不完美 GHOST 类比特币区块链中的顽固挖矿是否危害严重？定量分析

Haoran Zhu、Xiaolin Chang、Jelena Mišić、Vojislav B. Mišić、Lei Han、Zhi Chen

摘要——与最长链协议类似，GHOST 是一种链选择协议，其抵御自私挖矿攻击的能力已在比特币及其变体（类比特币）的不完美区块链中得到验证。本文探讨了一种基于解析模型的方法，用于研究顽固挖矿攻击对不完美 GHOST 类比特币区块链的影响。我们首先基于马尔可夫链量化链动态，随后推导出矿工收益和系统吞吐量的公式。我们还提出了一种新指标"危害指数"，可用于比较攻击严重程度，并帮助攻击者判断发动攻击是否有利可图。实验结果表明：1）算力超过 30 % 的攻击者发动顽固挖矿攻击，能够获得巨额利润，并极大降低系统吞吐量。2）理性的攻击者在算力低于 25% 时不应发动顽固挖矿攻击。3）在 GHOST 下，顽固挖矿攻击造成的损害大于自私挖矿攻击。我们的研究加深了对顽固挖矿攻击的认识，并有助于设计应对措施。

索引词——类比特币区块链、GHOST、工作量证明、定量分析、顽固挖矿攻击。

1 引INTRODUCTION

比特币 [1] 及其许多变体，如莱特币、比特币现金和比特币黄金，均采用工作量证明（PoW）作为区块生成机制，以最长链作为链选择协议，并将矿工的区块生成奖励作为收益。这些区块链统称为**类比特币区块链**，在过去十年间受到金融领域的关注。比特币的价值从2009年的0美元上涨至2022年1月的21,418美元，并在2021 [2]达到66,935美元的峰值。然而，类比特币区块链容易受到各种攻击，进而影响区块链系统的公平性和安全性 [3]-[5]。自私挖矿攻击 [6] 是一种经典攻击，而顽固挖矿攻击 [8] 是其变体（详见第2节.1），会增加区块链面临的危害 [8][9][18]。因此，有必要研究此类威胁性攻击的影响，以防止比特币及类比特币（**比特币**）区块链系统遭受经济损失。

现有的大多数研究仅探讨了理想网络中的自私挖矿和顽固挖矿攻击 [11]-[13][17][18]。然而，实际的区块链网络是**不完美** [15][16][22]。由于网络传输延迟（简称延迟），矿工需要一段时间才能收到新发现的区块。然而，矿工会继续挖矿，直到收到新区块。因此，在一个区块生成间隔内会生成多个有效区块，进而出现分叉现象（详见第2节 2.1）。我们将此称为**非故意分叉**。当前比特币网络中的分叉概率较低（约为 0.5%），因此理想网络中的结果与现实中的比特币并无太大差异。不过，其他 BTC 区块链的分叉概率更高（比特币现金为 1%，莱特币为 1.5% [23]）。理想网络与不完美网络之间仍存在不可忽视的差距。此外，非故意分叉极其有利于攻击者，并会对区块链产生巨大影响 [14]。因此，有必要研究不完美区块链中的攻击。

链选择机制是 BTC 区块链中用于处理分叉的基本组件，默认采用最长链协议；在发生非故意分叉时，该协议只考虑一个区块。矿工选择最长链，并在最高区块之后继续挖矿。也就是说，其他区块会被视为陈旧区块，导致算力浪费。GHOST [10] 是另一种链选择机制，应用于以太坊 2.0 [24]，其变体则用于以太坊经典 [25]。该机制会考虑所有已发布区块，并选择区块数量最多的链。图 1 展示了这两种链选择协议：在最长链协议中，矿工会在"M6"上生成区块；在 GHOST 协议中，矿工则会在"O7"上生成区块。这是因为"M6"比"O7"高一个区块，而"O7"所在的链比"M6"所在的链多两个区块。研究人员已探讨不完美 BTC 区块链中基于 GHOST 的自私挖矿攻击 [16][21]。**在采用 GHOST 作为链选择协议的不完美 BTC 区块链中，顽固挖矿攻击的表现如何？**

上述讨论促使我们开展本文的研究。本文旨在通过构建随机模型，对不完美 GHOST BTC 区块链中的顽固挖矿攻击进行定量分析。已有研究基于模拟分析了最长链协议下的顽固挖矿攻击 [20]。然而，由于链选择协议会同时影响链的演进和矿工行为，这类基于模拟的研究难以扩展到不完美 GHOST 区块链。此外，[22] 中的作者在 GHOST 比特币区块链中进行了模拟，但他们评估了

• *Haoran Zhu* 和 *Xiaolin Chang* 就职于北京智能交通安全与隐私重点实验室，该实验室隶属中华人民共和国北京交通大学。

从矿工收益和系统吞吐量的角度分析顽固挖矿攻击。我们不仅评估这些指标，还通过提出的“危害指数”指标考察攻击严重程度。此外，我们将顽固挖矿攻击与其他经典攻击进行比较，以说明攻击的严重程度。

已有研究提出基于解析模型的方法，用于分析最长链 [14][15] 和 GHOST [16] 下的不完美场景，但仅针对自私挖矿。尽管顽固挖矿攻击是自私挖矿的一种变体，矿工的行为却有所不同，从而产生了自私挖矿解析模型中不存在的额外系统状态。值得注意的是，[16] 的工作也研究了顽固挖矿模型。但他们的模型遗漏了一些关键状态和状态转移，因此只能描述T_1-顽固挖矿（详见第2.1节）。他们没有给出顽固挖矿攻击的指标公式，而且其计算指标的方法难以应用于顽固挖矿。此外，研究人员还建立了解析模型，研究最长链区块链遭受顽固挖矿攻击时的情况 [17]-[19]。这些解析模型很难（甚至不可能）用于 GHOST。

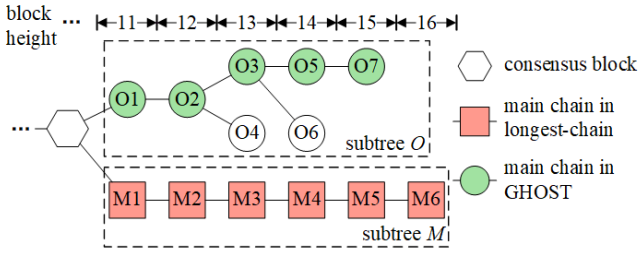


图1 GHOST 与最长链协议

在不完美的 GHOST BTC 区块链中，对顽固挖矿攻击进行基于模型的分析至少面临三项主要挑战（详见第3.1节）。本文的主要贡献总结如下。

- 我们采用连续时间马尔可夫链技术建立分析模型，以量化不完善 GHOST BTC 区块链的演化与动态。我们的模型适用于比特币及大多数类比特币区块链系统，这些系统满足以下条件：a) 使用工作量证明作为区块生成机制；b) 矿工通过生成有效区块获取收益；c) 存在由网络导致的分叉；d) 使用 GHOST 解决分叉。据我们所知，我们是首个对存在意外分叉的 GHOST 区块链中的顽固挖矿攻击进行建模和分析的研究者。

- 我们建立了计算所有顽固挖矿攻击策略下矿工收益和系统吞吐量的公式，可用于评估其对 GHOST 比特币区块链系统的影响。只有共识区块会获得奖励，且仅考虑共识区块中的交易。然而，有效区块是否会成为共识区块，取决于所有矿工的行为。攻击者会根据不同的顽固策略采取不同的行为。现有研究难以计算收益和吞吐量。我们创新性地推导出中间变量“子树选择概率”的公式，从而能够计算这些指标。据我们所知，我们是首个在不完美 GHOST 场景下，推导出所有顽固挖矿攻击策略相关指标公式的研究者。

- 我们提出一种名为“**危害指数**”（HI）的新指标，即单位算力带来的额外相对收益，用于评估攻击的威胁严重程度。现有研究 [11]-[21] 使用相对收益率（RR）评估攻击者的利润和攻击严重程度。然而，较高的 RR 可能是由更大的算力造成的。也就是说，除非攻击者的算力固定，否则 RR 无法用于比较不同攻击策略的威胁严重程度。此外，RR 无法告知攻击者实施攻击能获利多少。第4节 4.3.3 中的实验结果证明了 HI 的有效性。

