软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(5):1495−1525 [doi: 10.13328/j.cnki.jos.006213]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链系统攻击与防御技术研究进展*

田国华, 胡云瀚, 陈晓峰

(西安电子科技大学 网络与信息安全学院,陕西 西安 710071)

通讯作者: 陈晓峰, E-mail: xfchen@xidian.edu.cn

摘 要: 区块链作为一种多技术融合的新兴服务架构,因其去中心化、不可篡改等特点,受到了学术界和工业界的广泛关注.然而,由于区块链技术架构的复杂性,针对区块链的攻击方式层出不穷,逐年增加的安全事件导致了巨大的经济损失,严重影响了区块链技术的发展与应用.从层级分类、攻击关联分析两个维度对区块链已有安全问题的系统架构、攻击原理、防御策略展开研究.首先,按照区块链层级架构对现有区块链攻击进行归类,介绍了这些攻击方式的攻击原理,分析了它们的共性与特性;其次,分析总结了已有解决方案的思路,提出了一些有效的建议和防御措施;最后,通过攻击关联分析归纳出多个区块链攻击簇,构建了一个相对完整的区块链安全防御体系,展望了区块链技术在未来复杂服务场景下的安全态势.

关键词: 区块链;去中心化;不可篡改性;区块链安全;区块链攻击簇

中图法分类号: TP309

中文引用格式: 田国华,胡云瀚,陈晓峰.区块链系统攻击与防御技术研究进展.软件学报,2021,32(5):1495−1525. http://www.jos.org.cn/1000-9825/6213.htm

英文引用格式: Tian GH, Hu YH, Chen XF. Research progress on attack and defense techniques in block-chain system. Ruan Jian Xue Bao/Journal of Software, 2021,32(5):1495−1525 (in Chinese). http://www.jos.org.cn/1000-9825/6213.htm

Research Progress on Attack and Defense Techniques in Block-chain System

TIAN Guo-Hua, HU Yun-Han, CHEN Xiao-Feng

(School of Cyber Engineering, Xidian University, Xi'an 710071, China)

Abstract: Blockchain, as an emerging service architecture integrating multi-technology, has attracted extensive attention from the academia and industry due to its decentralization and immutability. However, blockchain is vulnerable to various attacks due to its complex architecture, and the increasing security incidents year by year lead to huge economic losses, which seriously hampers the development and application of blockchain technology. This work studies the architecture, principle, and defenses of existing blockchain attacks from two dimensions of hierarchical classification and attack association analysis. Firstly, the existing blockchain attacks are classified according to the hierarchical structure of the blockchain, the attack principles of these attacks are introduced, and their commonness and characteristics are analyzed. Secondly, some efficient defenses are given based on the analysis and summary of the existing solutions. Finally, this study constructs a comprehensive blockchain defense system based on several blockchain attack clusters summarized by attack association analysis, and prospects the security situation of blockchain in complex service scenarios in the future.

Key words: block-chain; decentralization; immutability; block-chain security; block-chain attack cluster

区块链是一种基于 P2P(peer to peer)网络、共识机制、密码学技术、智能合约等多种计算机技术的分布式账本技术,其多元融合的技术架构赋予了自身公开透明、去中心化、不可篡改和可编程等技术特点,为解决传统服务架构中的信任问题和安全问题提供了新思路,给社会传统行业的快速发展带来了新的契机.因此,区块链

* 基金项目: 山东省重点研发计划(2019JZZY020129)
Foundation item: Shandong Provincial Key Research and Development Program (2019JZZY020129)
收稿时间: 2020-07-30; 修改时间: 2020-10-20; 采用时间: 2020-11-29; jos 在线出版时间: 2021-01-15

技术的发展受到了学术界和工业界的广泛关注[1−4],其重要性甚至已经上升至我国的国家科技发展战略层面.

