密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2018, 5(5): 470–483

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

区块链技术专刊

比特币挖矿攻击研究*

韩 健[1], 邹 静[2], 蒋 瀚[3], 徐秋亮[3]

1. 山东大学 计算机科学与技术学院, 济南 250101
2. 国网经济技术研究院有限公司, 北京 102209
3. 山东大学 软件学院, 济南 250101

通信作者: 徐秋亮, E-mail: xql@sdu.edu.cn

摘 要: 比特币是中本聪在 2008 年提出的一种数字货币, 具有去中心化、去信任化、强健壮性、无监管、发行量固定等特点, 一经推出就受到全世界的关注. 作为当前最成功的数字货币, 比特币基于 P2P 网络中众多节点构成的分布式数据库来确认并记录所有的交易行为, 利用工作量证明机制解决共识问题, 并使用密码学的设计来确保货币流通的安全性. 随着比特币价格的提升、用户数的增加, 比特币的安全性越来越引起人们的重视, 比如双重支付问题、交易延展性问题和隐私保护问题. 针对比特币系统的不同方面出现了许多的攻击: 针对网络的日蚀攻击、路由攻击, 针对共识机制的挖矿攻击等等, 特别是矿池出现后, 出现了一些新的针对矿池的攻击行为. 本文主要介绍针对比特币挖矿的各种攻击如 51% 攻击、区块截留攻击、自私挖矿和 FAW 攻击, 分析攻击的基本思想、基本策略和现实危害, 并介绍一些应对攻击的方案.

关键词: 比特币; 51% 攻击; 区块截留攻击; 自私挖矿; FAW 攻击

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000257

中文引用格式: 韩健, 邹静, 蒋瀚, 徐秋亮. 比特币挖矿攻击研究[J]. 密码学报, 2018, 5(5): 470–483.

英文引用格式: HAN J, ZOU J, JIANG H, XU Q L. Research on mining attacks in Bitcoin[J]. Journal of Cryptologic Research, 2018, 5(5): 470–483.

Research on Mining Attacks in Bitcoin

HAN Jian[1], ZOU Jing[2], JIANG Han[3], XU Qiu-Liang[3]

1. School of Computer Science and Technology, Shandong University, Jinan 250101, China
2. State Grid Economic and Technological Research Institute Co. Ltd., Beijing 102209, China
3. School of Software, Shandong University, Jinan 250101, China

Corresponding author: XU Qiu-Liang, E-mail: xql@sdu.edu.cn

Abstract: Bitcoin is a cryptocurrency introduced by Satoshi Nakamoto in 2008, with the features of decentralization, detrusting, strong robustness and fixed total amount, it has received great attention

* 基金项目: 国家自然科学基金项目 (61572294); 国家自然科学基金重点项目 (61632020); 山东省自然科学基金项目 (ZR2017MF021); 山东省科技重大创新工程项目 (2018CXGC0702); 山东大学基本科研业务费专项资金项目 (2017JC019); 国网信息化项目 (B3441518G001)

Foundation: National Natural Science Foundation of China (61572294); Key Program of National Natural Science Foundation of China (61632020); Natural Science Foundation of Shandong Province (ZR2017MF021); Major Innovation Project of Science and Technology in Shandong Province (2018CXGC0702); Fundamental Research Funds of Shandong University (2017JC019); State Grid Informationization Project (B3441518G001)

收稿日期: 2018-08-07 定稿日期: 2018-09-26

all over the world. As the most successful cryptocurrency to date, Bitcoin recognizes and records all transactions based on a distributed database of nodes in a P2P network, makes use of PoW to solve the consensus problem and the cryptographic design to ensure the security of currency circulation. With the rising price and increasing number of users, the security of Bitcoin has attracted more attention, such as double spending, transaction malleability, privacy issues. There have been many attacks targeting different aspects of Bitcoin systems, including eclipse attack and routing attacks targeting Bitcoin network, mining attacks targeting consensus mechanism, etc. With the appearance of mining pools, there have been some new attacks targeting the pools. This paper focuses on the attacks targeting mining and mining pools, such as 51% attack, block withholding attack, selfish mining attack, and FAW attack, analyzes the basic idea, basic strategy, and the real threat of the attacks. In addition, some solutions to these attacks are also introduced.

Key words: Bitcoin; 51% attack; block withholding attack; selfish mining; FAW attack

1 引言

比特币作为一种去中心化的数字货币, 最早是由中本聪在 2008 年提出的 [1], 相比较于传统货币, 它完全依赖于 P2P 网络, 没有发行中心, 匿名、免监管、跨国境流通. 在 10 年时间内, 比特币已经从一个小众数字货币快速发展成了一个在全球范围内交易的资产. 它的价格在 2017 年 12 月飙升到 1.9 万美元, 创下纪录. 随着闪电网络等线下支付解决方案的提出 [2], 比特币的使用人数越来越多. ARK 投资公司和 Coinbase 公司 2017 年发布的联合报告指出: 全球比特币用户数量超过 1000 万, 每天交易金额超过 1.5 亿美元 [3]. 专攻加密数字货币技术的 Polymath 公司的首席执行官特雷弗 · 柯沃科 (Trevor Koverko) 认为, 未来比特币将会成为一种完备的支付网络.

伴随着比特币的发展, 比特币系统安全问题越来越受到关注, 如比特币的双重支付问题、交易延展性问题、隐私保护问题等等, 出现了一些针对比特币不同方面的攻击. 本文以共识机制安全为出发点, 综述比特币所面临的各种挖矿攻击, 详细分析攻击的基本原理和威胁危害, 并介绍一些现存的应对攻击的方案. 主要介绍以下四种挖矿攻击:

(1) 51% 攻击. 在数字货币中, 最重要的是如何解决双重支付问题, 即如何保证同一笔钱 (数字货币) 不被重复支付两次, 比特币利用全网公开交易、时间戳、工作量证明等机制来解决这一问题. 同时中本聪在比特币白皮书中提出实现双花的一种方法: 51% 攻击 [1], 这是比特币系统面临的最早的攻击行为. 比特币网络所有节点共同维护同一个账本, 如果想要篡改账本中的数据必须能够控制全网大部分节点, 即掌握 51% 的算力.

(2) 区块截留攻击. 比特币第一个用户 Finney 提出实现双花的一种方法: 芬尼攻击, 它利用区块截留的思想. Rosenfel [4] 在 2011 年首次提出区块截留攻击的概念, 他描述了一个区块截留攻击场景: Sabotage, 这是恶意矿工针对目标矿池的攻击, 矿池和恶意矿工的收益都减少. Courtois 和 Bahack [5]、Luu [6] 提出攻击者利用区块截留攻击可以提高自己的收益, 并对不同场景下的收益情况进行分析. Eyal [7] 分析了矿池间进行区块截留攻击的场景并提出矿工困境的概念. 2017 年 Bag 等人 [8] 又提出了一种新的区块截留攻击类型: 赞助区块截留攻击.

(3) 自私挖矿. 2010 年文献 [9] 最早提出选择性的延迟区块的公布可以获得更多的区块奖励的思想, Eyal 和 Sirer [10] 在 2013 年首次提出自私挖矿的概念. 同时 Bahack [11] 研究分析了一系列挖矿攻击策略, 他在文章中把自私挖矿攻击叫做块丢弃攻击. Sapirshtein 等人 [12] 扩展了自私挖矿攻击的基础模型, 提出了一种寻找最优攻击策略的算法, 利用此算法可以计算攻击者发动自私挖矿获得额外收益的算力下界, 此界值低于文献 [10] 的阈值. 文献 [10, 11] 中自私挖矿攻击者遵守最长链规则, 当公链长于私链时自私矿工立即放弃私链转到公链上挖矿. Nayak 等人 [13] 打破最长链规则, 扩展了自私挖矿的策略空间, 证明了在某种条件下甚至于公链比私链更长时, 自私矿工在私链上挖矿仍能够获得更高的期望收益.

