关于比特币中 BWH 攻击的一个注记

程恒喆[1,2], 冯秀涛[1]

[1] 中国科学院数学与系统科学研究院 数学机械化重点实验室, 北京 中国 100190
[2] 中国科学院大学, 北京 中国 100190

摘要 比特币是当前信息安全应用研究领域的热点问题之一. 在比特币所采用的 PoW 共识协议中, 挖矿具有重要作用. 在现实生活中, 矿工为获得更多的奖励, 往往聚集成矿池, 以达到在挖矿中获取更高算力进而获取更多区块奖励的目的. 针对比特币矿池, Meni Rosenfeld 首次提出了一种称为 BWH 攻击的攻击方式, Loi Luu 等人进一步从理论上证明了相对于诚实挖矿, 攻击者通过实施 BWH 攻击可以获得更高的收益. 在本文中, 我们分析了 BWH 攻击的理论基础, 发现 Loi Luu 等人关于 BWH 攻击的理论分析中存在的一个错误, 即 Loi Luu 等人忽略了整体算力改变对系统产生区块所需时间的影响, 从而导致其所对比的关于攻击者实施 BWH 攻击所获得的收益与不实施攻击所获得的收益, 实际上是在不同时间长度下的收益对比. 显然这种对比缺乏合理性. 在相同时间长度下, 我们进一步讨论了攻击者实施 BWH 攻击与不实施攻击所获得的收益对比, 得到了与 Loi Luu 等人完全相反的结论, 即相对诚实挖矿来说, 攻击者实施 BWH 攻击反而获得了相对较少的收益. 因此攻击者缺乏实施 BWH 攻击的动机, 除非其纯粹出于破坏矿池的目的而采用 BWH 攻击.

关键词 比特币; 区块链; 矿池; BWH 攻击
中图法分类号 TP309.7 **DOI 号** 10.19363/j.cnki.cn10-1380/tn.2018.05.05

A Note on Block Withholding Attack on Bitcoin

CHENG Hengzhe[1,2], FENG Xiutao[1]

[1] Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
[2] University of Chinese Academy of Sciences, Beijing 100190, China

Abstract Bitcoin is one of the hot issues in the application of information security. Mining plays an important role in the PoW protocol which is used in Bitcoin. In the real world, miners tend to gather into mining pools to get higher hash power and more rewards. Against mining pools, Meni Rosenfeld first proposed an attack called BWH attack, which is a kind of attack on Bitcoin pools. Loi Luu et al. gave a theoretical analysis of BWH attack and proved that the attacker could gain more rewards by implementing BWH attack than that got by mining honestly. In this paper, we analyze the theoretical basis of BWH attack and find a flaw in Loi Luu et al.'s theoretical analysis of BWH attack. Namely, Loi Luu et al. ignored the effect of changing hash power on the amount of time required for Bitcoin systems to generate a block. So Loi Luu et al. indeed compared the revenue from performing BWH attack and non-implementation attack over different length of time, which is clearly not justified. At the same length of time, we further discuss the revenue acquired by attacker in implementing BWH attacks versus non-implementation, and have an opposite conclusion to Loi Luu et al, that is, comparing with mining honestly, the attacker receives less revenue by implementing BWH attack. Therefore, the attacker lacks the motivation to implement BWH attack unless they use BWH attack solely for the purpose of damaging the mining pool.

Key words bitcoin; blockchain; mining pools; BWH Attack

1 引言

比特币[1]是世界上第一个完全实现了去中心化的密码货币。在比特币发明之后, 迅速出现了多种密码货币, 例如莱特币[2]、素数币[3]等等, 而比特币无疑是最为成功, 也最为吸引研究人员关注的一种密

通讯作者: 冯秀涛, 博士, 副研究员, Email: fengxt@amss.ac.cn。
本课题得到国家自然科学基金项目(No.11688101)以及北京太一云科技有限公司资助。
收稿日期: 2018-02-16; 修改日期: 2018-04-28; 定稿日期: 2018-05-02

码货币。比特币的出现直接导致了区块链技术的产生。区块链技术本质上是一种分布式账本的维护技术[4]。为维护账本的完整性和正确性, 比特币系统要求矿工通过不断地求解密码学难题生成工作量证明(Proof of Work, 简写为 PoW), 并将包含其工作量证明的区块写入到区块链上。同时, 比特币系统为第一个生成正确的工作量证明的矿工给予一定的比特币奖励, 以刺激矿工不断挖矿, 进而实现分布式账本的维护。