然而,区块链的多技术融合架构在赋予区块链技术多种优良技术特性的同时,也因为自身结构的复杂性和应用场景的多样性,而导致区块链面临诸多安全威胁.恶意攻击者可能针对区块链应用的底层技术缺陷、低耦合性等安全漏洞展开攻击,从而非法攫取利益[5].据区块链安全公司派盾(Peck Shield)的数据显示[6]:2019 年全年大约发生了 177 起区块链安全事件,给全球造成的经济损失高达 76.79 亿美元,环比增长了 60%.随着区块链应用进程的不断推进,越来越多的安全问题和攻击方式出现在人们的视野中,其中既存在针对区块链技术架构的普适性攻击方式,例如 51%攻击[7]、双花攻击[8]、交易顺序依赖攻击[9]等,也存在针对特殊场景的特定攻击方式,譬如芬尼攻击[10]、粉尘攻击[11]等.这些安全问题不仅会导致直接的经济损失,还会引起社会各界对区块链技术的质疑,严重影响了区块链技术的发展进程.因此,只有采用有效的防御策略和相关技术,才能保证区块链良好的网络环境,促进区块链技术的快速发展.

本文第 1 节概述区块链技术的系统架构、发展历程及安全态势,按照区块链层级架构对区块链网络中现有的安全问题进行归纳总结,确定层级分类、攻击关联分析两个综述维度.第 2 节~第 6 节从层级分类的横向维度出发,分别从攻击场景、攻击目标、攻击原理等方面分析论述已有区块链攻击的共性与特性,并在分析相应解决方案的同时,给出一些有效的防御策略.第 7 节从攻击关联分析的纵向维度出发,研究跨层级的区块链攻击场景,分析并归纳出一系列的区块链攻击簇,并针对性地构建出一个相对全面的区块链安全防御体系.第 8 节总结全文,评估区块链技术当前的安全态势,展望区块链技术在未来复杂服务场景中面临的机遇与挑战.

1 区块链概述

1.1 区块链简介

2008 年,Nakamoto 首次提出一种基于 P2P 网络、分布式数据存储、共识机制等技术的电子现金系统——比特币[12].该系统允许用户节点自由加入、退出,因此具备公开透明的特点;系统中的节点在不需要中心化机构的情况下,通过 P2P 网络维护分布式账本即可实现点对点的可信交易,所以该系统具备去中心化的特点;全网节点间不需要彼此信任,通过共识机制即可对各节点维护的账本达成一致认知,因此,该系统具备去信任化的特点;在维护账本的过程中,系统中的交易被矿工打包成区块并广播至全网,用户节点根据该区块中存储的上一区块的 hash 值进行链式存储.当入链“深度”超过 6 之后,该区块中的数据将无法被篡改,所以该系统具备不可篡改性[13].因此,比特币可以看作是一个由全网节点集体维护的分布式账本,为解决传统服务架构中的信任问题带来了新思路,在诸多领域中都具有十分重要的研究和应用价值[14].

区块链则是在比特币技术基础上提炼发展而来的新兴技术体系[15],在比特币原有技术架构上增加了智能合约、密码学技术等计算机技术,具备更好的可编程性和数据隐私保护.其发展历程可以大致分为 3 个阶段[16].

- 区块链 1.0,可编程货币时代,这个阶段奠定了区块链技术的理论基础,初步形成了相对完善的技术体系,应用场景主要为数字金融领域,经典应用为比特币.
- 区块链 2.0,可编程应用时代,通过引入新型的共识算法、智能合约等技术,赋予区块链更好的可编程性和兼容性.应用场景由金融服务领域向游戏、医疗、教育等领域延伸,代表应用为以太坊[17].
- 区块链 3.0,可编程社会时代,各行业的区块链应用发生融合,形成以现实社会为依托的区块链生态体系.由 2.0 时代的与行业相结合,转变为与社会相结合.

随着人们对区块链技术的不断重视,无论是区块链技术的理论研究还是应用开发都得到了快速的发展.到目前为止,关于区块链技术的理论研究已经进入 2.0,甚至 3.0 阶段,而区块链的应用开发则处于 1.0 到 2.0 的过渡阶段[18].大量数字货币钱包应用的研发部署以及交易所、商家的出现,使得区块链技术与金融服务行业相结合,形成了一个相对成熟的新支付体系.与此同时,各大银行携手金融科技公司组建区块链大联盟,例如 R3 CEV[19],China Ledger[20]等,通过成立区块链实验室来发展核心业务,尝试对区块链 2.0 阶段展开深入探索,旨在研究区块链技术与传统行业实际应用场景的兼容性,并以此建立区块链在 2.0 阶段的发展标准,加快区块链技术的应用进程.此外,Cisco[21]联合金融及其他行业公司组成超级账本(Hyperledger)[22]联盟,对区块链在 3.0 阶段

展开探索,旨在制定区块链技术未来的发展规划和标准.

