arXiv:2301.10944v1 [econ.GN] 26 Jan 2023

# 高吞吐量区块链中的交易打包框架

Yuxuan Lu[1]、Qian Qi[1]和 Xi Chen[2]

[1]北京大学计算研究前沿中心 [2]纽约大学伦纳德·N·斯特恩商学院yx lu@pku.edu.cn,qiqian@pku.edu.cn,xc13@stern.nyu.edu

**摘要**

我们构建了一个去中心化多边市场的协调与分配模型，其理论分析有望优化高吞吐量区块链或 Web 3.0 平台上的去中心化交易打包流程。不同于简化设定下的中心化平台，去中心化平台由区块链技术驱动，能够支持用户之间安全、透明的点对点交易。传统的单链区块链存在众所周知的 *blockchain trilemma*。超越单链方案，去中心化高吞吐量区块链采用并行协议来协调解决区块链不可能三角，从而实现各种任务及所需的分配。然而，不可忽视的网络延迟可能导致部分可观测性，进而使当前高吞吐量区块链协议中的去中心化交易打包流程出现协调失灵和分配不当问题。

为解决这一问题，我们采用博弈论方法，研究去中心化交易打包过程中的策略性协调机制。在一个易于处理的双期模型下，我们在部分可观测性条件下求得了矿工策略性交易打包的贝叶斯纳什均衡。结合用于计算均衡收益的新型算法，我们表明，去中心化平台能够实现高效且稳定的市场结果。该模型还表明，所提出的机制无需对初始区块链交易费用机制进行任何重构，即可内生地提供每单位 gas 基本费用。支撑这些算法的理论结果还意味着均衡收益的计算复杂度存在界限。

# 1 引言

本文旨在建立一个关于异质用户参与的去中心化多边平台中的协调与分配的一般理论，该理论可应用于高吞吐量区块链平台或 Web 3.0 平台设计。为此，本文聚焦于高吞吐量区块链，并提出一种基于博弈论方法的新型策略性交易打包机制。该机制还可应用于去中心化多边市场中的激励设计、共识机制设计和资源分配。

自 Nakamoto [2008], 以来，区块链协议的迅速发展提出了一种全新的商业生态系统范式（例如 Web 3.0 平台），并为计算机科学和平台经济的前景带来了新的启示。最近，高吞吐量区块链系统日益受到欢迎，这一趋势受到所谓的区块链不可能三角[1]的推动，该问题针对传统的基于单链的区块链协议（例如比特币（Nakamoto [2008]）和以太坊 1.0（Buterin 等人 [2014]））。区块链不可能三角的主要构成要素包括

- **去中心化** 构成了 Web 3.0 的基础。与充斥着由中心化平台控制的网络的 Web 2.0 协议不同，Web 3.0 是一种互联网，在其中，去中心化区块链技术让用户能够掌控自己的数据和线上生活。

- **安全性** 对于去中心化系统，尤其是区块链协议而言，也可以理解为解决拜占庭容错问题（以下简称 BFT）。以比特币为例，作为去中心化区块链安全性的代表，比特币网络采用了密码学与一种称为工作量证明（PoW）的网络共识机制相结合的方式，但仍面临可扩展性问题，因为 PoW 机制虽然安全，却相对缓慢，这是由于它保留了单链结构。

- **可扩展性** 是指设计一种区块链，使其能够支持更快的交易速度，或在单位时间内处理更多交易的目标。如果区块链技术要服务于更全面的 Web 3.0 平台，并在未来的 Web 3.0 时代为数十亿用户提供支持，那么可扩展性就十分重要。这正是许多高吞吐量区块链协议仍需改进之处：在提升可扩展性的同时，保持去中心化和安全性。

也就是说，高吞吐量区块链协议的核心理念，旨在解决传统基于单链的协议中普遍存在的区块链不可能三角问题，从而以更具可扩展性和实用性的方式为 Web 3.0 平台奠定基础。具体而言，高吞吐量区块链

[1]传统的单链区块链协议每秒只能处理有限数量的交易。例如，比特币网络每秒大约可以处理七笔交易。假设区块链技术要在全球范围内得到采用，主要用于支持最新的 Web 3.0 平台，那么它就应当能够处理海量数据，并提供更快的交易速度，从而让更多人可以使用该网络，而不会因速度过慢或使用成本过高而受到影响。然而，许多主流去中心化网络的基础设计意味着，提高可扩展性往往会削弱去中心化或安全性。这就是所谓的区块链不可能三角。该术语由以太坊联合创始人 $Vitalik\ Buterin$推广开来。因此，用户必须意识到区块链中三个理想要素：去中心化、安全性和可扩展性。换言之，区块链不可能三角也可以理解为这样一个问题：单链区块链协议很难同时实现这三种属性的最佳水平。提高其中一项通常会导致另一项减弱。

系统的目标是提供性能更高的分布式共识机制，通过取代单链结构来提高链上交易速度，同时希望保留传统基于单链的协议所具备的去中心化和安全特性。此类系统包括 Conflux（参见 Li 等人 [2020]）、Algorand（参见 Gilad 等人 [2017]和 Chen 与 Micali [2019]）、Cardano（参见 Kiayias 等人 [2017]和 Kiayias 与 Russell[2018]）等。这些高吞吐量区块链系统的区块生成过程由网络验证者（下文称为矿工）驱动，节点通过并行通信来最大限度地提高区块生成效率；我们也将此称为并行拜占庭容错共识。[2] 其挑战在于如何在高吞吐量场景下达成共识，确保所有节点在各自的账本中保有相同的记录（即实现协调）。

理想情况下，现有的代表性高吞吐量区块链通过并行 BFT 共识[3]提升链上交易吞吐量。然而，在网络负载较高的情况下，由基于并行 BFT 的高吞吐量共识所驱动的部分可观测性以及由网络延迟导致的用户异质性，会引发严重的协调和资源分配问题。这些问题可能导致区块容量利用率受限，进而大幅降低网络吞吐量。下面我们将介绍部分可观测性的关键机制：

- **不可观测区块** 指高吞吐量区块链中出现的一种部分可观测性，尤其是在区块生成过程处于亚秒级标准的情况下。这是因为区块生成过程由网络中的矿工驱动，而矿工受到网络延迟和区块容量上限的限制。在这种情况下，由于多个区块可能同时生成，每个矿工都无法准确观察内存池中的哪些订单已明确被纳入某个新生成的区块。这一现象也可以分为两个阶段，并在图 1 中作详细说明：

  – 日期0，交易者向内存池提交订单，并支付 Gas 费[4]。
  – 日期 1，矿工生成区块，从内存池中选取一些订单，并将其纳入自己的区块，以最大化利润（Gas 费用）。由于矿工无法直接观察其他矿工生成的区块中包含哪些订单，日期0提交到内存池的一些订单可能会在日期 1 被重复纳入多个区块。

  也就是说，矿工只能观察日期0内存池中的订单，却无法观察哪些订单已被纳入日期 1 的区块。这是部分可观测性的主要来源。换言之，在这种情况下，由于不可观测区块的影响，内存池中的同一订单可能会被重复纳入多个区块。

- **协调失灵** 是不可观测区块效应的核心经济后果。这种协调失灵源于矿工无法观察哪些订单已被

[2]许多区块链系统也采用并行拜占庭容错共识来提高交易速度，例如 Solana（见 Yakovenko [2018]）、Fantom（见 Choi 等人 [2018]）和 Bitgert Chain。[3] [2022] 这其中包括基于有向无环图的拜占庭容错共识；最新研究可参见 Spiegelman 等人的工作。[4] Gas 费是交易者在区块链上支付的区块链交易费。这笔 Gas 费通过智能合约自动支付给矿工，以酬谢他们为区块链提供的服务。若没有 Gas 费用，任何人都不会有动力进行质押、从中获益并帮助保障网络安全。

其他矿工的交易打包具有部分可观测性，因此这些订单已被纳入日期 1 区块。由此，矿工不得不在无法判断哪些订单已被纳入日期 1 区块的情况下，决定将哪些订单纳入日期 1 区块。这可能导致矿工相互竞争，将相同的订单纳入日期 1 区块，从而造成重复交易打包。

- **错配** 是不可观测区块效应的另一项重要经济后果。这一错配问题源于部分可观测性导致的协调失灵。例如，平台中的矿工需要分配资源（如算力），以便在日期 1 生成区块。然而，由于存在部分可观测性，矿工无法观察日期 1 的区块中包含了哪些订单，因此无法精准分配区块容量，以争取利润最高的交易。这可能导致矿工分配过多资源来竞争出价较高的交易，从而大幅降低网络吞吐量。

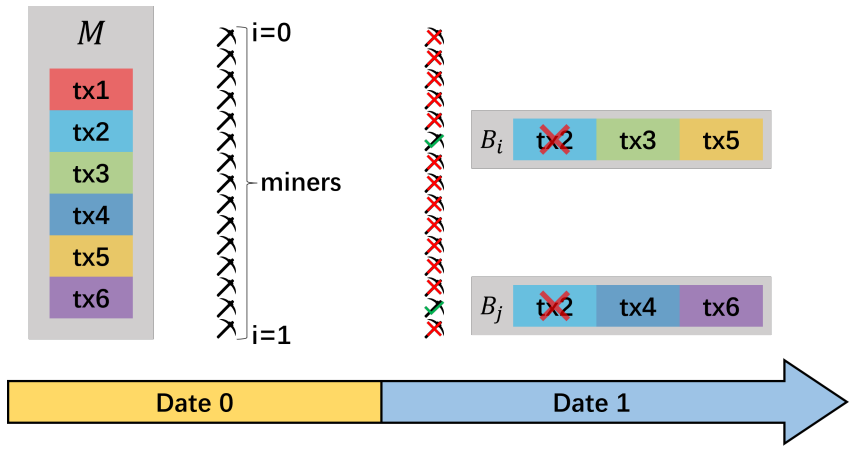


图 1：模型描述

再次强调，本文的主要目的是开发一种基于博弈论方法的新型交易打包机制，以解决高吞吐量区块链平台中的协调与资源分配问题。具体而言，所提出的机制旨在协调平台中的用户（矿工和交易者），并在系统中为用户分配资源，从而提高系统吞吐量。该机制基于博弈论方法，使矿工能够通过策略性地打包交易来最大化利润。