在实际中, 由于单个矿工的算力较弱, 为获得更高收益, 矿工往往聚集起来形成一个称为矿池的整体参与挖矿。在具体挖矿过程中, 当一个矿池挖到合法区块后, 系统会给予该矿池一定的比特币奖励。随后矿池再根据一定规则对内部矿工进行奖励分配。

2011 年 Meni Rosenfeld 针对比特币矿池提出了一种 BWH(Block Withholding)攻击[5]。在该攻击中, 攻击者虽然参与到某个矿池中进行挖矿, 但是当其找到合法区块时却并不将其提交给该矿池, 而是直接放弃该区块。这使得矿池损失了该区块中包含的比特币奖励, 即攻击者对矿池的挖矿没有作出贡献. 当该矿池中其他诚实矿工挖到合法区块后, 攻击者却依然可以获得矿池分配的比特币奖励。在这里需要注意的是, Hal Finney 提出了另外一种形式的 BWH 攻击, 即芬妮攻击, 它是双花攻击中的一种变体。但这种攻击不是本文研究的重点, 感兴趣的读者, 请参考文献[6]。

2015 年 Loi Luu 等人从理论上进一步证明了攻击者通过实施 BWH 攻击可以获得高于诚实挖矿所能获得的收益, 从而得出攻击者有动机实施 BWH 攻击的结论[7]。在本文中, 我们研究了 BWH 攻击, 发现 Loi Luu 等人关于攻击者实施 BWH 攻击与不实施 BWH 攻击时获得的收益分析, 实质上是在不同时间长度下所获收益的对比。显然这种对比是不合理的, 由此得到的结论同样缺乏合理性。在相同时间长度下, 我们进一步讨论了攻击者实施 BWH 攻击与不实施攻击所获得的收益对比, 得到了与 Loi Luu 等人完全相反的结论, 即相对诚实挖矿来说, 攻击者实施 BWH 攻击反而获得了相对较少的收益。

本文余下章节安排如下: 第 2 节介绍了与 BWH 攻击相关的工作; 第 3 节为预备知识; 第 4 节指出 Loi Luu 等人分析中存在的错误, 并进一步给出了我们的具体分析。最后第 5 节总结。

2 相关工作

比特币安全性是人们普遍关注的热点问题之一。现有研究表明比特币系统会受到多种不同攻击的影响。Ghassan O. Karame 等人[8]给出了一种快速支付情形下的双花攻击。Arthur Gervais 等人[9]进一步指出攻击者可以通过干预比特币交易和区块数据在 P2P 网络中的传播实现双花攻击。Juan Garay 等人[10]在比特币系统中挖矿难度是固定不变的假设下提出了比特币的骨架协议并对之进行了安全性分析。随后他们进一步考虑了挖矿难度不断变化情况下的比特币骨架协议[11]。Ittay Eyal 等人[12]给出了一种称为自私挖矿的攻击策略, 并且证明了比特币系统的奖励机制不具有激励相容性。Ayelet Sapirshtein 等人[13]在 Ittay Eyal 等人工作的基础上给出了最优的自私挖矿策略。Kartik Nayak 等人[14]给出了一种称为顽固挖矿(Stubborn mining)的攻击策略, 并将与 Eclipse 攻击[15]相结合, 进一步加强了自私挖矿攻击。我们在 Ittay Eyal 等人工作的基础上给出了脚本机制下的自私挖矿攻击[16]。Meni Rosenfeld 首次提出了 BWH (Block Withholding)攻击。一个称为“Eligius”的矿池曾于 2014 年遭受了 BWH 攻击, 该攻击导致“Eligius”矿池损失了 300BTC(约 350 万美元)[17]。Loi Luu 等人[7]提出一种被称为“算力分离游戏”(power splitting game)的模型, 并通过对比攻击者实施 BWH 攻击所获得的收益与不实施 BWH 攻击所获得的收益, 得出攻击者有动机实施 BWH 攻击的结论。Ittay Eyal 给出了两个矿池之间实施 BWH 攻击时的博弈分析[18]。Ittay Eyal 的工作表明该博弈导致了类似于囚徒困境的矿工困境的产生, 但是在纳什均衡下攻击双方为双输的局面。Yujin Kwon 等人[19]基于 BWH 攻击, 并结合自私挖矿攻击, 给出了一种新的攻击方式, 称为 FAW 攻击。Yujin Kwon 等人的分析表明, 矿工困境在 FAW 攻击下并不存在。Samiran Bag 等人[20]提出了一个防止矿池遭受 BWH 攻击的方案。该方案的核心思想是在矿池分配比特币奖励时引入额外奖励的概念, 使得矿池可以通过调整额外奖励的大小实现防止 BWH 攻击的目的。此外, 针对比特币的 PoW 中能源消耗过大、算力过于集中的问题, Iddo Bentov 等人[22]于 2014 年在 PoW 与 PoS (权益证明, 即 Proof of Stake) 的基础上给出了一种新的密码货币协议, 并将其称为活动证明 (PoA, 即 Proof of Activity)。I. Bentov 等人认为 PoA 协议为比特币系统提供了更高的安全性, 同时对网络通信与存储空间的影响并不大, 其安全性的改进主要体现在一定程度上规避了 PoW 协议带来的算力集中问题。Marcin Andrychowicz 等人[23]于 2014 年从安全多方计算协议角度出发, 抽象出比特币的三个主要性质:

