arXiv:2601.20783v1 [cs.DB] 28 Jan 2026

单调优先级系统：合约特定排序基础

Naveen Durvasula

哥伦比亚大学与Ritual

2026年1月

摘要

现代区块链应用受益于能够对与其交互的交易指定排序约束。本文提出一种有原则且得到公理化论证的方法，用于对智能合约函数调用添加排序约束，并在表达力与区块生产的可处理性之间取得平衡。具体而言，我们提出一个系统，允许合约开发者为他们的每个调用设置一个整数全局优先级，只要该调用所选的优先级不高于其任何被引用调用的优先级。区块构建者随后只需按优先级顺序（从高优先级到低优先级）对交易进行排序，并可以按自己的意愿打破平局。我们证明，该系统是满足五条独立公理的唯一系统。

1 引言

1.1 合约特定排序

区块链网络维护一个公开且防篡改的状态，用于跟踪可变性受限的信息，例如账户余额。网络状态由用户提交的交易进行更新。一笔交易可以是支付，或者更一般地说，是任何符合区块链执行语义的状态转换。由于现代区块链协议支持图灵完备执行，交易在执行时可能会进行一系列复杂的函数调用。由于区块链底层共识算法的要求，交易被批量打包为区块。每个区块都是一个交易有序序列，并且还额外满足协议所设定的若干有效性约束。标准的区块有效性约束包括对区块内交易所使用的网络资源总量的限制，以及要求其组成交易必须格式正确 [W+14]。

虽然区块必须遵守这些有效性约束，但通常只有一位区块生产者拥有广泛的自由，可以选择哪些交易纳入区块，以及这些交易的执行顺序。区块生产者利用这种自由所能获得的利润称为MEV（最大可提取价值），相关研究文献丰富，涉及多个学科——例如参见 [HKFTW23, BGR24, MS22, KZGJ20] 及其中引用的文献。如今，人们已经认识到，允许应用直接

对区块内与该应用智能合约在执行过程中发生交互的交易施加额外的排序约束，可能具有一定价值。此类约束可以帮助应用改善用户体验，减轻其他用户（或追求利润最大化的区块生产者）提交的对抗性交易所造成的负面影响[Sor24, Ecl24]。这已成为采用订单簿进行撮合的去中心化交易所的一项关键特性[1] [Hyp24, CPR25, YRB+25]。本文旨在提出一种有原则且有公理依据的方法，以实现允许智能合约开发者施加额外排序约束的系统。

允许合约施加排序约束的方法有很多种。一种极端做法是，允许合约对任意两笔交易指定任意排序约束。虽然这样能让合约开发者完全掌控排序过程，却会使区块构建在计算上完全不可处理。事实上，寻找一个包含指定交易集合的有效区块，相当于解决一个一般性的布尔可满足性问题，而且有效区块甚至可能不存在！另一种极端做法则是维持现状：区块构建仍然可处理，但合约开发者无法直接对交易排序。设计合约特定排序系统的关键挑战，在于平衡系统表达力（即合约开发者对排序约束的选择有多丰富）与可处理性（即区块生产者构建满足这些额外约束的区块有多容易）之间的张力。即使假设合约只能对与其直接交互的交易施加约束，当一笔交易在执行过程中可能嵌套调用众多合约时，如何构建一个可处理的系统也并非显而易见。这些合约是否都应有权对该交易的排序施加约束？如果是，又该如何确保区块构建仍然可处理？理想的排序系统必须在满足一些基本要求的同时施加限制，以保持可处理性；这些基本要求包括允许合约对与其交互的交易施加排序约束。本文提出了一种我们认为恰到好处的系统；在某种意义上，根据对排序可处理性的特定定义，它具有最大表达力。我们将这一系统称为单调优先级系统。

1.2 单调优先级：简单而富有表现力的排序约束

单调优先级系统适用于这样一种场景：智能合约各自包含一些函数调用，或包含能够修改区块链网络状态的可执行代码区块。关键在于，函数调用可以组合使用，也就是说，它们可以调用并执行

[1]对于感兴趣的读者，我们在此进一步解释额外的排序约束如何改善去中心化订单簿的用户体验。假设发生了价格冲击，导致订单簿中交易的资产价格大幅下跌。此时，订单簿中仍挂着买单，价格高于提交这些买单的用户愿意支付的价格。这就引发了一场竞赛：一方是希望取消未成交订单的用户，另一方则想以过时的较高价格成交这些订单。未成交订单通常属于做市商，他们通过充当普通用户交易的交易对手方，为交易所提供流动性。因此，人们普遍认为，优先处理撤单能让交易所更加成功，因为改善做市商的体验被认为比让套利者以过时价格成交订单更重要。传统（中心化）订单簿也有人提出了类似的优先级安排 [BM20]。合约特定排序将使去中心化订单簿能够直接施加约束，规定在一个区块内，取消优先于成交订单，而不是让追求利润最大化的区块生产者最终决定胜者。事实上，一些最受欢迎的去中心化交易所已经以临时的方式实现了这一点 [Hyp24, CPR25]。

在其执行过程中发生的其他函数调用。正如上一小节所暗示的，可组合性正是平衡表达力与可处理性之所以困难的原因：由于一次调用可以通过嵌套子调用触及许多合约，因此人们很容易倾向于将系统设计得足够灵活，允许所有这些合约对该调用所触发交易的排序施加某些约束。然而，构建一个同时满足所有这些约束的区块，仍必须保持简单。

在单调优先级系统中，我们允许每个合约为其每个组成调用独立选择一个整数全局优先性，并规定发起较高优先级根调用的交易应排在发起较低优先级根调用的交易之前。合约开发者可以为每个调用选择任意优先级，但须满足一个简单的约束：

调用的优先级不能高于它所引用的任何调用

如果一个区块按优先级从高到低排列交易（优先级相同时可任意排序），则该区块被视为有效。为防止合约开发者为函数调用指定任意高的优先级，实践中可以设置一个最大优先级 $\lambda_{\max}$，任何合约开发者都不能选择超过该值的优先级。

要检查调用的优先级是否有效，只需检查其优先级是否不高于它直接发起的任何调用。这可以递归地保证，无论嵌套子调用的层级有多深，一个调用的优先级都不会高于它发起的任何嵌套子调用。只要优先级有效，合约开发者就可以为调用设置任意优先级。

单调优先级系统：有效优先级

优先级为 λ 的调用在满足以下条件时有效：

1. 该调用只引用有效调用
2. 该调用所引用的任何调用，其优先级都不高于 λ

从宏观层面来看，单调优先级系统施加这一约束，是为了防止用户通过可组合性绕过合约的优先级。具体来说，假设合约 x 希望将其某个调用 a 排在另一个调用 b 之前，并通过令 a 的优先级高于 b 来实现。如果我们不要求调用具有有效优先级，那么希望调用 b 、且不希望自己的交易排在对 a 的调用之后的用户，就可以在一个新合约 x' 中发起对 b' 的调用来实现这一点。调用 b' 只需直接调用 b，即可执行其行为。如果 x' 可以为 b' 设置任意优先级，那么它就可以被排在来自合约 x 的调用 a 之前。有效性约束可以防止这种行为。

1.2.1 表达力

这个系统的表达能力如何？尽管合约不能任意选择每个调用的优先性（因为必须满足 VALID），但仍可以自由调整其组成调用之间的相对优先性排序。具体来说，假设与之前一样，有一个合约[2] x，其中包含两个函数

[2]一个例 此类合约的例子是前一条脚注中的去中心化订单簿，其中 a 是用于提 on 调用以便放置 交取消的函数调用，而 b 是用于提交成交订单的函数调用。

调用 a 和 b，且该合约希望 a的优先性高于 b。如果 a 和 b 都不调用其他合约，那么很容易看出， x 可以让 a的优先性高于 b。这是因为 x 可以为这两个调用任意选择优先性，且仍满足 VALID（例如，为 a 设为 0，为 b设为 -1）。然而，即使 a 和 b 任意调用其他合约，这一点依然成立。举例来说，假设 b 仍然不调用其他合约，而 a 则调用另一个合约 x'中的一个辅助函数[3] c，并且合约 x' 将 c 的优先性设为 -100。虽然 x 必须将 a 的优先性设为不高于 -100，才能满足 VALID，但 x 仍可以让 b 的优先性低于 a，例如将其设为 -101。更一般地说，合约总能在保持 VALID 的同时，随意设定其调用优先性的相对排序，因为单调优先级系统只会阻止合约将优先性设得过高。合约总能任意降低某个调用相对于另一个调用的优先性，以实现所需的相对排序。

