# **区块链工作量证明的安全性与性能研究**

**译者：丁靖3170105504**

|  |  |  |
| --- | --- | --- |
| Arthur Gervais  ETH Zurich, Switzerland arthur.gervais@inf.ethz.ch | Ghassan O. Karame  NEC Laboratories, Europe ghassan.karame@neclab.eu | Karl Wüst  ETH Zurich, Switzerland kwuest@student.ethz.ch |
| Vasileios Glykantzis  ETH Zurich, Switzerland glykantv@student.ethz.ch | Hubert Ritzdorf  ETH Zurich, Switzerland hubert.ritzdorf@inf.ethz.ch | Srdjan Capkunˇ  ETH Zurich, Switzerland srdjan.capkun@inf.ethz.ch |

## 摘要

工作量证明（POW）驱动的区块链目前占现有数字货币总市值的90％以上。尽管对比特币的安全性条款进行了彻底的分析，但是不同的（分叉的）POW区块链（用不同的参数实例化）的安全性保证在文献中并没有得到很多关注。

在本文中，我们引入一个新的量化框架来分析POW区块链的各种共识和网络参数的安全性和性能隐患。在这个框架的基础上，针对网络传播、区块的不同大小、区块生成间隔、信息传播机制、日食攻击影响等现实约束条件，我们设计了双重支出double-spending和私人挖掘selfish mining的最优对抗策略。因此，我们的框架允许我们捕获现有的基于POW的部署以及用不同参数具体化的POW区块链变体，并客观地比较权衡它们的性能和安全规定。

## **1.引言**

自2009问世以来，比特币的区块链推动了创新以及许多新的应用，比如智能合同，都是利用区块链设计的。比特币已经被多次分支，以调整共识(即块生成时间和散列函数)和网络参数(例如块的大小、信息传播协议、块的大小)，并提高区块链的效率。例如，Bit-coin（比特币）最杰出的分支——Lite-coin（Litecoin）和Doge-coin（多吉币）分别将区块生成时间从10分钟缩短到2.5分钟和1分钟。在这些努力的同时，基于区块链的可替代的分布式网络(如Ethereum)也出现了，以优化共识和网络参数，并在区块链之上简化分布式应用的部署。

虽然一些共识协议（拜占庭容错算法Practical Byzantine Fault Tolerance [5],权益证明Proof of Stake [29], 流逝时间量证明Proof of Elapsed Time [20]）已经提出，现有的大多数区块链还是举债经营昂贵的工作量证明（POW）的共识机制,POW目前占现有的数字货币的总市值的90%。虽然比特币的安全规定已深入分析[ 14,21,30,32 ]，POW区块链的安全保障也在文献中没有得到太多的关注。最近的研究表明，在不影响其安全性的前提下，基于POW的区块链的性能无法得到增强。 然而，POW区块链的性能和安全条款之间的关系至今还没有被详细研究。

|  |  |  |
| --- | --- | --- |
| 共识与网络参数 |  | 安全参数 |
| ↓ |  | ↓ |
| 工作量证明（POW）区块链 | 区块过期率  → | 安全模型 |
| ↓ |  | ↓ |
| ·区块过期率stale block rate |  | ·最优对抗策略optimal adversarial strategy |
| ·区块扩展次数block propagation times |  | ·安全条款security provisions |
| ·输出throughput |  |  |

图1：我们的定量框架的组成部分。

本文针对这一问题，提出了一种新的定量框架，以分析区块链的各种共识和网络参数的安全性和性能问题。利用我们的框架，我们研究了现有POW区块链的实例(例如， Bit-coin比特币, Ethereum, Lite-coinLitecoin, and Doge-coin多吉币)以及其他可能的实例，对这些实例的不同的共识和网络参数获取了它们的安全属性。我们的框架（参见图1）由两个关键要素组成：（i）区块链实例和（ii）区块链安全模型。区块链实例是一个POW区块链，给定其以一组共识和网络参数，例如网络延迟，区块生成时间，区块大小，信息传播机制等实例化。例如，Bit-coin比特币，Lite-coinLitecoin和Ethereum对应于3种不同的区块链实例。为了逼真地捕捉任何其他的区块链实例，我们设计了一个模拟器，通过实现基于广告的信息传播、主动区块推送、继电器网络系统、*Send-header*传播机制等来模仿区块链共识和网络层。区块链实例的主要输出是（测量的或模拟的）区块块过期（闲置）率，作为输入量输入到我们的安全模型中。另一方面，我们的安全模型是基于马尔可夫决策过程（Markov Decision Processes，MDP）的双重支出和私人挖掘（double-spending and selfish mining），并允许我们推理最优的敌对策略，同时考虑到敌对的挖掘能力，日食攻击的影响，区块奖励，真实世界的网络和共识参数，这些都可以由区块的过期率有效地捕捉。

鉴于目前比特币社区正在讨论一个适当的最大块大小，以确保系统[1]的可伸缩性和扩展性。我们的工作提供了一种在不同的参数（包括区块大小）的影响下，整体比较POW 区块链安全性和性能的方法。例如，我们发现从当前比特币交易中增加块大小（平均0.5MB）到4 MB，不会明显影响私人挖掘和区块链的双重支出弹性——证明了区块传播机制可以确保低的区块过期率。我们将我们的发现总结如下。

### **调查结果摘要****.**

* 我们证明，私人的挖掘并不总是一种理性的策略。为了捕捉理性对手，我们量化了POW区块链的双重支出弹性，并客观地比较了不同POW区块链对交易确认所需的数量的安全性。不同功率块链相对于所需数量的交易确认的可靠性。通过这样做，我们为商家提供知识来决定给定交易价值的确认次数，以防双重支出。
* 我们的结果表明，与比特币相比，由于Ethereum1 （以太坊）更少的块奖励和更高的区块过期率（比特币凭借更快的确认时间以0.41%的区块过期率领先于Ethereum的6.8%)，Ethereum(区块间隔在10到20秒之间)需要至少37次确认才能比得上比特币6次区块确认的安全性(区块平均间隔10分钟)，以对抗比特币这样一个拥有总挖掘能力30%的对手。类似地， Lite-coin需要28区块确认，Doge-coin需要 47区块确认才能与比特币的安全性相匹配。
* 我们表明，块链的块奖励越高(以美元为例)对双倍支出（double-spending）的抵抗力越强。

• 最后，我们分析改变块大小块间隔对自私挖掘和双重支出的影响。 我们的结果令人惊讶地表明，将块大小设置为平均1 MB，将块间隔时间减少到1分钟不会显着降低安全性。 因此，我们的结果表明POW区块链可以达到高于每秒60个交易（tps）的有效吞吐量（这意味着比特币的当前7 tps的吞吐量可以显著提高），而不损害系统的安全性。

论文的其余部分安排如下。在第二节中，我们概述了POW区块链的基本概念。在第三节中，我们引入了MDP模型，定量分析POW区块链的安全性。在第四节中，我们介绍了我们的模拟器，并评估了许多基于POW的变体区块链实例的安全性和性能。在第五节中，我们概述了相关的工作，我们在第六节中总结了这篇论文。

## **2.背景**

在本节中，我们简要回顾一下现有POW区块链的共识层和网络层的操作。

### **2.1共识层**

工作量证明（POW）共识机制是现有区块链中最广泛的部署共识机制。POW是由比特币[27]引入的，并且假设每个同行通过解决工作实例的证明和构建适当的区块来用他的“计算能力”投票。 例如，比特币使用基于散列的工作量证明，它需要寻找一个随机数值，这样当用额外的块参数（例如，Merkle散列，前面的块散列）进行散列时，散列值必须小于当前目标值。当发现这样的随机数时，挖掘者创建块并在网络层（参见2.2节）将其转发给其对等机。 网络中的其他对等体可以通过计算块的散列并检查它是否满足条件小于当前目标值来验证工作量证明。

区块间隔：区块间隔的定义是内容写入区块链的等待时间。 区块间隔越小，交易确认的速度越快，同时区块过期的概率越高。区块间隔调整直接关系到底层工作量证明机制的难度变化。 较低的难度导致网络中的块数量增加，较高的难度导致同一时间段内的块减少。

因此，分析改变难度是否会影响攻击最长链的对抗能力至关重要 - 这是大多数基于工作量证明的区块链的安全性的主要支柱。这也意味着调整商家必须等待的确认数量，以便安全地接受交易（避免双重消费攻击）（参见第3节）。

#### 2.1.1工作量证明的安全性

工作量证明的安全性依赖于这样一个原则，即任何实体都不应该收集超过50％的处理能力，因为这样一个实体可以通过维持最长的链条来有效地控制系统。 我们现在简要地概述已知的基于工作量证明的区块链的攻击。

首先，对手可以通过使用同一枚硬币发行两笔（或多笔）交易，从而有效地花费多于他拥有的硬币。最近的研究表明，接受交易而不要求区块链确认是不安全的[21]。 交易得到的确认越多，未来这笔交易逆转的可能性就越小。

其次，矿工可能试图进行自私的采矿[14]攻击，以通过有选择性地扣留矿区块，并逐渐将其逐步发布[14,31]，从而增加其在区块链中的相对采矿份额。 最近的研究表明，由于这些攻击，一个拥有33％采矿能力的自私矿工可以有效地获得50％的采矿能力。

如果区块链系统中的所有节点都紧密同步，则双重支出攻击和自私挖掘可以得到缓解。 请注意，除了网络延迟之外，由于日食攻击[16,17]，同步延迟会使对手在网络中创建逻辑分区，即向不同的区块链网络节点提供相反的区块和交易信息。

### **2.2网络层**

在网络层，我们确定了两个主要参数对于基于工作量证明的区块链特别重要，即：区块大小和信息传播机制。

#### 2.2.1区块大小（规模）

最大区块大小间接定义了块内进行交易的最大数量。因此，这个大小控制着系统达到的吞吐量。较大的块会导致较慢的传播速度，从而增区块过期率（并减弱前面所述的区块链的安全性）。

#### 2.2.2信息传播机制

区块请求管理系统会指示信息如何被传递给网络中的对等体。 最终，由于所有同行都希望接收所有的数据块，所以需要一个广播协议。 底层广播协议的选择明显影响网络的稳固性和可扩展性（参见第4节）。在下文中，我们将简要描述现有的基于工作量证明的区块 链的人们熟知的网络层体现。

基于广告的信息传播：大多数POW区块链借助基于广告的请求管理系统来传播消息。 如果节点A从另一个节点接收到关于新对象（例如，交易或区块）的信息，则A将通过向其它连接（例如节点B）发送一个inv调用消息（广告的散列和类型）。只有当节点B先前没有收到广播的对象时，B才会用get-data请求向A请求对象。 节点A随后将用比特币对象进行响应，例如交易或区块的内容。

发送标题（Send headers）：对等方可以选择发送send headers消息，以便将来自等方直接接收块标题 - 跳过使用inv消息。这减少了块消息传播的延迟和带宽开销，自0.12版本开始被比特币所采用。

