arXiv:2302.06136v1 [cs.CR] 13 Feb 2023

# PRAGTHOS：实用且在博弈论意义上安全的工作量证明区块链

预印本

**Varul Srivastava**海得拉巴印度信息技术学院机器学习实验室
varul.srivastava@research.iiit.ac.in

**Sujit Gujar博士**海得拉巴
印度信息技术学院机器学习实验室 sujit.gujar@iiit.ac.in

2023年2月13日

**摘要**

区块链技术的安全分析是一个活跃的研究领域。针对工作量证明（PoW）区块链，已有密码学安全分析和博弈论安全分析。重要研究包括基于通用可组合框架的密码学安全分析，以及采用理性协议设计的博弈论安全分析。这些安全分析模型依赖于更严格的假设，而这些假设未必成立。

本文分析 PoW 区块链协议的安全性。我们首先指出，先前模型所作的假设在现实中未必成立，而攻击者可以利用这一点发起这些模型无法捕捉的攻击。其中包括：(1) 难度交替攻击，在这种攻击下，挖矿算力为 $< \frac{1}{2}$ 的对手也可能实现分叉；(2) 快速分叉攻击；(3) 对自私挖矿攻击的一般性界限；以及 (4) 交易扣留攻击。随后，我们阐述先前的安全分析模型为何无法捕捉这些攻击，并提出一个更实用的安全分析框架——理性协议设计（RPD）。接着，我们提出一个构建 PoW 区块链的框架 **PRAGTHOS**，该框架能够抵御上述攻击。最后，我们论证，在奖励方案满足某些条件时，遵循 **PRAGTHOS** 框架的 PoW 区块链能够抵御计算能力受限的对手。

## 1 引言

区块链技术由中本聪 Nakamoto [2009]通过比特币提出，是中心化金融机构的一种替代方案。区块链是一种不可篡改的分布式账本，能够实现分布式信任。它将数据存储在区块中，并通过特定的密码学链接将区块连接起来，从而确保所有参与者对同一状态（区块的排序）达成共识。Vitalik Buterin 等人 [2013] 提出了以太坊区块链，它支持图灵完备的智能合约功能 Szabo [1997]。此后，区块链技术在多个领域得到了广泛应用，例如金融、供应链、智慧城市和物联网系统、去中心化治理、投票和拍卖系统等。区块链技术通过对系统状态保持分布式信任，并就其达成共识。

FLP不可能性定理（Fischer 等人 [1983]）指出，即使只有一个节点发生故障，确定性算法也无法在异步系统中实现共识。区块链是去中心化系统，利用激励机制工程来克服这些不可能性。它采用工作量证明（PoW）共识算法来确保一致性，并克服分布式系统中原本存在的此类不可能性。在工作量证明中，每个参与节点（矿工）都需要通过查询来解出特定的密码学谜题，以便向区块链写入数据。如果区块的哈希值小于某个设定的目标值，则查询成功。区块链协议之所以能够克服不可能性，是因为：（i）它们是基于激励的协议，会向写入区块的矿工提供奖励；（ii）它们具有非确定性。

随着区块链协议日益普及，研究人员对基于工作量证明的区块链进行了广泛的安全分析 Garay 等人 [2015, 2017], Eyal 和 Sirer [2014]。Badertscher 等人 Badertscher 等人 [2017] 使用通用可组合（*UC*）框架 （由 Canetti Canetti [2001]提出），为比特币提出了一种通用可组合处理。然而，在区块链的安全分析中，我们不仅应考虑密码学

还应考虑博弈论安全性。Garay 等人 Garay 等人 [2013] 提出了理性协议设计（RPD），用于对任意分布式密码协议进行博弈论安全分析。Badertscher 等人 Badertscher 等人 [2018,2021] 修改了 RPD 模型，以便对 PoW 区块链进行博弈论安全分析。关于 PoW 区块链的博弈论安全性，已有大量研究 Judmayer 等人 [2020],Liao 和 Katz [2017a,b],Han 等人 [2021], Tsabary 和 Eyal [2018], Siddiqui 等人 [2020], Chen 等人 [2021], Karakostas 等人 [2022], Azouvi 和 Hicks [2020]。特别是，Badertscher 等人 Badertscher 等人 [2018] 证明，在诚实多数假设下，比特币满足诸如强攻击收益安全性[1] 这类由 Garay 等人 [2013] 提出的强安全性概念。然而，这项研究展示了攻击者即使拥有 $< 50\%$ 的算力，也能利用难度篡改攻击比特币或许多 PoW 区块链。

现有框架之所以能够得出安全性结论，主要是因为它们假设以下一项或多项条件成立：(i) 加密货币兑法定货币的兑换率恒定，(ii) 区块奖励恒定，或 (iii) 难度恒定。现实中，这些都是动态参数。此外，这些研究将矿工划分为诚实方(HP)——诚实地遵循协议，或对抗方(AP)——对协议发起攻击。一些矿工通常会遵循协议，但如果某种策略能够带来更高效用且不会扰乱区块链，他们可能会有条件地偏离协议。我们将这类矿工称为理性方(RP)。本文表明，在 PoW 区块链中存在 RP 时，可能发生多种攻击，而基于 RPD 的模型无法捕捉这些攻击。因此，我们的目标是构建一个实用模型，使其符合现实世界环境，从而对 PoW 区块链进行博弈论安全分析。

**我们的贡献**

本文的贡献有三点。(i) 我们指出现有 PoW 区块链协议中的具体攻击，并解释现有安全模型为何无法捕捉这些攻击。(ii) 我们提出一种新模型——P实用 理性方协议设计 （PRPD (PRPD），以克服现有 PoW 区块链模型的局限性。(iii) 我们提出解决方案以应对已发现的攻击，并提出一种新颖框架 **PRAGTHOS** ，并对符合该框架的 PoW 区块链进行安全分析。

**攻击：**对于 PoW 区块链，我们证明存在此前尚未发现的攻击。此外，对于已知攻击，我们证明，发起现有攻击所需的对抗方算力比例远低于现有界限。

• 我们证明，存在难度篡改，使得拥有 $< \frac{1}{2}$ 的攻击者无需理性参与者的帮助即可成功发动分叉。此前对这一界限的估计为 1 2 （51% 攻击）。由此可推论，即使攻击者控制的挖矿算力仅占 45%，也能在比特币中发动此类攻击（定理 3.1）。

• 我们证明存在一种名为快速分叉的安全攻击，攻击者可利用理性参与者的激励驱动偏离行为（定理3.2）。

• 我们还证明，Eyal 和 Sirer [2014] 提出的自私挖矿界限是一个更一般界限的特例。通过采用我们提出的 PRPD 模型，在自私挖矿攻击结合巨鲸交易 Liao 和 Katz [2017b],时，我们可以刻画这一更一般的界限，并将其称为“带贿赂的自私挖矿”。

• 我们证明，在仅交易费模型（TFOM）2下，存在一种偏离*Gossip* 协议（引理 3.4）的策略，我们称之为交易扣留攻击。这种策略性偏离既可能降低 PoW 区块链的吞吐量，也可能导致协议中心化。

**PRPD：** 我们讨论以往研究为何未能捕捉到这些安全攻击，并作出相应修改，以提出一个更实用的 PoW 区块链协议安全分析模型——PRPD。在该模型中，我们考虑多个挖矿轮次，同时也捕捉系统的动态变化——区块奖励和难度可变。我们还通过外部性（兑换为法定货币时兑换率的变化）来捕捉系统的外部响应，而这些响应取决于矿工所采用的策略。此外，我们在分析中纳入了三类参与者：利他（诚实）参与者、有条件偏离的（理性）参与者，以及偏离的（对抗方）参与者。

**威慑攻击与PRAGTHOS：**为纠正上述安全攻击，我们提出了 PoW 区块链协议应采取的若干修正措施。结合这些修改，我们提出了一种构建 PoW 区块链的新型框架，名为**PRAGTHOS**。

• 我们确定了适当的超参数值，以确保难度调整攻击不可能发生（推论5.1）。

• 我们提出 PC-MOD 作为对 QUICK FORK 攻击的威慑机制。我们证明，只要存在这样一种协议（在发起 QUICK FORK 攻击时运行），就足以阻止该攻击。

[1]参见本文中的定义4.2[2]TFOM 的正式说明
见附录D

• 我们还给出了一个悲观的结果：不存在任何能够抵御自私挖矿、实现攻击收益安全的 PoW 区块链协议（定理 5.2）。

• 我们提出 $\Pi_{tx-inclusion}$ 协议，以确保偏离*Gossip*协议不会带来激励。
• 基于这些修改，我们提出**PRAGTHOS** 并进行安全分析。– 在通胀型区块奖励方案下，我们证明 **PRAGTHOS** 具有强攻击收益安全性（定理 6.1）。– 我们证明，在通缩型区块奖励方案下：(1) 没有任何 PoW 区块链协议对一般对手具有强攻击收益安全性（定理 6.3）。(2)**PRAGTHOS** 能够抵御攻击策略轮次数量有界的对手（定理 6.4）。

借助pRPD 和**PRAGTHOS**，我们得到了重要结果：(i) 即使诚实方占多数，比特币也不安全；(ii) 采用通缩型奖励方案的加密货币不具备强攻击收益安全性。因此，我们认为，这项工作为构建未来的 PoW 区块链协议奠定了基础。

**相关工作**

近年来，已有大量研究对 PoW 区块链协议的密码学安全性和博弈论安全性进行了分析，并发现和讨论了多种攻击。本节将我们的工作与现有攻击及其分析框架进行对比。

**一般安全性**。 Tsabary 和 Eyal 在 Tsabary 和 Eyal [2018] 中指出，如果补贴（交易费与区块奖励的总和）足够低，且挖矿成本足够高，那么矿工挖出区块的时间间隔会拉长。此外，这一间隔会随挖矿池相对规模的变化而变化，并且矿工有动力组成联盟以提高奖励。这意味着，稀疏的交易分布和较低的区块奖励会导致系统中心化。Wei 等人 Wei 等人 [2018] 研究了网络延迟对区块链网络的影响。作者提出了一个更通用的框架来建模网络延迟，其中可能出现较大的延迟，且发生概率不为零。然而，在他们的分析中，对手仅限于实施网络延迟。Gazi 等人 Gazi 等人 [2022] 提出了一种高效方法，可根据计算能力和网络延迟计算 PoW 区块链结算时间的界限。Yuan 等人 Yuan 等人 [2020] 讨论了一个包含 $(1+\mu)$ 名矿工的协议，其中 $\mu$ 名矿工已被攻陷。此外，对手可以在概率为 1 的情况下将网络延迟至多 $\frac{1}{np\Delta}$。在这种情况下，作者讨论了链增长、链质量和共同前缀性质成立的条件[3]。Momeni 等人 Momeni 等人 [2022] 提出了一种基于身份的加密机制，以防止抢先交易。然而，由于该方案所基于的协议依赖于执行共识的委员会成员身份，因此无法有效应用于公有 PoW 区块链。Badertscher 等人 [2017], 、Graf 等人 [2021]等研究对区块链进行了通用可组合处理。Graf 等人 [2021] 讨论的通用密码学安全分析框架适用于一般分布式账本，而我们的工作也分析博弈论安全性。Ke 等人（Ke 等人 [2020]）为区块链遭受严重攻击的情形建模应急计划。他们提出的框架以针对区块链的攻击为输入，并输出应急计划、检测计划和损害程度。他们的工作提出了应急计划框架，并评估给定攻击造成的损害程度；而我们的工作侧重于对系统建模，以涵盖所有可能的攻击，并提出解决这些攻击的框架。

**理性安全性**。Han 等人指出，诚实多数假设并不成立，尤其是对于某些可能成为对手的矿工而言，他们可能会受到激励机制设计的诱导，转而在分叉上工作。作者表明，如果考虑系统中存在多个区块链，那么就存在某些激励结构，可以激励矿工对算力较弱的区块链发起 51% 攻击。他们的工作与我们的不同，因为他们研究的是包含多个区块链的系统。我们讨论了多种攻击，即使在多数矿工诚实的区块链系统中，这些攻击也仍有可能发生。Kevin 和 Katz（Liao 和 Katz[2017b],Liao 和 Katz [2017a]）较早探讨了非对抗性理性参与者可能偏离最长链这一观点。他们通过巨鲸交易发动攻击，即交易手续费异常高的交易。Judmayer 等人（Judmayer 等人 [2020], Han 等人 [2021]）考虑了对手通过智能合约提供外部保证激励，贿赂理性参与者加入攻击的情形——作者将其称为算法激励操纵。我们的模型使用理性参与者来涵盖更大范围的矿工，因为即使没有贿赂，他们也可能偏离。因此，我们的模型更具一般性。另一类攻击发生在区块奖励降至微不足道的程度、矿工激励仅由交易手续费驱动时。现有的大多数研究（Karakostas 等人[2022], Siddiqui 等人 [2020], Möser 和 Böhme [2015], Li 等人 [2018], Houy [2014], Roughgarden [2021] ）要么研究交易提议者基于激励的偏离行为，要么对交易分布作出乐观假设。Badertscher 等人 Badertscher 等人 [2018] 和 Carlsten 等人 Carlsten 等人 [2016] 表明，在

[3]区块链安全性需要具备 3 项属性 ty

一种不利（但同样可能出现）的传入交易分布下，协议并不安全。我们讨论了一种可能的偏离行为，它会在此类交易分布下危及协议，并探讨了如何应对这种偏离行为。

**安全模型。** Badertscher 等人。Badertscher 等人 [2018, 2021] 对比特币进行了 RPD 分析，并研究了 51% 攻击情形下的双重支付。这些研究未能捕捉到使对手能够分叉并进行双重支付的攻击，$\beta_{adv} < \frac{1}{2}$ 而无需借助其他矿工的偏离行为。Badertscher 等人的效用模型 [2018]未能涵盖可变的区块奖励、可变的兑换率以及可变的挖矿成本。作者扩展了 RPD 中的效用模型，以涵盖 Badertscher 等人研究中的可变区块奖励和挖矿成本[2021]。作者认为，由于区块奖励递减，攻击收益—安全性 应仅针对有限时间范围进行考量。由于兑换率（加密货币与法定货币之间的兑换率）也是动态的（取决于参与者的策略以及加密货币的供应量），需要注意的是，这一兑换率可能会上升[4]，，使 Badertscher 等人提出的有限时间范围论证 [2021] 不切实际。另一方面，我们的模型同时涵盖贴现和通缩型区块奖励。因此，我们的结果反映了更真实的系统行为。

## 2 预备知识

本节将介绍本文后续讨论所需的背景知识、符号和形式化方法。

### 2.1 通用可组合性

首先，简要介绍定义 PoW 区块链安全性时所考虑的一组协议。Canetti Canetti[2001] 提出了通用可组合性（UC）框架，随后 Badertscher 等人 [2017] 提出了 PoW 区块链的 UC 分析。与以往工作类似，我们的模型假设所有参与方均为概率多项式时间（PPT）交互式图灵机（ITM）。

#### 2.1.1 $\mathcal{G}_{ledger}$ 理想功能

理想功能是所提出协议旨在实现的功能。PoW 区块链旨在实现 Badertscher 等人 [2017]所描述的$\mathcal{G}_{ledger}$ 功能。该功能存储一个账本，用于维护系统状态；每次状态转换均通过参与方提交的交易完成。不同参与方对状态头的看法可能不同，因此，该功能会根据各参与方分别存储一个指向状态头的指针。VALID-TX 谓词会检查交易的有效性，并在交易有效时将其追加到账本中（执行相应的状态交易）。该谓词确保账本增长性、链质量和交易活性。

#### 2.1.2 $\mathcal{G}_{weak-ledger}$ 宽松功能

放宽理想功能这一概念之所以存在，是因为现实世界中存在多种攻击和其他行为，需要在理想世界中进行模拟。$\mathcal{G}_{ledger}$ 的宽松理想世界功能定义如下：$\mathcal{G}_{weak-ledger}$，见 Badertscher 等人 [2018]。宽松功能将状态存储为一棵树，而非链表，因此可以存在任意长度的分叉；与所有类比特币 PoW 区块链一样，我们从这些分叉中选择最长链。

此外，由于在真实世界中，无法区分区块是由对抗方、理性方还是诚实矿工挖出的，因此该功能放宽了对链质量和链增长属性的检查；这些属性由 StateExtend策略验证。在 $\mathcal{G}_{weak-ledger}$ 中，StateExtend策略被放宽为WeakStateExtend。宽松功能接受状态缓冲区中的所有交易，而不检查它们相对于状态树的有效性，因为这些交易可能在状态树的多条链中的某一条上有效。此外，可以通过 Fork命令创建分叉：该命令从指定区块延伸区块链，而非使用传统的 Next Block命令从调用参与方的头部延伸区块链。（有关 $\mathcal{G}_{ledger}$ 和 $\mathcal{G}_{weak-ledger}$的更多详情，请分别参阅 Badertscher 等人 [2017] 和 Badertscher 等人 [2018]。）

