战发出时予以解决，且 *(ii)* 除瞬时故障外始终在线。如果对手每个时间窗口投入的次线性人类时间容量为 $m = o(s)$（等价地，每个时间窗口解决 $o(s)$ 个身份绑定挑战），那么

跨越窗口边界，诚实方的优势不会降低：对于任意窗口边界时刻 $t < t'$，

$$W_H(t') - W_A(t') \;\geq\; W_H(t) - W_A(t).$$

证明概要。在每个时间窗口内，诚实验证者通过 H_v 更新获得净参与度增量，并在纪元尺度上继续累积 P_v 和 U_v。对手只能通过身份绑定的 HCO 解答来提高参与度。在次线性容量下，引理 5.1 表明，越来越多的对手身份无法获得解答，因此其参与度停滞不前；当它们轮换下线时，其可用性会衰减。任何双重签名还会触发 P_v的乘法式罚没，进一步降低其未来权重。因此，诚实方与对抗方之间的差距在各个时间窗口中不会缩小。□

6.2 安全性

我们介绍以下情形的安全性：(i) 按承诺加权的最长链选择；以及 (ii) 可选的加权 BFT 最终性。对于最长链模式，我们用共同前缀性质来表述这一保证。

设每个纪元中当选领导者为诚实方的概率为

$$p_H(t) = \frac{W_H(t)}{W_{\text{tot}}(t)}.$$

根据定义 6.1，对于所有纪元，$p_H(t) > 1/2$。

定理 6.3（共同前缀（加权最长链））。假设 *GST* 之后为部分同步，且满足加权诚实多数：$W_A(t) < \frac{1}{2}W_{\text{tot}}(t)$ 对所有 t 均成立。那么，对于任意确认深度 k，两个诚实验证者采用的链若在某个深度为 k 的区块上存在分歧，其概率在 k 中可忽略不计。

证明概要。该结论遵循适用于承诺加权领导者选举的标准骨干链直觉：当 $p_H(t) > 1/2$ 时，诚实链的预期增长速度快于任何对抗方分叉。若要在深度为 k 的位置出现分歧，对手就必须在许多决定性纪元中维持一条竞争分叉，这意味着对抗方领导者选举出现了异常长的连续结果。此类事件的概率会随 k 指数级衰减。此外，双重签名行为可被罚没，从而降低对抗方未来的权重，并因此随着时间推移增强漂移效应（引理 6.2）。□

可选的加权 *BFT* 终局性。如果 PoCmt 与 HotStuff 风格的最终性组件配对，且投票按 $CS_v(t)$ 加权，那么在满足通常的法定人数交集条件时，安全性将具有确定性。

定理 6.4（加权 BFT 终局性的安全性）。如果一个区块只有在收集到总承诺权重的 $> 2/3$ 作为投票后才被终局确认，并且对所有 t 都有 $W_A(t) < \frac{1}{3}W_{\text{tot}}(t)$，那么两个冲突的已终局区块不可能同时存在。

证明概要。任意两个权重各自超过总权重 2/3 的法定人数集合，其交集的权重都超过总权重的 1/3。由于对手控制的权重严格小于 1/3，因此至少有一名诚实验证者必须同时为两个冲突区块投票，这与确定性诚实行为矛盾。□

6.3 活性与预期领导者延迟

定理 6.5（活性）。假设系统处于 *GST* 未知的部分同步环境中，且 *GST* 之后至少有一名诚实验证者保持在线。那么链将无限增长，诚实区块最终会得到确认（如果启用了 *BFT* 组件，则会最终确定）。

证明概要。GST 之后，诚实方的消息会在有界延迟内传播。根据漂移不变量（引理 6.2），诚实权重不会在时间窗口中落后于对手，并且在典型执行中，诚实权重相对于对抗权重会有所增加。因此，存在 $p_{\min} > 0$，使得对于所有充分大的 t，$p_H(t) \geq p_{\min}$。由此，在任意连续 k 个纪元内出现诚实领导者的概率为 $1 - (1 - p_{\min})^k$，且该概率以指数速度趋近于 1。每个由诚实领导者发起的提案都会扩展链，并根据分叉选择被诚实验证者采纳，从而保证链无限增长，并最终得到确认/终局性。□