一旦合约为其调用确定了相对排序，单调优先级系统就允许该合约在不受其他合约所作选择影响的情况下，作出以下两项保证。具体而言，对于该合约希望排在调用 b之前的任何调用 a，该合约都可以保证：

1.**对 a 进行根调用的交易，在任何有效区块中都排在对 b 进行根调用的交易之前**。这是因为，如上文所述，该合约始终可以为 a 和 b 设置有效优先级，使得 b 的优先级低于 a。

2. **对 a 进行根调用的交易，排在其完整执行轨迹中可能在某个时刻调用 b 的任何交易之前**。任何在执行期间可能引用 b 的调用 c，其优先级都必须不高于 b，才能成为有效优先级。由于 a 的优先级高于 b，因此它的优先级也会高于 c。

可以从这两项保证的角度来理解该系统的表达力。第二项保证体现了单调优先级系统如何处理可组合性：复杂调用所交互的每个合约，确实都可以在受限的范围内对该调用施加某些排序约束。正如我们接下来将要讨论的，这些限制使系统保持简洁。

1.2.2 简洁性

单调优先级系统将各个合约的排序约束转换为一条仍然易于满足的单一区块有效性约束。从已选定要纳入某一组交易的区块构建者的视角来看，只需将交易按优先性降序排序，并以任意所需方式打破平局，即可找到一个有效区块。聚合排序约束的简洁性，使得将其与现有区块有效性约束进行组合变得直接，例如对区块内交易累积“规模”（即这些交易所使用的最大网络资源）所施加的约束。我们给出一个简单算法，可在单调优先级系统[4]下找到一个有效的交易序列。

MonotonePriority 系统还让合约开发者能够轻松推理代码修改会如何影响调用其合约的交易的排序。排序约束仅取决于调用的名称，而不取决于当前网络状态。此外，也很容易推理优先性在组合下如何变化。该合约

[3]在贯穿全文的订单簿示例中，一次取消调用可能会调用另一合约中的托管函数，以释放锁定在一笔未完成的买单中的代币。[4]枚举所有平局决胜规则 τ 即可找出包含全部这些交易的所有有效区块。

单调优先级系统：有效区块

输入： 一组交易 t_1，.....， t_n，这些交易各自对具有有效优先级的合约进行根调用。

输出： 在单调优先级系统下有效的交易排序。

将 $\tau : [n] \longleftrightarrow [n]$ 初始化为平局判定规则。然后，

1. 首先按照每个 t_i 的根调用的优先性 λ_i，以降序进行排序。
2. 对具有相同优先性的交易 t_i，再按照 $\tau(i)$ 进行排序

返回： 所得的交易有序序列

如果开发者选择加入对高优先性调用的新引用，则其调用不会面临额外的排序约束。然而，如果合约开发者加入了对低优先性调用的引用，那么开发者的调用也必须具有低优先性。换言之，一个调用的最大可能优先性只会随着其加入对其他调用的更多引用而降低。

1.3 替代设计

是否可能构建一个表达能力更强、同时又不会使区块构建变得难以处理的系统？本文以形式化方式证明的主要技术结果是否定的。更具体地说，我们定义了五条自然公理，并证明单调优先级系统是唯一满足全部这些公理的系统。下面我们对这五条公理逐一进行非正式描述：

存在性。 我们的第一条公理——存在性——要求，无论每个合约对交易施加何种排序约束，都必须存在一个区块，以满足所有约束的方式对所有交易进行排序。若不存在性不成立，合约可能会选择相互冲突的排序约束（例如，一个合约要求交易 t 先于交易 t'，而另一个合约要求交易 t' 先于交易 t），从而不存在一个既包含所有交易、又满足全部排序约束的有效区块。

优先性。 我们的第二条公理——优先性——要求系统必须允许每个合约对任何会向该合约的任一组成调用发出根调用的交易进行相对排序，而不受其他合约所施加约束的影响。这为系统提供了基本的表达力。

扩展性。 我们的第三公理——扩展性——要求：如果排序系统允许某合约将调用 c 排在 c'之前，那么它也必须将该约束扩展为：将 c 排在所有引用 c' 的其他调用之前。若没有扩展性，就很容易绕过系统的排序约束：用户只需创建一个调用 c' 的新虚设合约，就能获得与 c' 相同的功能，却不必遵守该调用必须排在 c之后的约束。

可约性。 我们的第四公理——可约性——规定，除非交易 t' 在其完整调用轨迹中引用了该合约的某个调用，且该合约也将该交易排在 t之后，否则不得要求该合约将交易 t' 排在另一笔交易 t 之后。若没有可约性，合约开发者可能很难理解其他合约可以对调用其合约的交易排序施加哪些权利。

无关调用独立性。我们的第五条也是最后一条公理，即无关调用独立性，指出：系统是否赋予某合约将一笔交易排在另一笔交易之前的选项（或许取决于其他合约的选择），必须仅取决于这两笔交易的完整调用轨迹中所引用的调用。若无此公理，合约开发者就必须对其他合约中的无关调用进行推理，才能判断自己能否对两笔特定交易施加排序约束。

本文余下部分组织如下。在第 2 节中，我们形式化定义合约特定排序权系统的完整设计空间，以及上文列出的五条公理。该设计空间十分丰富：协议可以允许合约以可取决于其他合约所作选择的方式，提出任意一组排序约束。在第 3 节中，我们用这一语言形式化描述第 1.2.1 节中的表达能力保证。随后我们证明，实现这些保证的系统在第 3.1 节中满足全部五条公理（定理 1），并在第 3.2 节中进一步证明其在此意义上是唯一的（定理 2）。在第 4 节中，我们证明这五条公理对于唯一性而言事实上都是必要的：存在其他系统满足任意四条公理的组合，但不满足第五条（定理 3）。接下来，在第 5 节中，我们讨论一个排序约束系统何时可以通过为每个函数调用分配全局整数优先级来实现。我们证明，存在性公理并不能保证这一点（定理 4），但五条公理合在一起则蕴含这一点（定理 5）。随后，我们在第 5.1 节中形式化证明，单调优先级系统实现了第 1.2.1 节中的表达能力保证（定理 6）。最后，在第 6 节中，我们给出简要讨论与开放方向。

2 模型

2.1 调用、合约与引用

我们考虑这样一种情形：存在一个调用 $\mathbb{C}$集合和一个合约 $\mathbb{X}$集合。对于任意调用 $c \in \mathbb{C}$，都关联着一个调用集合 $r(c) \subseteq \mathbb{C}$，其中包含该调用直接引用的调用（即它对其进行根调用的调用）。给定引用映射，我们可以如下定义调用 $\mathbb{C} \to 2^{\mathbb{C}}$ 的调用轨迹 tr：

$$\mathrm{tr}(c) := \{c' \in \mathbb{C} \mid \exists (c_0 := c, c_1, c_2, \ldots, c_N) \text{ s.t. } c_N = c' \text{ and } c_i \in r(c_{i-1})\} \tag{1}$$

调用轨迹包含在一次调用的完整执行过程中可能被引用的所有调用。

2.2 权限系统与公理

一个权利系统 $\mathbb{R}(p)$是由映射 $p\colon \mathbb{C} \to \mathbb{X}$参数化的非空集合族，由形如 $(\succ_x)_{x\in\mathbb{X}}$的向量组成。映射 p 指明每次调用所对应的父合约。每个 $\succ_x$ 都是全体调用集合 $\mathbb{C}$ 上的严格偏序，可解释为合约 x 选择的排序约束。我们对用于参数化一个

权利系统的父映射 施加一项额外约束。我们要求存在一个部署顺序 $>_D$：对合约集合 $\mathbb{X}$ 上的严格全序，且满足性质

$$x >_D x' \implies c \notin \mathrm{tr}(c') \text{ for all } c, c' \in \mathbb{C} \text{ s.t. } p(c) = x \text{ and } p(c') = x' \tag{2}$$

换言之，合约不能拥有一个子调用，而该子调用引用了未来部署的合约的子调用。接下来，我们要求对于任意合约 x，如果存在一个在 x之后部署的合约 $x' >_D x$，那么该合约仅拥有有限数量的子调用 $|\mathbb{C}_x(p)| < \infty$。我们称这样的合约为 p 可部署合约。

现在我们列出人们可能希望此类系统遵守的五条公理。第一条公理是存在性，它断言：对于任意有限的交易集合（每笔交易都表示为一个调用），以及从权利系统中选出的任意严格偏序集合，都存在一种区块排序 B，能够在不违反任何合约所选定的排序约束的情况下，对所有交易进行排序。