a) 缺少中心机构控制交易; b) 交易的公开透明性; c) 除资金转移外, 其语法允许更加丰富的功能。同时, Marcin Andrychowicz 等人给出了这三条性质在安全多方计算中的应用。他们说明了比特币系统提供了一种新的方式来构建“时控承诺”(timed commitment), 其中承诺者必须在特定的时间内揭示他的秘密, 否则将收到惩罚。Samon Barber 等人[24]于 2012 年提出了比特币中可能存在隐私保护问题。之后, Fergal Reid 等人[25]于 2013 年给出了比特币匿名性的详细分析。同年, Ian Miers 等人[26]提出了一种称为零币(Zcash) 的密码货币。零币是首个采用零知识证明机制的区块链系统, 它可提供支付保密性, 同时仍能够使用公有区块链来维护一个去中心化网络。与比特币的不同之处在于, 零币交易自动隐藏区块链上所有交易的发送者、接受者及数额。只用那些拥有查看秘钥的人才能看到交易的内容。用户拥有完全的控制权, 他们可自行选择向其他人提供查看秘钥。

3 预备知识

3.1 比特币

2008 年, 中本聪提出了现在广为人知的比特币。比特币第一次比较完美地解决了密码货币中的去中心化问题。

比特币所采用的核心技术是区块链技术。比特币中的区块链结构是一种由区块链接而成的链式结构, 区块与区块之间通过区块的 Hash 值链接。比特币在区块链接时所采用的Hash算法是SHA-256算法, 即第 n 个区块中的区块 Hash 字段为 SHA-256(B_{n-1})。图 1 位比特币区块链的结构示意图。

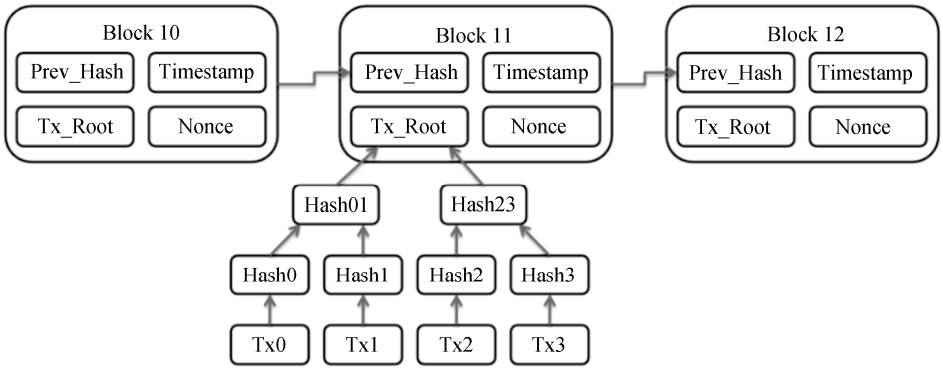

图 1 比特币区块链结构示意图

Figure 1 The figure of Bitcoin's blockchain

由于比特币系统剥离了中央机构, 因此比特币系统中的账本记录和维护问题是比特币中的重要问题。在比特币系统中, P2P 网络、PoW 共识机制与激励制度是比特币实现分布式账本所依赖的核心机制。