1.2 区块链安全态势

区块链的多技术融合架构在赋予自身公开透明、去中心化、不可篡改等特点的同时,也因其复杂性导致区块链面临诸多安全威胁.在区块链 1.0 的应用进程中,区块链技术的安全漏洞在复杂多样的应用场景中愈加明显,攻击者可以针对这些安全漏洞发起恶意攻击,从而非法攫取利益[5].此外,在数据即价值的时代,攻击者的目标不再局限于代币的双花和盗取,蕴涵交易隐私、用户隐私的区块链数据成为了攻击者的新目标.

在区块链网络中,针对相同的安全漏洞或攻击目标,可能存在多种不同的攻击方式.如图 1 所示,根据攻击漏洞或目标所属的区块链层级,可对现有区块链攻击方式做如下分类.

(1) 数据层攻击:数据层、网络层和共识层是区块链技术体系中最基础、最必要的 3 个层级,而数据层是其中最重要的一层,主要涉及区块链的数据结构、数字签名、哈希函数等密码学工具.这些密码学工具在保护区块链数据隐私的同时,其固有的碰撞攻击[23]、后门攻击[24]等安全问题也给区块链数据隐私带来了一定威胁.此外,攻击者也可能通过交易延展性攻击[25]和恶意信息攻击破坏交易秩序和区块链网络环境.因此,区块链数据层面临的安全威胁主要包含数据隐私窃取和恶意数据攻击.

(2) 网络层攻击:网络层是区块链技术体系中最基础的层级,主要包含 P2P 网络组网方式、消息传播协议等模块,赋予了区块链去中心化、不可删除、不可篡改的技术特性.区块链网络层面临的安全威胁主要是针对 P2P 网络的恶意攻击,攻击者可能通过漏洞植入、路由劫持、资源占用等方式扰乱区块链网络的正常运行,也有可能利用交易延迟攻击来破坏区块链网络交易环境.

(3) 共识层攻击:共识层是区块链技术体系的核心架构,其中的共识算法可以保证全网节点在去信任化的场景中对分布式账本数据达成共识,为区块链的去中心化、去信任化提供了保障.共识层面临的安全威胁主要是,攻击者可以通过各种手段阻止全网节点达成正确的共识.在授权共识机制中,各节点对共识过程的影响相同,所以易遭受女巫攻击[26];而在非授权共识机制中,各对等节点利用自身所持资源(如算力、权益)竞争记账权,进而达成共识.投入的资源越多,则成功率越高,因此易遭受 51%攻击.攻击者可能出于利益目的,通过贿赂攻击[27]、币龄累计攻击[28]等方式非法获取大量资源,从而发起 51%攻击,以实现代币双花、历史修复、期货卖空、自私挖矿等目的.此外,攻击者还可以通过无利害关系攻击[29]、预计算攻击[30]等方式影响全网共识进程,进而获利.

(4) 合约层攻击:合约层是区块链实现点对点可信交互的重要保障,主要包括智能合约的各类脚本代码、算法机制等,是区块链 2.0 的重要标志.合约层面临的安全威胁可以分为智能合约漏洞和合约虚拟机漏洞:智能合约漏洞通常是由开发者的不规范编程或攻击者恶意漏洞植入导致的,而合约虚拟机漏洞则是由不合理的代码应用和设计导致的.

(5) 应用层攻击:应用层是区块链技术的应用载体,为各种业务场景提供解决方案,可分为挖矿和区块链交易两类场景.在挖矿场景中,攻击者可能通过漏洞植入、网络渗透、地址篡改等方式攻击矿机系统,从而非法获利;“聪明”的矿工也可能利用挖矿机制的漏洞,通过算力伪造攻击[31]、扣块攻击[32]、丢弃攻击[33]等方式谋求最大化的收益.在区块链交易场景中,攻击者可能利用撞库攻击[34]、0day 漏洞[35]、API 接口攻击[36]等方式非法获取交易平台中用户的隐私信息,也可能通过钓鱼攻击[37]、木马劫持攻击[38]等方式获取用户账户的隐私和资产.

