復旦大學

本科毕业论文（设计）

论文题目：基于马尔科夫决策过程的区块链安全分析

院　　系：大数据学院

专　　业：统计学（数据科学与大数据技术方向）

姓　　名：周璐鹿　　学　　号：15307110349

指导教师：徐跃东　　职　　称：副教授

单　　位：复旦大学信息科学与工程学院

日　　期：2020　年　6月　9日

毕业论文（设计）撰写人诚信承诺

《学位论文作假行为处理办法》（节选）

（中华人民共和国教育部令第34号发布，自2013年1月1日起施行）

第二条

向学位授予单位申请博士、硕士、学士学位所提交的博士学位论文、硕士学位论文和本科学生毕业论文（毕业设计或其他毕业实践环节）（统称为学位论文），出现本办法所列作假情形的，依照本办法的规定处理。

第三条 本办法所称学位论文作假行为包括下列情形：

（一）购买、出售学位论文或者组织学位论文买卖的；

（二）由他人代写、为他人代写学位论文或者组织学位论文代写的；

（三）剽窃他人作品和学术成果的；

（四）伪造数据的；

（五）有其他严重学位论文作假行为的

第四条

学位申请人员应当恪守学术道德和学术规范，在指导教师指导下独立完成学位论文。

第五条

指导教师应当对学位申请人员进行学术道德、学术规范教育，对其学位论文研究和撰写过程予以指导，对学位论文是否由其独立完成进行审查。

第七条

学位申请人员的学位论文出现购买、由他人代写、剽窃或者伪造数据等作假情形的，学位授予单位可以取消其学位申请资格；已经获得学位的，学位授予单位可以依法撤销其学位，并注销学位证书。取消学位申请资格或者撤销学位的处理决定应当向社会公布。从做出处理决定之日起至少3年内，各学位授予单位不得再接受其学位申请。

前款规定的学位申请人员为在读学生的，其所在学校或者学位授予单位可以给予开除学籍处分；为在职人员的，学位授予单位除给予纪律处分外，还应当通报其所在单位。

第八条

为他人代写学位论文、出售学位论文或者组织学位论文买卖、代写的人员，属于在读学生的，其所在学校或者学位授予单位可以给予开除学籍处分；属于学校或者学位授予单位的教师和其他工作人员的，其所在学校或者学位授予单位可以给予开除处分或者解除聘任合同。

第九条

指导教师未履行学术道德和学术规范教育、论文指导和审查把关等职责，其指导的学位论文存在作假情形的，学位授予单位可以给予警告、记过处分；情节严重的，可以降低岗位等级直至给予开除处分或者解除聘任合同。

论文撰写人承诺：

本毕业论文是本人在导师指导下独立完成的，内容真实、可靠。本人在撰写毕业论文过程中不存在请人代写、抄袭或者剽窃他人作品、伪造或者篡改数据以及其他学位论文作假行为。

本人清楚知道学位论文作假行为将会导致行为人受到不授予/撤销学位、开除学籍等处理（处分）决定。本人如果被查证在撰写本毕业论文过程中存在学位论文作假行为，愿意接受学校依法作出的处理（处分）决定。

承诺人签名： **日期：** 2020 年 6月 9日

目录

目录 3
摘要 4
ABSTRACT 4
引言 5
第一章 区块链原理及区块安全基础 6
1.1 区块链原理及发展概况 6
1.1.1 区块链原理 6
1.1.2 区块链发展概况 6
1.2 对区块链协议的攻击 7
1.2.1 概述 7
1.2.2 自私挖矿攻击原理 7
1.2.3自私挖矿攻击收益分析 8
1.2.4 最优自私挖矿策略 9
1.2.5 最优自私挖矿模型求解及结果展示 10
1.2.6 区块截留攻击原理 11
1.2.7 区块链截留攻击收益分析 12
1.3 自私挖矿和区块截留攻击对比 13
1.3.1 收益比较 13
1.3.2自私挖矿和区块截留攻击的本质 14
第二章 联合两种攻击方法 15
2.1 混合攻击策略 15
2.2 混合攻击收益 15
第三章 最优混合攻击策略 17
3.1 最优化派出算力 17
3.2 有撤回的混合攻击马尔科夫模型 17
3.2.1 模型概述 17
3.2.2 模型假设 18
3.2.3 动作、状态转移及收益 19
3.2.4 模型求解方法及结果 19
3.2.5 结果分析 20
第四章 讨论及结论 21
4.1 混合攻击马尔科夫模型启示 21
4.2 不足及未来工作 21
4.3 结论 21
参考文献 22
附录 1 24
致谢 25

摘要

区块链通过巧妙的设计实现了无门槛的分布式交易系统。自从区块链系统诞生之初，区块链安全问题就备受关注。本文探索了 2 种重要的区块链攻击：自私挖矿攻击和区块截留攻击，求得了在攻击者算力不同情况下的最优攻击方法。更重要的是，我们通过建立马尔科夫决策模型，动态地结合两种攻击方式，创造出了一种新的区块链攻击策略，这种攻击策略能显著提升攻击者的收益，优于单独使用一种攻击方式或静态地结合两种攻击手段。

关键词：区块链，安全，马尔科夫决策模型，自私挖矿，区块截留攻击

ABSTRACT

Blockchain is a well-designed truly distributed transaction system. Since the invention of the blockchain system, blockchain security issues have received much attention. This paper focus on two important attacks on bitcoin protocol: selfish mining attack and block withholding attack. We did research on which the best attack strategy is on different computational power of attacker. What is more, we created a new attack by dynamically combining these two attack strategy with Markov decision process. This new attack strategy could increase the revenue of attacker significantly, better than using one attack strategy or statically combining two attack strategies.

Keywords: Blockchain, Security, Markov Decision Process, Selfish Mining, Block Withhodling Attack

引言

区块链系统自从诞生之初就广受关注。它第一次较为理想地解决了分布式的交易系统问题，使得去中心化的货币发行成为可能。相比于中心化的交易系统，区块链的安全是建立在区块协议的设计足够巧妙的基础上。因此，对区块链的攻击与对中心化系统的攻击不同，除了使用传统的网络攻击之外，也可以通过发掘区块链规则的漏洞来进行。本文就是通过研究对区块链规则的攻击方法来对区块链安全进行分析。通过揭示区块链的安全漏洞，我们可以为区块链的规则设计提供参考，从而提升区块链的安全性。

在区块链安全研究中，马尔科夫决策过程和博弈论是经常被使用的方法[11][12]。通过建立模型、考察各种攻击方式对区块链系统的破坏力，可以量化地衡量区块链系统的安全性。强化学习为自动化发掘区块链协议中的漏洞提供了新思路[10][15]。

本文使用的方法是基于马尔科夫决策模型的安全分析，通过建立模型、求解模型对新的攻击方法的收益进行探索。我们发现，当我们把自私挖矿攻击和区块截留攻击相结合，这种新的攻击方法可以显著提升攻击效果。因此，在评价区块链协议的安全性的时候，除了考虑其于一种攻击方式的防御效果以外，还需要考虑其对于混合攻击的防御效果，这样才能较好地衡量区块链的安全性。

第一章 区块链原理及区块安全基础

1.1 区块链原理及发展概况

1.1.1 区块链原理

2008 年，比特币[1]正式上线。在比特币出现之前，几乎所有的货币都需要由一个中心化的机构发行，一般是国家央行。即便是虚拟货币，通常也需要中心化机构来行使管理职能，本质上仍然是中心化的，而非分布式的。区块链技术的价值在于，通过让整个社区共同维护一个不可更改的公共账本的方法，实现了真正意义上的分布式交易系统，解决了去中心化系统中交易的多方互信问题。比特币系统的进入和退出没有门槛和审查，交易信息对系统内所有人公开，让每个成员保存所有的交易数据，避免了中心化机构腐败或者数据丢失的风险。