P2P 网络, 是无中心服务器、依靠用户群(peers)交换信息的互联网体系, 它的作用在于, 减低以往网路传输中的节点, 以降低资料遗失的风险。与有中心服务器的中央网络系统不同, 对等网络的每个用户端既是一个节点, 也有服务器的功能, 任何一个节点无法直接找到其他节点, 必须依靠其户群进行信息交流。比特币利用 P2P 网络实现了网络层面的去中心化。

比特币中 P2P 网络的运行步骤如下:

(1) 新的交易向全网进行广播;

(2) 每一个节点都将收到的交易信息纳入一个区块中;

(3) 每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明;

(4) 当一个节点找到了一个工作量证明, 它就向全网进行广播;

(5) 当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的, 其他节点才认同该区块的有效性;

(6) 其他节点表示他们接受该区块, 而表示接受的方法, 则是在跟随该区块的末尾, 制造新的区块以延长该链条, 而将被接受区块的 Hash 值视为先于新区块的 Hash 值。

PoW (Proof of Work), 又称工作量证明机制, 即求解一个特定的哈希原像问题的过程。由于在求解哈希原像的问题中, 没有高效的算法, 只能通过暴力计算的方式求解, 从而使得计算资源多、计算能力强的参与者可以有更高的概率率先解出该问题。在密码货币中, 第一个解出该问题的参与者将获得一定数额的相应密码货币的奖励。例如在比特币系统中, 共识链中的区块创建者现阶段可以获得 12.5BTC 的奖励。于是在这种经济奖励的刺激下, 大量矿工参与到通过寻找哈希原像而创建区块的行动中, 这就是我们通常所说的挖矿。挖矿的参与者称为矿工, 挖矿的过程实现了分布式账本的维护。

3.2 比特币矿池

当前世界上存在许多比特币挖矿矿池, 图 2 为一些主要矿池的算力分布情况[21]。这些矿池可分为开放性矿池和封闭性矿池。其中, 开放性矿池允许矿工自由注册并参与该矿池的挖矿。当矿池挖出区块并获得相应的比特币奖励时, 矿池管理员将根据矿池成员的算力大小进行奖励分配。当前世界上矿池算力排前三位的 BTC.com、AntPool 和 SlushPool 均属于开放性矿池。封闭性矿池只允许特定矿工加入, 不在本文考虑范围之内。

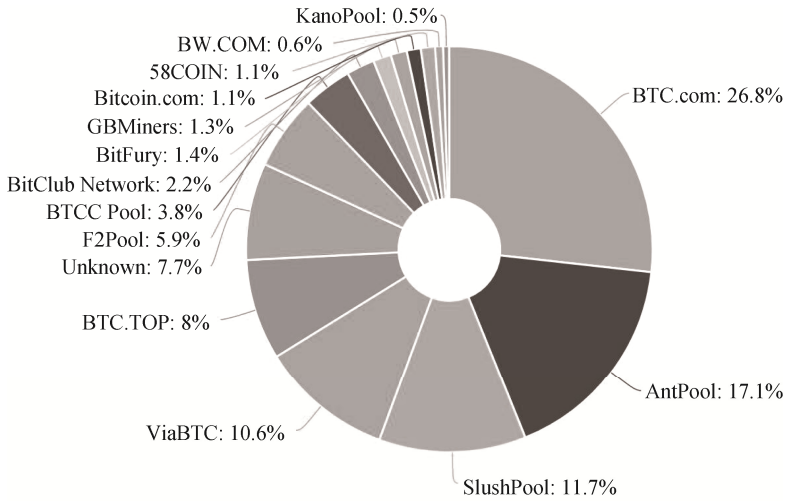

图 2 世界上主要矿池算力分布情况

Figure 2 The hashrate distribution amongst the largest mining pools in the world

矿工选择加入矿池挖矿的主要原因在于减少不确定性的发生, 即矿工期望获得收益的方式更加稳妥(即使该收益数量相对较少)而非赌博式地获取大额收益。矿池中的矿工与矿池管理员拥有同一个公钥, 即矿工与矿池管理员对外拥有同一个比特币地址。