公理 1（存在性）。对于所有可部署的 p： $\mathbb{C} \to \mathbb{X}$、$(\succ_x)_{x\in\mathbb{X}} \in \mathbb{R}(p)$ 以及所有有限序列（t_1，.....，t_N），其中每个 $t_i \in \mathbb{C}$，都存在一个双射 B： $[N] \longleftrightarrow [N]$，使得对于所有 i、j（其中$i < j$），不存在满足 $t_{B(j)} \succ_x t_{B(i)}$ 的 $x \in \mathbb{X}$。

我们的第二条公理是优先性，它指出，每个合约都有权对直接调用其子调用的交易进行排序，而不受其他合约所选排序约束的影响。为正式定义这一公理，我们先给出几个中间定义。给定一个指针映射 $p : \mathbb{C} \to \mathbb{X}$，我们将每个 $x \in \mathbb{X}$ 简写为

$$\mathbb{C}_x(p) := \{c \in \mathbb{C} \mid p(c) = x\}$$

也就是说， $\mathbb{C}_x(p)$ 是在指针映射 p 下直接包含于合约 x 中的调用。若严格偏序 $\succ_x^*$ 定义在 $\mathbb{C}_x(p)$ 上，且不存在满足 $c \succ_x^* c'$ 和 $c \in \mathrm{tr}(c)$ 的 c， $c' \in \mathbb{C}_x(p)$，则称该严格偏序为容许。换言之，在指针映射 p 下，定义于合约 x 的子调用上的可容许偏序，不允许 x 在 c 调用 c' 时将调用 c 排在 c' 之前。优先性公理允许每个合约按照任意可容许偏序对其子调用进行排序，而不受其他合约所选约束的影响：

公理 2（优先性）。对于所有可部署的 p： $\mathbb{C} \to \mathbb{X}$、$(\succ_x)_{x\in\mathbb{X}} \in \mathbb{R}(p)$、所有合约 $x^* \in \mathbb{X}$，以及所有关于合约 x^*子调用集合 $\mathbb{C}_x(p)$ 的可容许严格偏序 $\succ_{x^*}^*$，存在一个 $(\succ'_x)_{x\in\mathbb{X}} \in \mathbb{R}(p)$，使得对于所有 $x \neq x^*$、 $\succ'_x = \succ_x$和 $c_1 \succ'_{x^*} c_2 \iff c_1 \succ_{x^*}^* c_2$，以及所有$c_1$、$c_2 \in \mathbb{C}_x(p)$。

我们的第三公理是扩展性，其指出：如果合约 x^* 选择在权利系统下将调用 c的优先级排在调用 c' 之前，那么该排序约束必须扩展到任何其他调用 c''，只要它在执行轨迹中的某个时刻调用了 c'。如果没有扩展性公理，交易就可能通过在另一个合约中使用虚调用来规避排序约束。

公理 3 (扩展性**)**。对于所有可部署的 p： $\mathbb{C} \to \mathbb{X}$、$(\succ_x)_{x\in\mathbb{X}} \in \mathbb{R}(p)$，所有合约 $x^* \in \mathbb{X}$ 以及所有调用 $c, c' \in \mathbb{C}$, $c \succ_{x^*} c' \implies c \succ_{x^*} c''$，对于任意满足 $c' \in \mathrm{tr}(c'')$ 的 c''。

我们的第四公理是可约性，它指出，如果合约 x 希望将调用 c排在 c'之前，那么在执行 c' 的过程中，必须存在某个子调用 c''，而该子调用 x 也必须有权排在 c之前。可约性是开发者构建此类 c'时可能至关重要的一项性质：开发者可以借此保证， x 无权将调用 c排在它之前，方法是确保 c' 不引用 x在 c之后排序的任何子调用。

公理4 (可约性)。 对于所有可部署的 $p\colon\ \mathbb{C}\to\mathbb{X}$、$(\succ_x)_{x\in\mathbb{X}}\in\mathbb{R}(p)$、所有合约 $x^*\in\mathbb{X}$以及所有调用 c, $c'\in\mathbb{C}$，如果 $c\succ_{x^*}c'$，那么要么 $p(c')=x^*$，要么存在一个 $c''\in\mathrm{tr}(c')$，使得 $p(c'')=x^*$且 $c\succ_{x^*}c''$。

我们的第五条也是最后一条公理是无关调用独立性。它指出，如果一个合约 x 能够将调用 t 排序在 t'之前，那么（或许取决于其他合约的选择）从理论上讲，如果指针映射仅对与 t和 t'无关的调用发生变化，则必须可以让 x 将 t 排序在 t' 之前。

公理*5*（无关调用独立性）。设 $p\colon\ \mathbb{C}\to\mathbb{X}$ 可部署，$(\succ_x)_{x\in\mathbb{X}}\in\mathbb{R}(p)$、 $x^*\in\mathbb{X}$以及 t、 $t'\in\mathbb{C}$ 满足 $t\succ_{x^*}t'$。那么，对于任意可部署的 $p'\colon\ \mathbb{C}\to\mathbb{X}$，若 $p'(t)=p(t)$、$p'(t')=p(t')$，并且对所有 $c\in tr(t)\cup tr(t')$均有 $p(c)=p'(c)$，则存在一个 $(\succ'_x)_{x\in\mathbb{X}}\in\mathbb{R}(p')$，使得$t\succ'_{x^*}t'$。

3 唯一权利系统

我们将权利系统 $\mathbb{R}^*(p)$ 定义为与所有满足以下条件的 $(\succ^*_x)_{x\in\mathbb{X}}$ 构成的集合之间存在双射：每个 $\succ^*_x$ 都是定义在 $\mathbb{C}_x(p)$ 上的可容许严格偏序。对于任意这样的 $(\succ^*_x)_{x\in\mathbb{X}}$，我们定义一个 $(\succ_x)_{x\in\mathbb{X}}\in\mathbb{R}^*(p)$，其中 $t\succ_x t'$ 当且仅当

1. $p(t)=p(t')=x$ 和 $t\succ^*_x t'$，或者
2. $p(t)=x$ 和 $p(t')\neq x$，且存在一个 $c\in\mathrm{tr}(t')$，使得 $p(c)=x$ 满足 $t\succ^*_x c$

请注意，这与我们在第 1.2.1 节中非正式陈述的两项保证相同。本节将证明，在满足第2.2节中公理的权利系统中， $\mathbb{R}^*(p)$ 是唯一的。

3.1 满足性

接下来，我们证明如 $\mathbb{R}^*(p)$ 所述的系统满足五条公理。我们证明 $\mathbb{R}^*(p)$ 满足存在性（引理 1）时，利用了我们在上一小节中建立的与 MonotonePriority 系统之间的对应关系。

定理 1. 对于任意具有部署顺序 $>_D$ 的 $p\colon\ \mathbb{C}\to\mathbb{X}$， $\mathbb{R}^*(p)$ 满足存在性、优先性、扩展性、可约性和无关调用独立性。

证明。

引理 1. $\mathbb{R}^*(p)$ 满足存在性。

证明。 这可直接由定理 5 和定理 4 得出，二者将在第 5 节中讨论 . ■

引理 2. $\mathbb{R}^*(p)$ 满足优先性。

证明。 这显然是因为每个 $(\succ^*_x)_{x\in\mathbb{X}}$ 其中 $\succ^*_x$ 是定义在 $\mathbb{C}_x(p)$ 上的可容许严格偏序，都在 $\mathbb{R}^*(p)$ 中有一个扩展。■

引理 3. $\mathbb{R}^*(p)$ 满足扩展性。

证明。设 $p:\mathbb{C}\to\mathbb{X}$，且 $(\succ_x)_{x\in\mathbb{X}}\in\mathbb{R}(p)$。接下来，设 $x^*\in\mathbb{X}$ 和 $t,t'\in\mathbb{C}$，使得 $t\succ_x t'$。设 $t''\in\mathbb{C}$ 是一个调用，满足 $t'\in\mathrm{tr}(t'')$。由此可知，存在一个 $c\in\mathrm{tr}(t'')$，使得 $p(c)=x^*$，因此必有 $t\succ_x t''$，如所求。■

引理 4. $\mathbb{R}^*(p)$ 满足可约性。

证明。根据 $\mathbb{R}^*(p)$ 的定义，可约性显然成立：对于所有可部署的 $p:\mathbb{C}\to\mathbb{X}$、$(\succ_x)_{x\in\mathbb{X}}\in\mathbb{R}(p)$、所有合约 $x^*\in\mathbb{X}$ 以及所有调用 $t,t'\in\mathbb{C}$，如果 $t\succ_{x^*}t'$，那么要么 $p(t')=x^*$，要么存在一个 $c\in\mathrm{tr}(t')$，使得 $p(c)=x^*$ 且 $t\succ_{x^*}c$。■

