基于DAG的账本中活性攻击的缓解

Darcy Camargo‡、Andreas Penzkofer*、Sebastian M¨uller†、William Sanders*
*IOTA基金会，德国柏林，电子邮箱：research@iota.org
†普罗旺斯大学´，法国国家科学研究中心，I2M，UMR 7373，13453 马赛，法国，电子邮箱：sebastian.muller@univ-amu.fr
‡IOTA基金会，德国柏林，电子邮箱：darcy.camargo@iota.org

arXiv:2305.01207v1 [cs.DC] 2 May 2023

摘要——**账本数据结构的稳健构建是分布式账本安全运行的关键要素。传统的线性区块链系统中，向结构追加内容的权限由领导者掌控；而在基于有向无环图的账本中，写入权限可以采用无领导者方法进行组织。然而，这种无领导者方法依赖诚实的区块发行者公平对待未被引用的区块，即尖端。**

我们研究一部分区块发行者偏离标准尖端选择的影响，目的是完全阻止诚实区块得到确认。我们针对这种所谓的区块孤块现象建立模型，并通过开源仿真研究对其进行验证。研究表明，对手发行率存在一个临界阈值：超过该阈值时，尖端池会变得不稳定；低于该阈值时，孤块现象则会呈指数级减少。我们还研究了协议在尖端过期时间（也称为垃圾回收）以及修改每个区块的父区块引用情况下的稳健性。

I. 引言

分布式账本技术（DLT）必须解决网络中参与者之间的若干核心问题，这些参与者称为节点，彼此之间未必相互信任。节点必须就应将一组提供给它们的交易中的哪些交易添加到共享账本达成一致。由于任意两笔交易都可能请求相互冲突的操作——这种情况称为双重支付——因此必须就最终应应用哪笔交易达成一致，我们将这种状态称为已确认。所有上述问题都必须在拜占庭环境中得到处理，也就是说，网络中存在故障节点或恶意参与者。

为满足这些要求，在线性区块链系统（如比特币）中，交易会被打包进区块，再将区块依次追加成链。通过这条链可以推断交易处理的全序，并通过对交易集合进行全序排列来达成共识。为确保安全性，通过写入访问控制限制每个时间间隔内生成的区块数量。这种限制可以是时间上的概率性限制，例如比特币通过工作量证明实现；也可以通过基于轮次的领导者选举实现，例如权益证明系统。由于分布式账本技术运行于分布式环境中，可能会有多个区块同时创建，并试图扩展链的同一端点，即链的提示。因此，区块链中会产生分叉。随后必须应用其他规则（例如比特币中的最长链规则）来确定规范链。

越来越多的分布式账本技术也开始采用有向无环图（DAG）数据结构，并配套适用的共识规则、写入权限和区块分发。在这样的系统中，节点能够并行发布区块，每个引用多个先前区块的区块。因此，所形成的图推导出了区块之间的偏序。此类协议的示例包括 Aleph [1], 、Sui [2]（结合 Narwhal 和 Tusk [3], ）以及 Iota [4]。

由于协议所处的分布式环境、并行写入权限，以及可能出现的故障或拜占庭参与者，已发出的交易之间可能产生冲突。此时，可以通过追溯式领导者选举来确保对已接受交易达成共识，例如使用公共随机硬币 [1], [3], 或票数求和 [4], [5]。虽然具体的共识机制有所不同，但这些协议有一个共同点：区块DAG的构建对于交易确认和共识模块的性能至关重要。这种构建受三个方面的约束。

首先，与线性区块链系统类似，为了保护网络中的资源，需要一种写入权限机制，用于确定哪些节点可以向有向无环图添加区块。在许可型系统中，可以分轮次授予写入权限 [1], ，也可以通过单独的基于点对点的机制授予 [6]。

其次，每个节点都必须在本地维护一组构成有向无环图尖端的区块，这组区块称为尖端池，即新建区块时，选择算法将从中选取并批准的区块集合。这个尖端池也可以视为分布式内存池，它会形成节点间通信的因果结构化记录。区块之间的引用方案支持高效可靠的广播协议，而这可能是共识协议的必要前提条件，例如 [3]。

第三，分布式账本技术通常需要一种机制，以便节点修剪旧交易。一种方法是不考虑父区块（即被直接引用的区块）在过去“太久远”的区块。在基于DAG的协议中实施这条规则，意味着尖端在达到一定期限后可能会过期。这类区块将不会获得任何批准者，因而成为孤立区块。作为对比， [3], 将这一机制描述为垃圾回收。

A. 结果

在这项工作中，我们分析了协议在旨在（1）通过增加尖端数量实施资源攻击，以及（2）增加过期提示数量的攻击下的韧性。我们的分析表明，这些攻击彼此交织。

在任何基于有向无环图的分布式账本技术环境中，维持健康的尖端池缓冲区是节点正常运行的必要条件。事实上，恶意

行为者若意图破坏协议的共识过程，可以通过不断扩大节点的尖端池，迫使它们从中丢弃区块，进而造成不一致或导致节点崩溃。

此外，由于无法强制执行尖端选择算法，该算法必须处于纳什均衡。如果区块在轻微攻击情境或诚实环境中容易出现孤块现象，节点就会有很强的动机开发新的尖端选择算法，这可能会危及 Tangle 的稳定性。

在本文的第一个结果——定理 1 中，我们引入了一种旨在通过避免选择作为尖端的区块来扩大尖端池的对手。随后我们证明，若诚实区块的发布比例 μ 满足 $\mu \leq 1/k$，其中 k 是每个新区块均匀批准的区块数量，那么尖端池会随时间增长，最终超出缓冲区容量，从而成功发动攻击；同时还证明，当 $\mu > 1/k$ 时，尖端池大小会随时间保持稳定。

在定理 2 中，我们研究了在有无上述攻击者的情况下，健康的尖端池是什么样的，并表明在没有攻击者时，其大小的平均值为 $\mu k\lambda h/(\mu k-1)$，而新区块的产生速率为 λ，网络延迟为 h $\mu = 1$ 。