我们强调了“不可观测区块”对高吞吐量区块链中矿工的重要影响，尤其是在区块生成速度低于亚秒级时。在部分可观测性条件下，我们给出了策略性交易打包博弈的纳什均衡，并通过新颖的算法计算该均衡。我们还表明，与现有交易打包策略相比，所提出的机制能够提升系统吞吐量并降低交易延迟。

值得注意的是，我们提出了一种机制，使矿工无需获取任何外部信息即可协调其策略。该机制基于分布式账本，并依靠奖励系统激励矿工以最优方式打包交易。奖励系统旨在为矿工提供经济激励，促使他们高效地打包交易。该奖励系统具有协调性和洞察力，能够为矿工提供必要的策略，帮助他们在部分可观测性条件下决定如何进行交易打包。最后，所提出的机制使矿工能够以去中心化方式协作，并提供了一种扩展系统以处理更多交易的方法。

我们认为，所提出的模型能够通过多种方式惠及去中心化多边市场。首先，我们的模型为资源的高效协调与分配提供了理论框架。通过激励用户形成合作策略，该模型使多边市场能够利用区块链的底层特性，包括隐私、安全性和透明性。此外，我们提出的模型能够提高交易吞吐量，这对去中心化多边市场的可扩展性至关重要。最后，我们的模型可用于优化去中心化交易打包流程，从而实现更高效的资源分配与协调。

总的来说，由于各种区块链协议在服务需求、特性和架构方面各不相同，迄今为止，尤其是针对高吞吐量区块链协议交易打包机制的通用分析框架仍未建立。我们提出的模型为去中心化多边市场的协调与分配提供了一种通用解。我们认为，该模型可用于提升各种多边平台的效率和可扩展性，也可应用于各类基于区块链的应用。

## 1.1 文献综述

本文处于多个研究脉络的交汇处，将多边市场与去中心化平台及高吞吐量区块链结合起来。

本文与平台经济和多边市场领域的文献相关。值得注意的是，已有大量研究探讨多边市场，这些研究始于 Rochet and Tirole [2003], Rochet and Tirole [2006], Cail- laud and Jullien [2003], Armstrong [2006]关于双边市场的开创性著作；这一研究脉络中较近的贡献包括 Weyl [2010], Jullien and Pavan [2019], Tan and Zhou [2021], Teh [2022], 等。现有关于多边平台的文献大多聚焦于中心化垄断平台和双寡头平台。本文则在异质用户模型中，探讨去中心化平台的协调与资源分配问题。

我们的研究与近期关于高吞吐量区块链协议的文献相关。例如，Conflux networks（参见 Li 等人 [2020]）采用树图，其中每个区块都引用若干其他区块，其中之一是其父区块。Algorand（参见 Gilad 等人[2017], Chen 和 Micali [2019]）是另一个以高吞吐量著称的区块链平台。具体而言，该区块链采用权益证明（PoS）机制，随机选取验证者并奖励其工作。Cardano（参见 Kiayias 等人[2017]以及 Kiayias 和 Russell [2018]）是一个注重社区参与和安全性的区块链平台，其中的交易只需几秒即可得到确认。

Solana（参见 Yakovenko [2018]）采用权益证明（PoS）共识机制，凭借低廉的 Gas 费用和高吞吐量交易广受欢迎。Fantom（参见 Choi 等人[2018]）采用有向无环图（DAG）共识机制，实现了高可扩展性。然而，所有这些高吞吐量区块链协议都面临协调和分配问题，因为它们不再考虑策略性交易打包机制。我们对交易打包博弈中的协调与分配进行了理论分析，并据此提出一组均衡策略，以优化现有高吞吐量区块链协议的协调性和效率。

本文还对金融领域中关于去中心化金融、金融科技和区块链的大量不断增长的文献作出了贡献。其中包括 Cong and He [2019], Biais et al. [2019], Easley et al. [2019],Schilling and Uhlig [2019], Chiu and Koeppl [2019], Saleh [2021], Cong et al. [2021b], Cong et al. [2021a], Gryglewicz et al. [2021], Prat and Walter [2021], and Cong et al. [2022],Sockin and Xiong [2022], 等众多研究。我们的分析基于去中心化平台为实现协调和分配而进行的策略性交易打包博弈。理论结果有望为构建高效的 Web 3.0 平台和去中心化交易所（DEX）奠定基础。

本文其余部分安排如下。第 2 节介绍我们的模型和假设。第 3 节刻画两期区块链模型的模型解。第 4 节中，我们描述理论在适用区块链协议上的应用与扩展，并强调所提出的机制无需对区块链交易费用机制进行任何重构，即可内生地提供每单位 gas 基本费用。第 5 节总结全文。略去的证明和算法细节见附录。

# 2 框架

我们现在通过一个易于处理的双期模型，将高吞吐量区块链协议的共识机制形式化。具体而言，我们从传统的工作量证明（PoW）和权益证明（PoS）共识机制的角度刻画高吞吐量区块链。特别是，我们的框架也可以被视为一种多方异步区块链协议。[5] 在标准的基于单链的区块链协议中，区块生成过程的具体时间至关重要，因为区块链协议必须根据时间戳对生成的区块排序，以防止双重支付问题。然而，由于区块以多方异步的方式生成，并在同一时间戳内同时产生，标准方案已不再适用于高吞吐量区块链协议。本节将现有高吞吐量区块链协议的这一特性形式化，并据此分析若干经济后果。

## 2.1 模型

在传统区块链中，矿工可能不会尝试重放前序区块中的交易[6]。然而，在高吞吐量区块链中，由于网络延迟，矿工无法观察到完整的历史记录。相反，他们无法知晓一段时间内生成的区块

[5]需要指出的是，多方异步范式是迄今为止高吞吐量区块链系统广泛采用的关键模式之一，Li 等人 [2020] 提供了一个代表性案例，此外还有许多其他案例。[6]这样做可能导致区块未能通过合法性检查。如果矿工这样做，她将被视为发起攻击。

（即网络延迟）。因此，同一笔交易出现在不同区块中是很自然的。当一笔交易出现在多个区块中时，区块链会在最早的区块中执行该交易，并忽略它在其他区块中的存在。

该平台由两类用户组成：交易者和矿工。不同于中心化平台[7],，在任何交易者提交的未打包交易 tx $\in M$ 成为区块链（或去中心化平台）上的合法交易之前，都应保留在内存池 $M$中，等待某个潜在的去中心化矿工将其打包进区块。下面我们在定义 2.1 中对这些基本概念进行形式化，以消除任何歧义。

**定义 2.1**

- 交易者 广播交易请求，并聘请潜在矿工 $i$ 为其工作，将其订单打包为合法交易 *tx*，纳入特定区块 $B_i$；其中，订单指 $\tau = 0$中的交易。

- 内存池 $M = \{1, 2, ..., m\}$ 是每个矿工维护的订单集合。它充当尚未纳入区块的交易的等候室。请注意，交易被打包进区块后，经过一段网络延迟，应将其从内存池中移除。

- 交易 *tx* 是内存池 $M$ 中的一项，代表交易者提交的一个订单。当订单被广播时，它会通过点对点网络从交易者发送给所有矿工，以便打包成合法交易。

- ***Gas*** 价格 是每单位所占区块容量的出价。我们使用函数 $v(\cdot)$:$M \to \mathbb{R}^+$ 来表示交易的 *Gas* 价格出价。例如，交易 *tx* 的 *Gas* 价格为 $v(tx)$。此外，将函数 $s(\cdot)$: $M \to \mathbb{R}^+$ 定义为交易所占的区块容量后，交易 *tx* 需要向矿工支付的 *Gas* 费为 $s(tx) \times v(tx)$。

- 矿工 $i$ 负责生成区块，并将内存池中的订单打包进自己的区块 $B_i$。具体而言，矿工的主要动力来自 *Gas* 费用，因此，附带较高 *Gas* 价格的订单最有可能优先被打包。区块链平台由连续统个矿工组成，其测度为一，并以$i \in [0, 1]$为索引。

- 区块 $B_i$ 是矿工 $i$要打包的一组交易。每个区块的容量上限为 $k$。形式上， $k$ 是区块中所有交易所占用的最大容量之和，即 $\sum_{交易 \in B_i} s(交易) \leq k$ 对所有 $i \in [0, 1]$。

[7]例如，Web 2.0 平台在 21 世纪初作为计算机行业的一场商业革命应运而生。亚马逊、Meta（Facebook）、Twitter、YouTube 等平台强调访问、互动、移动性和参与的灵活性。然而，Web 2.0 的中心化也使其容易出现安全问题、出于恶意目的的数据收集、隐私侵犯以及成本高昂等问题。此外，中心化的 Web 2.0 平台具有垄断性，加剧了财富不平等和市场操纵。Web 3.0 背后的核心理念就是反对 Web 2.0 平台的这种垄断。随着去中心化网络得到越来越广泛的采用，区块链正作为 Web 3.0 的骨干发挥作用，推动万维网转向一种全新的去中心化使用和服务开发阶段。

为了构建便于理论分析的模型，我们对实际中的区块链协议提出了一些假设。具体而言，我们对网络延迟和交易的区块容量使用量施加了额外约束。

**假设2.1（网络延迟）**网络延迟是区块广播到矿工收到区块之间的时间差。本文简化了网络延迟的影响，并假设所有矿工的网络延迟都相同[8]。我们使用无量纲参数 $\lambda$ 来描述网络延迟。参数 $\lambda$ 定义为网络延迟这一时间区间内预期生成的区块数。此外，我们假设矿工无法获取其网络延迟范围内生成的任何区块的信息。

**假设2.2（交易的区块容量使用量）**在理论分析中，假设所有交易使用固定的区块容量，即每笔交易 $tx$ 均满足 $s(tx) = 1$。由于总区块容量为 $k$，每个区块最多可包含 $k$ 笔交易。在现实世界的区块链中，不同交易有时会使用不同的区块容量，而且这些容量也可能发生变化。如果在模型中考虑这些因素，至少会引入背包问题。在第*4.1*节中，我们将讨论如何将模型解扩展到实际区块链中。