未经请求的区块推送：该机制使得矿工能够在没有广告的情况下广播他们生成的区块（即，因为他们挖掘了区块）。 请注意，这个推送系统是推荐的，但没有在比特币中实现。

中继网络：中继网络[6]主要增强拥有共同交易池的矿工的同步。交易通常只在具有交易的ID的中继块中引用（每个交易2个字节，而不是每个交易平均250个字节）。 结果，所得到的区块大小比常规块小（参见比特币中继网络[6]）。

混合推送/广告系统：一些系统，如Ethereum，使用混合推送和广告传播。在这里，块被直接推送到对等体的临界数目上(例如，Ethereum直接将块推到n个对等点，其中n是连接到对等点的邻居的总数)。同时，发送方向其所有邻居发布区块散列通告。

## 2.3过期区块

过期区块指的是由于某种原因不包括在最长链中的块，例如，由于并发性、冲突。过期区块对区块链的安全性和性能是有害的，因为它们会引发连锁分叉 - 这种不一致的状态会减缓主链的增长，并导致对性能和安全的显著影响。 一方面，过期区块增加了网络中攻击者的优势（例如双重消费）。 另一方面，过期区块会导致额外的带宽开销，并且通常不会得到挖掘奖励（在Ethereum中除外）。

在我们进行的一个实验中，我们测量了比特币（块生成时间= 10分钟，平均块大小= 534.8KB），Lite-coin（块生成时间= 2.5分钟，平均块大小= 6.11KB）和Doge-coin （块生成时间= 1分钟，平均块大小= 8KB）的区块过期率。所有三个区块链依赖于基于工作量证明的区块链（具有不同的生成时间）和相同的信息传播系统（具有不同的区块大小）。

我们在2016年2月浏览了Lite-coin Doge-coin[3]的可用节点，分别找到了大约800和600个IP地址。 然后，我们通过记录应网络中所有连接的特定区块接收广告的时间来测量区块时间[9]。 我们为Lite coin和Doge coin运营了一个节点，我们分别连接了340个和200个同行。 一旦这些对等体之一以（i）块的新散列（inv消息）或（ii）块头（头部消息）的形式通告区信息，我们记录该区块出现的时间，随后每次接收特定的区息提供关于块传播的信息。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Bit coin | Lite coin | Doge coin | Ethereum |
| 区块间隔 | 10 min | 2.5 min | 1 min | 10-20 seconds |
| 公共节点 | 6000 | 800 | 600 | 4000 [11] |
| 矿池 | 16 | 12 | 12 | 13 |
| *tMBP* | 8.7 s [8] | 1.02 s | 0.85 s | 0.5 - 0.75 s [12] |
| *rs* | 0.41% | 0.273% | 0.619% | 6.8% |
| *sB* | 534.8KB | 6.11KB | 8KB | 1.5KB |

表1：比较不同比特币分叉，Ethereum以及参数选择对网络传播时间的影响。在最后的10000个块中测量区块过期率（rs）和平均块大小（sB）。 tMBP代表中值块传播时间。

我们的结果（参见表1）表明，区块过期率的确很大程度上取决于区块间隔和区块大小。例如，与Dogecoin和Litecoin不同的是，比特币由于更高的交易负载（高达1MB）而具有更大的块大小，导致更高的区块过期率（0.41％比0.273％） - 虽然比特币的块间隔是4倍 比Litecoin还要长，而且Litecoin和Dogecoin之间的区块过期率差异主要是由于区块间隔（2.5分钟vs. 1分钟）的差异所致，因为它们的平均区块大小相当（6.11KB和8KB）。鉴于确认时间缩短了60％，从Litecoin到Dogecoin的区块过期率上升了127％。

请注意，在Ethereum，*uncle区*块对应于主链中引用的过期区块。Ethereum的*uncle*区块率几乎为6.8％，而比特币的过期率为0.41％。 在第3节中，我们研究了区块过期率对POW区块链安全性的影响。

## 3.工作量证明安全模型

在本节中，我们介绍我们的区块链安全模型，我们利用这个模型来量化双重支出和自私挖掘的最优对抗策略。 然后，我们以这些策略作为基础，比较基于POW的区块链在使用不同参数实例化时的安全规定。

### 3.1安全模型

我们的模型扩展了[31]的马尔可夫决策过程（MDP），以确定最优的对抗策略，并得到：

**过期区块率** 过期区块率*rs*允许我们考虑到不同的区块大小，区块间隔，网络延迟，信息传播机制和网络配置（例如，节点数量）。

**挖掘能力**α是对手总挖掘能力的一部分(其余部分由诚实网络控制)。

**挖掘成本**对抗性开采成本*cm* ∈ [0*,α*]对应于对手的预期采矿成本（即，总开采成本，例如硬件，电力，人力），并以块奖励表示，并都是用块奖励来表示的。例如，如果*cm* = *α*，那么对手的开采成本等于其开采能力乘以区块奖励，即开采成本完全由在诚信开采中获得的区块收入覆盖。

**块确认次数**k对应于需要确认交易的块的数量，以使商家接受交易。

**传播能力传播参数γ**获取网络中攻击者的连通（即当攻击者和诚实的矿工在网络中同时释放它们的区块时，捕获接收攻击者区块的网络部分）。

**日食攻击的影响**我们的模型解释了日食攻击。 在这里，我们假设诚实网络的矿工受到区块过期率的影响，而对手和共谋受害者并没有发现过期区块。 这是因为攻击者可以使用任何开采块进行攻击，并且在采用诚实链之后只有很小的机会挖掘过期的块。 因此，在实践中，对手的真实区块过期率显著低于诚实网络。诚实的网络传播和验证有延迟 - 因此它将带来更高的区块过期率。请注意，日食攻击的受害者发现的区块也可以计算到对手的私密区块链中。

*我们将其与现有的模型（如Sapirshtein等人的[31]）进行对比，该模型只关注自私挖掘，不能捕获不同的区块链实例（具有各种过期区块率和确认环节）以及实际参数（比如网络延迟）。*

为了分析最优双重支出策略，我们定义了与最小交易价值相对应的双重支出金额 *vd* ，使得双重支出比诚实的采矿更有利可图。 我们认为 *vd* 是衡量双重支出攻击下安全性的一个强有力的指标。 也就是说，如果诚实采矿的报酬大于不诚实采矿的报酬，那么商家可以安全地接受价值*vd* 支付的交易（因为这样的价值被认为是安全的，例如基于给定的确认号码）。然而，如果敌对行为在经济上受益更多，商人应该意识到相关的双重支出风险和矿工的相关激励措施。

我们使用单人决策问题*M*:= <*S,A,P,R>* 来获得区块链模型，其中其他所有参与者遵循标准协议，S对应于状态空间，A代表行动空间，P代表随机过渡矩阵,R代表奖励矩阵。如3.2节和3.3节所述，我们将M实例化作为马尔可夫决策过程（MDP）。

在我们的模型中，对手可以采取以下行动：

**采纳** 攻击者接受诚实网络的区块链，这效果相当于重新启动攻击。如果对手认为赢得诚实链条的可能性很小，那么这个行动是合适的。

**覆盖** 攻击者比诚实的链多发布了一个区块，因此覆盖了相互冲突的区块。这种情况发生在对手的秘密链比当前已知的公共链更长（即 *la > lh*）时，攻击者最好用他自己的 *lh* +1来替换诚实的网络区块链。如果敌手利用受害者的采矿能力，对手可能会使用受害者的 *be* 区块来进行覆盖行为。

**竞争** 对手尽可能地发布和诚实链一样多的区块，并触发两条链之间的接纳竞赛，而不是压倒诚实区块链。

**等待** 敌人继续挖掘其隐藏的链，直到找到一个区块。

**出口** 这个行为只有在研究双重支出时才有意义，因为它相当于一个成功的经过*k*确认的双重支出，并且只有当*la > lh* 且*la > k*时才是可行的。

状态空间S被定义为形式(*la,lh,be,*fork)的四元组，其中*la*和*lh*分别代表对抗链和诚实链的长度，是受害者开采的块，分叉可以取三个值：相关、无关和激活：

**相关** 标签相关标志着（i）诚实网络发现最后一个区块，（ii）如果*la* ≥ *lh*，覆盖行为适用。例如，(*la,lh* − 1*,be,*·)的一种状态导致(*la,lh,be,*relevant).

**无关** 当对手发现最后一个区块时，前一个区块可能已经到达网络中的大部分节点。 因此对手无法执行覆盖操作。例如形式(*la*−1*,lh,be,*·)的一种状态导致(*la,lh,be,*irrelevant).

**激活** 如果攻击者执行了覆盖动作，即网络当前正在拆分并且正在确定最长的链，则该状态被描述为激活。

在我们的模型中，每个状态转换（出口除外）都对应于区块的创建。因此，状态改变意味着对诚实的网络，对手或受害者的奖励。

给定对抗挖掘能力α，初始状态（0,0,0，无关）以概率*α*过渡到（1,0,0，无关），即对手发现一个区块。如果这个诚实的网络发现一个非过期的区块，结果状态是（0,1,0，相关）。 另一方面，如果诚实网络的区块导致一个过期的区块，则状态保持（0,0,0，无关），因为过期的区块不计入最长的链。最后一种情况说明受害者找到一个区块的概率为*ω*，导致了状态（1,0,1，无关）。

*自私采矿与双重开支*

在这项工作中，我们单独考虑了双重开支和自私的开采，因为自私的开采并不总是一个合理的策略：自私开采的目标是增加对主链的对抗区块的相对份额，而双重开支旨在最大限度地提高其绝对收入。

也就是说，只要POW区块链的难度不变（例如比特币的难度每两周只能变化一次），自私的开采就会比真正的开采产生更少的区块回报。 在诚实的挖掘中，敌手每获得一块区块就会得到奖励，而采用主链进行自私挖掘时，则会失去先前开采的区块。由于对手的挖矿能力低于诚实网络，因此他有很大的可能性落后于主链，导致他在没有很大的追赶机会的情况下采用主链，从而导致失去区块奖励。例如，按照我们最优的自私挖掘策略（参见第3.2.1节），拥有30％采矿能力的对手平均可以获得209块区块奖励，在整个网络中挖掘1000块地块的时间内（而不是诚实采矿获得的300）。类似地，Eyal和Sirer [14]的策略平均可以获得205.80块的奖励。