诚实领导者的预期等待时间。如果 $p_H(t) \geq p_{\min}$，那么等待下一位诚实领导者的时间（以纪元计）服从几何分布，其

$$\mathbb{E}[T_{\text{honest}}] = \frac{1}{p_{\min}}.$$

6.4 远程攻击与僵尸验证者鲁棒性

远程攻击和“僵尸”验证者会利用曾经强大、后来却变得不活跃的身份。PoCmt 通过时间相关评分以及可用性衰减和（可选的）协议惩罚来缓解这一问题。

引理 6.6（不活跃意味着有效影响力丧失）。如果验证者连续离线 k 个纪元，那么其可用性会呈指数衰减：

$$U_v(t+k) \leq U_v(t)e^{-\lambda k},$$

因此，其对承诺分数的可用性贡献满足 γU_v（$t+k$）$\leq \gamma U_v$（t）$e^{-\lambda k}$。

讨论（僵尸抵抗性）。引理 6.6 形式化说明，不活跃身份无法保留源自可用性的影响力，因此若不重新上线，就无法无限期地保持竞争力。此外，不活跃的验证者不会累积参与度 P_v，而且如果试图进行双重签名，还可能因罚没而失去参与度。如果某个部署希望加强远程攻击抑制，PoCmt 可以选择对过时参与度 H_v 显式施加老化/衰减（这一参数选择与我们的成本理论上的区分正交），这只会进一步强化上述结论。

6.5 领导者选举公平性

PoCmt 按承诺分数的比例抽选领导者，从而在长期内实现诚实验证者之间的公平性。

引理 6.7（领导者选举公平性）。如果两个诚实验证者的承诺评分轨迹渐近相同，那么各自当选领导者的纪元比例将收敛至与其承诺成正比的概率：

$$\lim_{T\to\infty} \frac{\#\{\textit{epochs where } v \textit{ leads}\}}{T} = \lim_{T\to\infty} \frac{CS_v(T)}{\sum_u CS_u(T)}.$$

证明概要。领导者选举通过独立的可验证随机函数试验实现，成功概率与 $CS_v(t)$ 成正比（第 4.3 节）。标准的集中性结论（大数定律）表明，在较长的时间范围内，实际领导者频率将收敛至这些概率。□

备注（外包与协调人类）。如第 5 节所述，PoCmt 并不排除对手雇用许多人类或协调人类群体。这些行为不会违反安全性或活性；它们只是通过增加可用的人类时间容量来提高 $W_A(t)$。因此，最好将上述安全性陈述理解为相对于权重的：只要加权诚实多数成立（定义 6.1），PoCmt 就能享有与其他基于领导者的协议相同的骨干式保证，同时在对抗权重的扩展方式上存在根本差异。

7 仿真框架与评估

我们通过对 PoCmt 进行轻量而富有表现力的仿真，补充分析结果。仿真的目的不是性能基准测试，而是机制验证：我们通过实证展示：(i) 承诺表现出有利于诚实验证者的漂移优势；(ii) 对手影响力从根本上受人类时间容量 而非资本或身份数量限制；(iii) 承诺加权领导者选举从长远来看是公平的。

具体而言，实验旨在对应三项分析性主张：(i) 漂移不变量（引理 6.2）；(ii) 人类时间所导致的线性女巫成本壁垒（定理 5.3）；以及 (iii) 在承诺比例抽样下的领导者选举公平性（引理 6.7）。

该仿真器有意设计得简约且自包含。所有设计选择都直接对应第3节的形式化模型以及第3.3节的 HumanChallenge 预言机假设，从而能够清晰地解释结果。

7.1 仿真模型与双时间尺度结构

为简单起见，每个仿真纪元对应一个人类时间窗口。这样既保留了人类参与度的速率限制效应，又避免引入额外的嵌套时间循环。所有分析保证均基于时间窗口，因此能够直接反映在仿真纪元中。

