关于工作区块链的安全性和性能的证明

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

VasileiosGlykantzis ETH Zurich, Switzerland glykantv@student.ethz.ch

HubertRitzdorf ETH Zurich, Switzerland hubert.ritzdorf@inf.ethz.ch

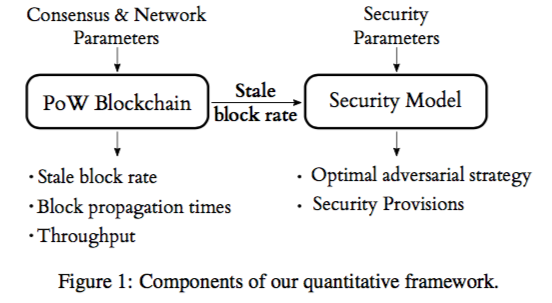
SrdjanCˇapkun ETH Zurich, Switzerland srdjan.capkun@inf.ethz.ch

文摘

现有数字货币的总市值的90%以上都是由“工作证明”(PoW)驱动的区块链。虽然已经对比特币的安全规定进行了深入的分析，但在文献中并没有过多的注意到变形(分叉)PoW区块链的安全保证(用不同的参数实例化)。

本文介绍了一种新的定量框架，分析了PoW区块链的各种参数和网络参数对安全性和性能的影响。基于我们的框架，在考虑网络传播、不同块大小、块生成间隔、信息传播机制以及eclipse攻击的影响等现实世界约束的基础上，设计出了双支出和自私挖掘的最优对抗策略。因此，我们的框架允许我们捕获现有的基于应用程序的部署，以及使用不同参数实例化的PoW区块链变体，并对它们的性能和安全条款之间的权衡进行比较。

1.介绍

自2009年成立以来，比特币的区块链一直在推动着inno的使用，而一些新颖的应用，如智能合同，已经被设计用来利用区块链。为了微调这个骗局，比特币已经被多次分叉。，块生成时间和哈希函数)，以及网络参数(例如，块大小和信息传播协议)，并提高区块链的效率。例如，Litecoin和dogecoin -比特币的最著名的forks——将block的生成时间从10减少到2.5和1分钟。与这些努力并行的是，备选的分散的基于区块链的网络(比如Ethereum)出现了，其目标是优化协商一致意见和网络参数，并简化在区块链之上部署分散的应用程序。

尽管有许多协商一致的协议(PBFT[5]，风险证明[29]，证明了经过的时间[20])，但大多数现有的区块链都利用了计算上昂贵的工作证明(PoW)共识机制，目前该机制占现有数字货币总市值的90%以上。虽然对比特币的安全规定进行了彻底的分析[14,21,30,32]，但不同的PoW区块链的安全保证在文献中并没有得到太大的重视。最近的研究表明，不能在不影响其安全性的前提下提高基于PoW的区块链的性能。然而，目前还没有对PoW区块链的性能与安全性的关系进行详细的研究。

本文针对这一问题，提出了一种新颖的权能框架，分析了PoW区块链的各种一致性和网络参数的安全性和性能。利用我们的框架，我们捕获了现有的PoW实例化(例如，比特币、Ethereum、Litecoin和Dogecoin)的安全属性，以及其他可能的实例，这些实例可能受到不同的一致意见和网络参数的影响。

我们的框架(cf .图1)包含两个关键元素:(i)区块链实例和(ii)区块链安全模型。一个区块链实例是一个PoW区块链，它实例化了一组给定的协商一致和网络参数，如网络延迟、块生成时间、块大小、信息传播mech - anisms等。例如，比特币、Litecoin和Ethereum corre- spond到3个区块链实例。为了逼真地捕捉到其他区块链实例，我们设计了一个仿真器，通过实现基于广告的信息传播、主动块推送、中继网络、sendheader传播机制等，来模拟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)陈旧的(孤立的)块速率，它被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(MDP)重复花费和自私的挖掘,让我们思考最佳的乱发广告——sarial策略时考虑到敌对的挖掘能力,eclipse攻击的影响,块奖励,和现实世界网络和共识parameters-effectively被陈旧的块率。

考虑到当前比特币社区中关于一个合适的最大块大小的讨论，确保了系统的可伸缩性和增长[1]，我们的工作提供了一种方法，可以在不同参数(包括块大小)的情况下，对PoW区块链的安全性和性能进行比较。例如,我们发现，将块大小从当前的比特币交易负载(平均0.5 MB)增加到4 MB，并不能明显地影响到区块链传播机制所提供的自私自利的挖掘和双支出的弹性，从而保证了低过期的块率。我们总结如下结论。

调查结果小结

* 我们表明，自私的开采并不总是理性的。为了捕获合理的对手，我们因此量化了PoW区块链的双支出弹性，并对不同的PoW区块链的安全性进行了对比，以获得所需的交易确认数量。通过这样做，我们向商家提供知识，以确定给定的交易价值所需的确认数量，以确保安全防范双支出。
* 我们的研究结果表明,由于小块奖励和更高的陈旧的块率Ethereum2相比,比特币(从0.41%到6.8%由于更快确认时间),Ethereum(块间隔10至20秒)需要至少37确认匹配比特币的安全(块间隔10分钟平均)6块确认对敌人总数的30%开采能力。类似地，Litecoin将需要28个，而Dogecoin 47块的确认则是为了匹配比特币的安全性。
* 我们表明，区块链(如美元)的区块奖励越高，其抗双重支出的能力就越强。
* 最后，分析了改变块体尺寸的影响以及/或在自私的采矿和双重消费上的区块间隔。我们的结果令人惊讶地显示，将块大小设置为平均1 MB，并将块间隔时间减少到1分钟，不会对安全性造成很大的损害。因此，我们的研究结果表明，PoW区块链可以达到每秒60次以上的效率(tps)，这意味着在不损害系统安全性的前提下，7个tps的当前比特币的吞吐量可以大大提高。

论文的其余部分组织如下。在第2节中，我们概述了PoW区块链背后的基本概念。在Sec - tion 3中，我们引入了MDP模型来定量分析PoW区块链的安全性。在第4节中，我们介绍了我们的仿真器，并评估了一些基于不同类型的基于powc的区块链实例的安全性和性能。在第5节中，我们将概述相关的工作，并在第6节中总结本文。

2.背景

在本节中，我们简要回顾了共识层和现有PoW区块链的网络层的操作。

2.1共识层

工作(PoW)共识机制的证明是现有区块链中最广泛的共识机制。PoW是由比特币[27]引入的，并假设每一位同行都通过解决工作实例的证明和构建适当的块来获得他的“计算能力”。例如，比特币使用的是基于哈希的PoW，它需要找到一个nonce值，这样当用额外的块参数(例如，Merkle散列，上一个块哈希)散列时，哈希值必须小于当前目标值。当发现这样一个nonce时，它会创建一个块并将其转发给它的对等节点(cf . section 2.2)。网络中的其他节点可以通过计算块的散列来验证PoW，并检查它是否满足小于当前目标值的条件。

块间隔:块间隔定义了将内容写入区块链的延迟。块间隔越小，事务被确认的速度越快，过期块的概率就越高。块区间调整直接关系到底层PoW机制的难度变化。较低的难度会导致网络中大量的块，而较高的难度会导致在相同的时间范围内减少块。

因此，分析是否改变这一困难对攻击最长链的对抗能力是至关重要的，这是大多数以粉末为基础的区块链安全的主要支柱。这也意味着，为了安全的接受交易(和避免双重支出攻击)，商户应该等待的con -固件数量的调整(cf .第3节)。

2.1.1pow安全

PoW的安全性依赖于一个原则，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来有效地控制系统。我们现在简要地概述已知对现有的基于粉末的区块链的攻击。

首先，一个对手可以通过使用相同的硬币来进行两次(或更多)交易，从而有效地花掉比他所拥有的更多的硬币。最近的研究表明，在不需要区块链确认的情况下接受事务是不安全的[21]。一个交易获得的确认越多，该交易在未来发生逆转的可能性就越小。

其次，矿工们可能会试图在tacks上进行自私的挖掘[14]，以增加他们在区块链的相对采掘份额，选择性地扣留开采的区块，并逐渐将他们的利益与他们的利益联系起来[14,31]。最近的研究表明，作为这些攻击的结果，一个拥有33%开采权的自私矿商可以有效地获得50%的开采权。