本文其余部分安排如下：第2节介绍背景和相关工作。第3节描述所研究系统的分析模型和度量公式。第4节给出实验结果。第5节总结全文并讨论未来工作。

2 PRELIMINARIES

2.1 背景

工作量证明（PoW）。 在 PoW 区块生成机制中，当基于哈希的谜题得到解答时，就会生成一个**有效区块**。矿工找到有效区块的概率与其算力成正比 [6][8]。两个相邻区块之间的时间称为**区块生成间隔**。比特币的平均区块生成间隔为 10 分钟 [1]，而莱特币为 2.5 分钟 [7]。

奖励机制。 这是 BTC 区块链的一项基本功能。矿工的区块获得所有矿工的共识后，便会获得区块生成奖励。得到所有矿工认可的区块称为**共识区块**。共识区块的矿工可获得一个单位的奖励。从**创世区块**（区块链的第一个区块）到最新共识区块的链称为**主链**，主链上的所有区块称为**主区块**。**高度**表示从该区块到创世区块之间的区块数，而**距离**是区块高度之差。

我们用图1来说明上述概念。此时已有10个共识区块，因此“M1”和“O1”的高度为11。“M1”与“M3”之间的距离为2。类似地，“M1”与“O7”之间的距离为4。链的**长度**是该链中的最大区块高度。在采用最长链协议的区块链中，红色链最长，因此它是主链。区块的**权重**是连接在该区块之后的区块数量。区块权重为0时，该区块就是叶区块。在图1中，“M2”的权重为4，“O2”的权重为5。“O4”、“O6”、“O7”和“M6”是叶区块。不过，在最长链协议中，诚实矿工只会在“M6”上挖矿；而在GHOST中，他们只会在“O7”上挖矿。

叶区块特指HPs可以在其上挖矿的区块，除非另有说明。在GHOST中，所有有效区块构成一个有向无环图，形成树结构。共识区块之后的有效区块也构成若干个**子树**（例如，包含“O1” ~ “O7”的子树O）。子树根的权重也就是该子树的权重。子树O比子树M更重，因此O的根（“O1”）所在的绿色链是主链。我们将攻击者挖矿所在的子树称为**私有子树**，其他子树则称为**公共子树**。

矿池。在总算力极大的区块链中，单个矿工很难找到工作量证明解 [26]。矿工只有在产生共识区块后才能获得收益。因此，矿工以矿池的形式聚集算力。一个矿池中有一名管理者和许多矿池矿工。管理者决定矿池矿工在哪个区块上挖矿，并发布矿池矿工产生的有效区块。矿池矿工不能在其他区块上挖矿，否则会被发现存在不诚实行为并被移出矿池。收益由所有矿池矿工平分。换言之，如果一名矿池矿工生成了一个共识区块，所有矿池矿工都能获得收益，且所有矿池矿工的总收益为一个奖励单位。

顽固挖矿攻击。这是 [8] 提出的一种自私挖矿攻击变体。[22] 给出了不完美 GHOST 区块链中的策略。共有 3 种基本策略：领先（Lead，***L***）、平分叉（equal-Fork，***F***）和落后（Trail，***T***）；以及 4 种混合策略：领先-分叉（Lead-Fork，*LF*）、领先-落后（Lead-Trail，*LT*）、分叉-落后（Fork-Trail，*FT*）和领先-分叉-落后（Lead-Fork-Trail，*LFT*）。攻击者可以采用其中任意一种策略发起顽固挖矿攻击。注意，*T* 策略是一个策略族。当私有子树落后于公共子树 j 个区块时，恶意矿池仍会尝试在私有子树上生成区块，希望追上公共子树，这种策略记为 T_j 策略。我们只研究 T_1 策略，因为它是*T*策略族中的主导策略[8].

令 Δ 表示私有子树与最重公共子树之间的权重差。 表示私有子树和公共子树的权重相同。如果 ，则子树的权重可以为 0（矿工在共识区块上挖矿），也可以为正数（两个子树都存在，并将 记作 0’）。 以下介绍三种基本策略在自私挖矿攻击中的区别。

$\Delta = 0$

$\Delta = 0$

- *L* 策略：攻击者仅在 且诚实矿工生成一个区块时，才发布第一个私有区块。 $\Delta = 2$
- *F* 策略：如果 且攻击者生成下一个区块，则不发布该区块。 $\Delta = 0$
- *T* 策略：如果 且诚实矿工在公共子树中创建区块，攻击者仍在私有子树上挖矿。如果 且攻击者生成一个区块，两条链的权重相等。然而，所有诚实矿工一直在公共子树上挖矿，我们用 表示这种情况。 $\Delta = 0$ $\Delta = -1$ 0"

自私挖矿攻击中的攻击者行为（下文记为“*S*”）以及顽固挖矿攻击的 3 种基本策略汇总于表1，其中斜体表示不同的行为。这些行为混合策略则是由基本策略中的不同行为组合而成。

2.2 相关工作

自私挖矿攻击。自从 [6], 提出自私挖矿攻击以来，许多研究都致力于探讨其对区块链系统的影响。Davidson等人 [11] 基于仿真研究了不同难度调整算法下自私挖矿的盈利能力。Lee等人 [12] 通过状态机从矿池收益的角度研究了自私挖矿。Ai等人 [13] 提出了一种优化的自私挖矿攻击 ESM，并通过仿真和状态机评估相对收益。[11]-[13] 的研究结果是在不存在意外分叉的理想网络中得出的。

[14][15] 的作者讨论了非理想网络中的自私挖矿。他们基于马尔可夫链模型，研究了比特币中矿池相对收益和系统吞吐量。上述研究均探讨了采用最长链协议的区块链。Yang等人 [16] 建立了一个关于非理想 GHOST 区块链中自私挖矿的马尔可夫链模型，并对 GHOST 与最长链协议进行了比较。这是目前唯一一项与我们的研究较为接近的工作。他们还探索了对顽固挖矿攻击进行建模的方法。但他们的模型遗漏了一些关键系统状态，且缺少许多状态转换，因此只能捕捉 *T* 策略。他们没有推导顽固挖矿攻击的指标公式。此外，他们计算自私挖矿指标的方法也难以应用于顽固挖矿攻击。

完美网络中的顽固挖矿攻击。作为自私挖矿的一种变体，顽固挖矿攻击也吸引了许多研究者。Grunspan等人 [17] 通过应用状态机，研究了完美网络中的*L*和*F*策略。[18] 中的作者从攻击者的相对收益、陈旧区块率、吞吐量和安全性指标等角度评估了顽固挖矿攻击。他们构建了马尔可夫链，并推导出指标公式。Xia等人[21] 通过模拟研究了GHOST中的顽固挖矿攻击，并考察了完美网络中自私挖矿和*LFT*策略的性能。这些研究均基于理想网络假设，因此可能与现实存在差距。

不完美网络中的顽固挖矿攻击 Wang等人 [19] 对不完美 PoW 以太坊中的自私挖矿攻击、*T* 和 *FT* 策略进行了建模。他们重点研究了叔块奖励（以太坊独有的一种奖励机制），并省略了与叔块奖励无关的一些状态转移。他们对“不完美”的定义与我们的不同。矿工确实会产生分叉，但会根据时间戳选择区块。同一代际间隔内的区块只有在时间戳最早时才能成为主区块。换言之，他们的研究基于一个隐含假设：大多数矿工拥有理想网络，少数矿工存在连接错误，因此整个网络是不完美的。我们研究的是全局不完美网络，其中所有矿工都会产生分叉，且每个区块都有概率成为主区块。Liu等人 [20] 通过模拟研究了

表1GHOST BTC 区块链中的自私挖矿与顽固挖矿攻击基本策略

	攻击者发现一个区块				诚实矿工在公共子树中找到i个区块（i>0）诚实矿工在私有子树中找到区块							
状态	Δ≥0	Δ=0’	Δ=0''	Δ=-1	Δ≥i+2	Δ=i+1	Δ=i	Δ=i-1	Δ≤i-2	Δ>0 和 Δ≠2	Δ=2	Δ=0
S	hold	发布	-	-	发布 i	全部发布	发布 all	我的 PB	我的 PB	发布 1	全部发布	在新区块上挖矿 在 pri 中
L		发布				发布 i					发布 *1*	
F		*hold*				全部发布					全部发布	
T		发布	发布	发布		全部发布		挖矿优先级			全部发布	