仿真遵循 PoCmt 的双时间尺度结构（第3.1节）。时间被离散为共识纪元 $t = 0$，1，2，……，用于驱动领导者选举和区块生产。同时，纪元被划分为由 $d = 0$，1，2，……索引的更粗粒度人类时间窗口。在每个时间窗口内，验证者可以解决少量 HCO 挑战，并在时间窗口边界更新参与度分量 H_v。

每个验证者 v 都维护一个承诺状态

$$S_v(t) = (H_v(t), P_v(t), U_v(t)),$$

反映累积的人类参与、协议参与和可用性。用于领导者选举的承诺分数采用

$$CS_v(t) = \alpha H_v(t) + \beta P_v(t) + \gamma U_v(t),$$

参数	值
诚实验证者 $\lvert H\rvert$	50
女巫身份 s	100
纪元范围 T	3000 个纪元
承诺权重（α，β，γ）	（1。0，0。5，0。1）
人类参与度增益 κ_h	1。0（每个已解决的挑战）
参与度增益 κ_P	0.5（每纪元）
可用性增益 κ_u	0.2（每个在线纪元）
可用性衰减率 λ	0.05（每个离线时期）
罚没系数 δ	0.1
诚实方解题概率	0.98
诚实方在线概率	0.995
对抗方人力时间容量 m	变化（每个时间窗口）

表 2：仿真参数。数值仅用于说明，旨在突出 PoCmt 的定性动态，而非进行性能调优。

固定权重（α，β，γ）。

我们初始化了 $\lvert H\rvert$ 个诚实验证者和 s 个对抗方 Sybil 身份，所有身份的初始承诺均为零。诚实验证者以较高概率解决其 HCO 挑战，以较高概率保持在线，并遵循协议。对抗方身份由一个中心化对手控制，同时受明确的人类时间容量约束。

7.2 对抗约束与人类时间容量

关键的建模选择是：对抗方的投入受人类时间容量 限制，而非受资本或身份数量限制。我们用参数 m表示对手在每个人类时间窗口内最多能解决的 HCO 挑战数量。这体现了 HCO 不可并行化假设：即使对手控制许多身份，提高总体参与度的唯一途径也是增加每个时间窗口内人工求解的数量。

对手可以将这些 m 个已解决的挑战分配给女巫身份（例如，集中在少数身份上，或在许多身份之间轮换），但每个时间窗口内的解决总数不能超过 m。这与第 5.2 节中的线性成本界以及定理 5.3 中的渐近要求直接对应。

7.3 参数

表 2 总结了默认仿真参数。选取这些数值是为了展示定性效果，而非优化吞吐量或延迟。

7.4 指标

我们从仿真轨迹中得出以下指标：

- **承诺权重轨迹：** 诚实方和对抗方的承诺权重总量 $= \sum_{a\in A} CS_a\ t$ $(t) = \sum_{v\in H} CS_v$ (t) 和 (t) ( )。
- **领导者占比：** 当选领导者为对抗方的纪元所占比例。
- **承诺权重占比：** 时间范围结束时的比率 W_H + $W_A\ T$ $(T)/(\ (T)\ (\ ))$。