如果区块链系统中的所有节点都是紧密同步的，则可以缓解双重开销攻击和自私的挖掘。注意，除了网络延迟之外，由于eclipse攻击[16,17]在网络中创建了一个逻辑分区，因此同步延迟可能会加剧。，为不同的区块链网络节点提供了相互矛盾的块和交易信息。

2.2网络层

在网络层上，我们确定了对基于粉末的区块链的两个主要参数，即块大小和信息传播机制。

2.2.1块大小

最大块大小间接地定义了在一个块中进行的事务的最大数量。因此，该大小控制系统获得的吞吐量。大块会产生较慢的传播速度，从而增加了陈旧的块率(并像前面提到的那样削弱了区块链的安全性)。

2.2.2信息传播机制

块请求管理系统指示信息如何传递给网络中的对等点。最终，由于所有的对等点都期望接收所有块，所以需要一个广播协议。基础广播协议的选择显然影响了网络的健壮性和可扩展性(cf .第4节)。在接下来的内容中，我们简要地描述了现有的基于粉末的区块链的网络层实现者。

基于广告的信息传播**:**大多数的PoW区块链在广告的帮助下传播信息,基于请求管理系统。如果节点A接收到来自另一个节点的新对象(例如，一个事务或一个块)的信息，那么A将通过发送一个inv消息(被广告对象的散列和类型)向其其他连接(例如节点B)做广告。只有当B节点之前没有收到广告对象时，B才会用getdata请求从A请求对象。节点A随后将响应比特币对象，例如，事务或块的内容。

发送头:对等点可以选择发送sendheader mes- sage，以便直接从他们的Peers -跳过对inv消息的使用中接收块标题。这减少了块消息传播的延迟和带宽开销，并且比特币自版本0.12开始采用。请注意，这个push系统是推荐的，但不是在比特币中实现的。

中继网络:中继网络[6]主要是增强了共享一个共同交易池的矿商的同步化。反式操作通常只在带有反式操作ID(每个事务的2字节，而不是平均每个事务250字节)的中转体中引用。因此，结果块的大小小于常规块[6]。

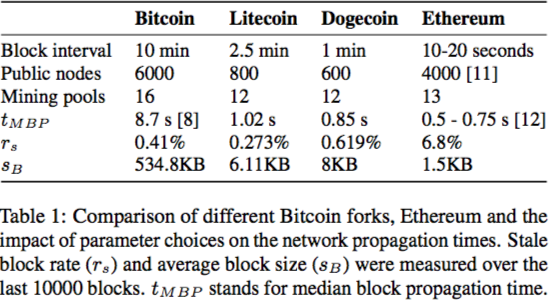
混合动力**/**广告系统:许多系统作为Ethereum，结合使用推送和广告传播。在这里，一个块直接被推到一个阈值的对等点(例如，Ethereum直接将block推给n个节点，其中n是连接到对等点的邻居的总数)。同时，发送方向所有的邻居宣传块散列。

2.3失效块

失效块是指不包含在最长的链中的块，例如，由于并发性，冲突。陈旧的块会对区块链的安全性和性能造成损害，因为它们会触发链式的forks——一个不一致的状态，会减慢主链的增长，并导致显著的性能和安全影响。一方面，陈旧的障碍增加了网络中对手的优势(例如，双支出)。另一方面，陈旧的块会导致额外的带宽开销，而且通常不会获得采矿奖励(在Ethereum除外)。

在我们进行了一个实验,我们测量的陈旧的块率的比特币(块世代时间= 10分钟,平均块大小= 534.8 kb),Litecoin(块世代时间= 2.5分钟,平均块大小= 6.11 kb)和Dogecoin(块世代时间= 1分钟,平均块大小= 8 kb)网络。这三个区块链依赖于基于粉末的区块链(具有不同的gen - eration时间)和相同的信息传播系统(不同的块大小)。

2016年2月，我们在Litecoin和Dogecoin[3]中抓取了可用的节点，并发现了大约800和600个IP地址。然后，我们通过记录在每个网络中从一个par - ticular块接收到块广告的时间来测量block的传播时间[9]。我们为Litecoin和Dogecoin操作了一个节点，这两个节点分别被连接到340和200个节点。一旦其中一个节点以(i)一个块的新散列(inv message)或(ii)块标题(标题消息)的形式发布了块信息，我们就注册了这个块信息出现的时间。一个特定的块信息的每个子序列接收，然后提供关于块的传播的信息。

我们的结果(cf . Table 1)表明，陈旧的块率实际上很大程度上取决于块的时间间隔和块大小。例如，与Dogecoin和Litecoin不同的是，比特币具有较大的块大小，因为它的事务负载更高(高达1MB，从而导致更高的块率(0.41%和0.273%)，尽管比特币的间隔时间比Litecoin的时间长4倍。此外，Litecoin和Dogecoin之间的陈腐差异主要是由于块间隔(2.5分钟与1分钟)之间的差异，因为它们的平均块大小可以比较(6.11 kb和8KB)。如果确认时间减少了60%，陈旧的块率从Litecoin到Dogecoin增加了127%。

注意，在Ethereum中，uncle块对应于主链中引用的陈旧块。Ethereum的比特率几乎是6.8%，相比之下，比特币的一个不新鲜的块率是0.41%。在第3节中，我们研究了失效块率对PoW区块链安全性的影响。

3.pow安全模型

在这一节中，我们将介绍我们的区块链安全模型，我们利用它来量化双支出和自私自利的最佳对抗性策略。然后我们将这些策略作为一个基础来比较基于不同参数的基于粉末的区块链的安全规定。

3.1安全模型

我们的模型扩展了[31]的Markov决策过程(MDP)来确定最优的对抗性策略，并捕获:不新鲜的块速率r允许我们考虑不同的块大小，块间隔，网络延迟，infor -传播机制和网络配置(例如，节点数)。矿业权力α的分数总挖掘对手的力量(其余由诚实的控制网络)。采矿成本敌对的采矿成本厘米∈(0,α)对应于预期的对手的采矿成本(即。，包括硬件、电力、人力等综合成本，并以块奖励的形式表示。例如,如果厘米=α,敌人的采矿成本相当于min - ing次方乘以块奖励,即。采矿成本完全由诚实开采的收入块收入所覆盖。块确认的数量与需要确认事务的块的num - ber对应，这样一个商家就接受了事务。

传播能力传播参数γ捕获对手的con - nectivity内部网络(即。当对手和诚实的矿工在网络中同时释放他们的阻滞时，捕捉到敌人的阻滞的部分。

eclipse的影响对我们的模型帐户造成了eclipse at- tacks的影响。在这里，我们假设诚实网络的矿工受到了陈旧的块率的影响，而对手和串通重叠的受害者并不是我的陈旧的街区。这是由于敌人可以使用任何已开采的石块进行攻击，并且在采取了诚实的链条后，有效地只有极小的机会在一个不新鲜的区块中。因此，在实际操作中，对手的实际失效块率要比诚实网络低得多。诚实网络的特点是传播和验证延迟——因此它将以一种更高的陈旧的速率。注意，被重叠的受害者发现的块也可以数到对手的私人链。

我们将其与现有的模型(如Sapirshtein et al. s[31])进行对比，后者只关注于自私的挖掘，无法捕获不同的区块链实例(有各种陈旧的块率和验证性)以及诸如网络延迟之类的实际参数。

为了分析最优的双支出策略，我们定义了对应于最小可转换值的双支出额vd，这使得双支出比诚实的挖掘更有利可图。我们认为，vd是一个强有力的度量指标，可以量化在双重支出攻击下的风险。也就是说，如果诚实挖掘的回报大于不诚实的行为，商家可以安全地接受价值vd的支付交易(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更有价值，那么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。

我们捕捉blockchain模型使用一个单人决策问题M:=⟨年代,a,P,R⟩所有其他参与者遵循标准的协议,和S对应于状态空间,操作空间,P的随机转移矩阵,矩阵R的奖励。我们将M实例化为Markov Decision Process(MDP)，如第3.2和3.3节所述。