* *“pb”*表示公共子树，*“pri”*表示私有子树。

表2符号说明的定义

符号说明	定义
Δ	私有子树与 最重公共子树之间的权重差。
Hs	HPs 生成的子树数量。
N	HPs 可以挖矿的叶区块数量。
θ	非故意分叉的概率。
α, β	恶意矿池和 HPs 的总算力，分别为 。它们也分别表示恶意矿池和 HPs 生成 区块的速率。
β^{12}, β	HPs 在一个区块生成间隔内生成一个区块和两个区块的速率 分别为一个区块生成间隔。 ， $\beta_2 = \beta \cdot \theta$ $\beta = \beta_1 + 2\beta_2$.
$P_{\beta 1}$	HPs 生成一个区块的概率。 $(\ )_{\beta 1} = \beta\ 1-$.
γ_n	当私有 子树中有 n 个叶区块时，HPs 生成一个区块的概率。
g_N^M	当 M* 上的 叶区块数量为 N 时。
$(,,)_A P_{HsN\Delta}$	私有（攻击者的）第一个区块的概率 当系统处于该状态时，子树成为主区块 处于状态 $(,,)HsN\Delta$
$(,,)_H P_{HsN\Delta}$	公共子树（诚实矿工的）第一个区块成为主区块的概率—— 工的）子树成为主区块时，系—— 统处于状态 。 $(,,)HsN\Delta$
$(,,)Hs\ N\pi\ \Delta$	状态 的稳态概率。 $(,,)HsN\Delta$
$_{H}EF_{,}^{M}$	恶意矿池和 HPs 的收益期望，分别为。
$_{,}{}^{M}{}_{H}$相对收益率 相对收益率	恶意矿池和 HPs 的相对收益，分别为。
TPS	每秒交易数。

* *M∈{A, AH, H, H1, H2}* 表示分叉场景。*A*、*AH*、*H*、*H1* 和 *H2* 分别表示 *HPs* 在攻击者的子树（私有子树）后方生成两个区块、攻击者的子树和一个诚实子树（公共子树）、诚实子树、一个诚实子树以及两个诚实子树。

$_{H}g^{3}g^{3}g = {}_{3}{}^{1} + {}_{3}{}^{2}\ {}^{H}$

顽固挖矿对不完美 PoW 以太坊的影响。以上所有工作均基于最长链协议。

[22] 中的作者提出了不完美 GHOST 区块链中的顽固挖矿攻击策略，并评估了矿工收益和系统吞吐量。我们不仅评估这些指标，还通过危害指数研究攻击严重程度。我们将顽固挖矿攻击与其他经典攻击进行了比较。然而，模拟方法必须精确还原现实，并且存在实验轮次多、结果不稳定的问题。

总而言之，现有研究要么考察最长链协议中的顽固挖矿攻击，要么考察 GHOST 中的部分顽固挖矿策略，要么仅通过模拟得出结果。此外，即使并非完全不可能，现有模型也难以用于分析我们所研究场景中的全部 7 种顽固挖矿策略。本文通过马尔可夫链模型，研究不完美 GHOST 比特币区块链中全部 7 种顽固挖矿攻击策略的影响。我们还构建了一个模拟器，以交叉验证研究结果。

3 系YSTEM 统ESCRIPTION 描ODEL述

本节首先在第3.1节介绍待研究的系统以及定量分析面临的挑战。随后分别在第3.2节和第3.3节给出模型和公式。表2列出了下文将使用的符号说明。

3.1 系统描述

比特币区块链采用工作量证明作为区块生成机制，并采用 GHOST 作为链选择协议。网络并不完善，因此可能出现意外分叉。矿池通过区块生成奖励获得收益。

矿工分为恶意矿工和诚实矿工两类。所有恶意矿工串通起来，组成一个恶意矿池（MP）。其余矿工（即诚实矿工）组成若干诚实矿池（HPs）。MP 发起顽固挖矿攻击，并能迅速检测到其他矿池生成的新区块，还能借助日蚀攻击和网络嗅探传播自己的区块 [8][20]。因此，可以合理且可行地假设 MP 连接良好，且不会发生意外分叉。HPs 采用诚实挖矿策略挖掘区块，具体如下。

- 矿池会持续在自己认为权重最大的子树上挖掘区块。• 矿池一旦找到区块便立即发布。也就是说，矿池不会扣留任何区块。• 由于网络不理想，矿池可能会产生非故意分叉。换言之，在一个区块生成间隔内至少会生成一个区块。• 矿池依据 GHOST 解决分叉。当存在多个权重相同的子树时，如果其中有包含自己区块的子树，矿池就会选择该子树；否则，矿池会随机选择一棵子树。算力是矿池的一项关键属性，它

决定了矿池在工作量证明系统中生成区块的概率。在 BTC 区块链中，区块生成概率与算力成正比。事实上，BTC 区块链中最大型矿池的算力约为 17%~30% [26]。算力超过一半的矿池可以发动双重支付攻击并获取全部收益，因此没有必要对此进行研究。此外，现有研究表明，算力较低的小型矿池发动顽固挖矿攻击并无收益[8][18]。为使我们的研究全面且有意义，我们研究矿池算力介于 5% 至 45% 的情形。结果可以展示顽固挖矿攻击对大型矿池带来的利润，以及对小型矿池造成的损失。我们所考虑的系统有若干假设。

- 系统中的总算力保持不变，所有矿工都持续挖掘区块。
- 系统中只有一组攻击者，他们只实施顽固挖矿攻击。• 系统中不存在独立矿工。单个矿工可视为由一名矿工组成的小型矿池，其中池内矿工同时也是管理者。• 由于三链分叉发生的概率较小，因此不会同时创建超过两个区块[27]。因此，当发生非故意分叉时，HPs 会生成两个新区块。

系统建模和公式计算至少面临以下挑战。

挑战 1。 MP 与 HPs 的行为相互关联。MP 在不同的顽固策略下表现不同。如何在一个模型中量化二者之间的交互，是第一个挑战。

挑战 2。 当 HPs 生成分叉时，两个新生成的区块可能位于不同的子树或同一子树中。这些区块也可能位于公共子树或私有子树中。这些情况随机组合，从而形成不同的区块链结构。如何刻画这些情形，是第二个挑战。

挑战 3。 在最长链协议中，恶意矿池发起自私挖矿攻击，在某些情
情况（例如 以及 HPs 找到区块）。然而，这些情况在 GHOST 中并未完全成立。顽固挖矿攻击会使系统发生分叉，而非达成共识。系统发生分叉后，难以准确计算收益。如何计算 GHOST 中顽固矿池的收益是一项巨大挑战。

3.2 系统模型

本节介绍 GHOST 比特币系统中顽固挖矿攻击下链动态的分析模型。符号说明和定义汇总于表2。

我们假设区块生成时间服从指数分布，与 [13]-[16]中的设定相同。使用三元组 表示系统状态:
( ) ,HsNΔ

- Δ 表示私有子树与最重公共子树之间的权重差。这是一个关键因素，决定了攻击者的行为。
- *Hs* 表示 HPs 生成的子树数量，也表示公共子树的数量。由于“”不完美”“这一特性，HPs 可以生成多个公共子树。矿池可以在任意子树上挖掘区块，这意味着算力分散，并有利于攻击者。请注意，子树定义为共识区块之后的分支。因此，可能为 0，表示共识区块之后 HPs 未生成新区块。

Hs

- *N* 表示矿池可以在其上挖矿的区块数量，包括私有子树上的区块、公共子树上的区块以及共识区块。

根据第3节 1 中的假设，，，。且 。以下列出元组所满足的约束 {0,1,2}*Hs* ∈ {1,2,3}*N* ∈

1) 恶意矿池只在私有子树上生成区块，且不会产生非故意分叉。因此，只有一棵私有子树，且其上只有一个叶区块。2) 由于子树中至少存在一个区块，。 3) 发生非故意分叉时会生成两个新区块，。4) 在*T*策略中，即使公共子树的权重大于私有子树，恶意矿池仍坚持在私有子树上挖矿。在这种情况下，所有诚实矿池都在公共子树上挖矿，且无法看到私有子树。 尽管私有 *N Hs*≥ 2

N Hs=

子树已发布。

图2展示了状态转移图，其中图2(a)中黑色虚线框内的细节在图2(b)中呈现。下面介绍如何计算图2中的转移率。不同 BTC 区块链的系统总算力差异很大（比特币为 286.56 Eh/s，比特币现金为 1.49 Eh/s [26]）。不同 BTC 区块链的区块生成率也有所不同（比特币为 1/600，莱特币为 1/150）。不失一般性，我们将系统的区块生成率和总算力归一化为 1。也就是说，平均每个时间单位可生成一个区块。我们将产生非故意分叉的概率定义为。 并且分别表示恶意矿池和诚实矿池的总算力。它们也分别表示恶意矿池和诚实矿池生成区块的速率。。回想一下，区块生成率总和为 1，且恶意矿池不会产生分叉。因此，矿池生成两个区块的速率为 ，所有矿池生成一个区块的总速率为 。 θ α β α + β = 1

$$\beta_2 = \beta \cdot \theta$$

$$_1 = 1 - 2\beta_2$$

顽固挖矿攻击中有 7 种不同的策略，因此状态转移也各不相同。在图 2 中，有些线分成两段，其中一段标有一个字母。例如，状态 (2,2,3) 沿绿色线转移到 (0,0,1)，并沿标有“*L*”的绿色线转移到 (1,1,2)。这表示如果攻击者采用*L**策略（即 *L*、*LF*和*LFT*），状态 (2,2,3) 将以的速率转移到 (1,1,2)。否则，状态 (2,2,3) 将以相同的速率转移到(0,0,1)。类似地，如果恶意矿池采用 策略*L**，状态 (2,1,2) 将以 的速率转移到 (1,1,2)，否则将以相同的速率转移到 (0,0,1)。 β β β1