*日食攻击。*

在一次日食攻击中，整体挖掘能力的*ω成分*从接收来自诚实网络的信息中遭到日食攻击[17,28]。在这里，一些日食攻击变种出现：

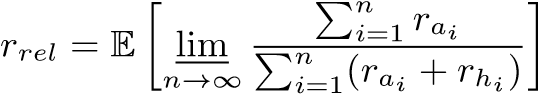
**没有日食攻击** 令ω= 0，我们的模型中有这种情况。

**隔离受害者** 这是在我们的模型中隐式捕获的。 也就是说，这相当于总采矿量的减少，因此增加了攻击者的采矿权达到.。

**利用日食受害者**在这里，敌手利用受害者的挖掘能力*ω*来推进他的私人链。在进行双重支出攻击时，这是理性对手最可能的选择。在这种情况下，我们假设受害者在网络中完全被屏蔽，除非攻击者允许，否则不会接收/发送区块[17,28]。

## 3.2自私采矿马氏决策过程MDP

我们的目标是找到自私挖掘的最佳敌对策略。回想一下，对手在自私挖掘中的目标不是优化绝对奖励，而是增加在网络接受的链中区块的份额。我们通过优化方程1中定义的相对收益*rrel*来捕获这个问题，其中*rai* 和 *rhi* 分别是步骤 *i* 对敌手和诚实网络的回报：

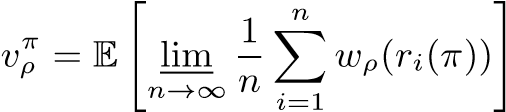
 (1)

由于攻击者的目标是在自私挖掘中增加他的相对报酬*rrel*（方程1），而不是绝对奖励，所以单人决策问题不能直接作为MDP建模，因为奖励函数是非线性的。为了将问题转化为MDP类，我们应用了Sapirshtein等人的技术[31]，我们将在下面介绍。

我们假设目标函数（即最优相对回报）的值为*rho*，并且定义了任意*ρ* ∈ [0*,*1]的变换函数*wρ*：N2 → R，其中对抗回报*ra*和诚实网络的回报*rh*在方程2中。

*wρ*(*ra,rh*) = (1 − *ρ*) · *ra* − *ρ* · *rh* (2)

这就得到了一个无穷状态 MDP *Mρ* =<*S,A,P,wρ*(*R*)>，其作用和状态空间与原来的决策问题相同，并有相同的转移矩阵，但报酬矩阵被*wrho*改变了。在策略*π*下的这种MDP的期望值之后由等式3中的*vρπ* 来定义，其中*ri*(*π*)是在策略*π*下的步骤i中的奖励元组。

 (3)

最优策略下的预期值如下：

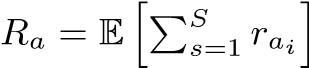
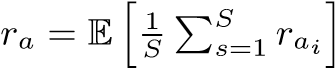
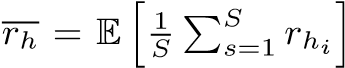
 (4)

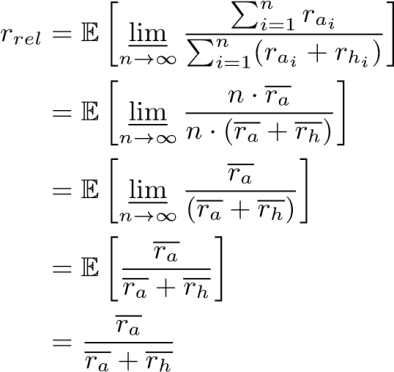
为了优化*rrel* ，我们采用以下命题[31]：

1.对于某个ρ∈[0,1]如果=0，则转换后的MDP *Mρ*中的最优策略*π*∗也使 *rrel* 最大且*rrel* = *ρ.*

2.在 *ρ*中单调递减。

由于标准MDP解算器不能解决无限状态MDP，所以我们通过仅允许任一链的长度至多为c来限制MDP类家族的状态空间，从而导致有限状态MDP。 如果任一链达到长度c，攻击者只允许执行覆盖或采纳操作。这给出了无限状态MDP的最优值的下界。

直觉上，我们可以如下推导出有界单人决策问题的第一个命题的正确性。在一个循环有限状态MDP中，经过一定数量的步骤*S*后，初始状态将再次被期望访问。在那段时间内，对手获得期望的回报，诚实的网络在原有的（有界的）决策问题中得到回报。 因此，马尔可夫链中每步的期望回报对于对手和诚实的网络分别为  ，因此，我们可以将预期的相对收入损失 *rrel* 简化为：

(5)

(6)

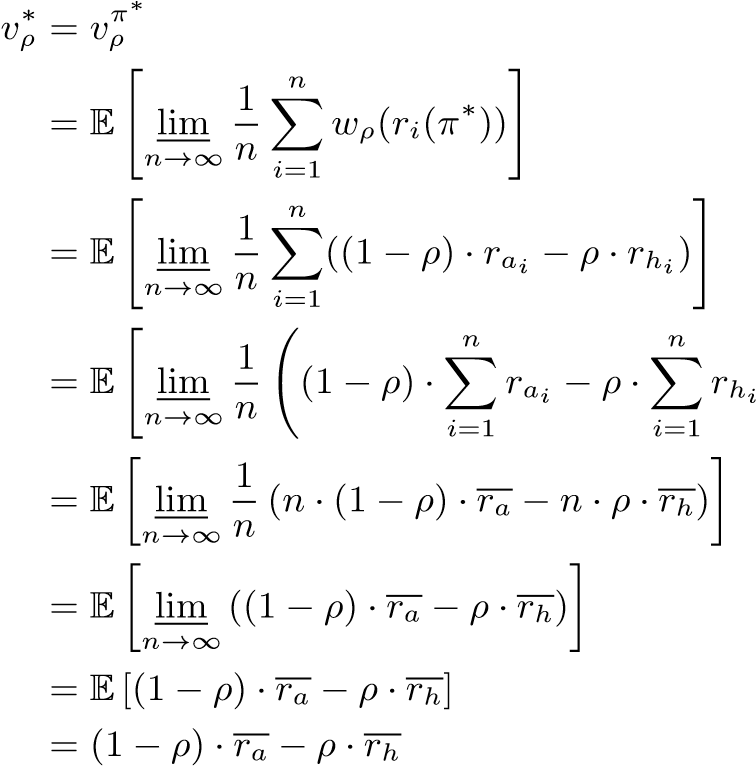
(7)

(8)

(9)

(10)

另外，我们如下改进：

(11)

(12)

(13)

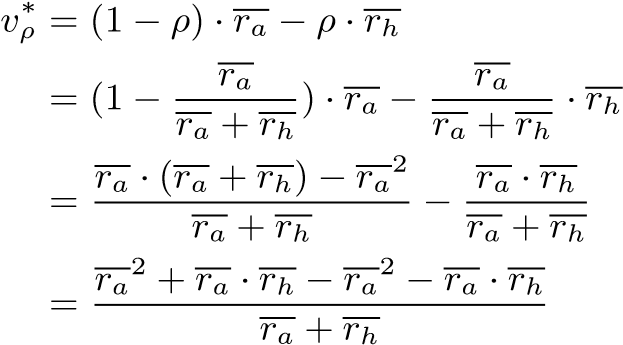
)](14)(15)

(16)

(17)

(18)

因此对于的情况:

(19)

(20)

(21)

(22)

= 0 (23)

第二个命题的推理很简单。 对于任何给定的策略*π*，对于对手和诚实网络，每一个带有奖励*ra* 和 *rh*的转换分别对于*ρ > ρ*0， *wρ*(*ra,rh*) ≤ *wρ*0(*ra,rh*)。

对于每一个策略*π*，直接有因此，即，*vρ*∗在ρ中是单调递减的。

我们在我们的受限MDP类中使用二分法搜索 *ρ* ∈ [0*,*1]，以便找到实例化的MDP中期望值为0的*ρ* ，从而使原始单人决策问题中的回报最大化[31]。由于单调递减，这可以有效地进行如下：

函数优化策略

*low* ← 0

*high* ← 1

repeat重复

*ρ* ← (*low* + *high*)*/*2

MDP\_SOLVE

if如果 then则

*low* ← *ρ*

else否则

*high* ← *ρ*

end if

until

return *π,ρ*

end function函数结束

据我们所知，这是第一个自私的挖掘模型，*(i)*它捕获了区块传播时间，区块大小，区块生成间隔等各种参数，*(ii)*已知的网络漏洞，如日食攻击。请注意，我们不考虑自私挖掘MDP中的挖掘成本，因为这里的目标是增加相对挖掘份额（而不是货币奖励）。

#### 3.2.1自私挖掘的最优策略

为了解决MDP的问题，我们将MDP求解器应用于有限状态空间MDP类[18]，并使用30个块的截止值。

.我们首先分析过期区块率对自私挖掘的影响。在图2中，我们比较了1％和10％的区块过期率下的自私开采，我们观察到对抗性开采力越高，私人矿工的相对收入越大（达到最大差异0.074）。 为了进行比较，我们绘制了自私挖掘的敌对相对收益的上限，这对应于通过利用一个区块来覆盖由诚实网络生成的一个块来最大化对手的优势的情况（如Sapirshtein等人报告[31]）。 正如我们所观察到的，考虑到网络延迟和我们通过区块过期率捕获的参数，超出了这个上限。

对于分别具有*α* = 0*.*1 and *α* =0*.*3的采矿权的对手，我们在图3中观察到，区块过期率与私人开采的相对开采收益之间存在非线性关系。

我们还研究了图4中日食攻击对自私挖掘的影响。在这里，我们只考虑攻击者*(i)*利用受害者挖掘力*ω*，并且*(ii)*利用所有受害者的块来推进他的私有链。 因此，我们只能确定这些限制条件下的最佳对抗选择。 我们观察到*ω*越高，他的自私挖掘能力就越强。我们注意到，对于一些*ω*值(例如, *ω* = 0*.*3, *α* = 0*.*38)，对于在其私有链中不包括受害者区块的对手来说更有价值。 这是因为受害者的奖励计入了诚实网络的奖励，因此减少了对手的相对份额。

## 3.3双重支出MDP

与自私挖掘不同的是，最优策略与诚实挖掘相比并不总是在财务上有所回报（参见第3节），我们继续研究最佳双重支出策略，我们假设一个理性对手对于最大化他的利益（以金融收益衡量）感兴趣。

我们默认要求每当攻击者开始双重支付攻击时（例如采取操作之后），他在网络中发布交易*Tl*，并且在其私有链中包括冲突的交易*Td* 。我们假定“失去”双重支出尝试的运营成本很小，因为对手有效地接受一个商品或服务来换取交易*Tl*。

除了自私挖掘所描述的状态之外，双重消费MDP还具有退出状态（参见表2）。 这个状态只有在敌对链在诚实的链（*la > lh*）之前至少有一个区块，经过*k*确认（*la > k*）之后，才能达到。 在达到退出状态之前，攻击者采取一个最优策略来使其报酬最大化，给出第3节所述的状态和行动空间。达到退出状态后，转换回诚实挖掘的退出状态模型奖励。请注意，由于我们假设对手是理性的，所以最优策略可能建议不要执行双重支出攻击（即对手永远不会达到退出状态)——取决于尝试攻击的值。在退出状态下，对手在日食攻击覆盖后获得区块奖励（因为对手的奖励需要打折作为*be* 受害者的区块，并且在对手进行覆盖操作后对手的区块链赢得比赛时奖励区块），对于每个状态转换我们打折采矿成本-*cm*。