根据比特币的设计, 单个独立矿工或者矿池挖矿的目的是寻找当前系统工作量证明问题的解, 即寻找一个合法的区块 B, 使得 $\mathrm{Hash}(B)<T$, 其中目标值 T 每隔一段时间由系统自动调整。在矿池内部, 矿池管理员在向矿池成员发布完整工作量证明(Full Proof of Work)任务的同时, 也向矿池成员发布部分工作量证明(Partial Proof of Work)任务。其中, 完整工作量证明任务要求矿工寻找使得 $\mathrm{Hash}(B)<T$ 成立的区块 B, 而部分工作量证明任务是指寻找使得 $\mathrm{Hash}(B')<T'$ 成立的区块 B', 这里 $T'\geqslant T$。显然, 部分工作量证明任务包含了完整工作量证明任务, 其难度小于完整工作量证明任务的难度。矿池管理员将矿池内部矿工提交的部分工作量证明作为其分配比特币奖励的依据。

3.3 BWH攻击

在比特币挖矿系统中, 设其总算力为 1, 攻击者拥有的算力为 α。在 BWH 攻击中, 攻击者将算力 α 中的部分算力 $\beta\alpha(0\leqslant\beta\leqslant1)$ 置入被攻击的矿池 P 中, 这部分算力仅向矿池 P 提交部分工作量证明, 而丢弃其产生的完整工作量证明。由于攻击者只向矿池 P 提供部分工作量证明, 这使得矿池 P 损失了一部分由攻击者产生的完整工作量证明, 从而损失了这部分完整工作量证明所对应的比特币奖励。与此同时, 攻击者利用另一部分算力 $\alpha-\beta\alpha$ 用于诚实挖矿。类似地, 矿池之间同样可以实施 BWH 攻击, 当矿池 P 对矿池 P' 实施 BWH 攻击时, 矿池 P 将部分算力转移到矿池 P' 中, 但是这部分算力并不对矿池 P' 的挖矿作出贡献, 但是却能够获得矿池 P' 根据算力所分配的比特币奖励。

对攻击者而言, 实施 BWH 攻击可以造成被攻击的矿池损失一定的比特币奖励。但仅此一点尚不足以保证攻击者有动机实施 BWH 攻击。

3.4 Loi Luu 等人关于 BWH 攻击的理论分析

Loi Luu 等人在文献[7]中针对 BWH 攻击给出了理论分析, 证明了攻击者可以通过选取适当的 β, 使得攻击者实施攻击时获得的收益高于不实施攻击时获得的收益, 从而攻击者有动机实施 BWH 攻击。下面简单回顾 Loi Luu 等人关于 BWH 攻击的理论分析过程。

在 Loi Luu 等人的分析中, 假设攻击者将其部分算力 $\beta\alpha(0\leqslant\beta\leqslant1)$ 置入矿池 P 并对其进行 BWH 攻击。设每个区块的奖励为 1, 矿池 P 原有算力为 p', 新算力为 p, 即 $p=p'+\beta\alpha$。由于攻击者将部分算力 $\beta\alpha$ 用于实施 BWH 攻击, 这部分算力在挖矿中没

有任何贡献, 因而系统的总算力实际为$1-\beta\alpha$. 于是在系统成功挖出一个区块的条件下由矿池 P 成功挖出该区块的概率为$\frac{p-\beta\alpha}{1-\beta\alpha}$。之后攻击者将获得矿池 P 根据算力占比 $\frac{\beta\alpha}{p}$ 分配的奖励 $\frac{p-\beta\alpha}{1-\beta\alpha}*\frac{\beta\alpha}{p}*1$; 同时攻击者将算力 $\alpha-\beta\alpha$ 用于诚实挖矿所获得的收益为$\frac{\alpha-\beta\alpha}{1-\beta\alpha}*1$。于是攻击者获得的总收益为

$$R=\frac{p-\beta\alpha}{1-\beta\alpha}\frac{\beta\alpha}{p}+\frac{\alpha-\beta\alpha}{1-\beta\alpha}=\frac{p\alpha-\beta^2\alpha^2}{p(1-\beta\alpha)}$$

3.5 BWH 攻击的意义

自比特币诞生以来, 研究人员提出了针对比特币的多种攻击方式。由于比特币自身的去中心化特点, 研究提出的攻击方式多着眼于比特币的去中心化部件上, 比如针对 P2P 网络、PoW 共识协议等。