### 2.2 工作量证明区块链协议

PoW 区块链由区块链和基于哈希指针的链表组成。此外，要添加一个区块，我们必须包含其所指向的父区块的哈希，并通过选择一个随机数来解决 PoW谜题，使该区块的哈希

[4]从比特币和以太坊的历史价格中可以明显看出 es

小于目标值。目标值越低，谜题的难度越高。我们将 UC实现（参见定义 20，Canetti [2001]）宽松理想功能的 PoW 区块链表示为 $\Pi$。

令 $C_i^{\lfloor k}$ 为区块链 $C_i$中除最后 $k$ 个区块外的所有区块所构成的子集。我们考虑对 $G_{ledger}$理想功能作进一步且实用的放宽，即采用可变难度。不同区块链上挖出区块的概率可能因区块链的难度而异。任何 $C_i$ 上挖出区块的难度都是公开已知的，因为可以根据公开可用的账本计算得出。Badertscher 等人 [2017],在第 5.1 节中定义的子协议 $isValidStruct(C)$，将作为输入给出的区块链所对应的难度参数作为输入，而非系统参数。系统通过奖励矿工区块奖励，鼓励他们通过解答 PoW 谜题来维护账本。

### 2.2.1 账本

账本包含矿工挖出的区块。区块 $b = (h_{parent},\ nonce,\ txMD,\ \{0,1\}^*)$ 包含：(i) 指向父区块 $h_{parent}$的哈希指针，(ii) 随机 nonce $nonce$，以及 (iii) 将纳入其中的交易集合的元数据。该元数据取决于区块链实现的具体细节。例如，它包括包含一组交易的默克尔树的根，而这些交易也包括比特币中的 coinbase 交易[5] Nakamoto [2009]。此外，合约还可以任意二进制字符串的形式包含其他信息，以便在账本中启用额外功能。

### 2.2.2 时间步

由于系统中没有全局时钟（系统运行于部分同步设置中，Dwork等人 [1984]），我们无法按时间来衡量事件。因此，我们采用轮次的概念，它取决于系统计算出的哈希数量。

**定义 2.1**（轮次）。 一个轮次 是指任何矿工进行 $q$ 次查询[6]所需的持续时间。

除了轮次，我们还定义纪元 来表示挖矿难度发生变化的事件，并定义阶段 来表示区块奖励发生变化（例如，在比特币中，奖励每挖出 210,000 个区块就减半）。

**定义 2.2**（纪元）。 一个纪元 是指系统以恒定难度挖出 $\lambda$ 个区块的持续时间。在一个纪元结束时，难度会按 $\tau$ 进行缩放，持续 $\tau \in [\tau_{min}, \tau_{max}]$。

**定义 2.3**（阶段）。 一个阶段 是指系统挖出 $\Lambda$ 个区块的持续时间。在一个阶段结束时 $j$，区块奖励会根据更新规则 $r_{block}^{new} \leftarrow \varrho(r_{block}^{old}, j)$[7] 针对某个 $\varrho$ 进行更新：$\mathbb{R} \times \mathbb{N} \to \mathbb{R}$

该协议 执行过程由每轮参与的不同参与方组成，其角色说明如下 .

### 2.2.3 参与方

基于工作量证明的区块链包含三类参与方——利他（诚实）方、对抗方和理性方。每类参与方由一组行为相同的矿工组成。为了对市场响应进行建模，我们在表述中引入一个虚拟的被动参与方，即外部观察者。

**外部观察者（EO）**负责观察区块链上的公开链。我们假设存在一个容忍因子 $\rho$，以考虑网络延迟和意外分叉。也就是说，EO 只有在此前存在另一条领先了 $\rho$ 个区块的链 $C_h$，并最终被 $C_f$ 超越 $C_f$ $C_h$ 时，才会将分叉链 $C_f$ 视为分叉（安全性）攻击。在本研究中，我们对一轮内可能发生的剧烈兑换率变化进行建模，而非对我们观察到的缓慢变化进行建模。在第 $t$ 轮，EO 向参与方发送信号 $\theta(t)$。如果 $\theta(t) = 1$，则意味着兑换率没有发生重大波动。

$$\theta(t) = \begin{cases} 1 & \text{if all follow protocol honestly} \\ e_{fairness} & \text{if fairness attacks} \\ e_{security} & \text{if security attacks} \end{cases} \tag{1}$$

1 **诚实参与方(诚实参与者):** 这些矿工控制着总挖矿算力的 $\beta_{hon}$。如果参与有利可图，诚实参与者就会遵循 PoW 区块链协议，诚实地参与系统；否则，他们不会参与。

[5]比特币向矿工支付区块奖励的机制[6]在 PoW 区块链中，这些是哈希查询[7]对于比特币而言 $\varrho(r_{block}^{old},\ j) = \frac{r_{block}^{old}}{2}$ ——

2 **对抗方(攻击者):** 这些矿工控制着总挖矿算力的 $\beta_{adv}$。对抗性矿工会发起攻击，并偏离诚实协议。他们通过加密货币以及卖空[8]获得收益。因此， $\theta(t)$的变化对攻击者而言无关紧要。

3 **理性方(RP):** 这些矿工控制着总挖矿算力的 $\beta_{rat}$ 比例，并遵循协议——Π 除非存在效用更高的偏离。然而，只有当该偏离不可能成为被 EO 观察到的安全攻击时，该参与方才会偏离，即可以保证偏离后 $\theta(t) \neq e_{security}$。

请注意，我们认为所有矿工的计算能力都受限，并且拥有固定的算力。不过，如果单个参与者提高其挖矿算力，我们将其视为多个矿工（不失一般性）；每个矿工在一轮中进行 $q$次查询。

接下来，我们将解释 EO 在建模市场响应、兑换率等方面所发挥的作用。

#### 2.2.4 建模外部性

在 PRPD 中，外部性在对理性参与者的行为进行建模时发挥着重要作用。Badertscher 等人 Badertscher 等人 [2018] 为协议描述符指定了一个极高的负收益（其数值随安全因子的多对数呈指数增长），以此建模对协议（或加密货币价值）的影响。在我们的情形中，我们定义了术语 $\theta(t)$，它会根据矿工采取的策略改变加密货币价值，具体以 EO 观察到的情况为准——若出现偏离，价值便会降至 $< 1$。如果以加密货币计的收益为 $\mathcal{R}$，那么实际收益就是 $\theta(t)CR\mathcal{R}$。我们通过 $\theta(t)$ 建模市场对不同策略的响应，并通过 $CR$ 处理供需波动。我们将针对区块链系统的攻击分为两类。

1 **公平性攻击** 会损害公平性，例如某些矿工获得的奖励超过其公平份额，或某些用户需要等待异常长的时间才能让交易被接受。在这些攻击中，安全性仍然完好。我们假设，如果 EO 观察到此类攻击，则 $\theta(t) = e_{fairness} < 1$。

2 **安全攻击** 是指协议的安全性遭到破坏。在这种情况下，外部性参数 $\theta(t)$ $= e_{security}$[9]。
例如，安全威胁可以建模为 $e_{security} = negl(\kappa)$。在这种情况下，$e_{security} = \frac{1}{poly(\kappa)}$。

### 2.3 PoW 区块链中现有的攻击

已有多种针对 PoW 区块链的攻击被提出：Eyal 和 Sirer [2014], Liao 和 Katz [2017a,b], Eskandari 等人 [2019],Breidenbach 等人 [2018], Kalodner 等人 [2015]。我们列举了此前发现且与本研究相关的攻击。

#### 2.3.1 自私挖矿

自私挖矿 是 Eyal 和 Sirer 提出的一种攻击 Eyal 和 Sirer [2014]。在这种攻击中，对于任意一段连续挖出的区块，对手获得的区块奖励总额占比高于其所持有的总挖矿算力占比。因此，这是一种针对系统公平性的攻击，而非安全攻击。然而，Eyal 和 Sirer [2014] 的作者表明，经过一定修改后，只有拥有 $\geq \frac{1}{4}$ 挖矿算力的对手才能成功发动自私挖矿攻击。

**命题2.1** (Eyal 和 Sirer [2014], 观察1)。 对于给定的 $\gamma$，规模为 $\beta_{adv}$ 的对手矿池在以下范围内获得的收益高于其相对规模： $\beta_{adv}$

$$\frac{1-\gamma}{3-\gamma} < \beta_{adv} < \frac{1}{2} \tag{2}$$

其中， $\gamma$ 是非对手方的比例：当两个区块竞争最长链时，这些参与方会在对手区块之上进行挖矿。

Carlsten 等人 Carlsten 等人 [2016]讨论了对手即使拥有任意低的挖矿算力，自私挖矿也可能获利的可能性。他们的结论仅适用于仅交易费模型（TFOM——区块奖励可以忽略不计），并且依赖于奖励的非均匀性。我们的工作提出，在存在 RP 的情况下，即使挖矿算力任意低的对手也可能受到激励而发起自私挖矿攻击；当区块奖励显著时，这种情况也是可能的。

[8]卖空是股票交易中的常用术语；卖方出售其并不拥有的股票（在此处指加密货币），并在未来以更低的价格回购。

[9]$e_{fairness} >> e_{security}$ 因为安全攻击会构成更严重的威胁。

### 2.3.2 分叉攻击

分叉攻击是针对 PoW 区块链的一种安全攻击。如果区块链 $C_A$ 在某个时刻被超越区块链 $C_H$，那么我们称之为分叉攻击，条件是：(1) 在某个时刻 $t_1$, $length(C_H - C_A) \geq k$ （其中 $k$ 是 PoW 区块链[10]设定的参数）；(2)$C_A$ 在某个时刻 $t_2 > t_1$超越了 $C_H$。此类攻击可能导致双重支付，因此是区块链面临的严重安全威胁。

### 2.3.3 时间扭曲攻击

存在多种对抗性操纵，例如 Friedenbach 的时间扭曲攻击 [2018]，该攻击通过错误地标记时间戳来降低挖矿难度。然而，只有当对手掌握 $> 51\%$ 的挖矿算力时，时间扭曲攻击才可行。每轮都进行难度重新计算的 PoW 区块链（如 Shirah 的 Verge [2008]）会面临安全威胁。然而，在诚实多数的情况下，比特币等 PoW 区块链能够抵御时间扭曲攻击。相比之下，即使多数参与者是诚实的，比特币及类似区块链仍可能遭受难度篡改攻击（第 3.1 节）。

### 2.3.4 抢先交易攻击

我们假设存在一类特殊的对抗方 PPT 交互式图灵机 $\mathcal{A}^*_{fr}$ ——抢先交易对手，最初由 Badertscher 等人定义 [2018]

**定义 2.4**（抢先交易，定义 2，Badertscher 等人 [2018]）。若对手 $A \in \mathcal{A}^*_{fr}$ 满足以下条件，则称其为抢先交易对手：

1. 收到参与方发出的广播消息后，它最多可以将其延迟一轮。
2. 对手发出的任何广播消息都会立即在网络中传播 y.

在这种对手的存在下，会出现 Eskandari 等人 [2019]、Breidenbach 等人 [2018]、、Kalodner 等人 [2015] 讨论过的攻击，例如（1）置换攻击和（2）插入攻击。不过，对我们而言，定义 2.4 才是关注重点。

### 2.4 理性方协议设计

Garay 等人的理性协议设计（RPD）是多种 PoW 区块链协议安全分析模型的基础，其中包括 Badertscher 等人的模型。我们的工作以 RPD 为基础，并针对 PoW 区块链协议对其进行修改，使其成为一种更实用的博弈论安全分析模型。

RPD 将安全性建模为两个参与者之间的博弈：（1）协议描述者（PD），负责提出实现宽松功能的协议；（2）对手，在 PD 选定协议后选择攻击策略。该博弈被建模为一个具有完全信息和有限时间范围（两步）的双人博弈——即斯塔克尔伯格博弈。RPD 对偏离行为的参与者（对手）和不偏离行为的参与者（利他者）进行建模。

Badertscher 等人对 RPD 协议进行了修改，使其适用于 PoW 区块链。该协议刻画了协议在各轮中的偏离行为。然而，这一模型未能刻画系统的动态特性，例如可由对手策略性操纵的可变挖矿难度（如第 3.1 节所示）、可变区块奖励等。此外，该博弈将偏离行为的参与者（对抗方）和不偏离行为的参与者（利他者）纳入模型，但未能刻画有条件偏离的（理性）参与者。我们旨在引入一种实用理性协议设计模型（PRPD，第4节），以对这类情形进行建模。

## 3 PoW 区块链攻击

Garay 等人 [2013], Badertscher 等人 [2018], Karakostas 等人 [2022]提出的先前安全分析模型都是很好的贡献。不过，这些分析仅限于固定难度、有限时域、固定区块奖励、固定兑换率和单一挖矿轮次。在实际场景中，这些因素都是动态变化的，对手可以利用它们发动攻击。本节将讨论我们发现的、先前研究未能涵盖的基于工作量证明的区块链攻击。我们还将探讨先前研究未能涵盖这些攻击的原因。
我们将这些攻击分为三类：(i) 拜占庭 对手攻击——这是最严重的一类攻击，拜占庭对手可以凭借 $\beta_a < \frac{1}{2}$ 单独发起攻击。(ii) 理性方-拜占庭 攻击——在这类攻击中，

[10]针对比特币 $k = 6$

拜占庭对手依靠理性参与者成功发起攻击。(iii) 理性方 攻击——理性方偏离原始协议 Π。这些攻击不涉及拜占庭对手。

### 3.1 拜占庭对手攻击

我们发现，拜占庭对手可以发起分叉攻击并进行双重支付。此前人们认为，如果 $\beta_a < \frac{1}{2}$，那么对于合理的区块确认时间，该协议能够以极高的概率抵御此类双重支付攻击。然而，我们表明，即使区块确认时间非常宽松，也存在一种对抗方攻击，能够以极高的概率造成分叉，即使对于 $\beta_a < \frac{1}{2}$ 也是如此。

#### 3.1.1 难度调整攻击

难度篡改发生在连续的两个纪元 $e_i$ 和 $e_{i+1}$ 中。在纪元 $e_i$ 中，攻击者降低其表观挖矿速率。这使得攻击者能够在纪元 $e_{i+1}$ 难度重新计算后，于 $C_A$ 上挖出难度值更低的区块，并超过 $C_H$。请注意，在此攻击中，攻击者在 $C_A$ 上挖矿，而诚实参与者和理性参与者则在 $C_H$ 上挖矿。

**攻击策略**。在 $e_i$，攻击者会对区块链进行分叉，形成私有链 $C_A$，此时 $r_1$ 的比例的 $e_i$ 已完成（即已挖出 $r_1\lambda$ 个区块）。攻击者创建带有特定时间戳的区块，使目标值重新计算后， $C_A$ 在下一个纪元 $e_{i+1}$的难度极低。因此，攻击者挖出区块的速度可以快于诚实参与者和理性参与者，并超越 $C_H$，成为最长链。当 $r_2$（$\in (0,1]$）占纪元 $e_{i+1}$ 中区块总数的比例（即 $r_2\lambda$个区块））被挖出时， $C_A$ 将超越 $C_H$。

请注意，攻击者不需要以较慢的速度挖出区块。他们只需设置时间戳，使区块公开后看起来像是挖得较慢。此外，广播区块的时间戳必须为 $<$广播时间。因此，尽管攻击者在纪元 $e_i$ 挖出区块的速度慢于诚实参与方（因为 $\beta_a < \frac{1}{2}$），但由于私有链难度降低，它挖出纪元 $e_{i+1}$ 剩余区块的速度会快于诚实参与者和理性参与者。

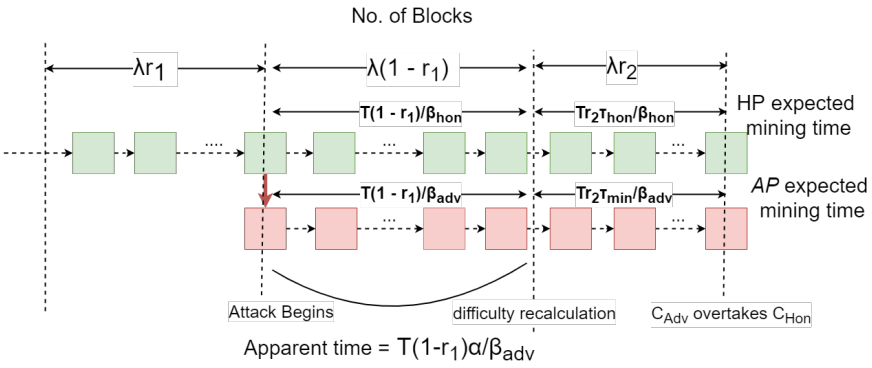


图1：难度调整攻击

**分析**。 设 $T$ 为所有参与方都在 $C_H$上挖矿时，挖出纪元 $e_i$ 的 $\lambda$ 个区块所需的时间。若发起难度篡改攻击，设 $\tau_{hon}$ 为 $C_H$ 的难度调整， $tau_{adv}$ 为 $C_A$的难度调整。若在难度重新计算后发起难度篡改攻击，在纪元 $e_{i+1}$中，$T\tau_{hon}$ 为在区块链 $C_H$ 上挖出所有区块所需的时间， $T\tau_{adv}$ 为在区块链 $C_A$上挖矿所需的时间。请注意，在此攻击中， $1-\beta_a$ 的算力在 $C_H$ 上挖矿，而 $\beta_a$ 的算力在 $C_A$上挖矿。因此，所有预期所需时间都需要相应地进行归一化。