对手要么遵守最佳的双重支出策略*π*，要么根据预期的奖励进行诚实的挖掘。因此，我们对最小双重支出值*vd*感兴趣，使得*vd*严格大于诚实的开采奖励（参见方程25）。

|  |  |
| --- | --- |
| *P* = (*α,γ,rs,k,ω,cm*) | (24) |

*vd* = min{*vd*|∃*π* ∈ *A* : *R*(*π,P,vd*) *> R*(honest mining*,P*)}

(25)

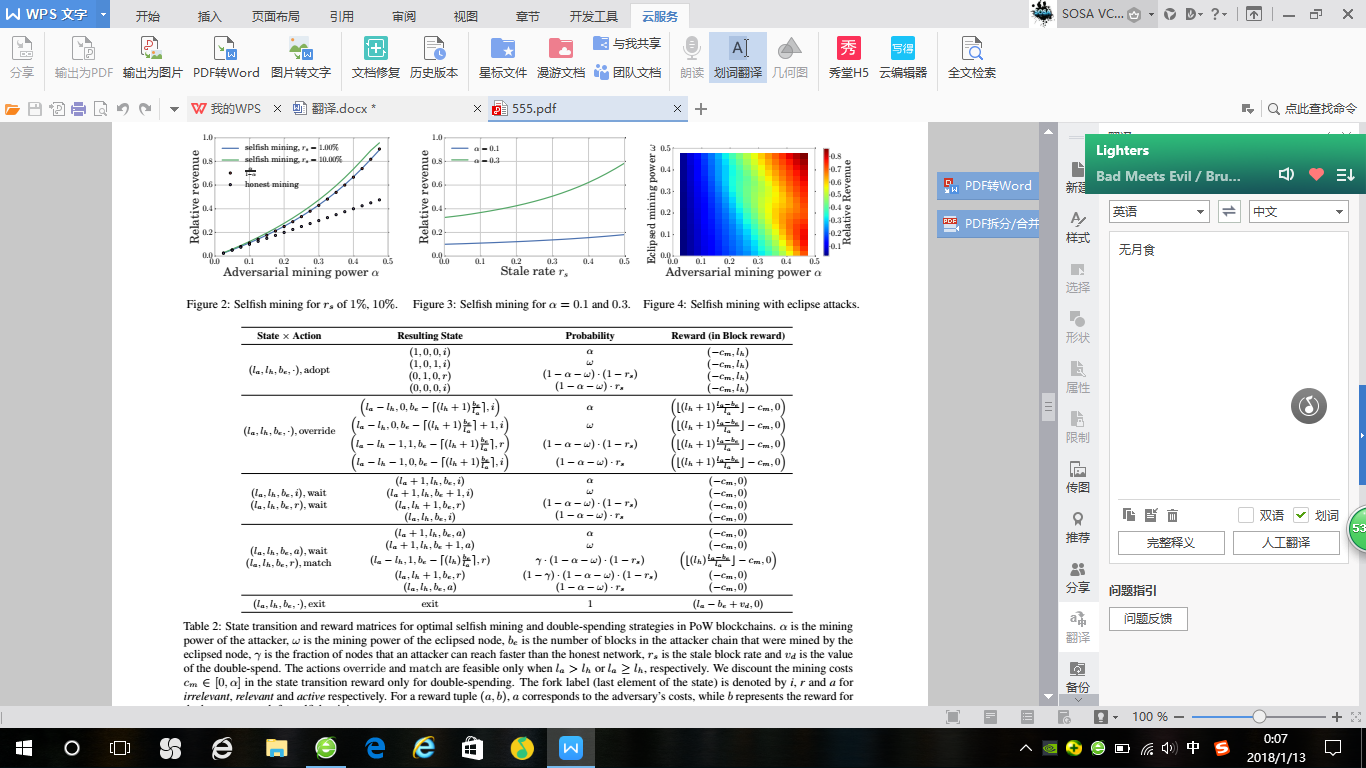
双重支出值*vd*可以作为一个通用指标来比较各种区块链实例的安全性。也就是说，如果对于给定的*α*, *γ 和ω*，如果区块链实例*A*的*vd* 大于区块链*B*，则区块链*A*可以被认为对于双重支出攻击更具抵抗性。

#### 3.3.1双重支出的最优策略

下面我们分析我们提到的各种参数的上述双重支出MDP的解决方案。为了解决我们MDP中的最优策略，我们依赖于pymdptoolbox库，并应用PolicyIteration算法[18] ，折扣值为0.999。 这种方法使我们能够评估交易确认数量*k*是否足以确保在存在理性对手的情况下的交易价值。也就是说，如果对手的双重支出的预期经济收益高于诚实的挖矿，那么在确认*k*的情况下交易不能被认为是安全的，并且商家应该等待额外的确认。

为了决定对手是应该选择遵循最优双重支出政策还是诚实挖掘（参见公式25），并确定最小值*vd*，我们将具有高双重支出值的双重支出MDP（> 109区块奖励）实例化，使得在最佳策略中可达到退出状态。如果策略包含退出状态，遵循最优双重支出策略的预期收益高于诚实的挖掘。否则，诚实开采是首选的策略。对于 *α*, *k*, *rs*, *γ* 和 *cm*，我们应用二进制搜索来找到最低的双重支出值（以区块奖励为单位，在0.1的误差范围内）。

在表3中，我们给出了*α* = 0*.*3（敌对开采能力），*γ* = 0（传播参数），*cm* = *α* （最大开采成本），*ω* = 0(没有日食攻击）



*表2：用于POW区块链中最佳自私挖掘和双重支出策略的状态转换和奖励矩阵。 α是攻击者的挖掘能力，ω是日食节点的挖掘能力，be 是日食节点挖掘的攻击者链中的区块数，γ是攻击者能够达到的比诚实的网络更快的比例，rs是陈旧的块率，vd是双重花费的价值。 只有当la > lh 或la* ≥ *lh时，这些动作重叠和覆盖才是可行的。 我们仅在双重开支的情况下折扣状态转换奖励的开采成本* *cm* ∈ [0*,α*] *。分标签（状态的最后一个元素）由i，r和a分别表示为不相关的，相关的和主动的。对于奖励元组*(*a,b*)*，a对应于对手的成本，而b表示对于自私挖掘的诚实网络的奖励。*

我们只观察等待，采取和退出行动。因为我们只能求解有限的MDP，所以我们选择20个区块的截断值，即对手的链条和诚实网络的链条都不能长于截断值。在下面的段落中，我们将更详细地讨论*α*, *γ*, *cm*, *rs*, *k*, *vd*和*ω*对最优双重支出策略的影响及其对交易确认安全性的影响。

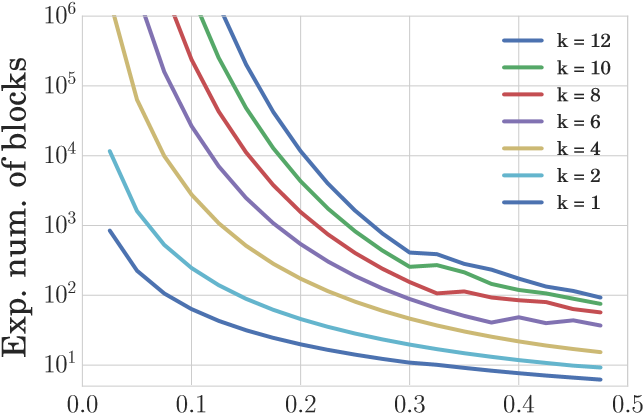
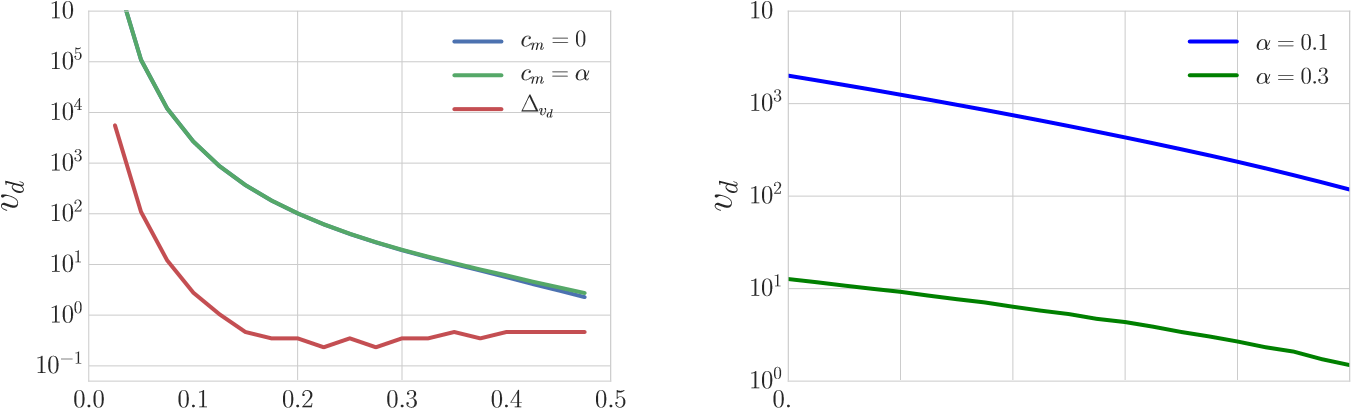
回想一下，我们的双重消费MDP的马尔可夫链的吸收状态[22]是退出状态。 通过计算马尔科夫链的基本矩阵[22]，我们计算马尔可夫链中预期的步数-在被退出状态吸收之前。这些步骤对应于成功的双重支出攻击所需的预期块数。在图5中，我们评估了预期的对抗开采能力和交易确认*次数k*的期望区块数。我们观察到，一个拥有超过0.25的挖掘能力的对手预计需要少于1000个成功的双重攻击（最多*k* = 10个确认），这相当于比特币的一周持续攻击时间。

**传播参数的影响**：回想一下，传播参数指定了攻击者的连接能力。在图8中，当分别*γ* = 0*,*0*.*5和1时，我们描述了与诚实开采相比可能导致经济收益的最小双重支出交易价值（参见公式25）。回想一下，只要商人接受的交易的价值低于*vd* ，给定这些参数，他就是安全的。

显然，

显然， *γ*越高，对手预期双重花费的交易价值就越低。 例如，如果攻击者在网络中具有*α* = 0*.*3的散列能力，假设*k* = 6 次确认，并且开采成本为*cm* = *α*，如果双重支出交易具有价值，则双重支出策略显然是有利的 在 *γ*= 1时，至少0.5区块奖励（一区块奖励是25比特币，其中一个比特币在写作时约为436.7美元，*rs* = 0*.*41%）。当 *γ*= 0.5时，最小交易值增加到12.9 块奖励。