(4) FAW 攻击. 2017 年 Kwon 等人 [14] 提出 FAW 攻击, 它综合运用区块截留攻击和故意分叉来增加攻击者的收益.

2 相关知识

本节主要介绍比特币的相关知识, 包括比特币区块、工作量证明、矿工和矿池、挖矿收益等.

(1) 比特币区块 [15]. 区块是一种被包含在公开账簿 (区块链) 里的聚合了交易信息的容器数据结构. 它由一个包含元数据的区块头和紧跟其后的构成区块主体的一长串交易组成. 区块头包含六个字段 (80 字节): 版本字段, 4 字节, 用于跟踪软件/协议的更新; 父区块哈希值字段, 32 字节, 表示引用的区块链中父区块的哈希值; Merkle 根字段, 32 字节, 表示该区块中交易的 Merkle 树根的哈希值; 时间戳字段, 表示该区块产生的近似时间 (精确到秒的 Unix 时间戳); 难度目标字段, 4 字节, 表示该区块工作量证明算法的难度目标; Nonce 字段, 4 字节, 表示用于工作量证明算法的计数器. 其中下面三个字段用于挖矿过程. 区块是由矿工挖矿产生, 比特币网络会调整难度值来保证平均每 10 分钟产生一个区块, 调整周期为 2016 个区块.

(2) 工作量证明 [16]. 比特币作为一种无中心的数字货币, 是由比特币网络中的所有节点来统一进行维护的, 这就需要一种共识机制来决定谁具有记账权. 比特币系统采用工作量证明 (POW) 来解决这一问题, 也叫做挖矿. 所有比特币节点基于各自的计算机算力相互竞争来解决一个求解困难但验证容易的 SHA-256 困难问题, 最快解决该难题的节点获得区块记账权, 即创建了一个区块, 所有其他节点验证新区块的合法性并更新本地区块链.

(3) 矿工和矿池. 矿工独立利用计算机或矿机进行挖矿, 找到有效区块后所有收益归矿工自己所有. 随着矿工数量的增加和专业挖矿设备的出现, 比特币全网的运算水准在不断的呈指数级别上涨, 单个矿工或少量的算力短时间内无法在比特币网络上挖到区块获得收益. 多个矿工将自己算力联合运作挖矿, 并按照参与矿工的贡献分配奖励, 使用这种方法建立的网站便被称作 “矿池”(mining pool). Rosenfeld [4] 证明了在矿池管理费用可忽略的情况下矿工独立挖矿和加入矿池挖矿, 收益是相等的, 只与自己的算力占比有关. 据 Bitcoinmining.com 统计, 目前已经存在 13 种不同的矿池分配机制, 主流矿池通常采用 PPLNS (pay per last N shares) 、PPS(pay per share) 和 PROP (PROPortionately) 等机制 [16]. 矿池相对于独立挖矿的优势: 降低了挖矿的门槛, 人人都可以参与挖矿; 矿工的收益比较稳定, 不会出现较大起伏. 但也存在一些弊端, 如矿池掌握着极其庞大的算力资源, 单个矿池或者几家矿池联合算力很容易达到 50% 以上, 能够发动 51% 攻击, 后果非常可怕.

(4) 挖矿收益. 比特币的发行和交易的完成是通过挖矿来实现的, 它以一个确定的但不断减慢的速率被铸造出来. 每一个新区块都伴随着一定数量从无到有的全新比特币, 它作为 coinbase 交易奖励给找到区块的矿工. 每个区块的奖励不是固定不变的, 每开采 210 000 个区块, 大约耗时 4 年, 货币发行速率降低 50%. 在比特币运行的第一个四年中, 每个区块创造出 50 个新比特币. 现在每个区块创造出 12.5 个新比特币. 除了块奖励外, 矿工还会得到区块内所有交易的手续费.

(5) 分叉. 如果两个矿工几乎在同一时间内各自都找到工作量证明的解, 它们都向网络广播各自的区块, 此时区块链产生分叉. 分叉可能偶然意外发生或有意为之. 因为工作量证明是一个泊松过程, 两个区块可能在几秒钟内被两个矿工同时发现, 这会导致产生一个意外分叉; 自私矿工挖到一个区块时可能秘密保存, 当另一个矿工紧接着相同的前块也挖到了一个区块并广播时, 自私矿工立即公布自己的秘密区块产生有意分叉.

3 51% 攻击

51% 攻击, 是指掌握了比特币全网 51% 算力的节点通过重新计算已经确认过的区块或控制新区块的产生, 成功伪造和篡改区块链交易数据的行为, 攻击的目的是实现双花. 下面具体分析 51% 攻击是如何实现双花的.

3.1 攻击者

攻击者可以分为两种类型: 理性攻击者, 攻击的目的是最大化自身的利益, 获取更多的金钱; 暴力攻击者, 攻击的目的纯粹是破坏, 满足自身的心理需要, 不计较个人得失, 是不理智、不理性的.

51% 攻击需要满足两个条件: 攻击者掌握了比特币全网 51% 的算力; 攻击者手里持有大量比特币.

攻击者能力: 修改自己的交易记录, 这可以使他进行双重支付; 阻止区块确认部分或者全部交易; 阻止部分或全部矿工开采到任何有效的区块; 阻止某些交易进入区块链. 攻击者无法做到: 修改他人的交易记录, 把不属于自己的比特币发送给自己或他人; 阻止他人发送交易; 改变每个区块产生的比特币数量; 凭空产生比特币.

3.2 攻击步骤

(1) 攻击者将手中的大量比特币充值各大交易所, 然后卖掉提现, 也可以直接卖给别人或者同别人交易换取资产资本等, 交易对方确认包含此交易的区块上链并经过确认后付给攻击者指定的金钱或者资产;

(2) 攻击者运用手中的算力, 从自己对外付款交易之前的区块开始, 生成新的交易将自己的之前花费的比特币转移到自己的新地址, 然后重新构造新的区块 (包含新交易), 并利用自己的算力优势与全网其余算力竞争, 当攻击者挖到的区块长度超过原主链区块, 成为新的主链则攻击完成;

攻击结果: 包含攻击者付款交易的区块链分支没有成为主链, 这就意味着付款交易不会被比特币网络认可, 相当于回收了攻击者交易掉的比特币, 实现了双花.

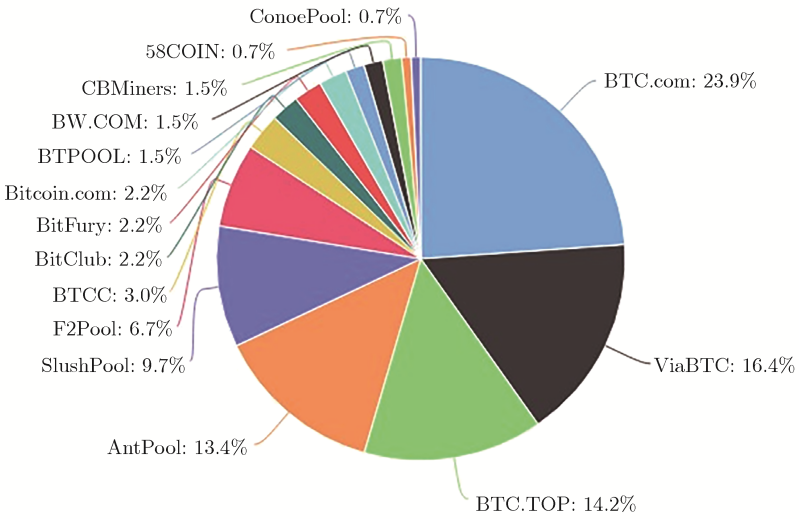


图 1 2017 年比特币算力分布

Figure 1 Bitcoin computing power distribution in 2017

3.3 攻击分析

(1) 51% 算力能否达到? 单个矿工挖矿时期, 某几个恶意矿工联合也很难掌握 51% 的算力, 矿池的出现使得 51% 攻击成为可能, 图1显示 2017 年比特币系统的全网算力分布情况, 可以看出算力排名前 3 的矿池若联合作恶, 其算力超过全网算力的 51%, 满足攻击的基本条件.