区块链中每个区块的头部包含了前一个区块的信息，所有区块因此相连而形成一条链。在比特币的系统中，用户发布在社区内的交易信息被区块中的参与者打包成区块。若参与者想要让自己打包的这个区块成为被全网所认可的合法区块，则需计算出一个随机串加入这个区块中，使得整个区块的哈希值小于某个特定值，然后再把这个块发布到网络中。使哈希函数的值小于某个特定值目前还没有启发式算法，只能暴力计算。这个通过不断尝试、消耗算力来求解符合要求的随机串的过程被称为“挖矿”，这些打包区块并尝试计算合法区块的参与者被称为“矿工”。当一个区块被系统中大部分节点接受而成为合法区块之后，矿工可以获得系统奖励的挖矿收益和区块所打包的交易的手续费。区块链在设计时设定的区块产生速度约为每 10 分钟产生一个区块。为了维持产生区块的速度稳定，每两周会自动进行一次挖矿难度调整[8]，即调整合法块哈希值的阈值，使得难度与当前的全网总挖矿算力相匹配。这种需要提供一个随机串作为消耗算力证明的系统设计被称为“工作证明”（proof of work）[20]。

目前，区块链中矿工的主要收益来自于系统对挖矿的奖励，但是按照一部分区块链（例如比特币）系统的设计，矿工最终的挖矿收益会主要来自于区块中的交易费。此时，由于每个区块中的交易费各不相同，每个区块的价值也就会有较大差异，因此会给区块链的安全带来新的挑战[13]。本文中，我们研究的依然是每个区块价值相同的情况。

1.1.2 区块链发展概况

2020 年 5 月比特币的均价约为 8000 美元，2017 年时曾达到近 20000 美元的峰值。继比特币之后，基于工作证明的区块链系统还有以太坊、莱特币等。这些虚拟货币的匿名性质使得它们被大量运用于对隐私保护要求很高的交易，包括黑市交易。据估计，比特币网络中的涉及到非法行为的交易占比约为二分之一[2]。同时，它们的无国界性

也为便捷的跨国汇款提供方便。而由于交易确认周期和各国法律限制等问题，虚拟货币用于实际生活交易（例如买咖啡）暂时还未普及。目前，比特币系统开发者们也致力于用多种方式减少交易延迟，提升系统的易用性[3]。目前，针对自私挖矿等区块链攻击，已经产生了不少新的区块链规则设计作为对抗[14]，但在后来的学者证明这些设计对抗攻击效果并非十分有效：新设计在某些情况下降低了攻击者收益，但在另外一些情况下却增加了攻击者收益[12]。

随着越来越多的矿工参加到比特币挖矿中，比特币挖矿的难度也随之上涨，单个矿工很可能需要等待很长时间才能挖出一个区块。因此，单个矿工收益的不确定性增加。为了降低挖矿的风险，矿池就应运而生了。矿池是矿工的集合，由矿池经理管理，挖矿所得的收益也按一定规则分配给矿工，以此降低矿工收益的不确定性。矿池分为公开矿池和私有矿池，公开矿池加入没有门槛，私有矿池只对特定矿工开放。同时，每个矿池所采用的收益分配规则也不尽相同。本文中分析的矿池是公开矿池，收益分配规则在下文中介绍。

1.2 对区块链协议的攻击

1.2.1 概述

比特币是一个无准入门槛的匿名系统，所以比特币系统的安全建立在这样一个基础上：遵守区块链规则可以使得参与者获得最优收益。如果有一种偏离规则的策略可以获得超额利润，那么这就是一种对区块链协议的攻击。攻击者获得的超额利润可以吸引更多的诚实挖矿者转而加入攻击者，从而使得攻击者算力增加，对区块链的安全造成进一步的破坏。对区块链协议的攻击体现出了区块链规则设计的漏洞，而对这些攻击策略的发现和研究可以揭示出区块链规则的本质，为区块链规则的设计提供参考。与对区块链协议的攻击相对的另一类攻击是对区块链网络的攻击，这类攻击可以通过让区块链节点之间通讯断开或延迟来达到攻击的目的。下面，我们分别介绍两种受到广泛关注的对区块链协议的攻击行为，自私挖矿攻击和区块截留攻击。

1.2.2 自私挖矿攻击原理

自私挖矿最早在2013年被提出[4]。自私挖矿的攻击策略如下：当自私挖矿者挖到一个区块的时候，他不立即发布这个区块，而是基于自己挖到的块继续挖矿。自私挖矿者私藏的块组成的链被称为私链，而区块链中其余的诚实挖矿者挖出的区块所组成的链为公链。公链和私链从同一个区块开始分叉，这个区块被称为起点。自私挖矿的过程中，可能出现3种不同情况，接下来分别介绍：

从起点开始，当对方挖出一个块的时候，自私挖矿者直接采用公链。这时诚实挖矿者获得1个块的收益。

如果自私挖矿者挖出了一个块，然后诚实挖矿者挖出了另一个块，那么自私挖矿者会立即发布自己挖出的块。这时候，自私挖矿者和部分诚实挖矿者会基于自私挖矿者的块挖矿，而部分诚实挖矿者会基于诚实挖矿者挖出个块挖矿。如果自私挖矿者首先挖出一个块，那么他可以获得 2 个块的收益；如果基于自私挖矿者的块挖矿的诚实矿工首先挖出一个块，那么自私挖矿者获得 1 个块的收益，诚实挖矿者获得 1 个块的收益。如果基于诚实挖矿者块挖矿的诚实矿工挖出了 1 个块，那么诚实挖矿者收益为 2，自私挖矿者收益为 0。

如果自私挖矿者领先于诚实挖矿者 2 个块及以上，那么自私挖矿者会持续自私挖矿，直到领先优势变为 1 的时刻立即发布私链，获得私链中所有块的收益。而诚实挖矿者的链短于自私挖矿者，所以诚实挖矿者的收益为 0。

自私挖矿的马尔科夫状态转移及收益的示意图见图 1.1，其中的状态代表自私挖矿者领先块的个数，R 表示该步带来的收益，没标注则表示回报为 0。参数 α 代表着自私挖矿者算力占全网总算力的比例。挖矿者的收益和区块链链网络的连通性也是相关的[16]，如果一个矿工发布的块能够更快地传播到网络中的大部分节点上，那么她在竞争中就占得了先机。在自私挖矿模型中，区块传播速度这个网络参数被包含在参数 γ 中。γ 的意义是当自私挖矿者和诚实挖矿者同时发布两条相同长度的链之后，接在自私挖矿者的链之后挖矿的诚实挖矿者的比例。当自私挖矿者的区块传播得越快时，γ 越大。

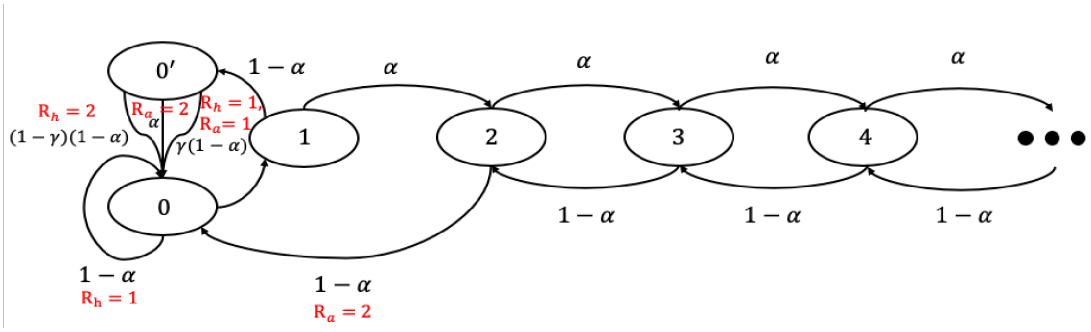

图 1.1: 自私挖矿攻击的马尔科夫链示意图

1.2.3自私挖矿攻击收益分析

通过马尔科夫链模型，可以计算出自私挖矿时各种状态发生的概率。求出每种状态发生的概率之后，再结合状态转移概率和相对应的回报，可以计算出自私挖矿的收益。在图 1.2 中，展示了自私挖矿的攻击者收益。同时，我们还复现了仿真模拟。仿真模拟用随机数模拟状态转移，通过平均多次实验的结果求出自私挖矿者的收益期望。模拟的结果证明了模型求得的理论结果的准确性。本文中的收益只考虑了平均收益，如果将自私挖矿收益的不确定性纳入考量，即考虑风险，收益的计算会更加复杂[17]。