**采矿成本的影响**：在图6中，我们分析了采矿成本对最小双重消费交易值的影响。我们的结果显示，开采成本可以忽略不计

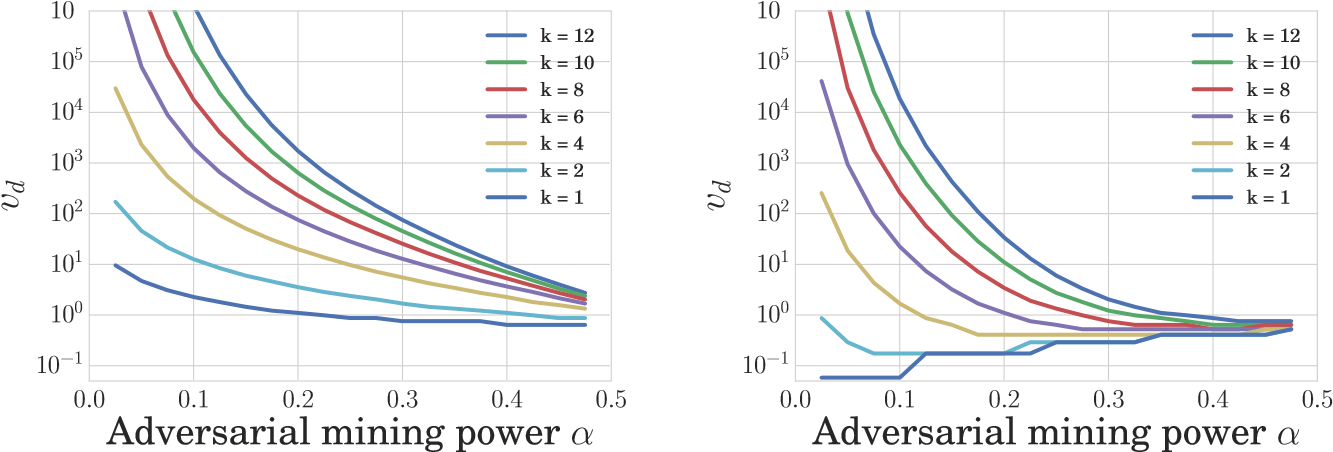
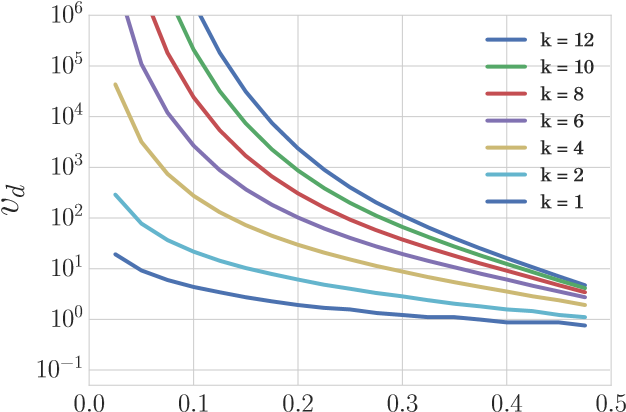


|  |  |
| --- | --- |
| *对抗性采掘能力α*  *图6：采矿成本cm对双重支出安全性的影响*(*rs* = 0*.*41%, *γ* = 0, *ω* = 0)*。*∆*vd是成本的差异。* | *区块过期率rs*  图7：对于*α* = 0*.*1, *α* = 0*.*3 and *k* = 6，*区块过期率rs*对双重支出的安全性的影响，给定*γ* = 0*.*5, *ω* = 0。 |

*对抗性采掘能力α*

图5：给定*rs* = 0*.*41%*,γ* = 0*,cm* = *α* 和*ω* = 0的预期成功双重消费区块数。

6

6 6

Adversarial mining POWer *α*

*对抗性采掘能力α*

|  |  |  |
| --- | --- | --- |
| (a) *γ* =0 | (b) *γ* =0*.*5 | (c) *γ* =1 |

图8：传播参数γ的影响。 我们观察到，参数*γ*越高，双重支出越低，比诚实开采更有利可图。*rs* = 0*.*41%（比特币的区块过期率），*cm* = *α* （最大开采成本），*ω* = 0（不发生日食攻击）。

*l*

*h*

*l*

*a*

7

5

3

4

0

1

2

6

8

0

\*\*\*

w\*\*

\*\*\*

\*\*\*

\*\*\*

\*a\*

\*\*\*

\*\*\*

\*\*\*

1

\*a\*

\*\*\*

\*\*\*

\*\*\*

\*\*\*

ww\*

\*\*\*

w\*\*

ww\*

2

ww\*

\*\*\*

ww\*

\*\*\*

\*\*\*

ww\*

\*a\*

w\*\*

ww\*

3

ww\*

ww\*

ww\*

\*a\*

\*\*\*

w\*\*

ww\*

ww\*

\*\*\*

4

ww\*

ww\*

\*a\*

ww\*

w\*\*

ww\*

\*\*\*

ww\*

ww\*

5

ww\*

ww\*

w\*\*

ww\*

ww\*

ww\*

ww\*

\*a\*

ww\*

6

ww\*

ww\*

ww\*

ww\*

ww\*

w\*\*

ww\*

ww\*

ww\*

7

e\*\*

e\*\*

ww\*

e\*\*

w\*\*

e\*\*

e\*\*

e\*\*

e\*\*

8

\*\*\*

e\*\*

w\*\*

\*\*\*

\*\*\*

\*\*\*

\*\*\*

\*\*\*

\*\*\*

表3：*α* = 0*.*3*,γ* = 0*,rs* = 0*.*41%*,cm* = *α,ω* = 0和*vd* = 19*.*5的最优双重支出策略。 这些行对应于对手链的长度la，列对应于诚实网络链的长度 *lh*。 每个表项中的三个值分别对应于不相关，相关和活动的分标签，其中*\**表示不可达的状态，*w*, *a*和*e*分别表示等待，采用和退出的操作。

对手策略影响

区块过期率的影响：我们评估了图7中采用*α* = 0*.*1 和 *α* = 0*.*3的挖掘强度的对手的区块过期率的影响。我们观察到，区块过期率和双重支出的价值有着非线性的关系，并且区块过期率越高，POW区块链的双重支出和自私的开采阻力越低（参见图7）。例如，对于采矿能力*α* = 0*.*3 和区块过期率为10％和20％的对手，双重支出值*vd*从9.2降低到6.4区块奖励。 同样，自私挖掘的相对收入（参见图3）也从0.37增加到0.43。

**日食攻击的影响**我们评估日食攻击对我们MDP的敌对策略的影响。 我们假设攻击者用采矿能力*ω*来掩盖

受害者，以增加维持区块链的优势（参见图9）。 我们观察到，日食攻击显然赋予对手权力，因为它允许敌手有效地提高其整体挖掘力量。 例如，一个*α* = 0*.*1的对手可以把*ω* = 0*.*025的双重消费值 *vd*从880区块奖励减少到0.75区块奖励。

#### 3.3.2比特币与 Ethereum

为了缓解过期区块降低工作量计算效率的问题，一些建议，如Ethereum，建议奖励矿工过期区块[4]。在这里，尽管包含在一个区块的uncle区块获得了奖励，但是他们并不参与计算链的总难度，也就是说， Ethereum 对uncle区块使用了最长的区块链法则。 这显然与 Ethereum 声称使用适应GHOST的区块链协议的声明相矛盾[33]。

Ethereum最近还修改了其最长区块链的算法，以合并均匀断系uniform tie breaking[10]。请注意，这样的策略意味着作为一种自私的采矿对策，但允许一个自私的矿工增加赶上诚实链的机会[31]。在表4中，我们扩展了我们的模型，以迎合uncle区块的奖励，并描述由此产生的双重消费MDP，以获得Ethereum的双重支出安全。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | 图9： | 图10: | 图11： | | *对于rs* = 0*.*41%*γ* = 0 和 *cm* = 0.的  日全食攻击 | 双重支出的阻力Ethereum(*k* ∈ {6*,*12}) 与比特币(*k* = 6)。2016-04-20USD汇率。 | Ethereum和Bitcoin之间的直接比较，k = 6，rs = 6.8％，各自的差值Δ*vd* 。 | |

在此分析的基础上，我们比较了图10中比特币（*rs*= 0.41％，参见表2中的MDP）和Ethereum（*rs*= 6.8％，参见表4中的MDP） 0，*cm* = 0和ω= 0。为了提供公平的成本比较，我们依靠美元的估值（比特币的块奖励比Ethereum的块奖励高200多倍）。

我们观察到，6个比特币区块确认比6个Ethereum（区块生成时间在10到20秒之间）区块确认更容易复原。其次，在比较12个Ethereum和6个比特币区块确认的情况下，Ethereum的双重支出恢复能力只比对于比特币散列功率小于11％的对手要好。请注意，在不到4分钟的时间内就可能生成12个Ethereum块，而6个比特币块则持续大约1个小时。第三，我们发现区块奖励的货币价值直接影响到双重支出的安全性：区块链的区块奖励（单位为美元）越高，抗双重支出的弹性就越大。除了将比特币与Ethereum进行比较，我们通过将比特币的区块过期率设置为等于Ethereum的区块过期率来比较图11中的两个区块链，以客观评估其安全隐患。我们观察到，尽管依靠uncle区块奖励和均匀断系，Ethereum的安全性还是比比特币更弱，可以断定是均匀断系和uncle奖励降低了Ethereum区块链的安全性。

## 4.POW区块链的性能与安全

在本节中，我们通过利用我们在第3节中的模型来评估各种区块链实例的性能（和安全性）。

为此，我们构建了比特币区块链模拟器，以便从性能角度评估不同的区块链实例。由于无论是正式的建模，还是数千个对等的部署（例如，目前在比特币中有6000个可到达的节点），依赖模拟是现实地捕捉不同参数下的区块链性能的唯一可行的选择