(2) 是否获得足够收益? 攻击的目的是获得利益. 作为掌握全网 51% 算力的攻击者, 是比特币网络的支持者, 通过攻击获得的收益必须足够大才值得攻击, 一旦攻击被发现, 整个比特币网络就失去信任甚至崩溃, 比特币变得一文不值, 攻击者的利益也受到损失. 相比于发动攻击, 攻击者可以利用这一算力进行挖矿, 其收益远大于攻击收益.

(3) 攻击者攻击成功的概率和需要的时间. 中本聪的论文描述了指定算力攻击成功的概率计算公式 [1], 它的计算是基于泊松分布的理论值. 若攻击者掌握了一半以上的算力, 那么概率上永远能够赢, 但是它只分析攻击成功的概率, 没有计算攻击成功需要的时间. 下面以固定算力计算 51% 攻击成功需要的理论时间 (图2): 诚实者算力 49%, 攻击者算力 51%, 它们都在各自的分支上挖块, 攻击者追上诚实者 (6 个区块差距) 所用时间约 1 个小时, 这个时间是非常长的.

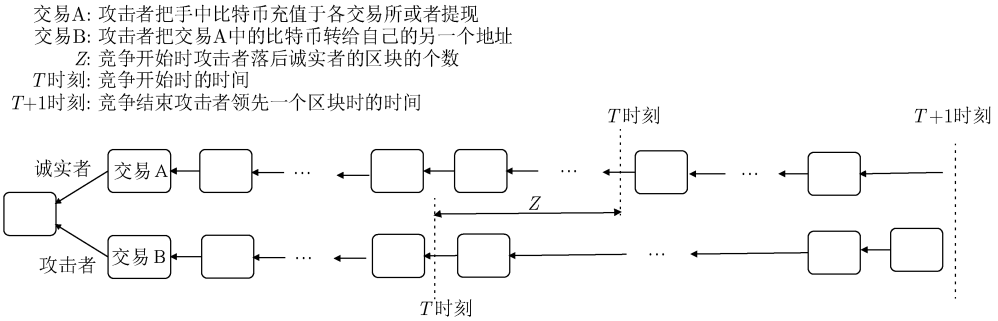


图 2 51% 攻击挖矿竞争

Figure 2 Mining competition of 51% attack

3.4 攻击防范

尽管 51% 攻击只存在理论意义上, 但是在现实中我们仍然要保持警惕并可以采取多种方法防范这种攻击, 如监管矿池发出的大额交易、遇有大额交易时多等几个确认区块、监管矿池的出块情况 (长时间不出块) 等等.

4 区块截留攻击

区块截留攻击是指矿工找到满足比特币网络难度目标要求的区块时扣在自己手里的攻击行为. 区块截留攻击主要有两种: (1) 芬妮攻击; (2) 矿池区块截留攻击.

4.1 芬尼攻击

芬尼攻击是一种利用比特币中未确认交易来欺诈接受比特币支付的商家的一种攻击行为. 服务提供者或商品销售者信任未确认交易, 在收到未确认交易后便立即提供服务或者商品. 具体过程: 攻击者挖到一个区块不立即公布 (这个区块中包含一个交易 Tx1: A 向 B 转账 10 BTC, 其中 A 和 B 都是属于攻击者自己的地址), 而是向愿意接受未确认交易的商家购买商品或服务, 并生成交易 Tx2: A 向 C (商家) 转账 10 BTC. 商家提供商品或服务后矿工立即公布刚刚挖到的区块, 比特币网络接受交易 Tx1, 并使交易 Tx2 无效, 实现了双花.

攻击分析: 攻击者生成区块和完成交易 Tx2 之间存在时间间隙, 在此期间网络上的其他矿工也可以生成有效块并广播它, 从而使攻击者生成的有效块变无效. 因此攻击的前提条件是, 从生成交易到完成这个交易的时间间隔足够小, 只能选择攻击购买软件产品的秘钥或在线服务等完成时间短的交易.

4.2 区块截留攻击 (矿池)

矿池形成后, 矿工加入矿池接受矿池管理者分配的任务开始挖矿, 管理者为了估计每个矿工的贡献值来分配收益, 设置一个小于比特币网络的难度目标值保证小矿工也能够以很快的频率找到满足此目标的哈希值 (份额), 并提交给矿池管理者, 这叫做部分工作量证明 (PPOW), 与之相对应的是完整工作量证明 (FPOW), 只有 FPOW 生成的区块才会被比特币网络认可, 并获得比特币奖励. 矿工在努力发现完整工作量证明的过程中, 很自然地会发现部分工作量证明. 区块截留攻击的基本思想是攻击者伪装为诚实矿工加入矿池挖矿, 只提交 PPOW, 当发现 FPOW 时立即抛弃, 攻击者享受矿池的收益但不实际贡献算力, 从而降低矿池的收益.

工作量证明只能被任务的创建者即矿池管理者使用, 攻击者不能将发起攻击的算力再用作它途, 这是因为矿工发现的完整的工作量证明不能自己提交给比特币网络, 即使能够提交, 生成新比特币的 coinbase 交易的输出地址是矿池管理者而不是攻击者. 另外, 攻击者仍然需要按照管理者要求利用自己的算力寻找满足目标值的 nonce, 否则他们不能提交部分工作量证明, 也就不能获得与自己算力相匹配的收益.

下面详细介绍几种常见的区块截留攻击类型.

4.2.1 经典区块截留攻击

文献 [4] 提出的 Sabotage 就是经典区块截留攻击, 它是矿池中单个矿工以牺牲自己收益为代价针对矿池和矿池中其它矿工的攻击行为, 攻击者是非理性的. 下面定量分析这种攻击行为的收益情况.

假设比特币网络的总算力为 1, 某个目标矿池的算力为 p (占全网算力的比例, 包含攻击者算力 α), 该矿池中诚实矿工的算力 $(p-\alpha)$, 矿池外矿工独立或者组成矿池诚实挖矿, 如图3所示. 定义变量相对增益 $\Delta_R = \frac{R}{R_h} - 1$ 来表示相对于诚实挖矿收益的变化情况, R_h 为诚实挖矿时的收益.

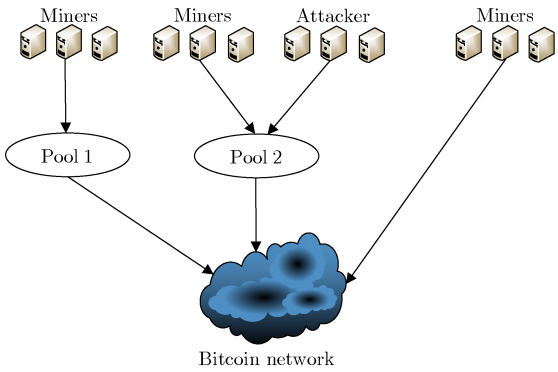


图 3 经典区块截留攻击

Figure 3 Classical block withholding attack

目标矿池中诚实矿工的相对增益:

$$\Delta_{R_p} = \frac{p-\alpha}{1-\alpha} \cdot \frac{p-\alpha}{p} \cdot \frac{1}{p-\alpha} - 1 = \frac{\alpha(p-1)}{(1-\alpha)p} < 0$$

攻击者的相对增益:

$$\Delta_{R_A} = \frac{p-\alpha}{1-\alpha} \cdot \frac{\alpha}{p} \cdot \frac{1}{\alpha} - 1 = \frac{\alpha(p-1)}{(1-\alpha)p} < 0$$

目标矿池外诚实矿工的相对增益:

$$\Delta_{R_O} = \frac{1-p}{1-\alpha} \cdot \frac{1}{1-p} - 1 = \frac{\alpha}{1-\alpha} > 0$$

由以上分析可知, 在经典区块截留攻击场景下目标矿池的收益减少, 攻击者的收益减少, 而矿池外进行诚实挖矿的矿工的收益增加.

