The Miner's Dilemma

Abstruct

摘要—一个开放的分布式系统可以通过要求参与者提供工作证明并对他们的参与进行奖励来确保安全。比特币数字货币引入了这一机制，几乎所有当代数字货币及相关服务都采用了这一机制。

在这样的系统中，参与者自然而然地会形成矿池，成员们聚集他们的力量并分享奖励。比特币的经验表明，最大的矿池通常是开放的，允许任何人加入。长期以来，人们都知道，一个成员可以通过看似加入矿池但实际上从不分享其工作证明来破坏一个开放的矿池。矿池与攻击者分享其收入，因此其每个参与者赚取的收益减少。

我们定义并分析了一个游戏，其中矿池使用其部分参与者渗透到其他矿池并执行此类攻击。在任意数量的矿池中，没有矿池攻击并不是纳什均衡。我们研究了两个特殊情况，即两个矿池或任意数量的相同矿池参与游戏，而其余参与者不参与。在这两种情况下，都存在一个构成公地悲剧的均衡，其中参与的矿池相互攻击，赚取的收益少于如果没有任何攻击的情况。

对于两个矿池，是否攻击的决定是矿工的困境，是迭代囚徒困境的一个实例。这个游戏每天由活跃的比特币矿池进行，显然它们选择不攻击。如果这种平衡被打破，开放矿池的收入可能会减少，使其对参与者不再有吸引力。

Introduction

比特币[1]是一种数字货币，正逐渐获得接受[2]和认可[3]，据估计，截至2014年11月，其市场资本化超过45亿美元[4]。比特币的安全性源于一个强大的激励系统。参与者需要提供昂贵的工作证明，并根据他们的努力获得奖励。这种架构已被证明既稳定又可扩展，并被大多数当代数字货币及相关服务所采用，例如[5]、[6]、[7]、[8]、[9]。我们的研究结果适用于所有此类激励系统，但由于比特币是一个活跃且典型的例子，我们使用比特币的术语和示例。

比特币通过一个称为区块链的数据结构来实现其激励系统。区块链是所有比特币交易的序列化记录。它是一个单一的全球账本，由一个开放的分布式系统维护。由于任何人都可以加入这个开放系统并参与维护区块链，比特币使用工作证明机制来防止攻击：参与需要消耗大量的计算资源。一个参与者通过工作证明证明她已经消耗了足够的资源，就可以在协议中迈出一步，通过生成一个区块。参与者因其努力而获得新铸造的比特币作为补偿。创建区块的过程称为挖矿，参与者称为矿工。

为了赢得奖励，许多矿工试图生成区块。系统自动调整区块生成的难度，使得每10分钟向区块链添加一个区块。这意味着每个矿工很少能生成一个区块。尽管其预期收入可能是正的，但矿工可能需要等待很长时间才能创建一个区块并实际赚取比特币。因此，矿工们组成矿池，所有成员同时挖矿，一旦其中一人创建了区块，他们就分享收入。

矿池通常由一个矿池管理者和一组矿工实现。矿池管理者作为单个矿工加入比特币系统。它不生成工作证明，而是将工作外包给矿工。为了评估矿工的努力，矿池管理者接受部分工作证明，并根据矿工提交此类部分工作证明的速度来估计每个矿工的算力。当一个矿工生成完整的工作证明时，它将其发送给矿池管理者，后者将其发布到比特币系统中。矿池管理者因此收到区块的全部收入，并根据其成员的算力公平分配。许多矿池是开放的——它们允许任何矿工通过公共互联网接口加入。

这种开放的矿池容易受到经典的区块扣留攻击[10]，其中矿工只向矿池管理者发送部分工作证明，并丢弃完整的工作证明。由于它向矿池发送的部分工作证明，该矿工被视为常规矿池成员，矿池可以估计其算力。因此，攻击者与其他矿池成员共享收入，但不做出贡献。它减少了其他成员的收入，也减少了自己的收入。我们在第二节中提供了比特币协议、矿池和经典区块扣留攻击的必要背景，并在第三节中指定了我们的模型。对于协议和生态系统的更广泛视角，读者可以参考Bonneau等人[11]的调查。

在这项工作中，我们分析了矿池之间的区块扣留攻击。实施矿池区块扣留攻击的矿池以常规矿工的身份注册到受害矿池。它从受害矿池接收任务，并将其转移给自己的一些矿工。我们称这些渗透矿工，并将矿池用于渗透的算力称为渗透率。当攻击矿池的渗透矿工提交部分工作证明时，攻击者将其转移到受害矿池，让被攻击的矿池估计他们的算力。当渗透矿工提交完整的工作证明时，攻击矿池将其丢弃。

这种攻击以多种方式影响矿池的收入。受害矿池的有效挖矿速率保持不变，但其总收入被分配给更多的矿工。攻击者的算力减少，因为其部分矿工用于区块扣留，但它通过渗透其他矿池获得额外收入。最后，系统中的总有效挖矿算力减少，导致比特币协议降低难度。

考虑到所有这些因素，我们观察到矿池可能通过攻击其他矿池来增加其收入。因此，每个矿池都会做出是否攻击系统中其他矿池的选择，以及以何种渗透率进行攻击。这导致了矿池游戏。我们在第四节中指定了这个游戏并提供了初步分析。

在第五节中，我们分析了只有两个矿池参与游戏且只有一个可以攻击另一个的场景。在这种情况下，攻击者总是可以通过攻击来增加其收入。我们得出结论，在一般情况下，任意数量的矿池中，没有矿池攻击并不是纳什均衡。