需要注意的是, 比特币系统的实际运行中, 在许多方面背离了中本聪的设计初衷。例如, 3.2 节中介绍的比特币矿池的形成, 在一定程度上打破了比特币的去中心化设计。部分矿池算力相对较高, 在比特币系统中具有相对较高的话语权, 比特币区块链面临随时被动分叉的危险。针对挖矿矿池的研究是密码货币安全性研究中不可或缺的一部分。BWH 攻击正是针对挖矿矿池的一种攻击方式。

BWH 攻击早在 2011 年便由 Meni Rosenfeld 提出, 但是 Meni Rosenfeld 未能给出一个较为完整的理论说明。直到 2015 年 L. Luu 等人才从理论上证明了 BWH 攻击对攻击者的良激励性(well-incentivized), 即攻击者实施 BWH 攻击相对于诚实挖矿可以获得更高的收益。此后, 研究人员开始逐渐关注 BWH 攻击, 最近的研究成果为 Yujin Kwon 在 CCS'17 上提出的 FAW 攻击, FAW 攻击吸取了 BWH 攻击的思想。但是, 在现实中却鲜有矿池遭受 BWH 攻击的报道。目前可被检索的实际遭受 BWH 攻击的消息来自 2014 年"Eligius"矿池遭受的 BWH 攻击。据"Eligius"矿池称, 攻击者实施 BWH 攻击是出于破坏该矿池的目的, 即攻击者通过实施 BWH 攻击, 减少了矿池中矿工的收益, 从而误导矿池中的矿工转向其他矿池挖矿, 实现了分散"Eligius"矿池算力的目的。因此, 我们认为 BWH 攻击可能并非是良激励性的。

4 BWH 攻击分析

4.1 Loi Luu 等人分析中的缺陷

Loi Luu 等人的分析存在缺陷的本质原因在于其忽略了比特币系统算力的改变对矿池(或矿工)挖矿所获得收益的影响。为便于理解, 我们首先做出以下两点说明。

4.1.1 系统算力的改变对区块产生时间的影响

设某时刻比特币系统的全部算力为 γ, 此时系统产生一个区块所需的时间为 t, 之后由于某些矿池或矿工的加入或退出, 导致系统算力发生改变。设算力改变之后比特币系统的算力为 γ', 此时系统产生一个区块所需的时间为 t'。

显然, 当 $\gamma'<\gamma$ 时, 即系统算力降低后, 有 $t'>t$. 由于区块奖励不变(仍为 1), 从而单位时间内比特币系统中的区块奖励有所减少。

4.1.2 Loi Luu 等人分析中的缺陷

在本小节中, 我们沿用 3.3 小节与 4.1.1 小节中的记号, 并设攻击者不实施攻击时系统总算力 γ 为 1, 此时系统产生一个区块的时间为 t。

当攻击者实施 BWH 攻击时, 攻击者将算力 $\beta\alpha$ 置于矿池 P 中, 但这部分算力仅向矿池 P 提交部分工作量证明, 而丢弃完整工作量证明, 因此这部分算力对整个比特币系统的挖矿过程没有贡献, 从而此时在比特币系统中挖矿的算力 $\gamma'<\gamma$。根据 4.1.1 小节的分析, 攻击者实施 BWH 攻击后, 系统产生一个区块的时间有所增加, 即 $t'>t$。Loi Luu 等人所计算的攻击者实施攻击时的收益 $\frac{p\alpha-\beta^2\alpha^2}{p(1-\beta\alpha)}$, 是在长度为 t' 的时间内攻击者获得的收益。同时, Loi Luu 等人认为此时攻击者不实施攻击获得的收益为 α, 并将 $\frac{p\alpha-\beta^2\alpha^2}{p(1-\beta\alpha)}$ 与 α 做对比。但是, 需要注意的是 α 是在长度为 t 的时间内攻击者获得的收益。显然, Loi Luu 等人对在不同时间长度内获得的两种收益进行对比是不合理的。

4.2 相同时间长度下攻击者实施与不实施 BWH 攻击时的收益对比

判断一个矿工是否有动机实施 BWH 攻击的一个重要准则就是其在相同时间长度内实施攻击时是否可以获得比不实施攻击时更高的收益。显然, 如果攻击者实施 BWH 攻击不能获得更高的收益, 那么他/她缺乏实施 BWH 攻击的动机。下面我们重新计算攻击者在实施 BWH 攻击与不实施 BWH 攻击时所获得的单位时间内的收益。