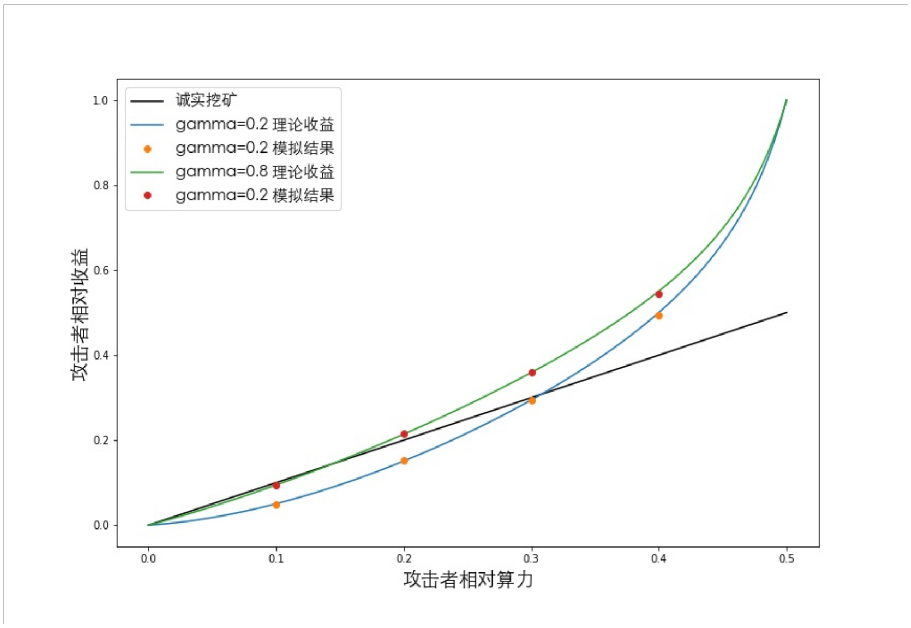

图 1.2：自私挖矿攻击者收益及模拟结果

1.2.4 最优自私挖矿策略

2013 年提出的自私挖矿策略并不是最优策略，Sapirshtein 等学者用马尔科夫决策过程来计算出了最优的策略和最优收益[5]。不过，最优自私挖矿策略没有显式解，只能在给定攻击者算力和网络参数的情况下用解出收益的上界和下界的数值解。

最优自私挖矿模型的动作空间包含 4 个动作，分别为接受、覆盖、竞争和等待。接受的含义是自私挖矿者放弃自己的私链，接在公链之后开始挖矿；覆盖表示自私挖矿者发布一条比公链更长的链，覆盖掉现有的公链；竞争代表着自私挖矿者发布一条和公链一样长的链，和公链竞争有效链的地位；等待的含义是不发布私链，继续在私链的基础上进行挖矿。

模型的状态空间由三元组(a,h,fork)组成。该三元组中，参数 a 表示攻击者私链的长度，h 表示公链长度。第三参数 fork 共有三个取值：{不相关, 相关, 竞争中}。“不相关”代表着从这个状态出发，竞争动作是不可行的，意味着上个块是自私挖矿者挖出来的，或者公链长度为 0。“相关”代表着从这个状态出发，竞争动作是可行的，比如上一个块是由诚实挖矿者挖出的。设置“相关”和不相关“两个状态的目的是决定竞争操作是否可行。考虑一种情况：当私链比公链短 1 个区块的时候，此时若自私挖矿者挖出一个区块，使得公链和私链长度一致。这种情况下，自私挖矿者也无法发起有效的竞争操作，因为公链发布的时间早于私链，已被大部分节点所接受，此时即使发布一条和公链一样长的链，也无法与公链进行有效的竞争。“竞争中”表示这个状态前上个动作是竞争；或者上个状态是竞争，动作为等待。设置竞争中这个状态的目的是考虑到私链发布之后部分诚实挖矿者会接在自私挖矿者后面挖矿，因此上个动作会影响下个状

态之后的转移概率，因此必须将上个动作是否是竞争纳入到状态参数中，否则模型的马尔科夫性无法保证。

状态× 动作	状态	概率	回报
$(a, h, \cdot)$，接受	$(1, 0,$不相关$)$	α	$(0, h)$
	$(0, 1,$ 不相关$)$	$1-\alpha$	
$(a, h, \cdot)$，覆盖†	$(a-h, 0,$ 不相关$)$	α	$(h+1, 0)$
	$(a-h-1,1,$相关$)$	$1-\alpha$	
$(a, h,$ 不相关$)$，等待 $\mid (a, h,$ 相关$)$, 等待	$(a+1, h,$ 不相关$)$	α	$(0, 0)$
	$(a, h+1,$ 相关$)$	$1-\alpha$	$(0, 0)$
$(a, h,$ 竞争中$)$，等待 $\mid (a, h,$ 相关$)$, 竞争‡	$(a+1, h,$ 竞争中$)$	α	$(0, 0)$
	$(a-h, 1,$ 不相关$)$	$\gamma(1-\alpha)$	$(h, 0)$
	$(a, h+1,$ 相关$)$	$(1-\gamma)(1-\alpha)$	$(0, 0)$

†仅当 $a > h$时可行 ‡仅当 $a \geq h$ 时可行

表格 1.1：自私挖矿马尔科夫决策模型的状态转移概率及收益

最优自私挖矿策略的马尔科夫决策模型的状态转移概率和收益如表格 1.1 所示。其中，收益的第一个元素表示攻击者的收益，收益的第二个元素表示诚实挖矿者的收益。

1.2.5 最优自私挖矿模型求解及结果展示

用数值法求解马尔科夫决策过程的值需要构造马尔科夫转移矩阵。表 1 中所示的状态可以有无穷多这种，而在实际求解的过程中必须对 α 和 h 的大小作出限制。这个限制被称为最大分叉长度，当 α 或 h 等于最大分叉长度的时候，就不能按照表 1 的转移方式进行转移，而是要强制返回初始状态。这里对强制返回初始状态的收益有两种处理方法：一种是对状态转移矩阵不作处理，即不考虑超过最大分叉长度之后可能获得的收益；另一种方法是将未来可能获得的收益用公式近似之后加入到该步的收益中。前一种处理方法计算出的是收益的下界，后一种处理方法计算出的是收益的上界。设定的最大分叉长度越长，则计算的时间尺度越大，因此约接近实际，上界和下界的差也就越小，趋向于收敛。从收益计算的结果可以看出当算力增加的时候，倾向于等待而不是接受，所以需要设定更大的最大区块分叉长度才能达到与小算力情况下相等的上下界之差。在求解过程中，算力小于 0.4 时我们设最大区块分叉长度为 80，大于等于 0.4 时我们设最大区块分叉长度为 160。另一个需要考虑的问题是自私挖矿的收益是相对收益而非绝对收益，因此需要对目标函数进行处理之后，用二分法求解收益。因

此，求解自私挖矿最优收益需要多次求解马尔科夫决策问题直至误差小于定值，计算时间复杂度远大于求解一个马尔科夫决策问题。

我们用$\gamma = 0.5$的情况下使用MATLAB的MdpToolbox[19]求解出$\alpha = 0.05 \sim 0.45$情况下收益的上限和下限，展示在图1.3中。结果显示，最优自私挖矿策略获得的利润高于原始的自私挖矿策略。通过观察不同算力情况下的最优解可以看出，当算力较小时，最优策略是诚实挖矿；当算力接近0.5时，即使在私链落后于公链1个区块时也不接受公链，而是继续等待，这种策略能获得比原始的自私挖矿策略更高的收益。这种即使略微落后也接受公链的策略也被称为“顽固挖矿”(stubborn mining)[6]。使用马尔科夫决策过程解得的最优策略在小算力情况下不会劣于诚实挖矿，因此可以适用于任何一个矿工，让自私挖矿这种攻击策略普适性更强。