在我们的模型中，对手可以采取以下行动:采用对手接受诚实网络的链，有效地对应于攻击的重新启动。这如果对手认为有可能，采取行动是适当的赢得诚实的链条是很小的。超越对手，比诚实的人多出一个区块链已经并且因此覆盖了冲突的块。当对手的秘密链比目前已知的公共链(即la > lh)长时，这就发生了，而对手发布他的block的lh + 1来替换诚实的网络链是最优的。如果对手利用了受害者的挖掘能力，对手可能会使用来自受害者的块来进行重写操作。

与对手相比，对手发布的区块与诚实的链一样多，并且触发了两家连锁企业之间的采用竞争，而不是凌驾于诚实的链条上。等对手继续在它的隐藏链上采矿，直到找到一个块。

退出此操作只在研究双支出时相关，因为它与k con -固件的成功的双开销相对应，只有当la > lh和la > k时才可行。状态空间被定义为形式的四元组(la,lh,be,fork)，其中la和lh分别代表了adversarial和honest chain的长度，是被重叠的受害者挖掘出来的块ork可以取三个值，无关的，相关的和活跃的:

相关的标签相关说明(i)最后一个区块已被发现。

(2)如果la≥lh匹配操作适用。表单状态(lh−1,拉·)例如导致(洛杉矶,lh,有关)。

当对手发现最后一个块时，前面的块可能已经到达了网络中的大多数节点。因此，对手不能执行匹配的动作。表单状态(la−1,lh,·)例如结果(洛杉矶,lh,无关紧要)。

如果对手执行匹配动作，则将状态描述为活动的标签。目前，该网络在确定最长链的过程中处于分裂状态。

在我们的模型中，每个状态转换(除了出口)对应于一个块的创建。因此，一个国家的转变意味着对诚实的网络，对手，或重叠的受害者的奖励。

鉴于α敌对的矿业大国,初始状态(0,0,0,无关紧要的)转换到(1,0,0,无关)概率α,即。敌人发现了一个街区。如果诚实的网络找到一个非过期的块，那么结果状态是(0,1,0，相关)。另一方面，如果诚实网络的块导致了一个不新鲜的块，则状态仍然是(0、0、0，无关)，因为一个陈旧的块不计入最长的链。过去的案例占黯然失色的受害者与概率ω,发现一块导致状态(1,0,1,无关紧要)。

自私的矿业和重复花费。

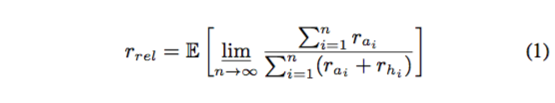
在这项工作中,我们考虑独立重复花费和自私的挖掘,从自私的挖掘并不总是理性的策略:自私挖掘的目标是增加的相对份额对抗块致力于主链,而在双——敌人的目标是最大化他的绝对收入支出。

也就是说，只要PoW区块链的困难没有改变(例如，比特币的困难每两周改变一次)，自私的开采会比诚实的采矿产生更少的阻碍。在诚实的采矿中，敌人会得到每一个开采区块的回报，而当他在自私的开采中开采主链时，他将失去任何先前开采的区块。因为对手的挖掘能力比诚实的网络少，所以他有很大的几率落在主链的后面，当他没有明显的机会赶上时，他就会采用主链，而这反过来又会导致损失块的回报。例如，按照我们最优的自私采矿策略(cf . Section 3.2.1)，一个30%的矿业公司的竞争对手平均在1000个区块被整个网络开采(而不是诚实开采的300个区块)时，平均能获得209块的奖励。同样，Eyal和Sirer的[14]策略收益率平均为205.80块。

Eclipse的攻击。在eclipse的攻击,一小部分整体采矿权力重叠的ω(17日28日)从网络接收信息从诚实。在这里，出现了一些eclipse攻击变体:没有eclipse攻击这种情况下在我们的模型中捕获如果ω= 0。将受害者隔离在我们的模型中。也就是说,这相当于减少了总采矿权因此增加了攻击者矿业权力α′=α。1−ω利用重叠的受害者,对手利用ω的维克——蒂姆的挖掘能力,用它来推进他的私人链。这是在进行双重支出攻击时最可能选择的理性对手。在这种情况下，我们假设受害者完全被网络所取代，除非对手允许，否则不会收到/发送块。

3.2自私矿业MDP

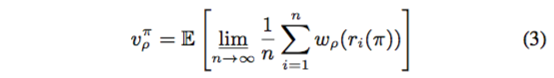
我们的目标是为自私的矿业找到最优的对抗策略。回想一下自私采矿的敌人的目标

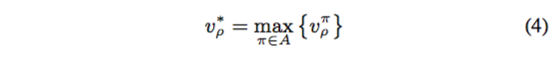
不是优化绝对报酬，而是增加被网络所接受的链中包含的块的份额。我们通过优化公式1中定义的相对收入rrel来获取这一点，其中rai和rhi分别是对对手和诚实网络的奖励，分别是:

由于一个对手的目的是提高他的相对奖赏rrel(Equa - tion 1)在自私的挖掘，而不是绝对的奖励，单玩家决策问题不能被直接建模为MDP，因为报酬函数是非线性的。为了将这个问题转化成一个MDPs的家族，我们应用Sapirshtein et al. s[31]的技术，我们在下面描述。

我们假设目标函数的值(即。op - timal相对奖励)ρ和定义为任何ρ∈[0,1]转换函数wρ:N2→R的对抗性的奖励ra和奖励诚实的网络方程2 rh。

这将导致无限状态MDP Mρ=⟨年代,A,P,wρ(R)为每个ρ⟩相同的动作和状态空间的原始决策问题和转移矩阵相同,但是使用wrho奖励矩阵转换。这种政策下MDP的期望值π然后由vρπ方程3,其中ri(π)是奖励我在政策π步中元组。



最优策略下的期望值如下:

就我们所知，这是第一个自私的挖掘模型(i)捕获了各种参数，如块传播时间、块大小、块生成间隔和(ii)已知的网络vul - ner异能，如eclipse攻击。注意，我们不考虑在自私的采矿MDP中开采成本，因为这里的目标是增加相对的开采份额(而不是货币奖励)。

3.2.1自私自利的最佳策略

为了解决MDP的问题，我们在有限状态空间MDPs上应用MDP求解器[18]，并使用30个块的截止值。

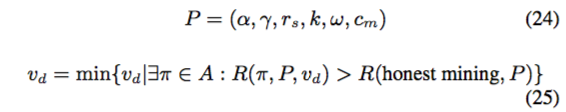
我们首先分析了陈旧的街区率对自私自利的影响。在图2中，我们比较了一种以1%和10%的不新鲜的块率为基础的自私的开采，我们观察到，一个自私的矿商的相对收入越高，其相对收入就越高(最高的差异是0.074)。作为比较,我们把敌对的相对的一个上界α1−α自私矿业收入对应的情况下,对手的优势是最大化利用一块覆盖一块生成的诚实的网络(据Sapirshtein et al .[31])。正如我们所观察到的，当考虑到网络延迟和通过不新鲜的块率捕获的参数时，这个上限会被超越。

与矿业敌人的力量分别α= 0.1和α= 0.3,我们观察到在图3中有一个陈旧的块率之间的非线性关系和自私的相对矿业收入挖掘。

我们还研究了eclipse攻击对图4中的自私挖掘的影响。在这里,我们只考虑对手的情况(我)利用ω的受害者挖掘能力,和(2)使用所有受害者的块来实现自己的私人链。因此，我们只确定这些限制条件下最优的对抗性选择。我们观察到ω越高,他的自私的采矿能力变得越强。我们注意,对于一些ω值(如ω= 0.3,α= 0.38),这是更有价值的对手不包括一些受害者块在他的私人链。这是因为受害者的块奖励计入了诚实网络的回报，因此减少了对手的相对块份额。