设比特币系统总算力为 1, 攻击者拥有的算力为 α, 攻击者不实施 BWH 攻击时, 亦即攻击者将全部算力 α 用于诚实挖矿, 系统产生一个区块所需的时间为 1。此时攻击者在单位时间内可获得的总收益为

$R_{HON}=\alpha$。当攻击者用部分算力 $\beta\alpha(0\leqslant\beta\leqslant1)$ 实施 BWH 攻击时, 我们有下面的结论。

引理 1. 设比特币系统产生一个区块所需的时间与系统算力成反比。那么攻击者实施 BWH 攻击时, 所获得的单位时间内的收益为

$$R_{\mathrm{BWH}}=\frac{p\alpha-(\beta\alpha)^2}{p}$$

证明: 在 BWH 攻击中, 当攻击者将算力 $\beta\alpha$ 投入到矿池 P 中实施攻击时, 由于这部分算力对系统挖矿没有贡献, 从而系统的总算力由 1 减小为 $1-\beta\alpha$, 此时区块产生的时间由 1 增大为 $\frac{1}{1-\beta\alpha}$, 相应的, 系统所获得的单位时间内的区块奖励为 $1-\beta\alpha$。

攻击者在矿池 P 中获得的单位时间内的收益为

$R_P=\frac{p-\beta\alpha}{1-\beta\alpha}\frac{\beta\alpha}{p}(1-\beta\alpha)=\frac{(p-\beta\alpha)\beta\alpha}{p}$。

攻击者通过使用算力 $\alpha-\beta\alpha$ 诚实挖矿所获得的单位时间内的收益为

$R_H=\frac{\alpha-\beta\alpha}{1-\beta\alpha}(1-\beta\alpha)=\alpha-\beta\alpha$。

从而攻击者单位时间内的总收益为

$$\begin{aligned}R_{\mathrm{BWH}}&=R_P+R_H\\&=\frac{(p-\beta\alpha)\beta\alpha}{p}+\alpha-\beta\alpha\\&=\frac{p\alpha-(\beta\alpha)^2}{p}。\end{aligned}$$

定理 1. 攻击者实施 BWH 攻击时单位时间内获得的收益总小于不实施 BWH 攻击时单位时间内获得的收益。

证明: 由引理 1 可得,

$$\begin{aligned}R_{\mathrm{BWH}}-R_{HON}&=\frac{(p-\beta\alpha)\beta\alpha}{p}-\beta\alpha\\&=\frac{1}{p}\big((p-\beta\alpha)\beta\alpha-p\beta\alpha\big)\\&=-\frac{(\beta\alpha)^2}{p}<0。\end{aligned}$$

由定理 1, 攻击者针对矿池 P 实施 BWH 攻击, 没有获得更高的收益. 从而攻击者不具有动机实施 BWH 攻击, 除非其纯粹出于破坏矿池 P 的目的而选择实施 BWH 攻击。

5 结论

本文考察了 Loi Luu 等人关于 BWH 攻击做出的分析, 说明了他们的分析忽略了算力改变对区块产生时间的影响, 从而 Loi Luu 等人对攻击者实施 BWH 攻击时获得的收益与不实施 BWH 攻击时获得的收益对比, 实质上是在不同时间长度下的对比, 而这显然不够合理。根据对相同时间内攻击者实施 BWH 攻击时与不实施 BWH 攻击时获得的收益情况对比, 我们发现攻击者实施攻击所获得的收益总小于不实施攻击时所获得的收益, 从而攻击者缺乏实施 BWH 攻击的动机, 除非其纯粹出于破坏矿池的目的而采用 BWH 攻击。

参考文献

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” www.academia.edu/download/32413652/BitCoin_P2P_electronic_cash_system.pdf, 2008

[2] Litecoin, https://litecoin.org/.

[3] Primecoin, http://primecoin.io/.

[4] “Blockchain,” https://en.wikipedia.org/wiki/Blockchain.

[5] M. Rosenfeld, “Analysis of bitcoin pooled mining reward systems,” https://arxiv.org/pdf/1112.4980.pdf, 2011.