接下来，第六节讨论了两个矿池的情况，每个矿池都可以攻击另一个。在这里，分析变得更加复杂，原因有二。首先，每个矿池的收入通过渗透矿工影响另一个矿池的收入。我们证明了对于静态选择的渗透率，矿池收入会收敛。其次，一旦一个矿池改变其对另一个矿池的渗透率，后者可能更愿意改变其对前者的渗透率。因此，游戏本身需要多个回合才能收敛。我们通过分析表明游戏有一个单一的纳什均衡，并通过数值研究了不同矿池大小的均衡点。对于小于50%的矿池，在均衡点上，两个矿池的收入都低于非均衡的无攻击策略。

由于矿池可以随时决定开始或停止攻击，这可以被建模为矿工的困境——迭代囚徒困境的一个实例。在每次迭代中，攻击是主导策略，但如果矿池能够同意不攻击，两者都会在长期内受益。

最后，我们在第七节中讨论了参与者是任意数量的相同矿池的情况。存在一个对称均衡，其中每个参与的矿池攻击其他所有参与的矿池。正如少数两个矿池的情况一样，在这里，在均衡点上，所有矿池的收入都低于无矿池攻击策略。

我们的结果表明，矿池之间的区块扣留导致了一个不利的均衡。尽管如此，由于矿工的匿名性，单个矿池可能会受到诱惑去攻击，导致其他矿池也进行攻击。这可能对开放矿池产生毁灭性的影响：如果它们的收入减少，矿工将更愿意形成封闭矿池，这些矿池不能以这种方式被攻击。虽然这可能被视为对公共挖矿矿池的坏消息，但总体上，这对比特币系统来说可能是好消息，因为它更倾向于小型矿池。我们在第八节中检查了攻击的实际可行性，并在第九节中讨论了影响和模型扩展。

总之，我们的贡献如下：

1. 定义了矿池游戏，其中在基于工作证明的安全系统中，矿池之间使用矿池区块扣留攻击相互攻击。
2. 在一般情况下，没有矿池攻击并不是一个均衡。
3. 当两个少数矿池参与时，唯一的纳什均衡是矿池相互攻击，并且两者的收入都低于如果没有任何攻击的情况。因此，矿工面临着矿工的困境，这是迭代囚徒困境的一个实例，不断在攻击和无攻击之间做出选择。
4. 在多个相同大小的矿池中，存在一个对称的纳什均衡，其中所有矿池的收入都低于如果没有任何攻击的情况。
5. 对于比特币，开放矿池的低效均衡可能通过减少它们的吸引力并推动矿工转向更小的封闭矿池来服务于系统。

经典的区块扣留攻击与矿池本身一样古老，但直到最近才有人提出矿池使用这种攻击。我们在第十节中概述了相关的攻击和先前的工作，并在第十一节中得出最终结论。

Preliminaries--Bitcoin and pooled mining

比特币是一种分布式、去中心化的数字货币[12]、[13]、[1]、[14]。用户通过发起交易来使用该系统，系统的唯一任务是将交易序列化到一个单一的账本中，并拒绝那些由于与之前的交易冲突而无法序列化的交易。比特币交易受到加密技术的保护，确保只有比特币的合法所有者才能转移它。交易账本由矿工网络存储在一个称为区块链的数据结构中。

A. 工作证明的收益

区块链以区块的形式记录交易。第一个区块，被称为创世区块，是协议的一部分。一个有效的区块包含前一个区块的哈希、当前区块中交易的哈希以及一个比特币地址，该地址将因生成该区块而获得奖励。

任何矿工都可以通过（概率性地）证明它已经花费了一定量的工作，并通过覆盖网络向所有其他矿工发布带有证明的区块，将一个有效的区块添加到链中。当矿工创建一个区块时，它因其努力而获得比特币作为补偿。这种补偿包括用户为包含其交易而支付的每笔交易费用，以及因此引入系统的新铸造比特币的数量。

矿工需要做的工作是重复计算一个哈希函数——具体来说是区块头的SHA-256的SHA-256。为了表明他已经完成了这项工作，矿工提供了一个概率证明，如下所示。生成的区块有一个随机数（nonce）字段，可以包含任何值。矿工在这个字段中放置不同的值，并计算每个值的哈希。如果哈希的结果小于目标值，则随机数被视为解决方案，并且区块有效。

因此，**找到单个哈希的尝试次数是随机的，服从几何分布，因为每次尝试都是一个成功概率由目标值决定的成功伯努利试验。在现有的巨大哈希速率和小的目标值下，找到单个哈希的时间可以近似为指数分布。因此，矿工找到解决方案的平均时间与其哈希速率或挖矿算力成正比。**

为了维持比特币生成的恒定速率，并作为其防御拒绝服务和其他攻击的一部分，系统规范化了区块生成的速率。为了实现这一点，协议根据生成最近区块所需的时间确定性地定义了每个区块的目标值。目标值或难度每2016个区块更新一次，使得找到每个区块的平均时间为10分钟。

请注意，指数分布是无记忆的。如果所有矿工都在挖掘区块b，一旦在时间t找到了该区块，所有矿工都会在t时刻切换到挖掘后续区块b + 1，而不改变他们在t之后找到区块的概率分布。因此，具有挖矿算力mi的矿工i找到下一个区块的概率是其相对于系统总挖矿算力m的比例。

fork

在覆盖网络中，区块的传播需要几秒钟，因此两个远距离的矿工有可能生成竞争性的区块，这两个区块都将同一个区块作为它们的前驱。这种分叉或分叉是罕见的，因为平均挖矿间隔是10分钟，它们平均每60个区块发生一次[15]。**系统有一个机制来解决分叉，导致其中一个区块被丢弃。**