在实际的区块链攻击场景中,攻击者发起攻击旨在非法获取最大化的利益,但并不是所有的区块链攻击方式都可以使攻击者直接获利.此外,部分区块链攻击对实施场景和条件要求过高,使得其可行性受到了严重的制约.因此,攻击者通常采用一系列跨层级的区块链攻击方式来实现最大化的获利目的,本文称这种攻击序列为攻击簇.例如:现实场景中,攻击者利用自身资源发起 51%攻击是不现实的,所以他们可能通过傀儡挖矿[39]、贿赂攻击、币龄累计攻击等方式非法获取记账权竞争资源,然后发起 51%攻击,进而实现双花攻击、历史修复攻击[40]、卖空攻击[41]等.显然,研究区块链安全态势,不仅要从层级分类的横向维度对单个攻击展开分析,还要从攻击关联分析的纵向维度对跨层级的攻击簇进行研究,才有可能构建出全面有效的区块链安全防御体系.

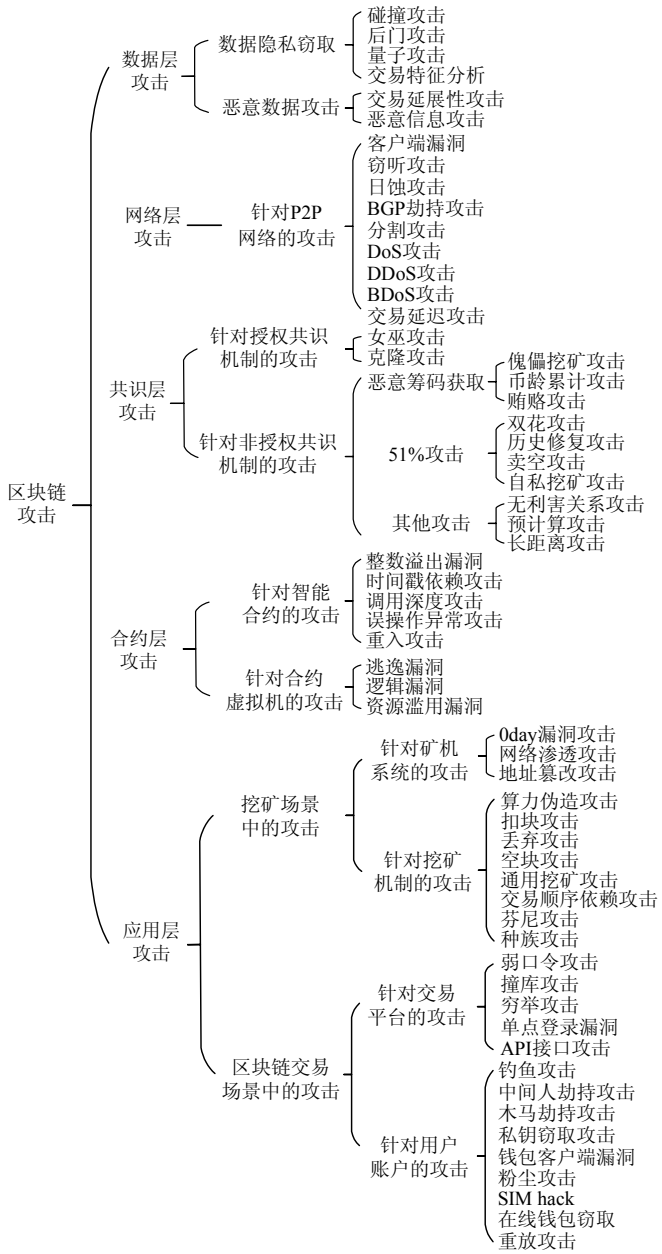


Fig.1 Classification of attacks in block-chain

图 1 区块链攻击分类

2 区块链数据层攻击

数据层是区块链技术中最底层的技术框架,主要封装了区块链中的各式数据结构,其安全性从根本上决定着区块链网络的安全性.本节将从数据隐私窃取和恶意数据攻击两个方面对数据层的潜在安全威胁进行剖析.

2.1 数据隐私窃取

区块链数据层使用了大量的密码学工具来保证区块链数据的不可篡改性和安全性.然而,这些密码学工具

的固有安全隐患给区块链安全性带来了严峻的挑战.此外,区块链网络中用户节点在参与区块链交易、账本维护时需要公开一些信息,如交易内容、交易金额、用户身份等,而这些信息与用户节点的行为特征密切相关,存在泄露用户隐私的风险.因此,区块链网络的数据隐私主要面临以下威胁.