引理 5. $\mathbb{R}^*(p)$ 满足无关调用独立性。

证明。设 $p:\mathbb{C}\to\mathbb{X}$、$(\succ_x)_{x\in\mathbb{X}}\in\mathbb{R}(p)$、$x^*\in\mathbb{X}$ 和 $t,t'\in\mathbb{C}$ 满足 $t\succ_{x^*}t'$。根据 $\mathbb{R}^*(p)$ 的定义，恰有以下两种情况。

案例 3.1.1。 $p(t)=p(t')=x^*$

在此情形下，任取 $p':\mathbb{C}\to\mathbb{X}$，使得对所有 $c\in\mathrm{tr}(t)\cup\mathrm{tr}(t')$，均有 $p'(t)=p(t)$、$p'(t')=p(t')$，且 $p(c)=p'(c)$。由于 $p'(t)=p'(t')=x$，且 $\succ_{x^*}$ 在 $\mathbb{C}_{x^*}(p)$ 上是容许的，因此存在一个 $(\succ'_x)_{x\in\mathbb{X}}\in\mathbb{R}(p')$，使得 $t\succ'_{x^*}t'$。

情形 3.1. 2. $p(t)=x^*$，$p(t')\neq x^*$，并且存在一个 $c\in\mathrm{tr}(t')$，满足 $p(c)=x^*$，使得 $t\succ_{x^*}c$。

在此情形下，任取 $p':\mathbb{C}\to\mathbb{X}$，使得对所有$c\in\mathrm{tr}(t)\cup\mathrm{tr}(t')$，均有 $p'(t)=p(t)$、$p'(t')=p(t')$，且 $p(c)=p'(c)$。对于这样的 p'，我们仍必须有 $p'(t)=p'(c)=x^*$。由于 $\succ_{x^*}$ 在 $\mathbb{C}_{x^*}(p)$ 上是容许的，因此存在一个 $(\succ'_x)_{x\in\mathbb{X}}\in\mathbb{R}(p')$，使得 $t\succ'_{x^*}c$。由此可知 $t\succ'_{x^*}t'$，因为 $c\in\mathrm{tr}(t')$ 仍然成立。■

■

3.2 唯一性

接下来，我们证明，$\mathbb{R}(p)$ 是满足全部五条公理的唯一权利系统。为了证明这一结果，我们需要对调用空间作出丰富性假设，即总能创建一个新调用，该调用不同于一组现有调用，并引用另一个现有调用。

假设1 (丰富性)。对于任意有限调用集合 $N\subseteq\mathbb{C}$ 和一个调用 $c\in\mathbb{C}$，存在一个调用 $c'\in\mathbb{C}\setminus N$，使得 $c\in r(c')$。

特别是，图灵完备执行环境满足这一基本的丰富性假设。

定理 2 (唯一性)。设 $\mathbb{R}(p)$是任意一个满足存在性、优先性、扩展性、可约性和无关调用独立性的权利系统。那么，对于任意 $p:\mathbb{C}\to\mathbb{X}$, $\mathbb{R}(p)=\mathbb{R}^*(p)$。

证明。首先，假设存在矛盾：对于某个 $p:\mathbb{C}\to\mathbb{X}$，存在一个满足全部五条公理的权利系统 $\mathbb{R}(p)$，使得 $\mathbb{R}(p)\not\subseteq\mathbb{R}^*(p)$。那么，存在一个 $(\succ_x)_{x\in\mathbb{X}}\in\mathbb{R}(p)$，使得 $(\succ_x)_{x\in\mathbb{X}}\notin\mathbb{R}^*(p)$。

Lemma 6. 对于每个 $x\in\mathbb{X}$，$\succ_x$ 在限制于 $\mathbb{C}_x(p)$时都是可容许严格偏序 .

证明。假设这不成立，从而导致矛盾。那么，存在一个 $x \in \mathbb{X}$ 和 $c,\ c' \in \mathbb{C}_x(p)$，使得 $c \succ_x c'$ 且 $c' \in \mathsf{tr}(c)$。由于 $\mathbb{R}(p)$ 满足扩展性，因此可推出 $c \succ_x c$，这就构成了矛盾。■

由引理6可知，存在一个 $(\succ_x^*)_{x\in\mathbb{X}}$，使得每个 $\succ_x^*$ 都是 $\mathbb{C}_x(p)$上的可容许严格偏序，并且对于任意 $x \in \mathbb{X}$ 和 $c,\ c' \in \mathbb{C}_x(p)$，$c \succ_x^* c' \iff c \succ_x c'$。现在令 $(\succ_x')_{x\in\mathbb{X}} \in \mathbb{R}^*(p)$ 为严格偏序构成的唯一向量，它在每个 $\mathbb{C}_x(p)$上也与 $(\succ_x^*)_{x\in\mathbb{X}}$ 一致。为导出矛盾，我们证明对于任意 $x \in \mathbb{X}$ 和 $t,\ t' \in \mathbb{C}$, $t \succ_x t' \iff t \succ_x' t'$。

有三种相关情形需要考虑。

情形 3.2.1。 $p(t) = p(t') = x$

显然，$t \succ_x t' \iff t \succ_x' t'$成立，因为对于任意这样的$t,\ t' \in \mathbb{C}_x(p)$，$\succ_x$ 和 $\succ_x'$ 都与 $\succ_x^*$ 一致。

情形 3.2.2. $p(t) = x$ 和 $p(t') \neq x$。

我们首先证明 $t \succ_x t' \implies t \succ_x' t'$。反设此结论不成立。于是，$t \succ_x t'$ 且 $t \not\succ_x' t'$。由此可知，不存在满足 $t \succ_x^* c$ 的 $c \in \mathsf{tr}(t)$，其中 $p(c) = x$。然而，这意味着 $\mathbb{R}(p)$ 不满足可约性，从而导致矛盾。

接下来，我们证明 $t \succ_x' t \implies t \succ_x t$。反设此结论不成立。于是，$t \succ_x' t'$ 且 $t \not\succ_x t'$。由此可知，存在满足 $t \succ_x^* c$ 的 $c \in \mathsf{tr}(t')$，其中 $p(c) = x$。根据 $(\succ_x^*)_{x\in\mathbb{X}}$ 的定义，进一步可得 $t \succ_x c$。然而，此时我们发现 $\mathbb{R}(p)$ 不满足扩展性，从而导致矛盾。

情形 3.2.3. $p(t) \neq x$

由于 $t \not\succ_x' t'$ 对所有 t, t'，满足 $p(t) \neq x$，只需证明 $t \not\succ_x t'$。为证明这一点，反设 $t \succ_x t'$，从而得到矛盾。根据假设1，存在一个调用 $c' \in \mathbb{C}$，使得$t' \in r(c')$，且 $c' \notin \mathsf{tr}(t) \cup \mathsf{tr}(t') \cup \{t, t'\}$。接下来，由于 $\mathbb{R}(p)$ 满足无关调用独立性，存在一个 $(\succ_x)_{x\in\mathbb{X}} \in \mathbb{R}(p')$，使得 $t \succ_x t'$，其中

$$p'(c) := \begin{cases} p(t) & c = c' \\ p(c) & \text{else} \end{cases}$$

令 $x' := p(t)$。根据优先性，存在一个 $(\succ_x')_{x\in\mathbb{X}} \in \mathbb{R}(p')$，使得 $t \succ_x' t'$ 且 $t' \succ_{x'}' t$。接下来，考虑交易序列 $(t_1, t_2) := (t, t')$。因此，对于任意 $B\colon [2] \longleftrightarrow [2]$，都有 $t_{B(2)} \succ_x' t_{B(1)}$ 或 $t_{B(2)} \succ_{x'}' t_{B(1)}$。然而，$\mathbb{R}(p)$ 此时必定不满足存在性，从而得到所需的矛盾。