为了简化，我们忽略了分叉。由于在分叉时丢弃的区块是随机的，可以将此事件纳入找到区块的概率中，并考虑找到不会被丢弃的区块的概率。

B. 矿池

随着比特币价值的上升，比特币挖矿已经成为一个快速发展的行业。技术进步，导致更高效的哈希ASICs[16]，全球各地都在建设挖矿数据中心[17]。使用尖端挖矿设备以外的硬件进行挖矿是不盈利的，否则能源成本会超过预期收入。

尽管挖矿的预期收入与使用的挖矿设备的功率成正比，但使用小型设备的单个家庭矿工可能多年都不会挖到一个区块[18]。因此，矿工们经常组织成矿池。从逻辑上讲，**矿池是一组矿工，当其中一人成功挖到一个区块时，他们共享收入。对于每个挖到的区块，收入按其挖矿算力比例分配给矿池成员。因此，矿池成员的预期收入与其单独挖矿的收入相同。然而，由于矿池的强大算力，它以更高的速率挖到区块，因此收入收集的频率更高，允许稳定的每日或每周收入。**

在实践中，大多数矿池由一个集中的矿池管理者控制。2 矿工向矿池管理者注册并代表其挖矿：矿池管理者生成任务，矿工根据这些任务寻找可以作为工作证明的解决方案。一旦他们找到解决方案，他们就将其发送给矿池管理者。矿池管理者在比特币系统中作为一个单一的矿工行事。一旦它从其矿工那里获得一个合法的区块，它就发布它。区块将收入转移到矿池管理者的控制之下。然后，矿池管理者根据矿工的挖矿算力将收入分配给矿工。该架构如图1所示。

为了估计矿工的挖矿算力，矿池管理者为每个成员设置了一个部分目标，远大于（即更容易）比特币系统的目标。每个矿工都需要向矿池管理者发送根据部分目标正确的区块。部分目标被选择为大，以便部分解决方案频繁到达，足以让管理者准确估计矿工的算力，但小（难）以减少管理开销。矿池通常收取一小部分收入作为费用。我们在第九节中讨论了这种费用对我们分析的影响。

许多矿池是开放的，接受任何感兴趣的矿工。矿池接口通常由一个用于注册的网页接口和一个用于挖矿软件的矿工接口组成。为了为矿池挖矿，矿工通过网页接口注册，提供一个接收未来收入份额的比特币地址，并从矿池接收挖矿凭证。然后，他将他的凭证和矿池的地址输入到他的挖矿设备中，开始挖矿。挖矿设备从矿池获取任务，并发送部分和完整的工作证明，通常使用STRATUM协议[20]。当它找到区块时，矿池管理者根据其工作份额向矿工的账户记账，并根据请求或自动将这些资金转移到上述比特币地址。

过大的矿池
尽管矿池在允许小规模挖矿方面发挥了重要作用，但如果矿池规模过大，它们可能对比特币系统构成威胁。如果一个矿池控制了大部分挖矿算力，系统就会变得不稳定[21]、[22]（并且[23]警告说，即使矿池规模较小，系统也会不稳定）。可以说，在比特币系统的现实场景中，没有矿池控制着大部分挖矿算力。例如，在2014年6月的一天，一个名为GHash.IO的矿池在比特币主链上产生了超过50%的区块。比特币社区对矿池进行了强烈反对（矿池除了非常成功之外，并没有做任何更糟糕的事情）。GHash.IO减少了其相对挖矿算力，并公开承诺远离50%的限制。

C. 区块扣留及其检测

经典的区块扣留[10]是矿池成员对其他矿池成员发起的攻击。攻击矿工向矿池注册，并表面上开始诚实地挖矿——它定期向矿池发送部分工作证明。然而，攻击矿工只发送部分工作证明。如果它找到了构成完整工作证明的完整解决方案，它会丢弃该解决方案，减少矿池的总收入。3 这种攻击如图2所示。

攻击者不会改变矿池的有效挖矿算力，也不会直接影响其他矿池的收入。然而，被攻击的矿池与攻击者共享其收入。因此，每个矿工的收入减少，因为相同的收入被分配给了更多的矿工。

回想一下，工作证明只对特定的区块有效，因为它是使区块的哈希小于其目标的随机数。攻击矿工无法使用它。

此外，与单独挖矿或诚实地参与矿池相比，这种攻击减少了攻击者的收入：它像其他矿池参与者一样遭受收入减少，并且其收入少于其在系统总挖矿算力中的份额。因此，这种攻击只能用于破坏，对攻击者来说是有成本的。

检测：即使矿池检测到它正在遭受区块扣留攻击，它可能也无法确定其注册矿工中哪些是肇事者。矿池可以通过其矿工提供的部分工作证明和完整工作证明的速率来估计其预期挖矿算力和实际挖矿算力。超出设定置信区间的差异表明存在攻击。为了检测单个矿工是否在攻击，矿池必须使用类似的技术，比较基于攻击者部分工作证明估计的挖矿算力与其从未提供完整工作证明的事实。如果攻击者拥有较小的挖矿算力，它将频繁发送部分工作证明，但矿池只会预期以非常低的频率看到完整的工作证明。因此，它无法获得统计上显著的结果，这些结果会表明存在攻击。

攻击者可以使用多个小型区块扣留矿工，并频繁替换它们。例如，一个小型矿工的预期完整工作证明频率是每年一次。这样的矿工将看到不可忽略的平均每日收入（B25/365 ≈ B0.07）。如果攻击者每月替换这样一个小型矿工，他将在每个月底收集大约B2。矿池必须在这个月内决定该矿工是否是攻击者（并撤销其收入），或者只是一个不幸的诚实矿工。由于这种功率的诚实矿工在一个月内找到完整工作证明的可能性很小（根据指数分布的概率约为8%），因此基于这一标准的拒绝矿工的矿池将拒绝其大多数诚实矿工。拒绝小型矿工或按年分配收入的一般替代方案与矿池挖矿的目标相矛盾。