3.3重复花费MDP

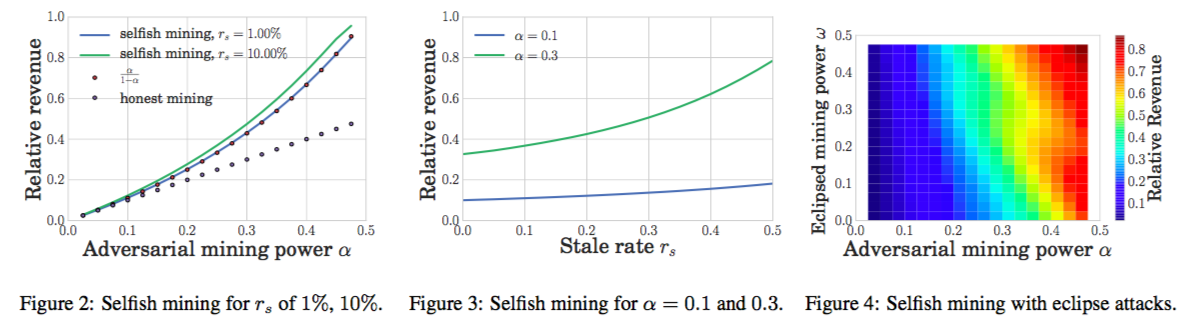
不像自私的开采，最优策略在财务上并不总是与诚实采矿相比较(cf .第3节)，我们在接下来的研究中研究最优的双支出策略，我们假设一个理性的对手对最大化他的利益(以财务收益来衡量)感兴趣。

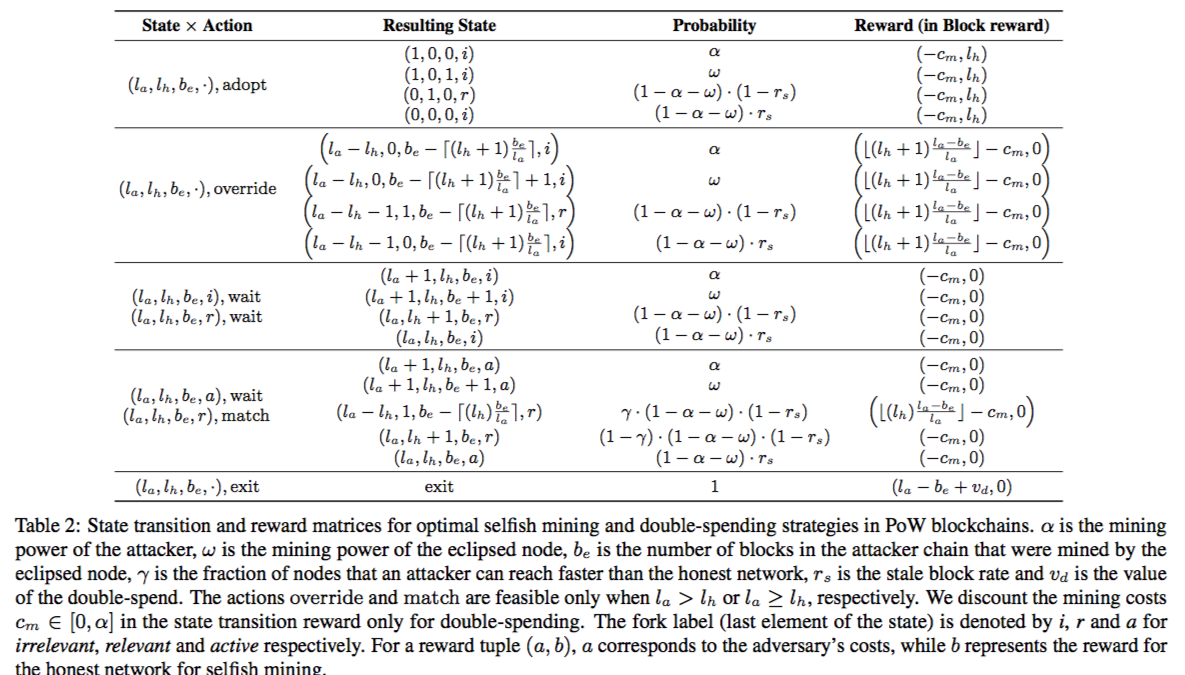
我们含蓄地要求每一次对手发起双倍的开支攻击(例如采取行动后)，他在网络上发布一个transac - tion Tl，并在他的私有链中包括一个冲突的transac - tion Td。我们假设经营成本“失败”是一个小的尝试，因为对手有效地接收到一个好的或服务来交换交易的Tl双支出MDP具有退出状态(cf . Table 2)只有提供了对抗性的链，才能联系到吗在k确认后，一个街区在诚实的链条前面(la > lh)(la > k),一个诚实的网络与矿业电源1−α。之前到达出口状态时，对手采取了最佳策略考虑到所描述的状态和动作空间，最大化它的奖励第三节。到达退出状态后，转换回退出状态国家模式奖励诚实开采。请注意，我们假设对手是理性的一个最优策略可能会建议，反对进行双重支出攻击(即对手将会)永远不要到达退出状态)-取决于尝试的值攻击。在退出状态中，对手获得了块奖励la−+ vd,⌊(lh + 1)la−⌋−厘米块奖励后覆盖与eclipse攻击(因为对手的奖励需要折扣是受害者的块和⌊(lh)la−⌋−厘米块奖励如果拉对手的链条在比赛后赢得比赛。对于每一个国家转变我们折扣采矿成本−厘米。对手要么遵循最佳的双支出strat -egyπ或执行诚实的矿业,取决于预期的回报。因此，我们对最小的双支出价值vd感兴趣，这样vd严格大于诚实的采矿奖励(cf . Equation 25)。

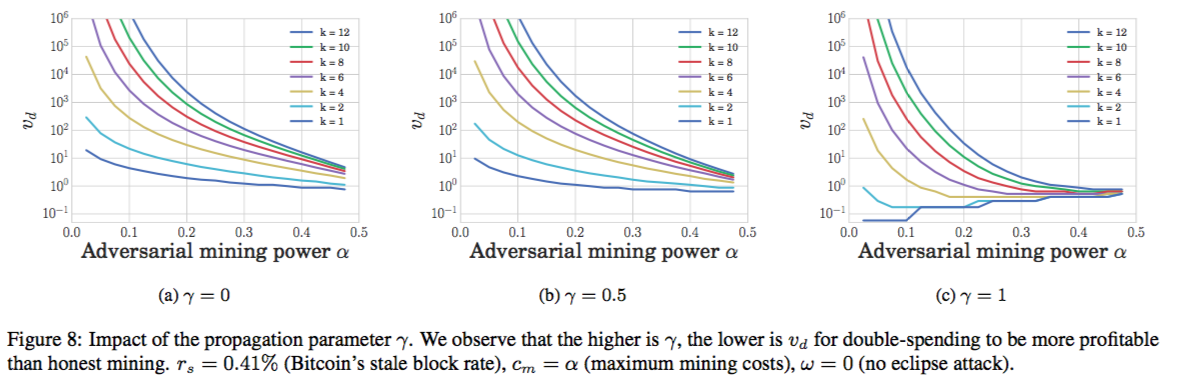
double -开销值vd可以作为一个通用度量来比较各种区块链实例化的安全性。即如果vd blockchain实例blockchain B的一个大于给定的α,γ和ω,然后blockchain对重复花费攻击可以被认为是更强的抵抗力。

3.3.1双支出的优化策略

在接下来的内容中，我们分析了前面提到的双花费MDP给出的各种参数的解决方案。为了解决MDP中最优策略，我们依赖pymdptoolbox library4，并应用PolicyIteration算法[18]，折现值为0.999。这种方法允许我们评估交易确认的数量是否足以保证在一个理性的对手面前的安全，以及考虑到的交易价值。也就是说，如果对手比诚实的采矿有更高的预期经济收益，那么交易就不能被认为是安全的，如果有k的确认，商人应该等待更多的确认。