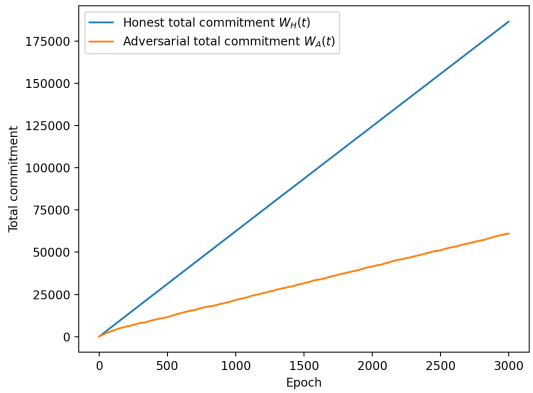


图 1：人类时间稀缺情况下的承诺漂移。随时间变化的诚实方和对抗方承诺权重总量，$W_H(t) = \sum_{v \in H} CS_v(t)$ 以及 $W_A(t) = \sum_{a \in A} CS_a(t)$。由于诚实验证者能够解决挑战，并且以较高概率保持在线，诚实承诺大致呈线性增长；而对手受到固定人类时间容量的限制 m（每个时间窗口内可解决的 HCO 挑战的最大数量）。持续存在的差距 $W_H(t) - W_A(t)$ 从经验上展现了引理 6.2 所预测的漂移行为。

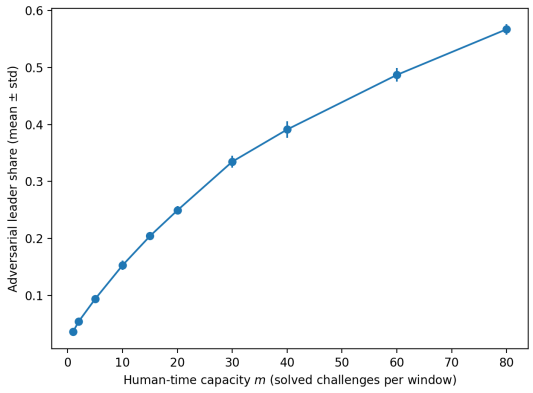


图 2：对抗方领导者份额受人类时间容量控制。对抗方领导者比例的均值（以及不同随机种子间的标准差）随对抗方人力时间容量 m（每个时间窗口内已解决的挑战数）变化。增加 m 会平稳地提高对抗方领导者份额；然而，要取得多数领导权，m 本身必须足够大。这体现了不可并行化资源这一主张：仅靠资本或身份复制，无法使领导者份额超过人类时间所允许的范围（定理 5.3）。

- **公平性：**诚实验证者的实际领导者频率与理想的、与承诺成比例的概率之间的偏差。

这些指标与第 6 节和第 5 节的分析性论断直接对应。

7.5 结果

承诺漂移。 图 1 绘出了诚实承诺和对手承诺总量随时间的变化。诚实承诺稳步增长，且斜率更大；而对手承诺增长较慢，因为参与度只能通过在每个时间窗口内解决数量有限的 HCO 挑战来提升。差距 $W_H(t) - W_A(t)$ 不会递减，这从经验上验证了漂移不变量（引理 6.2）。

人类时间容量扫描。 图 2 和图 3 改变对手的人类时间容量 m，同时保持所有其他参数不变。随着 m 增加，对手影响力平稳增长；然而，要获得多数影响力，m 本身必须足够大。单纯增加女巫身份数量或重新分配投入，并不能绕过这一限制。

容量扫描揭示了不可并行化机制的核心：即使对手控制许多身份，提高总体参与度的唯一方法也是增加每个时间窗口内人工求解的次数。这与第 5.2 节中的界以及定理 5.3 中的渐近要求直接对应。

领导者选举公平性。 图 4 将诚实验证者的实测领导者频率与其理想的、与承诺成比例的概率进行比较。我们通过将实测领导者频率与协议所采用的理想的、与承诺成比例的概率进行比较，在实现层面评估公平性

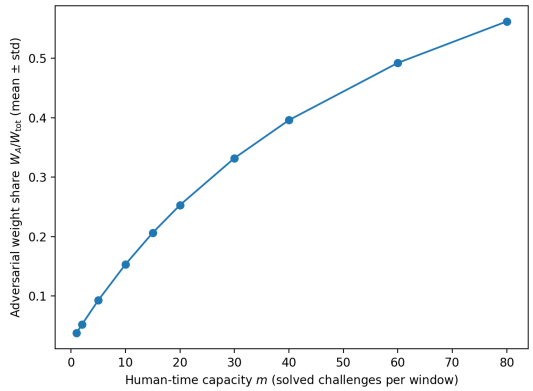


图 3：在承诺比例抽样下，权重份额与领导者占比相符。最终对手承诺份额 $W_A(T)/(W_H(T) + W_A(T))$ 与人类时间容量 m 的关系。权重份额（本图）与领导者占比（图 2）高度一致，证实所实现的领导者抽样符合第 4.3 节中的理想承诺比例规则，并支持引理 6.7 中关于公平性的陈述。