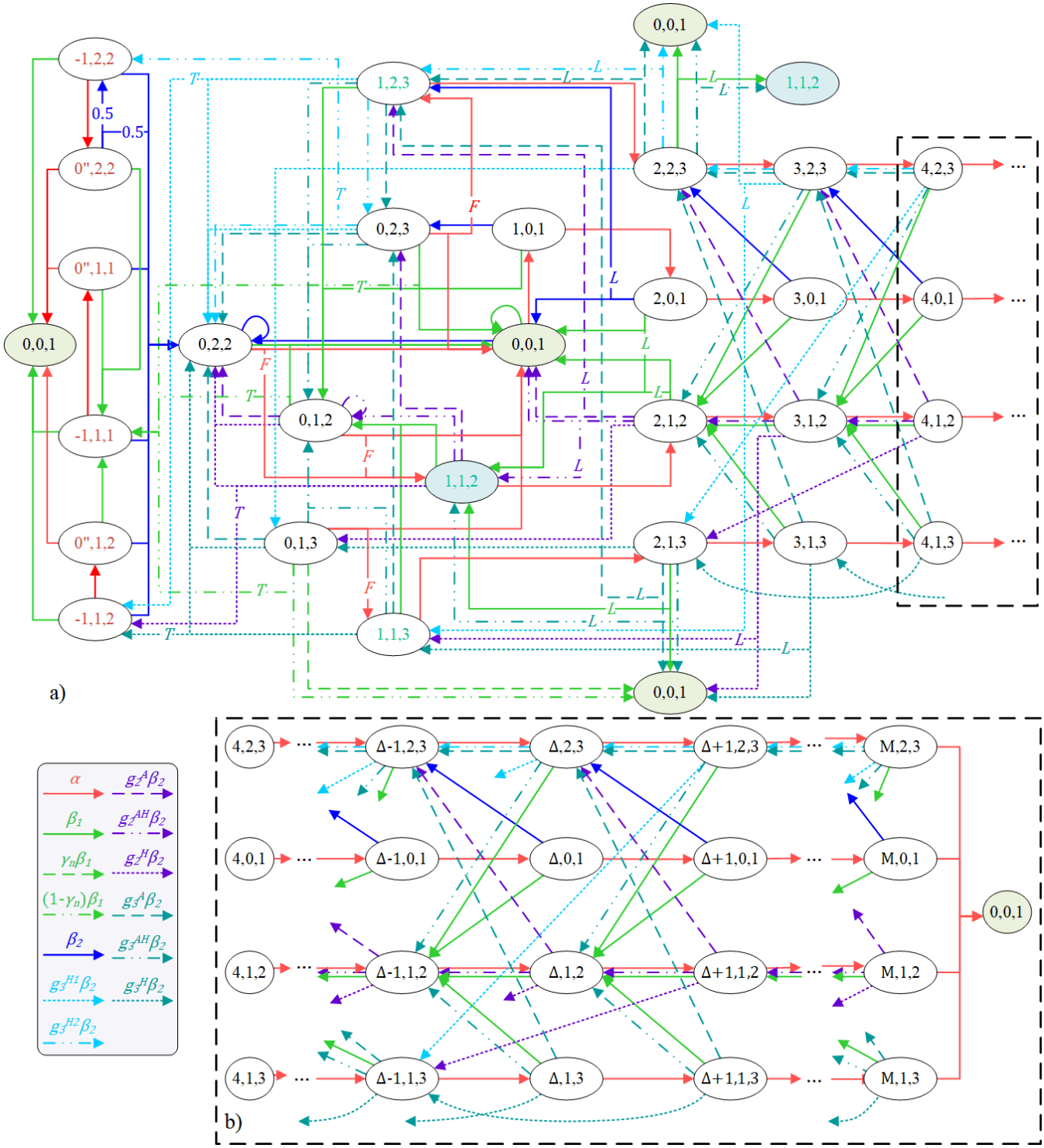


图 2 状态转移图

3.3 度量公式

令 表示状态的稳态概率。我们可以通过求解全局平衡方程，得到所有状态的稳态概率，并利用结果计算各项指标。本节首先计

算 GHOST 比特币链中恶意矿池和诚实矿池的收益。然后，我们使用这一指标来计算矿池相对收益、每秒交易数以及顽固挖矿攻击的危害指数。

3.3.1 矿池收益

矿池收益是预期值的加权平均

各系统状态下的矿池收益。权重为各状态的稳态概率。我们考虑每种状态下的所有区块生成事件（记为)），包括恶意矿池生成区块、HPs 生成区块，以及 HPs 生成两个区块。恶意矿池的收益（记为) ）和 HPs 的收益（记为) 可以通过公式 (1)-(2) 得出。

$$E_{\mathrm{M}}=\sum_{(\Delta,Hs,N)}\pi\left(\Delta,Hs,N\right)\sum_{x}G\left(x\right)\cdot n\cdot P_{A}\left(S\left(x\right)\right) \tag{1}$$

$$E_{H}=\sum_{(\Delta,Hs,N)}\pi\left(\Delta,Hs,N\right)\sum_{x}G\left(x\right)\cdot n\cdot P_{H}\left(S\left(x\right)\right) \tag{2}$$

其中 $G(x)$ 是区块生成事件 的发生率， 是矿池发布的区块数， 而 是子树选择概率，且 是事件 发生后的新系统状态。

现在给出子树选择概率的定义和计算方法，它是公式 (1)–(2) 中唯一未知的变量。当同时存在公共子树和私有子树时，只有其中一棵子树可能是最大的子树，且该子树的第一个区块会成为共识区块。我们将某棵子树的第一个区块成为共识区块的概率称为子树选择概率。设 和分别表示私有子树（攻击者）和公共子树（HPs）中第一个区块在状态下成为主区块的概率。。在公式 (3) 中定义，用于辅助计算子树选择概率。子树选择概率的计算公式见**命题 1**。

命题 1。 子树选择概率可推导如下

by solving Eqs. (3)-(4).

$$\begin{cases}
Pb(0,1,N)=P_{\beta1}(\gamma_N+(1-\gamma_N)P_A(-1,1,N-1)T)+\beta_2(g_N^A+g_N^{AH}P_A(0,1,2))\\
Pb(1,1,N)=P_{\beta1}(\gamma_N+(1-\gamma_N)P_A(0,1,2))+\beta_2(g_N^A+g_N^{AH}+g_N^HP_A(-1,1,N-1)T)\\
Pb(2,1,N)=P_{\beta1}(\gamma_N+(1-\gamma_N)((1-L)+P_A(1,1,2)L))+\beta_2(g_N^A+g_N^{AH}+g_N^HP_A(0,1,3))\\
Pb(3,1,N)=P_{\beta1}(\gamma_N+(1-\gamma_N)P_A(2,1,2))+\beta_2(g_N^A+g_N^{AH}+g_N^H((1-L)+P_A(1,1,3)L))\\
Pb(\Delta,1,N)=P_{\beta1}(\gamma_N+(1-\gamma_N)P_A(\Delta-1,1,2))+\beta_2(g_N^A+g_N^{AH}+g_N^HP_A(\Delta-2,1,3))\\
Pb(0,2,3)=P_{\beta1}(\gamma_3+(1-\gamma_3)P_A(-1,1,1)T)+\beta_2(g_3^A+g_3^{AH}P_A(0,1,2)+g_3^{H2}P_A(-1,2,2)T)\\
Pb(1,2,3)=P_{\beta1}(\gamma_3+(1-\gamma_3)P_A(0,1,2))+\beta_2(g_3^A+g_3^{AH}+g_3^{H2}P_A(0,2,3)+g_3^{H1}P_A(-1,1,2)T)\\
Pb(2,2,3)=P_{\beta1}(\gamma_3+(1-\gamma_3)((1-L)+P_A(1,1,2)L))+\beta_2(g_3^A+g_3^{AH}+g_3^{H2}((1-L)+P_A(1,2,3)L)+g_3^{H1}P_A(0,1,3))\\
Pb(3,2,3)=P_{\beta1}(\gamma_3+(1-\gamma_3)P_A(2,1,2))+\beta_2(g_3^A+g_3^{AH}+g_3^{H2}P_A(2,2,3)+g_3^{H1}((1-L)+P_A(1,1,3)L))\\
Pb(\Delta,2,3)=P_{\beta1}(\gamma_3+(1-\gamma_3)P_A(\Delta-1,1,2))+\beta_2(g_3^A+g_3^{AH}+g_3^{H2}P_A(\Delta-1,2,3)+g_3^{H1}P_A(\Delta-2,1,3))
\end{cases} \tag{3}$$