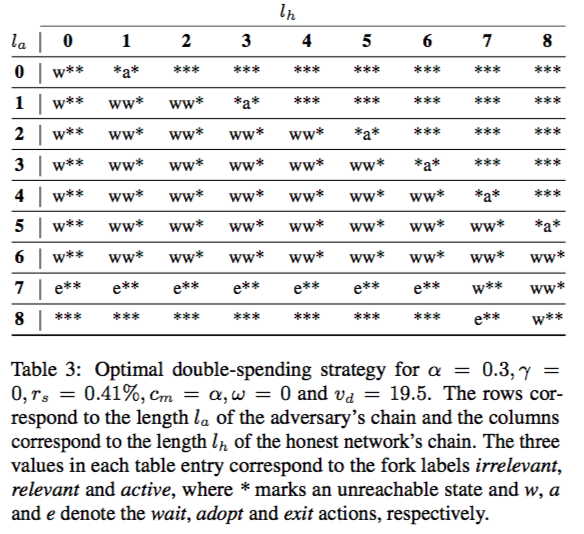
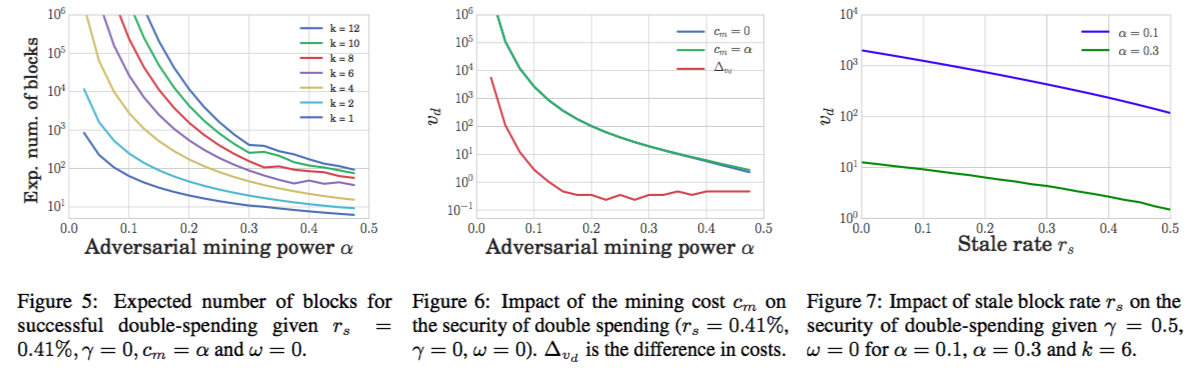
为了决定是否对手应该选择追随最优重复花费政策或诚实的矿业(cf。方程,25),并确定最低vd,我们实例化重复花费MDP重复花费价值高(> 109块奖励),这样最优政策的退出状态是可获得的。如果政策包含退出状态，那么最优的双支出策略的预期收益大于诚实的挖掘。否则，诚实采矿是首选策略。我们应用二叉搜索找到重复花费最低的价值(以块为单位的奖励,在0.1的误差),α,k,rs、γ和cm。

我们只观察等待，采取和退出行动。因为我们只能解决有限的MDPs，我们选择20个块的截止值，即，无论是对手的链还是诚实网络的链都不能超过截止值。在下面的文章中,我们将讨论更多的细节的影响α、γ,厘米,rs,k,vd和ω最佳重复花费战略及其影响的安全交易确认。

回想一下，我们的双支出MDP的Markov链的吸收状态[22]是退出状态。通过计算马尔可夫链的funda - mental matrix[22]，我们计算了马尔可夫链中所期望的步数，然后被退出状态吸收。这些步骤对应于成功的双支出攻击所需的块的预期数量。在图5中,我们评估预期数量的块adversar请愿矿业权力和事务的数量确认k。我们观察到敌人矿业预计超过0.25的力量需要不到1000块对于一个成功的两倍——支出攻击(k = 10确认),对应于一个一个星期攻击持续时间在比特币。

传播参数的影响**:**回想一下传播参数指定了对手的连接能力。在图8中,我们描述的最小重复花费交易值将导致经济利益相比,诚实矿业(cf。方程25)γ= 0时,分别为0.5和1。重新调用一个商家是安全的，只要他接受小于vd的交易，就会得到这些参数。

显然,γ越高,较低的是敌人的成交价格预计将double spend。例如,如果对手α= 0.3的散列电力网络中,假设k = 6确认,和采矿成本厘米=α,重复花费策略显然是有利可图的,如果重复花费事务的价值至少0.5块奖励(一块25位奖励——硬币,其中一个比特币约为436.7美元在撰写本文时,rs = 0.41%)当γ= 1。当γ= 0.5,最低成交价格增加到12.9块的回报。

采矿成本的影响**:**在图6中，我们分析了采矿成本对最低要求的双支出反式行动价值的影响。我们的结果表明开采成本是可以忽略不计的,而一个不新鲜的块率是10%和20%，双消费价值vd从9.2下降到6.4块。同样，自私采矿的相对收入(cf .图3)从0.37增加到0.43。

陈旧的块率的影响**:**我们评价对手陈旧的块率的影响与矿业α= 0.1的力量和α= 0.3,如图7所示。我们观察到存在陈旧的块率之间的非线性关系和重复花费价值和陈旧的块率越高,更糟糕的是双-支出和自私的挖掘阻力的战俘区块链(cf。图7)。例如,一个对手与矿业α= 0.3而一个不新鲜的块率是10%和20%，双消费价值vd从9.2下降到6.4块。同样，自私采矿的相对收入(cf .图3)从0.37增加到0.43。

**eclipse**攻击的影响，我们评估eclipse攻击对我们的MDP的对抗性策略的影响。我们假设对手日食受害者与矿业权力ω为了增加其优势在保持区块链(cf,图9),我们观察到一个eclipse攻击显然让对手,因为它允许对手有效提高其整体采矿能力。例如,α= 0.1的对手可以减少重复花费总额从880块奖励0.75块vd奖励如果超过一个矿工ω= 0.025。

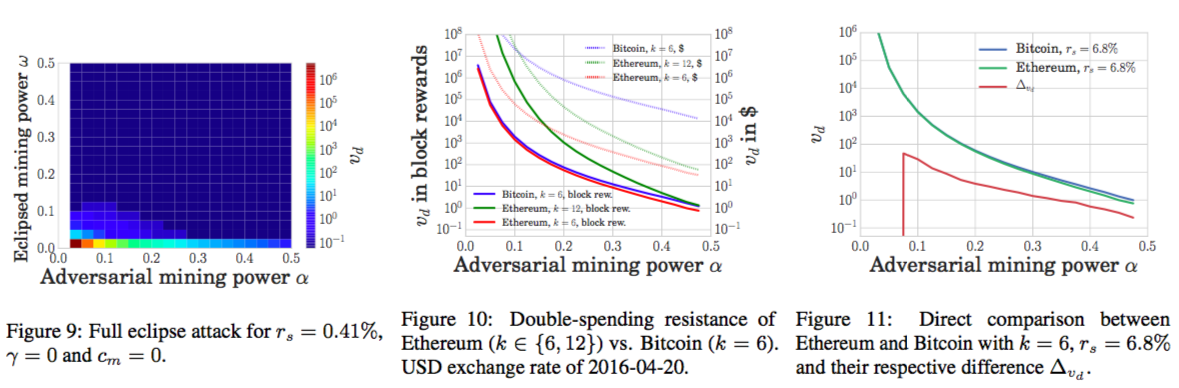
3.3.2比特币与Ethereum

为了缓解陈旧的街区降低PoW效率的问题，一些建议，比如Ethereum，建议奖励那些陈旧的街区的矿工[4]。在这里，尽管包含在块中的叔叔块获得了奖励，但它们并不计入链的总困难，即。以太会使用一个最长的链式法则来增加对叔叔的奖励。这清楚地说明了Ethereum关于使用区块链协议来适应GHOST的要求[33]。

Ethereum最近还修改了其最长的链算法，以合并一致的tie断开[10]。请注意，这样的策略是自私的采矿对策，但允许一个自私的矿工增加抓住诚实链条的机会[31]。在表4中，我们扩展了我们的模型，以满足叔叔的奖励和统一的平局，并描述了结果的双花费MDP，以获得对双消费的Ethereum的安全性。

在此分析的基础上,我们比较在图10中,比特币的双重-支出弹性(rs = 0.41%,cf。表2中MDP)的Ethereum(rs = 6.8%,cf。MDP在表4),鉴于γ= 0,厘米= 0,ω= 0。为了提供公平的成本比较，我们依靠基于美元的估值(比特币的方块奖励比Ethereum的块奖励高出200倍以上)。

我们观察到6个比特币区块的确认比6个Ethereum5块确认更有弹性。其次，当比较12个比特币和6个比特币区块的确认时，Ethereum的双重支出弹性比比特币对一个不到11%的PoW哈希电力的对手更好。注意，12个Ethereum块很可能在4分钟内生成，而6个比特币块的生成时间大约为1小时。第三，我们发现，区块奖励的货币价值直接影响了双支出的安全性:区块链(在美元)中，阻止双重支出的效果越强。