4.2.2 理性区块截留攻击

经典的区块截留攻击者是非理性的, 纯粹为了破坏目标矿池, 不考虑个人的收益是否增加. 但对于一个理性的攻击者, 攻击的目的是增加自己的收益. 通过经典区块截留攻击的分析可以看到目标矿池外的矿工的收益是增加的, 基于这一结论攻击者可以利用部分算力去攻击, 剩余算力诚实挖矿, 是否能获得额外收益?

文献 [5] 在 Sabotage 攻击的基础上提出了一种新的区块截留攻击行为, 攻击者 (多个恶意矿工的集合) 利用自己一部分算力对矿池发动区块截留攻击, 另一部分算力在矿池外诚实挖矿, 结合具体的数值证明了这种这种攻击相比于诚实挖矿能够获得额外收益, 进一步证明了当攻击者利用自己一半的算力发动攻击时, 获得的收益最大. 但是它只分析了基于比特币网络整体作为一个开放矿池被攻击这一特定的场景的收益情况. 文献 [6] 构造了一种新的分布式计算模型 (CPS Game): 多个管理者互相竞争解决计算难题来获得最终收益, 利用此模型研究比特币系统的挖矿问题, 分析了多种场景下区块截留攻击的收益情况, 并在实际的比特币系统上验证有关结论的正确性. 定义了相对增益来表示相对于诚实挖矿区块截留攻击的收益增加幅度. 图4列出了 4 种攻击场景, 下面具体分析收益情况.

场景 1: 比特币网络整体作为一个开放矿池

攻击者算力为 α, 其余的矿工组成矿池挖矿, 算力为 $(1-\alpha)$, 攻击者利用 β 比例的自身算力攻击矿池, 剩余的算力诚实挖矿, 那么网络总算力变为 $(1-\alpha\beta)$.

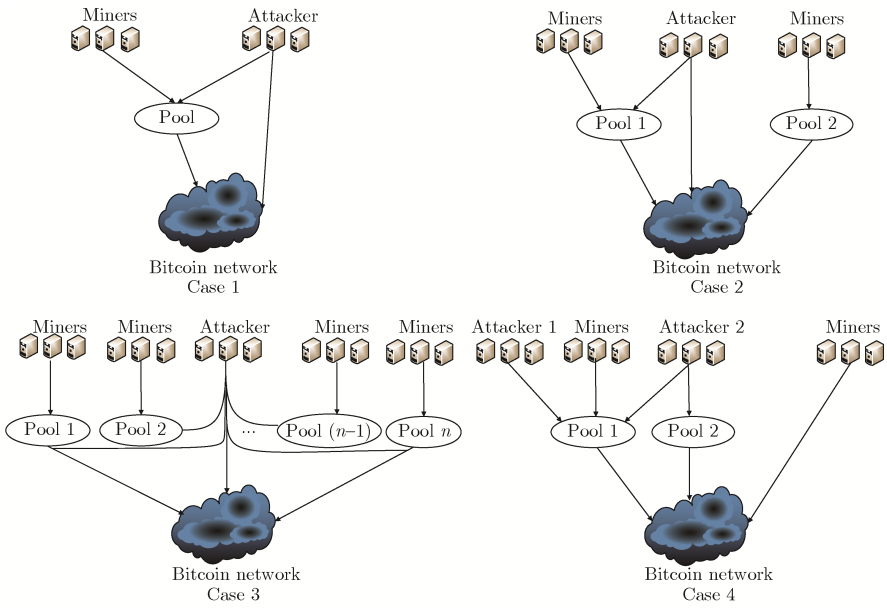


图 4 理性区块截留攻击

Figure 4 Rational block withholding attack

攻击者的总收益:

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

攻击者的相对增益:

$$\Delta_R = \frac{R}{R_h} - 1 = \frac{\alpha\beta(1-\alpha)(1-\beta)}{(1-\alpha\beta)(1+\alpha\beta-\alpha)}$$

可证明 ①$\forall\alpha,\beta\in(0,1),\Delta_R>0$ 即无论攻击者的算力是多少, 利用多少比例的算力进行攻击, 攻击者总会获得比诚实挖矿更多的收益. ②当攻击利用自身 50% 的算力 ($\beta=0.5$) 攻击时, 获得最大的收益.

场景 2: 比特币网络存在多个矿池, 攻击者只攻击其中一个

假设比特币网络中存在着 2 个矿池, 矿池 1、矿池 2, 矿池 1 为目标矿池, 矿池 2 为封闭矿池, 攻击者自身算力为 α, 利用 β 比例的算力攻击矿池 1. 其算力分布如表1所示:

表 1 挖矿算力分布

Table 1 Mining power distribution

	矿池 1	矿池 2	单独挖矿	总算力
攻击者	$\alpha\beta$	0	$\alpha(1-\beta)$	α
诚实矿工	p'	$1-p'-\alpha$	0	$1-\alpha$
矿池总算力	$p=p'+\alpha\beta$	$1-p'-\alpha$	$\alpha(1-\beta)$	1

攻击者的相对增益:

$$\Delta_R = \frac{R}{R_h} - 1 = \frac{\alpha\beta(p-\beta)}{p(1-\alpha\beta)}$$

可证明: ① 无论攻击者和目标矿池的算力是多少, 攻击者选择合适比例的算力去发动攻击, 总会获得额外收益. ② 攻击者用来攻击的算力比例低于某个值 ($\beta<p'/1-\alpha$) 时, 发动攻击才会获得更多的收益. ③ 给定攻击者的算力和用于攻击的算力比例时, 攻击算力大的矿池能够获得更多收益. ④ 给定攻击者和目标矿池算力时, 存在着一个最优攻击策略即攻击者选择某个 β 值使得发动攻击能够获得最大收益.

场景 3: 多个矿池, 攻击者可能攻击多个矿池

当攻击者攻击矿池的算力比例 β 小于某个值时, 发动攻击总会获得额外收益, 并且外部矿池的收益也会增加, 因此攻击者应当攻击每一个矿池以求获得最高收益. 在此场景中攻击者应攻击每一个矿池, 并找到最优的算力分配 (用于攻击每个矿池的算力比例) 使得收益最大.

场景 4: 存在多个攻击者

在场景 2 的基础上, 矿池 1 内已经存在攻击者的情况下又被其它攻击者攻击, 此时场景 2 的结论 ①–④ 同样成立.

4.2.3 矿工困境

攻击者利用区块截留攻击可以减少目标矿池的收益, 同时增加自己的收益, 矿池为了追求利益也可能派出隶属于自己的矿工去攻击其它矿池, 此时矿工会面临矿工困境, 即比特币矿工版本的囚徒困境. 在矿工困境下, 矿工可以选择攻击其他矿工, 或者不攻击独自诚实挖矿. 任何一个开放的矿池可以通过攻击其他矿池, 增加自己的收益, 如果他们都选择攻击对方, 那么他们获得的收益要少于他们在都不选择攻击对方的情况下获得的收益. 定义了收益密度 (矿池中矿工的平均收益与它诚实挖矿时平均收益的比率) 来衡量收益的变化情况. 下面具体分析矿工困境 [7]:

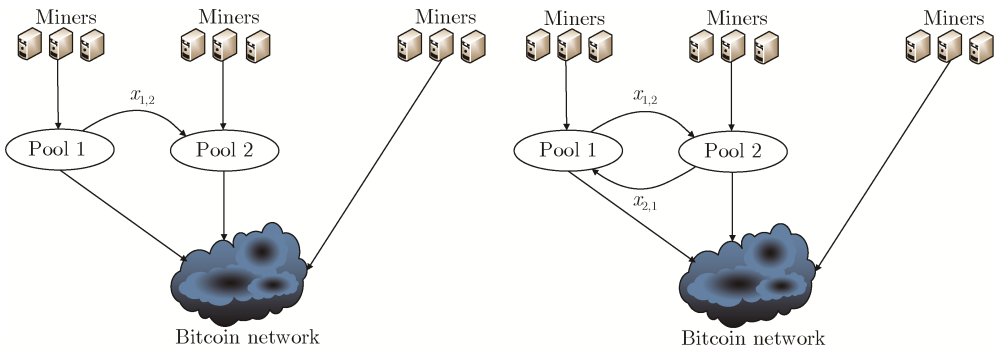


图 5 矿工困境

Figure 5 Miner's dilemma

(1) 单方攻击

比特币网络存在两个矿池: 矿池 1 和矿池 2, 矿池 1 可以攻击矿池 2, 矿池 2 不能攻击矿池 1, 矿池外的矿工单独挖矿. 矿池 1 的算力为 m_1, 矿池 2 的算力为 m_2. 矿池 1 攻击矿池 2 的算力为 $x_{1,2}$.