$\Delta\geq4$

$$\begin{cases}
P_A(0,Hs,N)=Pb(0,Hs,N)+\alpha(1-F)\\
+F\sum_{i\geq1}\alpha^i\cdot Pb(i,Hs,N)\\
P_A(\Delta,Hs,N)=Pb(\Delta,Hs,N)+\alpha P_A(\Delta+1,Hs,N)(1-F)\\
+F\sum_{i\geq1}\alpha^i\cdot Pb(i+\Delta,Hs,N)\\
P_A(0'',1,1)=\alpha/(1-P_{\beta1}\alpha)\\
P_A(0'',2,2)=\alpha/\left(1-(P_{\beta1}+1/2\beta_2)\alpha\right)\\
P_A(0'',1,2)=\alpha/(1-P_{\beta1}\alpha)\\
P_A(-1,1,1)=\alpha^2/(1-P_{\beta1}\alpha)\\
P_A(-1,2,2)=\alpha^2/\left(1-(P_{\beta1}+1/2\beta_2)\alpha\right)\\
P_A(-1,1,2)=\alpha^2/(1-P_{\beta1}\alpha)\\
\Delta\geq0,(Hs,N)\neq(0,1)
\end{cases} \tag{4}$$

其中 表示 HPs 生成区块的概率，是恶意矿池策略的标志变量。若攻击者采用相应策略，其值为 1；否则为 0。例如，如果恶意矿池采用LT策略，，，。

3.3.2 矿池相对收益

恶意矿池（MP）收益的增加并不意味着诚实矿池（HPs）收益会减少，反之亦然。总收益会随攻击和分叉概率而变化。因此，我们计算矿池的相对收益（RR），以衡量发起顽固挖矿攻击所获得的收益。矿池相对收益定义为该矿池收益占所有收益的比例。若恶意矿池（MP）的相对收益（() 增加，则诚实矿池（HPs）的相对收益（ ）会增加。式（5）可计算和。

$$\begin{cases}
R_T=E_M+E_H\\
RR_M=E_M/R_T\\
RR_H=E_H/R_T
\end{cases} \tag{5}$$

3.3.3 每秒交易数

与 [14] 和 [15], 类似，我们使用每秒交易数（TPS）来评估系统吞吐量。在 BTC 区块链中，只有主区块中的交易才会计入。每个区块中的交易数量几乎恒定[26], ，因此可以根据常规区块生成率评估 TPS。由于每次常规奖励都意味着生成一个主区块，我们可以通过常规奖励计算常规区块生成率。由于每个 BTC 区块链的主区块中的交易数量各不相同，我们假设一个主区块中只有一笔交易，这一点不同于 [14] 和 [15]。因此，最大 TPS 为 1。

3.3.4 危害指数

我们提出危害指数（危害指数）（HI），即单位算力的额外相对收益，用于量化攻击的严重程度。HI 定义为额外相对收益与诚实挖矿相对收益之比。设 表示攻击者诚实挖矿时的相对收益，表示攻击者算力所占的比例。攻击者的诚实挖矿相对收益等于

其算力的比例。公式（6）给出了计算危害指数的公式。

$$HI = \frac{RR_M - RR_{HM}}{RR_{HM}} = \frac{RR_M - C_M}{C_M} \tag{6}$$

I 的取值范围为 。 当矿工诚实行事时，I 为 0，表示不会对系统造成危害。当矿工发起攻击并获得额外利润时，HI 为正值，这会损害系统公平性和安全性。当矿工损失其应得收益时，HI 可能为负值。HI 为负并不意味着获益或不会对系统造成损害，而是表示攻击者不发起攻击的概率。HI 越大，表示奖励率越高，也意味着攻击严重程度越高。尽管 HI 仍与攻击者的算力有关，但二者呈负相关。

现有研究 [8][9][12]-[16] 使用 RR 评估攻击者的利润和攻击严重程度。如果 ，攻击者会发起攻击以获得额外利润，且该攻击会危害区块链系统。如果 ，攻击者 不会发起攻击。与之间的差值表示攻击者的 损失。RR 无法进行比较，而 HI 可以直接比较的原因如下。

- 如果小型矿池和大型矿池通过发起攻击获得相同的相对收益率（RR），那么小型矿池获得的额外收益比大型矿池更多。小型矿池的危害指数（HI）高于大型矿池。• 如果两个矿池通过发起攻击获得相同的危害指数（HI），那么小型矿池的相对收益率（RR）低于大型矿池，但两个矿池的奖励率相同。

大型矿池的相对收益率（RR）自然高于小型矿池。因此，相对收益率（RR）的上升可能是由更高的算力或攻击本身造成的。也就是说，除非固定攻击者的算力，否则无法使用相对收益率（RR）比较不同攻击策略的威胁严重程度。相反，危害指数（HI）反映了攻击严重程度，可以直接用于比较。

4 实验结果

本节首先在第4.1节介绍参数设置，然后在第4.2节展示模型和公式的近似准确性。第4.3节从攻击者

盈利能力、系统TPS和危害指数。第4.4节给出了将顽固挖矿攻击与其他攻击进行比较的实验结果。

4.1 系统和参数配置

如第3.1节所述，恶意矿池的算力从 5%（0.05）变化到 45%（0.45）。比特币、比特币现金和莱特币最近的 2016 个主区块表明，这些比特币区块链的分叉概率约为 0.6%~1.2% [23][26]。尽管这些区块链生成区块只需几分钟，但也有工作量证明区块链能在几秒内生成区块，例如 PoW以太坊和 Bitcoin Fast。它们的分叉概率较高，约为 5% [14][15]。为全面研究区块链系统，我们将分叉概率 设为 0.5%、1%（低分叉概率）、5%、10%（高分叉概率）和 20%（极高分叉概率）。其他参数设置见表 3。数值实验使用 MAPLE

[28].

表3 参数设置

符号	设置	符号	设置
γ_n	$1/n$	g_3^A	γ_3^2
g_2^A	γ_2^2	g_3^{AH}	$(2\gamma_3(1-\gamma_3$
g_2^{AH}	$(2\gamma_2(1-$	g_3^H	$(1-\gamma_3^2$
g_2^H	$(1-\gamma_2^2$		$(1-\gamma_3^2/(1-\gamma_3$

4.2 模型与公式验证

我们从相对收益率的两个方面验证所提出的模型和公式：1）与现有研究进行比较；2）与仿真结果进行比较。

文献综述表明，只有文献[16] （以下简称 Yang模型）与我们的工作相似。我们复现了该研究中的实验，并将结果与我们的工作进行比较。Yang模型仅考虑了不完善 GHOST区块链系统中的自私挖矿攻击。我们的模型和公式也可以评估自私挖矿攻击，而 Yang模型可视为我们系统的一个特例。通过设置 L、F、T

$= 0$, ,

0 0

并将我们模型的其他参数设置为与 Yang 相同，我们可以得到 Yang 的结果。我们的结果与 Yang 的结果的比较见图 3。“RRM”和“RRH”分别表示恶意矿池和 HPs 的相对收益率。“-num”和“-Yang”分别表示我们模型和 Yang模型的结果。散点几乎完全落在曲线上，表明我们的结果与 Yang 的结果相同，从一个方面验证了我们模型的近似准确性。

为了在更一般的场景中验证我们的模型和公式，我们使用C语言开发了一个模拟器，并开展了一系列仿真实验。每轮仿真都会创建一条包含 1000 万个主链区块的区块链，并针对每组参数进行 100 轮仿真。受篇幅所限，我们仅给出自私挖矿攻击和 *LFT* 策略的结果。其他顽固策略的结果也类似。图 3 和图 4 展示了结果，其中“-sim”表示仿真结果。我们观察到，在不同的分叉概率下，数值结果与仿真结果都非常接近。这些结果表明，我们的模型和公式具有较高的近似准确性，进而验证了定量分析方法的正确性。