随着这一案例的结论得出，我们已经证明了 $\mathbb{R}(p) \subseteq \mathbb{R}^*(p)$。接下来，我们证明$\mathbb{R}^*(p) \subseteq \mathbb{R}(p)$。为此，反设存在一个不属于 $\mathbb{R}(p)$的 $(\succ_x)_{x\in\mathbb{X}} \in \mathbb{R}^*(p)$。由此可知，对于某个 $(\succ_x^*)_{x\in\mathbb{X}}$，其中每个 $\succ_x^*$ 都是 $\mathbb{C}_x(p)$上的容许严格偏序，不存在一个 $(\succ_x')_{x\in\mathbb{X}} \in \mathbb{R}(p)$，使其在每个 $\mathbb{C}_x(p)$上都与 $(\succ_x^*)_{x\in\mathbb{X}}$ 一致。然而，由于 $\mathbb{R}(p)$必定非空，我们可以反复应用优先性来找到这样的 $(\succ_x')_{x\in\mathbb{X}} \in \mathbb{R}(p)$，从而得到矛盾。■

4 独立性

在本节中，我们证明五条公理彼此独立。

定理 3. 存在性、优先性、扩展性、可约性和无关调用独立性是彼此独立的公理。

证明。 为证明这一论断，我们需要展示一个模型：它满足任意四条公理，却不满足第五条。因此，这个证明分为五个引理。

引理7。 存在一个模型不满足存在性，但满足优先性、扩展性、可约性和无关调用独立性。

证明。设 $\mathbb{C} := \{a, a', b\}$，其中 $r(a) = r(b) = \emptyset$，且 $r(a') = \{a\}$。设 $\mathbb{X} = \{A, B\}$。给定任意可部署的 $p : \mathbb{C} \to \mathbb{X}$，我们按如下方式定义一个权利系统 $\mathbb{R}(p)$。合约 A 可以在 $\mathbb{C}_A(p)$ 上选择任意可容许严格偏序 $\succ_A$。于是，对于任意 $c \in \mathbb{C}_A(p)$ 和 $c' \in \mathbb{C}_B(p)$，我们令$c \succ_A c'$，当且仅当存在一个 $c'' \in \mathbb{C}_A(p)$，使得 $c' \in \mathrm{tr}(c'')$。合约 B 以类似方式选择一个$\succ_B$。然而， B 还可以（可选地）选择添加任何形式为 $c \succ_B c'$ 的约束，其中 $p(c') = B$，且 $c \notin \mathrm{tr}(c')$。对于添加的任何此类约束，也必须添加约束 $c \succ_b c''$，其中任意 c'' 均满足 $c' \in \mathrm{tr}(c'')$。如果相应的 $\succ_B$ 仍为严格偏序，则 B 可以选择它。

权利系统 $\mathbb{R}^*(p)$ 显然满足优先性（因为 B 可以选择不施加任何额外约束）。它还满足扩展性，因为我们已明确在该约束下闭合所有 $\succ_A$ 和 $\succ_B$。接下来请注意， A对 $\succ_A$ 的选择显然满足可约性。 B 的选择同样满足可约性，因为如果它添加任何额外约束 $c \succ_B c'$，那么要么 $p(c') = B$，要么存在某个 c''，使得 $c \succ_B c''$, $p(c'') = B$，且 $c'' \in \mathrm{tr}(c')$。最后，该权利系统满足无关调用独立性，因为任一合约 $x \in \mathbb{X}$ 是否可以为某个c， $c' \in \mathbb{C}$ 选择 $c \succ_x c'$，只取决于 p 在集合 $\{c, c'\} \cup \mathrm{tr}(c) \cup \mathrm{tr}(c')$ 上的值。

然而，考虑特定的父映射

$$p^*(c) := \begin{cases} A & c \in \{a', b\} \\ B & c = a \end{cases}$$

该映射在排序 $A >_D B$ 下是可部署的。然而，在权利系统 $\mathbb{R}^*(p^*)$ 下，可以选择 $\succ_B$ 使得 $b \succ_B a$ 且 $b \succ_B a'$，同时也可以选择 $\succ_A$ 使得$a' \succ_A b$。这与存在性相矛盾，因为对于交易序列 $(t_1, t_2) := (a', b)$，对任意B：$[2] \longleftarrow [2]$，都将存在某个合约 $x \in \mathbb{X}$ 使得 $t_{B(2)} \succ_x t_{B(1)}$。 ■

引理 8. 存在一个不满足优先性、但满足存在性、扩展性、可约性以及无关调用独立性的模型。

证明。 取 $\mathbb{C} := \{a, b, c, d\}$，其中对所有 $t \in \mathbb{C}$， $r(t) = \emptyset$ $\mathbb{X} := \{A, B\}$，并令 $\mathbb{R}(p)$ 仅含一个元素 $(\emptyset_A, \emptyset_B)$，其中每个 $\emptyset_x$ 都是空序关系。这显然满足存在性（因为它不产生任何约束）、扩展性（因为没有需要扩展的约束）、可约性（因为没有需要约简的约束）以及无关调用独立性（因为它是常量）。它不满足优先性，因为对于任意 $(\succ_A^*, \succ_B^*)$（其中每个 $\succ_x^*$ 都是 $\mathbb{C}_x(p)$ 上的严格偏序；在此模型中，所有此类排序都是容许的），若某个 $\succ_x^*$ 不是空序关系，则不存在一个 $(\succ_A, \succ_B) \in \mathbb{R}(p)$，使得当限制到 $\mathbb{C}_x(p)$ 时， $\succ_x = \succ^*$。 ■

引理 9。 存在一个不满足扩展性，但满足存在性、优先性、可约性和无关调用独立性的模型。

证明。设 $\mathbb{C} := \{a, a', b\}$ 且 $X := \{A, B\}$，其中 $r(a) = r(b) = \emptyset$ 且 $r(a') = a$。然后我们将$\mathbb{R}(p)$定义为一个权利系统，其中包含所有满足以下条件的 $(\succ_A, \succ_B)$： $\succ_A$ 恰好是 $\mathbb{C}_A(p)$上的严格偏序，且 $\succ_B$ 恰好是 $\mathbb{C}_B(p)$上的严格偏序，并且不允许任何约束 $c \succ_x c'$，其中对任意 $x \in \mathbb{X}$有 $p(c) \neq p(c')$。

该系统满足存在性，因为我们可以任意排列这些合约，然后对任意交易序列 $(t_1, \ldots, t_N)$ 先按其合约在 p 下的顺序排列，再按该合约所选择的偏序排列。该系统平凡地满足优先性和可约性（因为它仅在 $p(c') = x$ 时允许$c \succ_x c'$ ）。最后，它满足无关调用独立性，因为合约 x 对 $c \succ_x c'$ 进行排序的选择仅依赖于 $p(c)$ 和 $p(c')$。

然而， $\mathbb{R}(p)$不满足扩展性。选择

$$p^*(c) := \begin{cases} A & c = a' \\ B & c = \{a, b\} \end{cases}$$

（这很容易验证为可部署），虽然存在一个 $\succ_B$ 使得 $b \succ_B a$，但不存在$\succ_B$ 使得 $b \succ_B a'$，尽管 $a \in \mathrm{tr}(a')$。■

引理 10. 存在一个模型不满足可约性，但满足存在性、优先性、扩展性和无关调用独立性。

证明。令 $\mathbb{C} := \{a', a, b\}$ 和 $\mathbb{X} := \{A, B\}$。令 $r(a) = r(b) = \emptyset$ 和 $r(a') = \{a\}$。给定任意可部署的 $p : \mathbb{C} \to \mathbb{X}$，我们定义权利系统 $\mathbb{R}(p)$如下。合约 A 可以在 $\mathbb{C}_A(p)$ 上选择任意可容许严格偏序 $\succ_A$ 。然后，对于任意 $c \in \mathbb{C}_A(p)$ 和 $c' \in \mathbb{C}_B(p)$，我们令$c \succ_A c'$ 当且仅当存在一个 $c'' \in \mathbb{C}_A(p)$使得 $c' \in \mathrm{tr}(c'')$。合约 B 以类似方式选择一个$\succ_B$。然而， B 还可以（可选地）选择添加任意形式为 $c \succ_B c'$ 的约束，其中 $p(c) = B$、$p(c') \neq B$、 $c \notin \mathrm{tr}(c')$，并且存在某个 $c'' \in \mathrm{tr}(c)$使得 $p(c'') = B$。对于任何此类添加的约束，也必须添加约束 $c \succ_b c''$ ，对于任意满足 $c' \in \mathrm{tr}(c'')$ 的 c'' 。如果相应的 $\succ_B$ 仍然是严格偏序，那么 B 可以选择它。