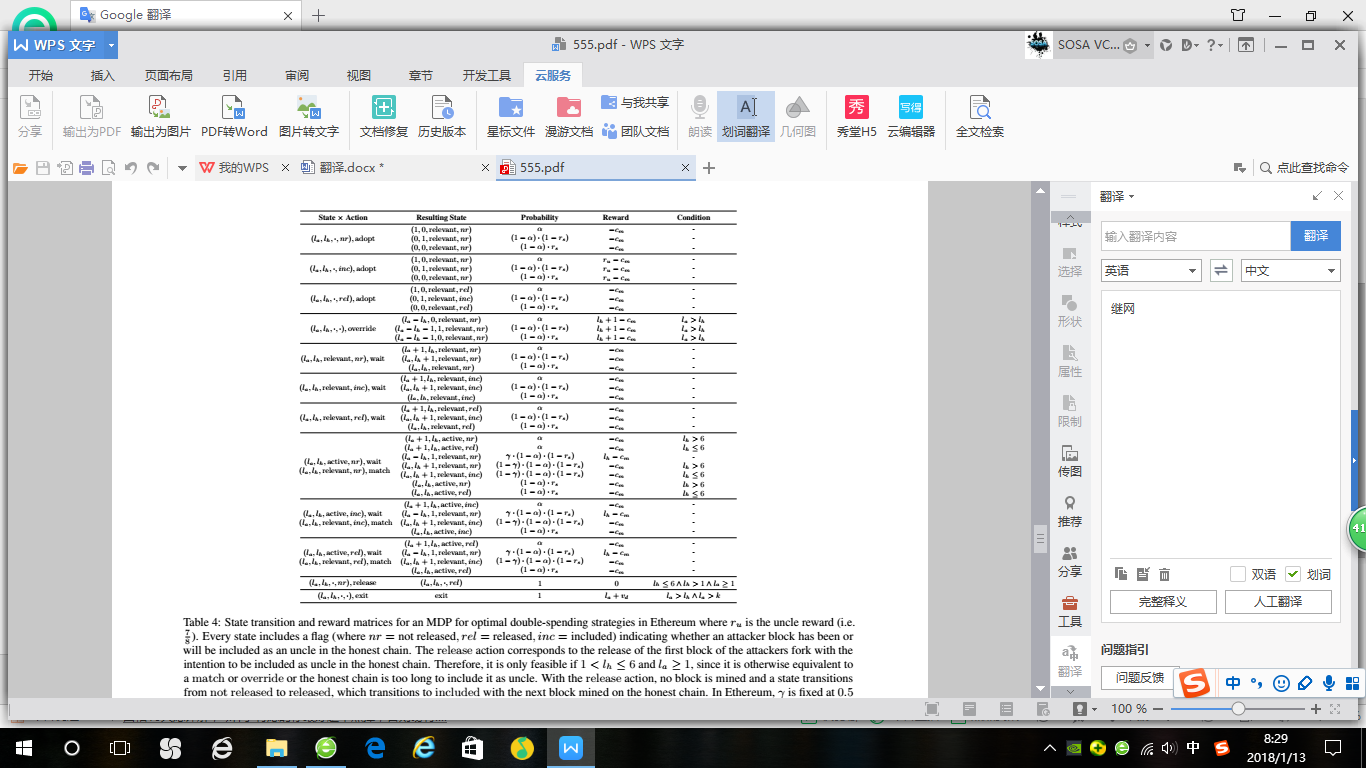
通过我们的模拟器，我们评估不同的区块链参数，如区块间隔，区块大小，传播机制，通过测量结果的区块过期率 ，吞吐量和区块传播时间。这也使我们能够在一个统一的框架中将我们的区块链模拟器连接到我们的MDP模型。也就是说，我们将模拟器输出的区块过期率，并将其输入到我们的MDP模型中，以评估区块链实例的安全性（在自私挖掘和双重支出情况下）。

### 4.1区块链模拟器

在表5中，我们总结了模拟器捕获的参数。在这里，我们通过给每个矿工赋予特定的采矿能力来模拟矿工的工作量。基于块间隔分布（其定义了块被发现的时间），然后将新区块归属于矿工。符合现有POW区块链的操作，矿工挖掘他收到的第一个区块的矿工矿，我们假设分叉最本质的解决了最长的链规则。一旦分叉解决了，那些对主链没有贡献的块被认为是陈旧的块。在我们的模拟中，我们不考虑不同块之间的难度变化;因此最长的链只是由其区块的数量来定义。

在建立节点之间的连接时，我们在它们之间建立点对点的通道，从而将任何中间设备（路由，交换机等）都抽象出来。这些渠道有两个特点：延迟和带宽。为了捕捉网络中的实际等待时间，我们采用了Verizon的全球IP等待时间统计[36]，并假设了一个Pareto分布，其方差占平均等待时间的20％[2]。另一方面，为了模拟网络中现实的带宽分配，我们在testmy.net调整了分配6[34]。

我们的模拟器不能模拟交易的传播，因为我们模拟器的焦点是研究块大小，区块间隔和区块请求管理系统的影响 - 所有这些都可以独立于交易传播而被捕获。请注意，交易是在区块大小内隐式捕获的。在我们的模拟器中，我们区分两种节点类型：（i）常规节点和（ii）矿工。对于常规节点（高达6000），我们从位节点检索21.co当前的地理节点分布（参考图12a）并采用这种分布来定义我们的模拟节点的位置。我们还根据Verizon [2,36]和testmy.net [34]调整了带宽和网络延迟（根据地理位置）。为了模拟矿工，我们从blockchain.info中检索矿池分配，并相应地将矿池的公共节点分配到各个区域（参见图12b）。采矿池通常保持彼此之间的私人对等连接 - 这是我们在模拟中获取的。除了直接对等外，目前许多采矿池都参与了Matt Corallo的中继网络[6]，该网络独立于默认的比特币P2P覆盖网络运行（参见2.2节）。我们还捕获中继网络，并假设我们的模拟中，每当中继时，所有的矿工都参与中继网络。



.表4：一个MDP的状态转换和奖励矩阵，用于Ethereum中最佳的双重支出策略，其中*ru* 是uncle的奖励。（即）。 每个状态都包含一个标志（其中*nr*=未释放，*nr* =释放，*inc* =包含），指示攻击者块是否已经或将被包含在诚实链中的uncle中。释放行动相当于释放第一批袭击者的分叉，意图被列为诚实链中的uncle。 因此，，仅当 1 *< lh* ≤ 6 且 *la* ≥ 1是可行的，因为它在其他方面相当于覆盖或超越，或者诚实链条太长而不能将其包含为uncle。 通过释放动作，没有区块被挖掘，并且状态从未释放到已释放的状态转换，转换到包含在诚实链上的下一个块中。对于Ethereum，γ固定为0.5。

即使没有准备好的块，也可以进行比赛。

|  |  |
| --- | --- |
| **共识参数** | 说明 |
| 块区间分布 | 查找区块的时间 |
| 矿工采矿能力分配 | 工作量证明能力分配 |
| **网络层参数说明** | 说明 |
| 块大小分布 | 可变交易负载 |
| 可达网络节点# | 打开TCP端口节点 |
| 地理·节点分布 | 全球分布 |
| 地理·采矿池分布 | 全球分布 |
| 网络中每个节点的连接数# | 在网络中 |
| 挖掘者连接数量# | 在网络中 |
| 区块请求管理系统 | 可能的协议 |
| 标准机制 (inv/getdata) | 默认 |
| 主动的区块推送 | 矿工只生产区块 |
| 中继网络 | Miner network矿工网络 |
| Sendheaders | 比特币v0.12 |

表5：区块链模拟的参数

网络选项已启用。

### 4.2评估结果

接下来，我们介绍我们评估的结果。

#### 4.2.1 模拟器验证

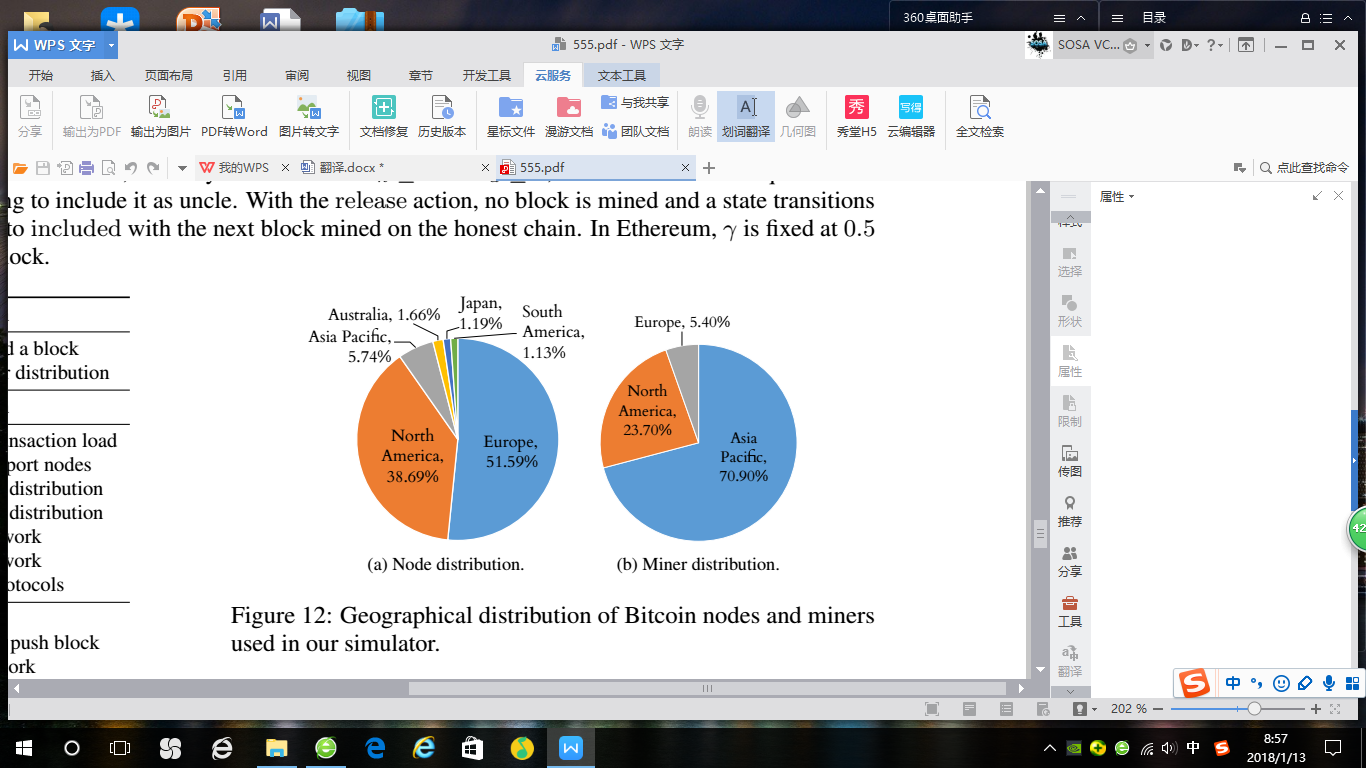


图12：在我们的模拟器中使用的比特币节点和矿工的地理分布。

为了实验验证我们的模拟，我们将比特币，Litecoin和Dogecoin与他们各自的模拟对手进行了比较。 对于每个区块链，我们根据已调查区块链的现有部署所具有的当前参数调整了表5的参数。 例如，我们在2015年5月至11月的实际比特币网络中测量比特币的区块大小分布以及区块生成率 [21]。

|  |  |  |  |
| --- | --- | --- | --- |
|  | Bitcoin比特币 | Litecoin | Dogecoin |
| 区块间隔 | 10 min | 2.5 min | 1 min |
| 测得的 *tMBP* | 8.7 s [8] | 1.02 s | 0.98 s |
| 模拟的 *tMBP* | 9.42 s | 0.86 s | 0.83 s |
| 测得的 *rs* | 0.41 % | 0.27 % | 0.62 % |
| 模拟的*rs* | (a)0.14%-(b)1.85% | (b)0.24 % | (b)0.79 % |