(1) 碰撞攻击(collision attack)[23]:Hash 函数是一种单向散列函数,可以将任意长度的输入转换为固定长度的输出,而其输出值的长度决定了输出值的数量空间.从数学角度来看,从均匀分布的区间[1,d]中随机取出 n 个整数,至少两个数字相同的概率可用如下公式表示:

$$P(d,n)=\begin{cases}1-\prod_{i=1}^{n-1}\left(1-\frac{i}{d}\right), & n\leqslant d\\ 1, & n>d\end{cases},$$

即 Hash 函数中,不同的输入可能会获得相同的输出,这种现象被称为 Hash 碰撞.攻击者可能利用 Hash 函数中存在的 Hash 碰撞发起碰撞攻击,进而实现获取用户数据隐私、破坏区块链系统的目的.

(2) 后门攻击(backdoor attack)[24]:密码算法、零知识证明[42]等工具的使用,保证了区块链数据的机密性和完整性,而在实际的区块链开发过程中,开发人员更倾向于直接调用已有的开源密码算法.这些开源算法中可能存在被植入的后门,这严重威胁到了区块链数据的安全性.比较典型的案例是:美国国家安全局在 RSA 算法中安插后门[43],一旦用户调用了被植入后门的 RSA 算法,攻击者便可以直接通过用户公钥计算得出私钥,进而解密并访问被加密数据.

(3) 量子攻击(quantum attack)[44]:时间复杂度是衡量密码算法相对于现有计算水平安全性的重要指标,而量子计算技术带来的计算能力提升,打破了密码学算法的安全现状.很多原本计算上不可行的恶意攻击,在量子计算的架构下变得可行,这种新的攻击模式被称为量子攻击.量子攻击的出现,将给现有信息安全体系带来毁灭性打击,而与信息安全相关的产业势必受到强烈的冲击.在区块链技术体系中,比特币的挖矿机制、区块链的不可篡改性、区块链数据的机密性等方面都将面临严峻的挑战.

(4) 交易特征分析(transactional analysis)[45]:攻击者通过窃听、木马劫持等手段获取大量的用户公开信息,并对匿名账户进行身份画像,通过用户行为特征分析和交易特征分析相关联的方式,获取目标用户的身份隐私和交易隐私.以比特币为例,用户使用一次性身份(假名)进行匿名交易,而用户资产上的签名是可以被公开验证的.恶意敌手可以通过对用户行为建模分析,分析比对假名信息,从而获取用户的真实身份.Androulaki 等人[46]在学校中设计模拟实验,让学生使用比特币作为日常交易货币,分析人员采用基于行为的聚类技术对比特币交易数据进行分析,发现即使用户采用比特币推荐的隐私保护方法(一次性地址策略),也能够将 40%的学生身份和区块链地址匹配.

2.2 恶意数据攻击

去中心化的分布式架构赋予区块链不可篡改的特性,数据一旦上链,则通过区块链网络广泛流传,并且不可篡改.攻击者可能利用区块链数据结构的技术弱点,通过以下方式影响区块链正常运转,破坏网络环境.

(1) 交易延展性攻击(transaction malleability attack)[25]:以比特币系统为例,攻击者在发出提现交易 A 后,可以在 A 确认之前,通过修改某些交易数据,使得一笔交易的唯一标识(交易哈希)发生改变,得到新交易 B.假设交易 B 先被记录到比特币账本中,那么矿工会认为交易 A 存在双重支付问题,拒绝打包进区块中.此时,攻击者可以向交易所申诉,尝试获取交易 A 中标明的代币数量.一旦申诉通过,则将导致交易所资金大量流失.

(2) 恶意信息攻击(malicious information attack)[47]:随着区块链技术的不断更迭,链上数据内容也不再局限于交易信息,这为一些文件、工程代码,甚至个人敏感信息上链提供了可能.多元化的数据结构和类型在促进区块链技术快速发展的同时,也为恶意信息上链提供了可能.而恶意信息攻击的主要方法就是攻击者在区块链中写入恶意信息,例如病毒特征码、恶意广告、政治敏感话题等,借助区块链分布式的结构广泛流传.由于区块链不可删除、不可篡改的特性,一旦恶意信息被写入区块链,则将导致杀毒软件报毒,或者引起政治敏感等多方面的问题.