矿池 1 的收益密度: $r_1 = \frac{m_1(m_2+x_{1,2})-x_{1,2}^2}{m_1(m-x_{1,2})(m_2+x_{1,2})}$

矿池 1 管理者为了获得最大的收益, 应选择一个合适的值 $x_{1,2} \in [0, m_1]$, 使得 r_1 最大. 因为矿池 2 不能对于矿池 1 的攻击作出反应, 系统达到稳定状态. 此时矿池 1 的收益大于诚实挖矿收益, 矿池 2 的收益小于诚实挖矿收益.

(2) 双方互相攻击

在上面的场景的基础上, 矿池 2 也派出去 $x_{2,1}$ 的算力攻击矿池 1. 此时矿池 1、矿池 2 的收益密度分别为: $r_1(x_{1,2}, x_{2,1}) = \frac{m_2R_1+x_{1,2}(R_1+R_2)}{m_1m_2+m_1x_{1,2}+m_2x_{2,1}}$, $r_2(x_{2,1}, x_{1,2}) = \frac{m_1R_2+x_{2,1}(R_1+R_2)}{m_1m_2+m_1x_{1,2}+m_2x_{2,1}}$. 在两个矿池相互攻击游戏中, 每个矿池都会调整自己的攻击算力来使得自己的收益最大. 矿池 1 在第 t 步, 它会选取合适的 $x_{1,2}$ 达到最大收益, 即 $x_{1,2}(t) \leftarrow \arg\max_{x'} r_1(x', x_{2,1}(t-1))$, 相应的矿池 2 在第 t 步, 它也会选取合适的 $x_{2,1}$ 达到最大收益即 $x_{2,1}(t) \leftarrow \arg\max_{x'} r_2(x', x_{1,2}(t-1))$. 当两个矿池都不能改变攻击算力来增加收益时达到平衡状态, 即在满足 $0 < x_1' < m_1, 0 < x_2' < m_2$ 的限制条件下, 存在 x_1', x_2' 使得

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

文献 [7] 结合具体的数值分析矿池 1、矿池 2 在不同算力情况下互相攻击达到平衡状态时的收益密度, 在矿池的算力不会超过 50% 的条件下, 矿池 1、矿池 2 的收益都小于他们都不攻击时的收益, 从而证明矿工困境的存在.

在单轮游戏中, 矿池因为不知道对方是否攻击, 为了避免自己的收益受到更大损失而选择攻击对方. 但是矿池间可进行多轮挖矿竞争形成超级游戏, 游戏的每一轮矿池可能选择攻击或者不攻击. 因此矿池可以约定都不攻击, 并通过检测自己是否受到攻击来推断是否有人破坏约定, 此时矿池达到稳定状态.

4.2.4 赞助区块截留攻击

赞助区块截留攻击基本思想: 攻击者可以与某个矿池合谋并在他的雇佣支持下派出一定比例的算力去攻击目标矿池, 攻击者找到 FPOW 后提交给自私矿池, 减少目标矿池矿工挖到区块的概率, 间接增加自私矿池挖到区块的概率, 当然攻击者诚实挖矿部分算力挖到区块的概率也增加. 这种情况下, 攻击者应当从自私矿池中获得一定的收益, 这个收益与因为发动攻击而引起的自私矿池收益的增加量成正比 [8]. 在之前的讨论中, 攻击者除了自己诚实挖矿的收益外仅能从目标矿池中分得的收益, 因此, 赞助区块截留攻击者的预期收益应当高于文献 [6] 中攻击者的收益. 文献 [8] 定量分析了比特币网络只有两个矿池的场景中, 攻击者攻击 1 个矿池和同时攻击 2 个矿池情况下的收益, 得出一些有趣的结论: ①攻击者能够采取合适的攻击策略来最大化自己的利益. ②当矿池算力保持固定时, 攻击者应当同时攻击两个矿池来获得更多收益. ③当满足某些条件时, 相比于独立诚实挖矿, 攻击者应当利用全部算力发动攻击来获得更多收益. ④当矿池算力不固定时, 满足一些条件, 攻击者同时攻击两个矿池来获得更多收益.

4.3 攻击危害及对策

区块截留攻击违反了比特币协议的要求, 对任何开放矿池具有很大的破坏性, 侵害了诚实矿工的利益, 减弱了挖矿的积极性, 同时越来越多的矿工截留区块, 会使得比特币系统的安全性面临更大威胁. 2014 年 6 月, Eligius 矿池遭受区块截留攻击, 损失 300 比特币 [5]. 那么如何应对这种攻击行为呢? 对矿工进行审核登记, 严格矿工准入审查等措施虽然有效但是不利于矿工的流动, 与比特币系统去中心化、去信任化的要求相违背. Rosenfeld [4] 提出了一种蜜罐技术, 管理者生成一个已知挖矿难题解答的挖矿任务交给所有矿工完成, 诱使恶意矿工进入陷阱, 恶意矿工因不提交解答而被管理者识别. 但是这种方案浪费矿工的算力去做没有意义的计算.

当前存在的应对区块截留攻击的方案主要分为两种类型:

(1) 针对矿工自利的特点, 设计新的矿池分配方案, 减少区块截留攻击收益, 使恶意矿工丧失发动攻击的动机. Schrijvers [17] 提出一种激励相容的分配方案, 当提交的份额多于难度目标时, 按算力比例分配收益, 当提交的份额少于难度目标时, 每个份额分配 1/D (D 为挖矿难度值) 的收益, 剩余的收益分配给挖到区块的矿工, 可以鼓励矿工发现区块时立即公布. Bag 和 Sakurai [18] 提出另一种分配方案, 给予实际挖到区块的矿工特殊奖励, 区块截留因为从不提交有效区块而不能获得特殊奖励, 显著减少了攻击者的收益. 攻击者因为无利可图而放弃这种攻击行为. 二者的区别: 第二种方案提交有效区块的矿工总会获得特殊奖励, 第一种方案只有存在矿工未及时提交 PPOW 时, 提交有效区块的矿工才会获得特殊奖励.

(2) 改变比特币挖矿协议, 使矿工无法识别有效区块或者使矿工私藏的区块无效. Rosenfeld [4] 引入 “oblivious share” 的概念, 使矿工无法确定自己提交的份额是否是一个有效的区块, 并提出一个实现该概念的方案. Dash L Jr [19] 提出在当前区块的工作量证明中包含下一个区块候选者的哈希值, Bag 等人 [8] 提出基于加密承诺和基于哈希函数的 2 种方案来使矿工不能区分部分工作量证明和完整工作量证明.

5 自私挖矿

自私挖矿基本思想: 攻击者挖到区块后不立即向比特币网络广播, 继续在此区块后秘密挖矿, 然后有选择性的公布区块, 有时甚至牺牲自身利益, 向网络连续公布区块, 在同其它矿工的竞争中获得胜利, 减少其它人收益, 吸引更多的矿工跟随自己挖矿, 从而获得额外收益.