该模型持续两个日期 $\tau \in \{0, 1\}$。在日期0，订单到达，矿工选择订单，并尝试自行将选中的订单打包进即将生成的区块。在日期1，所有区块生成，订单通过区块打包成为合法交易。模型的具体时间线如图 1 所示。

**日期 0：订单到达与订单选择** 在日期0，矿工 $i$维护公共内存池 $M$，其中存放着所有已提交但尚未打包的订单。与此同时，她从内存池中选取一些订单放入自己的（尚未挖出的）区块 $B_i$，并开始挖掘该区块 $B_i$。

**日期 1：区块生成** 在日期1，新生成的集合 $\Gamma$ 由 $\gamma$ 个随机矿工组成。随机矿工的生成规则服从均匀分布，每个矿工 $i \in \Gamma$ 都可以自行挖出一个区块，这些 $\gamma$ 区块可以添加到区块链中。注意，$\gamma$（即挖出区块的矿工数量）服从泊松分布 Poisson(λ)。我们选择泊松分布 Poisson(λ) 的原因是，现实中矿工无法获知其网络延迟期间挖出的区块信息，而其网络延迟期间挖出的区块数量服从泊松分布 Poisson(λ)（见假设2.1）。

## 2.2 策略空间

矿工的策略空间 $\mathcal{S}$ 是当前内存池中所有交易的一个子集，其大小不超过 $k$，表示被选入区块的交易。当$|M| \geq k$时，我们可以忽略包含少于 $k$ 笔交易[9], 的策略，因为它们显然处于劣势。当 $|M| < k$时，最优策略显然是打包

[8]可以放宽这一假设，认为大多数矿工的网络延迟相同。[9]注意，$|X|$ 是集合 $X$的基数。

$M$中的所有交易。因此，基于假设 $|M| \geq k$，我们只需考虑恰好打包 $k$ 笔交易的策略。形式化地，

$$\mathcal{S} = \left\{ D \middle| D \subset M, |D| = k \right\}. \tag{1}$$

对于混合策略，设 $\Delta\mathcal{S}$ 为可能的混合策略集合，即 $\mathcal{S}$上的所有概率分布构成的集合。对于每个混合策略 $\sigma$，我们将 $p^{\sigma}(D)$ 定义为混合策略 $\sigma \in \Delta\mathcal{S}$ 选取交易集合 $B$的概率。此外，我们将$p^{\sigma}$(tx) 也用于表示交易 tx 被选中的边际概率 。形式化地，我们有

$$p^{\sigma}(\text{tx}) = \sum_{D \subset \mathcal{S}} p^{\sigma}(D) \times \mathbf{1}\left[\text{tx} \in D\right], \tag{2}$$

其中， $\mathbf{1}\left[\text{tx} \in D\right]$ 是一个指示函数，用于表示集合 $D$ 是否包含交易 tx；其中$\mathbf{1}\left[\text{tx} \in D\right] = 1$ 表示 tx $\in D$，否则 tx $\notin D$。

## 2.3 效用

实际上，矿工的效用主要可分为三部分：静态区块奖励、Gas 费和矿工可提取价值（MEV）。

- **静态区块奖励** 是指区块链共识给予该区块矿工的奖励。静态区块奖励的数值可能与报告的叔块数量等因素有关，但与区块中包含哪些交易无关。

- **Gas 费** 是指区块中所包含的交易支付给区块创建者的费用。每笔交易 tx 都会指定一个 Gas 价格 $v$(tx)。当交易被打包进区块时，提交该交易的交易者将自动支付$v$(tx) $\times$ $s$(tx)的 Gas 费，其中 $s$(tx)是该交易的区块容量使用量。在高吞吐量区块链中，同一笔交易可能出现在多个区块中。此时，该交易会在最早出现的区块中执行，交易费也将支付给该区块的创建者。

- **矿工可提取价值（MEV）**是指矿工通过抢先交易、审查和重新排序交易等特定操作所能提取的潜在利润（Daian 等， [2020]）。矿工可提取价值可能是矿工的重要收入来源（Qin 等， [2022]）。

**假设 2.3** 我们假设，在基准情形下，矿工只能获得静态区块奖励和 *Gas* 费，以排除矿工可提取价值（*MEV*）的任何影响；在这种情况下，可以将包含 *MEV* 的情形作为基准模型的正式扩展。

**备注 2.1** 请注意，我们可以忽略静态区块奖励，因为它是固定的，且与打包的交易无关。因此，我们将挖出区块 $B_i$ 的矿工 $i$ 的效用定义为其获得的预期 *Gas* 费。

回想一下，在高吞吐量区块链中，同一笔交易出现在多个区块时，该交易会在最早的区块中执行，交易费用将支付给

该区块的创建者。因此，当且仅当网络延迟范围内的所有区块均不包含交易 tx 时，区块 $B_i$ 才能获得交易 tx 的交易费；也就是说，它需要与 Poisson($\lambda$) 个区块竞争。在该模型中，已知矿工 $i$ 挖出一个区块时，其他区块的数量仍服从 Poisson($\lambda$) 分布。因此，自然可以定义：当且仅当交易 tx 未出现在其他区块中时，区块$B_i$ 才能获得该交易的交易费用 $\in B_i$ 。

如果矿工不挖出区块，其效用必定为 0。形式上，在 $i \in \Gamma$（即矿工 $i$ 成功挖出区块）的条件下，效用 $u_i$ 为

$$u_i(\sigma_i, \sigma_{-i}) = \mathrm{E}_{B_i \sim \sigma_i, B_{-i} \sim \sigma_{-i}} \left[ \sum_{\mathsf{tx} \in B_i} v(\mathsf{tx}) \times \Pr\left[\nexists j \in \Gamma \text{ s.t. } \mathsf{tx} \in B_j \cap j \neq i\right] \right], \tag{3}$$

其中， $\sigma_{-i}$ 表示除矿工 $i$以外所有矿工的混合策略。注意，$\Pr\left[\nexists j \in \Gamma \text{ s.t. } \mathsf{tx} \in B_j \cap j \neq i\right]$ 这一项衡量的是交易 tx 仅被打包进唯一一个区块 $B_i$的概率。应用我们在第2.2节中提到的边际概率，可以将效用简化为矿工成功挖出区块的条件下所获得的预期收益：

$$u_i(\sigma_i, \sigma_{-i}) = \sum_{\mathsf{tx} \in M} p^{\sigma_i}(\mathsf{tx}) v(\mathsf{tx}) \times \Pr_{B_{-i} \sim \sigma_{-i}} \left[\nexists j \in \Gamma \text{ s.t. } \mathsf{tx} \in B_j \cap j \neq i\right]. \tag{4}$$

# 3 模型解

本节提出第 2 节模型所生成博弈的一个纳什均衡。所提出的纳什均衡可以嵌入区块链的挖矿协议中。为了将该均衡编码为矿工的挖矿协议，所有矿工必须采用相同的混合策略。否则，矿工必须就其标签达成共识。幸运的是，对于所有矿工，该纳什均衡都具有相同的混合策略 $\sigma^*$ 。

**定义3.1（均衡策略）** $\Delta\mathcal{S}$ 是每个矿工的所有混合策略的集合。设 $\sigma^* \in \Delta\mathcal{S}$ 为一种混合策略。若每个矿工都选择 $\sigma^*$ 作为其策略时形成的策略组合满足纳什均衡，则混合策略 $\sigma^*$ 就是一种均衡策略。形式上，若

$$\forall i \in [0,1] \forall \sigma_i \in \Delta\mathcal{S}, u_i(\sigma_i, \sigma^*_{-i}) \leq u_i(\sigma^*, \sigma^*_{-i}),$$

即效用最大化问题

$$\forall i \in [0,1] \sigma^* \in \arg\max_{\sigma_i \in \Delta\mathcal{S}} u_i(\sigma_i, \sigma^*_{-i}),$$

其中，$\sigma^*_{-i}$ 是除选择混合策略 $\sigma^*$的 $i$ 之外所有矿工的策略组合。

**定理3.1（主定理）**对于内存池 $M$，存在一个均衡策略 $\sigma^*$，即每个采用 $\sigma^*$ 的矿工都达到纳什均衡。此外，均衡策略$\sigma$可在时间复杂度为 $O(|M|\log|M|)$的情况下求得。

在第3.1节和第3.2节中，我们对定理3.1给出了详细证明。在开始正式证明之前，我们先概述证明概要。首先，我们证明，对于满足某些基本要求的任意函数 $p(\cdot)$，算法 1 都能输出一个混合策略 $\sigma$，其对所有 tx $\in M$ 的边际概率均为 $p^{\sigma}$(tx) $= p$(tx)。然后，我们给出一个具体函数 $\hat{p}(\cdot)$，其对应策略是一个均衡策略。在这一步中，函数 $\hat{p}(\cdot)$ 不一定满足基本要求，即可能存在$\exists$tx $\in M$，$\hat{p}$(tx) $\notin [0,1]$。最后，定理3.1对计算得到的函数进行细致调整，使其满足基本要求，同时保持均衡性质。

## 3.1 将边际概率映射为混合策略

**引理 3.1（边际概率的对应策略）**对于任意函数 $p(\cdot): M \to \mathbb{R}$，若满足 *(1)* $\forall tx \in M, 0 \le p(tx) \le 1$；且 *(2)* $\sum_{tx \in M} p(tx) = k$，则存在一个混合策略 $\sigma \in \Delta\mathcal{S}$，其边际概率 $p^{\sigma}(tx) = p(tx)$ 对所有 $tx \in M$均成立。此外，策略 $\sigma$ 可在 $O(|M|)$ 的时间复杂度内求得。在本文余下部分，我们称策略 $\sigma$ 为函数 $p(\cdot)$的对应策略。