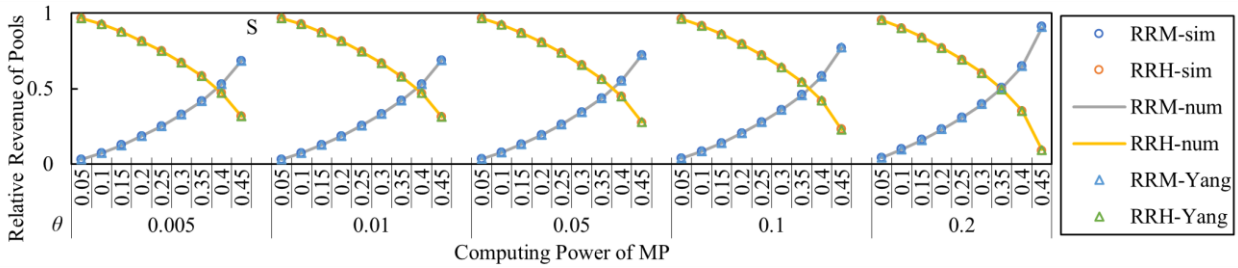


图3 自私挖矿下对我们的模型和公式进行验证

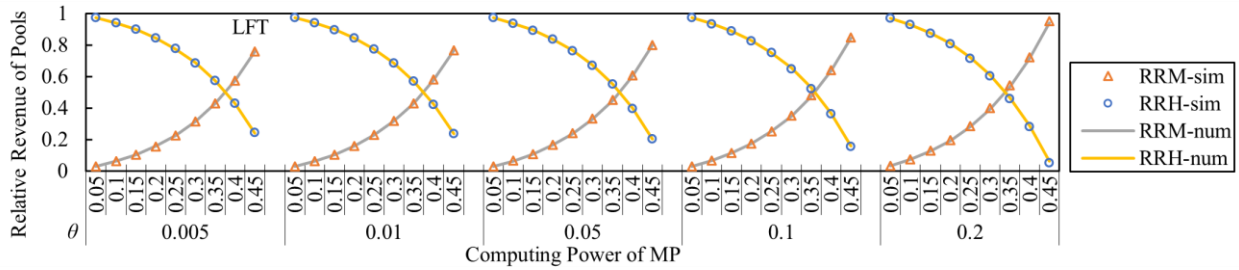
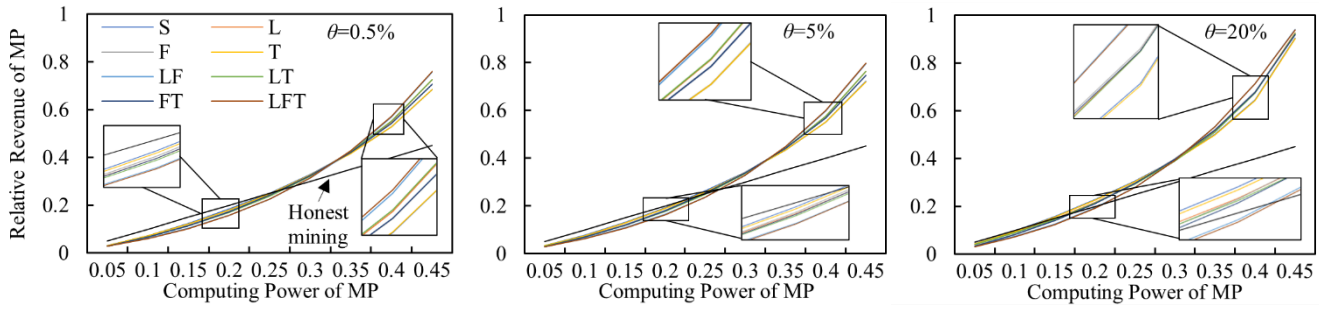
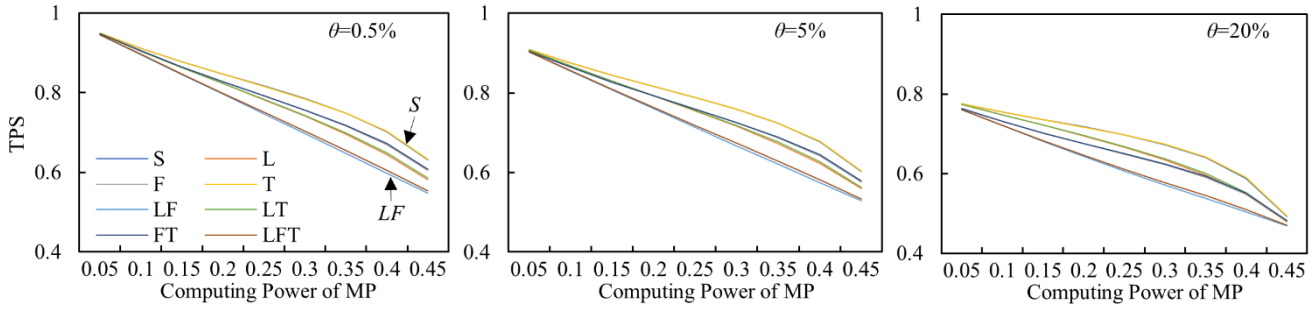


图4 在*LFT*策略下对我们的模型和公式进行验证



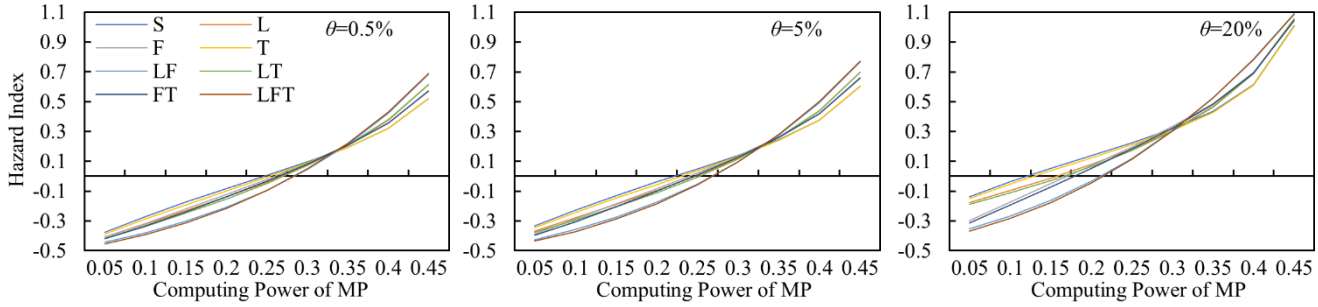
a) 分叉概率为0.5%　　b) 分叉概率为5%　　c) 分叉概率为20%

Fig.5 恶意矿池在各顽固策略和自私挖矿攻击下的相对收益与算力的关系



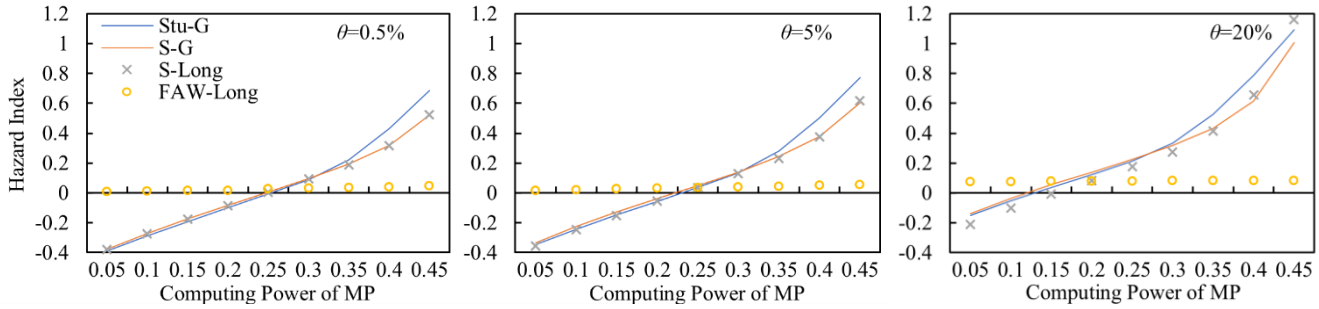
a) 分叉概率为 0.5%　　b) 分叉概率为 5%　　c) 分叉概率为 20%

图 6 不同顽固策略和自私挖矿攻击下系统 TPS 随恶意矿池算力的变化



a) 分叉概率为 0.5%　　b) 分叉概率为 5%　　c) 分叉概率为 20%

图7 恶意矿池算力的自私与顽固挖矿攻击危害指数



a) 分叉概率为 0.5%　　b) 分叉概率为 5%　　c) 分叉概率为 20%

图5 恶意矿池算力变化时不同攻击的危害指数对比

4.3 顽固挖矿攻击的影响评估

本节首先比较恶意矿池随分叉概率变化而产生的相对收益。然后，我们评估其对系统吞吐量的影响，并根据危害指数评估顽固挖矿攻击。我们在第4.1节提到的各种分叉概率下进行实验。由于篇幅限制，我们选择分叉概率的三个典型值：0.5%、5%和20%，分别说明顽固挖矿攻击在低、高和超高分叉概率下的影响。

4.3.1 相对收益

图5展示了恶意矿池相对收益的结果，其中“S”表示自私挖矿攻击的结果。我们发现：

- High分叉概率会使攻击者受益。无论恶意矿池（MP）采用哪种策略，其相对收益都会随着分叉概率的增加而上升。比较图5（a）–（c）中各图可见，所有曲线都会随着分叉概率增大而上升，这证实了这一点。攻击者有动机发动网络攻击以提高分叉

p概率　y.