The $C_A$ 完成 $e_{i+1}$ 纪元中 $r_2$ 比例部分所需的总时间应为 $< C_H$，由此得到 u s

$$\frac{T\tau_h r_2}{1-\beta_a} + \frac{T(1-r_1)}{1-\beta_a} > \frac{T(1-r_1)}{\beta_a} + \frac{Tr_2\tau_{adv}}{\beta_a} \tag{3}$$

在上述方程中，对手将 $C_A$ 上的表观挖矿速率降低了 $\alpha$ （$> 1$）倍。因此，$\tau_{adv}$ 和 $\tau_{hon}$ 的计算方式如下：

$$\tau_{adv} = max\left(\frac{1}{r_1 + \frac{\alpha(1-r_1)}{\beta_a}}, \tau_{min}\right) \qquad \tau_{hon} = max\left(\frac{1}{r_1 + \frac{(1-r_1)}{1-\beta_a}}, \tau_{min}\right)$$

**定理 3.1** (DIFFICULTY ALTERING 攻击)**：** 当 $\tau_{min} < \frac{1}{2}$ 时，对手可以使用DIFFICULTY ALTERING 攻击，以概率 $> 1 - negl(\Theta\varepsilon)$ 对 *PoW* 区块链发起分叉，条件是 $\beta_a \geq \beta_a$。

*(i)* 任一参与方挖掘一个区块的预期时间为 $\propto \Theta$,
*(ii)* $2\varepsilon$ 是以下两者之间的时间差：对手与理性参与者挖出纪元 $e_{i+1}$的最后一个区块,
以及 *(iii)* $\beta_a = \frac{(3+\tau_{min}) - \sqrt{(3+\tau_{min})^2 - 4(\tau_{min}+1)}}{2}$

证明。 证明分为三个步骤。在步骤 1 中，我们陈述对手为最大化其效用所设定的环境。在步骤 2 中，我们确定对手发起攻击所需的算力比例，并在步骤 3 中以压倒性概率对其进行量化。完整证明见附录 A.1。 □

**推论 3.1** (比特币难度调整攻击)。 比特币无法抵御针对难度调整的攻击，其概率为$\beta_a > 0.4457$。

该结果可通过代入比特币中所使用的 $\tau_{min} = \frac{1}{4}$ 值得到。此前，人们认为比特币能够以较高概率抵御分叉，即使对于 $\beta_a < \frac{1}{2}$ 也是如此；然而，我们由此表明，即使对于$0.4457 < \beta_a < \frac{1}{2}$，分叉也是可能的。有人可能会认为，由于这会损害安全性，该攻击会降低货币价格，并且$\theta = e_{security}$ 在该攻击之后。因此，AP 从加密货币中获得的任何利润都会被浪费。然而，AP 可以通过持有该代币的空头头寸获利。我们将在附录 D.3 中详细解释这种激励操纵。

### 3.2 理性拜占庭攻击

理性拜占庭攻击是指攻击者发起攻击，并依赖理性参与者偏离协议，使攻击得以成功。我们讨论两种攻击：（i）快速分叉——对安全性的威胁；（ii）带贿赂的自私挖矿——对协议公平性的威胁。

#### 3.2.1 快速分叉攻击

在快速分叉中，对手会在最长链的最新区块之前 $k(< \rho)$ 个区块处创建一条分叉。如果外部观察者没有将该分叉视为攻击，理性参与者就会受到激励，在这条分叉链上挖矿，以获得更高的期望收益。由于诚实参与者继续在 $C_H$ 上挖矿，偏离协议的参与方会获得更大份额的奖励。Liao 和 Katz [2017a,b] 讨论的攻击与快速分叉不同，因为快速分叉不需要异常庞大的交易来促使理性参与者偏离协议。外部观察者无法观察到快速分叉，而前述攻击则很容易被外部观察者发现[11]。

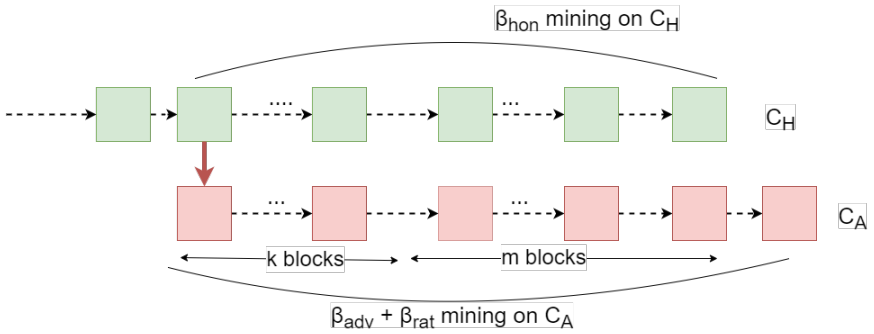


图 2：成功的快速分叉攻击

**攻击策略**。 设 $C_H$ 为诚实链， $C_A$ 为分叉链。要发起此攻击，对手必须确保在任何时候， $C_H$ 领先 $C_A$的区块数都不超过 $\rho$，其中 $\rho$ 是 EO 的容忍因子 。这可确保 EO 不会将该分叉视为攻击，从而激励 RP 在分叉链上挖矿，因为他们可能比在 $C_H$上挖矿获得更多区块奖励。

**定义 3.1**（快速分叉）。如果对手成功分叉了诚实链——即在距最长链最新区块 $k < \rho$ 个区块之前分叉，并创建 $C_A$，且 (ii) $C_A$ 成为最长链，同时 (iii) 攻击期间 $C_H$ 与 $C_A$ 的差距不超过 $> \rho$ 个区块——则称对手成功发起了快速分叉。

[11]例如：交易 – cc455ae 816e6cdafdb58d54e35d4f46d860047458eacf1c740 5dc634631c570d

如果 $k \geq \rho$，理性参与者不会在分叉链 $C_A$ 上挖矿，因为 EO 会将 $C_A$ 视为攻击，兑换率 $\theta(t)$ 会降至 $e_{security}$。因此，理性参与者不会转向 $C_A$，后者也就无法超越 $C_H$。因此，只有在距离最长链末端 $k < \rho$ 个区块以内，快速分叉才有可能发生。

**分析**。我们证明，QUICK FORK攻击策略对 II 的攻击者和理性参与者占优。我们还证明了在何种条件下，QUICK FORK攻击能够以高概率成功。

**定理3.2**（QUICK FORK 攻击)。对手以 $\frac{n-1}{n}$ 的概率成功发动QUICK FORK —— *if*

- $\eta > \frac{n-\beta_h n-1}{n\beta_h-1}$
- $\beta_a + \beta_r \geq \frac{1}{2}$
- $\beta_h > \frac{\chi}{r_{block}}$
- $k < \rho - \varpi$

系统挖出一个区块所付出的成本为 $\chi_1$。$r_{block}$ 是当前阶段的区块奖励 $P_i$ 和$\eta = \frac{r_{block}}{\chi_1}$、$\phi = \frac{\beta_h}{\beta_a+\beta_r}$ 以及 $\varpi = log_{\phi}(\frac{1+(n-1)\phi^{\rho}}{n})$

证明。在证明中，我们比较 RP 遵循协议与偏离协议时的收益，比较范围从区块链的 $C_H$ state 开始，即从分叉发生时起，直到 $C_A$ 超过 $C_H$为止。证明分为四个步骤。在步骤 1 中，我们计算偏离协议时的收益；在步骤 2 中，我们计算遵循协议时的收益。在步骤 3 中，我们比较步骤 1 和步骤 2 的结果，并给出使 QUICK FORK 可行的条件。在步骤 4 中，我们论证攻击成功的概率。完整证明见附录A.2。 □

### 3.2.2 带贿赂攻击的自私挖矿

Eyal 和 Sirer Eyal 和 Sirer [2014], 证明，当算力为 $\frac{1}{4}$（即 $\beta_a = 0.25$ 或更高）时，攻击 自私挖矿 （见第 2.3.1 节所述）是可行的。在该攻击中，攻击者挖出区块后不向网络公布（称为私有链），并在适当时机公布其私有链（更多详情请参见 Eyal 和 Sirer [2014] ），从而获得超过其公平份额的奖励，导致 $\theta(t) = e_{fairness}$。作者假设所有矿工要么属于攻击者（即发起自私挖矿攻击的矿池成员），要么属于诚实参与者。在我们的模型中，矿工可以属于攻击者、理性参与者或诚实参与者。对于这种更符合现实的场景，我们证明，即使 $\beta_a < \frac{1}{4}$，攻击仍然可能成功。其核心直觉是，对手可以贿赂理性参与者，使其转而支持自己的区块链（$C_A$），从而提高攻击成功的概率。总之，Eyal 和 Sirer [2014] 中的 $\frac{1}{4}$ 界，是关于 $\beta_a$（定理 3.3）可行性的更一般界限的特例。

因此，我们的贡献在于说明：如果考虑由诚实参与者、攻击者和理性参与者组成的系统，那么在自私挖矿中引入贿赂后，自私挖矿的界限实际上会更具一般性。

**攻击策略**。攻击模型与 Eyal 和 Sirer [2014] 所讨论的模型相似。唯一的区别是，攻击者每挖出一个区块（并将其私下保留），都会在其中加入一笔贿赂交易[12]。Eyal 和 Sirer [2014] 提出的修改后的协议要求参与方随机选择一个竞争区块，并在所选区块之上继续挖矿。其他参与方和外部观察者都无法得知这一选择。因此，理性参与者可以选择在对抗区块之上挖矿以获取贿赂，而不让外部观察者察觉这一偏离行为。

**分析**。在非对抗区块之上挖矿的总算力为 $\frac{\beta_h}{2}$（因为诚实参与者中的每个矿工都会随机选择 $C_H$ 或 $C_A$ 之一进行挖矿），而在对抗区块之上挖矿的总算力为 $\frac{\beta_h}{2} + \beta_r + \beta_a$。因此，这条区块链赢得竞赛（即区块被挖出）的概率更高，为 $\frac{\beta_h}{2} + \beta_r + \beta_a$。分析得出定理 3.3，该定理的证明见附录 A.3。

**定理 3.3**(带贿赂的自私挖矿 攻击)。攻击策略 带贿赂的自私挖矿 *i* *s* 优于 *Ho* *nest* 协议的

$$\beta_a > \underline{\beta}^{SMB} = \frac{\beta_h}{2\beta_r + 4\beta_h} \tag{4}$$

此处 $\underline{\beta}^{SMB}$ 是使带贿赂的自私挖矿攻击有利可图的 $\beta_a$ 下界 *e.*

由定理 3.3，我们推导出带贿赂的自私挖矿攻击的界限：$\beta_a$ 情况 1：（完全理性设置）在此，$\beta_h = 0$，因此 $\gamma = 1$。该攻击有利可图 对于 $\beta_a > 0$。

[12]很容易获得 挖出对抗方 区块。

情况 2：（混合设置）在此设置下 $\beta_h > 0$，因此，当该攻击对攻击者可行时，界限变为$\beta_a > \beta^{SMB}$。

通过简单分析，我们可知 $\beta^{SMB} \leq \frac{1}{4}$（当 $\beta_r = 0$ 时取等号）。然而，实际的 $\beta^{SMB}$ 可能小得多，具体取决于 $\beta_r$。分析的要点在于，即使存在理性参与方，自私挖矿所需的算力也远低于此前已知的 25% 界限。

### 3.3 理性攻击

理性攻击是对原始协议 $\Pi$ 或其某个子程序 $\Pi$ 的偏离行为。在这种情况下，每个理性代理都会偏离协议，且不存在对手。我们讨论一种对 $\Pi$ 的 *Gossip* 子协议的此类偏离行为，即交易扣留攻击。

#### 3.3.1 交易扣留攻击（$\sigma_{tw}$

矿工收到一笔交易后，会将其添加到内存池并与对等节点共享，这是 Gossip 协议的预期行为 $\Pi_{Gossip}$。在区块奖励模型（BRM）中，理性参与方几乎没有动机偏离$\Pi_{Gossip}$。而在仅交易费模型中，这类偏离行为会受到激励，正如 Badertscher 等人 [2018] 的定理 6 所示。我们展示了这样一种偏离行为——交易扣留攻击（表示为 $\sigma_{tw}$），如引理 3.4 所示，它优于$\Pi_{Gossip}$。

**引理 3.4.** 在 *TFOM* 中，对于任何理性方，以下 $\sigma_{tw}$ 严格优于 $\Pi_{Gossip}$。

证明。 我们首先计算理性参与方在以下 $\Pi_{Gossip}$ 中的收益，以证明这一点。然后计算其在以下 $\sigma_{tw}$ 中的收益，并证明后者严格高于前者。完整证明见附录 A.4。 □

这种偏离行为会带来以下两种可能威胁之一（或两者兼有）：

✠ 低吞吐量：单个理性参与者挖出区块的概率极低；因此，交易需要很长时间才能被区块链接受，从而降低了吞吐量。

✠ 中心化：如果交易提议者将交易发送给大型矿池，希望交易能尽快发布，那么协议就会变得中心化。

**以往的框架有哪些不足?**

我们讨论了 PoW 区块链中的四种可能攻击。下面将讨论以往的模型（尤其是理性协议设计（RPD））为何无法捕捉这些偏离行为。以往的研究未能捕捉到三项属性，以下将对此进行讨论。

#### 3.3.2 智能体建模

有些矿工可能是理性的，即他们希望在不破坏协议的前提下最大化自身效用。在 Badertscher 等人的工作中，[2018], 协议描述符的效用由诚实矿工的效用，以及针对分叉等事件的极高负收益组成（$exp(polylog(\kappa))$）。它未能体现协议描述符的目标——最大化遵循协议的参与方与偏离协议的参与方之间的差异。因此，RPD 无法捕捉第3.2节中讨论的偏离行为。

#### 3.3.3 外部性

在 RPD 中，底层加密货币兑换为法定货币的兑换率被视为常数。然而，由于安全性攻击造成的效用损失，应通过改变外部性来计算，这会影响 $\theta(t)$。对这种外部性建模，可以量化攻击者和理性参与者偏离协议时的效用损失。

#### 3.3.4 系统动态

RPD 及其衍生模型未考虑 (i) 区块奖励随时间变化，以及 (ii) 挖矿难度可变。因此，先前的模型无法捕捉第 3.1 节讨论的攻击。

# 4 面向区块链的 PRPD

本节将介绍实用理性协议设计（PRPD]），这是一种改进的 PoW 区块链博弈论安全分析模型。pRPD 将区块链建模为协议描述符与对手之间的双人斯塔克尔伯格博弈。

## 4.1 参与者

存在 在将协议建模为博弈时，有两个参与者：(i) 协议描述符和 (ii) 攻击者 .