（第 4.3 节）。由此得到的对齐结果为引理 6.7 提供了经验性合理性检验。

可选消融实验：可用性衰减。为检验可用性在抑制休眠身份方面的作用，我们在改变衰减率 λ 的同时，重复基准实验。更大的 λ 会加速

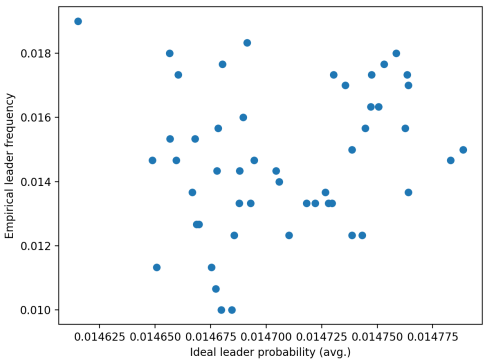


图 4：诚实验证者之间承诺加权领导者选举的公平性。对于每个诚实验证者，x 轴表示其随时间平均的理想领导者概率（与 $CS_v(t)$ 成正比），y 轴则显示其在模拟时段内的实际领导者频率。各点聚集在对角线附近，表明除累积承诺的差异外，领导者选举不会系统性地偏袒诚实节点，这与引理 6.7 一致。

离线身份会损失 $U_v(t)$，从而降低轮换或间歇性在线的女巫身份的可行性。这项实验补充了引理 6.6 中关于远程攻击和僵尸验证者的直觉，表明可用性组件在实践中充当可调节的“新鲜度”过滤器。

7.6 讨论

综合各项实验，模拟结果支持 PoCmt 的理论主张：

- 对抗方影响力随人类时间容量而变化，而非随身份数量或资本变化，这与第 5 节中的成本分离相符。
- 要维持大量具有影响力的女巫身份，每个时间窗口都需要线性的人力投入（定理 5.3）；而次线性投入则会导致局势逐渐向诚实验证者倾斜（引理 6.2）。
- 承诺加权领导者选举在诚实验证者之间表现出经验上的公平性（引理 6.7），这与协议的承诺比例抽样规则一致（第 4.3 节）。
- 可用性衰减为抑制休眠或轮换身份提供了一种实用手段，这与长程稳健性直觉一致（引理 6.6）。

结合分析结果，这些实验为 PoCmt 实现了一种定性上不同、以不可并行化的人力投入为基础的安全态势提供了经验证据。

8 讨论与局限性

PoCmt 为无许可共识引入了一种从根本上以人为中心的权重资源，以实时人力投入取代可由机器并行化的资源。前文各节分别确立了成本理论保证（第 5 节）、骨干式安全属性（第 6 节）以及实证机制验证（第 7 节），但将 PoCmt 应用于实际部署的系统时，还会出现若干实际问题。

8.1 人类努力作为一种安全资源

PoCmt 将人类认知、感知和时间可用性视为稀缺资源。这带来了类 PoW/PoS 系统中不存在的设计约束。

认知负荷与可持续性。 验证者必须定期在限定的响应时间窗口内完成 Human Challenge Oracle（HCO）任务。这些任务必须足够简短，以避免疲劳和流失，同时仍保持显著的人机差距。确定一个稳定的难度—频率区域，以及它与验证者更替之间的相互作用，是部署中的核心问题。

包容性与无障碍性。 挑战类别必须能够适应不同的语言、文化和无障碍需求。与 PoW/PoS 不同，PoCmt 的安全性取决于人类能力和用户体验；因此，可用性也成为首要的安全参数。