根据定理 3 中的结果，我们提出在尖端池中引入过期时间 Δ，作为应对这类攻击的对策，以防止缓冲区超出容量，并让网络有机会恢复。我们得到，尖端池大小的平均值为 $L_0\lambda$，其中 L_0 是方程的解

$$L_0 = \frac{\mu k h}{\mu k - 1 + e^{-\Delta \mu k / L_0}}.$$

上述通过过期时间实现的保护带来了一种可能性：区块可能在未经引用的情况下从尖端池中移除，从而变成孤立区块。定理 4 表明，由过期导致区块孤立的概率上限为

$$\exp\{-\Delta(\mu k - 1)/h\},$$

该概率随 Δ 呈指数衰减，因此就区块孤立现象而言并不构成问题。

B. 论文结构

在第二节中，我们讨论一种针对节点尖端池的特定攻击，以及由此产生的区块孤立现象要求。在第三节中，我们介绍区块DAG模型和确认规则，并在第四节中利用它们研究该攻击的影响。在第五节中，我们根据仿真结果验证模型。在第六节中，我们展望未来的研究方向。最后，在第七节中，我们讨论所得结果。

II. 孤块现象与尖端池膨胀

孤块现象 指区块及其内容未被写入最终由所有节点共同认可的账本共享版本中。有几种方式可能导致区块被孤立，我们将在下文讨论。

A. 确认

在区块链中，如果区块获得了足够的支持，通常就会被视为已确认，即属于“公共”账本。例如，在比特币中，属于最长链且获得一定数量区块认可的区块会被视为已确认。类似地，在基于DAG的协议中，例如 [1], [4], [7],区块必须获得足够数量的区块或领导者区块认可。不过，与线性链不同，每个区块都可以引用多个区块。达到给定支持阈值的区块将获得**已确认** 状态，并被添加到永久账本中。

为防止节点硬件因内存占用过多而受到影响，必须限制未确认区块的存储时长。因此，如果区块长时间未能达到确认状态，就需要将其从节点的内存中删除，因为无法保证它最终一定能达到该状态。我们称通过此机制被协议丢弃的区块遭遇了**确认孤儿化**或**活性失效**。

我们注意到，虽然协议应允许确认过程中的孤块现象，以防止存储问题，但遵循协议的节点（即诚实节点）所产生的孤立区块数量应尽可能少，且不应损害确认过程。

B. 过期孤儿化

实现上述限制的具体方式因协议而异。此处我们假设每个区块都带有其生成时的时间戳。此类时间戳可能会受到一定范围的约束，例如在比特币中， [8], 时间戳是通过链的顺序来约束的。为简单起见，我们在模型中假设所有节点的时钟均已同步，因此时间戳会按照生成顺序单调递增。接着，我们设定一个年龄差 Δ，即区块与其任一父区块之间允许的最大时间差。因此，如果某个区块的任一父区块与其时间戳之差大于 Δ，则该区块被视为无效。

因此，某个区块在被纳入尖端池后，可能在一段时间 Δ 内无法获得任何批准者，从而面临**过期孤儿化**。这种孤块现象还可能导致区块的未来锥中断，即所有批准该区块的尖端均发生过期孤儿化。这种所谓的**未来锥孤儿化**将在第六节中进行更详细的讨论。

C. 尖端池膨胀攻击

考虑以下攻击，称为**尖端膨胀攻击**，其试图增大尖端池大小，以提高区块的孤儿概率。在这种攻击中，一名称为**垃圾信息发送者** 的对手发布不确认尖端的区块。此外，对手可能以这样的方式附加，使得不会产生任何

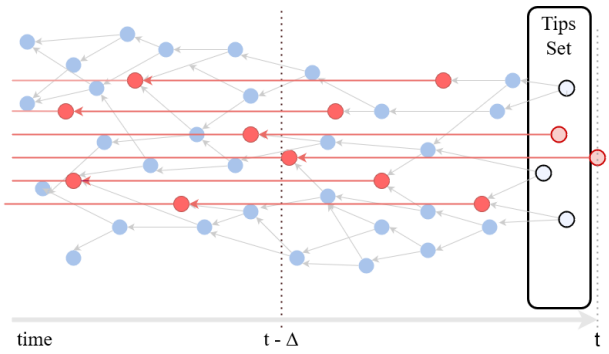


图1. 区块DAG上的尖端膨胀攻击的实际实现。对手附加到旧区块，而不是附加到诚实节点通常会在其尖端池中找到的区块。

对确认的贡献（例如，附加到已确认区块，或仅附加到其自身的区块）。这种攻击旨在尽可能增大尖端池大小。对于不具有过期时间和具有过期时间的协议而言，这种膨胀会带来不同的后果。

首先，在**无过期时间**的变体中，攻击的目标是尖端池的稳定性，即随着时间推移增大尖端集合的大小。一段时间后，不断增大的尖端池会给节点硬件带来资源问题。此外，由于批准流入有限，在尖端池不断增大的情况下，及时确认将成为一项挑战。在第四节中，我们证明，如果垃圾信息发送者拥有足够大的区块份额，就会导致尖端池膨胀。在 [9], 中，曾研究过此类攻击，但未考虑过期时间。研究表明，如果对手获得了显著的发行速率，该攻击就会造成资源问题。

对于**有过期时间**的变体，过期时间限制对尖端选择过程起到了保护作用。由于tip池大小现在受到限制，该攻击最多只能提高由诚实节点发行的区块的确认孤儿率。在第四节中，我们将从理论上展示尖端膨胀攻击和过期孤儿化对平均尖端池大小的影响；在第五节中，我们将通过与模拟结果进行比较来验证所得结果。

有关带过期时间的尖端膨胀攻击的实际实现，请参见图 1。由于过期时间的存在，对手会将区块附加到尖端池之外。此外，为了尽可能增加诚实区块的孤块现象，对手还可以只选择自己的尖端，因此从不批准任何来自诚实节点的区块。