Model and standard operation

在第三部分A节中，我们明确了参与者操作的基本模型，接着在第三部分B节和C节中描述了诚实矿工如何在这个环境中运作，并在第三部分D节中阐述了如何在我们的模型中实施经典的区块扣留攻击。

A. 模型

该系统由比特币网络和具有唯一ID的节点组成，并按步骤推进。节点i生成与其ID i相关联的任务。节点可以在一个步骤的时间内处理一个任务。这项工作的结果是一组部分工作证明和一组完整的工作证明。每个集合中的证明数量遵循泊松分布，部分证明的平均值较大，而完整证明的平均值较小。处理任务的节点被称为矿工，矿工具有相同的算力，因此生成工作证明的概率相同。

比特币网络为完整的工作证明支付报酬。为了获得这种报酬，实体会向网络发布一个任务及其相应的工作证明。报酬归属于与任务相关联的ID。比特币协议对收入进行标准化，使得每个步骤中分配的平均总收入在整个系统执行过程中保持恒定。任何节点都可以通过发起比特币交易向另一个节点转移比特币。

生成任务但将工作外包出去的节点被称为矿池。矿池通过网络向矿工发送任务，矿工接收任务，执行工作，并将部分和完整的工作证明发送回矿池。

除了处理任务之外，所有本地操作、支付、消息发送、传播和接收都是即时的。我们假设矿工的数量足够多，以至于挖矿能力可以任意分割而不会受到解决约束。

用p表示矿池的数量，用m表示系统中的总挖矿能力，用mi表示参与矿池i（$1 \le i \le p$）的矿工数量。我们采用准静态分析，其中矿工参与矿池的情况在时间上不会发生变化。

B. 独立挖矿

独立矿工是一个自行生成任务的节点。在每个步骤中，它生成一个任务，并在该步骤的时间内对其进行工作。如果找到了完整的工作证明，它会将此证明发布以赚取报酬。

C. 矿池

矿池是一个充当协调者的节点，多个矿工可以注册到矿池并为它工作。在每个步骤中，矿池为每个注册的矿工生成一个任务，并通过网络发送。每个矿工接收其任务并在该步骤的时间内进行工作。在步骤结束时，矿工将其找到的完整和部分工作证明发送给矿池。矿池接收所有矿工的工作证明，记录部分工作证明，并发布完整的工作证明。它计算其总体收入，并继续在矿工之间分配。每个矿工根据其在当前步骤中的成功比例获得收入，即其部分工作证明占矿池接收的所有部分工作证明的比例。我们假设矿池不从收入中收取费用。矿池费用及其对我们的分析的影响在第九节中讨论。

D. 区块扣留矿工

注册到矿池的矿工可以执行经典的区块扣留攻击。攻击者矿工的操作就像为矿池工作一样。它接收其任务并在它们上工作，只是在每个回合结束时，它只发送其部分工作证明，如果找到了任何完整的工作证明，则省略它们。矿池记录矿工的部分工作证明，但无法区分运行诚实的矿工和区块扣留矿工。

其影响是，从事区块扣留的矿工不为其矿池的整体挖矿能力做出贡献，但仍根据其发送的部分工作证明按比例分享矿池的收入。

为了评估矿池的效率，我们定义了其每矿工收入如下。

定义1（收入密度）。矿池的收入密度是其成员平均收入与作为独立矿工平均收入的比率。

独立矿工的收入密度，以及与未受攻击矿池合作的矿工的收入密度为1。如果矿池受到区块扣留攻击，其收入密度会下降。

E. 连续分析

由于我们的分析将关注平均收入，我们将考虑工作证明，无论是完整的还是部分的，作为根据其概率的连续确定性大小。因此，处理任务的结果是工作证明的确定性分数。

The Pool Game

A. 矿池间的区块扣留攻击

就像矿工可以在矿池j上执行区块扣留一样，矿池i可以使用其部分挖矿能力渗透到矿池j并对其实施区块扣留攻击。用xi,j(t)表示在步骤t时这种渗透挖矿能力的数量。为矿池i工作的矿工，无论是诚实挖矿还是用于渗透矿池j，都对矿池i忠诚。在回合结束时，矿池i汇总其在当前回合的挖矿收入以及在前一回合的渗透收入。它根据矿工的部分工作证明将收入平均分配给所有忠诚的矿工。矿池的矿工对其角色一无所知，他们像常规的诚实矿工一样工作，处理任务。

B. 收入收敛

注意，矿池 j 在步骤结束时将其收入发送给来自矿池i的渗透者，而矿池i在后续步骤开始时计算这笔收入。如果存在一个长度为的矿池链，其中每个矿池都渗透下一个矿池，那么矿池收入将不会是静态的，因为渗透收入需要一步才能完成每次跳转。如果max是系统中最长的链，收入将在max步后稳定下来。如果在渗透图中存在循环，系统将收敛到一定的收入，如下面的引理所述。

引理1（收入收敛）。如果渗透率是恒定的，矿池的收入将收敛。

证明：用ri(t)表示矿池i在步骤t结束时的收入密度，并定义收入密度向量

$$\mathbf{r(t)} \triangleq (r_1(t), \ldots, r_p(t))^T$$

在每个回合中，矿池i使用其挖矿能力$m_1 - \sum_j x_{1,j}$用于直接挖矿（而非攻击），并将其分配给其$m_1 + \sum_j x_{j,1}$成员，包括恶意渗透者（所有求和范围为1,...,p）。用向量表示每个矿池的直接挖矿收入密度（忽略标准化，这是一个常数因子）。

$$\mathbf{m} \triangleq \left(\frac{m_1 - \sum_j x_{1,j}}{m_1 + \sum_j x_{j,1}}, \ldots, \frac{m_p - x_{p,j}}{m_p + \sum_j x_{j,p}} \right)^T$$