8.2 维持人类持续努力的激励机制

为何这很重要。 实际部署必须说明，理性参与者为何会长期持续提供人力投入，尽管他们会面临疲劳、放弃、流失和替换。我们的分析聚焦于将人类时间用作稀缺权重资源所带来的安全后果，因此采用标准的诚实且持续参与 假设：诚实验证者会持续完成 HCO 挑战并长期参与。

完整的激励模型（包括效用、疲劳、进入／退出和劳动力市场效应）与成本理论上的区分及骨干式保证正交，但对于预测现实世界中的参与至关重要。

自然激励机制。 PoCmt 支持多种激励机制，能够在不改变安全核心的情况下维持参与者的投入：(i) 窗口级奖励可直接与近期参与度挂钩（例如挑战解答奖励，和／或根据近期 H_v 设定的乘数奖励）；(ii) 承诺可作为一种类似声誉的信号，影响区块奖励分配和委员会选举，从而让持续参与带来长期收益；(iii) 验证者运营可拆分为基础设施运营者（负责维护在线节点）和人类解答者（定期提供 HCO 响应），从而支持人员流失和替换，同时维持线性成本壁垒。

要将这些激励机制形式化，需要在考虑人类疲劳、外包和流失的情况下进行均衡分析。我们将此视为未来工作的主要方向之一，并指出，只要任何激励机制都能维持每个时间窗口内 HCO 不可并行化的上界，我们的安全结果就仍然成立（第 3.3 节）。

8.3 参数敏感性与调优

PoCmt 引入了参与度提升参数 κ_h、可用性衰减率参数 λ、罚没因子参数 δ 和评分权重（α，β，γ）。参数设定不当可能会降低安全性或参与度：

- 过度衰减可能会惩罚连接性不稳定的诚实验证者，

- 过度的参与度提升可能会造成高方差增长动态，
- 即使出于诚实意图，激进的罚没也可能遏制参与。

可用性敏感度通过 λ 以及人类响应窗口的持续时间进行显式参数化（第3.1节）。更大的时间窗口和更小的衰减率会降低对间歇性连接的惩罚，而更小的时间窗口和更大的衰减率则有利于实施更严格的新鲜度保证。这揭示了部署层面的权衡：一方面是对不稳定连接的容忍度，另一方面是针对休眠或已放弃验证者的响应性（参见第 7 节中的衰减消融实验）。

对安全且稳健的参数区域进行完整刻画，仍是未来工作的重要方向。

8.4 超越女巫攻击泛洪的对抗方

PoCmt 保证线性女巫成本，但仍有若干对抗行为值得关注。

人类劳动力市场与外包。资金充足的对手可以将 HCO 任务外包给受雇人员。这并不违反安全模型：外包仍保留定理 5.3 的线性成本结构。不过，这会使权力来源从技术资源转向劳动力市场。从这个意义上说，PoCmt 能抵御女巫攻击，但不一定能抵御经济集中：对手可以通过持续支付可观测的劳动力成本来扩大影响力。

自动化的进步与长期的人机差距。PoCmt 依赖于这样一种挑战类别：在有限时间窗口内保持人类在实践中的优势（第 3.3 节）。这一假设在理念上类似于标准的困难性假设，但其长期稳定性可能受到自动化进展的影响。因此，要让 PoCmt 在较长时间范围内持续有效，就需要采用自适应的挑战生成机制并保持多样性：部署时应预期定期更新挑战类别和难度参数，并应将挑战层视为可演进的基础设施，而非固定不变的原语。

协调一致的人类群体。 PoCmt 有意不强制实行一人一身份。真实人类组成的协调群体可以在不违反任何规则的情况下积累承诺。这并不会削弱线性的女巫攻击成本保证——每增加一单位影响力，仍需在每个时间窗口内投入额外的同期人力——但它引出了另一个问题：实现了何种社会去中心化？PoCmt 在投入层面而非社会结构层面实现去中心化：它保证影响力反映实时人类参与，而不保证人类彼此不协调。