---

**算法 1：** 将 $p(\cdot)$ 映射为其对应策略

---

**输入：** 内存池 $M$，边际概率 $p(\cdot)$，区块容量 $k$，参数 $\lambda$。
**结果：** 混合策略 $\sigma$。
$sum[0] \leftarrow 0$； $dv[0] \leftarrow 0$;
**对于**$tx \in 1, 2, ..., |M|$ **执行**
  $sum[\text{tx}] \leftarrow sum[\text{tx} - 1] + p(\text{tx})$;
  $sum[\text{tx}] \leftarrow sum[\text{tx}] - \lfloor sum[\text{tx}] \rfloor$; // $\lfloor x \rfloor$ 是小于或等于该值的最大整数
  大于 $x$
  $dv[\text{tx}] \leftarrow sum[\text{tx}]$;
**end**
将 $dv$ 中的元素按从小到大的顺序排序； $S \leftarrow$**无**;
**对于** $j \in 1、2、...、|M|$ **执行**
  $p \leftarrow dv[j] - dv[j-1]$;
  $A \leftarrow \{\text{tx} \mid sum[\text{tx} - 1] \le dv[j] < sum[\text{tx}]\}$;
  将**“**以概率 $p$ 选择交易集合 $A$ **”**添加到 $\sigma$ 中;
**end**
**返回** $\sigma$;

---

证明： 算法 1 展示了获取混合策略 $\sigma$ 的方法。具体而言，该方法分为三个步骤。第一步，将每笔交易视为长度为 $p$(tx) 的线段，然后依次将所有线段排列在正半轴上。接下来，从 $[0, 1)$ 中均匀随机生成一个实数 $r$。最后，输出所选交易，即覆盖轴上位置 $\{r + n | n = 0, 1, ..., k-1\}$ 的那些线段所对应的交易。

需要证明两个事实，首先，该方法恰好会选出 $k$ 笔交易。这是因为每条线段的长度都不超过 1，因此在 $\{r + n | n = 0, 1, ..., k-1\}$ 中最多只能覆盖一个位置。其次，对于每笔交易 tx，其边际概率 $p^{\sigma}$(tx) $= p$(tx)。我们将

线段 tx 在数轴上的起始位置记为 $L$。当且仅当 $L-\lfloor L\rfloor \le r < L-\lfloor L\rfloor+1$ 或 $L-\lfloor L\rfloor-1 \le r < L-\lfloor L\rfloor$ 时，我们才会选中交易 tx。因此，边际概率 $p^{\sigma}$(tx)，即选择 tx 的 $r$ 范围，为 $p$(tx)。□

**示例 1** 图 *2* 详细展示了算法 *1* 的过程。具体而言，在内存池 $M$ 中有 7 笔交易，区块容量为 $k=3$。在表 *1* 中，第一列是交易 *ID*；第二列是每笔交易的 $p(\cdot)$ 值；第三列显示了每笔交易所创建片段的覆盖区间；第四列是矿工应为每笔交易打包的 $r$ 值。当随机选取的 $r\sim$均匀分布(0, 1) 值为 0.37 时，矿工应选择交易 $\{2,3,5\}$ 进行打包。

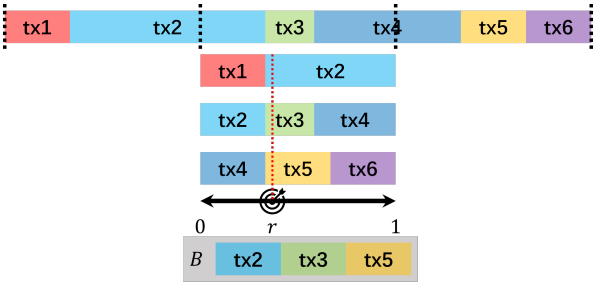


图 2：寻找函数的对应策略

| tx | $p$(tx) 区间 | $r$ 值 |
|---|---|---|
| 1 | $\frac{1}{3}$ | $\left[0,\frac{1}{3}\right)$ |
| 2 | 1 | $\left[\frac{1}{3},\frac{4}{3}\right)$ | $\left[\frac{1}{3},1\right)\cup\left[0,\frac{1}{3}\right)$ |
| 3 | $\frac{1}{4}$ | $\left[\frac{4}{3},\frac{19}{12}\right)$ | $\left[\frac{1}{3},\frac{7}{12}\right)$ |
| 4 | $\frac{3}{4}$ | $\left[\frac{19}{12},\frac{7}{3}\right)$ | $\left[\frac{7}{12},1\right)\cup\left[0,\frac{1}{3}\right)$ |
| 5 | $\frac{1}{3}$ | $\left[\frac{7}{3},\frac{8}{3}\right)$ | $\left[\frac{1}{3},\frac{2}{3}\right)$ |
| 6 | $\frac{1}{3}$ | $\left[\frac{8}{3},3\right)$ | $\left[\frac{2}{3},1\right)$ |
| 7 | 0 | $\emptyset$ | $\emptyset$ |

表 1：示例 1 的数据表

## 3.2 寻找均衡策略

**引理 3.2（均衡策略的充分条件）**混合策略 $\sigma^*$ 是均衡策略，如果

$$\exists w\in\mathbb{R}\forall tx\in M,\begin{cases} p^{\sigma^*}(tx)=0 \implies v(tx)\exp\left(-\lambda p^{\sigma^*}(tx)\right)\le w \\ 0<p^{\sigma^*}(tx)<1 \implies v(tx)\exp\left(-\lambda p^{\sigma^*}(tx)\right)=w \\ p^{\sigma^*}(tx)=1 \implies v(tx)\exp\left(-\lambda p^{\sigma^*}(tx)\right)\ge w \end{cases},$$

其中，$p^{\sigma}(\cdot)$ 已在公式（2）中定义。注意，$w$ 是每笔交易的预期 Gas 费用阈值。证明：回顾一下，$\Delta\mathcal{S}$ 表示某个矿工的所有可能混合策略组成的集合，而 $U(\sigma_i,\ \sigma_{-i})$ 表示当该矿工采用策略 $\sigma_i$、其余矿工采用策略 $\sigma_{-i}$ 时，矿工 $i$ 挖掘一个区块所获得的效用。我们将 $\tilde{v}$(tx) 简写为 $v$(tx)$\times\exp\left(-\lambda p^{\sigma^*}(\text{tx})\right)$，并假设策略 $\sigma^*$ 满足该引理的前提。

随后，我们可以得到，对于所有 $i \in [0,1]$，对于所有 $\sigma \in \Delta\mathcal{S}$，

$$
\begin{aligned}
u_i(\sigma^*, \sigma^*_{-i}) &= \sum_{\mathsf{tx} \in M} p^{\sigma^*}(\mathsf{tx}) v(\mathsf{tx}) \times \Pr_{B_{-i} \sim \sigma^*} [\nexists j \in \Gamma \text{ s.t. } \mathsf{tx} \in B_j \cap j \neq i] && \text{(Equation (4))} \\
&= \sum_{\mathsf{tx} \in M} p^{\sigma^*}(\mathsf{tx}) v(\mathsf{tx}) \times \mathrm{E}_{\gamma \sim \mathrm{Poisson}(\lambda)} \left(1 - p^{\sigma^*}(\mathsf{tx})\right)^{\gamma} \\
&= \sum_{\mathsf{tx} \in M} p^{\sigma^*}(\mathsf{tx}) v(\mathsf{tx}) \times \exp\left(-\lambda p^{\sigma^*}(\mathsf{tx})\right) \\
&= \sum_{\mathsf{tx} \in M} p^{\sigma^*}(\mathsf{tx}) \tilde{v}(\mathsf{tx}) \\
&= \sum_{\mathsf{tx} \in M, 0 \leq p^{\sigma^*}(\mathsf{tx}) < 1} p^{\sigma^*}(\mathsf{tx}) \tilde{v}(\mathsf{tx}) + \sum_{\mathsf{tx} \in M, p^{\sigma^*}(\mathsf{tx}) = 1} \tilde{v}(\mathsf{tx}) \\
&= \sum_{\mathsf{tx} \in M, 0 \leq p^{\sigma^*}(\mathsf{tx}) < 1} p^{\sigma^*}(\mathsf{tx}) w + \sum_{\mathsf{tx} \in M, p^{\sigma^*}(\mathsf{tx}) = 1} \tilde{v}(\mathsf{tx}) \\
&= \sum_{\mathsf{tx} \in M, 0 \leq p^{\sigma^*}(\mathsf{tx}) \leq 1} p^{\sigma^*}(\mathsf{tx}) w + \sum_{\mathsf{tx} \in M, p^{\sigma^*}(\mathsf{tx}) = 1} (\tilde{v}(\mathsf{tx}) - w) \\
&= k v + \sum_{\mathsf{tx} \in M, p^{\sigma^*}(\mathsf{tx}) = 1} (\tilde{v}(\mathsf{tx}) - w) \\
&\geq \sum_{\mathsf{tx} \in M, 0 \leq p^{\sigma^*}(\mathsf{tx}) \leq 1} p^{\sigma}(\mathsf{tx}) w + \sum_{\mathsf{tx} \in M, p^{\sigma^*}(\mathsf{tx}) = 1} p^{\sigma}(\mathsf{tx}) (\tilde{v}(\mathsf{tx}) - w) \\
&= \sum_{\mathsf{tx} \in M, 0 \leq p^{\sigma^*}(\mathsf{tx}) < 1} p^{\sigma}(\mathsf{tx}) w + \sum_{\mathsf{tx} \in M, p^{\sigma^*}(\mathsf{tx}) = 1} p^{\sigma}(\mathsf{tx}) \tilde{v}(\mathsf{tx}) \\
&\geq \sum_{\mathsf{tx} \in M, p^{\sigma^*}(\mathsf{tx}) = 0} p^{\sigma}(\mathsf{tx}) \tilde{v}(\mathsf{tx}) + \sum_{\mathsf{tx} \in M, 0 < p^{\sigma^*}(\mathsf{tx}) < 1} p^{\sigma}(\mathsf{tx}) \tilde{v}(\mathsf{tx}) + \sum_{\mathsf{tx} \in M, p^{\sigma^*}(\mathsf{tx}) = 1} p^{\sigma}(\mathsf{tx}) \tilde{v}(\mathsf{tx}) \\
&= \sum_{\mathsf{tx} \in M} p^{\sigma}(\mathsf{tx}) \tilde{v}(\mathsf{tx}) \\
&= \sum_{\mathsf{tx} \in M} p^{\sigma}(\mathsf{tx}) v(\mathsf{tx}) \times \Pr_{B_{-i} \sim \sigma^*} [\nexists j \in \Gamma \text{ s.t. } \mathsf{tx} \in B_j \cap j \neq i] \\
&= u_i(\sigma, \sigma^*_{-i}).
\end{aligned}
$$