该系统满足存在性，因为至多只能有一个形式为 $c \succ_x c'$where $p(c) \neq p(c')$ 的约束。这是因为，只有存在某个 $c'' \in \mathrm{tr}(c')$，使得 $p(c'') = p(c)$，才会产生此类约束。只有一对调用（a 和 a'）可能满足这一关系，因此，对于两个合约，不可能同时存在这样的 c 和 c' 。由于所有其余约束在关于 $\mathbb{C}_x$的偏序下彼此一致，因此存在一个满足所有约束的全序。该系统从构造上显然满足优先性和扩展性。它也满足无关调用独立性，因为对于任何在 $\{c, c'\} \cup \mathrm{tr}(c')$ 上保持不变的 p'，合约 x’ 添加约束 $c \succ_x c'$ 的能力不会改变。

然而， $\mathbb{R}(p^*)$ 不满足可约性，原因是

$$p^*(c) := \begin{cases} A & c = a' \\ B & c = \{a, b\} \end{cases}$$

这是因为我们可以让 $a \succ_B b \succ_B a'$ 在 $\mathbb{R}(p^*)$ 下成立。这与可约性矛盾，因为 $b \succ_B a'$，但不存在满足 $b \succ_B c$ 的 $c \in \mathrm{tr}(a')$。■

引理11. 存在一个模型不满足无关调用独立性，但满足存在性、优先性、扩展性和可约性。

证明。设 $\mathbb{C} := \{a', a, b\}$ 且 $\mathbb{X} := \{A, B\}$。令 $r(a) = r(b) = \emptyset$ 且 $r(a') = \{a\}$。对于任意可部署的 $p : \mathbb{C} \to \mathbb{X}$，我们定义权利系统 $\mathbb{R}(p)$ 如下。合约 A 可以在 $\mathbb{C}_A(p)$ 上选择任意可容许严格偏序 $\succ_A$。然后，对于任意 $c \in \mathbb{C}_A(p)$ 和 $c' \in \mathbb{C}_B(p)$，我们令$c \succ_A c'$ 当且仅当存在一个 $c'' \in \mathbb{C}_A(p)$，使得 $c' \in \mathsf{tr}(c'')$。合约 B 同样选择一个 $\succ_B$。然而， B 还可以（选择性地）添加约束 $b \succ_B a$ 和 $b \succ_B a'$，当且仅当 $p(b) = A$、$p(a) = B$且 $p(a') = B$。

该系统满足存在性，因为如果 B 不选择添加额外约束，那么就只有针对同一合约子调用的排序约束。如果 B 选择添加额外约束，那么就不可能存在冲突约束 $a \succ_A b$ 或 $a' \succ_A b$，因为 $p(a) = p(a') \neq A$。该系统按构造显然满足优先性和扩展性。它也满足可约性，因为原有约束满足可约性，而只有在 $p(a) = p(a') = B$时，才能添加额外约束$b \succ_B a$ 和 $b \succ_B a'$。

然而， $\mathbb{R}(p)$ 不满足无关调用独立性，因为若 $p(a') = B$，则约束 $b \succ_B a$ 可以实现；但若 $p(a') = A$，则无法实现。由于 $a' \notin \{a, b\} \cup \mathsf{tr}(a) \cup \mathsf{tr}(b)$，因此违反了无关调用独立性。■

■

5 全局排序

除了第2.2节列出的公理之外，要实现第1.2.2节所述的可处理区块构建过程，还需要满足一项额外性质：由权利系统诱导的排序约束可以表示为针对所有调用的静态全局优先级。全局优先序可以理解为将调用集合 $\mathbb{C}$ 嵌入全序集 $(A, >)$，使得该全序遵循各合约设定的所有排序约束。

定义 1 (可排序性)。 设 $(A, >)$ 为一个全序集。若对于所有可部署的 $p : \mathbb{C} \to \mathbb{X}$ 以及 $(\succ_x)_{x \in \mathbb{X}} \in \mathbb{R}(p)$，存在一个 $\lambda : \mathbb{C} \to A$，使得对于任意 $c, c' \in \mathbb{C}$ 和 $x \in \mathbb{X}$, $c \succ_x c' \implies \lambda(c) > \lambda(c')$，则称权利系统 $\mathbb{R}(p)$ 是 A-可排序的。

不难看出，可排序性蕴含存在性。如果所有调用的集合 $\mathbb{C}$能够以尊重权利系统下各合约所选择的全部排序约束的方式被全序排列，那么对于任意有限的交易集合，都可以通过按全局排序对交易进行排序来构建一个有效区块。人们很容易认为其逆命题同样成立：如果任意有限的交易集合都可以被排序，那么或许也存在一种适用于所有调用的全局排序。从某种意义上说这是对的，但前提是我们允许优先级顺序嵌入到有理数 $\mathbb{Q}$中，而这过于丰富，对实际实现并无用处。若不使用无限多的比特，就不可能存储任意有理数。因此，对于满足存在性的任意权利系统，可能并不存在一种将每个调用静态分配到全局整数优先级的方法，使得该优先级无需在每次部署新合约时重新计算。要求存在一种具有固定最大优先级 $\lambda_{\mathtt{max}}$的全局整数优先级排序，则是一个更强的约束。

定理 4. 一个权利系统 $\mathbb{R}(p)$ 满足存在性，当且仅当它是 $\mathbb{Q}$-可排序的。然而，存在性并不蕴含 $\mathbb{Z}$-可排序性，且 $\mathbb{Z}$-可排序性对任意 $\lambda_{max} \in \mathbb{Z}$都不蕴含 $\mathbb{Z}_{\leq \lambda_{max}}$-可排序性。

证明。我们首先证明，$\mathbb{Q}$-可排序性蕴含存在性。设 $\mathbb{R}(p)$ 是一个 $\mathbb{Q}$-可排序的权利系统。对于任意 $(\succ_x)_{x\in\mathbb{X}}$，必然存在一个 $\lambda : \mathbb{C} \to \mathbb{Q}$ 使得对于任意 $c,\ c' \in \mathbb{C}$ 以及 $x \in \mathbb{X}$，$c \succ_x c' \implies \lambda(c) > \lambda(c')$。接下来，设 $(t_1, \ldots, t_N)$ 是任意有限调用序列。任选一个$B\colon [N] \longleftarrow [N]$，按照 $\lambda(t_i)$ 对 t_i进行降序排序。由此可知，不存在一个 $i < j$ 和 $x \in \mathbb{X}$ 使得 $t_{B(j)} \succ_x t_{B(i)}$，所需结论随即得证。

接下来，我们证明存在性蕴含 $\mathbb{Q}$-可排序性。首先注意，对于任意可部署的 p以及任意 $(\succ_x)_{x\ in\mathbb{X}} \in \mathbb{R}(p)$，由 $\bigcup_{x\in\mathbb{X}} \succ_x$ 在传递性下的闭包所给出的二元关系 $\succ$ 必然是严格偏序。这是因为，如果它不是非自反的或反对称的，那么必然存在某些 $c_1, \ldots, c_k \in \mathbb{C}$ 以及 $x_1, \ldots, x_k \in \mathbb{X}$ 使得

$$c_1 \succ_{x_1} \cdots c_k \succ_{x_k} c_1$$

然而，此时，权利系统 $\mathbb{R}(p)$ 对调用序列 $(c_1, \ldots, c_k)$ 将不满足存在性。众所周知，$\succ$上的任意严格偏序都可以扩展为 $\mathbb{C}$ 上的全序 $>$。此外，众所周知，可数集上的任意全序都可以嵌入 $\mathbb{Q}$。由此即可得出结论。

其余两项陈述也可直接由一些众所周知的结果推出：$\mathbb{Q}$ 的子集未必能够在保持序关系的情况下嵌入 $\mathbb{Z}$（类似地，$\mathbb{Z}$ 也不能在保持序关系的情况下嵌入$\mathbb{Z}_{\leq \lambda_{\max}}$）。不过，为了体现这些论证的直观含义，我们明确给出一个反例，说明为什么满足存在性的权利系统未必是 $\mathbb{Z}$-可排序的。

为此，令 $\mathbb{C}$ 为一个可数无限集，并令 $\mathbb{R}(p)$ 只包含一个元素 $(\succ_x)_{x\in\mathbb{X}}$。该元素定义如下：首先，令 $x^* \in \mathbb{X}$ 为 $\mathbb{X}$ 中的一个特定元素。对于所有 $x \neq x^*$，我们定义 $\succ_x := \emptyset$ 为 $\mathbb{C}$ 上的空序关系（即，$\mathbb{C}$ 中的所有元素都彼此不可比较）。接着，我们如下定义 $\succ_{x^*}$。首先，令 $c_0, c_F \in \mathbb{C}$ 为 $\mathbb{C}$ 中任意的调用。然后，定义 $\mu\colon \mathbb{C} \setminus \{c_0, c_F\} \longleftrightarrow \mathbb{Z}$ 为任意一个双射。这样的双射必定存在，因为 $\mathbb{C} \setminus \{c_0, c_F\}$ 是可数的。接着，对于任意 $c, c' \in \mathbb{C}$:

$$c \succ_{x^*} c' \iff \mu(c) > \mu(c') \text{ or } [c = c_0 \text{ and } c' \neq c_0] \text{ or } [c \neq c_F \text{ and } c' = c_F]$$