- 对于小型矿池，自私挖矿攻击比顽固挖矿攻击更有利可图。这一点可以从图中看出：当恶意矿池的算力低于约30% 时，自私挖矿攻击曲线高于所有顽固策略（当 时为0.31，当 时为 0.3，当 时为 0.28）

0.5%　　θ = 5%　　20%

如图5 (a)-(c) 所示。原因在于，自私挖矿攻击会使矿工试图获取区块领先优势，而顽固挖矿攻击则倾向于弥补落后。例如，当 和 HPs 找到一个区块时，恶意矿池在

Λ=2

自私挖矿中会发布两个私有区块，而在 *L* 策略中只发布一个区块。 *L* 策略希望 HPs 在私有子树上挖矿，从而分散并浪费 HPs 的算力。 然而，*L* 策略会增加失去区块领先优势的概率。HPs 可能在同一个公共子树上产生分叉，随后恶意矿池因落后而不得不放弃第二个私有区块。当其算力较低时，恶意矿池领先公共子树两个以上区块的概率很低。因此，顽固挖矿攻击不适合算力较低的攻击者。

- 对于大型矿池，顽固挖矿攻击的表现优于自私挖矿攻击。当恶意矿池（MP）的算力超过 30% 时，图5（a）和图5（b）中自私挖矿攻击的曲线最低，而在图5（c）中则是第二低。算力较强的矿池更有可能生成有效区块，因此更有机会从落后状态追赶上来。因此，就攻击者的相对收益而言，顽固挖矿策略展现出了优势。

- **T* 策略（*LT*、*FT*、*LFT*）在大多数情况下比攻击者采用的 * 策略（*L*、*F*、*LF*）利润更高。这一点可由以下结果证明：“**T*”曲线

非常接近且略低于 “*”（即 *LT* 和 *L*、*FT* 和 *F*、*LFT* 和 *LF*，以及 *T* 和 *S*），如图5（a）—（c）所示。换言之，如果攻击者不确定当前的分叉概率和自身算力，就应选择 * 策略，而不是 **T* 策略。不过，当恶意矿池的算力为 34%~45% 时， LFT 策略在图*5*（*a*）和（*b*）中确实表现最佳。如果攻击者想在这些情形下获得最大利润，仍应采用 *LFT* 策略。

4.3.2 系统吞吐量

图6给出了恶意矿池算力变化时，各种顽固策略下系统TPS的结果。由于第3.3节将常规区块生成率和区块生成率归一化为1，因此系统的最大TPS为1。图6的结果表明：

- 随着恶意矿池算力增加以及分叉概率升高，TPS会下降。如图6（a）—（c）所示，所有曲线都随着恶意矿池算力的增加而向下变化。图6（a）中的曲线高于图6（b）中的曲线，这是因为分叉概率越高，意味着陈旧区块越多。顽固挖矿攻击会故意制造分叉。需要注意的是，区块生成率保持稳定。如果同一时间段内陈旧区块增多，主区块的数量就会减少。

- 无论恶意矿池掌握多少算力，在所有分叉概率下，*LF*和*LFT*的TPS都最低，而自私挖矿攻击和*T*策略的TPS都最高。原因在于，顽固策略会比自私挖矿攻击故意制造更多分叉，尤其是*L**和*F**策略。此外，*S*、*L*、*F*、*LF*的曲线分别与*T*、*LT*、*FT*、*LFT*的曲线非常接近，且略高于后者（见图6 (a)-(c)）。在大多数情况下，就TPS而言，**T*策略造成的损害小于*策略。

- 小规模恶意矿池下，*L*的*TPS*高于F，而大规模恶意矿池下则相反。这一现象在图 6(b) 和 (c) 中更加明显。这是因为小规模恶意矿池下， 更可能等于 0，且F策略会奏效。对于大规模恶意矿池，更容易生成区块并且 ha

具有更重的私有子树。因此， 的概率大于恶意矿池较小时的概率，且*L*策略有效。

4.3.3 危害指数

度量危害指数（危害指数）反映了对区块链系统造成的、单位算力对应的攻击损害。它与攻击者的算力相关，可以告诉攻击者是否应发动攻击：1）危害指数为正，意味着攻击者可以发动攻击并获得额外收益；2）危害指数为负，意味着攻击者会损失本应获得的收益，因此理性的攻击者不会发动攻击。请注意，危害指数为负并不意味着系统受益或未受损，而是表明攻击者不会发动攻击的概率。图7展示了恶意矿池算力不同时，顽固挖矿攻击和自私挖矿攻击的危害指数。我们观察到：

- 大型矿池发动的顽固挖矿攻击对系统危害更大。图7（a）—（c）中，随着恶意矿池算力的增加，危害指数也随之上升。这也表明，大型矿池通过实施顽固挖矿攻击可以获得更多收益。

- 对于小型矿池来说，发动顽固挖矿攻击并非有利之选。事实证明，当恶意矿池的算力低于约25%时，在低（图7 (a)）和高分叉概率（图7 (b)）下，顽固挖矿攻击的危害指数为负；而在超高分叉概率（图7 (c)）下，该阈值约为18%。收益阈值会随着分叉概率的增加而降低。具体而言，阈值为25%~30%（当 且为23%~27%（当

0.5%θ = θ = 5% .

当 时，*S* 和 *LF*的阈值为 12%，*LF* 和 *LFT*的阈值为 22%，其他策略的阈值为~20%。

- 在分叉概率较高的区块链中，攻击者往往会发动顽固挖矿攻击以获取额外收益。图7 (a)-(c) 中的结果表明，危害指数会随着分叉概率的增加而上升。如图7 (c) 所示，算力占比为 45% 的恶意矿池通过顽固挖矿，可以将相对收益翻倍

g 当 时发动攻击。20%θ =

- 与相对收益率不同，危害指数能够有效帮助攻击者判断发动攻击的盈利程度。当攻击的相对收益率低于诚实挖矿时，现有研究会据此计算恶意矿池的损失。在图5 (a) 中，算力占比为 0.05 的恶意矿池采用*L*策略时，相对收益率为 0.03；当其算力占比为 0.15 时，相对收益率为 0.115。算力占比为 0.05 的恶意矿池损失较少（0.02），低于算力占比为 0.15 的恶意矿池（0.035）。由于损失很小，算力占比为 0.05 的恶意矿池可能会发动攻击。然而，在图7 (a) 中，算力占比为 0.05 的恶意矿池采用*L*策略时，危害指数为 -0.41；算力占比为 0.15 的恶意矿池的危害指数则为 -0.23。实际上，算力占比为 0.05 的恶意矿池损失远高于算力占比为 0.15 的恶意矿池，因此不会发动攻击。

4.4 危害指数中顽固挖矿攻击与其他攻击的比较

在不完美网络场景中，目前尚无针对最长链协议下顽固挖矿攻击的解析模型，且仅有针对 GHOST 下自私挖矿攻击动态的建模。因此，我们通过与下列其他区块链攻击进行比较，评估 GHOST 中顽固挖矿攻击造成的损害严重程度：

1) 最长链协议下的自私挖矿攻击。该攻击在 [14] 中进行了建模。2) GHOST 下的自私挖矿攻击。我们和 [16] 中的工作均可对此进行建模，结果与第4.2节所示相同。3) 最长链协议下的扣留后分叉（FAW）攻击。该攻击在 [31] 中进行了建模。区块扣留（BWH）攻击 [29] 是一种经典攻击，易于实施且难以检测。扣留后分叉