III. 模型

考虑一组用户，也称为节点，每个用户都有一定的权重（例如声誉或质押权益）$\mathcal{N} = \{(N_1, w_1)、(N_2, w_2)\ldots\ldots、(N_n, w_n)\}$。这种权重是一种有限资源，用于衡量节点对维持网络正常运行所作的贡献。声誉系统的例子包括比特币中的工作量证明，以及权益证明网络中的质押代币。

每个节点 N_i 都关联一个速率为$\lambda_i = \lambda w_i / \sum_j w_j$的泊松过程。参数 λ 表示传入区块的总速率，而 λ_i 表示资源 w_i 的比例分配，该分配满足由 [10]规定的公平性标准。

区块DAG的构建基于标记泊松过程。这是一种泊松过程，其中每个点还关联一个称为标记、速率为 λ的数据向量。本文中，我们将使用标记一词同时指代泊松过程中的点（区块）及其关联数据。每个标记 B_i 的结构如下：

$$B_i = (t_i, \mathrm{Ref}_i, \mathrm{Node}_i) \tag{1}$$

并按照其在泊松过程 t_i 中的出现时间排序，因此 $t_i < t_j$ 当且仅当 $i < j$。我们还将 Ref_i视为 k 较旧标记的子集，这些标记将定义我们的有向无环图中的有向边，而 Node_i 是发行者节点。

考虑一个固定的 $B_0 = (-\infty, \emptyset, \emptyset)$，即在过程开始时的一个固定标记，我们称之为 创世块。时间 $t \geq 0$ 时有向无环图的视图由 $\mathcal{T}(t) := \{B_i : t_i \leq t\}$ 给出。

根据定义 $\mathcal{T}(0) = \{B_0\}$。我们还将由 $\mathcal{T}$表示通过在每个标记与 Ref_i 的元素之间定义有向边而构建的相应有向无环图。

A. 尖端与批准

如果 B_i 直接批准 B_j，记为 $B_i \to B_j$，则称 $B_j \in \mathrm{Ref}_i$。如果存在区块序列 $B_{b_1}, B_{b_2}, \ldots, B_{b_M}$，使得对于 $1 \leq m \leq M-1$ 有 $B_1 \to B_{b_1}$, $B_{b_m} \to B_{b_{m+1}}$ 以及 $B_{b_M} \to B_j$，则称 B_i 批准 B_j，并记为 $B_i \rightsquigarrow B_j$。这对应于有向无环图中区块 B_i 与 B_j之间存在一条有向路径。我们将已批准区块的集合 $\mathcal{A}(t) \subsetneq \mathcal{T}(t)$ 定义为

$$\mathcal{A}(t) = \{B_i : B_i \in \mathrm{Ref}_j \text{ for some } B_j \text{ with } t_j \leq t\}.$$

时间 t 的尖端集合 $\mathrm{Tips}(t)$ 定义为 $\mathrm{Tips}(t) = \mathcal{T}(t) \backslash \mathcal{A}(t)$。我们用 $L(t) := |\mathrm{Tips}(t)|$ 表示时间 t 的提示数量。

区块选择每个引用集合 Ref_i （见 (1)）中的 k 元素的方式定义了这一过程。我们考虑这样一种简化模型：每个节点在选择要批准的区块时，只从尖端集合中选择元素，但由于网络的特性，会存在固定延迟 h 。此外，我们假设选择是均匀进行的，即 $\mathrm{Ref}_i = \mathrm{Uniform}_k(\mathrm{Tips}(t_i - h))$，其中 $\mathrm{Uniform}_k$ 表示按照给定参数从均匀分布中选择 k 个独立样本，而h 表示由于网络延迟，每个节点对哪些内容属于提示的认知延迟。

最后，我们指出，为了简洁起见，我们不全面介绍概率原语，例如构建带有其 σ-代数的有向无环图空间、定义表示泊松过程和尖端选择的概率测度，以及定义滤过以使 $\mathcal{T}(t)$ 成为恰当的随机过程。这些内容虽然在技术上很重要，但可以从我们的定义中推导出来，并且与接下来的证明无关。

IV. 理论结果

本节介绍关于尖端膨胀攻击、其对尖端池的影响，以及过期和孤块现象的理论结果。我们首先给出一个重要定义，用数学方式表示该过程的长期稳定性：

定义 1 (渐近平稳性)。如果存在一个随机变量X，使得当 $t \to \infty$ 时，X_t $X_t \to X$ 几乎必然成立，那么我们称过程 X_t 渐近平稳。

A. 平稳性

根据我们定义的有向无环图模型，在任意时刻 t，根据提示状态及有向无环图的局部视图，可将提示分为三类。为此，回顾一下：如果有向无环图处于时刻 t，每个节点都有其在时刻 $t-h$ 对有向无环图的局部视图。据此，提示可分为：

1) **隐藏tip**。在区间（$t-h$；t]内发布的区块，因此由于网络延迟，其他节点仍然不知道这些区块。

2) **真实tip**。这些区块在时刻 $t-h$ 之前发布，且从发布时刻到时刻 t 都未获得任何批准。时刻 t 的真实tip数量记为 $R(t)$。

3) **虚假tip**。最后，这些区块是在时间 $t-h$之前发布的，在时间$t-h$ 之前没有收到任何批准，但在区间（$t-h$; t]内至少收到了一次批准。由于批准它们的区块因网络延迟而对其他节点不可见，因此即使该区块已被引用，节点仍将其视为提示。时间 t 的虚假tip数量记为 $F(t)$。

我们将说明在什么条件下，tip池大小会呈现增加或减少的趋势（正漂移或负漂移）。在负漂移的情况下，我们可以通过超鞅论证得出其收敛到一个适当的随机变量，而这正是我们所寻求的渐近平稳性。