为了测量实际区块链网络中的区块过期率*rs*，我们检索了10万Litecoin和24万Dogecoin区块24,000个比特币区块。 此外，我们还采用了来自公共资源探索者矿业开采权力分配的方式。在我们的模拟中每个节点的连接数量遵循Miller等人的分布。[26]。

表6：实际网络和仿真中的中值块传播时间（tMBP，以秒为单位）和*rs*（每个区块链10000个块）。 （a）假定所有的矿工都使用中继网络和自发的区块推送，而（b）只有标准的传播机制。 我们得出这样的结论：并不是比特币中的所有矿工都使用中继网络和自主的块推送。

我们的发现（参见表6）表明，我们的模拟器很大程度上捕获了现有区块链部署的性能。例如，我们的结果显示，测量的和模拟的中值块传播时间相对接近。 Litecoin和Dogecoin的过期区块率特别接近。 在比特币的情况下，在所有矿工使用中继网络和主动模块推送的情况下，以及极端情况下过期区块率降低，此时矿工不使用中继网络和主动模块推送。 请注意，Litecoin和Dogecoin没有任何中继网络。

#### 4.2.2 区块间隔的影响

在本节中，我们研究块区间对中间块传播时间的影响以及基于区块链中的区块过期率。为此，我们运行我们的模拟器，用于25分钟到0.5秒的不同块间隔时间（参见表7）。每个模拟独立运行10000个连续的块，和四个不同的块请求管理系统组合中的每一个：（情况1）标准块请求管理，（情况2）由矿工主动块推动增强的标准块请求管理，（情况3）以前的组件加上中继网络，以及（情况4）具有未经请求的块推送和中继网络的发送报头机制。

我们首先观察到，对于10分钟的块间隔时间和标准的请求管理系统，我们的区块过期率为1.85％，这与Wattenhofer等人报道的1.69％相当[9]。回想一下，在Wattenhofer的研究时间，未经请求的块推送和中继网络尚不可用。

其次，我们观察到，对矿工的主动推销大大降低了区块过期率。这是因为（i）矿工相互联系并从主动推块中获得最大利益，以及（ii）第一个节点的传播方法对于快速到达大多数网络是至关重要的。中继网络的增加似乎不会显著地影响区块过期率（考虑到比特币的交易负载），而且主动的数据块推送比较少，而且传播时间也只是略微减少。然而，对于更大的块大小（例如> 2MB），中继网络确实比主动块推送提供了优势（参见表8）。此外，除了传统的P2P覆盖网络之外，中继网络还提供了额外的块信息源。注意，尽管发送头部机制与完全部署的中继网络和主动的块推送的影响有限，但这种机制可以减轻偏食攻击[16]。

为了评估块间隔对POW区块链安全性的影响，我们将得到的区块过期率输入到我们的MDP模型中，如表7所示。我们的结果表明，对于配备30％总采矿能力[[1]](#footnote-0)的对手，共识时间越少，自私挖掘的相对收入就越高，双重支出价值更低。我们观察到，区块传播机制显着影响区块链的安全性，因为它直接影响区块过期率。与其他评估块传播机制相比，标准块传播机制提供了较小的弹性（在双重开支和自私挖掘方面）。我们还注意到，当将块间隔从25分钟减少到0.5秒时，表7中对于情况4的块传播机制（其导致与其他调查机制相比最低的区块过期率）的双花费值减半。同样，自私采矿的相对收入也从0.33增加到0.42。

#### 4.2.3区块大小的影响

我们现在研究区块大小对区块链性能和安全性的影响（参见表8）为此，我们模拟区块大小从0.1 MB到8 MB，给定10分钟的区间间隔。

我们的结果表明块传播时间随着块大小线性增加到4MB; 在8 MB块之后，块传播时间和区块过期率呈指数增长。其次，我们清楚地看到，更好的块传播机制显著减少了传播时间和区块过期率 。

这也表明，与我们的MDP模型一致，区块越大，自私挖掘的相对收入越高，双重支出价值越低（参见表8）。然而显而易见的是，一个高效的数据块传播机制可以有效地使网络保持几乎相同的安全规定，防止自私挖掘和双重支出，正如我们在案例3（标准传播机制，未经请求的数据块推送，中继网络）和案例4 （发送头传播机制，主动推块，中继网络）。这证实了高效的网络传播机制有助于提高区块链的安全性。有趣的是，考虑到情况4的区块传播机制，当将区块大小从0.1MB增加到8MB（*vd* 从12.9变化到12.68区块奖励时），表8中的恢复能力（在双重支出值方面）没有显着变化）。同样，当所有的矿工都使用中继网络时，自私采矿的相对收入保持在*rrel* = 0.33。

目前，许多提议建议将区块分块并且同时下载这些块（例如，Blocktorrent [35]）。在我们进行的一个单独的实验中，我们实现了一个区块传播机制，将块分成可以从多个对等设备查询的几千字节的块。我们的结果表明，当处理适度的块大小（即，小于8MB）时，与发送报头和中继网络协议相比，这种协议不会改进中值块传播时间。这是由于分块的块传播比节点的第10和第25个百分点慢，这是因为：（i）由块引起的通信开销，以及（ii）因为如果相应的块具有块，则节点仅转发块块已被验证。

#### 4.2.4吞吐量

我们现在评估各种区块链实例的吞吐量。 为此，我们改变块大小（从0.1M B到8MB）和块间隔（从0.5秒到25分钟），以捕获更多的区块链实例与我们的模拟器。 在这里，我们假设网络依赖于有效的传播

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  | Case 1 |  |  |  | Case 2 |  |  |  | Case 3 |  |  |  | Case 4 | |  | | Block interval | *tMBP* | *rs* | *vd* | *rrel* | *tMBP* | *rs* | *vd* | *rrel* | *tMBP* | *rs* | *vd* | *rrel* | *tMBP* | *rs* | *vd* | *rrel* | | 25 minutes | 35.73 | 1.72 % | 12.47 | 0.34 | 25.66 | 0.16 % | 12.86 | 0.33 | 22.50 | 0.03 % | 12.89 | 0.33 | 22.44 | 0.02 % | 12.89 | 0.33 | | 10 minutes | 14.7 | 1.51 % | 12.52 | 0.34 | 10.65 | 0.13 % | 12.88 | 0.33 | 9.41 | 0.14 % | 12.86 | 0.33 | 9.18 | 0.13 % | 12.87 | 0.33 | | 2.5 minutes | 4.18 | 1.82 % | 12.45 | 0.34 | 2.91 | 0.16 % | 12.86 | 0.33 | 2.60 | 0.16 % | 12.86 | 0.33 | 2.59 | 0.15 % | 12.86 | 0.33 | | 1 minute | 2.08 | 2.15 % | 12.35 | 0.34 | 1.34 | 0.35 % | 12.81 | 0.33 | 1.30 | 0.25 % | 12.83 | 0.33 | 1.27 | 0.29 % | 12.77 | 0.33 | | 30 seconds | 1.43 | 2.54 % | 12.06 | 0.34 | 0.84 | 0.45 % | 12.78 | 0.33 | 0.84 | 0.51 % | 12.77 | 0.33 | 0.84 | 0.52 % | 12.69 | 0.33 | | 20 seconds | 1.21 | 3.20 % | 11.73 | 0.34 | 0.67 | 0.86 % | 12.68 | 0.33 | 0.69 | 0.85 % | 12.68 | 0.33 | 0.68 | 0.82 % | 12.68 | 0.33 | | 10 seconds | 1.00 | 4.77 % | 10.73 | 0.35 | 0.35 | 1.73 % | 12.46 | 0.34 | 0.33 | 1.41 % | 12.54 | 0.34 | 0.53 | 1.59 % | 12.50 | 0.34 | | 5 seconds | 0.89 | 8.64 % | 10.08 | 0.37 | 0.37 | 2.94 % | 11.85 | 0.34 | 0.45 | 2.99 % | 11.80 | 0.34 | 0.44 | 3.05 % | 11.78 | 0.34 | | 2 seconds | 0.84 | 16.65 % | 7.35 | 0.41 | 0.40 | 6.98 % | 10.47 | 0.36 | 0.39 | 7.28 % | 10.37 | 0.36 | 0.38 | 7.10 % | 10.42 | 0.36 | | 1 seconds | 0.82 | 26.74 % | 4.37 | 0.53 | 0.53 | 12.44 % | 8.34 | 0.39 | 0.38 | 12.59 % | 8.24 | 0.39 | 0.37 | 12.52 % | 8.30 | 0.39 | | 0.5 seconds | 0.82 | 38.15 % | 2.78 | 0.60 | 0.61 | 20.62 % | 6.22 | 0.42 | 0.49 | 20.87 % | 6.16 | 0.42 | 0.36 | 21.10 % | 6.02 | 0.42 |   表7：在给定当前比特币块大小分布的情况下，区块间隔对中值块传播时间（tMBP）以秒为单位的区块过期率*rs*, *vd* 和 *rrel*的影响，*α* = 0*.*3且*k* = 6的对手。情况1是指标准块传播机制，情况2是指标准机制加上主动块推送，情况3是情况2加上中继网络，情况4到发送头与主动块推送和中继网络的组合。   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  | Case 1 |  |  |  | Case 2 |  |  |  | Case 3 | |  |  | Case 4 | |  | | Block Size | *tMBP* | *rs* | *vd* | *rrel* | *tMBP* | *rs* | *vd* | *rrel* | *tMBP* | *rs* | *vd* | *rrel* | *tMBP* | *rs* | *vd* | *rrel* | | 0.1 MB | 3.18 | 0.32 % | 12.80 | 0.33 | 2.12 | 0.03 % | 12.89 | 0.33 | 2.02 | 0.03 % | 12.89 | 0.33 | 2.02 | 0.2 % | 12.90 | 0.33 | | 0.25 MB | 7.03 | 0.88 % | 12.67 | 0.33 | 4.93 | 0.11 % | 12.87 | 0.33 | 4.49 | 0.05 % | 12.88 | 0.33 | 4.46 | 0.17 % | 12.87 | 0.33 | | 0.5 MB | 13.62 | 1.63 % | 12.48 | 0.34 | 9.84 | 0.13 % | 12.87 | 0.33 | 8.65 | 0.05 % | 12.88 | 0.33 | 8.64 | 0.06 % | 12.87 | 0.33 | | 1 MB | 27.67 | 3.17 % | 11.79 | 0.34 | 20.01 | 0.38 % | 12.79 | 0.33 | 17.24 | 0.07 % | 12.88 | 0.33 | 17.14 | 0.07 % | 12.88 | 0.33 | | 2 MB | 57.79 | 6.24 % | 10.57 | 0.36 | 44.6 | 1.12 % | 12.61 | 0.34 | 35.49 | 0.08% | 12.87 | 0.33 | 35.38 | 0.1 % | 12.86 | 0.33 | | 4 MB | 133.30 | 11.85 % | 8.20 | 0.38 | 126.57 | 5.46 % | 10.51 | 0.35 | 78.01 | 0.12 % | 12.85 | 0.33 | 78.40 | 0.13 % | 12.66 | 0.33 | | 8 MB | 571.50 | 29.97 % | 4.11 | 0.53 | 875.97 | 15.64 % | 7.64 | 0.41 | 555.49 | 0.43 % | 12.65 | 0.33 | 550.25 | 0.4 % | 12.68 | 0.33 |   表8：考虑到当前比特币块生成间隔和α= 0.3和k = 6的对手，区块大小对以秒为单位的块中值传播时间（tMBP），区块过期率*rs*, *vd* 和 *rrel*的影响。 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| tps | *vd* | *rrel* | 区块大小 | 区块间隔 |
| 33.4 | 12.75 | 0.33 | 0.25MB | 30 seconds |
| 40 | 12.38 | 0.34 | 0.10MB | 10 seconds |
| 50 | 12.45 | 0.34 | 0.25MB | 20 seconds |
| 66.7 | 12.06 | 0.34 | 0.25MB | 15 seconds |
| 66.7 | 12.65 | 0.33 | 0.50MB | 30 seconds |
| 66.7 | 12.71 | 0.33 | 1.00MB | 1 minute |