• **协议描述者（PD）**：协议描述者是选择协议 $\Pi$ 的参与者，该协议将被视为诚实协议。PD 必须确保：(i) 放宽的理想功能 $\mathcal{G}_{weak-ledger}$ 由该功能实现；(ii) 该协议能为其带来最大效用。

• **对抗方（攻击者）：** 我们采用 AP 这一记法，既指对抗性矿工集合，也指参与双人博弈的对手。这是因为，对抗性矿工集合由一个概率多项式时间交互式图灵机 $\mathcal{A}$ 控制，该图灵机执行对抗策略。这个 $\mathcal{A}$ 根据给定的协议 $\Pi$ 决定对抗策略，因而就是本博弈中的 AP。

## 4.2 攻击模型

正如 Garay 等人 [2013], 和 Badertscher 等人 [2018], 所定义的那样，我们需要定义一种攻击模型，以便对协议的安全性进行博弈论分析。攻击模型由元组 ($\mathcal{F}$，$<\mathcal{F}>$，$v_A$，$v_D$) 参数化。其中，$\mathcal{F}$ 是该协议希望在真实世界中实现的理想功能。$<\mathcal{F}>$ 是对理想功能的放宽。对于 PoW 区块链协议，$\mathcal{G}_{ledger}$ 是理想功能，而 $\mathcal{G}_{weak-ledger}$ 功能则是对它的放宽。

此外，$v$ 是 $v$：$\mathcal{S}\times\mathcal{Z}\longrightarrow\mathbf{R}$ 从模拟器映射而来，用于在环境$\mathcal{Z}$ 中模拟针对协议 Π的攻击策略 $\mathcal{A}$，映射到实值收益。效用定义为关于该收益函数的期望。在我们的情形中，三类参与方 HP、RP 和 AP 的收益向量分别为 $v_H$、$v_R$和 $v_A$。因此，我们的攻击模型为

$$\mathcal{M}=(\mathcal{G}_{ledger},\mathcal{G}_{weak-ledger},v_A,v_R,v_H)$$

## 4.3 博弈

通常，区块链系统由两类参与者组成：(i) 协议描述符和 (ii) 矿工——我们将每类矿工称为参与方（已在第 2.2.3节中描述）。此外，我们假设存在一名外部观察者，其不属于该博弈。博弈过程如下：

❒ 协议描述符定义协议。其职责是选择能够最大化自身效用（并且按照设计，也最大化遵循该协议的参与者的效用）的最佳协议 Π Π。❒ AP 观察 Π，并针对所选择的 Π选择一种由任意 ITM $\mathcal{A}\in\mathcal{C}_A$ 实现的攻击策略。

我们将对手方与系统之间的交互建模为协议描述符与对手之间的双人斯塔克尔伯格博弈，其中协议描述符是博弈的领导者，攻击者是跟随者。在系统中，外部观察者决定兑换率 $\theta(t)$——即在第 $t$ 轮，单位底层加密货币兑换法定货币的价格。我们的博弈 $\mathcal{G}_{\mathcal{M}}$ 定义在攻击模型 $\mathcal{M}=(\mathcal{G}_{ledger}$，$\mathcal{G}_{weak-ledger}$，$v_H$，$v_R$，$v_A)$ 上。理性参与者和诚实参与者不属于斯塔克尔伯格博弈：协议描述符行动时，诚实参与者的策略是固定的 $\Pi$；而攻击者选定策略后，理性参与者会从所有可能的偏离行为中采取最优策略。

### 4.3.1 安全性定义

与 Badertscher 等人 [2018, 2021] 类似，我们将对手在实践中能够实现的“最佳可能行为”称为半诚实抢先交易策略。半诚实抢先交易对手 $A_{fr}$ 是抢先交易对手 $A^*_{fr}$ 的子集。

**定义 4.1**（抢先交易半诚实对手（定义 2，Badertscher 等人 [2018]））。对手 $\mathcal{A}$ 若属于对手集合 $\mathcal{A}_{fr}$，则称其为半诚实抢先交易对手，当且仅当

• 激活后，对手腐化矿工并遵循 Π （诚实协议）。

• 对手想要广播的任何消息，都会立即广播

• 如果非对抗方　　参与方想要广播消息时，对手会将该消息最多延迟一个轮次　　.

既然我们已经定义了期望实现的对手行为，接下来便定义协议所能达到的最强安全保证：强攻击收益安全性。我们参考 Badertscher 等人 [2018]，阐述强攻击收益安全性的定义。

**定义 4.2**（强攻击收益安全（定义 3，Badertscher 等人 [2018]））。若对于半诚实、抢先交易对手 $A \in \mathcal{A}_{fr}$这一集合中的某个对手，攻击者采用 $A$ 时是近似最佳响应策略，则协议 Π 在攻击模型 $\mathcal{M}$ 下具有强攻击收益安全性。这意味着，$\forall A_2 \in$ PPT ITM 和 $A_1 \in \mathcal{A}_{fr}$,

$$U_A(\Pi, A_2) \leq U_A(\Pi, A_1) + negl(\kappa)$$

### 4.4 效用

为计算效用，我们为每个 $\mathcal{A}$、$\mathcal{R}$ 和 $\mathcal{H}$ 的收益定义随机变量。随机变量 $v_{\mathcal{X}}$ for$\mathcal{X} \in \{\mathcal{A}, \mathcal{R}, \mathcal{H}\}$ 定义在环境 $\mathcal{Z}$ 上。按照通用可组合范式，由于该博弈是斯塔克尔伯格博弈，假设协议描述符选择策略 Π，而攻击者选择 $\mathcal{A} = A(\Pi)$。在这种情况下，令 $\mathcal{S}$ 为 $\mathcal{A}(\Pi)$ 的理想世界模拟器，其中 $\mathcal{S}$ 对 $< \mathcal{F} >$发起攻击。所有此类模拟器的集合为 $\mathcal{C}_A$。

#### 4.4.1 模型的目标

攻击者的目标是为自身获取更多收益。此外，我们注意到，对于攻击者和外部观察者（两者均为 PPT 交互式图灵机）而言，诚实参与者与理性参与者彼此不可区分。因此，协议描述符的目标是为诚实参与者和理性参与者争取更多收益，同时减少攻击者的收益。请注意，效用模型正是在这一点上有别于大多数先前的研究。它还通过考量协议参数不断变化时不同轮次中的收益，捕捉协议的动态特性。

以往的效用模型只涵盖了能使对手获益的偏离行为。然而，从长远来看，攻击者可以通过降低诚实参与者的收益来获得更高效用。我们在附录 D.2 中详细说明了这一点。因而，协议描述符的收益是未偏离的参与方（即诚实参与者和理性参与者，外部观察者看来如此）的收益与偏离的参与方（即攻击者）的收益之差。与 RPD 的另一项区别在于，矿工收益中的外部性建模方式。在我们的工作中，我们通过外部性（由兑换率 $\theta(t)$ 体现）来计入严重的安全威胁和中等程度的公平性威胁。这一项会降低攻击者和协议描述符的收益。不过，如果攻击者持有针对该加密货币的空头头寸，其收益可能会上升。为对此类情况建模，在计算 $U_A$ 时，我们在 $v_A$ 中加入一个额外项，该项与货币的兑换率成反比。

#### 4.4.2 效用模型

考虑第 4.2 节所述的攻击模型。若在选定协议 Π 上定义攻击 $A(\Pi)$，令 $C_{\mathcal{A}}$ 为模拟器集合，用于模拟针对放宽后的理想功能 $< \mathcal{G}_{weak-ledger} >$的攻击。给定 $\mathcal{S} \in C_{\mathcal{A}}$ 和环境 $\mathcal{Z}$，$v_H$，$v_A$，$v_R$ 分别为诚实参与者、攻击者和理性参与者的期望收益。我们将单个矿工的归一化收益定义为：单个诚实矿工（对外部观察者而言未偏离）的收益为 $n\ t^{\frac{v_H+v_R}{()(\beta_{Hon}+\beta_{Rat})}}$，单个攻击者（相对于外部观察者而言发生偏离）的收益为 $n\ t^{\frac{v_A}{()\beta_{Adv}}}$。若将效用模型乘以一个正数，我们可以利用参与者的最优策略不会改变这一事实，并省略 $n(t)$——第 $t$ 轮系统中的矿工数量。

对于攻击者，我们在集合 $C_{\mathcal{A}}$ 上对模拟器 $\mathcal{S}$ 的选择取最小值。这是因为 $C_{\mathcal{A}}$ 包含所有能够发起攻击的模拟器。其中许多模拟器可能会调用与攻击无关的额外事件。然而，攻击者的目的是迫使模拟器在理想世界中发起攻击。因此，最相关的收益是那个“仅仅”在理想世界中模拟该攻击的模拟器所获得的收益。因此，对于攻击者，我们在所有模拟器组成的集合 $\mathcal{C}_{\mathcal{A}}$ 上取最小值。对于协议描述符的效用（它是 HP、RP 和攻击者的期望收益的函数），我们考虑最坏环境（$\mathcal{Z}$）；对于攻击者的效用，则考虑最佳环境。总之，给定协议描述符策略 Π 的对抗策略 $A$（Π）的效用如下。

$$U_{\mathcal{D}}^{\Pi,<\mathcal{F}>}(A) = \min_{\mathcal{Z} \in ITM} \left\{ \min_{\mathcal{S} \in C_{\mathcal{A}}} \left\{ \frac{v_{\mathcal{H}} + v_{\mathcal{R}}}{\beta_{Hon} + \beta_{Rat}} - \frac{v_A}{\beta_{Adv}} \right\} \right\} \tag{5}$$

$$U_{\mathcal{A}}^{\Pi,<\mathcal{F}>}(A) = \max_{\mathcal{Z} \in ITM} \left\{ \min_{\mathcal{S} \in C_{\mathcal{A}}} \left\{ \frac{v_A}{\beta_{Adv}} \right\} \right\} \tag{6}$$

我们的对手是一个 $\mathcal{M}$–效用最大化对手。这意味着，给定由协议描述符选定的协议 Π，对手会选择最佳响应攻击 $A$，以最大化其效用函数 $U_A(\cdot)$。

**定义 4.3**。 如果给定的协议 Π 实现了功能 $<\mathcal{F}>$，对手会选择使其效用函数 $U^{\Pi,}{}_{\mathcal{A}}{}^{<\mathcal{F}>}(\cdot)$ 最大化的策略，那么该对手就是 $\mathcal{M}$–效用最大化对手。

$$U_{\mathcal{A}}^{\Pi,<\mathcal{F}>} = \max_{A \in ITM} U_{\mathcal{A}}^{\Pi,<\mathcal{F}>}(A)$$

#### 4.4.3 我们的效用模型的优势

我们的效用模型具有以下优势：

1. 它能更灵活地建模外部性，使 EO 能够将某些类型的偏离行为视为攻击，并相应地降低 $\theta(t)$。这也使我们能够针对不同类型的攻击，以不同方式建模市场响应。

2. 它可以表示可变区块奖励。此外，它不局限于特定类型的奖励模型[13]，，而是可以采用一个能够收敛或发散的一般数列。

3. 它捕捉了 可变难度，因为每一轮的挖矿概率彼此不同 er.

4. 协议描述符的 效用不仅试图提高诚实参与者的收益，还降低了诚实参与者与攻击者效用之间的差异。这优于以往的模型，因为它不允许此类攻击获得较高效用；这类攻击会提高诚实参与者的效用，却进一步提高攻击者的效用（可能是由于外部收益）。

## 5 威慑攻击

在本节中，我们提出对原始 PoW 区块链协议进行修改，以帮助我们应对第3节中讨论的攻击。

### 5.1 难度调整攻击

根据定理 3.1，显然，如果 $\beta_{adv}$ 至少为 1 2，我们就能克服难度篡改攻击的可能性。如果$\beta_{adv} > \beta_{adv} = 0.5$，则没有任何 PoW 区块链是安全的。在本小节中，作为定理 3.1 的推论，我们将证明，只要适当设置 $\tau_{min}$，就能实现这一点。

**推论 5.1.** 当$\beta_{adv} < \frac{1}{2}$时，若 $\tau_{min} \geq \frac{1}{2}$，则 *PoW* 区块链能够抵御难度篡改 攻击 –

证明。 根据定理 3.1 的证明，发起难度篡改攻击所需的 $\beta_{adv}$ 下界为 $\beta_{adv} = \frac{(3+\tau_{min}) - \sqrt{(3+\tau_{min})^2 - 4(\tau_{min}+1)}}{2}$。我们希望 $\beta_{adv} \geq \frac{1}{2}$。通过简单的代数运算，可以得出 $\beta_{adv} \geq 0.5$，如果$\tau_{min} \geq \frac{1}{2}$。[14]

– □

### 5.2 QUICK FORK 攻击

为了抵御 QUICK FORK 攻击，我们利用了对攻击者（AP）而言，理性参与者（RP）与诚实参与者（HP）无法区分这一点。为了让 RP 在对抗链（$C_A$）上挖矿，攻击者（AP）会在 RP 的帮助下公开 $C_A$，使诚实参与方（HPs）也能看到。我们建议允许所有参与方（不偏离协议者）向任何短于其挖矿所在链的链添加无效性证明 （POI）。借助 POI，我们可以阻止 QUICK FORK 攻击。

PC-MOD **解决方案** 我们建议区块链协议允许参与方 $par$ 在高度为 $a_{par}$ 的区块链 $C_{par}$ 上挖矿时，如果观察到 $C_A$ 的高度为 $\leq a_{par} - k_{th}$，则可在分叉链（$C_A$）上添加一个包含 POI 的区块。其中， $k_{th}$ 是阈值间隔，其定义如下。

**定义 5.1** （阈值间隔）。 阈值间隔（$k_{th}$）是最长链（$C_H$）与分叉链（$C_A$）之间的高度差，使得在 $C_A$ 上挖矿的 $\beta_{rat} + \beta_{adv}$ 以 $\geq 1 - \mu$ 的概率（w.p.）能够超越 $C_H$。

$$k_{th} = \rho - log_{\phi}(\mu + \phi^{\rho}(1 - \mu)) \tag{7}$$

这里， $\phi = \frac{\beta_{hon}}{1-\beta_{hon}}$ 和 $\rho$ 是 EO 的容忍因子。该关系是通过遵循与定理3.2的步骤 4及 Ross [1975] 的第 4.5.1 节中结果类似的论证推导得出的。

[13]大多数先前的研究都采用固定的区块奖励 [14]我们不讨论 $\beta_{adv} > \frac{1}{2}$ 因为在这种情况下，可以通过 51% 攻击进行分叉。

我们希望 PoI 满足两个条件。（1）包含该 POI 的区块与任何其他区块都无法区分；否则，RP 和攻击者会忽略该区块，并在其父区块之上挖矿；（2）对手不能在诚实最长链上添加 POI 并使该区块链失效。我们根据以下定义构造 PoI，使其满足这两个要求。

**定义 5.2**（无效性证明）。 POI 交易 被发布在分叉链上，以证明该链的无效性。其构造如下：

• POI 由字符串 $h$ 组成，该字符串是哈希值 $H(H_{a_{par}}||m_{secret})$[15]。其中， $H_{a_{par}}$ 是 $C_H$上高度为$\geq a_{par}$ 的区块的哈希值，而 $m_{secret}$ 是 POI 提议者选择的秘密字符串。

• 由于 $h$ 是任意字符串，因此该交易与任何其他交易都无法区分。

• 由于无效性交易的提议者是 HP，因此，如果该链通过公开 $m_{secret}$而超越 $C_H$ 成为最长链，他们就可以使其无效。如果 POI 在高度 $\leq a_{par} - k_{th}$处被添加到 $C_A$，则该 POI 被视为有效。

**命题 5.1.** 诚实参与者在 $C_A$ 上成功添加 *POI* 的概率为 $\geq 1 - e^{-\beta_{hon} \cdot k_{th}}$。

证明。 初始时， $C_A$ 落后于 $C_H$ 个区块，相差 $k_{th}$ 个区块。诚实参与者只能在这 $k_{th}$ 个区块中添加 POI，因为 POI 所在的高度必须低于其哈希值所属区块的高度（该区块位于高度 $a_{hon}$）。因此，如果对手在这 $k_{th}$ 个区块中挖出一个区块，就能成功将 POI 添加到该区块。设 $E_{mit}$ 为诚实参与者在这 $k_{th}$ 个区块中成功挖出一个区块的概率。利用不等式 $e^{-x} > 1 - x$，我们得到 $P[E_{mit}] = 1 - (1 - \beta_{hon})^{k_{th}} > 1 - e^{-\beta_{hon} k_{th}}$ □

请注意，上述概率仅考虑了诚实参与者通过挖出区块来添加 POI 的情况。实际上，诚实参与者可以广播利益证明交易，而所有在 $C_A$ 上挖矿的参与方都会将该交易添加进去，因为它与其他任何交易并无不同。因此，实际概率高于命题 5.1 中的概率。

**定理 5.1**。 采用 *PC-MOD* 的 *PoW* 区块链协议 *(i)* 理性参与者在最长链上挖矿且不转向 $C_A$（即 快速 分叉 攻击中的分叉链），构成一种均衡。*(ii)* 对于 $\beta_{adv} < \frac{1}{2}$，该协议以高概率抵御快速 分叉 攻击。

证明。 PC-MOD 修改要求诚实参与方在 $C_A$ 上挖矿，除非其 POI 交易已被纳入区块链中的某个区块。这使得发起（并加入）快速分叉攻击的偏离行为失去诱因，原因有三：

1 所有 $\beta_{adv} + \beta_{rat} + \beta_{hon}$ 参与方都在 $C_A$ 上挖矿，因此理性参与者或攻击者可能因区块奖励份额增加而获得的任何优势，如今都不复存在。

2 理性参与者没有动力在 $C_A$ 上挖矿，因为 (i) 区块奖励并不高于在最长链 $C_H$ 上挖矿所得，且 (ii) 如果理性参与者转而在 $C_A$ 上挖矿，那么在 $C_H - C_H^{\lfloor k^{th}}$ 上、介于 $C_H$ 之间的挖矿成本就会白白浪费，因此其效用低于在 $C_H$ 上挖矿所得。

3 如果此类攻击仍然发生，HP 挖出区块，或有效的 POI 交易（与其他交易无法区分）被纳入 $C_A$ 的风险始终存在，从而导致 $\theta(t) = e_{security}$。这种情况发生的概率为 $> (1 - (1 - \beta_{hon})^{k_{th}})$，因此会抑制 RP 参与攻击。

因此，对于 $\beta_{adv} < \frac{1}{2}$，只有当 $\beta_{adv}$ 能够独自使区块链分叉时，攻击才会发生，而这种情况发生的概率可忽略不计。 □

### 5.3 带贿赂的自私挖矿攻击

针对带贿赂的自私挖矿攻击，我们给出了一个相当悲观的结果。该结果表明，不可能存在一种实现账本功能 $\mathcal{G}_{weak-ledger}$ 的协议，能够抵御带贿赂的自私挖矿攻击。

**定理 5.2** (自私挖矿不可能性)。 对于任何 *UC*实现 $\mathcal{G}_{weak-ledger}$ 的工作量证明区块链，该协议都不可能是强攻击收益安全 的，因为只要抢先交易可行，带贿赂的 自私挖矿 攻击 就总是可能发生。

[15]这里 $H$ 是 PoW 区块链所使用的哈希函数 ain.