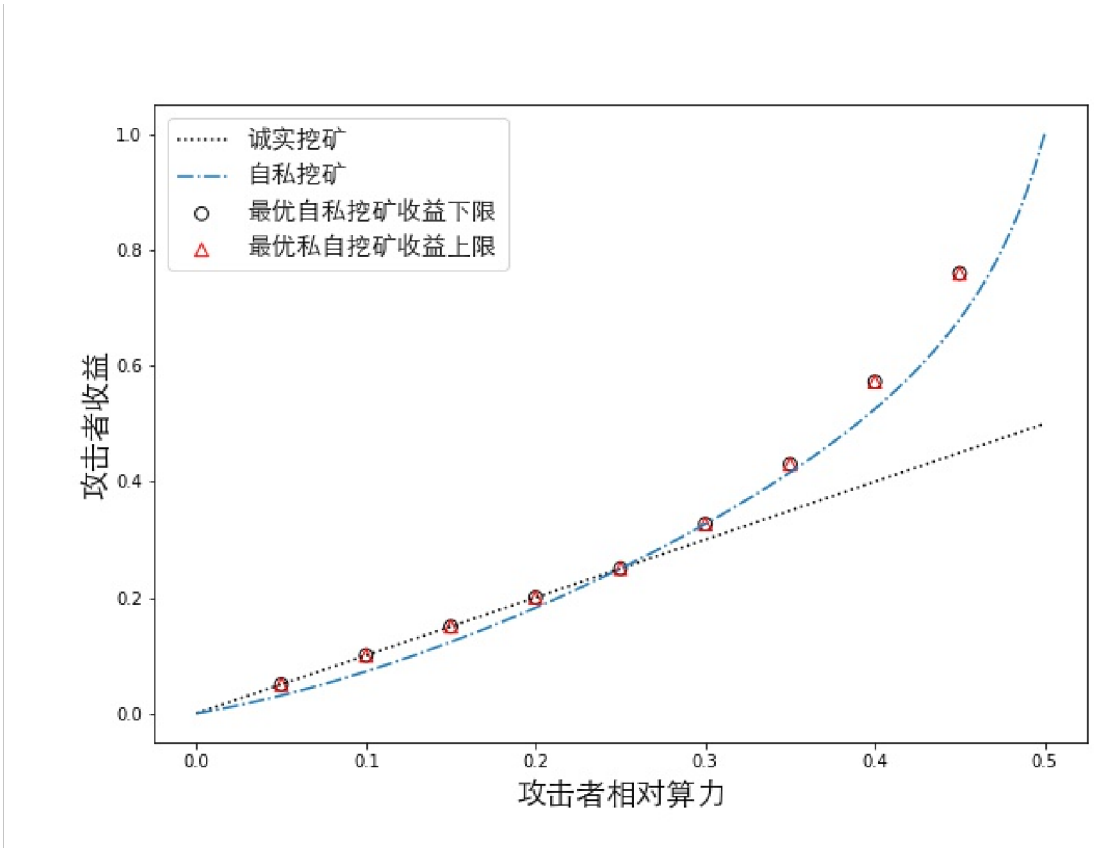

图1.3：最优自私挖矿和自私挖矿收益对比

1.2.6 区块截留攻击原理

区块链截留攻击最早由[9]提出。它的策略是派出一些算力去其它矿池挖矿，只提供部分工作证明但不提供完全工作证明，当挖出有效区块的时候会立即丢弃这个区块。这些被派到其它矿池挖矿的算力被称为间谍算力。这些间谍算力可以通过部分工作证明获得回报；同时由于间谍会丢弃挖出的有效区块，即降低了全网算力，自留算力获得的报酬也增加了。如果区块截留攻击者只使用一个账号进行区块截留攻击，那么矿

池经理可以通过对比每个账号提交的部分工作证明和完全工作证明而鉴别出攻击者；但是由于区块链是匿名的系统，任何一个参与者都可以获得任意多个账号，所以当攻击者不断切换账号时这种攻击就变得非常隐蔽。

1.2.7 区块链截留攻击收益分析

假设攻击者的总算力为 α，被攻击的矿池算力为 β，派出的间谍算力占攻击者总算力的比例为 k，即派出的间谍算力为 kα。区块链截留攻击的收益来自于两方面：派出的间谍算力所获得的收益和自留算力所获得的收益。具体计算结果见附录 1。当派出算力比例分别为 20%，50%和 80%时，获得的收益随攻击者算力变化如图 1.4 所示。我们发现，区块截留攻击的最优派出算力比例 k 的最优值随攻击者总算力的变化而变化，因此，我们用数值方法计算出了不同派出算力下的最优派出算例比例k，同时求出最大收益(图 1.5)。