除了将比特币与Ethereum进行比较，我们还通过将比特币的不新鲜的块率设置为以太的陈旧的块率来客观地评估其对安全的影响，来比较图11中的两个区块链。我们观察到，尽管依赖于uncle block奖励，以及统一的平局，Ethereum的安全性弱于比特币，并得出结论，统一的平局和叔叔的奖励降低了Ethereum区块链的安全性。

4.安全性与性能的pow-区块链

在本节中，我们将通过在第3节中利用我们的模型来评估var - iou区块链实例化的性能(和安全性)。为此，我们构建了一个比特币区块链模拟器

从性能角度评估不同的区块链实例。依赖于模拟是唯一可行的替代方案，它可以实际捕获不同参数下的区块链性能，因为既没有正式建模，也没有数千个对等点的部署(例如，目前比特币中有6000个可访问的节点)是可行的。

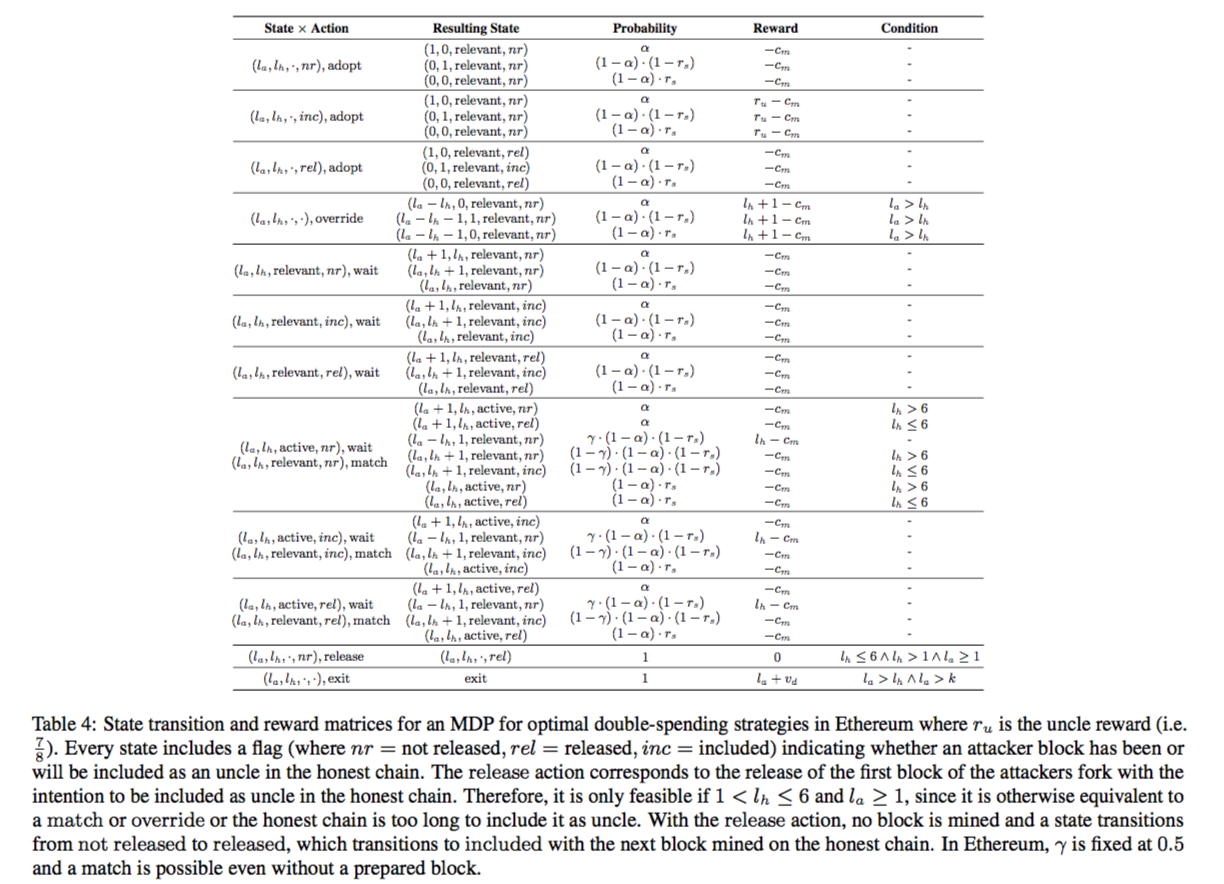
通过利用我们的模拟器，我们评估了不同的区块链pa - rameter，如block interval、块大小、传输机制，通过测量产生的失效块率、吞吐量和阻塞传播时间。这也使我们能够将区块链模拟器与MDP模型连接在一个统一的框架中。也就是说，为了评估结果区块链实例的安全性(在自私的挖掘和双重开销下)，我们将模拟程序输出到我们的MDP模型中。

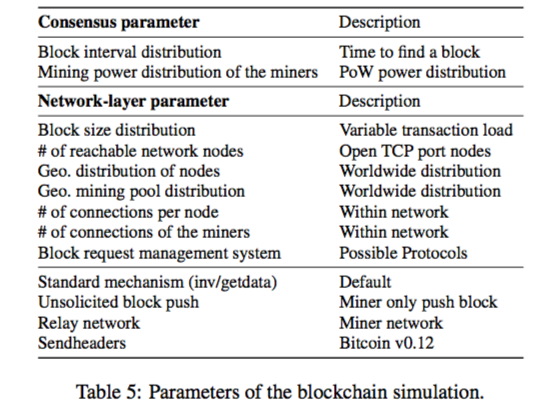
4.1 区块链模拟器

在表5中，我们总结了我们的sim - ulator捕获的参数。在这里，我们模拟矿工的战俘，将一个特殊的采矿权归到每个矿工身上。基于块区间分布(定义了一个块被发现的时间)，然后将一个新的块归因于一个矿商。与现有的粉末-区块链的操作相一致，在他接收到的第一块矿石上，我们假定，叉是由最长的链式法则决定的。一旦分叉被解决，不为主链做出贡献的块被认为是陈旧的块。在我们的模拟中，我们不认为困难在不同的块之间变化;因此，最长的链是由它的块的数量来定义的。

在建立节点之间的连接时，我们在它们之间创建点对点通道，它可以抽象出任何中间设备(路由、交换机等)。这些通道有两个特点;延迟和带宽。为了捕获网络中的实际延迟，我们采用了来自Verizon[36]的全局IP延迟统计数据，并假设一个帕累托流量分布的方差占平均延时的20%[2]。另一方面，为了对网络中的实际带宽分布进行建模，我们采用了testmy.net[34]的分布。

我们的模拟器不模拟交易的传播，因为我们的模拟器的焦点是研究块大小、块间隔和块请求管理系统的影响——所有这些都可以独立于trans - action传播来捕获。注意，事务在块大小内隐式捕获。

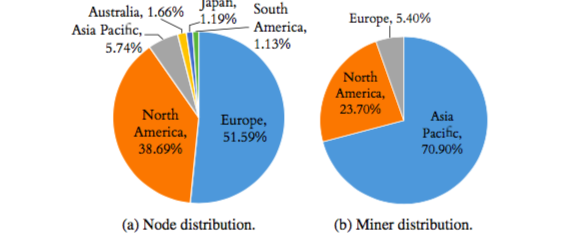
在我们的模拟器中，我们区分了两个节点类型:(i)规则节点和(ii)矿工。对于常规节点(多达6000个)，我们从位节点检索当前的地理节点分布。21。co(cf . Figure 12a)并通过这个分布来定义模拟节点的位置。我们还根据Verizon[2,36]和testmy.net[34]调整了带宽和网络延迟(根据地理位置)。对于模型的采矿者，我们从blockchain.info获取了挖掘池分布，并相应地将挖掘池的公共节点分配给相应的区域(cf .图12b)。在我们的模拟中，挖掘池通常会保持私有的凝视欺诈行为。除了直接观察外，在Matt Corallo的中继网络[6]中，大量的矿库都在运行，这是默认的比特币P2P覆盖网络(cf . Section 2.2)。我们还捕获了中继网络，并在模拟中假设所有的矿工都参加中继网络启用网络选项。

4.2评价结果

在接下来的内容中，我们给出了我们的评价结果。

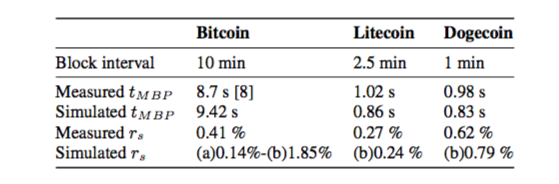
4.2.1模拟器准备验证

通过实验验证我们的模拟，我们将比特币、Litecoin和Dogecoin与他们各自的模拟相比较。对于每个区块链，我们根据当前的参数调整表5的pa - rameters