5.1 攻击策略

以文献 [10] 为例, 分析自私挖矿攻击策略. 攻击者记录自己的与比特币网络公链相对应的 “私链”. 攻击者总是在私链挖矿并保留他私下挖到的区块, 按照一定的策略决定什么时候公布区块. 开始时公链和私

链是一样的, 所有矿工开始在各自的链上挖矿. 若诚实的矿工挖到区块, 那么攻击者立即验证并更新私链; 若攻击者挖到区块, 它不公布而是在私链上链接这个区块, 并在新的区块后面挖矿, 若紧接着诚实矿工也挖到一个区块, 此时公链和私链长度一样, 攻击者立即公布自己的私链, 让两个链进行竞争谁成为主链. 假设攻击者的哈希算力 α, 诚实矿工的哈希算力 $(1-\alpha)$, 当比特币网络同时存在着两个广播的区块时, 诚实矿工中紧跟着攻击者的区块继续挖矿的矿工所占的比例为 γ. 图6 阐述了存在自私挖块时, 比特币系统状态的转化过程. 系统的状态表示私链领先公链的区块的数目, 当私链和公链一样长时, 又分为状态 0 和状态 $0'$.

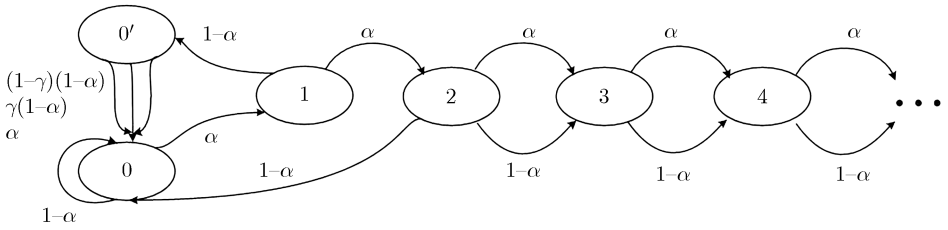


图 6 自私挖矿状态机转换
Figure 6 State machine of selfish mining

状态 0: 开始时攻击者的私链和比特币网络公链一样, 攻击者在私链上挖矿, 诚实矿工在公链上挖矿. 若攻击者挖到一个区块, 系统状态提升到状态 1 (领先私链 1 块), 概率为 α; 若诚实矿工挖到一个区块, 攻击者就更新他的私链和公链一样, 概率为 $(1-\alpha)$, 系统状态保持不变.

状态 1: 攻击者的私链领先公链 1 块, 攻击者在私链上挖矿, 私链没有公开. 若攻击者又挖到一个区块, 系统提升到状态 2 (领先公链 2 块), 概率为 α; 若诚实矿工挖到一个区块, 系统状态转到状态 0', 概率为 $(1-\alpha)$.

状态 $0'$: 当攻击者的私链领先公链 1 个区块时, 攻击者在私链上挖矿, 诚实矿工在公链挖矿. 然后诚实矿工挖到 1 个区块并广播, 此时攻击者立即广播他私藏的区块, 比特币网络同时存在两个长度一样且相互抵触的链. 下一步会出现三种情况: 攻击者挖到下一个区块, 私链成为主链, 攻击者获得 2 个区块的块奖励, 系统复位到状态 0, 概率为 α; 一部分诚实矿工在攻击者的私链上挖矿并挖到 1 个区块, 攻击者和这部分矿工获得 1 个区块的块奖励, 系统复位到状态 0, 概率为 $(1-\alpha)\gamma$; 另一部分诚实矿工在公链上挖矿并找到一个区块, 他们获得 2 个区块的块奖励, 系统复位到状态 0, 概率为 $(1-\alpha)(1-\gamma)$.

状态 2: 攻击者挖到 1 个区块, 系统提升到状态 3, 并获得 1 个区块的块奖励, 概率为 α; 诚实矿工挖找到一个区块, 此时攻击者立即广播他的私链, 同公链竞争获得优势, 攻击者的私链成为主链, 攻击者获得 2 个区块的块奖励, 概率为 $(1-\alpha)$.

状态 n $(n>2)$: 攻击者挖到 1 个区块, 系统提升到状态 (n+1) 并获得 1 个区块的块奖励, 概率为 α; 诚实矿工挖到 1 个区块, 系统后退到状态 $(n-1)$, 概率为 $(1-\alpha)$.

5.2 攻击分析

自私攻击者是如何获利的呢? 攻击者挖到区块时不公布, 然后在私链上挖矿, 并争取使自己的私链一旦公布能够成为主链, 作废诚实矿工挖到的区块, 浪费诚实矿工的算力来增加自己的收益. 当同时存在着两个分支时, 攻击者采取一些手段, 如 Sybil 攻击 [20] 来使得更多的诚实矿工在自己的分支挖矿, 增加成为主链的概率.

文献 [10] 指出攻击者获利情况由攻击者算力占比 α 和追随者占比 γ (即诚实结点和攻击者分别生成的 2 个合法区块同时广播时, 诚实节点支持攻击者的比例) 决定, α、γ 满足公式2 发动攻击可以获得额外收益. 在理想情况下 $\gamma=100\%$ 时, 即存在竞争时所有诚实的矿工都跟随攻击者的区块继续挖矿的情况下, 无论攻击者矿池的算力是多少总是能够获利 (收益超过攻击者诚实挖矿). 当 $\gamma=50\%$ 时, 攻击者算力达到 25% 即可通过自私挖矿获得额外收益. 当 $\gamma=0$ 时, 即没有任何诚实矿工跟随攻击者挖矿, 攻击者算力 $\alpha>1/3$ 总会获得额外收益.

$$\frac{1-\gamma}{3-2\gamma} < \alpha < \frac{1}{2} \tag{2}$$

5.3 攻击危害及对策

比特币的设计者隐含地假设了挖矿协议的公平性: 超过一半的矿工遵循协议, 矿工获得下一个块奖励的概率与该矿工的算力比例成正比, 但是自私挖矿打破了这一假设. 矿工采取自私挖矿能够增加自己的收益, 且收益增加速度与挖矿算力是超线性关系, 特别是具有更快区块传播速度的矿工即使算力再小也可发动自私挖矿获得更多收益, 理性的矿工倾向于进行自私挖矿, 这破坏了比特币去中心化的结构. 另外结合自私挖矿, 双花攻击不必满足 51% 算力就能够发起, 比特币的信任体系面临更大威胁.

现在针对自私挖矿的防御方案主要分为两种:

(1) 对区块有效性规则进行改变. Bahack [11] 提出了一种分叉惩罚规则, 竞争区块没有区块奖励, 包含分叉区块证明的第一个矿工获得惩罚奖励的一半, 但是这种方案会导致诚实矿工受到损害. Shult [21] 为有效区块附加一定量的签名来证明这个区块被网络认可并且网络中不存在竞争区块. Solat 和 Potop-Butucar [22] 提出利用零块来应对自私挖矿, 其基本思想是在一定时间内, 诚实节点或者接收别人的区块或者生成并广播自己的区块, 如果以上情况都没有发生, 该节点生成一个包含预期时间索引和前一区块哈希值的虚拟区块 (零块). 当某个时刻自私节点公布了私藏的区块, 因为不包含零块的哈希值而被诚实节点拒绝. 但是这两种方案都没有提供一种机制来评估有效区块的证明是否充足. Zhang 和 Preneel [23] 从分叉时节点如何选择这一方面着手, 提出一种新的分叉解决策略 (FRP): 用权重 FRP 来替换当前使用的长度 FRP. 在此方案中, 作者改变了挖矿算法并定义了区块链权重的概念, 矿工在面对分叉时比较链的权重而不是长度, 选择在权重大的链上挖矿, 当权重相同时随机选择, 对于自私矿工来说, 无论是否公布区块, 公链和私链的权重同时增加或减少. 这个方案是基于特定的威胁模型, 而实际的比特币网络更复杂, 仍不能保证绝对公平, 但优于现存的方案.