考虑离散时间过程 X_n，它定义为每个区块到达后tip池的大小：$X_n = L(t_n)$。n 中 X_n 的长期行为等价于 $L(t)$中的 t。

定理 1. 对于任意 $x > 0$，几乎必然地成立。

$$\mathbb{E}[X_n - X_{n-1} | X_{n-1} = x] > 1 - \mu k, \tag{2}$$

因此，如果当 $t \to \infty$ 时，尖端的数量无限增长，即趋于无穷大。此外，令 $\mu k > 1$ 并固定 $0 < \varepsilon' < \mu k - 1$。那么存在依赖于 ε' 的 x'，使得如果 $x > x'$，则几乎必然地有 #+#+#+#+

$$\mathbb{E}[X_n - X_{n-1} | X_{n-1} = x] \leq -\varepsilon'. \tag{3}$$

因此，如果 $\mu k > 1$，对于较大的值，*tip*池大小会出现负漂移，并在 $t \to \infty$ 时渐近平稳。

证明。差值 $X_n - X_{n-1}$ 表示区块 B_n 对 tip池大小所作的变化；该区块将将自身添加为一个（隐藏的）尖端，并在此过程中移除一定数量的尖端。移除的数量取决于其选择算法所选择的虚假尖端和真实尖端的数量，以及发行者是诚实的还是垃圾信息发送者（在这些情况下，不会移除任何尖端）。令 $D_n = X_n - X_{n-1}$ 表示这一变化的变量，则显然有

$$\mathbb{E}[D_n | X_{n-1} = x] = 1 - \mu \mathbb{E}[SR_n | X_{x-1} = x], \tag{4}$$

其中，SR_n 是 B_n所选择的真实tip数量。我们首先证明（2）：注意，B_n 的尖端选择中所选的不同区块至多全部是真实tip，因此$SR_n \leq DB_n$，其中 DB_n 是 B_n所选不同区块的数量。现在注意，根据定义 $DB_n \leq k$，并且 $\mathbb{P}[DB_n = k | X_{n-1} = x] < 1$，因为无论时刻 $t-h$的tip池大小如何，B_n 的选择都是独立且均匀的。基于此。

$$\mathbb{E}[SR_n | X_{x-1} = x] \leq \mathbb{E}[DB_n | X_{n-1} = x] < k. \tag{5}$$

将（5）代入（4）可得（2）。

现在来看（3）：进行选择时，B_n 从 L（$t_n - h$）中进行选择，但这些元素分布在 R（t_n）和 F（t_n）之间，这实际上使 SR_n 成为从 R（t_n）中选取的不同元素数量，而选择次数服从具有 k 次选择和事件概率R（t_n）$/L$（$t_n - h$）的条件二项分布。将其应用于（4），得到

$$\mathbb{E}[D_n | X_n = x] \leq 1 - \mu k \mathbb{E}[R(t_n)/L(t_n - h) | X_n = x]. \tag{6}$$

令 $K_{t_n} = |\{i : t_i \in (t_n - h, t_n]\}|$ 表示至多在 h 之前于 t_n发布的区块数量。现在注意到，L（$t_n - h$）$\geq L$（t_n）$- kN_{t_n}$，并且 R（t_n）$\geq L$（$t_n - h$）$- kK_{t_n}$，其中第二个结果源于这样一个事实：在最坏情况下，区间（$t_n - h$, t]）内每个新发布的区块都会从 L（$t_n - h$）中的尖端中移除 k个尖端。利用这一点，（6）变为

$$\mathbb{E}[D_n | X_n = x] \leq 1 - \mu k \mathbb{E}\Big[\frac{L(t_n) - 2kK_{t_n}}{L(t_n) - kK_{t_n}} | X_n = x\Big] \tag{7}$$

$$= 1 - \mu k \mathbb{E}\Big[\frac{x - 2kK_{t_n}}{x - kK_{t_n}} | X_n = x\Big]. \tag{8}$$

现在，由于 K_{t_n} 是一个具有指数尾部的泊松变量，我们可以选择一个常数 C_1，使得 $\mathbb{P}[K_{t_n} < C_1] > (1-\varepsilon)$，从而

$$\mathbb{E}[D_n | X_n = x] \leq 1 - \mu k (1 - \varepsilon) \frac{x - 2kC_1}{x - kC_1}. \tag{9}$$

因此，如果 $\mu > 1/k$，我们可以将 ε 选得足够小（从而将 C_1 选得足够大），使得存在一个足够大的 x'，满足当 $x > x'$时，$\mathbb{E}[D_n | X_n = x] \leq -\varepsilon' < 0$。这保证了负漂移，再结合标准的非周期性考量，结论即得。 □

备注 1. 使用渐近负漂移证明平稳性，受 *[11]*和 *[12],* 的启发，其中研究了局部尖端池大小的平稳性。

B. 提示数量

我们提出以下命题

命题 1. 令 $\mu k > 1$ 并考虑到，根据定理 *1*，$L(t) \to_{t\to\infty} L_\infty$，则 L_∞ 几乎必然地满足 $L_\infty/\lambda \to L_0$，当 $\lambda \to \infty$时，其中 L_0 为常数。

这是定理 1 的推论，也源于将尖端池解释为一个排队过程，其中尖端代表系统中的顾客。关于这种关系的更详细描述及其理论依据可见于[13]。

定理 2. *[无过期机制的提示池大小]* 如果传入区块的速率全部来自诚实节点，即 $\lambda_H = \lambda$，那么提示数量几乎必然地满足（当 $\lambda \to \infty$ 时）

$$L(t) \to \frac{k}{k-1}\lambda h. \tag{10}$$

此外，在速率为 λ_S 的垃圾信息发送者发起攻击、满足 $\lambda = \lambda_H + \lambda_S$ 且 μ 固定的情况下：$= \lambda_H/\lambda$，如果 $\mu k > 1$，则提示数量几乎必然地满足（当 $\lambda \to \infty$ 时）

$$L(t) \to \frac{\mu k}{\mu k - 1}\lambda h. \tag{11}$$

对于 [14], [15], 和 [16]中无垃圾信息发送者的情形，这一结果已为人所知。虽然 [14] 和 [15] 中使用的技术也适用于我们的情形，但我们提出了另一种技术，事实证明它有助于定理 3 的证明。