矿池 i 在步骤 t 通过从矿池 j 在步骤 $t-1$ 的收入中渗透获得的收入是 $x_{i,j} r_j(t-1)$ 。矿池i将其收入分配给其 $m_i + \sum_k x_{k,i}$ 成员——忠诚者和渗透者。通过其 i，j 元素定义 $p \times p$ 渗透矩阵

$$\mathbf{G} \triangleq \left[\frac{x_{i,j}}{m_i + \sum_k x_{k,i}} \right]_{ij}$$

步骤t的收入向量是

$$\mathbf{r}(t) = \mathbf{m} + \mathbf{G}\mathbf{r}(t-1) \tag{1}$$

由于渗透矩阵的行和都小于1，根据Perron-Frobenius定理，其最大特征值小于1。因此，所有矿池的收入收敛如下：

$$\mathbf{r}(t) = \left(\sum_{t'=0}^{t-1} G^{t'} \right) \mathbf{m} + G^t \mathbf{r}(0) \xrightarrow{t \to \infty} (1 - \mathbf{G})^{-1} \mathbf{m} \tag{2}$$

C. 矿池博弈

在矿池博弈中，矿池试图优化其对其他矿池的渗透率，以最大化其收入。在整个游戏中，矿工总数和忠于每个矿池的矿工数量保持不变。

时间以轮次推进。设s为一个足够大的常数整数，使得收入可以近似为其收敛极限。在每一轮中，系统进行s步，然后按照轮询策略选择一个矿池，该矿池可以改变其对所有其他矿池的渗透率。每一步的总收入被标准化为1/s，因此每轮的收入为1。

采取行动的矿池知道攻击它的渗透者（尽管不知道他们的身份）和其他每个矿池的收入率。这种知识对于优化矿池的收入是必要的，正如我们接下来所见。我们在第八节中解释了矿池如何技术上获得这种知识。

D. 一般分析

回想一下，m_i 是忠于矿池 i 的矿工数量，$x_{i,j}(t)$ 是矿池 i 在步骤 t 时用于渗透矿池 j 的矿工数量。

因此，矿池 i 的挖矿率是其忠实矿工数量减去用于渗透的矿工数量。这个有效的挖矿率除以系统中不参与区块扣留的所有矿工的总挖矿率。用以下公式表示矿池 i 在步骤 t 的直接挖矿率：

$$R_i \triangleq \frac{m_i - \sum_{j=1}^{p} x_{i,j}}{m - \sum_{j=1}^{p} \sum_{k=1}^{p} x_{j,k}} \tag{3}$$

矿池 i 在步骤 t 结束时的收入密度是其直接挖矿收入加上从被渗透矿池获得的收入，除以其忠实矿工数量加上攻击它的区块扣留渗透者数量：

$$r_i(t) = \frac{R_i(t) + \sum_{j=1}^{p} x_{i,j}(t) r_j(t)}{m_i + \sum_{j=1}^{p} x_{j,i}(t)} \tag{4}$$

此后，我们转向静态状态分析，并在表达式中省略 t 参数。

No attack

如果没有矿池参与区块扣留，

$$\forall i, j : x_{i,j} = 0$$

并且我们有：

$$\forall i : r_i = 1/m$$

也就是说，每个矿工的收入与其算力成正比，无论是在矿池中还是独立挖矿。

One Attacker

我们从两个矿池的简化博弈开始分析，即矿池1和矿池2，其中矿池1能够渗透矿池2，而矿池2则不能渗透矿池1。在两个矿池之外的m - m1 - m2个矿工独立挖矿（或与不参与攻击且无法被攻击的封闭矿池合作）。这一情景如图3所示。虚线红箭头表示矿池1的x1,2挖矿能力通过区块扣留攻击的方式渗透矿池2。

由于矿池2不参与区块扣留，其所有m2个忠实矿工都为其工作。另一方面，矿池1没有使用其忠实矿工中的x1,2，其直接挖矿能力仅为m1 - x1,2。比特币系统通过所有发布完整证明的矿工总数（即除x1,2之外的所有矿工）来标准化这些比率。因此，矿池的直接收入为

$$R_1 = \frac{m_1 - x_{1,2}}{m - x_{1,2}}$$
$$R_2 = \frac{m_2}{m - x_{1,2}} \tag{5}$$

Pool 2 将其收入分配给其忠实的矿工和渗透其中的矿工。因此其收入密度为

$$r_2 = \frac{R_2}{m_2 + x_{1,2}} \tag{6}$$

矿池1将其收入分配给其注册的矿工。收入包括其直接挖矿收入以及其渗透者在矿池2获得的收入，即 $r_2 \cdot x_{1,2}$ 。因此，每个忠于矿池1的矿工的收入为

$$r_1 = \frac{R_1 + x_{1,2} \cdot r_2}{m_1} \tag{7}$$

我们通过将r2从方程6和R1、R2从方程5代入，得到了方程7中r1的表达式：

$$r_1 = \frac{m_1 \left(m_2 + x_{1,2}\right) - x_{1,2}^2}{m_1 \left(m - x_{1,2}\right) \left(m_2 + x_{1,2}\right)}$$