(2) 当公链与私链长度相等时, 增加诚实矿工在公链挖矿的概率, 从而提高攻击者发动攻击获利的算力阈值. Eyal 和 Sirer [10] 提出当一个矿工发现两个相同长度的分支正在竞争时, 矿工应该随机的选择一个分支进行挖矿, 此时的阈值 ($\alpha > 25\%$), 在文献 [12] 最优自私挖矿策略下采用此方案阈值为 23.21%. Heilman [24] 提出 “Freshness Preferred” (FP) 方案, 利用不可伪造的时间戳惩罚隐藏区块的矿工来减少自私挖矿的收益, 从而提高阈值 ($\alpha > 32\%$), 但是此方案引入了额外信任方违背比特币去中心化的思想.

6 FAW 攻击

6.1 攻击概述

FAW 攻击基本思想: 当外部矿工 (既不属于攻击者又不属于目标矿池) 找到区块时, 若攻击者手上握有有效区块应当立即公布产生分叉, 攻击者分支有一定的概率成为主链, 能够获取收益. FAW 攻击相比于区块截留攻击额外获得了分叉后成为主链的那部分收益, 所以 FAW 攻击总会获得额外收益, 且收益不小于区块截留攻击收益. 在实际的矿池攻击行为中, 每个矿池使用 FAW 攻击的次数几乎是 BWH 攻击的 4 倍, 当考虑多个矿池时, FAW 攻击比区块截留攻击的收益增加 56%, 而且两个矿池互相进行 FAW 攻击时, 不存在矿工困境, 在某种情况下大矿池总是能获利 [14].

6.2 攻击分析

以攻击单个目标矿池为例进行分析. 攻击者分配自己的算力进行诚实挖矿和攻击目标矿池. 如果通过诚实挖矿找到一个区块, 它立即广播获得收益. 如果它在目标矿池中找到一个区块, 不立即广播, 可以采取以下三种行为: (1) 当攻击者诚实挖矿挖到另一个区块, 它抛弃在目标矿池中找到的区块; (2) 当目标矿池的诚实矿工找到区块, 攻击者抛弃找到的区块; (3) 当外部的矿工找到一个区块, 攻击者手立即向目标矿池管理者提交区块, 比特币网络同时存在两个区块, 产生分叉; 可以看出 1、2 就是 BWH 攻击, FAW 攻击多第三种情况. 图7列出了攻击一个矿池出现的四种情况.

假设攻击者算力为 α, 目标矿池的算力为 β, 攻击者参与攻击的算力的比例为 τ, 分叉时攻击者区块成为主链的概率为 c. 图7中四种情况出现的概率:

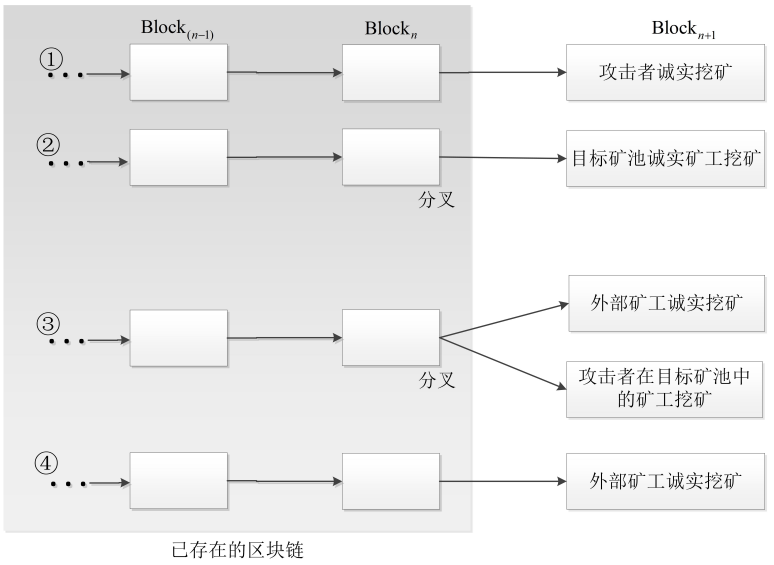


图 7 FAW 攻击结果的四种情况 (攻击一个矿池)
Figure 7 Four cases of FAW attack results against one pool

①攻击者诚实挖矿找到区块: $\frac{(1-\tau)\alpha}{1-\tau\alpha}$
②目标矿池中诚实矿工找到一个区块: $\frac{\beta}{1-\tau\alpha}$
③外部诚实矿工找到一个有效区块, 攻击者立即公布自己的之前发现的区块产生分叉: $\tau\alpha \cdot \frac{1-\alpha-\beta}{1-\tau\alpha}$
④外部诚实矿工找到一个有效区块, 攻击者没有找到区块: $1-\alpha-\beta$
攻击者在情况①–③发生时获得收益, 包括诚实挖矿的收益和在目标矿池中分配的收益:

$$R_\alpha(\tau) = \frac{(1-\tau)\alpha}{1-\tau\alpha} + \left(\frac{\beta}{1-\tau\alpha} + c\tau\alpha \cdot \frac{1-\alpha-\beta}{1-\tau\alpha}\right) \cdot \frac{\tau\alpha}{\beta+\tau\alpha}$$

目标矿池在情况②③发生时获得收益:

$$R_p(\tau) = \frac{\beta}{1-\tau\alpha} + c\tau\alpha \cdot \frac{1-\alpha-\beta}{1-\tau\alpha}$$

收益分析: ①攻击者的收益 R_α 是关于 τ 的函数, 求导得到 $\bar{\tau}$ 使攻击者收益最大即当攻击者应当利用 $\bar{\tau}$ 比例的算力攻击时将获得最大收益. 当 $c=0$ 时, 即攻击者公布自己握有的区块并产生分叉, 它的区块成为主链的概率为 0, 此时所获得的收益等于发动区块截留攻击所获得的收益. 而区块截留攻击选择合适比例的算力所获得的收益总是大于诚实探矿的. 又因为 R_α 是一个相对于 c 的递增函数, 无论攻击的算力为多少都会获得额外收益. 因此 FAW 攻击相比于诚实挖矿总会获得更多收益, 且收益不小于 BWH 攻击所获得收益.

②可以证明 $R_p < \beta + \tau\alpha$ 总是成立, 所以目标矿池受 FAW 攻击时收益总会受到损失. 又因为 R_p 相对于参数 c 是线性递增的, 所有矿池的损失是随着 c 的增大而减小, 因此矿池管理者应该尽可能快的传播自己找到的区块增加成为主链的概率以减少自己的损失, 但这同时也会增加攻击者的收益.

文献 [14] 进一步分析了攻击者同时攻击 2 个矿池的收益情况, 并拓展到 n 个矿池, 给出了攻击者收益的表达式, 并证明结论①②同样满足. 2 个矿池互相进行区块截留攻击时存在纳什均衡和矿工困境, FAW 攻击是否也是同样的情况? 文献 [14] 分析并证明了 2 个矿池互相进行 FAW 攻击能够达到纳什均衡, 均衡点落在满足 $\frac{\partial R_1}{\partial f_1}=0$, $\frac{\partial R_2}{\partial f_2}=0$ (f_1、f_2 是矿池 1、矿池 2 用来攻击对方的算力值) 的点上或者满足限制条件的边界上, 但是矿工困境不存在, 算力大的矿池总会获得额外收益.