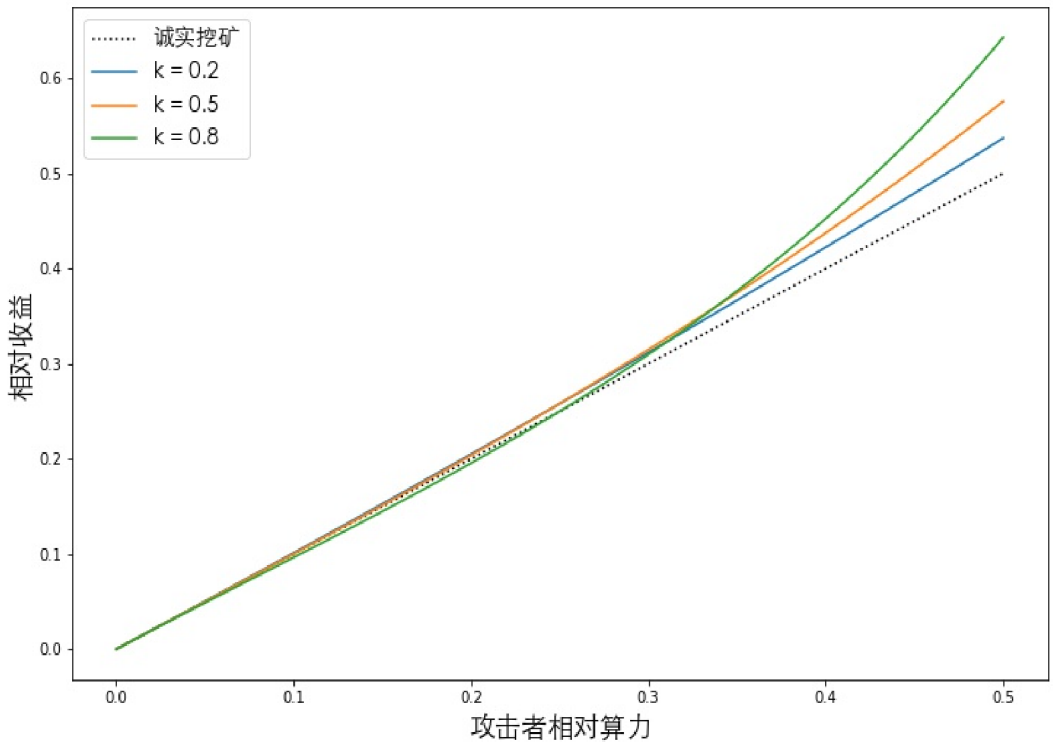

图 1.4：区块截留攻击收益

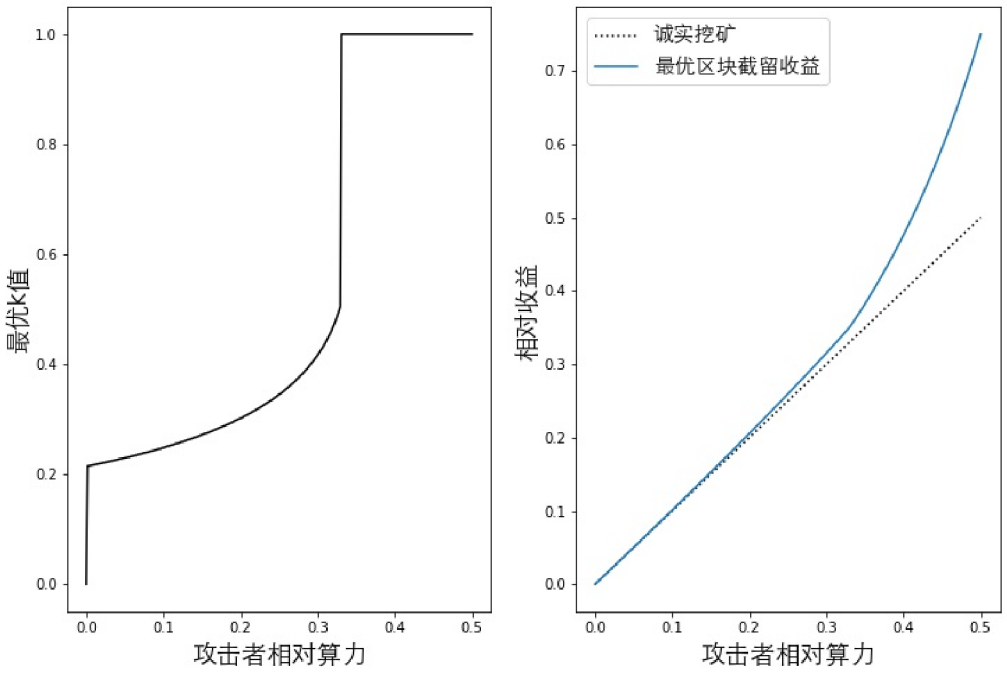

图 1.5：区块截留攻击最优派出算力及最大收益

1.3 自私挖矿和区块截留攻击对比

1.3.1 收益比较

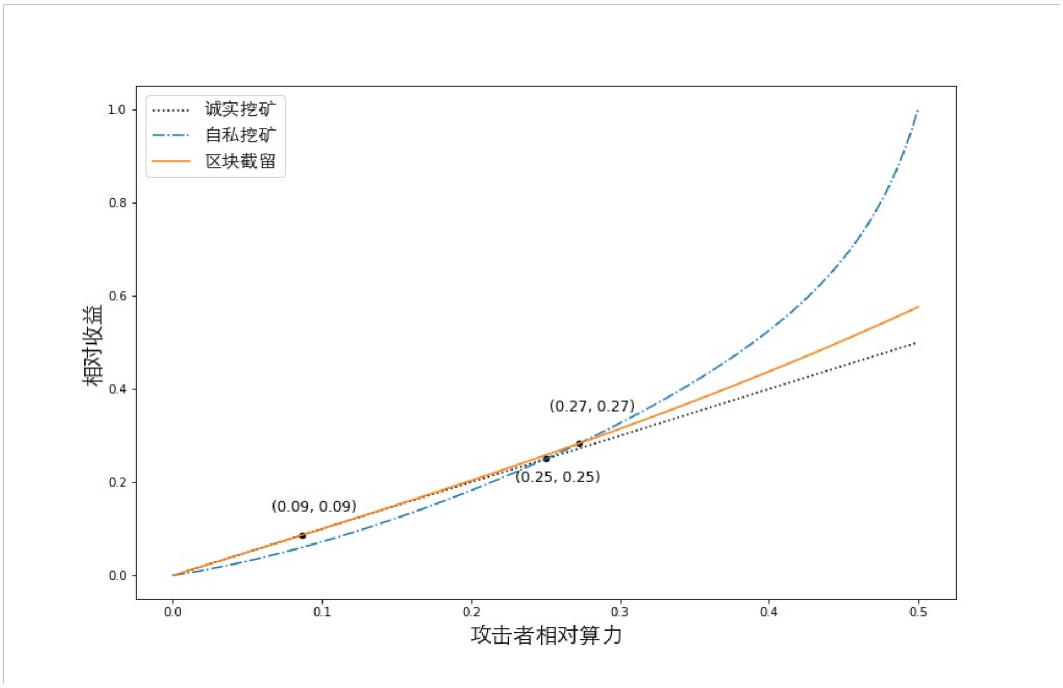

图 1.6：两种攻击及诚实挖矿的收益对比

图 1.6 中的曲线展示了 3 种挖矿方式的收益，点表示收益曲线的交点。网络参数 $\gamma = 0.5$，派出算力比例 $k = 0.5$，被攻击矿池算力 $\beta = 0.3$。由此可以看出，当攻击者的算力占全网算力的 0.09 以下时，诚实挖矿收益最高；当攻击者算力占全网算力的 0.09至0.27 时，区块链截留攻击收益最高；当攻击者算力占全网算力的 0.27 以上时，自私挖矿收益最高。

1.3.2自私挖矿和区块截留攻击的本质

自私挖矿和区块截留攻击（以及几乎所有的对区块链规则的攻击）的本质都是通过侵占诚实挖矿者的收益达到的。因为比特币系统会通过难度调整使得平均每 10 分钟产生一个块，所以单位时间内所有参与者的收益总和是一定的，所以自私挖矿和区块截留具体来说是对难度调整的攻击[18]。在这样一个零和博弈的系统中，对手的损失就是攻击者的收益。无论是自私挖矿攻击，还是区块截留攻击，在攻击开始时都减少了比特币系统中产生块的数量。它们没有使攻击者获得更多的区块，但是使得区块链中的被攻击者挖出更少的（有效）块，从而增加了自己挖出块的占比。这两种攻击都是有代价的，所以攻击者自己挖出的有效区块的数量比诚实挖矿时也有所减少。但由于比特币系统的零和性质，只要攻击者挖出的有效区块占所有有效区块的比重增加，攻击者就能获得超额收益。自私挖矿攻击还会导致区块链系统中的分叉增多，自私挖矿者发布了更长链覆盖了诚实挖矿者的公链之后，本来已经被打包加入区块链的交易可能因此而无效，这会让区块链交易的安全性降低，所以自私挖矿攻击的受害者不仅仅是诚实挖矿的矿工，而是整个区块链系统。

第二章 联合两种攻击方法

当一个攻击者将两种攻击混合使用的时候，在某些特定的条件下可能获得比单一攻击更多的收益。一种受到较多关注的混合攻击是同时使用自私挖矿和区块截留攻击，以下简称混合攻击。[8]提出了一种区块截留攻击的同时自私挖矿的攻击方法，下面介绍它的攻击策略和收益。

2.1 混合攻击策略

攻击者派出部分算力到其它矿池进行区块截留攻击，同时自己进行自私挖矿。定义该攻击策略的参数如下：

参数	意义
α	攻击者总算力
k	攻击者派出的间谍算力比例
β	被攻击矿池的算力

表格 2.1：混合攻击参数定义

由定义可知，$k\alpha$为派出的间谍算力的总数，$(1-k)\alpha$ 为攻击者用来自私挖矿的算力，$1-\alpha-\beta$为全网其它算力。γ为网络参数，表示的是全网基于攻击者挖出的块挖矿的比例，这和自私挖矿模型中的定义是一致的。

2.2 混合攻击收益

攻击者的收益分为两部分：派出到其它矿池的算力所产生的收益和自己自私挖矿所产生的收益。这里，自私挖矿收益的计算和原始的自私挖矿收益一致，仅需要改变部分参数；区块截留的收益计算和单独区块截留攻击的计算也是相似的。

区块截留攻击会截留一部分被挖出来的块，从而减少全网有效算力，所以攻击时全网有效算力是$1-k\alpha$。其中，有效的诚实算力为$1-\alpha$; 有效的自私挖矿算力为$(1-k)\alpha$。混合攻击的收益分为区块截留攻击和自私挖矿攻击收益，具体计算过程见附录 1。

混合攻击收益展示如图 4 左侧。这是按照[7]的计算方法复现的，其中被攻击矿池的算力被作者设为(1-攻击者算力)，因为攻击者算力小于 0.5，所以此处的被攻击矿池的算力大于 0.5。然而，在实际情况下不会存在一个矿池算力占全网算力超过 0.5，因为如果存在这样的矿池，比特币的安全就已经不复存在了。