通过现有的研究区块链的部署。对于站姿，我们测量了比特币的块大小分布，以及在2015年5月到11月之间真实比特币网络上的块产生率7[21]。

为了测量真正的区块链网络中陈腐的速率，我们用了24,000个比特币，100,000个Litecoin和240,000个Dogecoin blocks9。此外，我们还采用矿用矿权分配给不同区块链的公共区块

在我们的仿真中每个节点的连接数遵循Miller等[26]的分布。

我们的发现(cf . Table 6)表明，我们的模拟器在很大程度上捕获了现有区块链部署的性能。例如，我们的研究结果表明，测量和模拟的中位块传播时间相对较近。对Litecoin和Dogecoin的不新鲜的街区收费尤其接近。在比特币的情况下，当所有的矿工都使用中继网络和未经请求的区块推送时，这种陈旧的利率会下降，而在这种极端情况下，任何矿商都不使用中继网络和主动块推。注意，Litecoin和Dogecoin没有任何中继网络。

4.2.2块间距的影响

在本节中，我们研究了块区间对中块传播时间的影响，以及基于PoW的区块链中的失效块率。为此,我们运行我们的模拟器不同块间隔时间从25分钟到0.5秒(cf Ta - ble 7)。每个模拟独立运行连续10000块,和四个不同的块请求管理系统组合:(案例1)标准块请求管理,,(例2)标准块请求管理增强了主动阻止推动这些矿工,两位前组件(例3)+中继网络,和(4)送头机制与主动块推动和传递网络。

我们首先观察到，在10分钟的块间隔时间和标准的请求管理系统中，我们的失效块率是1.85%，这与Wattenhofer等[9]所报告的一样，是1.69%。回想一下，在Wattenhofer的研究中，未经请求的区块推送和中继网络还没有出现。

其次，我们注意到，引入主动块推动矿商显著降低了陈旧的块率。这是由于(i)矿商是相互关联的，并且大部分来自主动的块推送，(ii)第一个节点的传播方法对于快速到达网络的大多数是至关重要的。与未经请求的块推送相比，中继网络的添加似乎不会显著影响到过时的块速率(考虑到比特币的交易负载)，并且只略微减少了传播时间。然而，对于较大的块大小(例如> 2MB)，中继网络确实比非请求的块推送(cf . Table 8)提供了一个优势。此外，中继网络除了传统的P2P覆盖网络外，还提供了一个额外的块信息来源。请注意，尽管发送头机制的影响与完全部署的中继网络和请求的块推送相比是有限的，但这种机制可以减轻部分eclipse攻击[16]。

为了评估块间隔对PoW区块链安全性的影响，我们将产生的过期块速率输入到MDP中模型如表7所示。我们的结果表明，对于一个装备了30%的总开采power11的对手，较低的是con - sensus时间，较高的是来自自私采矿的相对收益，而较低的是双重消费的价值。我们观察到，块传播机制对区块链的安全性有明显的影响，因为它直接影响到过期的块率。stan- dard块传播机制(在双开销和自私的挖掘方面)比其他评估的块传播机制提供的弹性更小。我们还注意到，Case 4的块传播机制(与其他研究机制相比)，在表7中双花费值为2 / 2，将块的间隔从25分钟减少到0.5秒。同样，自私开采的相对收入也从0.33增加到0.42。

4.2.3块大小的影响

我们现在研究的是block size对区块链性能和安全性的影响(cf . Table 8)。为此，我们模拟块大小，从0.1 MB到最多8 MB，给定一个块间隔10分钟。

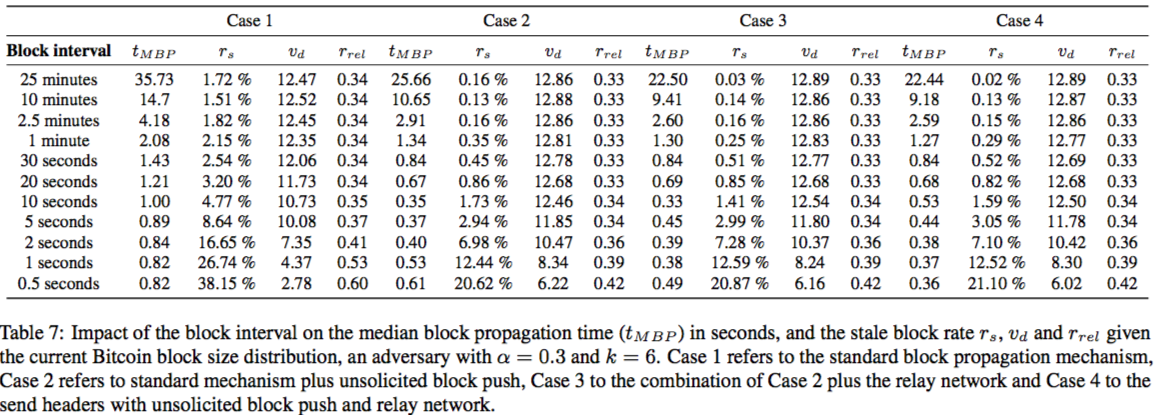
我们的结果表明，块传播时间随块大小线性增加到4 MB;在8 MB的块后，块的传播时间和陈旧的块率呈指数级增长。其次，我们清楚地看到，更好的块传播机制大大减少了传播时间和不新鲜的块率。

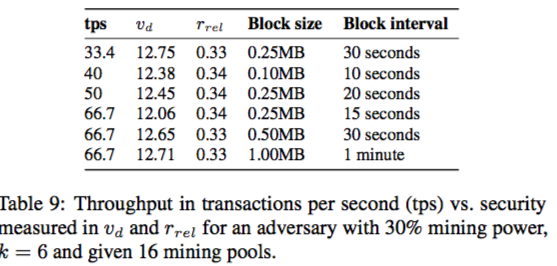
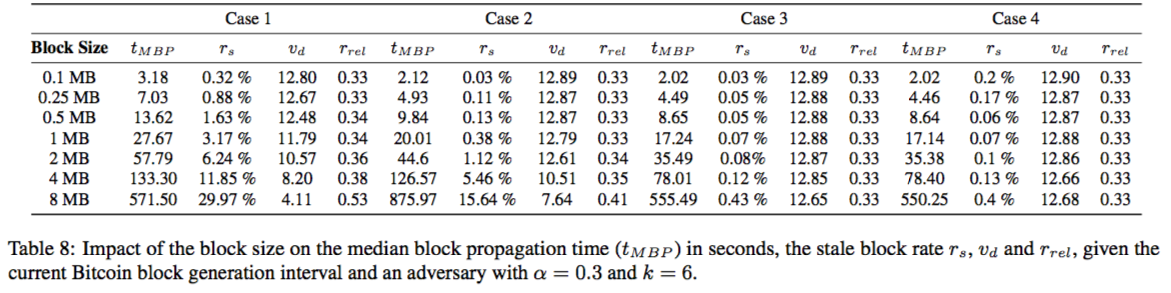
这也表明,符合我们的MDP模型、块大小越大,相对自私的采矿和收入越高越低(表8)。重复花费价值。然而明显是一种有效的阻止传播机制有效地允许网络保持几乎相同的安全职业——愿景对自私的采矿和重复花费,我们可以看到,以防3(标准传播机制,主动推动,继电器网络)和案例4(发送标题传播机制,主动推动,继电器网络)。这证实了一个有效的网络传播机制有助于提高区块链的安全性。有趣的是，考虑到案例4中的block传播mecha - nism，当将块大小从0.1 MB增加到8 MB(vd从12.9到12.68块奖励时)，在表8中，弹性(在双支出值方面)并没有显著的变化。同样，当所有矿商使用中继网络时，自私自利采矿的相对收入仍停留在rrel = 0.33。