证明。对于每个区块 B_j，将其作为提示的时间记为 τ_j，也就是直到另一个区块批准它所经过的时间。此证明的主要思路是尝试将排队论中的所谓 Little定律 [17] 应用于提示选择问题，把已存在区块的提示存续时间相加，并将结果与平均尖端数量进行比较。令区块DAG截至时间 t 的总提示存续时间为:

$$\Theta(t) := \sum_{B_i \in \mathcal{T}(t)} \min\{\tau_i, t - t_i\}.$$

求和项中的最小项用于确保提示存续时间不超过当前时间（如果 $t_i + \tau_i > t$）。

由于提示恰好是提示存续时间尚未结束的区块，我们还有

$$\Theta(t) = \int_0^t L(s)ds.$$

现在，对于样本空间中的任意元素 ω，若 $L(t) := L(t,\omega) \to L_\infty(\omega)$，则有

$$\frac{1}{t}\int_0^t |L(s,\omega) - L_\infty(\omega)|ds \to 0 \tag{12}$$

这显然成立，因为 $|L(s,\ \omega) - L_\infty(\omega)| < \varepsilon$ 意味着 (12) 的左侧也小于 ε。由于

定理 1 中，(12) 成立的样本路径集合的测度为 1，因此几乎必然极限

$$\frac{1}{t}\int_0^t L(s)ds \to L_\infty, \text{ as } t \to \infty, \tag{13}$$

成立。最后，利用命题 1，几乎必然地成立:

$$\lim_{\lambda\to\infty}\lim_{t\to\infty}\frac{\Theta(t)}{t\lambda} = L_0. \tag{14}$$

在提示数量渐近平稳的条件下，我们有 τ_i 渐近同分布且具有恒定方差。因此，我们可以应用强大数定律来得到

$$\begin{aligned}\lim_{\lambda\to\infty}\lim_{t\to\infty}\frac{\Theta(t)}{\lambda t} &= \lim_{\lambda\to\infty}\lim_{t\to\infty}\frac{1}{\lambda t}\sum_{B_i\in\mathcal{T}(t)}\min\{\tau_i, t-t_i\}\\ &= \lim_{\lambda\to\infty}\lim_{i\to\infty}\mathbb{E}\tau_i. \end{aligned}\tag{15}$$

由此我们可以得出

$$L_0 = \lim_{\lambda\to\infty}\lim_{i\to\infty}\mathbb{E}\tau_i. \tag{16}$$

至此，Little定律在有向无环图区块发行过程中的类比推导完成。注意，（16）中关于 i 的极限等价于关于 t 的极限。

现在我们继续计算 $\mathbb{E}\tau_i$。B_i 发行后，它会作为一个隐藏尖端停留 h 时间；随后，过程中每个新区块都有一定概率选中它（从而结束它作为提示的时间）

$$p(L(t)) = 1 - (1 - 1/L(t))^k, \tag{17}$$

其中 t 是区块的发行时间。这意味着，在首次批准之后，直至 h 时刻，对 B_i 的批准过程遵循一个非齐次泊松过程 $P_B(t)$，其速率函数为 $\lambda p(L(t))$。这种过程中的首次到达时间的期望（对我们而言即表示量 $\tau_i - h$）是已知的，由（16）可得

$$\begin{aligned} L_0 - h &= \lim_{\lambda\to\infty}\lim_{i\to\infty}\mathbb{E}\tau_i - h\\ &= \lim_{\lambda\to\infty}\lim_{i\to\infty}\mathbb{E}\int_0^\infty x\lambda p(L(t_i+x))e^{-\int_0^x \lambda p(L(t_i+y))dy}dx\\ &= \lim_{\lambda\to\infty}\mathbb{E}\int_0^\infty x\lambda p(L_\infty)e^{-\int_0^x \lambda p(L_\infty)dy}dx \qquad (18)\\ &= \lim_{\lambda\to\infty}\mathbb{E}\int_0^\infty x\lambda p(L_\infty)e^{-x\lambda p(L_\infty)}dx = \mathbb{E}\lim_{\lambda\to\infty}\frac{1}{\lambda p(L_\infty)}\\ &= \mathbb{E}\lim_{\lambda\to\infty}\frac{1}{\lambda\left(1-(1-\frac{1}{L_\infty})^k\right)} = \frac{L_0}{k}, \qquad (19)\end{aligned}$$

由此我们得到 $L_0 = kh/(k-1)$，从而完成诚实场景下的证明。

对于尖端池膨胀场景，考虑节点（或多个节点） N_S 通过发行执行尖端膨胀攻击。

速率 λ_S，而网络的其余部分以速率$\lambda_H = \sum_{i\neq S}^{n} \lambda_i$保持诚实的状态，形成总速率 $\lambda = \lambda_S + \lambda_H$。

请注意，无论尖端来自垃圾信息发送者还是诚实节点，每个尖端的平均存续时间都不会因此改变，因为垃圾信息发送者在选择尖端时会忽略所有尖端，而诚实节点不会区分它们。这意味着，在此场景下，推导出 (16) 的计算仍然成立。与诚实场景不同，为了计算预期尖端存续时间，我们需要考虑到，在区块批准的泊松过程 $P_B(t)$ 中，只有诚实速率 λ_H 有机会批准尖端，因此 $P_B(t)$ 的速率变为 $\lambda_H p(L(t)) = \mu\lambda p(L(t))$。用新的速率重复推导出 (19) 的计算，可得

$$L_0 - h = \mathbb{E}\lim_{\lambda\to\infty} \frac{1}{\mu\lambda p(L_\infty)} = \frac{L_0}{\mu k} \tag{20}$$