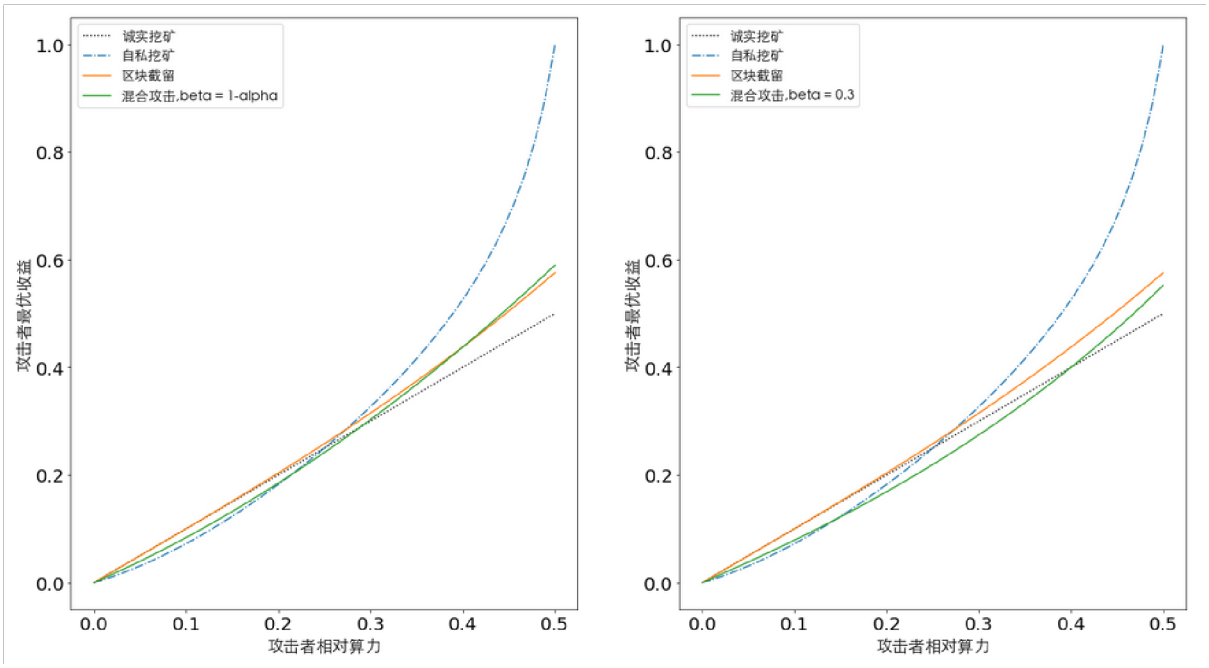

图 4: 混合攻击与其它攻击方式的收益对比

因此，我们采用了更加合理的假设，假设攻击者算力为固定值 0.3，再计算出混合攻击的收益，展示在图 2 的右侧。对比图 2 中的两张图，我们发现当被攻击者的算力值固定为 0.3 的时候混合攻击的表现会更差。更重要的是，无论采取何种假设，虽然在算力较小的情况下混合攻击收益大于自私挖矿攻击，但混合攻击收益都没有超过分段单独使用区块截留攻击和自私挖矿攻击。所以，对单个矿池进行混合攻击不是一个好策略。

第三章 最优混合攻击策略

3.1 最优化派出算力

派出算力的比例 k 是可变的，但[7]中的模型直接假设派出算力和自私挖矿算力是相等的。因此，一个最直观的优化方法是算出攻击者在不同算力情况下的最优派出算力比例 k，从而求得混合攻击的最优收益。图 5 中的红色线表示最优混合攻击收益。可以看出，当算力较小时，最优方法是所有算力都派出为最优；当算力较大时，最优方法是所有算力都进行自私挖矿。鉴于区块截留在算力小时占优，自私挖矿在算力大时占优，这种最优算力分布很好理解。不幸的是，由于我们已经知道混合攻击相严格劣于分段使用区块截留攻击和自私挖矿策略，所以最优化派出算力的混合攻击也的收益无法大于分段使用区块截留攻击和自私挖矿策略。因此，想要获得更好的算法，必须从攻击策略出发对混合攻击方法作出本质性的完善。

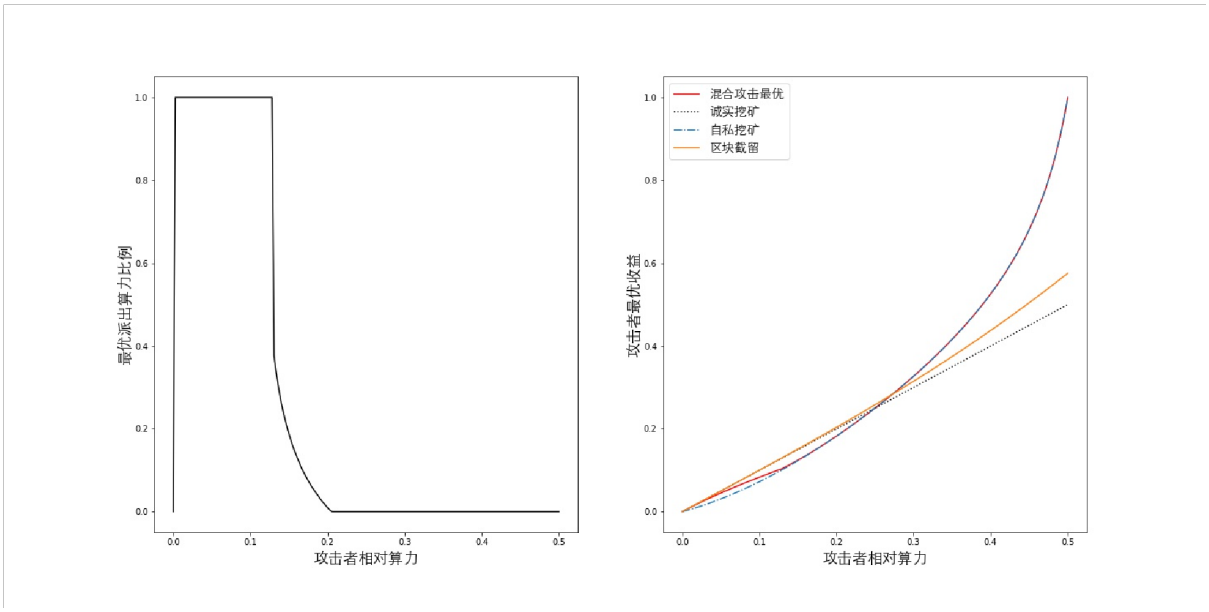

图 3.1: 最优化派出算力比例的混合攻击与其它攻击方式的收益对比

3.2 有撤回的混合攻击马尔科夫模型

3.2.1 模型概述

我们通过研究发现，在用自留算力自私挖矿时，有一种方法有提升攻击的收益率的潜力：增加撤回间谍算力的选择。直观来看，如果在自私挖矿的时候能够实时撤回间谍算力，那么就可以在区块竞争的关键时刻增加胜算，提高收益；若私链落后于公链，此时正是自私挖矿攻击亏损的时刻，也不妨派出一部分间谍算力进行区块截留攻击，通过分享诚实矿工的收益获得更高的收益。

在马尔科夫决策模型中，动作空间必须是离散的，所以不能用来求解 k 的最优值。所以，我们设 k 为定值，同时在马尔科夫决策模型的状态空间中加入“派出或不派出间谍算力”动作，用来表示派出或者收回间谍算力。

3.2.2 模型假设

本模型采用了区块链攻击研究方法中常用的假设，包括：

1. 只考虑挖矿收益，不考虑交易费收益。
2. 收益用相对收益表示，相对收益的定义是攻击者收益占比特币系统中所有参与者收益的比例。攻击者的算力也用攻击者占全网算力的比例表示。
3. 攻击者攻击所矿池的收益分配规则是：矿工的收益与他提交的“部分工作证明”的数量成正比。
4. 攻击者可以在系统内一个区块生成之后瞬时加入或者退出一个矿池，并且加入和退出矿池没有成本。
5. 模型参数定义与 2.1 中一致。

状态× 动作	状态	概率	回报
$(a, h, s, \cdot)$，接受+不派出	$(1, 0, 0,$ 不相关$)$	α	$(\frac{k\alpha}{1-\alpha}\cdot\frac{s}{a+h}h, (1-\frac{k\alpha}{1-\alpha}\cdot\frac{s}{a+h})h)$
	$(0, 1, 0,$ 不相关$)$	$1-\alpha$	
$(a, h, s, \cdot)$，覆盖+不派出†	$(a-h,\ 0,\ 0,$ 不相关$)$	α	$(h+1, 0)$
	$(a-h-1, 1, 0,$ 相关$)$	$1-\alpha$	
$(a, h, s,$ 不相关$)$，等待+不派出 | $(a, h, s,$ 相关$)$, 等待+不派出	$(a+1, h,\ s,$ 不相关$)$	α	$(0, 0)$
	$(a, h+1, s,$ 相关$)$	$1-\alpha$	$(0, 0)$
$(a, h, s,$ 竞争中$)$，等待+不派出 | $(a, h, s,$ 相关$)$, 竞争+不派出‡	$(a+1, h, s,$ 竞争中$)$	α	$(0, 0)$
	$(a-h, 1, 0,$ 不相关$)$	$\gamma(1-\alpha)$	$(h, 0)$
	$(a, h+1, s,$ 相关$)$	$(1-\gamma)(1-\alpha)$	$(0, 0)$
$(a, h, s, \cdot)$，接受+派出	$(1, 0, 1,$ 不相关$)$	$\frac{(1-k)\alpha}{1-k\alpha}$	$(\frac{k\alpha}{1-\alpha}\cdot\frac{s}{a+h}h, (1-\frac{k\alpha}{1-\alpha}\cdot\frac{s}{a+h})h)$
	$(0, 1, 1,$ 不相关$)$	$\frac{1-\alpha}{1-k\alpha}$	
$(a, h, s, \cdot)$，覆盖+派出†	$(a-h, 0, 1,$ 不相关$)$	$\frac{(1-k)\alpha}{1-k\alpha}$	$(h+1, 0)$
	$(a-h-1, 1, 1,$ 相关$)$	$\frac{1-\alpha}{1-k\alpha}$	
$(a, h, s,$ 不相关$)$，等待+派出 | $(a, h, s,$ 相关$)$, 等待+派出	$(a+1, h, s+1,$不相关$)$	$\frac{(1-k)\alpha}{1-k\alpha}$	$(0, 0)$
	$(a, h+1, s+1,$相关$)$	$\frac{1-\alpha}{1-k\alpha}$	$(0, 0)$
$(a, h, s,$ 竞争中$)$，等待 | $(a, h, s,$ 相关$)$, 竞争+派出‡	$(a+1, h, s+1,$ 竞争中$)$	$\frac{(1-k)\alpha}{1-k\alpha}$	$(0, 0)$
	$(a-h, 1, 1,$ 不相关$)$	$\gamma\frac{1-\alpha}{1-k\alpha}$	$(h, 0)$
	$(a, h+1, s+1,$ 相关$)$	$(1-\gamma)\frac{1-\alpha}{1-k\alpha}$	$(0, 0)$