A. 游戏进程

矿池1控制其对矿池2的渗透率，即 $x_{1,2}$，并将选择在矿池博弈第一轮中最大化收入密度（每矿工收入）r_1 的值。r_1 在可行范围 $0 \leq \ x_{1,2} \ \leq m_1$ 内有一个最大值点。由于矿池2无法对矿池1的攻击做出反应，这一点是系统的稳定状态，我们用 $\bar{x}_{1,2} \triangleq \arg\max_{x_{1,2}} r_1$ 表示 $x_{1,2}$ 在该点的值，以及相应的矿池收入 $\bar{r}_1$ 和 $\bar{r}_2$。通过替换稳定的 $x_{1,2}$ 值，我们得到了两个矿池的收入；所有这些都在图4中给出，为了简化表达式，我们将m = 1进行标准化。

$$\bar{x}_{1,2} = \frac{m_2 - m_1 m_2 - \sqrt{-m_2^2(-1 + m_1 + m_1 m_2)}}{-1 + m_1 + m_2}$$
$$\bar{r}_1 = \frac{m_1 + (2 + m_1)m_2 - 2\sqrt{-m_2^2(-1 + m_1 + m_1 m_2)}}{m_1(1 + m_2)^2}$$
$$\bar{r}_2 = \frac{m_2(-1 + m_1 + m_2)^2}{\left(m_2^2 - \sqrt{-m_2^2(-1 + m_1 + m_1 m_2)}\right)\left(1 - m_1(1 + m_2) - \sqrt{-m_2^2(-1 + m_1 + m_1 m_2)}\right)}$$

Figure 4. Stable state where only pool 1 attacks pool 2.

B. 数值分析

我们通过找到最大化r1的 $x_{1,2}$值，并将此值替换为r1和r2来数值分析这个游戏。我们通过整个可行范围改变矿池的大小，并在图5中描绘了最佳的 $x_{1,2}$和相应的收入。每个图中的每个点代表具有相应m1和m2大小的游戏的均衡点，其中我们标准化m = 1。所有图的右上部分范围是不可行的，因为m1和m2的总和大于1。我们使用这个范围作为参考颜色，并使用虚线显示这个值在可行范围内的边界。

图5a显示了最佳渗透率。在整个可行范围内，我们看到矿池1选择了一个严格正的 $x_{1,2}$值。实际上，矿池1的收入在图5b中显示，并且在整个可行区域内，它严格大于1，这是矿池在没有攻击（ $x_{1,2} = 0$ ）时会得到的。图5c描绘了矿池2的收入，它在整个范围内严格小于1。

第三方：请注意，当矿池1选择渗透矿池2时，整个系统的挖矿能力会减少。因此，不属于任何矿池的第三方矿工的收入从 $1/m$ 增加到 $1/(m - x_{1,2})$。因此，矿池2为攻击者及其系统中其他所有人的增加收入买单。

C. 对一般情况的启示

考虑p个矿池的情况。对于任何矿池大小m1,...,mp的选择，至少有一个矿池会选择进行区块扣留：

引理2. 在具有p个矿池的系统中，点 $\forall j,k\ :x_j^k=0$ 不是均衡点。

证明：假设与事实相反，这不是情况，并且 $\forall j,k\ :x_j^k=0$ 是一个均衡点。现在考虑只有矿池1和矿池2的情况，并将其他矿池视为独立矿工。这是上面分析的设置，我们已经看到矿池1可以通过对矿池2进行区块扣留攻击来增加其收入。用x˜1,2 > 0表示矿池1的渗透率。现在，将这些值带回到具有p个矿池的当前设置中。当

$$x_{1,2}=\tilde{x}_{1,2}\forall\,(j,k)\neq(1,2)\ :x_{1,2}\ =\ 0$$

时，矿池1的收入更好。因此，矿池1可以通过攻击矿池2来改善其收入，没有人攻击不是一个均衡点。

D. 测试案例

作为一个测试案例，我们采用了2015年1月16日的矿池分布情况[24]，如图6所示。我们分析了每个矿池攻击所有其他开放矿池的情况，所有这些矿池都表现诚实。请注意，以与其大小成比例的力量攻击所有矿池，与攻击它们总大小的单个矿池得到的结果相同。将数字代入上述分析显示，较大的矿池需要使用其挖矿能力中较小比例的力量进行渗透，并且其收入密度的增加比小矿池更多。最大的矿池DiscusFish在其挖矿能力的25%达到其最佳攻击率，其收入增加了近3%。这相当于每天增加B26比特币，或按当时汇率计算的近5500美元。这代表了矿池净收入的显著增加。然而，对于最小的矿池Eligius来说，攻击的利润要小得多。为了达到最佳状态，它需要几乎三分之一的电力用于攻击，但其收入密度仅增加了0.6%，相当于每天B0.86或18美元。

Two Pool

我们继续分析两个矿池可能相互攻击，而其他矿工独立挖矿的情况。再次我们有大小为m1的矿池1和大小为m2的矿池2；矿池1控制其对矿池2的渗透率x1,2，但现在矿池2也控制其对矿池1的渗透率x2,1。这一情景如图8所示。

系统中的总挖矿能力是m - x1,2 - x2,1。矿池的直接收入R1和R2来自挖矿，是其有效挖矿率（不包括渗透挖矿能力）除以总挖矿率。

$$R_1=\frac{m_1-x_{1,2}}{m-x_{1,2}-x_{2,1}}$$
$$R_2=\frac{m_2-x_{2,1}}{m-x_{1,2}-x_{2,1}}$$

每个矿池的总收入是其直接挖矿收入（如上所述）和前一轮的渗透收入，即被攻击矿池的总收入乘以其渗透率。矿池的总收入在其忠实矿工和渗透它的矿工之间分配。在稳定状态下，这是

$$r_1=\frac{R_1+x_{1,2}r_2}{m_1+x_{2,1}}$$
$$r_2=\frac{R_2+x_{2,1}r_1}{m_1+x_{1,2}}$$