根据纳什均衡的定义，策略 $\sigma^*$ 是均衡策略，当且仅当$\forall i \in [0,1] \forall \sigma \in \Delta\mathcal{S}$，$u_i(\sigma^*, \sigma^*) \geq u_i(\sigma, \sigma^*)$。因此，策略 $\sigma^*$ 是均衡策略。

□

**引理 3.3（弱均衡策略）**对于内存池 $M$，定义函数 $\hat{p}(\cdot)$：$M \to \mathbb{R}$ 如下

$$
\hat{p}(\mathsf{tx}) = \frac{1}{|M|} \left( k + \sum_{\mathsf{tx}' \in M} \frac{\ln v(\mathsf{tx}) - \ln v(\mathsf{tx}')}{\lambda} \right), \tag{5}
$$

其中，$\mathsf{tx}'$ 枚举内存池 $M$ 中的每个订单。如果$\hat{p}(\cdot)$ 满足 $\forall \mathsf{tx} \in M, 0 \leq \hat{p}(\mathsf{tx}) \leq 1$，那么函数$\hat{p}(\cdot)$ 的对应策略就是均衡策略。此外，

$$
\forall \mathsf{tx} \in M, v(\mathsf{tx}) \exp\left(-\lambda \hat{p}(\mathsf{tx})\right) = \exp\left(-\frac{\lambda k}{|M|}\right) \exp\left(\frac{1}{|M|} \sum_{\mathsf{tx}' \in M} \ln v(\mathsf{tx}')\right).
$$

证明：首先，我们需要验证$\hat{p}(\cdot)$是否对应一个混合策略。根据引理 3.1，$\hat{p}(\cdot)$应满足 $\forall \mathsf{tx} \in M$, $0 \leq \hat{p}(\mathsf{tx}) \leq 1$ 以及 $\sum_{\mathsf{tx}\in M} \hat{p}(\mathsf{tx}) = k$。第一个要求已在假设中成立，因此我们只需检查第二个要求。

$$
\begin{aligned}
\sum_{\mathsf{tx}\in M} \hat{p}(\mathsf{tx}) &= \sum_{\mathsf{tx}\in M} \frac{1}{|M|}\left(k + \sum_{\mathsf{tx}'\in M} \frac{\ln v(\mathsf{tx}) - \ln v(\mathsf{tx}')}{\lambda}\right) \\
&= \left(\sum_{\mathsf{tx}\in M} \frac{1}{|M|} k\right) + \frac{1}{|M|}\sum_{\mathsf{tx}\in M}\sum_{\mathsf{tx}'\in M} \frac{\ln v(\mathsf{tx}) - \ln v(\mathsf{tx}')}{\lambda} \\
&= k + \frac{1}{|M|}\sum_{\mathsf{tx}\in M}\left(\frac{|M|\ln v(\mathsf{tx})}{\lambda} \sum_{\mathsf{tx}'\in M} \frac{-\ln v(\mathsf{tx}')}{\lambda}\right) \\
&= k + \frac{1}{|M|}\left(\left(\sum_{\mathsf{tx}\in M} \frac{|M|\ln v(\mathsf{tx})}{\lambda}\right) - \left(|M| \sum_{\mathsf{tx}'\in M} \frac{-\ln v(\mathsf{tx}')}{\lambda}\right)\right) \\
&= k.
\end{aligned}
$$

现在，我们可以简要验证 $\hat{p}(\cdot)$ 是否满足引理 3.2 的要求，从而完成证明。事实上，我们将证明，对于每个 $\mathsf{tx} \in M$，$v(\mathsf{tx}) \exp\left(-\lambda \hat{p}(\mathsf{tx})\right)$ 完全相同：

$$
\begin{aligned}
v(\mathsf{tx}) \exp\left(-\lambda \hat{p}(\mathsf{tx})\right) &= v(\mathsf{tx}) \exp\left(-\frac{\lambda}{|M|}\left(k + \sum_{\mathsf{tx}'\in M} \frac{\ln v(\mathsf{tx}) - \ln v(\mathsf{tx}')}{\lambda}\right)\right) \\
&= v(\mathsf{tx}) \exp\left(-\frac{\lambda k}{|M|}\right) \exp\left(-\frac{\lambda}{|M|} \sum_{\mathsf{tx}'\in M} \frac{\ln v(\mathsf{tx}) - \ln v(\mathsf{tx}')}{\lambda}\right) \\
&= v(\mathsf{tx}) \exp\left(-\frac{\lambda k}{|M|}\right) \exp\left(-\frac{1}{|M|}\left(|M|\ln v(\mathsf{tx}) - \sum_{\mathsf{tx}'\in M} \ln v(\mathsf{tx}')\right)\right) \\
&= v(\mathsf{tx}) \exp\left(-\frac{\lambda k}{|M|}\right) \exp\left(-\ln v(\mathsf{tx}) + \frac{1}{|M|} \sum_{\mathsf{tx}'\in M} \ln v(\mathsf{tx}')\right) \\
&= v(\mathsf{tx}) \exp\left(-\frac{\lambda k}{|M|}\right) \frac{1}{v(\mathsf{tx})} \exp\left(\frac{1}{|M|} \sum_{\mathsf{tx}'\in M} \ln v(\mathsf{tx}')\right) \\
&= \exp\left(-\frac{\lambda k}{|M|}\right) \exp\left(\frac{1}{|M|} \sum_{\mathsf{tx}'\in M} \ln v(\mathsf{tx}')\right).
\end{aligned}
$$

可以观察到，公式右侧是一个与 $M$ 相关但与 $\mathsf{tx}$ 无关的常数。根据引理 3.2，函数 $\hat{p}(\cdot)$ 的对应策略是均衡策略。□

鉴于引理 3.3 表明，函数 $\hat{p}(\cdot)$ 当且仅当 $\forall \mathsf{tx} \in M, \hat{p}(\mathsf{tx}) \in [0,1]$ 时，才能作为均衡策略 $\sigma$ 的边际概率 $p^{\sigma^*}(\cdot)$。也就是说，$\hat{p}(\cdot)$ 在区间 $[0,1]$, 之外可能产生不合理的结果；换言之，对于给定的每个内存池 $M$，我们并不总能得到一个均衡策略。为了解决这个问题，我们通过提出以下定理，拓展引理 3.3 的适用范围。

**定理 3.2（均衡策略）**定义一类函数 $p_x(\cdot)\colon M \to \mathbb{R}$，其下标为 $x \in \mathbb{R}$，如下所示

$$p_x(tx) = \begin{cases} 0 & \hat{p}(tx) \le x \\ \hat{p}(tx) - x & x < \hat{p}(tx) < x+1 \\ 1 & \hat{p}(tx) \ge x+1 \end{cases},$$

其中，函数 $\hat{p}(\cdot)$ 定义于引理 3.3。令 $\hat{x} \in \mathbb{R}$ 为方程 $\sum_{tx \in M} min(max(\hat{p}(tx) - x, 0), 1) = k$ 的最小解。则函数 $p_{\hat{x}}(\cdot)$ 满足：(1)$\forall tx \in M, p_{\hat{x}}(tx) \in [0,1]$；以及 (2) $\sum_{tx \in M} p_{\hat{x}}(tx) = k$。$p_{\hat{x}}(\cdot)$ 的对应策略 $\sigma$ 是均衡策略[11]。

**示例 2** 图 3 详细展示了计算边际概率 $p_{\hat{x}}(\cdot)$ 的过程。具体而言，在内存池 $M$ 中有 7 笔交易，且区块容量为 $k = 3$。表 1 的第一列是交易 ID。第二列是每笔交易的 Gas 价格 $v(\cdot)$。第三列是根据引理 3.3 计算出的 $\hat{p}(\cdot)$ 值，第四列则是求解方程 $\sum_{tx \in M} \min(\max(\hat{p}(tx) - x, 0), 1) = k$ 得到 $\hat{x} = \frac{1}{3}$ 后的边际概率 $p_{\hat{x}}(\cdot)$。

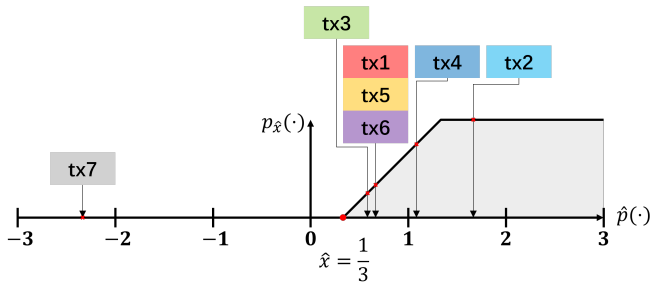


图 3：计算边际概率 $p_{\hat{x}}(\cdot)$

| tx | $v$(tx) | $\hat{p}$(tx) | $p_{\hat{x}}$(tx) |
|---|---|---|---|
| 1 | 1 | $\frac{2}{3}$ | $\frac{1}{3}$ |
| 2 | exp (1) | $\frac{5}{3}$ | 1 |
| 3 | exp $\left(-\frac{1}{12}\right)$ | $\frac{7}{12}$ | $\frac{1}{4}$ |
| 4 | exp $\left(\frac{5}{12}\right)$ | $\frac{13}{12}$ | $\frac{3}{4}$ |
| 5 | 1 | $\frac{2}{3}$ | $\frac{1}{3}$ |
| 6 | 1 | $\frac{2}{3}$ | $\frac{1}{3}$ |
| 7 | exp(−3) | $-\frac{7}{3}$ | 0 |