持有（FAW）攻击 [30] 是最具威胁的基于阻挖矿的攻击之一，使攻击者始终能够获得额外的相对收益。因此，我们比较顽固挖矿攻击与 FAW攻击，以评估它们造成的损害。

我们实现了这三个模型及相关的度量公式。图 8 展示了结果，其中“S”表示自私挖矿，“Stu”表示最优顽固挖矿策略（即使危害指数最大化的策略），“-G”和“-Long”分别表示 GHOST 和最长链。我们观察到：

- 顽固挖矿攻击比自私挖矿攻击危害更大。在 GHOST系统中，当恶意矿池的算力超过 35% 时，图 8(a)–(c) 中最优顽固策略（记为 opt-stubborn）的危害指数明显高于自私挖矿攻击。当恶意矿池持有的算力低于 35% 时，opt-stubborn 的危害指数略低于自私挖矿攻击。此外，opt-stubborn 与自私挖矿攻击的奖励阈值几乎相同。就对区块链造成的严重程度而言，opt-stubborn 优于自私挖矿攻击。• 小型矿池倾向于发动 FAW攻击，而大型矿池倾向于发动顽固挖矿攻击。在最长链系统中，FAW攻击的危害指数始终为正，且随着恶意矿池的算力增加，波动很小。但该值较小（图 8(a) 中危害指数<0.05， 图 8(c) 中危害指数为 < 0.085 ）。当恶意矿池的算力超过 25% 时，自私挖矿攻击造成的损害要大得多。在图 8(a) 和 (b) 中，如果恶意矿池持有的算力低于 25%，自私挖矿和 opt-stubborn 的危害指数均为负。

- GHOST 能表现出抵御大型矿池发起链自私挖矿攻击，但抵御小型矿池攻击的表现较差。GHOST 与最长链协议的比较结果表明，在图 8（a）所示的低分叉概率（0.5%）网络中，自私挖矿的危害指数非常接近。如图 8 （ b ）所示，在高分叉概率下，当恶意矿池的算力低于 35% 时，GHOST 自私挖矿的危害指数高于最长链协议。GHOST 抵御小型矿池攻击的表现不如最长链协议。当恶意矿池的算力超过 40% 时，最长链协议的危害指数高于 GHOST。在超高分叉概率系统中也会出现这一现象（见图 8（c））。

5 Conclusion and Future Work

本文建立了一个马尔可夫模型，用于评估不完美网络中的顽固挖矿攻击。我们提出了一种名为“危害指数”的新指标，用于定量衡量攻击造成的损害程度。本文建立了攻击者相对收益、系统吞吐量和危害指数的度量公式。基于这些公式，我们对不完美 BTC 区块链中的顽固挖矿攻击进行了定量研究，并将其与自私挖矿攻击在 GHOST 中的情况，以及最长链场景下的自私挖矿攻击和 FAW攻击进行了危害指数比较。

参考文献

[1] S. Nakamoto，《比特币：一种点对点电子现金系统》，Decentralized Business Review，21260，2008。[2] https://www.coindesk.com/price/bitcoin/。访问于2023年1月。[3] D. Berdik、S. Otoum、N. Schmidt、D. Porter 和 Y. Jararweh，《区块链在信息系统管理与安全中的应用综述》，Information Processing & Management，58(1)，102397，2021。[4] J. Leng、M. Zhou、J. Zhao、Y. Huang 和 Y. Bian，《区块链安全：技术与研究方向综述》，发表于 IEEE Transactions on Services Computing，第15卷，第04期，第2490-2510页，2022。[5] V. Schlatt、*T*. Guggenberger、J. Schmid 和 N. Urbach，《攻击信任机器：制定区块链网络安全的信息系统研究议程》，International Journal of Information Management，102470，2022。[6] I. Eyal 和 E. G. Sirer，《多数并非足够：比特币挖矿易受攻击》，金融密码学 2014，柏林，海德堡，2014，第436-454页。[7] https://en.wikipedia.org/wiki/Litecoin/。访问于2023年1月。[8] K. Nayak、S. Kumar、A. Miller 和 E. Shi，《顽固挖矿：推广自私挖矿并结合日蚀攻击》，2016 IEEE欧洲安全与隐私研讨会（EuroS&P），2016，第305-320页。[9] Y Zhang、M Zhao、T Li、Y Wang 和 T Liang，《通过状态转移分析实现加密货币顽固挖矿的最优奖励》，Information Sciences，625：299-313，2023。[10] Y. Sompolinsky 和 A. Zohar，《比特币中的安全高速交易处理》，金融密码学与数据安全国际会议。Springer，柏林，海德堡，2015，第507-527页。[11] M. Davidson、*T*. Diamond，《多种难度调整算法下自私挖矿盈利能力研究》，Cryptology ePrint Archive，94，2020。[12] S. Lee、S. Kim，《重新思考矿池挖矿中的自私挖矿》，ICT Express，2022，印刷中。[13] S. Ai、G. Yang、C. Chen、K. Mo、W. Lv 和 A. S. V. Koe，《ESM：兼顾生态足迹的自私挖矿》，Information Sciences，606：601-613，2022。[14] R. Yang、X. Chang、J. Mišić 和 V. B. Mišić，《不完美网络中的区块链自私挖矿评估：诚实矿工与自私矿工视角》，Computers & Security，97，101956，2020。[15] H. Kang、X. Chang、R. Yang、J. Mišić 和 V. B. Mišić，《理解扩展分叉下不完美比特币与以太坊网络中的自私挖矿》，发表于 IEEE Transactions on Network and Service Management，第18卷，第3期，第3079-3091页，2021年9月。[16] R. Yang、X. Chang、J. Mišić、V. B. Mišić 和 H. Kang，《自私挖矿攻击下两种链选择协议的定量比较》，发表于 IEEE Transactions on Network and Service Management，第19卷，第2期，第1142-1158页，2022年6月。[17] C. Grunspan 和 R. Pérez-Marco，《顽固挖矿的盈利能力研究》，arXiv 预印本 arXiv:1808.01041，2018。

[18] R. Yang、X. Chang、J. Mišić 和 V. B. Mišić，《比特币和以太坊中自私挖矿与顽固挖矿的深入分析》，arXiv 预印本 arXiv:2112.02588，2021。[19] Z. Wang、J. Liu、Q. Wu、Y. Zhang、H. Yu 和 Z. Zhou，《不完美以太坊网络中自私挖矿和顽固挖矿对叔块影响的解析评估》，Computers & Security，87，101581，2019。[20] Y. Liu、Y. Hei、*T*. Xu 和 J. Liu，《日蚀攻击下叔块机制对以太坊自私挖矿与顽固挖矿的影响评估》，发表于 IEEE Access，第8卷，第17489-17499页，2020。[21] Q. Xia、W. Dou、*F*. Zhang 和 G. Liang，《GHOST 中自私挖矿的性能》，载于2021年 IEEE 第20届计算、信任、安全与隐私国际会议（TrustCom）（第26-33页）。IEEE，2021。[22] H. Zhu、Z. Chen、J. Mišić、V. B. Mišić、X. Chang 和 J. Bai，《不完美 GHOST 比特币区块链中顽固挖矿的威胁能力》，IEEE ICC 2023，已录用。[23] https://gz.blockchair.com/。访问于2023年1月。[24] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ gasper/。访问于2023年1月。[25] V. Buterin，《下一代智能合约与去中心化应用平台》，白皮书，3(37)，2014。[26] https://www.blockchain.com/explorer。访问于2023年1月。[27] J. Misic、V. Misic 和 X. Chang，《比特币区块链传输网络中的账本不一致时间》，IEEE GLOBECOM 2019：1-6。[28] https://www.maplesoft.com/。访问于2023年1月。[29] S. Bag、S. Ruj 和 K. Sakurai，《比特币区块扣留攻击：分析与缓解》，发表于 IEEE 信息取证与安全汇刊，第12卷，第8期，第1967-1978页，2017年8月。[30] Y. Kwon、D. Kim、Y. Son、E. Vasserman 和 Y. Kim，《自私行事，避免困境：针对比特币的扣留后分叉（FAW）攻击》，ACM CCS 2017，美国得克萨斯州达拉斯，第195-209页，2017。[31] H. Zhu、X. Chang、J. Mišić、V. B. Mišić 和 R. Yang，《重新审视不完美工作量证明区块链中的 FAW 攻击》，Peer-to-Peer Networking and Applications，15(5)，2430-2443，2022。