†仅当 $a > h$时可行 ‡仅当 $a \geq h$ 时可行

表格 3.1：混合攻击策略马尔科夫决策模型的状态转移概率及收益

3.2.3 动作、状态转移及收益

与 2.1.3 中最优自私挖矿的马尔科夫决策过程相比，与私自挖矿相关的问题的结构并未改变，因此可以沿用其关于自私挖矿的决策模型。但是混合攻击模型的马尔科夫决策过程需要多做一个决策：本次挖矿是否派出间谍算力。因此，我们将原模型的 4 个动作与”派出“和”不派出“相结合，决策过程的动作空间的元素增加了一倍，共有 8 个动作。如果派出了间谍算力，那么攻击者会按比例拿走诚实挖矿者的一部分收益，导致收益产生变化；同时，转移概率也因为算力的变换而产生变化。为了记录在本轮挖矿过程中究竟有多少次派出了间谍算力，我们在状态参数中添加一个参数 s，代表着本轮挖矿过程中派出间谍算力的次数。这个状态参数会被用来计算攻击者通过区块截留攻击会拿走多少比例的诚实挖矿收益。

带有撤回的马尔科夫决策模型的动作、状态转移函数及收益如表格 3.1。

3.2.4 模型求解方法及结果

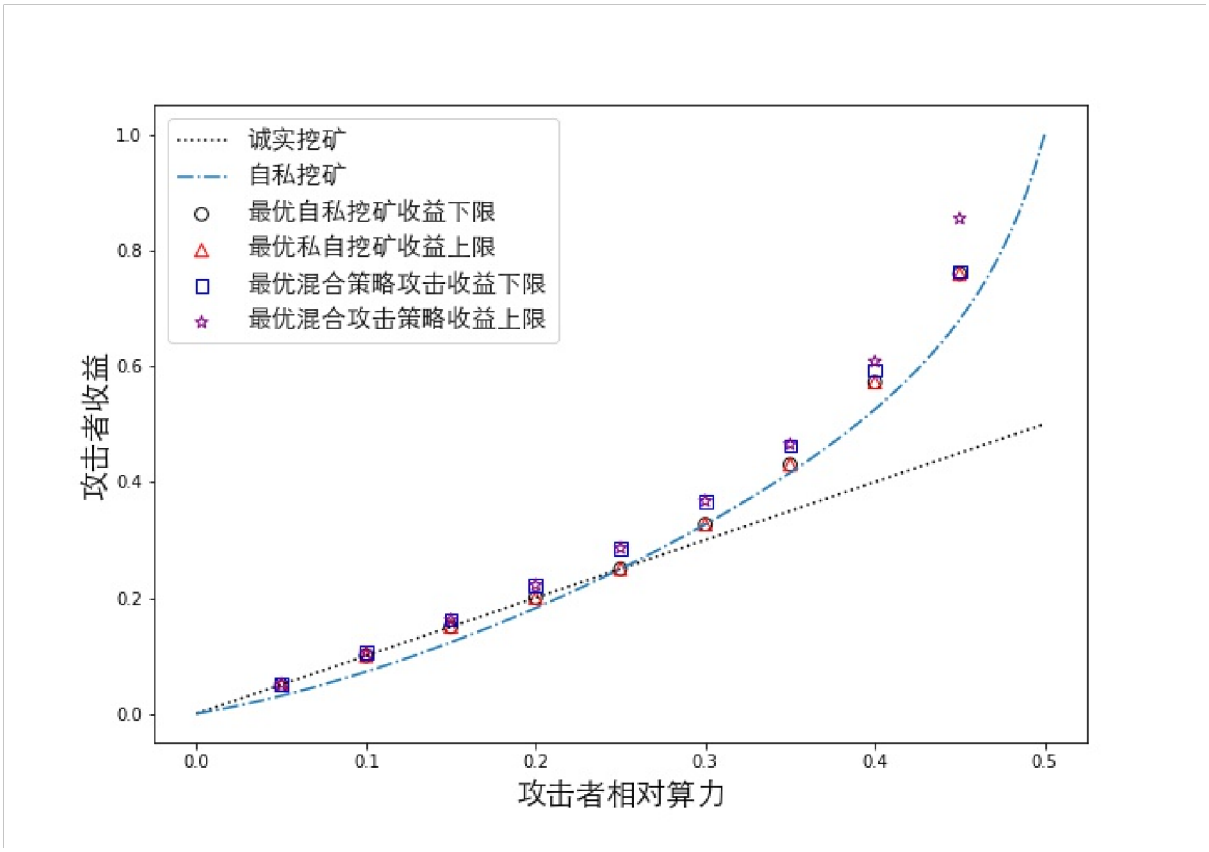

图 3.2: 最优混合攻击收益与最优自私挖矿攻击收益对比

由于目标函数的形式并未产生变化，我们在修改了状态转移矩阵和收益矩阵之后可以直接用2.1.4 中的求解方法求解模型的最优解。需要注意的是，状态 s 的最大值是 2 倍的最大分叉区块长度，因为一轮中挖出块的次数最多是 2 倍的最大分叉区块长度，而如果每次都派出间谍算力，s 的最大值即为 2 倍的最大分叉区块长度。同时，由于增加了一个状态参数，使得状态个数大为增加，为了保证能在合理时间内求得结果，当攻击者算力小于 0.3 的时候，最大分叉区块长度被设为 10；当攻击者算力大于等于 0.3 的时候，最大分叉区块长度被设为 20。求得的最优混合攻击收益和自私挖矿收益的对比展示在图 3.2，具体数值展示对比在表 3。求解时，网络参数 $\gamma = 0.5$，派出算力比例 $k = 0.5$。

攻击者算力	最优自私挖矿收益下限	最优混合攻击收益下限	最优自私挖矿收益上限	最优混合攻击收益上限
0.05	0.0500	0.0513	0.0500	0.0513
0.10	0.1000	0.1053	0.1000	0.1053
0.15	0.1500	0.1622	0.1500	0.1622
0.20	0.2000	0.2222	0.2000	0.2222
0.25	0.2500	0.2857	0.2500	0.2857
0.30	0.3269	0.3663	0.3269	0.3670
0.35	0.4302	0.4634	0.4302	0.4651
0.40	0.5725	0.5934	0.5725	0.6081
0.45	0.7596	0.7637	0.7596	0.8637

表 3.2: 最优混合攻击收益与最优自私挖矿攻击收益对比

3.2.5 结果分析

从已经计算出的数据点来看，混合最优攻击优于自私挖矿、诚实挖矿和区块截留攻击三种攻击的任意一种。通过观察求解所得的最优挖矿策略，我们发现了如下 2 个规律：

1. 当参数 s 较小时，倾向于采取派出策略；当参数 s 较大时，倾向于采取“不派出”策略。我们认为，这是因为在一轮攻击中派出间谍算力的次数有最优值，当累计派出次数较大时就倾向于不再派出间谍算力。
2. 当私链长度领先于或等于公链长度时，倾向于采取不派出策略；当公链长度长于私链长度时，倾向于采取派出策略。我们认为，当私链领先于公链时是自私挖矿的关键时刻，因为此时自私挖矿者在诚实挖矿者不知道的区块的基础上挖矿，可以赢得时间，获取更多利润。而当公链长度长于私链长度时，是自私挖矿策略亏钱的时刻，这时如果派出间谍算力，就可以弥补自私挖矿的亏损，提升总体收益。