8.5 部署约束

实际部署会面临后勤和系统层面的约束。

挑战交付与隐私。 挑战必须安全地交付，同时避免预计算、身份关联或验证者元数据泄露。设计必须在透明性（公开可验证性）与隐私（限制不同窗口之间的可关联性）之间取得平衡。

客户端环境。 PoCmt 不要求使用可信硬件，但实际部署可能受益于安全客户端环境（例如加固型移动客户端或可信执行环境），以降低欺骗攻击和重放风险，并支持可靠的挑战交互。

连接性假设。 由于可用性会影响承诺，互联网接入不稳定的地区可能受到不公平惩罚。调整 λ、延长人类响应窗口或引入宽限机制可以缓解这一影响，但可能需要在响应性与休眠身份之间权衡。

8.6 与人格证明的关系

PoCmt 介于匿名无许可系统与全球身份体系方案之间。它不要求身份与真实人类一一对应，但：

- 维持多个积极参与的身份仍然代价高昂，但并非不可能，
- 身份转售或委托无法被完全阻止，
- PoCmt 不保证一人一身份。

因此，PoCmt 避免了全球身份系统带来的治理复杂性，同时仍能实现线性的女巫攻击成本保障。它应被视为一种以人类时间为基础的共识加权原语，而非身份系统。

8.7 理论局限性

即使在理想化假设下，仍存在若干局限性。

对部分同步的依赖。 人类时间尺度上的参与以及及时的 HCO 响应需要较弱的时序假设。在完全异步环境中，实时承诺将变得定义不清。

网络分区。 长时间的网络分区可能导致诚实方验证者在无法联系挑战预言机或其他验证者时累积可用性衰减，从而暂时降低其承诺和影响力。

吞吐量限制。 人工验证本质上限制了参与度累积的速率。因此，如果不进行混合化，PoCmt 不适用于极高吞吐量环境。

8.8 未来方向

PoCmt 开辟了多个研究方向：

- 在疲劳、流失和劳动力市场条件下对激励机制进行均衡建模，
- 自适应且多样化的抗人工智能挑战生成，
- 将人类时间与权益、存储或其他信号相结合的多资源共识，
- 关于串谋和协调行动的人类群体的形式化模型，
- 用于量化参与、可用性和噪声的原型部署。

总体而言，PoCmt 利用人类注意力这一内在稀缺且不可并行化的资源，拓展了无许可共识的设计空间；但要充分发挥其潜力，还需解决上述实践、经济和行为层面的复杂问题。

9 结论

本文提出了承诺证明 承诺证明 (PoCmt)，这是一种新型无许可共识原语，以实时、可由人类验证的参与度为基础，而非依赖可由机器并行化的资源。我们将可分解承诺状态 $S_v(t) = (H_v(t)\ P_v(t)\ U_v(t))$ 其演变受窗口化参与提升、可用性衰减以及针对协议违规的罚没所支配。这种结构确保验证者影响力只能通过持续的人力投入逐步累积，并会在不活跃或行为不端时按可预测的规律衰减。

通过 HumanChallenge 预言机（HCO），我们将人类时间建模为一种明确的不可并行化资源，并确立了它与经典范式之间鲜明的成本理论上的区分。我们证明，任何维持 s 个活跃身份的对手，每个时间窗口都必须投入 $\Theta(s)$单位的人类时间；若不持续支付这一线性成本，对手承诺就不可能超越诚实承诺。相比之下，我们指出，基于可分割、可并行化资源的共识协议——例如工作量证明和权益证明——在其标准假设下无法实现线性女巫成本。

基于这一资源模型，我们提出了完整的 PoCmt 共识协议，其中包括按承诺加权的领导者选举、区块提议与验证、分叉选择，以及可选的 BFT 风格最终性。我们的安全性分析在部分同步条件下确立了类似骨干协议的安全性、活性和比例公平性保证，并表明该协议通过时间依赖的承诺衰减，天然能够抵御远程攻击和“僵尸”攻击。模拟研究补充了分析结果，并通过实证验证了承诺漂移不变量、对手影响力与人类时间容量之间的线性关系，以及按承诺比例进行领导者选择的公平性。