为了看出 $\mathbb{R}(p)$ 满足存在性，请注意，对于任意有限调用序列 $(t_1, \ldots, t_N)$，我们可以先按 $\mu(t_i)$ 对所有 $t_i \notin \{c_0, c_F\}$ 降序排序，再将所有 $t_i = c_0$ 排在开头、所有 $t_i = c_F$ 排在末尾，从而找到一个合适的双射 B。然而，这个 $\mathbb{R}(p)$ 并不满足 $\mathbb{Z}$-可排序性。为了看出这一点，假设为了导出矛盾它确实满足，并以 $\lambda : \mathbb{C} \to \mathbb{Z}$ 作为相应的排序。那么，$G := \lambda(c_0) - \lambda(c_F) < \infty$。然而，由于 μ 是一个双射，对于任意这样的 G，存在 $G+1$ 个调用 $c_1, \ldots, c_{G+1} \in \mathbb{C} \setminus \{c_0, c_F\}$，使得

$$c_0 \succ_{x^*} c_1 \succ_{x^*} \cdots \succ_{x^*} c_{G+1} \succ_{x^*} c_F$$

由此可得 $\lambda(c_{G+1}) \leq \lambda(c_0) - G$，但这样一来我们必然有 $\lambda(c_{G+1}) \leq \lambda(c_F)$，从而得出矛盾。■

5.1 单调优先级

尽管存在性并不蕴含 $\mathbb{Z}_{\leq \lambda_{\max}}$-可排序性，但在本小节中，我们将说明存在性、优先性、扩展性、可约性和无关调用独立性这五条公理如何共同

蕴含这一良好性质。具体而言，我们将证明，满足全部五条公理的唯一权利系统 $\mathbb{R}^*(p)$具有 $\mathbb{Z}_{\leq \lambda_{\max}}$-可排序性。按照第 1.2 节中的描述，我们通过将$\mathbb{R}^*(p)$与单调优先级系统正式关联起来，构造性地证明这一点。

令 $\lambda_{\max} \in \mathbb{Z}$ 为一个整数，表示调用所能具有的最大优先级。我们将单调优先级系统 λ: $\mathbb{C} \to \mathbb{Z}_{\leq \lambda_{\max}}$ 定义为一个映射，它为所有调用定义全局整数优先级，使得对于任意调用 $c \in \mathbb{C}$, $\lambda(c) \leq \min\{\lambda(c') \mid c' \in \mathrm{tr}(c)\}$。请注意，此定义与第 1.2 节中的 VALID 定义一致。我们首先证明， $\mathbb{R}^*(p)$ 的任意元素都可以由单调优先级系统排序。

定理 5. 对于任意 p： $\mathbb{C} \to \mathbb{X}$，其部署顺序为 $>_D$，且 $(\succ_x)_{x\in\mathbb{X}} \in \mathbb{R}^*(p)$，存在一个单调优先级系统 λ： $\mathbb{C} \to \mathbb{Z}_{\leq \lambda_{max}}$，使得对于任意 $x \in \mathbb{X}$ 和 $t, t' \in \mathbb{C}_x(p)$， $t \succ_x t' \implies \lambda(t) > \lambda(t')$。

证明。令 $(\succ_x)_{x\in\mathbb{X}} \in \mathbb{R}^*(p)$。我们利用部署顺序 $>_D$归纳地定义 λ。令x_0、x_1、$\cdots \in \mathbb{X}$为 $\mathbb{X}$中所有合约的唯一排序，使得当 $i < j$时， $x_i >_D x_j$。注意到 $\bigcup_{x\in\mathbb{X}} \mathbb{C}_x(p) = \mathbb{C}$，我们通过定义其在每个 $\mathbb{C}_x(p)$上的值，构造性地定义 λ。

首先，令 $\{c_1^0, \ldots, c_{N_0}^0\} := \mathbb{C}_{x_0}(p)$ 表示 x_0 在 p下的子调用。此外，令 c_1^0、.....、 $c_{N_0}^0$ 满足

$$c_i^0 \succ_{x_0} c_j^0 \implies i < j$$

该排序存在，直接源于任何严格偏序都可以扩展为全序这一事实。随后，我们对所有 $i \in [N_0]$定义 $\lambda(c_i^0) := \lambda_{\max} - i$。注意，由于 $\succ_{x_0}$限制在 $\mathbb{C}_{x_0}(p)$上时必须是容许的，因此对于所有 $c \in \mathbb{C}_{x_0}(p)$，必然有 $\lambda(c) \leq \min\{\lambda(c') \mid c' \in \mathrm{tr}c\}$。因此，除了为 $\mathbb{C}_{x_0}(p)$ 中的所有调用定义 λ 之外，我们还证明了将 λ 限制在这些调用上时，它是一个有效的单调优先级系统。

接下来，对于任意满足 x_k 在部署排序中并非末位的 $k > 0$，令 $\{c_1^k, \ldots, c_{N_k}^k\} := \mathbb{C}_{x_k}(p)$。同样，还需确保

$$c_i^k \succ_{x_k} c_j^k \implies i < j$$

现在我们通过归纳定义 $\lambda(c_i)$。从 c_1^k开始，我们定义

$$\lambda(c_1^k) := \min\left\{\lambda(c) \mid c \in \mathrm{tr}(c_1^k)\right\},$$

当 $\mathrm{tr}(c_1^k) = \emptyset$ 时，将其定义为 $\lambda_{\max} - 1$。这是良定义的，因为对于所有满足 $\mathrm{tr}(c_1^k)$ 的此类 $c \in$，我们已经通过归纳定义了 λ。接下来，对于任意 $1 < i < N_k$，我们定义

$$\lambda(c_i^k) := \min\left(\lambda(c_{i-1}^k) - 1, \min\left\{\lambda(c) \mid c \in \mathrm{tr}(c_i^k)\right\}\right)$$

请注意，这也是良定义的，因为将 $\succ_x$ 限制在 $\mathbb{C}_{x_k}(p)$ 上时是容许的，因此在所有引用 λ 的情况下，我们都已通过归纳定义了它。此外，还需注意，对于所有 $c \in \mathbb{C}_{x_k}(p)$，必定还有 $\lambda(c) \leq \min\{\lambda(c') \mid c' \in \mathrm{tr}(c)\}$。因此，我们也证明了将 λ 限制于这些调用时，它是一个有效的单调优先级系统。

最后，对于终端合约 x_F（如果存在），我们令 $\{c_1^F, c_2^F, \ldots\} := \mathbb{C}_{x_F}(p)$。同样，请确保

$$c_i^F \succ_{x_F} c_j^F \implies i < j$$

然后，我们以与之前完全相同的方式对 $\lambda(c_i^F)$ 进行归纳定义，并注意到，在每个归纳步骤中，由于其中仍然只有有限项，最小值始终是定义良好的。同样的

论证表明，将 λ 限制在 $\mathbb{C}_{x_F}(p)$ 上时，它是一个有效的单调优先级系统。因此，λ 确实是一个单调优先级系统。

接下来，我们证明对于这个 λ，如果对于某个 $x \in \mathbb{X}$ 有 $t \succ_x t'$，且 $t,\ t' \in \mathbb{C}$，那么 $\lambda(t) > \lambda(t')$。我们通过分成两个穷尽的情形来证明这一点。

情形 5.1.1。 $p(t) = p(t') = x$

在这种情形下，我们有：对于某个 $k \in \mathbb{N} \cup \{F\}$，$x = x_k$，并且对于 $i < j$，有 $t = c_i^k$ 和 $t' = c_j^k$。注意，在基础情形和归纳情形中，我们都确保对于 $i < j$，$\lambda(c_i^k) > \lambda(c_j^k)$。因此，所需的 $\lambda(t) > \lambda(t')$ 成立。

情形 5.1.2。 $p(t) = x$ 且 $p(t') \neq x$，并且存在一个 $c \in \mathrm{tr}(t')$，满足 $p(c) = x$，使得 $t \succ_x c$