表 2 挖矿攻击汇总表
Table 2 Summary of mining attack

攻击类型	攻击条件	攻击危害	防御措施
51% 攻击	攻击者拥有 51% 算力	实现双花	监管矿池发出的大额交易和算力变化; 大额交易时多等几个确认区块
区块截留攻击	攻击者选取合适比例攻击算力 (与自身算力和目标矿池算力有关)	损害诚实矿工和矿池的利益	设计合理的矿池分配方案; 改变比特币挖矿协议, 使矿工无法识别有效区块或者使矿工私藏的区块无效
自私挖矿攻击	攻击者具备一定的算力和较好的网络条件, 满足公式 (2)	损害诚实矿工和矿池的利益, 攻击者算力不必满足 50% 就能发动 51% 攻击	改变区块有效性规则, 使攻击者无法识别有效区块或者无效掉私藏的区块; 改变分叉解决策略, 提高攻击者获利的算力阈值
FAW 攻击	攻击者具备一定的算力和较好的网络条件	兼具区块截留攻击和自私挖矿攻击的危害	适用区块截留攻击和自私挖矿的防御措施

7 结束语

本文介绍了比特币系统常见的 4 种挖矿攻击, 见表2, 分析其攻击原理和现实危害, 并对当前存在的防范攻击的措施进行了介绍, 使人们对比特币的安全性有了更深入的认识. 作为出现最早、市值最高、用户最多的数字货币, 比特币的发展面临的威胁越来越多, 比特币系统的安全问题应当受到更广泛的重视, 针对比特币共识机制 (挖矿) 的攻击和防御措施研究仍是比特币安全问题研究的重点. 希望本文的总结对以后的研究工作有一定的推动作用.

References

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. https://bitcoin.org/bitcoin.pdf. 2008.
[2] POON J, DRYJA T. The Bitcoin lightning network: Scalable off-chain instant payments[EB/OL]. http://lightning.network/lightning-network-paper.pdf. 2016.
[3] ZHU L H, GAO F, SHEN M, et al. Survey on privacy techniques for blockchain technology[J]. Journal of Computer Research and Development, 2017, 54(10): 2170–2186. [DOI: 10.7544/issn1000-1239.2017.20170471]
祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述 [J]. 计算机研究与发展, 2017, 54(10): 2170–2186. [DOI: 10.7544/issn1000-1239.2017.20170471]
[4] ROSENFELD M. Analysis of Bitcoin pooled mining reward systems[J]. arXiv preprint arXiv:1112.4980, 2011.
[5] COURTOIS N T, BAHACK L. On subversive miner strategies and block withholding attack in Bitcoin digital currency[J]. arXiv preprint arXiv:1402.1718, 2014.
[6] LUU L, SAHA R, PARAMESHWARAN I, et al. On power splitting games in distributed computation: The case of Bitcoin pooled mining[C], In: 2015 IEEE 28th Computer Security Foundations Symposium—CSF 2015. IEEE, 2015: 397–411. [DOI: 10.1109/CSF.2015.34]
[7] EYAL I. The miner's dilemma[C]. In: 2015 IEEE Symposium on Security and Privacy (SP). IEEE, 2015: 89–103. [DOI: 10.1109/SP.2015.13]
[8] BAG S, RUJ S, SAKURAI K. Bitcoin block withholding attack: Analysis and mitigation[J]. IEEE Transactions on Information Forensics & Security. 2017, 12(8): 1967–1978. [DOI: 10.1109/TIFS.2016.2623588]
[9] Btchris Bytecoin. Mtgox, RHorning: Mining cartel attack[EB/OL]. https://bitcointalk.org/index.php?topic=2227. 2010.
[10] EYAL I, SIRER E G. Majority is not enough: Bitcoin mining is vulnerable[C]. In: Financial Cryptography & Data Security—FC 2014. Springer Berlin Heidelberg, 2014: 436–454. [DOI: 10.1007/978-3-662-45472-5_28]
[11] BAHACK L. Theoretical Bitcoin attacks with less than half of the computational power (draft)[J]. arXiv preprint arXiv:1312.7013, 2013.
[12] SAPIRSHTEIN A, SOMPOLINSKY Y, ZOHAR A. Optimal selfsh mining strategies in Bitcoin[C]. In: Financial Cryptography and Data Security—FC 2016. Springer Berlin Heidelberg, 2016: 515–532. [DOI: 10.1007/978-3-662-54970-4_30]
[13] NAYAK K, KUMAR S, MILLER A, et al. Stubborn mining: Generalizing selfish mining and combining with an

eclipse attack[C]. In: 2016 IEEE European Symposium on Security and Privacy. IEEE, 2016: 305–320. [DOI: 10.1109/EuroSP.2016.32]

[14] KWON Y, KIM D, SON Y, et al. Be selfish and avoid dilemmas: Fork after withholding (FAW) attacks on Bitcoin[C]. In: 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017: 195–209. [DOI: 10.1145/3133956.3134019]

[15] YU H, ZHANG Z Y, LIU J W. Research on scaling technology of Bitcoin blockchain[J]. Journal of Computer Research and Development, 2017, 54(10): 2390–2403. [DOI: 10.7544/issn1000-1239.2017.20170416]
喻辉, 张宗洋, 刘建伟. 比特币区块链扩容技术研究 [J]. 计算机研究与发展, 2017, 54(10): 2390–2403. [DOI: 10.7544/issn1000-1239.2017.20170416]

[16] YUAN Y, WANG F Y. Blockchain: The state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481–494. [DOI: 10.16383/j.aas.2016.c160158]
袁勇, 王飞跃. 区块链技术发展现状与展望 [J]. 自动化学报, 2016, 42(4): 481—494. [DOI:10.16383/j.aas.2016.c160158]

[17] SCHRIJVERS O, BONNEAU J, BONEH D, et al. Incentive compatibility of Bitcoin mining pool reward functions[C]. In: Financial Cryptography & Data Security—FC 2016. Springer Berlin Heidelberg, 2016: 477–498. [DOI: 10.1007/978-3-662-54970-4_28]

[18] BAG S, SAKURAI K. Yet another note on block withholding attack on Bitcoin mining pools[C]. In: Information Security—ISC 2016. Springer Cham, 2016: 167–180. [DOI: 10.1007/978-3-319-45871-7_11]

[19] DASH L Jr. Defeating the block withholding attack[EB/OL]. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2012-June/001506.html.

[20] DOUCEUR J R. The sybil attack[C]. In: Peer-to-Peer Systems—IPTPS 2002. Springer Berlin Heidelberg, 2002: 251–260. [DOI: 10.1007/3-540-45748-8_24]

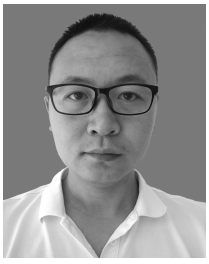
[21] SHULTZ B L. Certification of witness: Mitigating blockchain fork attacks[EB/OL]. http://bshultz.com/paper/Shultz Thesis.pdf.

[22] SOLAT S, POTOP-BUTUCARU M. Zeroblock: Preventing selfish mining in Bitcoin[J]. arXiv preprint arXiv:1605.02435, 2016.

[23] ZHANG R, PRENEEL B. Publish or perish: A backward-compatible defense against selfish mining in Bitcoin[C]. In: Cryptographers' Track at the RSA Conference—CT-RSA 2017. Springer Cham, 2017: 277–292. [DOI: 10.1007/978-3-319-52153-4_16]

[24] HEILMAN E. One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner[C]. In: Financial Cryptography & Data Security—FC 2014. Springer Berlin Heidelberg, 2014: 161–162. [DOI: 10.1007/978-3-662-44774-1_12]

作者信息



韩健 (1986–), 山东济宁人, 硕士研究生. 主要研究领域为区块链和数字货币.
174223317@qq.com

邹静 (1979–), 山东烟台人, 博士后, 高级工程师. 主要研究领域为网络与信息安全.
zoujingpaper@126.com

蒋瀚 (1974–), 山东济南人, 博士, 讲师. 主要研究领域为密码学理论、格密码和密码协议.
jianghan@sdu.edu.cn

徐秋亮 (1960–), 山东济南人, 博士, 教授. 主要研究领域为公钥密码学.
xql@sdu.edu.cn