$\Pi_{Tx-Inclusion}$

**输入**: $dest^a$, $tx^b$, $\mathfrak{H}^c$
如果 最后 $l$ 位比特 $\mathbf{H}(tx, \mathfrak{H}) = \mathbf{H}(dest, \mathfrak{H})$ 返回 True
否则返回False

[a]矿工的目标地址
[b]交易
[c]父区块哈希

证明。 证明可直接由下文陈述的引理 5.3 得出。如果对于每个协议，每次诚实执行都有一个与之不可区分的带贿赂的自私挖矿对应执行，那么对于每个这样的协议，带贿赂的自私挖矿攻击都是可能的。请注意，与文献中的标准做法一致，Badertscher 等人[2018, 2021], 的证明本质上假设，对任何对手而言，最佳响应 $A$ 都是抢先交易，即 $A \in \mathcal{A}_{fr}$。 □

**引理 5.3**。 对于协议 $\Pi$，存在一个环境 $Z_1$ 和一个用于抢先交易对手 $S_1 \in \mathcal{A}_{fr}$的模拟器，以及一个相应的环境 $Z_2$ 和一个用于使用 SELFISH MINING WITH BRIBING $S_2 \in \mathcal{A}_{SMB}$ 的对手的模拟器，使得对于任意 *PPT* 观察者，执行 $(S_1, Z_1)$ 与 $(S_2, Z_2)$ 不可区分。

证明。 证明见附录 B.1 □

### 5.4 $\Pi_{tx-inclusion}$协议

为解决交易扣留攻击（第 3.3 节），我们提出对 $\Pi_{gossip}$进行修改，增加一个子协议。该子协议（$\Pi_{Tx-Inclusion}$）是一种过滤器，每个矿工只能在当前区块中加入满足特定条件的交易。通过此修改，我们可以论证，RP 因扣留交易而获得的效用增益可忽略不计，这意味着遵循 $\Pi_{gossip}$ 是针对交易扣留偏离的近似纳什均衡。

#### 5.4.1 拟议修改

理性参与者挖出区块时，只能在区块中添加满足条件**C1**的交易。

**C1：** 如果给定区块和 coinbase 地址 $dest$ （类似于比特币 En.bitcoin.it [2021] 中的 Pay2PubHash），以及父区块哈希 $\mathfrak{H}$，交易 $tx$ 满足**C1** 的条件，当且仅当$\mathbf{H}(tx, \mathfrak{H})$和$\mathbf{H}(dest, \mathfrak{H})$的最后 $l$ 位相同。如果 coinbase 是脚本（例如比特币 En.bitcoin.it [2017] 中的 Pay2ScriptHash）， $dest$ 就是脚本哈希。
为了尽可能多地添加交易，诚实参与方可能需要维护多个密钥。我们可以使用 PKI 树（Buldas 等人 [2017]），其密钥存储所需空间为对数级。经过这些修改后，参与方挖出区块并同时纳入被扣留交易的概率会降低，原因有以下两种:

1 如果参与方随机选择一个地址，并将全部算力用于工作量证明（PoW）以挖出区块，那么该交易有效、能够被纳入区块的概率为 $\frac{1}{2^l}$。
2 如果参与方将部分挖矿算力用于寻找有利的地址映射，那么它能进行的工作量证明查询次数就会减少，从而降低其挖出区块的概率。此外，该参与方创建的地址映射对下一轮没有用处。

**引理 5.4.** 如果遵循 $\Pi_{tx-inclusion}$，那么对于 $\epsilon_G = tx \cdot O(2^{-l})$， $\Pi_{gossip}$是 $\epsilon_G-$纳什均衡。这里， $tx$ 是发送给参与方的交易所产生的累计手续费，并且是关于 $l$ 的多项式。

总之，遵循 $\Pi_{tx-inclusion}$时，交易扣留攻击不会带来显著收益，如引理 5.4 所示。证明方法是计算遵循和偏离 $\Pi_{gossip}$所带来的收益之差，即 $\leq \epsilon_G$。计算过程见附录 B.2。

## 6 PRAGTHOS 与理论分析

我们发现了针对 PoW 区块链的多种攻击（比特币中也存在这些攻击）。此前的博弈论分析 Badertscher 等人 [2018], Garay 等人 [2013], Karakostas 等人 [2022], Judmayer 等人 [2020] 主要关注静态参与者群体以及区块奖励和难度保持不变的时间范围。我们提出的分析框架

在第4节中提出，具有很强的通用性，可以发现上述攻击（第3节）。在第5节中，我们通过以下方式提出了针对这些攻击的新颖解决方案：(1) 在 PoW 区块链中提出额外的子协议，或 (2) 指定超参数值。通过这些修改，我们抽象出了一个新的 PoW 区块链协议框架。我们称之为 **PRAGTHOS**——实用理性博弈论安全（Practical Rational Game Theoretically Secure）。它也是以下两个词的组合："务实的"，意为合乎逻辑（理性），以及"精神特质"，大致可译为性格，用于描述协议用户的理性特征。在本节中，我们首先总结**PRAGTHOS**，然后（第6.2节）对其进行安全分析。

### 6.1 对 PoW 区块链的修改

**工作量证明框架** 如第2.2节所述，在工作量证明区块链中，参与方通过解答密码学谜题来挖掘区块。该谜题要求找到一个随机 nonce 和交易数据的默克尔根，再次对区块头数据进行哈希运算，最终哈希值应小于由每个纪元开始时进行的难度重新计算所确定的某个目标值。参与方应收集他们听到的所有交易，并在纪元结束时调整难度，以尽可能保持两个区块之间的平均持续时间不变。先前难度与新难度的比值必须为 $\in [\tau_{min}, \tau_{max}]$。区块奖励在不同阶段之间按因子 $\vartheta$ 变化。设协议所遵循的区块奖励方案为 $g(0)\ g(1)\ldots$ 其中 $g(i) = r_{block}(0) \cdot \vartheta(i)$。[16] 表示阶段 $i$ 的区块奖励。对于比特币，$\vartheta(i) = \frac{1}{2^i}$。

当序列 $< \vartheta >$ 收敛时（即对于所有 $L$，$\sum_{i=0}^{L} \vartheta(i)$ 都是有限的），底层加密货币称为通缩型；否则称为通胀型。

**定义6.1**（通胀型加密货币）。如果一种 PoW 加密货币的区块奖励按照 $r_{block}^{new} = \varpi(r_{block}^{old}, i) = r_{block}^{old} \vartheta^{(i)}$ ( $_{i-1)}$更新，且 $< \vartheta >$ 发散[17]，则称其为通胀型。

按照图3所述对工作量证明协议进行修改后，若满足 $\beta_{adv} < \frac{1}{2}$，**PRAGTHOS** 具有强攻击收益安全性；若满足 $\beta_{adv} < \beta^{SMB}$，则可确保公平性（抵御带贿赂的自私挖矿攻击）。

在**PRAGTHOS**中，PoW 区块链进行了以下修改。
❑ *PC-MOD*。所有参与方在观察到一条至少比其当前区块链落后 $k_{th}$个区块的分叉时，都应添加 POI（定义5.2）（式7）。❑ 难度调整。为防范难度调整攻击，各参与方应在每个纪元结束时更新难度的过程中使用 $\tau_{min} = \frac{1}{2}$。❑ 添加交易。在区块中收集交易时，遵循 $\Pi_{Tx-inclusion}$。

图 3：PRAGTHOS 框架

首先，我们需要假设，如果每个矿工都是诚实的，那么奖励结构能够使挖矿有利可图，从而补偿所产生的成本。我们称之为全体诚实时的盈利性。这一条件确保对所有诚实参与者而言，协议都是个体理性[18]。请注意，我们在分析中并未假设 $\beta_H = 1$。

**定义 6.2**（全体诚实时的盈利性）。我们称某 PoW 区块链的区块奖励方案在第 $t$ 轮满足全体诚实时的盈利性，如果对于满足 $\beta_H = 1$ 的系统，我们有 $\theta(t) r_{block}(t) p_H > \chi(t)$。这里，$p_H$ 是单个矿工在第 $t$ 轮挖出区块的概率。

### 6.2 结果

攻击者可以凭借多数算力（通过 51% 攻击）使 PoW 区块链发生分叉，因此挖矿对诚实参与者而言未必有利可图。因此，我们假设 $\beta_{adv} \leq \frac{1}{2}$。然而，如第 3.1 节所示，即使如此，典型的 PoW 区块链仍容易受到攻击，这些攻击可能导致 $\theta(t) = e_{security}$，使挖矿无利可图。

[16] 此关系也可以写作 $r_{block}^{new} = \varpi(r_{block}^{old}, i) = r_{block}^{old}\ ^{\vartheta_{(i)}\,\vartheta(i-1)}$ [17] 发散的 $\Rightarrow$ $i \longrightarrow \infty$ $\lim_{L\to\infty} \sum_{i=0}^{L} \vartheta(\,)$ 个体理性意味着，参与协议所获得的收益 $\geq$ 高于[18] 弃权、不参与所获得的收益。

### 6.2.1 通胀型货币的强攻击收益安全性

在本节中，我们分析并证明了定理 6.1：在通胀型区块奖励方案下，**PRAGTHOS**具有强攻击收益安全性（定义4.2）（充分性条件）。我们进一步证明，这种通胀对于**PRAGTHOS**是必要的，任何 PoW 区块链协议要实现强攻击收益安全性都必须如此（定理 6.3）。

**定理 6.1** (强攻击收益安全性——充分性)。 ***PRAGTHOS*** 在 $\beta_{adv} < \frac{1}{2}$ 奖励方案为通胀型且满足全体诚实时的盈利性时，具有强攻击收益安全性。

证明。 为证明该结果，我们采用了由 Canetti 最初提出的可组合性框架 Canetti [2001], , 并由 Badertscher 等人进一步将其应用于区块链 Badertscher 等人 [2017]。我们已在第 2.1 节简要介绍该框架。由此，证明可直接由引理 6.2 得出，因为 **PRAGTHOS**满足引理的全部三个条件（C1-C3）。 □

**引理 6.2**。 令 $A_{fr}$ 为半诚实抢先交易对手的类别。对于每个对抗策略 $A_2$，都存在对抗策略 $A_1 \in A_{fr}$，

$$U(\Pi, A_1) + negl(\kappa) \geq U(\Pi, A_2)$$

当且仅当满足以下条件时，该结论成立：

*C1* 奖励方案与外部性满足全体诚实时的盈利性。

*C2* $\beta_{adv} < \frac{1}{2}$

*C3* 区块奖励方案是通胀型的。

证明。 本证明分为 3 个步骤（7 个子步骤）。在步骤 1 中，我们求出抢先交易对手 $A_1 \in A_{fr}$的效用。具体而言，我们在步骤 1a 中找出该对手存在的环境以及奖励 $\mathcal{R}_{A_1}$。随后，在步骤 1b 中，考虑可变难度和动态参与者数量后，我们为 $A_1$挖矿的概率求出一个适当的下界。最后，在步骤 1c 中，我们将可变区块奖励（通胀型）纳入考量，并为 $A_1$或 $E[\mathcal{R}_{A_1}]$求出期望奖励的下界。
在证明的步骤 2 中，我们针对任意其他对手 $A_2$ 及其收益最大化环境$Z_2$，求出其收益的上界。在此情形下，我们求出对手 $A_2$的期望收益上界。然后，在步骤 3a 中，我们论证对于每个 $Z_2$，总存在一个环境 $Z_1$，使某个条件成立。我们论证，在这样的环境下，除可忽略概率外，$A_1$ 的收益超过 $A_2$的期望收益。最后，在步骤 3b 中，我们通过反证论证，对抗设置（$S_1$，$Z_1$）是强攻击收益安全的。其中，$S_1$ 是 $A_1 \in A_{fr}$的理想世界模拟器。（完整证明参见附录 C.1） □

全体诚实时的盈利性条件旨在确保未偏离的参与方参与系统。此外，攻击者既有内部激励（通过代币），也有外部激励（通过对货币持有空头头寸），因此无论全体诚实时的盈利性条件如何，都会受到激励而参与。由于我们针对一般发散级数 $\vartheta$ 证明了这一结论，因此它也适用于常数序列（$\vartheta(i) = c$）、调和级数（$\vartheta(i) = \frac{1}{i}$）等。

### 6.2.2 通货紧缩货币的结果

PRAGTHOS 的优势之一是，即使在通货紧缩奖励方案下，它也能针对一类攻击轮次数有上限的对手，提供强攻击收益安全性。本节首先说明，采用几何递减区块奖励方案的 PoW 区块链（如比特币）无法针对 PPT ITM 对手实现强攻击收益安全。随后我们将说明，遵循 PRAGTHOS 框架的此类 PoW 区块链，能够针对攻击轮次数有上限的 PPT ITM 对手实现强攻击收益安全。

**定理 6.3** （通货紧缩奖励方案）。 采用几何递减通货紧缩奖励方案的 *PoW* 区块链（$\vartheta(i) = \vartheta^i$ 对于 $\vartheta < 1$）在区块奖励模型中无法实现强攻击收益安全。我们假设协议最初（在 $t = 0$ 时）满足全诚实多数。

证明。 证明分为三个步骤。步骤 1 中，我们说明当奖励不满足全体诚实时的盈利性（定义 6.2）时，结论为何成立。对于全体诚实时的盈利性，证明进一步分为步骤 2 和步骤 3。步骤 2 中，我们为任何在挖矿概率上略有优势的对手 $A_2$ 找到一个环境 $Z_2$（例如，这种优势可能源于自私挖矿）。步骤 3 中，我们通过证明 $A_2$ 在环境 $Z_2$ 中的期望收益高于任何抢先交易半诚实对手 $A_1 \in A_{fr}$，完成证明。完整证明见附录 C.2。 □

**定理 6.4**。 对于 $A_2$ 延续阶段数少于 $\alpha_{th}$ 的攻击，***PRAGTHOS*** 采用通缩型（$\vartheta$ 呈几何递减）区块奖励方案时，对于$\beta_{adv} < \frac{1}{2}$，可针对计算能力受限的对手 $A \in \mathcal{A}^{\alpha_{th}}$ 其中，

$$\alpha_{th} = 1 + \lfloor \frac{log(1 - p_{fr})}{log(\vartheta)} \rfloor$$

这里 $p_{fr}$ 是协议接受抢先交易半诚实对手查询的概率。

证明。 该定理的证明使用了定理 6.3 中讨论的对手。该对手是能够通过任何抢先交易策略获得更高收益的最弱强力对手。为得出此结果，我们将攻击者限制为弱于该对手。完整证明见附录 C.3 □

## 7 结论与未来工作

**结论**。 本文分析并发现了区块链协议中可能存在的安全攻击。例如，比特币无法抵御对手控制 。45 的算力。我们指出了以往安全分析模型无法捕捉这些攻击的原因。为此，我们提出了一种新颖的理性协议设计（ʀRPD）模型。基于该模型，我们设计了解决这些攻击的方案，并提出了一个用于设计 PoW 区块链协议的框架，即 **PRAGTHOS**。我们证明，在通胀型区块奖励方案下，**PRAGTHOS** 具有强攻击收益安全性。在通缩型区块奖励方案下，我们证明，**PRAGTHOS** 能够抵御受轮次数量限制的对手。