求解r1和r2，我们得到了每个矿池的封闭表达式。我们将收入表示为 $x_{1,2}$ 和 $x_{2,1}$ 的函数。

$$r_1\left(x_{1,2},x_{2,1}\right)=\frac{m_2R_1+x_{1,2}\left(R_1+R_2\right)}{m_1m_2+m_1x_{1,2}+m_2x_{2,1}}$$
$$r_2\left(x_{2,1},x_{1,2}\right)=\frac{m_1R_2+x_{2,1}\left(R_1+R_2\right)}{m_1m_2+m_1x_{1,2}+m_2x_{2,1}}\qquad(11)$$

每个矿池只控制自己的渗透率。在矿池博弈的每一轮中，每个矿池都会优化其对另一个矿池的渗透率。如果矿池1在步骤t采取行动，它会优化其收入通过

$$x_{1,2}(t) \leftarrow \arg\max_{x'} r_1\left(x', x_{2,1}(t-1)\right) \tag{12}$$

而如果矿池2在步骤 t 采取行动，它会优化其收入通过

$$x_{2,1}(t) \leftarrow \arg\max_{x'} r_2\left(x', x_{1,2}(t-1)\right) \tag{13}$$

存在一个均衡点，其中池1和池2都无法通过改变其渗透率来提高其收入。也就是说，任何一对值x_1', x_2'满足以下条件：

$$\begin{cases} \arg\max_{x_{1,2}} r_1\left(x_{1,2}, x_{2,1}'\right) = x_{1,2}' \\ \arg\max_{x_{2,1}} r_2\left(x_{1,2}', x_{2,1}\right) = x_{2,1}' \end{cases} \tag{14}$$

在约束条件

$$\begin{aligned} 0 < x_1' < m_1 \\ 0 < x_2' < m_2 \end{aligned} \tag{15}$$

下，池的大小可行区域为$m_1 > 0, m_2 > 0$，且$m_1 + m_2 \leq m$。对于所有可行的变量值，r_i的收入函数在x_i上是凹的$\left(\partial^2 r_i / \partial x_i^2 < 0\right)$。因此，方程12和13的解是唯一的，并且位于可行区域的边界上或满足$\partial r_i / \partial x_{i,j} = 0$。

从第五节我们知道，无攻击不是一个均衡点，因为每个池可以通过选择严格正的渗透率来增加其收入，即$x_{1,2} = x_{2,1} = 0$不是方程14-15的解。

因此，纳什均衡存在，其中$x_{1,2}, x_{2,1}$的值满足

$$\begin{cases} \frac{\partial r_1(x_{1,2}, x_{2,1})}{\partial x_{1,2}} = 0 \\ \frac{\partial r_2(x_{2,1}, x_{1,2})}{\partial x_{2,1}} = 0 \end{cases} \tag{16}$$

使用符号计算工具，我们发现对于任何可行的m_1和m_2选择，方程16只有一个值对成立。

A. 数值分析

一项数值分析证实了这些观察结果。我们对一系列池大小进行了池游戏的模拟。对于每种池大小的选择，我们从两个池都不互相渗透的状态开始模拟，即$x_{1,2} = x_{2,1} = 0$，且收入密度为$r_1 = r_2 = 1$。在每一轮中，一个池根据池大小和被渗透的速率选择其最优的渗透率，并使用方程11计算收敛后的收入。回想一下，池游戏中的玩家是按照轮流政策选择的，因此池轮流进行，我们让游戏运行直到收敛。结果如图7所示。

每次运行具有某些m_1, m_2值的结果在图7的每个图中产生一个点。我们在图7a-7b中描绘了两个池的渗透率$x_{1,2}, x_{2,1}$，在图7c-7d中描绘了池的收入密度r_1, r_2。因此，对于每种m_1和m_2的选择，$x_{1,2}, x_{2,1}, m_1$和m_2的值是每个图中具有相应坐标的点。

对于$x_{i,j}$图，我们在均衡状态下i不攻击的区域周围画了一个边界。对于r_i图，我们在收入与无攻击场景相同，即1的区域周围画了一条线。

我们首先观察到，只有在极端情况下，一个池不会攻击其对手。具体来说，在均衡状态下，一个池只有在另一个池大于约总挖矿能力的80%时才会停止攻击。

但更重要的是，我们观察到，只有当一个池控制了严格多数的总挖矿能力时，它才能提高其收入，相比于无池攻击的场景。这些是图7c和7d中的小三角形区域。在其余的空间，即图中的梯形区域，池的收入比无池攻击场景下的收入要低。

B. 囚徒困境

在一个健康的比特币环境中，当没有任何一个池控制严格多数的挖矿能力时，两个池在均衡状态下的收入将低于两个池都不攻击时的收入。在这种情况下，我们可以分析一个游戏，其中每个池选择要么攻击并优化其收入，要么不攻击。

不失一般性地考虑池1。正如我们在第五节中看到的，如果池2不攻击，池1可以通过攻击将其收入提高到1以上。如果池2攻击但池1不攻击，我们用$\tilde{r}_1$表示池1的收入。$\tilde{r}_1$的确切值取决于m_1和m_2的值，但它总是小于1。如上所述，如果池1确实选择攻击，其收入会增加，但不会超过1。这个游戏在图9中进行了总结。

Pool 1 / Pool 2	no attack	attack
no attack	$(r_1 = 1, r_2 = 1)$	$(r_1 > 1, r_2 = \tilde{r}_2 < 1)$
attack	$(r_1 = \tilde{r}_1 < 1, r_2 > 1)$	$(\tilde{r}_1 < r_1 < 1, \tilde{r}_2 < r_2 < 1)$

Figure 9. Prisoner's Dilemma for two pools. The revenue density of each pool is determined by the decision of both pools whether to attack or not. The dominant strategy of each player is to attack, however the payoff of both would be larger if they both refrain from attacking.