解该方程得 $L_0 = h\mu k/(\mu k - 1)$，由此完成证明的第二部分。

□

定理 3. *[过期情况下的尖端池大小]* 考虑与定理 *2* 相同的设置，其中垃圾信息发送者实施尖端膨胀攻击。此外，若尖端在尖端池中停留的时间超过 Δ，则将其移除（即过期）。在这些条件下，对于较大的 t 和较大的 λ，尖端池大小 $L(t)$ </style>渐近表现为 $L_0\lambda$，其中 L_0 是下列方程的解

$$L_0 = \frac{\mu k h}{\mu k - 1 + e^{-\Delta\mu k/L_0}}. \tag{21}$$

证明。在此情形下，我们同样假设存在总速率为 λ_S 的节点实施尖端膨胀攻击，而网络中的其余部分以速率 $\lambda_H = \lambda - \lambda_S$ 保持诚实。此情形的主要区别在于引入了限制 Δ：区块作为提示留存的时间不得超过该限制，超过后便会从池中移除，因而成为孤立区块。

在此情形下，式 (16) 中的渐近关系仍然成立，但每个区块的提示存续时间现在受限于 Δ。若用 E_i 表示速率为 $r(t) = \lambda_H p(L(t_i + t))$ 的泊松过程首次到达时间所对应的随机变量，则有

$$\tau_i \overset{\text{law}}{=} h + \min\{E_i, \Delta\}, \tag{22}$$

利用式 (22) 和渐近关系 (16)，可得

$$\begin{aligned} L_0 - h &= \lim_{\lambda\to\infty}\lim_{i\to\infty} \mathbb{E}\tau_i - h \\ &= \lim_{\lambda\to\infty}\lim_{i\to\infty} \mathbb{E}\int_0^\Delta x r(x) e^{-\int_0^x r(s)ds} dx \\ &\quad + \Delta \lim_{\lambda\to\infty}\lim_{i\to\infty} \mathbb{P}[E_i \geq \Delta]. \end{aligned} \tag{23}$$

由命题 1 可知，对于每个 x，当 $i\to\infty$ 时，$r(x) \to \lambda_H p(L_\infty)$ 几乎必然地成立，因此我们可以对 (23) 使用与 (18) 中相同的计算，得到

$$\begin{aligned} L_0 - h &= \lim_{\lambda\to\infty} \mathbb{E}\int_0^\Delta x\lambda_H p(L_\infty) e^{-x\lambda_H p(L_\infty)} dx \\ &\quad + \Delta \lim_{\lambda\to\infty} \mathbb{E} e^{-\Delta\lambda_H p(L_\infty)} \\ &= \mathbb{E}\lim_{\lambda\to\infty} \frac{1 - (\Delta\lambda_H p(L_\infty) + 1)e^{-\Delta\lambda_H p(L_\infty)}}{\lambda_H p(L_\infty)} \\ &\quad + \Delta\mathbb{E}\lim_{\lambda\to\infty} e^{-\Delta\lambda_H p(L_\infty)}. \end{aligned} \tag{24}$$

由 (20) 可知，当 $\lambda\to\infty$ 时，$\lambda_H p(L_\infty) \to \mu k/L_0$ 几乎必然地成立。将其代入 (24) 得到

$$L_0 - h = \frac{L_0 - (\Delta\mu k + L_0)e^{-\frac{\Delta\mu k}{L_0}}}{\mu k} + \Delta e^{-\frac{\Delta\mu k}{L_0}}. \tag{25}$$

将上式视为关于 $L_0 \to 0$ 和 $L_0 \to \infty$ 的方程，可以确定解一定存在。重新整理式 (25) 中的各项，即完成定理的证明。

□

C. 过期孤块概率

现在我们已经充分了解了 tip池大小，可以计算区块因过期而在尖端池中变为孤立区块的概率。

定理 4。 *[过期概率]* 考虑与定理 *3* 相同的设置。那么，区块在尖端池中停留超过 Δ 个时间单位后被移除（即过期）的概率满足

$$\begin{aligned} \lim_{\lambda\to\infty}\lim_{j\to\infty} \mathbb{P}[\textit{Block } B_j \textit{ expires}] &= \exp\Big\{-\frac{\Delta\mu k}{L_0}\Big\} \\ &\leq \exp\Big\{-\frac{\Delta(\mu k - 1)}{h}\Big\}. \end{aligned} \tag{26}$$

对 j 的限制表示该过程的渐近平稳性。来自 [9] 的模拟表明，对于合理范围内的垃圾邮件发送者比例，该过程通常会迅速收敛到其平稳测度，因此我们得到的渐近结果与现实场景中的预期结果相近。现在开始证明该定理。

证明。回顾一下，固定区块B_j 收到的批准过程是一个条件非齐次泊松过程$P_j(t)$，其速率为 $\lambda_H p(L(t))$，因此区块 B_j 的过期事件 E_j 满足

$$\lim_{j\to\infty} \mathbb{P}[E_j] = \lim_{j\to\infty} \mathbb{P}[P_j(t_j + h, t_j + h + \Delta] = 0]. \tag{27}$$

但是，$P_j(t_j + h,\ t_j + h + \Delta]$ 是参数为 $\int_0^\Delta \lambda_H p(L(t_j+h+s))ds$ 的泊松随机变量，因此根据命题 1，我们有

$$\begin{aligned} \lim_{\lambda\to\infty}\lim_{j\to\infty} \mathbb{P}[E_j] &= \lim_{\lambda\to\infty}\lim_{j\to\infty} \mathbb{E} e^{-\int_0^\Delta \lambda_H p(L(t_j+h+s))ds} \\ &= \mathbb{E}\lim_{\lambda\to\infty} \exp\Big\{-\Delta\lambda_H p(L_\infty)\Big\} \\ &= \exp\Big\{-\Delta\mu h/L_0\Big\}. \end{aligned}$$