**未来工作**。 用于分析 PoW 区块链协议安全性的模型未能捕捉由系统外部因素激励的理性偏离行为，例如 Judmayer 等人提出的攻击 [2020]。我们认为，可以通过推广 PRPD 来描述此类攻击。我们认为，我们的结果将现有的区块链博弈论安全性模型扩展到了一个更通用的模型。将安全模型扩展到其他类型的区块链协议（例如 PoS），以及针对激励驱动型对手的其他密码协议，或许也值得研究，这留待未来工作探讨。

## 参考文献

中本聪。比特币：一种点对点电子现金系统，2009年。Vitalik Buterin 等人。以太坊白皮书，2013年。尼克·萨博。形式化并保障公共网络上的关系安全。*First Monday*，2，1997年。Michael J. Fischer、Nancy A. Lynch 和 Mike Paterson。一个进程发生故障时分布式共识的不可能性。载于数据库系统原理（*PODS*）’*83*，1983年。Juan A. Garay、Aggelos Kiayias 和 Nikos Leonardos。比特币骨干协议：分析与应用。载于*EUROCRYPT*，2015年。Juan A. Garay、Aggelos Kiayias 和 Nikos Leonardos。具有可变难度链的比特币骨干协议。载于*CRYPTO*，2017年。Ittay Eyal 和 Emin Gün Sirer。多数并不足够：比特币挖矿易受攻击。载于金融密码学，2014年。Christian Badertscher、Ueli Maurer、Daniel Tschudi 和 Vassilis Zikas。比特币作为交易账本：一种可组合处理。*IACR*密码学电子印本文档库，2017:149，2017年。Ran Canetti。通用可组合安全：密码协议的新范式。*2001*年*IEEE*集群计算国际会议论文集，第136–145页，2001年。Juan A. Garay、Jonathan Katz、Ueli Maurer、Björn Tackmann 和 Vassilis Zikas。理性协议设计：针对激励驱动型对手的密码学。*2013*年*IEEE*第*54*届计算机科学基础年会，第648–657页，2013年。Christian Badertscher、Juan A. Garay、Ueli Maurer、Daniel Tschudi 和 Vassilis Zikas。但它为何有效？比特币的理性协议设计处理。*IACR*密码学电子印本文档库，2018:138，2018年。Christian Badertscher、Yun Lu 和 Vassilis Zikas。对51%攻击的理性协议处理。载于*IACR*密码学电子印本文档库，2021年。Aljosha Judmayer、Nicholas Stifter、Alexei Zamyatin、Itay Tsabary、Ittay Eyal、Peter Gazi、Sarah Meiklejohn 和 Edgar R. Weippl。综述：针对无许可工作量证明加密货币的算法性激励操纵攻击。载于*IACR*密码学电子印本文档库，2020年。Kevin Liao 和 Jonathan Katz。激励比特币中的双重支付合谋。2017a年。Kevin Liao 和 Jonathan Katz。通过巨鲸交易激励区块链分叉。载于金融密码学研讨会，2017b年。Runchao Han、Zhimei Sui、Jiangshan Yu、Joseph K. Liu 和 Shiping Chen。事实与虚构：对无许可区块链诚实多数假设的挑战。*2021*年*ACM*亚洲计算机与通信安全会议论文集，2021年。Itay Tsabary 和 Ittay Eyal。间隙博弈。第*11*届*ACM*国际系统与存储会议论文集，2018年。Shoeb Siddiqui、Ganesh Vanahalli 和 Sujit Gujar。BitcoinF：在仅交易费模型下实现比特币的公平性。载于自主智能体与多智能体系统（*AAMAS*），2020年。Lin Chen、Lei Xu、Zhimin Gao、Ahmed Imtiaz Sunny、Keshav Kasichainula 和 W. Shi。非线性区块链系统的博弈论分析。载于自主智能体与多智能体系统，*AAMAS*，2021年。Dimitris Karakostas、Aggelos Kiayias 和 Thomas Zacharias。区块链纳什动力学与合规追求。*arXiv*，abs/2201.00858，2022年。Sarah Azouvi 和 Alexander Hicks。综述：加密货币安全博弈论模型的工具。*arXiv*，abs/1905.08595，2020年。Puwen Wei、Quan Yuan 和 Yuliang Zheng。区块链对长延迟攻击的安全性。*IACR*密码学电子印本文档库，2018:800，2018年。Peter Gazi、Ling Ren 和 Alexander Russell。工作量证明区块链的实用结算界限。载于*2022*年*ACM SIGSAC*计算机与通信安全会议论文集，CCS ’22，第1217–1230页，美国纽约州纽约市，2022年。计算机协会。ISBN 9781450394505。doi:10.1145/3548606.3559368。URL https://doi.org/10.1145/3548606.3559368。Quan Yuan、Puwen Wei、Keting Jia 和 Haiyang Xue。对抗性矿工遭受长延迟攻击时区块链协议的分析。中国科学：信息科学，63:1–15，2020年。

Peyman Momeni、Sergey Gorbunov 和 Bohan Zhang。Fairblock：以极低开销防止区块链抢先交易。密码学电子印本档案，论文 2022/1066，2022年。Mike Graf、Daniel Rausch、Viktoria Ronge、Christoph Egger、Ralf Küsters 和 Dominique Schröder。分布式账本安全框架。载于*2021*年*ACM SIGSAC*计算机与通信安全会议论文集，CCS '21，第 1043–1064 页，美国纽约，2021年。计算机协会。ISBN 9781450384544。doi:10.1145/3460120.3485362。URL https://doi.org/10.1145/3460120.3485362。Junming Ke、Pawel Szalachowski、Jianying Zhou 和 Qiuliang Xu。以通用可组合安全形式化比特币崩溃。载于*IACR*密码学电子印本文档库，2020年。Malte Möser 和 Rainer Böhme。趋势、建议与成本：比特币交易手续费的纵向研究。载于 Michael Brenner、Nicolas Christin、Benjamin Johnson 和 Kurt Rohloff 编，《style id='5'>金融密码学与数据安全，第 19–33 页，柏林，海德堡，2015年。施普林格柏林海德堡。ISBN 978-3-662-48051-9。Juanjuan Li、Yong Yuan、Shuai Wang 和 Fei-Yue Wang。比特币区块链中的交易排队博弈。载于*2018*年*IEEE*智能车辆研讨会 *(IV)*，第 114–119 页，2018年。doi:10.1109/IVS.2018.8500403。Nicolas Houy。比特币交易费的经济学。*ERN*：其他微观经济学：生产，2014年。Tim Roughgarden。交易费机制设计。*ACM SIGecom*交流，19：52–55，2021年。Miles Carlsten、Harry Kalodner、S. Matthew Weinberg 和 Arvind Narayanan。论没有区块奖励时比特币的不稳定性。载于*2016*年*ACM SIGSAC*计算机与通信安全会议论文集，CCS '16，第 154–167 页，美国纽约，2016年。计算机协会。ISBN 9781450341394。doi:10.1145/2976749.2978408。URL https://doi.org/10.1145/2976749.2978408。Cynthia Dwork、Nancy A. Lynch 和 Larry J. Stockmeyer。部分同步条件下的共识（初步版本）。载于*ACM SIGACT-SIGOPS*分布式计算原理研讨会，1984年。Shayan Eskandari、Seyedehmahsa Moosavi 和 Jeremy Clark。SOK：透明的不诚实行为：区块链上的抢先交易攻击。计量经济学：计算机程序与软件电子期刊，2019年。Lorenz Breidenbach、Philip Daian、Florian Tramèr 和 Ari Juels。迎接九头蛇：迈向有原则的漏洞悬赏和抗漏洞利用智能合约。载于第*27*届*USENIX*安全研讨会论文集，SEC'18，第 1335–1352 页，美国，2018年。USENIX协会。ISBN 9781931971461。Harry A. Kalodner、Miles Carlsten、Paul Ellenbogen、Joseph Bonneau 和 Arvind Narayanan。Namecoin 的实证研究及其对去中心化命名空间设计的启示。载于信息安全经济学研讨会，2015年。Mark Friedenbach。链上前向区块／无需硬分叉即可提高结算容量。2018年。Gregory W. Shirah。《边缘》。载于计算机图形学与交互技术国际会议，2008年。Sheldon M. Ross。概率模型导论。《技术计量学》，40：78–78，1975。En.bitcoin.it。比特币脚本——比特币维基，2021年。URL Available:https://en.bitcoin.it/wiki/Script。En.bitcoin.it。支付至脚本哈希——比特币维基，2017年。URL https://en.bitcoin.it/wiki/Pay_to_script_hash。Ahto Buldas、Risto Laanoja 和 Ahto Truu。无密钥签名基础设施与公钥基础设施：前量子与后量子时代的哈希树签名。国际服务技术管理期刊，23：117–130，2017年。Savva Shanaev、Arina Shuraeva、Mikhail Vasenin 和 Maksim Kuznetsov。加密货币价值与51%攻击：事件研究的证据。载于《另类投资期刊》，2019年。Michael Mitzenmacher 和 Eli Upfal。《概率与计算：事件与概率》。2005年。Joseph Bonneau。恶意区块链接管（短文）。载于金融密码学研讨会，2018年。

# A 关于攻击的定理证明

## A.1 定理 3.1 的证明

步骤 1：注意，对手的效用为

$$U_A = \max_{\mathcal{Z} \in ITM} \min_{\mathcal{S} \in C_A} E[v_A^{\mathcal{G}_{weak-ledger}, \mathcal{S}, \mathcal{Z}}]$$

由于协议描述符旨在确保最坏情况下的安全性，我们考虑一个使 $U_A$ 最大化的环境。对手会最优地选择其控制下的参数（$\alpha$，$r_1$，$r_2$），如下所示：

❶ 为了使成功攻击的概率最大化，对手会延长持续时间，即设置 $r_1 = 0$，$r_2 = 1$.❷ 对手发起攻击时，最优策略是调整 $\alpha$，使得 $\tau_{adv} = \tau_{min}$；当其设置为 $\alpha = \frac{\beta_{adv}}{\tau_{min}}$ 时即可实现这一点。

在这些参数下，公式 3 化简为

$\frac{\tau_{hon}}{1-\beta_{adv}} + \frac{1}{1-\beta_{adv}} > \frac{1}{\beta_{adv}} + \frac{\tau_{adv}}{\beta_{adv}} \Rightarrow \frac{\beta_{adv}}{1-\beta_{adv}} > \frac{1+\tau_{min}}{1+\tau_{hon}}$

步骤 2：我们的分析仅涉及 $\beta_{adv} < \frac{1}{2}$，因为对于 $\beta_{adv} > \frac{1}{2}$，Shanaev等人指出，使用 51% 攻击进行分叉始终是可能的 [2019]。此外，由于该攻击属于安全攻击，EO 会观察到该攻击，因此根据定义，RP 会遵循诚实策略，我们将其视为诚实参与者。因此，我们证明 $\tau_{min} < \frac{1}{2} \Rightarrow 1-\beta_{adv} > \frac{1}{2} > \tau_{min}$ 的结果。步骤 3：按照步骤 1 和步骤 2 所述设置参数后，我们得到以下不等式：

$$\frac{2\beta_{adv} - \beta_{adv}^2 - 1 + \beta_{adv}}{1 - \beta_{adv}} > \tau_{min}$$

对 $\beta_{adv}$ 求解后，我们得到

$$\beta_{adv}^2 - (3 + \tau_{min})\beta_{adv} + (1 + \tau_{min}) < 0$$

该方程的根为 $L_1$，$L_2$，其中

$$L_1 = \frac{(3 + \tau_{min}) - \sqrt{(3 + \tau_{min})^2 - 4(\tau_{min} + 1)}}{2}$$

$$L_2 = \frac{(3 + \tau_{min}) + \sqrt{(3 + \tau_{min})^2 - 4(\tau_{min} + 1)}}{2}$$

$\beta_{adv}$ 的可行区域为（$L_1$，$L_2$）。然而，$L_2 > 1$，因此，将可能的 $\beta_{adv}$ 值与 DIFFICULTY ALTERING 攻击的可行值取交集，可得到界限 $\beta_{adv} \geq \frac{(3+\tau_{min}) - \sqrt{(3+\tau_{min})^2 - 4(\tau_{min}+1)}}{2}$。

步骤 4：令 $Q_i^{adv}$ 和 $Q_i^{hon}$ 分别为攻击者和诚实参与者挖掘一个区块所需时间的随机变量（RV）。我们定义两个随机变量 $Q^{adv}$ 和 $Q^{hon}$ 如下。$Q^{adv} = \sum_{i=0}^{2*\lambda} Q_i^{adv}$ 和 $Q^{hon} = \sum_{i=0}^{2\lambda} Q_i^{hon}$。$Q^{adv}$ 和 $Q^{hon}$ 表示挖掘 $2 * \lambda$，个区块所需的总时间；攻击会持续 2 个阶段，因此因子 2 即由此而来（因为 $1 - r_1 = r_2 = 1$）。由于对于不同的 $i$，随机变量 $Q_i^{adv}$s（同理，$Q_i^{hon}$）彼此独立，因此我们可以应用 Chernoff 界（参见 Mitzenmacher 和 Upfal [2005]，公式 4.2 和公式 4.5）

$$Pr[Q^{adv} \geq (1 + \varepsilon)E[Q^{adv}]] < e^{-\frac{E[Q^{adv}]\varepsilon^2}{3}}$$

$$Pr[Q^{adv} \leq (1 - \varepsilon)E[Q^{adv}]] < e^{-\frac{E[Q^{adv}]\varepsilon^2}{2}}$$

将偏离概率相加，挖掘 $\lambda$（$r_1 + r_2$）个区块所需的时间偏离超过 $\varepsilon$ 的概率为 $negl$（$\Theta\varepsilon^2$），因为挖掘一个区块的预期时间为 $\propto \Theta$。因此，难度调整攻击成功的概率为 $> 1 - 2 \cdot negl$（$\Theta\varepsilon^2$）。

## A.2 定理 3.2 的证明

我们分四个步骤证明：首先计算偏离协议和遵循协议时的收益（步骤 1 和 2），然后比较两者以推导出界限（步骤 3），最后计算此次攻击的成功概率（步骤 4）。

步骤 1 **偏离时的收益：**偏离后，区块链 $C_H$ 中 $P_i$ 的最后 $k$ 个区块会成为孤块，而攻击者、理性参与者和诚实参与者在主链上为这些区块付出的挖矿成本也会白白浪费。这会从$par \in \{rat, adv\}$的收益中扣除 $k\beta_{par}\chi_1$。此外，在 $C_A$ 上挖矿会产生成本 $= \frac{(k+m\ \beta_{par}\chi_1)}{\beta_{rat}+\beta_{adv}}$。由于诚实参与者没有在

$C_A$上挖矿。此外，$par$ 获得的区块奖励占主链中这~~$k+m$~~ 个区块总区块奖励的 $\frac{\beta_{par}}{\beta_{rat}+\beta_{adv}}$。该值等于 $(k+m\vartheta)\frac{r_{block}\beta_{par}}{\beta_{adv}+\beta_{rat}}$。综合这三项，~~我们得到偏离~~时的期望收益为：

$$v_{par}(\pi') = \frac{n-1}{n}\frac{\beta_{par}}{\beta_{rat}+\beta_{adv}}\big(r_{block}(k+m\vartheta) - \chi_1(k+m)\big) - k\beta_{par}\chi_1$$

QUICK FORK 攻击以 $\frac{n-1}{n}$ 的概率成功，这一点将在证明的步骤 4 中展示。

步骤 2 **遵循以下协议的收益：**遵循协议时，$par$（RP 或 AP）的收益为 $r_{block}(k+m\vartheta)$，产生的成本为 $\chi_1(k+m)$。因此，总收益为：

$$v_{par}(\pi) = \beta_{par}\big(r_{block}(k+m\vartheta) - (k+m)\chi_1\big)$$

我们可以将 $v_{par}(\pi')$ 改写为 $v_{par}(\pi') = \frac{n-1}{n}\big(\frac{v_{par}(\pi)}{\beta_{rat}+\beta_{adv}} - \chi_1 k\beta_{par}\big)$。此外，我们代入 $\eta = \frac{r_{block}}{\chi_1}$

步骤 3：条件 $v_{par}(\pi') - v_{par}(\pi) > 0$

$$\Rightarrow \chi_1\beta_{par}(\frac{(n\beta_{hon}-1)}{n(1-\beta_{hon})})((\eta-1)k + (\eta\vartheta-1)m > \chi_1\beta_{par}k$$

$$\Rightarrow (\frac{(n\beta_{hon}-1)}{n(1-\beta_{hon})})((\eta-1)k + (\eta\vartheta-1)m > k$$