在这种情形下，我们有 $x = x_k$，且对于某个 $k,\ k' \in \mathbb{N} \cup \{F\}$，有 $p(t') = x_{k'}$，并且 $t = c_i^k$, $c = c_j^k$ 满足 $i < j$，且 $t' = c_\ell^{k'}$。注意，根据部署顺序的性质（此处将 F 记作大于所有自然数），必有 $k' > k$；由此可知，在归纳步骤中，

$$\lambda(t) = \lambda(c_i^k) > \lambda(c_j^k) \geq \lambda(c_\ell^{k'}) = \lambda(t'),$$

由此即得所需结果。 ■

接下来，我们证明不存在“额外的”单调优先级系统，即每一个单调优先级系统实际上都对 $\mathbb{R}^*(p)$ 中的某个元素给出全局排序。

定理 6. 对任意 $p : \mathbb{C} \to \mathbb{X}$，其部署顺序为 $>_D$，以及单调优先级系统 $\lambda : \mathbb{C} \to \mathbb{Z}_{\lambda_{max}}$，存在一个 $(\succ_x)_{x \in \mathbb{X}} \in \mathbb{R}^*(p)$，使得对任意 $x \in \mathbb{X}$ 与 $c,\ c' \in \mathbb{C}$，$c \succ_x c' \implies \lambda(c) > \lambda(c')$

证明. 对任意 $x \in \mathbb{X}$ 与 $t, t' \in \mathbb{C}_x(p)$，首先注意到，存在一个定义在 $\mathbb{C}_x(p)$ 上的容许 $\succ_x^*$，使得 $\lambda(t) > \lambda(t') \iff t \succ_x^* t'$。设 $(\succ_x)_{x \in \mathbb{X}}$ 为 $\mathbb{R}^*(p)$ 中与 $(\succ_x^*)_{x \in \mathbb{X}}$ 相关联的唯一元素。接下来，设 $x \in \mathbb{X}$ 为任意合约，并设 $c, c' \in \mathbb{C}$ 为满足$c \succ_x c'$的任意调用。我们证明 $\lambda(c) > \lambda(c')$。我们通过划分为两种穷尽情形来证明这一点。

案例 5.1.3. $p(c) = p(c') = x$

在此情形下，根据构造可知 $c \succ_x c' \implies c \succ_x^* c' \implies \lambda(c) > \lambda(c')$。

情形 5.1.4. $p(c) = x$ 以及 $p(c') \neq x$，并且存在一个 $f \in \mathrm{tr}(c')$，满足 $p(f) = x$，使得 $c \succ_x f$

在此情形下，我们有 $c \succ_x f \implies c \succ_x^* f \implies \lambda(c) > \lambda(f)$。接下来，根据单调优先级系统的定义可知 $\lambda(c') \leq \lambda(f)$，由此便得到所需结果。这证明了定理的第一部分。■

6 讨论

在这项工作中，我们定义了单调优先级系统，并证明它是唯一满足五条自然公理的系统。该系统允许合约将额外的排序约束作为区块有效性的一部分进行非平凡的指定，同时又足够简单，有望在当前基础设施上实现。接下来，我们将更详细地讨论这五条公理。

定理 3 表明，如果我们的五条公理中任意一条被舍弃，那么除单调优先级系统之外，还存在其他满足其余四条公理的排序系统。这些系统中是否有值得考虑的？如果有，这类系统不满足的是哪条（哪些）公理？

关键公理：存在性、优先性与扩展性。很难想象任何合理的系统会不满足这三条公理。失去存在性将导致对交易纳入增加有实质意义的额外约束，而不是仅仅对排序施加约束。很难想象这会是可处理的。没有优先性的系统将缺乏基本水平的表达能力。没有扩展性的系统根本无法强制执行，因为用户届时可以轻易通过创建新合约来规避排序约束。

话虽如此，也许可以有一种合理的系统，采用修改后的扩展性。例如，可以允许合约指定其组成调用之间不容许的偏序，而只要求扩展性对其他合约中的调用成立。在这种情况下，系统确实会变得更加复杂：假设合约 x 包含两个调用 a 和 b，其中 $b \in \mathsf{tr}(a)$ 优先于 $a \succ_x b$（因此不容许）。再假设另一个合约 x' 中的调用 c引用了 a。一个微妙的问题是，系统是否应强制要求 $a \succ_x c$。这仍然是一个可约化的约束，因为 $b \in \mathsf{tr}(c)$（因为它属于 $\mathsf{tr}(a)$，且 $a \in \mathsf{tr}(c)$），并且 $a \succ_x b$。然而，为了适应这一点而修改单调优先级系统会带来复杂性，因为现在对合约开发者所选优先级的限制，不仅取决于被直接引用的调用，还取决于被间接引用的调用。反之，如果系统不强制要求 $a \succ_x c$，那么我们就可以保留像单调优先级系统这样简单的优先级排序系统，但所作出的具体扩展性保证会变得更加复杂，不过仍可能具有实用性。

可协商公理：可约性、无关调用独立性。失去其中任何一条公理，都会导致这样一种系统：从合约开发者的角度来看，理解对合约代码的修改将如何影响排序，会变得明显更加复杂。然而，与其他三条公理相比，这些公理对于一个实用系统而言，似乎并非那么不可或缺。

拥有静态的全局整数排序（如第 5 节所述）也是一项非常便利的性质，有助于使区块构建保持可处理性。它使第1.2.2节讨论的简单排序算法能够根据一组交易找到一个有效区块。虽然有可能存在一种缺乏全局整数优先级排序、但仍然支持实用排序算法的合理权利系统，但失去这一性质会使区块构建明显变得更加难以处理。

贯穿本文的最后一条隐含公理是无状态性。很难想象在保持区块构建可处理性的同时，能够表达状态依赖的排序约束，因为交易的相对排序会影响底层状态。至于是否存在另一种排序系统，能够在不同方面做出具有实际意义的权衡，我们将这一问题留待进一步研究。

7 致谢

谨向 Noam Nisan 和 Tim Roughgarden 致谢，感谢他们就该系统的描述与阐释方式提出了宝贵意见。

引用

[BGR24] Maryam Bahrani、Pranav Garimidi 和 Tim Roughgarden。《后 MEV 世界中的交易费用机制设计》。密码学电子印刷档案，2024年。[BM20] Markus Baldauf 和 Joshua Mollner。《高频交易与市场表现》。《金融学杂志》，75(3)：1495–1526，2020年。[CPR25] Cavey、Jakob Povˇsiˇc 和 Max Resnick。《通过异步市场队列（AMQ）实现应用控制执行（ACE）》。https://www.temporal.xyz/writings/application-controlled-execution-ace-through-asynchronous-marke t-queues-amqs，2025年9月。Temporal 研究文章。发布于2025年9月22日。[Ecl24] Eclipse Labs。《深入了解应用专属排序》。https://www.eclipse.xyz/articles/a-deep-dive-into-application-specific-sequencing，2024年10月。发布于2024年10月9日。[HKFTW23] Lioba Heimbach、Lucianna Kiffer、Christof Ferreira Torres 和 Roger Wattenhofer。《以太坊的提议者-构建者分离：承诺与现实》。载于*2023*年 *ACM* 互联网测量大会论文集，第406–420页，2023年。[Hyp24] Hyperliquid。《Hyperliquid 上的延迟与交易排序》。https://hyperliquid.medium.com/latency-and-transaction-ordering-on-hyperliquid-cf28d f3648eb，2024年1月。Medium 博文。发布于2024年1月6日。[KZGJ20] Mahimna Kelkar、Fan Zhang、Steven Goldfeder 和 Ari Juels。《拜占庭共识的排序公平性》。载于国际密码学年会，第451–480页。施普林格，2020年。[MS22] Dahlia Malkhi 和 Pawel Szalachowski。《基于有向无环图的最大可提取价值（MEV）保护》。*arXiv* 预印本 *arXiv:2208.00940*，2022年。[Sor24] Sorella Labs。《去中心化金融与应用专属排序的新时代》。https://sorellalabs.xyz/writing/a-new-era-of-defi-with-ass，2024年10月。发布于2024年10月14日。[W+14] Gavin Wood 等。《以太坊：安全的去中心化通用交易账本》。以太坊项目黄皮书，151(2014)：1–32，2014年。[YRB+25] Anatoly Yakovenko、Max Resnick、Lucas Bruder、Austin Federa、Chris Heaney 和 Kyle Samani。《互联网资本市场路线图》。https://www.anza.xyz/blo g/the-internet-capital-markets-roadmap，2025年7月。Anza 博文。发布于2025年7月24日。