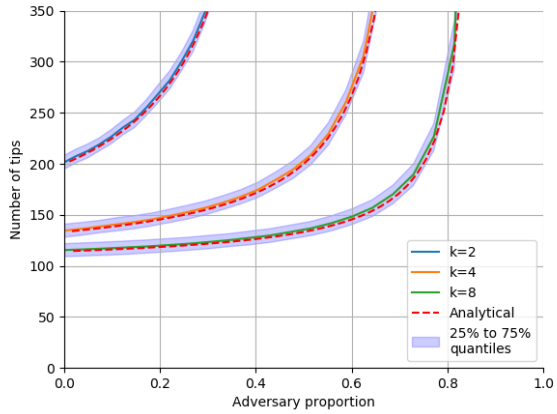


图 2。尖端池大小与对手发布的区块比例之间的关系。将模拟的平均值与若干 k对应的解析值进行比较。通过分位数范围展示尖端池的方差。

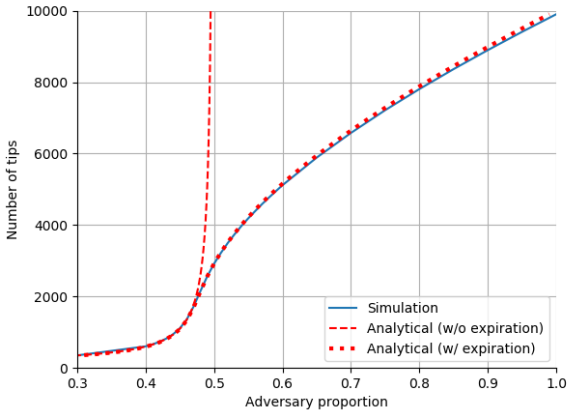


图 3. 对手发布的区块比例不同时的 tip池大小， $\Delta = 100h$。

最后一个关系式由连续性和式（20）得出。

不等式 (26) 是通过将 L_0 替换为定理 3 中的值，并利用以下事实得到的

$$\mu k - 1 \leq \mu k - 1 + \exp\Big\{-\frac{\Delta \mu k}{L_0}\Big\}.$$

□

V. 仿真研究与验证

我们将推导出的模型与使用开源仿真代码 [18] 开展的研究进行比较。在仿真器中，我们采用以下假设，这些假设此前也曾用于例如 [19], [14]。区块通过泊松过程创建，我们维护区块DAG和尖端池的全局视图。为模拟新建区块在网络中的传播，区块会在创建后延迟 h 加入全局尖端池。在全局尖端池中，尖端选择机制会选取父尖端。对于每个创建的区块，我们以 μ 的概率采用诚实尖端选择，否则采用对手尖端选择。对于已加入引用区块的区块，或创建时间超过 Δ 的区块，我们会将其从尖端池中移除。为获得高精度，对于每个数据点，我们运行仿真 $n = 100$ 次，每次运行生成的区块DAG至少包含 300。000 个区块。对于尖端池大小，均值的误差（标准差）小于 1%。对于孤块率，我们在图中标出结果的标准差。我们研究的参数如表 I 所示。

表 I 默认参数

参数	值
λ	100 个区块 / h
Δ	100 h
μ	$\{0, .., 1.\}$
k	$\{1, .., 8\}$

首先，为了说明对手发行率较高时所面临的挑战，我们在图 2 中研究不限制过期时间（即 $\Delta = \infty$）时的尖端池大小。解析值与仿真结果的均值吻合良好。我们还通过给出第 25 和第 75 百分位数，展示尖端池的方差。根据定理 1，当 $\mu k > 1$ 时，尖端池不再处于平稳状态；从 μ 接近这些数值时尖端池大小不断增大，可以看出这一点。我们可以看到，增加父区块引用的数量，能够显著增强协议抵御此类攻击的能力。

我们通过将 Δ 设为有限值来应对发散问题。图 3 展示了在对手发布的区块比例不同时， $\Delta = 100h$的 tip池大小。由于过期机制，tip池大小会收敛，且所得值与模型一致。显然，引入过期机制后，即使区块发布由对手主导，tip池大小也受到 Δ内发布的区块数量的限制。

图4展示了对手发布的区块比例不同时的孤块率。对于仿真结果，图中显示了误差的标准差；由于样本数量很大，所有数据点的标准差都很低。可以看出，解析模型（L_0 含过期机制）与仿真所得值吻合良好。对于 $\mu > 1/k$，孤块现象的概率大幅降低，且所有曲线的指数衰减率均相符。

最后，我们还将从定理2（无过期）中获得的 L_0 值作为定理 4的输入，以支持第五节中关于未来锥孤块现象的后续讨论。

VI. 讨论

在本节中，我们将展望未来锥孤立现象这一主题，它扩展了过期孤立现象的概念。

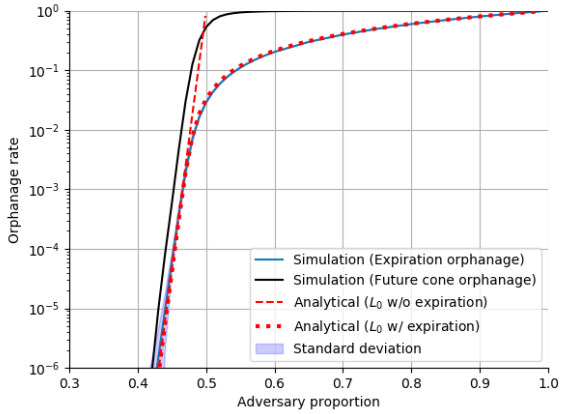


图4. 对于 $\Delta = 100h$、 $k = 2$，随着对手发布的区块比例变化，孤儿概率的变化。

如前所述，某个区块即使已经获得一个或多个批准者，其未来锥中的所有尖端仍可能过期孤立。因此，有向无环图不再以这样的区块为基础继续增长。如果在其未来锥中的尖端孤立之前，该区块未获得足够数量的区块引用，那么它自身就无法达到确认状态。未来锥以这种方式中断的区块被称为遭遇未来锥孤立现象。

未来锥孤儿化也可能导致一致性失败。例如，考虑新节点加入网络的过程。这样的节点可以通过与对等节点的连接获悉新的区块，这些区块即为尖端。随后，该节点可以通过称为固化的过程，递归地请求这些新区块过去锥中缺失的区块。因此，加入网络的节点只能获知那些可从当前通过 gossip 传播的区块集合中到达的尖端。然而，某些区块可能在成为未来锥孤立区块后仍得到确认，从而导致新加入的节点与网络其余部分之间出现一致性失败。