第四章 讨论及结论

4.1 混合攻击马尔科夫模型启示

混合攻击的马尔科夫决策模型本质上是将自私挖矿、诚实挖矿和区块截留攻击三种方法中进行实时算力分配。因此，求得的最优策略所产生的收益在任何情况下不会劣于单独使用三种方法中的任意一种。但是如果只是单纯采取分配算力在不同攻击方法上的策略，则有可能会得到一个劣于单独使用三种攻击方法的策略（如 3.1 所示）。因此，在混合攻击模型的求解时使用马尔科夫决策过程来动态地结合几种攻击方法，从而创造出新的攻击策略是很有优势的。不过，由于策略空间元素和状态空间元素的增加，混合攻击模型的求解复杂度会随状态参数个数呈指数型上升，遭遇维度爆炸的困难。因此，马尔科夫决策模型是一种高计算复杂度的求解最优决策的方法。

同时，我们发现，多种攻击方法相结合能够使区块链攻击获利更多，从而让区块链的安全受到进一步的损害。所以在考虑区块链安全性的时候，有必要将各种攻击的混合纳入考虑范畴。

4.2 不足及未来工作

该模型利用了马尔科夫决策模型，所以没有最优化派出的间谍算力的比例，这需要用连续动作空间的强化学习来实现。同时，在现实中矿池的加入和退出不能瞬时完成，在这里我们也没有考虑加入矿池和退出矿池的规则限制以及时间成本，也没有考虑多种矿池收益分配原则。所以，未来的工作方向可以是将矿池的加入退出机制和多种矿池收益分配机制考虑到模型中，让模型更加符合实际情况。

4.3 结论

本文使用马尔科夫决策方法，结合自私挖矿和区块截留攻击，产生了一种新的对区块链协议的攻击方法，对攻击效果有明显提升，使得攻击者可以获得超额利润。本文的发现为区块链协议的设计提供了参考，有助于提升区块链的安全性。

参考文献

[1] Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system." Consulted,1(2012):28, 2008.

[2] Foley, Sean, Jonathan R. Karlsen, and Tālis J. Putniņs. "Sex, Drugs, and Bitcoin: HowMuch Illegal Activity Is Financed Through Cryptocurrencies?." Review of Financial Studies 32.5 (2019): 1798-1853.

[3] Lin, Jian Hong , et al. "Lightning Network: a second path towards centralisation of the Bitcoin economy." (2020).

[4] Eyal, Ittay, and Emin Gun Sirer. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable."financial cryptography (2014): 436-454.

[5] Sapirshtein, Ayelet, Yonatan Sompolinsky, and Aviv Zohar. "Optimal Selfish MiningStrategies in Bitcoin." financial cryptography (2016): 515-532.

[6] Nayak, Kartik , et al. "Stubborn Mining: Generalizing Selfish Mining and Combiningwith an Eclipse Attack." IEEE European Symposium on Security & Privacy IEEE, 2016.

[7] Dong, Xuewen, et al. "SelfHolding: A Combined Attack Model using Selfish Mining with Block Withholding Attack." Computers & Security 87(2019):101584.

[8] Kwon, Yujin , et al. "Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin." the 2017 ACM SIGSAC Conference ACM, 2017.

[9] Courtois, Nicolas T , and L. Bahack . "On Subversive Miner Strategies and BlockWithholding Attack in Bitcoin Digital Currency." Eprint Arxiv (2014).

[10] Wang, Taotao , S. C. Liew , and S. Zhang . "When Blockchain Meets AI: Optimal Mining Strategy Achieved By Machine Learning." (2019).

[11] Wenjuan, et al. "Intelligent Network Information Security Game Model Based on Blockchain Technology." 2018.

[12] Zhang, Ren, and Bart Preneel. "Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols' Security." *ieee symposium on security and privacy* (2019): 175-192.

[13] Miles Carlsten, et al. "On the Instability of Bitcoin Without the Block Reward." *Acm Sigsac Conference on Computer & Communications Security* ACM, 2016.

[14] Heilman, Ethan. "One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner (Poster Abstract)." *financial cryptography* (2014): 161-162.

[15] Hou, Charlie, et al. "SquirRL: Automating Attack Discovery on Blockchain Incentive Mechanisms with Deep Reinforcement Learning.." *arXiv: Cryptography and Security* (2019).

[16] Xiao, Yang, et al. "Modeling the Impact of Network Connectivity on Consensus Security of Proof-of-Work Blockchain." arXiv: Cryptography and Security (2020).

[17] Michael Kaiser. “Simulation and analysis of the selfish-mining attack on Bitcoin” (2016)

[18] Grunspan, Cyril , and Pérez-Marco, Ricardo. "On profitability of selfish mining." (2018).

[19] Chadès, Iadine, et al. "MDPtoolbox: a multi-platform toolbox to solve stochastic dynamic programming problems." *Ecography* 37.9(2014):916–920.

[20] Gervais, Arthur , et al. "On the Security and Performance of Proof of Work Blockchains." *the 2016 ACM SIGSAC Conference* ACM, 2016.

附录 1

1. 区块截留攻击收益求解:

假设攻击者的总算力为 α，被攻击的矿池算力为 β，派出的间谍算力占攻击者总算力的比例为 k，即派出的间谍算力为 $k\alpha$。区块链截留攻击的收益来自于两方面：派出的间谍算力所获得的收益和自留算力所获得的收益。派出算力的收益为$\frac{k\alpha}{k\alpha+\beta}\cdot\frac{\beta}{1-k\alpha}$, 自留算力的收益为$\frac{(1-k)\alpha}{1-k\alpha}$。总算力为自留算力收益加上派出算力收益，为$\frac{k\alpha}{k\alpha+\beta}\cdot\frac{\beta}{1-k\alpha}+\frac{(1-k)\alpha}{1-k\alpha}$。

2. 混合攻击收益求解:

区块截留攻击会截留一部分被挖出来的块，从而减少全网有效算力，所以攻击时全网有效算力是$1-k\alpha$。其中，有效的诚实算力为$1-\alpha$; 有效的自私挖矿算力为$(1-k)\alpha$。

派出算力的收益：派出算力会提供 PPOW 按比例获得矿池的收益，这部分算力的收益应为$\frac{k\alpha}{k\alpha+\beta}\cdot\frac{\beta}{1-k\alpha}\cdot R_h$。其中，$R_h$为全网所有诚实矿工所获得的收益。$R_h=1-R_s$，$R_s$即自私挖矿算力获得的收益，在下面给出。

自私挖矿的收益：令自私挖矿算力占全网(有效)算力的比重为$w=\frac{(1-k)\alpha}{1-k\alpha}$。将算力比重带入到自私挖矿收益求得：$R_s=\frac{w(1-w)^2(4w+\gamma(1-2w))-w^3}{1-w(1+(2-w)w)}$

所以，攻击者的总收益为：$R_a=wR_h+R_s$

致谢

感谢徐跃东老师对我毕业论文的指导，也同时感谢复旦大学为我提供优质的学术资源。日月光华，旦复旦兮，在 2020 这个特殊的年份中，我没有机会在母校度过完整的毕业季，但是我在复旦学习的朝朝暮暮已经成为我珍贵的一部分。

指导教师对论文独立性的审查意见：

指导教师应依据《学位论文作假行为处理办法》第五条的规定对毕业论文撰写人进行学术道德与学术规范教育，并在此基础上对其撰写论文进行指导。

☐ 本人经过尽职审查，未发现毕业论文撰写人有学位论文作假行为。本人认为毕业论文撰写人独立完成了本毕业论文。

☐ 本人经过尽职审查，发现毕业论文撰写人有如下学位论文作假行为：

指导教师签名： **日期： 20 年 月 日**

指导教师评语：

周璐鹿同学勤奋刻苦，学习态度端正，在毕设期间积极与导师和课题组成员讨论，积极汇报论文工作进展，展现出良好的科研素养。本论文着眼于区块链自私挖矿攻击的理论建模、仿真、和攻击策略设计，是目前区块链共识机制的前沿问题。周璐鹿同学复现了现有基于马尔科夫决策的最优自私攻击策略，并基于前任工作，设计自私挖矿和 witholding联合攻击的马尔科夫决策模型，具有良好的创新性。毕业论文的结构安排合理，书写符合规范，内容比较详实，研究内容具有较好的创新性，仿真结果比较可靠。

签名：

2020 年 6月 25日

答辩委员会（小组）评语：

签名：

20 年 月 日

学分：		成绩：	

备注：