由于 $C_A$ 以 $m$ 个阶段 $P_{i+1}$的区块领先于 $C_H$，因此，使用 $\beta_{hon}$ 挖矿算力在 $C_H$ 中挖出 $m$ 个区块所需的时间，与使用 $\beta_{rat}+\beta_{adv}$ 挖矿算力在 $C_A$ 中挖出 $k+m$ 个区块所需的时间相同。为简化符号表示，我们记作 $J = \frac{\beta_{hon}}{1-2\beta_{hon}}$。因此，

$$\frac{m}{\beta_{hon}} \geq \frac{m+k}{1-\beta_{hon}} \Rightarrow m \geq \frac{k\beta_{hon}}{1-2\beta_{hon}} = kJ$$

显然，当 $m > 0$时，$\beta_{hon}\pi < \frac{1}{2}$，这意味着 $\beta_{adv} + \beta_{rat} > \frac{1}{2}$。我们取可能的最早 $m$，得到 $m = \frac{k\beta_{hon}}{1-2\beta_{hon}}$。由此可得 $v_{par}(\pi') - v_{par}(\pi) > 0$，因为

$$\Rightarrow (\frac{(n\beta_{hon}-1)}{n(1-\beta_{hon})})(\eta - 1 + J\eta\vartheta - J) > 1$$

代入 $J$ 并化简后，得到

$$\eta > \frac{1-\beta_{hon}}{n\beta_{hon}-1}\cdot\frac{n-\beta_{hon}n-1}{1-(2-\vartheta)\beta_{hon}}$$

步骤 4：要使攻击成功，HP 的领先幅度必须在达到 $\rho$ 之前，从 $k$ 降至 0。这可以作为赌徒破产问题来求解（第 4.5.1 节，Ross [1975]），其中随机游走以概率$\beta_{hon}$朝有利于 HP 的方向移动。由此，攻击成功的概率为 $\frac{1-\phi^{\rho-k}}{1-\phi^{\rho}}$，其中 $\phi = \frac{\beta_{hon}}{\beta_{rat}+\beta_{adv}}$。若$\frac{1+(n-1)\phi^{\rho}}{n} > \phi^{\rho-k}$，此概率大于 $\frac{n-1}{n}$。我们可以将其化简为

$$k < \lfloor \rho - log_{\phi}(\frac{1+(n-1)\phi^{\rho}}{n}) \rfloor \tag{8}$$

由此，$k$ QUICK FORK 攻击成功的概率至少为 $> \frac{n-1}{n}$。

### A.3 定理 3.3 的证明

证明。为了证明这一攻击，我们假设贿赂金额为单个区块的区块奖励（$z > 0$，但取较小值）的 $z$ 比例。攻击者、理性参与者和诚实参与者的行为遵循第3.2.2节中所述的攻击策略。如果攻击者与诚实参与者挖出的区块打成平手，且攻击者挖出的区块成为最长链的一部分，那么对手的收益为（$1-z$）$r_{block}$，而在攻击者区块上继续挖出区块的参与方，其收益为（$1+z$）$r_{block}$。

贿赂会激励理性参与者偏离协议。因此，可以安全地采用与 Eyal 和 Sirer [2014] 中相同的收益；不过，$\gamma$ 在最长链出现平局时，挖在对抗区块上的非对手方所占比例为 $\frac{\frac{\beta_h}{2}+\beta_r}{\beta_h+\beta_r}$。将此值代入 Eyal 和 Sirer [2014]，的结果（公式2中也给出），得到 $\frac{1}{2} > \beta_a > \frac{\beta_h}{2\beta_r+4\beta_h}$

□

### A.4 引理 3.4 的证明

证明。 首先，我们计算理性参与者 $i$ 遵循协议 $\Pi_{Gossip}$时的效用，即广播其听到的、交易费为 $tx_i$ 的交易 $\mathfrak{T}$。然后，计算其不广播 $\mathfrak{T}$时的效用。我们考虑对攻击者不利的事件： (i) 其他参与方可能会添加 $\mathfrak{T}$； (ii) 如果该参与方之后添加 $\mathfrak{T}$，则奖励会被贴现。接着我们论证，后一种情况会带来更高的效用。
广播 $\mathfrak{T}$ 单个参与方在第 $t$ 轮挖出区块的概率为 $p_{su}(t)$，且每轮可以进行 $q$ 次查询。对于挖矿算力由其掌控的比例为 $\beta_i$ 的参与方，遵循 Gossip 协议时的效用为：

$$u_i^*(\beta_i) = (\sum_{j=1}^{n} tx_j)(\sum_{t=1}^{\infty} \delta^t p_{su}(t)(1-p_{su}(t))^{n(t)\cdot t})$$

不广播 $\mathfrak{T}$ 参与方 $i$ 的效用变为：

$$u_i^{'}(\beta_i) = (\sum_{j=1, j\neq i}^{n} tx_j)(\sum_{t=1}^{\infty} \delta^t p_{su}(t)(1-p_{su}(t))^{n(t)\cdot t}) + \frac{tx_i}{p_{su}}$$

由于 $\mathfrak{T}$ 在每轮被接受的概率为 $p_{su}$。设 $K$ 是一个随机变量：当参与方挖出区块时取 1，否则取 0。那么，$K$ 是一个参数为 $E[K] = \frac{1}{p_{su}}$ 的几何随机变量。显然可知， $u_i^*(\beta_i) \prec u_i^{'}(\beta_i)$。因此， $\sigma_{tw}$ 支配 $\Pi_{gossip}$。

□

## B 威慑攻击的证明

### B.1 引理 5.3 的证明

证明。 我们的证明分为三个步骤。步骤 1 中，我们为 $S_1 \in \mathcal{A}_{fr}$ 定义一个环境（$Z_1$， $S_1$）。步骤 2 中，我们定义（$Z_2$， $S_2$），其中 $S_2 \in \mathcal{A}_{SMB}$。然后在步骤 3 中，我们证明这两种执行彼此不可区分。

步骤 1：考虑一个模拟器 $S_1 \in \mathcal{A}_{fr}$ 是一个半诚实对手。环境 $Z_1$ 会观察所有链；如果两条链的高度相同而发生竞争，则会最大限度地延迟来自在某条链上挖矿的矿工的消息，该链的最后一个区块并非由被 $S_1$ 腐化的参与方挖出。

步骤 2：考虑任意一个模拟带贿赂的自私挖矿攻击（$S_2 \in \mathcal{A}_{SMB}$）的模拟器，以及任意一个通用环境 $Z_2$；该环境对攻击者、理性参与者和诚实参与者均以相同的（部分同步）方式通信。
步骤 3：显然，通过比较可知，对于任何观察这两个系统的参与方， $E[v^{\Pi,S_1,Z_1}] \equiv E[v^{\Pi,S_2,Z_2}]$，其中 $v$表示系统的外部视图。这意味着，任何 PPT 交互式图灵机都无法区分这两个系统。令 $D$ 为区分器，它是一个 PPT 交互式图灵机。我们将两个系统记为 $\rho_1 =< \Pi, S_1, Z_1 >$和 $\rho_2 =< \Pi, S_2, Z_2 >$。我们记随机变量 $C$，其取值为 1 或 2，且概率相等。根据 $C$的取值，我们选择系统 $\rho = \rho_C$ 发送给区分器 $D$。于是，若 $D$ 是 PPT 交互式图灵机，则 $Pr[D(\rho) = C] = \frac{1}{2} + negl(\varepsilon)$。

因此，由于这两个环境不可区分，我们无法确保攻击收益安全性（对手遵循 $A \in \mathcal{A}_{fr}$，同时也不允许带贿赂的自私挖矿）。

□

### B.2 引理 5.4 的证明

令 $Pool$ 为共同偏离 $\Pi_{tx-inclusion}$ 并扣留一组交易的参与方，其累计交易费为 $tx$。令 $\beta_{Pool}$ 为它们的总算力。

首先，我们将重点比较 $Pool$ 遵循 Gossip协议与采用交易扣留所获得的效用。接下来，由于分析针对交易网络，我们假设参与方会正确遵循 PoW协议。为便于抽象，我们考虑在一轮 $t$ 中，单个参与方挖出一个区块的概率为$p_{su}(t)$，参与方总数为 $n(t)$。遵循 Gossip协议所获得的收益为：

$$v(\Pi_{gossip}) = \sum_{i=1}^{\infty} \delta^{i-1} v_i(\Pi_{gossip})$$

$\mathcal{Z}_1^{Network}$

在接收()时
$M \leftarrow \{0,1\}^*$ （接收广播消息）
如果发送方($M$)是 $\mathcal{A}$
- $B_{\mathcal{A}} \leftarrow B_{\mathcal{A}} \cup M$
else
- 广播 $max(2, |B_{\mathcal{A}}|)$ 条 $B_{\mathcal{A}}$ 消息
- 广播 $M$

图4：环境 $Z_1$

其中， $\delta$ 为折扣因子，用于反映提议者将交易发送给另一参与方的概率不断增加，从而降低当前参与方专门为该交易挖矿的机会。 $v_i$ 为该交易在 $i^{th}$ 轮次中的期望收益。

$v_i\ (\Pi_{gossip})\ =$

$$(1-(1-p_{su}(i))^{\beta_{Pool}n(i)})(1-p_{su}(i))^{n(i)\cdot(i-1)}\frac{tx}{2^l}$$

将 $\sum_{i=0}^{\infty} v_i(\pi_{gossip})$ 相加，得到

$$\sum_{i=0}^{\infty}\delta^i(1-(1-p_{su}(i+1))^{\beta_{Pool}n})(1-p_{su}(i+1))^{n(i+1)\cdot i}\frac{tx}{2^l}$$

对于偏离协议 ($\Pi_{secret}$)，第 $i^{th}$ 轮的效用 $v_i(\Pi_{secret})$ 变为，

$$(1-(1-p_{su}(i))^{\beta_{Pool}n(i)})(1-p_{su}(i))^{n(i)\cdot(i-1)\beta_{Pool}}\frac{tx}{2^l}$$

因此我们有

$$v_i(\Pi_{secret})-v_i(\Pi_{gossip})=(1-(1-p_{su}(i))^{\beta_{Pool}n(i)})\frac{tx}{2^l}$$
$$(1-p_{su}(t))^{n(i)\cdot(i-1)\beta_{Pool}}(1-(1-p_{su}(t))^{n(i)\cdot(i-1)(1-\beta_{Pool})})$$

如果将此式对几何递减的 $\delta$求和，我们得到

$$v(\Pi_{secret})-v(\Pi_{gossip})=\sum_{i=1}^{\infty}(1-(1-p_{su}(i))^{\beta_{Pool}n(i)})\frac{tx}{2^l}\mathfrak{R}$$

$$\mathfrak{R}=(1-p_{su}(i))^{n(i)\cdot(i-1)\beta_{Pool}}(1-(1-p_{su}(i))^{n(i)\cdot i(1-\beta_{Pool})})$$

将概率上限取为 1，适用于 $(1-(1-p_{su}(i))^{n(i)\ i_{(1-\beta_{Pool})}})$, · 我们得到

$$\mathfrak{R}\leq(1-p_{su}(i))^{n(i)\cdot(i-1)\beta_{Pool}}=\mathfrak{M}$$

因此， $\mathfrak{M}$ 是在第 $i$轮没有矿工挖出区块的概率。

$$v(\Pi_{secret})-v(\Pi_{gossip})\leq\sum_{i=1}^{\infty}(1-(1-p_{su}(i))^{\beta_{Pool}n(i)})\frac{tx}{2^l}\mathfrak{M}$$

如果将剩余概率项的上界设为 1，我们得到如下表达式

$$v(\Pi_{secret})-v(\Pi_{gossip})\leq\frac{tx}{2^l}\sum_{i=0}^{\infty}\mathfrak{M}$$

由于区块未被挖出的总概率为（$\sum_{i=1}^{\infty}\mathfrak{M}\leq 1$），我们得到以下界

$$v(\Pi_{secret})-v(\Pi_{gossip})\leq\frac{tx}{2^l}$$

由于 $tx$ 是多项式　　在 $l$中， $\frac{tx}{2^l}$ 可忽略不计。令 $\epsilon_G=O(tx\cdot 2^{-l})$。因此我们得到 $v(\Pi_{secret})-v(\Pi_{gossip})\leq\epsilon_G$

# C PRAGTHOS 分析的证明

6.2 和 6.3 的证明基于攻击模型 $< \mathcal{F},\ < \mathcal{F} >,\ \upsilon >$，如 4.2 节所述，攻击模型为$< \mathcal{G}_{ledger},\ \mathcal{G}_{weak-ledger},\ (\upsilon_A,\ \upsilon_R,\ \upsilon_H) >$

## C.1 引理 6.2 的证明

证明。 步骤 1a 设 $A_1 \in A_{fr}$ 是一个进行 $q^*$ 次查询的抢先交易对手。进一步考虑环境 $Z_1$，该环境运行协议的执行，其中对手被激活并进行 $q^*$ 次查询后停止；同时，HPs 被激活，直到其中至少一方在其最长链中输出对手挖出的所有区块。我们考虑真实世界 UC 执行，并相应地定义所有随机变量。

考虑随机变量 量 $X_i$，当 $i^{th}$ 次查询中的对手成功挖出区块时，其值为 1；否则为 0。因此，攻击者在 $q^*$ 次查询为中的收益

$$\mathcal{R}_{A_1} = \sum_{i=1}^{q^*} X_i r_{block}\theta - \chi$$

注意，我们不计入对手通过降低 $\theta(t)$ 的值而获得的收益，该收益来自安全攻击——链分叉；因为在 **PRAGTHOS** 中，$\beta_{adv} < \frac{1}{2}$ 无法分叉。

步骤 1b 由于矿工数量存在变化，挖矿难度以及区块被接受的概率也会随每个纪元而变化，因此在纪元 $e$ 中，区块被接受的概率为 $p_e$。由于矿工数量不会在各轮次间呈指数增长，我们可以假设存在一个多项式 $s(t)$，使得 $n(t) \leq s(t)\ \forall t$。令 $p_e^{min}$ 表示如果 $n(t)$ 的增长恰好符合 $s(t)$，则 $A_1$ 在第 $t$ 轮挖出区块的概率。显然，$\forall$ 个纪元，$p_e \geq p_e^{min}$。令 $p_{min} = \min_{\forall e} p_e^{min}$。

步骤 1c 设截至 $a$ 次查询的区块奖励总和记为 $\mathfrak{J}(a) \cdot r_{block}(0)$。

$$\mathfrak{J}(a) := \sum_{i=0}^{a} \frac{r_{block}(i)}{r_{block}(0)} \approx \sum_{j=0}^{\alpha_a} \Lambda\vartheta(j)$$

我们将查询次数替换为挖出的区块数，因为查询次数较大时，挖出的区块数的期望值偏差极小；而在 $q$ 次查询中，挖出的区块数以压倒性概率不会偏差超过可忽略的量。该结果由 Chernoff 界分析得出。由于协议运行期间，从第 1 轮到 $r_1$ 轮的 $\theta$ 和 $\chi$ 均为变量，我们定义 $\eta_{max} = \max^{t\in[1,r_1]}{}_{p_e\theta}\, t^{\chi}{}_{()r_{block}}$。由于挖矿有利可图，我们可以得出 $\eta_{max} < 1$。此外，$\theta = \theta(t)$ 相同，因为 $\Pi$ 和对抗策略均为固定的。现在，我们可以得出

$$E[\mathcal{R}_{A_1}] \geq \mathfrak{J}(q^*)(1-\eta_{max})p_{min}r_{block}\theta$$

步骤 2 现在，考虑任意对手 $A_2 \in ITM$。该对手在环境 $Z$中执行期间进行 $Q$ 次查询。设 $P_Q$ 为该对手所进行查询次数的分布，$q = \max\ \text{support}(P_Q)$。设 $Z_2$ 为满足 $Q = q$的环境。考虑此 $(A_2,\ Z_2)$，其中通过将每次查询的挖矿概率取为 1，可得对手的期望收益上界，即

$$E[\mathcal{R}_{A_2}] \leq \mathfrak{J}(q)r_{block}\theta$$

这个上界源于这样一个事实：在$\mathcal{F}$ 功能中，单次查询最多只能将区块链延长一个区块。然而，如果其 UC 实现——状态交换协议 $\Pi$——并非如此，那么$EXEC_{\mathcal{F},\ \mathcal{S}_2,\ \mathcal{Z}_2} \not\approx EXEC_{\Pi_B,\ \mathcal{A}_2,\ \mathcal{Z}_2}$，进而 $C_{A_2} = \phi$，这是不可能的。

步骤 3a 我们选择 $Z_1$，使条件 $\mathfrak{J}(q^*) \geq$ $^{\mathfrak{J}(q)\kappa\ (1-\delta)(1-\eta_{max})p_{min}}$ 得到满足。由于加密货币本质上具有通胀性，我们可以确定这样的环境始终存在。这是因为对于通胀级数 $\mathfrak{J}$，总存在 $a_2 > a_1$，使得 $\mathfrak{J}(a_2) > \mathfrak{J}(a_1)$，

$$\because \lim_{a_2\to\infty} \mathfrak{J}(a_2) - \mathfrak{J}(a_1) \longrightarrow \infty\ \forall\ a_1$$