PoCmt 通过将安全性建立在一种内在稀缺且无法摊销的资源——人类注意力——之上，而非计算或资本之上，拓展了无许可共识的设计空间。尽管这一转变围绕激励机制、可用性和挑战设计提出了新的实践问题，但它表明，强大的女巫攻击抵抗能力不必依赖由机器主导的资源。通过围绕人类时间重新构建共识，PoCmt 为去中心化协议开辟了新的路径，使其安全性体现真正且持续的人类参与，而非技术或金融放大效应。

参考文献

[1] Joseph Bonneau、Andrew Miller、Jeremy Clark、Arvind Narayanan、Joshua A. Kroll 和 Edward W. Felten。2015。《SoK：比特币与加密货币的研究视角与挑战》。*IEEE 安全与隐私研讨会 (2015)*。[2] Miguel Castro 和 Barbara Liskov。1999。《实用拜占庭容错》。发表于*OSDI*。[3] John R. Douceur。2002。《女巫攻击》。发表于国际点对点系统研讨会（*IPTPS*）。[4] Cynthia Dwork、Nancy Lynch 和 Larry Stockmeyer。1988。《部分同步条件下的共识》。*《ACM学报》(1988)*。[5] Stefan Dziembowski、Sebastian Faust 和 Vladimir Kolmogorov。2018。《SpaceMint：一种基于空间证明的加密货币》。发表于金融密码学与数据安全（*FC*）。[6] Ittay Eyal 和 Emin Gün Sirer。2014。《多数并不足够：比特币挖矿易受攻击》。发表于金融密码学与数据安全（*FC*）。[7] Juan Garay、Aggelos Kiayias 和 Nikos Leonardos。2015。《比特币骨干协议：分析与应用》。发表于*EUROCRYPT*（*LNCS*）。Springer。[8] Yossi Gilad、Rotem Hemo、Silvio Micali、Georgios Vlachos 和 Nickolai Zeldovich。2017。《Algorand：为加密货币扩展拜占庭协议》。发表于*SOSP*。

[9] Aggelos Kiayias、Alexander Russell、Bernardo David 和 Roman Oliynykov。2017。《Ouroboros：一种可证明安全的权益证明区块链协议》。发表于*CRYPTO*（*LNCS*）。Springer。[10] Silvio Micali。2016。《Algorand：高效且安全的区块链》。发表于*CRYPTO*（*LNCS*）。Springer。[11] Silvio Micali、Michael Rabin 和 Salil Vadhan。1999。《可验证随机函数》。发表于*FOCS*。IEEE。[12] Malte Möser 和 Jeremy Clark。2019。《人格证明：利用社会验证降低女巫攻击的成本》。发表于金融密码学。[13] Satoshi Nakamoto。2008。《比特币：点对点电子现金系统》。https: //bitcoin.org/bitcoin.pdf。[14] Rafael Pass 和 Elaine Shi。2017。《休眠共识问题与白雪协议》。发表于*ASIACRYPT*（*LNCS*）。Springer。[15] Yonatan Sompolinsky 和 Aviv Zohar。2015。《比特币中的安全高速交易处理》。发表于金融密码学与数据安全。Springer。[16] Luis von Ahn、Manuel Blum、Nicholas J. Hopper 和 John Langford。2003。《验证码：利用困难的人工智能问题保障安全》。发表于*EUROCRYPT*（*LNCS*）。Springer。[17] Maofan Yin、Dahlia Malkhi、Michael K. Reiter、Guy Golan Gueta 和 Ittai Abra- ham。2019。《HotStuff：具有线性性和响应性的拜占庭容错共识》。发表于*PODC*。[18] Haifeng Yu、Phillip B. Gibbons、Michael Kaminsky 和 Feng Xiao。2008。《Sybil-Guard：通过社交网络防御女巫攻击》。发表于*SIGCOMM*。