我们通过仿真研究孤儿概率，方法与上一节类似。在图4中，我们仅考虑位于最后一批尖端过去至少 $\tau = 3\Delta$ 的区块。我们从分析中移除较新的区块，因为它们不能很好地代表未来锥孤儿化概率。更具体地说，最近才从尖端池中移除的区块，其未来锥中仍存在尚未过期的尖端的可能性更高。因此，计算得到的未来锥孤儿化值表示一个下界，因为即使在所考虑的区块中，也有一部分最终可能成为未来锥孤立区块。如图所示，如果我们考虑由定理 2 在定理 4 中计算得到的 L_0 值，即“不考虑过期”，则可以获得对未来锥孤儿化更好的估计。

VII. 结论

在基于DAG的分布式账本技术中，区块可以通过引用先前的区块，以异步和并发的方式添加。为了保持由此生成的区块DAG具有良好的性能，尖端池的稳定性至关重要。我们提出了一种试图扩大尖端池、进而导致节点资源耗尽的攻击。为保护节点，我们建议为提示引入过期时间。我们提出了模型，用于分析预测有无过期时间时的尖端池大小。我们证明，如果对手获得了足够的写入权限，在没有过期机制的情况下，该攻击能够破坏尖端池的平稳性（稳定性）。另一方面，引入过期时间后，尖端池大小将保持在有限范围内；如果攻击持续时间有限，这可能使节点得以恢复。此外，我们还给出了关于过期孤儿化率的理论结果，并表明，如果对手发出区块的速率低于某个临界值，该比率就会呈指数级下降。

我们使用仿真工具将分析结果与仿真结果进行了比较。由于过期孤儿化可以扩展为未来锥孤儿化，因此我们也利用该仿真器研究未来锥孤儿化。

引用

[1] A. Gagol、D. Le´sniak、D. Straszak 和 M. ´Swietek，《Aleph：拜占庭节点存在时异步网络中的高效原子广播》，载于第一届 *ACM* 金融科技进展会议论文集，2019年，第214–228页。[2] MystenLabs，《Sui智能合约平台》，2022年。 [在线]。可访问：https://github.com/MystenLabs/sui/blob/main/doc/paper/sui. pdf [3]G. Danezis、L. Kokoris-Kogias、A. Sonnino 和 A. Spiegelman，《Narwhal 与 Tusk：基于DAG的内存池与高效拜占庭容错共识》，载于第十七届欧洲计算机系统会议论文集，系列：EuroSys '22。美国纽约州纽约市：计算机协会，2022年，第34–50页。 [在线]。可访问：https://doi.org/10 1145 3492321 3519594 。/。S. Muller、A. [4] Penzkofer、N. Polyanskii、J. Theis、W. Sanders 和 H. Moog，《Tangle 2.0：最重DAG上的无领导者中本聪共识》，*IEEE Access*，2022年。[5] T. Rocket、M. Yin、K. Sekniqi、R. van Renesse 和 E. G. Sirer，《通过亚稳态实现可扩展的概率型无领导者拜占庭容错共识》，2019年。[6] A. Cullen、P. Ferraro、W. Sanders、L. Vigneri 和 R. Shorten，《对抗性物联网网络中分布式账本的拥塞控制》，*CoRR*，卷 abs/2005.07778，2020年。[7] V. Bagaria、S. Kannan、D. Tse、G. Fanti 和 P. Viswanath，《Prism：解构区块链以逼近物理极限》，载于*2019*年 *ACM SIGSAC* 计算机与通信安全会议论文集，系列：CCS '19。美国纽约州纽约市：计算机协会，2019年，第585–602页。[8] S. Nakamoto，《比特币：点对点电子现金系统》，2008年。[9] P. Ferraro、A. Penzkofer、C. King 和 R. Shorten，《分布式账本的反馈控制：基于有向无环图的分布式账本技术的攻击缓解策略》，2022 [ ] 2204 11691 。在线。可访问：[10] https://arxiv.org/abs/。A. Cullen、P. Ferraro、W. Sanders、L. Vigneri 和 R. Shorten，《物联网中的分布式账本访问控制：一种网络方法》，*IEEE*物联网期刊，第1–1页，2021年。[11] N. Kumar、A. Reiffers-Masson、I. Amigo 和 S. Ruano Rinc´on，《网络延迟对基于有向无环图的分布式账本的影响：数学模型》，*SSRN 4253421* 可获取，2022年。[12] S. M¨uller、I. Amigo、A. Reiffers-Masson 和 S. Ruano-Rinc´on，《局部尖端池大小的稳定性》，2023年。 [在线]。可访问：https://arxiv.org/abs/ 2302 01625 。[13] S. Popov、O. Saa 和 P. Finardi，《Tangle中的均衡》，《计算机与工业工程》，第136卷，第160–172页，2019年。[14] S. Popov，《Tangle》，版本*1.4.3*，2018年。[15] B. Kusmierz、W. Sanders、A. Penzkofer、A. Capossele 和 A. Gal，《均匀随机与随机游走尖端选择下Tangle的性质》，载于*2019*年 *IEEE*区块链国际会议（*Blockchain*）。IEEE，2019年，第228–236页。

[16] A. Cullen、P. Ferraro、C. King 和 R. Shorten，《智能出行的分布式账本技术：可变延迟模型》，载于*2019*年 *IEEE* 第*58*届决策与控制会议（*CDC*），2019年，第8447–8452页。[17] J. D. Little，《排队公式的证明：$L = \lambda W$》，运筹学，第9卷，第3期，第383–387页，1961年。[18] 《模拟器：Res-Sim-Tangle》，2022年，https://github.com/iotaledger/res-sim-tangle。[19] B. Kusmierz、W. Sanders、A. Penzkofer、A. Capossele 和 A. Gal，《均匀随机与随机游走尖端选择下Tangle的性质》，载于*2019*年 *IEEE*区块链国际会议（*Blockchain*），2019年，第228–236页。