表 2：示例 2 的数据表

证明：证明分为三个部分。在第一部分中，我们将证明方程 $\sum_{tx \in M} \min(\max(\hat{p}(tx) - x, 0), 1) = k$ 始终有解，并说明计算该解的方法。由于对于所有 $tx \in M$，项 $\min(\max(\hat{p}(tx) - x, 0), 1)$ 关于 $x$ 连续且单调不增，因此项 $\sum_{tx \in M} \min(\max(\hat{p}(tx) - x, 0), 1)$ 关于 $x$ 连续且单调不增。根据以下事实

$$\begin{cases} \lim_{x \to -\infty} \sum_{tx \in M} \min(\max(\hat{p}(tx) - x, 0), 1) = |M| \ge k \\ \lim_{x \to +\infty} \sum_{tx \in M} \min(\max(\hat{p}(tx) - x, 0), 1) = 0 \end{cases},$$

我们可以断言，方程 $\sum_{tx \in M} \min(\max(\hat{p}(tx) - x, 0), 1) = k$ 有一个解。为了计算该解 $\hat{x}$，我们可以使用标准二分搜索算法，得到时间复杂度为 $O(|M| \log |M|)$。二分搜索算法的伪代码见附录 B。

[10]该方程的解可能不唯一，但任意一个解 $\hat{x}$ 都会导出相同的函数 $p_x(\cdot)$。[11]我们可以高效地计算解 $\hat{x}$。详情请参见附录 B。

第二部分要证明函数 $p_{\hat{x}}(\cdot)$ 满足以下条件：(1) $\forall \mathsf{tx} \in M$， $p_{\hat{x}}(\mathsf{tx}) \in [0,1]$；以及 (2) $\sum_{\mathsf{tx}\in M} p_{\hat{x}}(\mathsf{tx}) = k$。这两点都显而易见。由于函数 $p_x(\cdot)$ 定义中的三种情况，其取值都在区间 $[0,1]$, 内，因此满足第一个条件。由于 $\hat{x}$ 是方程 $\sum_{\mathsf{tx}\in M} \min(\max(\hat{p}(\mathsf{tx}) - x, 0), 1) = k$ 的一个解，因此满足第二个条件。由此，函数 $p_{\hat{x}}(\cdot)$ 是混合策略 $\sigma$的边际概率。

最后，我们将证明，函数 $p_{\hat{x}}(\cdot)$的对应策略 $\sigma$ 满足引理 3.2 的条件。根据引理 3.2 和引理 3.3, 我们设

$$w = \exp\left(-\frac{\lambda k}{|M|}\right) \exp\left(\frac{1}{|M|} \sum_{\mathsf{tx}'\in M} \ln v(\mathsf{tx}')\right) \exp(-\lambda \hat{x})$$

并得到，对于所有 $\mathsf{tx} \in M$,

$$\begin{aligned}
& v(\mathsf{tx}) \exp\left(-\lambda\left(\hat{p}(\mathsf{tx}) - x\right)\right) \\
=& v(\mathsf{tx}) \exp\left(-\lambda \hat{p}(\mathsf{tx})\right) \exp(-\lambda x) \\
=& \exp\left(-\frac{\lambda k}{|M|}\right) \exp\left(\frac{1}{|M|} \sum_{\mathsf{tx}'\in M} \ln v(\mathsf{tx}')\right) \exp(-\lambda \hat{x}) && \text{(Lemma 3.3)} \\
=& w.
\end{aligned}$$

因此，我们推导出

$$\begin{cases}
p_{\hat{x}}(\mathsf{tx}) = 0 \implies v(\mathsf{tx}) \exp\left(-\lambda p_{\hat{x}}(\mathsf{tx})\right) < v(\mathsf{tx}) \exp\left(-\lambda\left(\hat{p}(\mathsf{tx}) - \hat{x}\right)\right) = w \\
0 < p_{\hat{x}}(\mathsf{tx}) < 1 \implies v(\mathsf{tx}) \exp\left(-\lambda p_{\hat{x}}(\mathsf{tx})\right) = v(\mathsf{tx}) \exp\left(-\lambda\left(\hat{p}(\mathsf{tx}) - \hat{x}\right)\right) = w \\
p_{\hat{x}}(\mathsf{tx}) = 1 \implies v(\mathsf{tx}) \exp\left(-\lambda p_{\hat{x}}(\mathsf{tx})\right) > v(\mathsf{tx}) \exp\left(-\lambda\left(\hat{p}(\mathsf{tx}) - \hat{x}\right)\right) = w,
\end{cases}$$

从而满足引理 3.2 的条件。因此，函数$p_{\hat{x}}(\cdot)$的对应策略 $\sigma$ 是均衡策略。

□

根据引理 3.1 和定理 3.2，我们可以直接得到主定理。

# 4 讨论

## 4.1 应用与扩展

在第 3 节中，我们讨论了高吞吐量区块链模型中的均衡策略。本节重点介绍引理 3.1 和定理 3.1 的扩展，以获得适用于实际区块链的广义交易打包策略。在我们的模型中，我们假设对于所有转换， $s(\mathsf{tx}) = 1$ 。相比之下，实际中不同交易会使用不同的区块容量。例如，一个区块可能包含数千笔代币转账，但也可能被少数几笔包含智能合约规范中嵌套调用的交易占满。

回顾一下，我们的模型假设每笔交易具有相同的区块容量使用量。没有这一假设，引理 3.1 将不再成立。因此，我们可以采用以下随机化方法，以替代引理 3.1 中的算法 1：

首先，取一个略低于上限 $k$ 的区块容量 $k'$，然后计算交易选择的边际概率 $p(\cdot)$，使得 $\sum_{\mathsf{tx}\in M} s(\mathsf{tx})p(\mathsf{tx}) = k'$。最后，按照概率 $p(\mathsf{tx})$ 独立地继续随机选择每笔交易 tx，直到所选交易集合 $D$ 满足 $k - 2k' \le \sum_{\mathsf{tx}\in D} s(\mathsf{tx}) \le k$。

在解决了将交易选择的边际概率转换为打包策略这一难题后，我们只需将 $s(\mathsf{tx})$ 引入定理 3.2。这里，我们提出定理 3.2 的修订版本，并在附录A中附上算法和证明。

**定理 4.1** 对于内存池 $M$，定义函数 $p_x(\cdot): M \to \mathbb{R}$，其下标为 $x$，如下：

$$p_x^{\text{real}}(\mathsf{tx}) = \begin{cases} 0 & \hat{p}^{\text{real}}(\mathsf{tx}) \le x \\ \hat{p}^{\text{real}}(\mathsf{tx}) - x & x < \hat{p}^{\text{real}}(\mathsf{tx}) < x+1 \\ 1 & \hat{p}^{\text{real}}(\mathsf{tx}) \ge x+1 \end{cases},$$

其中[12]

$$\hat{p}^{\text{real}}(\mathsf{tx}) = \frac{1}{\sum_{\mathsf{tx}'\in M} s(\mathsf{tx}')} \left( k + \sum_{\mathsf{tx}''\in M} s(\mathsf{tx}'') \frac{\ln v(\mathsf{tx}) - \ln v(\mathsf{tx}'')}{\lambda} \right). \tag{6}$$

令 $\hat{}x$ 为方程 $\sum_{\mathsf{tx}\in M} \min(\max(\hat{}p^{\text{real}}(\mathsf{tx}) - x, 0), 1) = k$ 的最小解。则函数 $p_{\hat{x}}(\cdot)$ 满足：*(1)* $\forall \mathsf{tx} \in M, p_{\hat{x}}^{\text{real}}(\mathsf{tx}) \in [0,1]$；以及 *(2)* $\sum_{\mathsf{tx}\in M} p_{\hat{x}}^{\text{real}}(\mathsf{tx}) s(\mathsf{tx}) = k$。如果存在混合策略 $\sigma$，使得 $\forall \mathsf{tx} \in M, p^{\sigma}(\mathsf{tx}) = p(\mathsf{tx})$，那么 $\sigma$ 是均衡策略[13]。

## 4.2 基础费用

2021年8月5日，以太坊启用了名为伦敦硬分叉的一项重大升级，以实施 EIP-1559（以及其他几个 EIP）。实施 EIP-1559 后，区块链共识中增加了一个名为基础费用的参数。基础费用表示订单在每个区块中必须出价的最低 Gas 价格。根据 EIP-1559 提案中的描述，基础费用的存在可以帮助用户更好地估算交易费，从而减少或消除“交易费用水平的波动与交易的社会成本之间的不匹配”。

EIP-1559 对以太坊的交易费用机制进行了实质性改变，以提供基础费用 Leonardos et al. [2021],Liu et al. [2022],Roughgarden [2021]。令人惊讶的是，本文提出的交易打包策略无需对交易费用机制做任何修改，便可产生一个自然的基础费用参数。

设有一个虚拟交易 tx，其区块容量使用量为 $s(\mathsf{tx}) = 0$，并将其加入内存池 $M$。由于 $s(\mathsf{tx}) = 0$，它不会影响其余交易的 $\hat{}x$ 和 $\hat{}p^{\text{real}}(\cdot)$ 值（参见方程（6））。随后，当该虚拟交易 tx 满足方程 $\hat{}p^{\text{real}}(\mathsf{tx}) = \hat{}x$ 时，其 Gas 价格 $v_{\text{low}}$ 就是该交易可能被打包时的最低 Gas 价格。当该虚拟交易 tx 恰好满足方程 $\hat{}p^{\text{real}}(\mathsf{tx}) = \hat{}x + 1$ 时，其 Gas 价格 $v_{\text{high}}$ 就是该交易必须被任一区块打包时的最低 Gas 价格。我们用 sum 作为 $\sum_{\mathsf{tx}'\in M} s(\mathsf{tx}')$ 的简写，即总区块

[12]枚举器 tx″ 和 tx″ 枚举内存池 $M$ 中的每个订单。[13]在实践中，我们使用 $k'$ 代替 $k$，并获得近似均衡。

内存池中所有交易的区块容量使用量。通过求解上述两个方程，我们得到

$$v_{\text{low}} = \exp\left\{\frac{1}{\text{sum}}\left(-k\lambda + \sum_{\mathsf{tx}'\in M} s(\mathsf{tx}')\ln v(\mathsf{tx}')\right)\right\}$$
$$v_{\text{high}} = \exp\left\{\frac{1}{\text{sum}}\left((\text{sum}-k)\lambda + \sum_{\mathsf{tx}'\in M} s(\mathsf{tx}')\ln v(\mathsf{tx}')\right)\right\}.$$