当只玩一次时，这是经典的囚徒困境。攻击是主导策略：无论池2选择攻击与否，池1在攻击时的收入都比不攻击时大，对池2也是如此。在这个攻击或不攻击的游戏的均衡状态下，当两个池都攻击时，每个池的收入都比两个池都不攻击时的收入小。

然而，这个游戏不是只玩一次，而是持续不断地进行，形成了一个超级游戏，其中每个池可以在攻击和不攻击之间改变其策略。池们可以同意（即使是隐含地）不攻击，并且在每一轮中，一个池可以检测到它是否正在被攻击，并推断出另一个池正在违反协议。在这种超级游戏中，尽管在每一轮中单一的纳什均衡是攻击，但两个池都不攻击的合作状态是一个可能的稳定状态[25]，[26]。

C. 测试案例

作为一个例子，我们再次采用图6中显示的池大小，并研究两个最大的池，DiscusFish和AntPool，相互攻击的情况。最优的渗透率（相对于总系统挖矿能力）分别为8%和12%，而这两个池相比无攻击场景将分别损失4%和10%的收入。

q Identical Pools

假设有 q 个大小相同的矿池相互进行区块扣留攻击。其他矿工既不攻击也不被攻击。在这种情况下，存在一个对称均衡。不妨考虑矿池 1 的一个步骤。它控制着对其他每个矿池的攻击率，并且由于对称性，这些攻击率都是相同的。用 $x_{1,\neg 1}$ 表示矿池 1 对任何其他矿池的攻击率。其他每个矿池也可以攻击其同伴。由于对称性，所有攻击者的攻击率都是相同的。用 $x_{\neg 1,*}$ 表示任何非 1 矿池对任何其他矿池（包括矿池 1）的攻击率。

用 R_1 表示矿池 1 的直接收入（来自挖矿），用 $R_{\neg 1}$ 表示其他每个矿池的直接收入。类似地，用 r_1 和 $r_{\neg 1}$ 分别表示矿池 1 和其他矿池的收入密度。

通用方程 3 和 4 被实例化为

$$
\begin{aligned}
R_1 &= \frac{m_i - (q-1)x_{1,\neg 1}}{m - (q-1)(q-1)x_{\neg 1,*} - (q-1)x_{1,\neg 1}} \\
R_{\neg 1} &= \frac{m_i - (q-1)x_{\neg 1,*}}{m - (q-1)(q-1)x_{\neg 1,*} - (q-1)x_{1,\neg 1}}
\end{aligned}
\tag{17}
$$

和

$$
\begin{aligned}
r_1 &= \frac{R_1 + (q-1)x_{1,\neg 1} r_{\neg 1}}{m_i + (q-1)x_{\neg 1,1}} \\
r_{\neg 1} &= \frac{R_{\neg 1} + (q-2)x_{\neg 1,*} r_{\neg 1} + x_{\neg 1,*} r_1}{m_i + (q-2)x_{\neg 1,*} + x_{1,\neg 1}}
\end{aligned}
\tag{18}
$$

将方程 17 代入方程 18 并求解，我们得到一个单一表达式，因为在对称情况下我们有 $r_1 = r_{\neg 1}$。该表达式显示在方程 18（图 10）中。

给定任何 q 和 m_i 的值（其中 $qm_i < 1$），渗透率的允许范围是 $0 \leq x_{i,j} \leq m_i/q$。在这个范围内，$r_i$ 是连续的、可微的，并且关于 $x_{1,\neg 1}$ 是凹的。因此，矿池 1 的最优点是 $\partial r_1 / \partial x_{1,\neg 1} = 0$ 的地方。由于函数是凹的，该方程产生一个单一的可行解，它是其他矿池的攻击率，即 $x_{\neg 1,1}$ 和 $x_{\neg 1,*}$ 的函数。

为了找到对称均衡，我们令 $x_{1,\neg 1} = x_{\neg 1,1} = x_{\neg 1,*}$ 并得到一个单一的可行解。均衡渗透率和相应的收入显示在方程 20（图 11）中。

与两个矿池的情况一样，对称均衡时的收入低于无人攻击的非均衡策略。

$$
r_i = -\frac{m_i^2 + m_i x_{1,\neg 1} - (q-1)x_{1,\neg 1}((q-1)x_{\neg 1,*} + x_{1,\neg 1})}{((q-1)x_{1,\neg 1} + (q-1)^2 x_{\neg 1,*} - 1)\left((m_i + x_{1,\neg 1})(m_i + (q-1)x_{\neg 1,1}) - (q-1)x_{1,\neg 1}x_{\neg 1,*}\right)}
\tag{19}
$$

Figure 10. Expression for r_i in a system with pools of equal size.

$$
\begin{aligned}
\bar{x}_{1,\neg 1} = \bar{x}_{\neg 1,1} = \bar{x}_{\neg 1,*} &= \frac{q - m_i - \sqrt{(m_i - q)^2 - 4(m_i)^2(q-1)^2 q}}{2(q-1)^2 q)} \\
\bar{r}_1 = \bar{r}_{\neg 1} &= \frac{2q}{q - m_i + 2m_i q + \sqrt{(m_i - q)^2 - 4(m_i)^2(q-1)^2 q}}
\end{aligned}
\tag{20}
$$

Figure 11. Symmetric equilibrium values for a system of q pools of equal sizes.