表9：采用30％采矿能力，k = 6，给定16个采矿池的对手每秒交易吞吐量（tps）与*vd* 和*rrel*的安全性。

对于每个模拟区块链实例，我们计算每秒交易处理的结果吞吐量（tps），测量区块过期率并推断*vd* 和*rrel*，以便用我们的MDP模型评估区块链的安全性（参见第3节）。 我们还假定平均交易规模为250字节，k = 6，双重支出确认和0.3采矿权和γ= 0.5的对手。

在表9中，我们有选择地列出候选区块链实例，其可以实现超过60 tps的交易吞吐量，并实现与现有比特币系统类似的安全措施。 显然，我们的结果表明，不同的参数配置可以产生相同的吞吐量 - 虽然具有不同的安全规定（由于不同的区块过期率 ）。 具体来说，我们观察到低的一致性间隔提供了较低的安全性，相比于整体吞吐量相同的较高的一致性区间，因为网络需要更多的往返行程才能将相同的信息提交到区块链。 我们的研究结果表明，在不明显影响安全性的情况下，有足够的空间来提高现有POW的可扩展性。

## 5.相关工作

一些成果分析了比特币的双重支出攻击[15,30]），但他们并没有考虑最佳的对抗策略。

Eyal和Sirer [14]表明，一个自私的矿工可以通过不直接发布他的块来增加其相对的矿业收入。 同样，Courtois和Bahack [7]研究颠覆性的采矿策略。 我们的工作与Sapirshtein等人有相似之处。[31]。 在这里，作者为比特币的自私挖掘设计了最佳对抗策略。 与[31]不同的是，我们的工作捕获了POW驱动区块链的最优对抗自私挖掘策略，并考虑了网络延迟和日食攻击。 我们另外捕获最佳的双重支出策略 - 我们也考虑到对手的开采成本，所需的块确认次数和双重支出值，以便正确计算出攻击的成本。

GHOST [33]是用于在基于POW的区块链中建立共识的最长链规则的替代方案，并且旨在减轻陈旧区块的负面影响。已经提出了许多替代方案。在证明权益（PoS）[29]中，同行的投票权基于他们在各个区块链系统中拥有的“股份”数量。烧伤证明（PoB）是一个建议，以烧毁交易输出来替代POW，使其不能再花费。然而，现有的基于PoB的区块链依赖于POW来创建区块，因此最终依靠POW来创造硬币。容量证明（PoC），旨在使用可用的硬盘空间来替换POW。 Bitcoin-NG [13]执行POW的领导者选举，允许领导者签署微型组织，直到选出新的领导者。文献中提出了一些额外的建议[19,23,25,37]，这些建议依赖于经典的拜占庭容错共识协议，希望能够提高共识效率，实现高交易吞吐量。最近的研究提出结合使用POW和BFT协议来实现高性能开放共识协议（Byzcoin [24]）。

## 6.结语

在这项工作中，我们引入了一个新颖的定量框架，客观地比较了POW区块链，给出了真实世界网络影响和区块链参数。 我们的框架使我们能够评估网络层参数对基于POW的区块链安全性的影响。 通过这样做，我们展示了如何客观比较不同POW区块链实例的安全规定。 也就是说，我们的框架允许我们在每秒交易吞吐量方面推动POW动力区块链的边界，同时观察对最优自私挖掘和双重支出策略的区块链安全规定的影响。

例如，我们发现Ethereum需要至少37个区块确认，才能将比特币的安全性与6个区块确认结果进行匹配，因为对手拥有30％的采矿权。我们的结果间接表明比特币的区块链比Ethereum的区块链提供更多的安全性，奖励矿工uncle的奖励，并为区块链分辨率执行统一的平局。我们的结果还表明，现有的POW区块链可以实现每秒60个交易的吞吐量，而不会显着影响区块链的安全性。据我们所知，这是定量评估过期区块率对POW区块链的最佳双重支出和自私采矿抵抗的影响的第一个贡献（参见图7和图3）。通过这样做，我们的结果定量捕捉交易的安全性，基于它们的价值和区块确认 - 有效地量化比特币中着名的所需六个区块确认所实现的安全水平。

我们的见解不仅允许商家在接受交易时考虑到安全条款，并评估他们各自的双重支出风险，而且还帮助矿工量化POW区块链对自私挖掘的抵御能力。

## 7.参考文献

1. Bitcoin block size limit controversy, 2016. Available from:

https://en.bitcoin.it/wiki/Block\_size\_limit\_controversy.

1. Frederik Armknecht, Jens-Matthias Bohli, Ghassan O Karame, Zongren Liu, and Christian A Reuter. Outsourced proofs of retrievability. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 831–843. ACM, 2014.
2. Bitnodes. Bitnodes ip crawler. Available from: https://github.com/ayeowch/bitnodes.
3. V. Buterin. A next-generation smart contract and decentralized application platform, 2014.
4. Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In *OSDI*, volume 99, pages 173–186, 1999.
5. Matt Corallo. Bitcoin relay network. Available from: http://bitcoinrelaynetwork.org/.
6. Nicolas T. Courtois and Lear Bahack. On subversive miner strategies and block withholding attack in bitcoin digital currency. *CoRR*, abs/1402.1718, 2014.
7. Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, and Emin Gün. On scaling decentralized blockchains.
8. C. Decker and R. Wattenhofer. Information Propagation in the

Bitcoin Network. In *13-th IEEE International Conference on Peer-to-Peer Computing*, 2013.

1. Ethereum. Ethereum tie breaking. Available from: https://github.com/ethereum/go-ethereum/commit/ bcf565730b1816304947021080981245d084a930.
2. Ethereum. ethernodes. Available from:

https://www.ethernodes.org/network/1.

1. Ethereum. ethstats. Available from: https://ethstats.net/.
2. Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer, and Robbert van Renesse. Bitcoin-ng: A scalable blockchain protocol. *arXiv preprint arXiv:1510.02037*, 2015.
3. Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security*, pages 436–454. Springer, 2014.
4. The Finney Attack, 2013. Available from: https:

//en.bitcoin.it/wiki/Weaknesses#The\_.22Finney.22\_attack.

1. Arthur Gervais, Hubert Ritzdorf, Ghassan O Karame, and Srdjan Capkun. Tampering with the delivery of blocks and transactions in bitcoin. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 692–705. ACM, 2015.
2. E. Heilman, A. Kendler, A. Zohar, and S. Goldberg. Eclipse attacks on bitcoin’s peer-to-peer network. 2015.
3. Ronald A Howard. *Dynamic Probabilistic Systems, Volume I: Markov Models*, volume 1. Courier Corporation, 2012.
4. IBM. Ibm openblockchain. Available from: http://www.ibm.com/blockchain/.
5. Intel. Proof of elapsed time (poet). Available from: http://intelledger.github.io/.
6. Ghassan O. Karame, Elli Androulaki, and Srdjan Capkun.

Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS ’12, New York, NY, USA, 2012. ACM.

1. John G Kemeny, J Laurie Snell, and Gerald L Thompson.

Finite mathematics. *DC Murdoch, Linear Algebra for Undergraduates*, 1974.

1. Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. Enhancing bitcoin security and performance with strong consistency via collective signing. *arXiv preprint arXiv:1602.06997*, 2016.
2. Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. Enhancing bitcoin security and performance with strong consistency via collective signing. *CoRR*, abs/1602.06997, 2016.
3. D. Mazieres. The stellar consensus protocol: A federated model for internet-level consensus. Available from: https: //www.stellar.org/papers/stellar-consensus-protocol.pdf.
4. Andrew Miller, James Litton, Andrew Pachulski, Neal Gupta, Dave Levin, Neil Spring, and Bobby Bhattacharjee.

Discovering bitcoin’s public topology and influential nodes.

1. S. Nakamoto. Bitcoin: A p2p electronic cash system, 2009.
2. Kartik Nayak, Srijan Kumar, Andrew Miller, and Elaine Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. Technical report, IACR Cryptology ePrint Archive 2015, 2015.
3. QuantumMechanic. Proof of stake. Available from:

https://bitcointalk.org/index.php?topic=27787.0.

1. Meni Rosenfeld. Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*, 2014.
2. Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar. Optimal selfish mining strategies in bitcoin. *arXiv preprint arXiv:1507.06183*, 2015.
3. Yonatan Sompolinsky and Aviv Zohar. Accelerating bitcoin’s transaction processing. fast money grows on trees, not chains.

*IACR Cryptology ePrint Archive*, 2013:881, 2013.

1. Yonatan Sompolinsky and Aviv Zohar. Secure high-rate transaction processing in bitcoin. In *Financial Cryptography and Data Security*, pages 507–527. Springer, 2015.
2. testmy.net. testmy.net. Available from: http://testmy.net/country.
3. Jonathan Toomim. blocktorrent. Available from: http://lists.linuxfoundation.org/pipermail/bitcoin-dev/ 2015-September/011176.html.
4. Verizon. Verizon latency. Available from:

http://www.verizonenterprise.com/about/network/latency/.

1. Marko Vukolic. The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In *Proceedings of the IFIP WG 11.4 Workshop iNetSec 2015*. 2015.

1. 比特币对恶意矿工的适应能力是基于这样的假设，即对手不能收获总采矿能力的30％以上[14,16] [↑](#footnote-ref-0)