$v_{\text{low}}$ 和 $v_{\text{high}}$ 的含义是

- $v_{\text{低}}$：如果订单的 Gas 价格低于 $v_{\text{low}}$，则无法将其纳入区块；
- $v_{\text{高}}$：如果订单的 Gas 价格出价高于 $v_{\text{高}}$，那么它必定会被纳入每个区块（在网络延迟范围内）。

因此，$v_{\text{low}}$ 可以视为类似以太坊的基础费用。此外，$v_{\text{high}}$ 为急于打包的订单提供了 Gas 价格上限。具体而言，Gas 价格为 $v_{\text{high}}$ 的交易可以迫使每一位潜在矿工将其打包。

# 5 结论

本文提出了一个框架，用于研究高吞吐量区块链中的交易打包博弈的策略行为。我们采用一个易于处理的两期区块链模型来形式化高吞吐量区块链，并揭示其因网络延迟而导致的协调不足和错配。具体而言，我们考察了交易成本、协调和市场均衡对去中心化平台的影响，并发现，与高吞吐量平台现有的交易打包方法相比，我们提出的策略均衡能够带来效率更高、稳定性更强的市场结果。

此外，我们讨论了研究结果对去中心化多边市场发展的启示，并提出了未来研究的可能方向。我们认为，去中心化平台有望彻底改变市场协调与分配的方式。我们相信，本研究是释放去中心化多边平台全部潜力的重要一步。

最后，本文的理论结果也指出了若干潜在的研究方向。首先，本文以静态方式构建了一个基准模型，其中内存池 $M$ 是静态的。直观而言，应考虑一个动态模型，在该模型中，内存池 $M$ 会随时间变化。另一个方向是关注现实中内存池 $M$ 的部分可观测性。本文假设每位矿工都能观察到整个内存池 $M$。然而，现实中由于网络延迟，每位矿工只能观察到内存池的一个子集。因此，研究部分可观测条件下的交易打包最优策略颇有意义。作为高吞吐量区块链交易打包研究的先行者，我们将网络延迟建模为恒定不变。为了准确地刻画高吞吐量区块链中的网络延迟，合理的做法是考虑可能影响订单和区块延迟的各种因素。

# 参考文献

Mark Armstrong。2006。双边市场中的竞争。《兰德经济学杂志》37，3（2006），668–691。Bruno Biais、Christophe Bisiere、Matthieu Bouvard 和 Catherine Casamatta。2019。区块链民间定理。《金融研究评论》32，5（2019），1662–1715。Vitalik Buterin 等。2014。新一代智能合约与去中心化应用平台。白皮书3，37（2014），2–1。Bernard Caillaud 和 Bruno Jullien。2003。鸡与蛋：中介服务提供商之间的竞争。《兰德经济学杂志》（2003），309–328。Jing Chen 和 Silvio Micali。2019。Algorand：安全高效的分布式账本。《理论计算机科学》777（2019），155–183。Jonathan Chiu 和 Thorsten V Koeppl。2019。资产交易的区块链结算。《金融研究评论》32，5（2019），1716–1753。Sang-Min Choi、Jiho Park、Quan Nguyen 和 Andre Cronje。2018。Fantom：一种可扩展的异步分布式系统框架。*arXiv* 预印本 *arXiv:1810.10360*（2018）。Lin William Cong 和 Zhiguo He。2019。区块链颠覆与智能合约。《金融研究评论》32，5（2019），1754–1797。Lin William Cong、Zhiguo He 和 Jiasun Li。2021a。在中心化矿池中进行去中心化挖矿。《金融研究评论》34，3（2021），1191–1235。Lin William Cong、Ye Li 和 Neng Wang。2021b。代币经济学：动态采用与估值。《金融研究评论》34，3（2021），1105–1155。Lin William Cong、Ye Li 和 Neng Wang。2022。基于代币的平台金融。《金融经济学杂志》144，3（2022），972–991。Philip Daian、Steven Goldfeder、Tyler Kell、Yunqi Li、Xueyuan Zhao、Iddo Bentov、Lorenz Breidenbach 和 Ari Juels。2020。闪电男孩2.0：去中心化交易所中的抢先交易、矿工可提取价值与共识不稳定性。载于*2020 IEEE*安全与隐私研讨会（*SP*）。IEEE，910–927。David Easley、Maureen O'Hara 和 Soumya Basu。2019。从挖矿到市场：比特币交易费的演变。《金融经济学杂志》134，1（2019），91–109。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。载于第二十六届操作系统原理研讨会论文集。51–68。Sebastian Gryglewicz、Simon Mayer 和 Erwan Morellec。2021。代币融资的最优策略。《金融经济学杂志》142，3（2021），1038–1067。

Bruno Jullien 和 Alessandro Pavan。2019。平台市场中的信息管理与定价。经济研究评论 86, 4 (2019), 1666–1703。Aggelos Kiayias 和 Alexander Russell。2018。Ouroboros-bft：一种简单的拜占庭容错共识协议。密码学电子印本档案 (2018)。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。载于年度国际密码学会议。施普林格，357–388。Stefanos Leonardos、Barnab´e Monnot、Dani¨el Reijsbergen、Efstratios Skoulakis 和 Geor- gios Piliouras。2021。EIP-1559 以太坊手续费市场的动力学分析。载于第 *3* 届 *ACM* 金融科技进展会议论文集。114–126。Chenxin Li、Peilun Li、Dong Zhou、Zhe Yang、Ming Wu、Guang Yang、Wei Xu、Fan Long 和 Andrew Chi-Chih Yao。2020。一种具有高吞吐量和快速确认能力的去中心化区块链。载于 *2020* {*USENIX*} 年度技术会议（{*USENIX*}{*ATC*}*20*}）。515–528。Yulin Liu、Yuxuan Lu、Kartik Nayak、Fan Zhang、Luyao Zhang 和 Yinhong Zhao。2022。EIP-1559 实证分析：交易费用、等待时间与共识安全性。载于*2022* 年 *ACM SIGSAC* 计算机与通信安全会议论文集 （美国加利福尼亚州洛杉矶）（*CCS '22*）。美国计算机协会，纽约，美国纽约州，2099–2113。https://doi.org/10.1145/3548606.3559341 中本聪。2008。比特币：一种点对点电子现金系统。去中心化商业评论 (2008), 21260。Julien Prat 和 Benjamin Walter。2021。比特币挖矿市场的均衡模型。政治经济学杂志 129, 8 (2021), 2415–2452。Kaihua Qin、Liyi Zhou 和 Arthur Gervais。2022。量化区块链可提取价值：这片森林有多黑？载于*2022* 年 *IEEE* 安全与隐私研讨会（*SP*）。IEEE，198–214。Jean-Charles Rochet 和 Jean Tirole。2003。双边市场中的平台竞争。欧洲经济学会期刊 1, 4 (2003), 990–1029。Jean-Charles Rochet 和 Jean Tirole。2006。双边市场：进展报告。兰德经济学杂志 37, 3 (2006), 645–667。Tim Roughgarden。2021。交易费用机制设计。*ACM SIGecom*交流 19, 1 (2021), 52–55。Fahad Saleh。2021。无浪费的区块链：权益证明。《金融研究评论》 34, 3 (2021), 1156–1190。Linda Schilling 和 Harald Uhlig。2019。比特币经济学简论。货币经济学杂志 106 (2019), 16–26。Michael Sockin 和 Wei Xiong。2022。通过代币化实现去中心化。技术报告。即将刊出。

Alexander Spiegelman、Neil Giridharan、Alberto Sonnino 和 Lefteris Kokoris-Kogias。2022。Bullshark：让 DAG BFT 协议变得实用。载于*2022 年 ACM SIGSAC 计算机与通信安全会议论文集*。2705–2718。Guofu Tan 和 Junjie Zhou。2021。竞争与进入对多边市场的影响。经济研究评论 88, 2 (2021), 1002–1030。Tat-How Teh。2022。平台治理。《美国经济学杂志：微观经济学》14, 3 (2022), 213–54。E Glen Weyl。2010。多边平台的价格理论。《美国经济评论》100, 4 (2010), 1642–72。Anatoly Yakovenko。2018。Solana：面向高性能区块链的新架构 v0. 8.13。白皮书 (2018)。

# 定理 4.1 的证明

**定理 4.1** 对于内存池 $M$，定义函数 $p_x(\cdot)$：$M \to \mathbb{R}$，其下标为 $x$

$$p_x^{\text{real}}(\mathsf{tx}) = \begin{cases} 0 & \hat{p}^{\text{real}}(\mathsf{tx}) \le x \\ \hat{p}^{\text{real}}(\mathsf{tx}) - x & x < \hat{p}^{\text{real}}(\mathsf{tx}) < x+1 \\ 1 & \hat{p}^{\text{real}}(\mathsf{tx}) \ge x+1 \end{cases},$$

其中[14]

$$\hat{p}^{\text{real}}(\mathsf{tx}) = \frac{1}{\sum_{\mathsf{tx}' \in M} s(\mathsf{tx}')} \left( k + \sum_{\mathsf{tx}'' \in M} s(\mathsf{tx}'') \frac{\ln v(\mathsf{tx}) - \ln v(\mathsf{tx}'')}{\lambda} \right). \tag{6}$$

令 $\hat{x}$ 为方程 $\sum_{\mathsf{tx} \in M} \min(\max(\hat{p}^{\text{real}}(\mathsf{tx}) - x, 0), 1) = k$ 的最小解。则函数 $p_{\hat{x}}(\cdot)$ 满足：*(1)* $\forall \mathsf{tx} \in M$，$p_{\hat{x}}^{\text{real}}(\mathsf{tx}) \in [0,1]$；以及 *(2)* $\sum_{\mathsf{tx} \in M} p_{\hat{x}}^{\text{real}}(\mathsf{tx}) s(\mathsf{tx}) = k$。如果存在混合策略 $\sigma$ 使得 $\forall \mathsf{tx} \in M$，$p^{\sigma}(\mathsf{tx}) = p(\mathsf{tx})$，则 $\sigma$ 是均衡策略[15]。