现在，考虑 $A_1$ 的收益低于 $A_2$的期望收益的概率。我们可以说，对于每个 $S_2$，总存在这样的 $Z_1$，因为由于级数 $\vartheta$的发散性，对于 $q$总存在这样的 $q^*$。

$$Pr[\mathcal{R}_{A_1} < E[\mathcal{R}_{A_2}]] \leq Pr[\mathcal{R}_{A_1} < \mathfrak{J}(q)r_{block}\theta]$$

$$\leq Pr[\mathcal{R}_{A_1} < (1-\delta)(1-\eta_{max})\mathfrak{J}(q^*)r_{block}p_{min}\theta]$$
$$\leq Pr[\mathcal{R}_{A_1} < (1-\delta)E[\mathcal{R}_{A_1}]] = Pr[\sum_{i=1}^{q^*} X_i \leq (1-\delta)E[\sum_{i=1}^{q} X_i]$$
$$< e^{-\frac{\delta^2 q^* p}{2}}$$

最后一个不等式由 Chernoff 界得出（Mitzenmacher 和 Upfal [2005]）。真实执行和理想执行中的所有随机变量（$Q$，$\mathcal{R}_{A_1}$，$\mathcal{R}_{A_2}$，$X_i$...）的期望值之差不会超过一个很小的量$\epsilon$。这是因为，如果期望值偏差超过 $\epsilon$，这一事件就可以被观察到，而根据 Chernoff 界分析[19]，其概率很小。因此，这样的事件发生意味着，以极高的概率有 $EXEC_{\Pi_{B,\ A,\ Z}} \not\approx EXEC_{\mathcal{F},\ S,\ Z}$；这与 $S \in C_A$相矛盾。因此，对于理想收益 $v_A$，我们有 $E[v_A^{\mathcal{F},S_1,Z_1}] \approx E[\mathcal{R}_{A_1}]$。

利用这一点，我们可以得出结论：$E[v_A^{\mathcal{F},S_1,Z_1}] \geq S(q)r_{block}\theta \geq E[v_A^{\mathcal{F},S_2,Z_2}]$ 以压倒性概率成立。步骤 3b 现在，我们需要证明 $U_A(\Pi,\mathcal{A}_1) + negl(\kappa) \geq U_A(\Pi,\mathcal{A}_2)$。假设这不成立。这意味着存在 $\exists S_2, Z_2$，使得

$$\max_{Z_2 \in ITM}\left\{\min_{S_2 \in C_{A_2}}\left\{E[v_A^{\mathcal{F},S_2,Z_2}]\right\}\right\} \geq$$
$$\max_{Z_1 \in ITM}\left\{\min_{S_1 \in C_{A_1}}\left\{E[v_A^{\mathcal{F},S_1,Z_1}]\right\}\right\}$$

这意味着存在 a $Z_2$，使得 $\forall Z_1$

$$\min_{S_2 \in C_{A_2}} E[v_A^{\mathcal{F},S_2,Z_2}] \geq \min_{S_1 \in C_{A_1}} E[v_A^{\mathcal{F},S_1,Z_1}]$$

但我们已经证明，除非发生可忽略概率的情况，否则这是错误的。这意味着我们的假设是错误的，而实际上，存在 $\forall A_2 \exists A_1$，使得攻击收益安全条件成立。 □

### C.2 定理 6.3 的证明

证明。需要指出的是，我们讨论的是几何递减收敛级数这一方案，因为现有的大多数 PoW 区块链都采用这种级数。不过，该结果对任何收敛的 $<\vartheta>$都成立。

步骤 1（不存在全体诚实时的盈利性）：由于协议最初（启动时）遵循全体诚实时的盈利性，因此在这种情况下，经过若干轮次后，条件 $r_{block}(t)p_{hon}(t)\theta(t) < \chi$ 会变为真。诚实参与者和理性参与者的占优策略是不参与该协议。然而，对攻击者而言，这种情形仍可能有利可图：通过做空加密货币（遵循 $\mathcal{A}_{ahp}$）获利。

$\mathcal{A}_{\overline{ahp}}$

1. 在 ahp[a] 满足的某一轮次，对加密货币建立空头头寸。
2. 当 $ahp, \overline{\beta_{adv}} = 1$ 时，因为所有理性参与者和诚实参与者都退出了该协议。
3. 当 $\beta_{adv} > \frac{1}{2}$ 时，对该协议发起安全攻击，压低加密货币的价值，并从已持有的空头头寸中获利。

[a]全体诚实时的盈利性

步骤 2（全体诚实时的盈利性）：为了证明协议不具备攻击收益安全性，我们需要证明存在一种攻击策略 $A_2$，由模拟器 $S_2$ 在环境 $Z_2$ 中模拟，使得对于任意满足以下等式的环境 $\nexists A_1 \in A_{fr}\, Z_1$

$$E[v_A^{\mathcal{F},S_1,Z_1}] < E[v_A^{\mathcal{F},S_2,Z_2}]$$

这里，所有的 $A_1$、$A_2$、$S_1$、$S_2$、$Z_1$&$Z_2$ 都是 PPT 交互式图灵机[20]。我们考虑任意一种攻击：对手每次查询接受区块的概率为 $p_{attack}$，高于抢先交易半诚实

[19] $Pr[X_{ideal} \geq (1-\epsilon)E[X_{real}]] < exp(-\frac{\epsilon^2 E[X_{real}]}{2})$ [20]概率多项式时间交互式图灵机

矿工 $p_{fr}$。请注意，至少带贿赂的自私挖矿， $p_{attack} > p_{fr}$。由于我们的证明具有一般性，因此考虑任何满足这一条件的攻击。现在，对于攻击策略 $A_2$，它由模拟器 $S_2 \in C_{A_2}$模拟，并进行 $q$次查询，这些查询分布在 $\alpha_{opt}$ 个阶段中。考虑该对手的期望收益

$$E[\mathcal{R}_{A_2}] = \Lambda\theta r_{block} p_{attack} \sum_{i=0}^{\alpha_2 - 1} \vartheta^i - q\chi$$

$$= \Lambda\theta r_{block} p_{attack} \frac{1-\vartheta^{\alpha_2}}{1-\vartheta} - q\chi$$

现在考虑任意一个抢先交易对手 $A_1 \in A_{fr}$，其由 $S_1 \in C_{A_1}$ 和环境 $Z_1$ 模拟；该环境允许对手进行 $q^*$ 次查询，并等待至少一个 HP 输出包含所有对手区块的区块链，然后再停止执行。设在此持续时间内，期望挖出的区块数量为 $\Lambda\alpha_1$。此类对手的期望收益为 $E[\mathcal{R}_{A_1}] = \Lambda\theta r_{block} p_{fr} \sum_{i=0}^{\alpha_1 - 1} \vartheta^i - q^*\chi$，即

$$E[\mathcal{R}_{A_1}] = \Lambda\theta r_{block} p_{fr} \left(\frac{1-\vartheta^{\alpha_2}}{1-\vartheta} + \vartheta^{\alpha_2} \sum_{j=0}^{\alpha_1 \vartheta^j - \alpha_2}\right) - q^*\chi$$

由于 $p_{attack} > p_{fr}$，令 $p_{attack} - p_{fr} = \Delta$。我们希望 $\alpha_{opt}$ 作为最优 $\alpha_2$，使得对于所有 $A_1$， $Z_1$， $A_2$ 的期望收益高于 $A_1$ 的期望收益。由于该结果 $\forall\, Z_1$ 成立，我们考虑一个挖矿成本可忽略不计的环境，因为在此环境中，对手 $A_1$ 可以进行任意次数的查询而无需承担额外成本，并且最适合用于 $A_1$，因为 $q \leq q^*$。此外，由于该条件应当 $\forall\, A_1$ 成立，我们取 $\lim_{\alpha_1 \to \infty}$，由此得到条件

$$(p_{fr} + \Delta)\frac{1-\vartheta^{\alpha_2}}{1-\vartheta} > p_{fr}\frac{1-\vartheta^{\alpha_2}}{1-\vartheta} + \frac{p_{fr}\vartheta^{\alpha_2}}{1-\vartheta}$$

令 $\alpha_{opt}$ 为满足上述条件的最小 $\alpha_2$

$$\Delta\frac{1-\vartheta^{\alpha_2}}{1-\vartheta} \geq \frac{p_{fr}\vartheta^{\alpha_2}}{1-\vartheta} \Rightarrow 1-\vartheta^{\alpha_2} > \frac{p_{fr}}{\Delta}\vartheta^{\alpha_2}$$

$$\Rightarrow \vartheta^{\alpha_2} < \frac{\Delta}{p_{fr}+\Delta} \Rightarrow \alpha_2 log(\vartheta) < log(\frac{\Delta}{p_{fr}+\Delta})$$

由于 $log(\vartheta) < 0$，而我们希望最小化 $\alpha_2$，因此可以说

$$\alpha_{opt} = 1 + \lfloor \frac{log(\frac{\Delta}{p_{fr}+\Delta})}{log(\vartheta)} \rfloor$$

$$E[\mathcal{R}_{A_2}] = \Lambda\theta r_{block} p_{attack} \frac{1-\vartheta^{\alpha_{opt}}}{1-\vartheta} - \Lambda\alpha_{opt}\chi$$

$$E[\mathcal{R}_{A_1}] = \Lambda\theta r_{block} p_{fr} \sum_{i=0}^{\alpha_1} \vartheta^i - q^*\chi$$

$$E[\mathcal{R}_{A_1}] = \Lambda\theta r_{block} p_{fr} (\sum_{i=0}^{\alpha_{opt}} \vartheta^i + (\vartheta^{\alpha_{opt}} \sum_{i=0}^{\alpha_1 - \alpha_{opt}} \vartheta^i)) - q^*\chi$$

步骤 3：取模拟器 $S_2$ 和环境 $Z_2$，使得 $\alpha_2 = \alpha_{opt}$。令 $D = \mathcal{R}_{A_2} - \mathcal{R}_{A_1}$。我们还给差值$(q^* - \Lambda\alpha_{opt})\chi = 0$一个下界。因此，$E[D]$ 的下界为

$$E[D] \geq \Lambda\theta r_{block} \Big( \frac{1-\vartheta^{opt}}{1-\vartheta}(p_{attack} - p_{fr}) + \frac{\vartheta^{opt} p_{fr}(1-\vartheta^d)}{1-\vartheta} \Big)$$

令 $d = \alpha_1 - \alpha_{opt}\,(d \geq 0)$且 $\Delta = p_{attack} - p_{fr}$。

$$\Rightarrow E[D] \geq \Lambda\theta r_{block} \Big( \frac{1-\vartheta^{\alpha_{opt}}}{1-\vartheta}\Delta - \vartheta^{\alpha_{opt}} p_{fr} \frac{1-\vartheta^d}{1-\vartheta} \Big) \geq 0$$

最后一个不等式根据 $\alpha_{opt}$的定义得出。由于我们针对任意 $A_1, Z_1$ 求解了这个问题（通过证明结果对 $\forall\, d \geq 0$成立），因此可以得出， $A_2$ 满足 $S_2$；在环境 $Z_2$ 中模拟它的对象不存在任何 $A_1 \in A_{fr}^{\infty}$，使得对于任意 $Z_1$，$(S_1, Z_1)$都能取得更高的收益。

此外，我们假设 $\Delta > 0$，因此即使存在一种能让对手获得略高挖矿概率的攻击（例如带贿赂的自私挖矿），该协议也并非强攻击收益安全。 □

### C.3 定理 6.4 的证明

证明。 在此定理中，我们证明，任何通缩型区块奖励加密货币都能抵御受限于 $\alpha_{opt}$ 轮次的对抗策略集合，满足攻击收益安全性。也就是说， $\forall\ A \in \mathcal{A}^{\alpha_{opt}}$

$$\alpha_{opt} = 1 + \lfloor \frac{log(1-p_{fr})}{log(\vartheta)} \rfloor$$

考虑任意一个对手 $A_2 \in \mathcal{A}^{\alpha_{opt}}$ 及其环境 $Z_2$，其中该对手进行 $Q = q$ 次查询，满足 $q = maxsupport(P_Q)$。$P_Q$, $Q$ 的定义与引理 6.2 的证明中相同。在这种情况下，设 $q$ 次查询挖出区块，使得对于 $\alpha_2 < \alpha_{opt}$，预期完成 $\alpha_2$个阶段。将每次查询导致挖出区块的概率均取为 1，即可得到对手 $R_{A_2}$ 的收益上界。

$$R_{A_2} \leq \Lambda r_{block} \theta \sum_{i=0}^{\alpha_2 - 1} \vartheta^i = \Lambda \theta r_{block} \frac{1-\vartheta^{\alpha_2}}{1-\vartheta}$$

考虑一个抢先交易半诚实对手 $A_1$ 和一个环境 $Z_1$，该对手在环境停止前进行 $q^*$ 次查询。在这种情况下，设 $p_{fr}$ 为每次查询被接受的概率。考虑 $q^*$，使其预期运行 $\alpha_1$ 轮。关系应满足 $(1-\vartheta^{\alpha_1}) \geq (1-\vartheta^{\alpha_{opt}})\kappa\ (1-\delta)(1-\eta_{max})p_{min}$，其中所有术语的定义均与附录 C.1 中步骤 1b 的定义相同。在这种情况下，对手 $A_1$ 的收益为

$$R_{A_1} \geq \Lambda \theta r_{block} \sum_{i=0}^{\alpha_1 - 1} \vartheta^i - \Lambda \theta r_{block} \frac{1-\vartheta^{\alpha_1}}{1-\vartheta}$$

$$P[R_{A_1} < R_{A_2}] \leq P[\Lambda \theta r_{block} p_{fr} \tfrac{1-\vartheta^{\alpha_1}}{1-\vartheta} < \Lambda \theta r_{block} \tfrac{1-\vartheta^{\alpha_2}}{1-\vartheta}]$$

$$= P[p_{fr} \frac{1-\vartheta^{\alpha_1}}{1-\vartheta} < \frac{1-\vartheta^{\alpha_2}}{1-\vartheta}] = P[\frac{p_{fr}}{1-\vartheta^{\alpha_2}} < \frac{1}{1-\vartheta^{\alpha_1}}]$$

对于每个 $\alpha_2 < \alpha_{opt}$，总是存在这样的 $\alpha_1$；对于某个 $Z_1$，该概率为 1。（注意，我们在 C.2 中计算了 $\alpha_{opt}$，以确保这一点成立。） □

## D 其他细节

### D.1 区块链中的奖励机制

此前的研究已探讨区块链奖励机制，包括 Karakostas 等人 [2022], 和 Badertscher 等人 [2018]。这些奖励机制大致可分为两类：（1）区块奖励机制（BRM）；（2）仅交易费机制（TFOM）。

**区块奖励机制（BRM）**。在区块奖励机制中，挖矿激励通过一种特殊的“coinbase”交易提供。如果每经过有限数量的挖出的区块，区块奖励就会减少，且区块奖励净额之和保持不变，那么这种加密货币就是通缩型的。在比特币中，每挖出 210000 个区块，区块奖励就会减半。与区块奖励相比，BRM 中交易手续费带来的收益非常小，不会导致策略性偏离。

**仅交易费机制（TFOM）**。在 TFOM 中，矿工获得的区块奖励微不足道，收益的主要来源是区块链中所含交易产生的交易手续费。

### D.2 差分效用

本节将说明，将协议描述符的效用建模为偏离与未偏离的参与方之间的效用差异所具有的优势。

以这种方式对效用进行建模，可以涵盖这样一些情况：对手的收益并未显著增加，但却降低了其他参与方每轮的收益。这样一来，对手便能从某一阶段获得更多比例的区块奖励。此外，将效用表示为偏离参与方与未偏离参与方之间的收益差，也更贴合协议描述符的目标，即尽量减少参与方通过偏离协议所获得的收益。

### D.3 Goldfinger攻击

Goldfinger攻击 Bonneau [2018] 是对手持有加密货币空头头寸后发动安全性攻击的一种攻击。在这种情况下，他们会从加密货币兑换率的下降中获利。这可以在对手的收益中建模为

$$v_A = \theta(t)E[R_B] + (\theta_{init} - \theta(t))c_1$$

这里的 $\theta_{init}$ 是建立空头头寸时的代币兑换率。因此，随着 $\theta(t)$ 下降，第二项会增加。Badertscher 等人 [2018] 等先前研究的效用结构中并未对此进行建模。通过对此建模，我们可以论证，即使挖矿无利可图，对手也能通过做空加密货币获得正收益。