[6] “Best practice for fast transaction acceptance - how high is the risk?”, https://bitcointalk.org/index.php?topic=3441.msg48384#msg48384.

[7] L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor, “On power splitting games in distributed computation: The case of bitcoin pooled mining,” in Computer Security Foundations Symposium (CSF’15), pp. 397-411, 2015.

[8] G. O. Karame, E. Androulaki and S. Capkun, “Double-spending fast payments in bitcoin,” in Proceedings of the 2012 ACM conference on Computer and communications security(CCS’12), pp. 906–917, 2012.

[9] A. Gervais, H. Ritzdorf, G. O. Karame and S. Cap-kun, “Tampering with the delivery of blocks and transactions in bitcoin,” in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security(CCS’15). pp. 692–705, 2015.

[10] J. Garay, A. Kiayias and N. Leonardos, “The bitcoin backbone protocol: Analysis and applications,” in Advances in Cryptology - EUROCRYPT 2015, pp. 281—310, 2015.

[11] J. Garay, A. Kiayias and N. Leonardos, “The bitcoin backbone protocol with chains of variable difficulty,” in Advances in Cryptology-CRYPTO 2017, pp. 291—323, 2017.

[12] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in International conference on financial cryptography and data security(FC’14), pp. 436–454, 2014.

[13] A. Sapirshtein, Y. Sompolinsky and A. Zohar, “Optimal selfish mining strategies in bitcoin,” in International conference on financial cryptography and data security(FC’16), pp. 515-532, 2016.

[14] K. Nayak, S. Kumar, A. Miller and E. Shi, “Stubborn mining: Generalizing selfish mining and combining with an eclipse attack,” in IEEE European Symposium on Security and Privacy (EuroS&P), pp.305-320, 2016.

[15] E. Heilman, A. Kendler, A. Zohar and S. Goldberg, “Eclipse attacks on bitcoin’s peer-to-peer network,” in USENIX Security Symposium. Washington (SP’15), pp.129-144, 2015.

[16] H. Cheng, X. Feng, “ Selfish mining attack under the scripting mechanism”. preprint.
(程恒喆, 冯秀涛. 脚本机制下的自私挖矿攻击. preprint.)
[17] “Eligius,” https://bitcointalk.org/?topic=441465.msg728267.
[18] I. Eyal, “The miner's dilemma”, in IEEE Symposium on Security and Privacy(SP’15), pp.89-103, 2015.
[19] Y. Kwon, D. Kim, Y. Son, E. Vasserman and Y. Kim, “Be selfish and avoid dilemmas: Fork after withholding (FAW) attacks on bitcoin,” in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security(CCS’17), pp.195-209, 2017.
[20] S. Bag and K. Sakurai, “Yet another note on block withholding attack on bitcoin mining pools,” in International Conference on Information Security, pp.167-180, 2016.
[21] “Pools,” https://blockchain.info/zh-cn/pools.
[22] I. Bentov, C. Lee, A. Mizrahi, et al. Proof of activity: Extending bitcoin’s proof of work via proof of stake [J]. ACM SIGMETRICS Performance Evaluation Review, pp.34-37, 2014.
[23] M. Andrychowicz, S. Dziembowski, D. Malinowski, et al. Secure multiparty computations on bitcoin[C]. Security and Privacy (SP), pp.443–458,2014.
[24] S. Barber, X. Boyen, E. Shi, et al. Bitter to better—how to make bitcoin a better currency[C]. International Conference on Financial Cryptography and Data Security, pp.399–414,2012.
[25] F. Reid, M. Harrigan. An analysis of anonymity in the bitcoin system[M]. Security and privacy in social networks, pp.197–223,2013.
[26] I. Miers,C. Garman, M. Green, et al. Zerocoin: Anonymous distributed e-cash from bitcoin[C]. Security and Privacy (SP), 2013 IEEE Symposium on, pp.397–411, 2013.

程恒喆 于 2014 年在曲阜师范大学数学与应用数学专业获得学士学位。现在中国科学院数学与系统科学研究院应用数学专业攻读硕士学位。研究兴趣包括: 密码货币与区块链技术。Email: chenghengzhe15@mails.ucas.ac.cn

冯秀涛 于 2006 年在中科院大学信息安全专业获得博士学位。现任中国科学院数学与系统科学研究院副研究员。研究领域为信息安全与密码学。Email: fengxt@amss.ac.cn