证明：

回顾一下，$k$ 是区块的总容量，$v(\mathsf{tx})$ 是交易 tx 的 Gas 价格，而 $s(\mathsf{tx})$ 是交易 tx 使用的区块容量。可以验证，在该设定下，引理 3.2 的证明仍然有效。我们使用 sum 作为 $\sum_{\mathsf{tx}' \in M} s(\mathsf{tx}')$ 的缩写，表示内存池中所有交易的总区块容量使用量。

与引理 3.3 类似，关于函数 $\hat{p}^{\text{real}}(\cdot)$，我们有以下两个事实：

$$\begin{aligned}
&\sum_{\mathsf{tx} \in M} s(\mathsf{tx}) \hat{p}^{\text{real}}(\mathsf{tx}) \\
=&\sum_{\mathsf{tx} \in M} \frac{s(\mathsf{tx})}{\text{sum}} \left( k + \sum_{\mathsf{tx}' \in M} s(\mathsf{tx}') \frac{\ln v(\mathsf{tx}) - \ln v(\mathsf{tx}')}{\lambda} \right) \\
=&\left( \sum_{\mathsf{tx} \in M} \frac{s(\mathsf{tx}) k}{\text{sum}} \right) + \frac{s(\mathsf{tx})}{\text{sum}} \sum_{\mathsf{tx} \in M} \sum_{\mathsf{tx}' \in M} s(\mathsf{tx}') \frac{\ln v(\mathsf{tx}) - \ln v(\mathsf{tx}')}{\lambda} \\
=&k + \frac{s(\mathsf{tx})}{\text{sum}} \sum_{\mathsf{tx} \in M} \left( \text{sum} \frac{\ln v(\mathsf{tx})}{\lambda} \sum_{\mathsf{tx}' \in M} \frac{-(\ln v(\mathsf{tx}')) s(\mathsf{tx}')}{\lambda} \right) \\
=&k + \frac{s(\mathsf{tx})}{\text{sum}} \left( \left( \sum_{\mathsf{tx} \in M} \frac{\text{sum} \ln v(\mathsf{tx})}{\lambda} \right) - \left( \text{sum} \sum_{\mathsf{tx}' \in M} \frac{-\ln v(\mathsf{tx}')}{\lambda} \right) \right) \\
=&k,
\end{aligned}$$

[14]枚举器 $\mathsf{tx}''$ 和 $\mathsf{tx}''$ 枚举内存池 $M$中的每个订单。[15]在实践中，我们使用 $k'$ 代替 $k$，从而获得近似均衡。

$$
\begin{aligned}
& v(\mathsf{tx}) \exp\left(-\lambda \hat{p}^{\mathrm{real}}(\mathsf{tx})\right) \\
=& v(\mathsf{tx}) \exp\left(-\frac{\lambda}{\mathrm{sum}}\left(k+\sum_{\mathsf{tx}' \in M} s(\mathsf{tx}') \frac{\ln v(\mathsf{tx})-\ln v(\mathsf{tx}')}{\lambda}\right)\right) \\
=& v(\mathsf{tx}) \exp\left(-\frac{\lambda k}{\mathrm{sum}}\right) \exp\left(-\frac{\lambda}{\mathrm{sum}} \sum_{\mathsf{tx}' \in M} s(\mathsf{tx}') \frac{\ln v(\mathsf{tx})-\ln v(\mathsf{tx}')}{\lambda}\right) \\
=& v(\mathsf{tx}) \exp\left(-\frac{\lambda k}{\mathrm{sum}}\right) \exp\left(-\frac{1}{\mathrm{sum}}\left(\mathrm{sum} \ln v(\mathsf{tx})-\sum_{\mathsf{tx}' \in M} s(\mathsf{tx}') \ln v(\mathsf{tx}')\right)\right) \\
=& v(\mathsf{tx}) \exp\left(-\frac{\lambda k}{\mathrm{sum}}\right) \exp\left(-\ln v(\mathsf{tx})+\frac{1}{\mathrm{sum}} \sum_{\mathsf{tx}' \in M} s(\mathsf{tx}') \ln v(\mathsf{tx}')\right) \\
=& v(\mathsf{tx}) \exp\left(-\frac{\lambda k}{\mathrm{sum}}\right) \frac{1}{v(\mathsf{tx})} \exp\left(\frac{1}{\mathrm{sum}} \sum_{\mathsf{tx}' \in M} s(\mathsf{tx}') \ln v(\mathsf{tx}')\right) \\
=& \exp\left(-\frac{\lambda k}{\mathrm{sum}}\right) \exp\left(\frac{1}{\mathrm{sum}} \sum_{\mathsf{tx}' \in M} s(\mathsf{tx}') \ln v(\mathsf{tx}')\right).
\end{aligned}
$$

接着，与定理 3.2 类似，证明的其余部分分为三个部分：
1. 证明方程 $\sum_{\mathsf{tx} \in M} \min(\max(\hat{} p^{\mathrm{real}}(\mathsf{tx})-x,\ 0),\ 1)=k$ 始终有解；2. 证明 $p_{\hat{x}}^{\mathrm{real}}(\cdot)$ 满足：(1) $\forall \mathsf{tx} \in M,\ p_{\hat{x}}^{\mathrm{real}}(\mathsf{tx}) \in [0,1]$；以及 (2) $\sum_{\mathsf{tx} \in M} p_{\hat{x}}^{\mathrm{real}}(\mathsf{tx}) s(\mathsf{tx})$ $=$ $k$；3. 证明函数 $p_{\hat{x}}^{\mathrm{real}}(\cdot)$ 的对应策略 $\sigma$ 满足引理 3.2 的条件。

第 (1) 和 (2) 部分与定理 3.2 的证明完全相同，因此略去。在第 (3) 部分，我们设

$$
w=\exp\left(-\frac{\lambda k}{\mathrm{sum}}\right) \exp\left(\frac{1}{\mathrm{sum}} \sum_{\mathsf{tx}' \in M} s(\mathsf{tx}') \ln v(\mathsf{tx}')\right) \exp(-\lambda \hat{x})
$$

并可得，对所有 $\mathsf{tx} \in M$，

$$
\begin{aligned}
& v(\mathsf{tx}) \exp\left(-\lambda\left(\hat{p}^{\mathrm{real}}(\mathsf{tx})-x\right)\right) \\
=& v(\mathsf{tx}) \exp\left(-\lambda \hat{p}^{\mathrm{real}}(\mathsf{tx})\right) \exp(-\lambda x) \\
=& \exp\left(-\frac{\lambda k}{\mathrm{sum}}\right) \exp\left(\frac{1}{\mathrm{sum}} \sum_{\mathsf{tx}' \in M} s(\mathsf{tx}') \ln v(\mathsf{tx}')\right) \\
=& w.
\end{aligned}
$$

因此，

$$
\begin{cases}
p_{\hat{x}}^{\mathrm{real}}(\mathsf{tx})=0 \implies v(\mathsf{tx}) \exp\left(-\lambda p_{\hat{x}}^{\mathrm{real}}(\mathsf{tx})\right)<v(\mathsf{tx}) \exp\left(-\lambda\left(\hat{p}^{\mathrm{real}}(\mathsf{tx})-\hat{x}\right)\right)=w \\
0<p_{\hat{x}}^{\mathrm{real}}(\mathsf{tx})<1 \implies v(\mathsf{tx}) \exp\left(-\lambda p_{\hat{x}}^{\mathrm{real}}(\mathsf{tx})\right)=v(\mathsf{tx}) \exp\left(-\lambda\left(\hat{p}^{\mathrm{real}}(\mathsf{tx})-\hat{x}\right)\right)=w \\
p_{\hat{x}}^{\mathrm{real}}(\mathsf{tx})=1 \implies v(\mathsf{tx}) \exp\left(-\lambda p_{\hat{x}}^{\mathrm{real}}(\mathsf{tx})\right)>v(\mathsf{tx}) \exp\left(-\lambda\left(\hat{p}^{\mathrm{real}}(\mathsf{tx})-\hat{x}\right)\right)=w,
\end{cases}
$$

从而满足引理 3.2 的条件。因此，如果对于每个 tx $\in M$，都存在一种混合策略 $\sigma$ with$p^{\sigma}$(tx) $= p^{\text{real}}_{\hat{x}}$(tx)，那么 $\sigma$ 就是一种均衡策略。□

# B 计算$x$的算法ˆ

该算法的目标是计算方程的最小解

$$\sum_{j=1}^{m} \min(\max(p[j]-x,0),1) \times s[j] = k,$$

其中， $p[1..m]$ 和 $s[1..m]$是特定的非负数组。

**算法 2:** 计算 ˆ$x$

输入：数组 $p[1..m]$、数组 $s[1..m]$、参数 $k$。结果：ˆ$x$，方程 $\sum_{j=1}^{m}$ min(max( $p[j]-x$, 0), 1)$s[j] = k$ 的最小解。新建数组 $b[1..2m]$; 对于 $j \in \{1,2,...,m\}$，执行 $b[j] \leftarrow p[j]$; $b[j+m] \leftarrow p[j]-1$; 结束。将 $b$[]数组按从小到大排序; 定义函数 $f$: $\mathbb{R} \to \mathbb{R}$ 为 $f$(x) $= \sum_{j=1}^{m}$ min(max($p[j]-x$, 0), 1) $\times\, s[j]$; /* $f(\cdot)$ 是连续、单调不增且分段线性的。*//* $f(\cdot)$ 在每个 $[b[j], b[j+1]]$ 区间上都是线性的。*/$l \leftarrow 1$; $r \leftarrow 2m$; 当 $l+1 \neq r$ 时，执行$mid \leftarrow \lfloor \frac{l+r}{2} \rfloor$; 如果 $f(b[mid]) > k$，则$l \leftarrow mid$; 否则$r \leftarrow mid$; 结束。结束。/* 我们得到 $f(b[l]) > k$和 $f(b[l+1]) \leq k$。*/ $pos = \frac{b[l]+b[l+1]}{2}$； $d \leftarrow 0$; 对于 $j \in \{1,2,...,m\}$，如果 $pos < p[j] < pos+1$，则 $d \leftarrow d - s[j]$结束。结束。/* $d$ 是函数 $f$ 在点 ($b[l]$,$b[l+1]$) 处的斜率。*/返回 $b[l] + \frac{k-b[l]}{d}$；