目前，许多建议都建议块块，并并行下载这些块(例如，Blocktorrent[35])。在我们进行的另一个实验中，我们实现了一个块传播机制，该机制将块划分为几个千字节的块，这些块可以从多个节点查询。我们的结果表明，与发送头和中继网络协议相比，这样的协议在处理中等大小的块时不会提高中值块的传播时间。，小于8 MB)。这是由于块块的传播速度慢于第10和第25百分比的节点，原因是:(i)块造成的通信开销;(ii)因为只有在验证了相应的块时，节点才会转发块块。

4.2.4吞吐量

我们现在评估通过各种区块链实例化实现的吞吐量。为此，我们将块大小(从0.1M B到8mb)和块间隔(从0.5秒到25分钟)更改为通过我们的模拟器捕获更多的区块链实例。在这里，我们假设网络依赖于一个有效的传播机制(为所有的矿工发送不请自来的块推送和中继网络)。对于每个模拟区块链实例,我们计算产生的吞吐量在每秒事务数(tps),测量的块率和推断vd和rrel为了评估区块链的安全与我们的MDP模型(cf。第三节)。我们也假定平均交易规模为250字节,k = 6确认对重复花费和一个对手0.3矿业权力和γ= 0.5。

在表9中，我们有选择地列出了可以实现超过60个tps的事务吞吐量的候选区块链实例，并在现有的比特币系统中实现类似的安全规定。很明显，我们的结果表明不同的参数配置可以产生相同的吞吐量，尽管有不同的安全支持(由于不同的陈旧的块率)。特别是，我们观察到，相对于较高的一致性间隔，较低的一致性间隔提供的安全性更低，因为网络需要更多的往返，以便将相同的信息提交到区块链。我们的研究结果表明，在没有显著降低安全性的情况下，可以提高现有PoW的可伸缩性。

5.相关工作

一些捐款分析了比特币的双重支出攻击[15,30]，但他们不考虑最优的对抗性策略。Eyal和Sirer[14]表明，一个自私的矿工可以通过不直接发布他的区块来增加其相对的矿业收入。[7]研究颠覆性的采矿策略。

我们的工作与Sapirshtein等[31]有相似之处。在这里，作者设计了针对比特币的自私挖掘的最优的对抗策略。与[31]不同的是，我们的工作捕获了基于powc的区块链的最优adversar -自私的挖掘策略，并考虑了网络延迟和eclipse攻击。此外，我们还捕获了最优的双支出策略——我们还考虑到了对手的开采成本、重新计算的区块确认数量和双重支出价值，以便合理解释攻击的成本。

GHOST[33]是在基于PoW的区块链中存在的一种可替代的最长链规则，它的目的是减轻失效块的负面影响。已经提出了许多备选方案。在股权证明(PoS)[29]中，对等点的投票权是基于他们在各自的区块链系统中拥有的“股份”数量。燃烧的证明(PoB)是一种通过燃烧事务输出来代替PoW的提议，这样它们就不能再使用了。然而，现有的基于pob的区块链依赖于PoW来创建区块，因此最终依赖于PoW来创造硬币。容量证明(PoC)，目的是使用可用的硬盘空间来替换PoW。bitcoin - ng[13]执行领导人选举，允许领导人签署微程序，直到选出新的领导人。文献中还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式容错协议，希望能提高效率，实现高的交易吞吐量。最近的研究建议结合使用PoW与BFT协议来实现高性能的开放协商一致协议(拜占庭[24])。

6.结束语

在这项工作中，我们引入了一个新的定量框架，以客观地比较PoW区块链的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粉末的区块链的安全性的影响。通过这样做，我们展示了如何客观地比较不同PoW区块链的安全条款。也就是说，我们的框架允许我们以每秒事务吞吐量的方式来突破PoW的边界，同时观察到区块链在最优的自私挖掘和双重消费策略方面的安全条款的影响。

举例来说，我们发现，为了匹配比特币的安全性，为了匹配比特币的安全性，以太需要至少37个block con- mations，给了一个占总开采能力30%的对手。我们的研究结果间接地表明，比特币的区块链比Ethereum的区块链提供了更多的安全保障，它会奖励那些有叔叔奖励的矿工，并对区块链叉号决议进行统一的捆绑。我们的研究结果还表明，现有的PoW区块链可以在不影响区块链的安全性的情况下，每秒实现60个事务的吞吐量。我们所知,这是第一个贡献,关丽珍titatively评估失效块率的影响最优重复花费和自私的挖掘阻力的战俘区块链(cf。图7和图3)。通过这样做,我们的研究结果定量地捕捉交易安全的基于他们的价值观,和块confirmations-effectively量化所需的安全级别通过著名的六块确认比特币。

我们的见解不仅允许商人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，同时也帮助矿工们量化PoW区块链对自私采矿的韧性。

7.参考资料

. [1]  Bitcoin block size limit controversy, 2016. Available from: https://en.bitcoin.it/wiki/Block\_size\_limit\_controversy.

. [2]  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.

. [3]  Bitnodes. Bitnodes ip crawler. Available from: https://github.com/ayeowch/bitnodes.

. [4]  V. Buterin. A next-generation smart contract and decentralized application platform, 2014.

. [5]  Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In *OSDI*, volume 99, pages 173–186, 1999.

. [6]  Matt Corallo. Bitcoin relay network. Available from: http://bitcoinrelaynetwork.org/.

. [7]  Nicolas T. Courtois and Lear Bahack. On subversive miner strategies and block withholding attack in bitcoin digital currency. *CoRR*, abs/1402.1718, 2014.

. [8]  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.

. [9]  C. Decker and R. Wattenhofer. Information Propagation in the Bitcoin Network. In *13-th IEEE International Conference on Peer-to-Peer Computing*, 2013.

. [10]  Ethereum. Ethereum tie breaking. Available from: https://github.com/ethereum/go-ethereum/commit/ bcf565730b1816304947021080981245d084a930.

. [11]  Ethereum. ethernodes. Available from: https://www.ethernodes.org/network/1.

. [12]  Ethereum. ethstats. Available from: https://ethstats.net/.

[13] Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer, and Robbert van Renesse. Bitcoin-ng: A scalable blockchain protocol. *arXiv preprint arXiv:1510.02037*, 2015.

[14] 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.

[15] The Finney Attack, 2013. Available from: https: //en.bitcoin.it/wiki/Weaknesses#The\_.22Finney.22\_attack.

[16] 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.

[17] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg. Eclipse attacks on bitcoin’s peer-to-peer network. 2015.

[18] Ronald A Howard. *Dynamic Probabilistic Systems, Volume I: Markov Models*, volume 1. Courier Corporation, 2012.

[19] IBM. Ibm openblockchain. Available from: http://www.ibm.com/blockchain/.

[20] Intel. Proof of elapsed time (poet). Available from: http://intelledger.github.io/.

[21] 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.

[22] John G Kemeny, J Laurie Snell, and Gerald L Thompson. Finite mathematics. *DC Murdoch, Linear Algebra for Undergraduates*, 1974.

[23] 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.

[24] 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.

[25] D. Mazieres. The stellar consensus protocol: A federated model for internet-level consensus. Available from: https: //www.stellar.org/papers/stellar- consensus- protocol.pdf.

[26] Andrew Miller, James Litton, Andrew Pachulski, Neal Gupta, Dave Levin, Neil Spring, and Bobby Bhattacharjee. Discovering bitcoin’s public topology and influential nodes.

[27] S. Nakamoto. Bitcoin: A p2p electronic cash system, 2009. [28] 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.

[29] QuantumMechanic. Proof of stake. Available from: https://bitcointalk.org/index.php?topic=27787.0.

[30] Meni Rosenfeld. Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*, 2014.

[31] Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar. Optimal selfish mining strategies in bitcoin. *arXiv preprint arXiv:1507.06183*, 2015.

[32] Yonatan Sompolinsky and Aviv Zohar. Accelerating bitcoin’s transaction processing. fast money grows on trees, not chains. *IACR Cryptology ePrint Archive*, 2013:881, 2013.

[33] Yonatan Sompolinsky and Aviv Zohar. Secure high-rate transaction processing in bitcoin. In *Financial Cryptography and Data Security*, pages 507–527. Springer, 2015.

[34] testmy.net. testmy.net. Available from: http://testmy.net/country.

[35] Jonathan Toomim. blocktorrent. Available from: http://lists.linuxfoundation.org/pipermail/bitcoin-dev/ 2015- September/011176.html.

[36] Verizon. Verizon latency. Available from: http://www.verizonenterprise.com/about/network/latency/.

[37] 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.