2.3 防御策略与方法

数据层攻击的共性在于攻击者均以区块链数据为攻击目标,其特性则在于攻击者攻击目的和攻击原理的不同:数据隐私窃取攻击旨在帮助攻击者获得区块链数据中蕴含的用户隐私,从攻击原理上又可划分为基于密码学工具安全隐患的攻击和基于交易关联分析的攻击;而恶意数据攻击则是攻击者根据区块链的技术弱点或特性生成恶意数据并上链,从而达到妨碍区块链系统正常运行的攻击目的.

从隐私保护的角度来看,尽管当前区块链技术体系中使用的密码学工具都被认为是安全的,只要能在开发过程中确保使用无后门的密码算法,即可保证区块链网络的安全性.但从长远来看,现有密码学工具的安全性势必受到以量子计算为代表的新一代计算技术的冲击,只有在适当的时间节点替换更安全、更高效的密码学工具,才能保证区块链的稳健性和安全性.一方面,尽管区块链使用的 SHA-256 等哈希算法目前是相对安全的,但被攻破只是时间问题,所以必须加快推进安全哈希算法的研究进展,设计具备强抗碰撞性的哈希算法,以保证区块链技术的不可篡改性;另一方面,区块链数据的安全性主要依靠密码算法的安全性,而当前常用的密钥长度为 1 024 位的 RSA 加密算法,在量子攻击下只需几秒即可完成破译,所以必须加快以抗量子密码算法为核心的抗量子区块链技术体系的预研进程,保证区块链技术在后量子时代的安全性和可用性.

此外,虽然当前几乎所有的区块链技术都支持匿名交易,用户的交易地址通常由用户自行创建保存,且与真实身份无关,部分区块链系统尝试利用零知识证明等技术(如 Zcash[48])来保护交易过程中用户的身份隐私,然而,交易数据关联性分析、用户行为习惯分析等技术仍然可以在一定程度上帮助攻击者获取用户的身份隐私和交易隐私.为此,用户节点可以考虑采用以下 3 种防御策略.

(1) 数据混淆:对交易内容的数据进行混淆,降低攻击者获取目标信息的成功率,增加攻击难度.

(2) 数据加密:将交易中的特定信息加密,减少攻击者可获取的信息量,降低其用户身份画像的准确性.

(3) 隐蔽传输:通过隐蔽信道传输对隐私要求较高的交易数据,阻止攻击者获取相关信息.

从区块链数据的角度来看,攻击者之所以可以进行交易延展性攻击,是因为当前大多数挖矿程序采用 OpenSSL 开源软件库校验用户签名,而 OpenSSL 兼容多种编码格式,部分编码方案的实现存在一定的问题.例如:在 OpenSSL 实现的椭圆曲线数字签名算法(ECDSA)中,签名(r,s)和签名$(r,-s(\mathrm{mod}\ n))$都是有效的.因此,只要签名数据没有产生太大的变化,都能够被认为是有效签名.Wuille 等人[49]提出了一种叫做隔离见证(segregated witness)的方法,通过将区块签名信息单独存放,使得区块头的交易哈希值完全由交易信息决定,在交易内容没有发生变化的情况下,即使签名信息被改变,交易哈希也不会发生变化.此时,攻击者只有掌握了私钥,才能改变交易的哈希值.同时,当遇到无法确认的交易时,矿工应该立即停止交易验证,并根据区块链上的交易报错信息,查看是否在短时间内已经发起了这样的交易,再做进一步处理.

此外,攻击者实施恶意信息攻击则是因为区块链网络中不存在可以审查上链数据的独立节点,简单增加内容监管节点的方式势必会弱化区块链网络的去中心化特性,不具备可行性.所以可以尝试以下方法和策略.

(1) 从区块链通用模型设计入手,通过设计特定的区块结构来限制可存储数据的格式,在一定程度上限制特定格式病毒、文件等数据上链,缓解恶意数据给区块链网络带来的威胁.

(2) 设计相应的激励和奖惩机制,结合智能合约等技术,鼓励矿工验证待上链数据的合理性和合法性,对上传恶意数据的节点进行惩罚,限制其链上交易行为.

(3) 利用机器学习[50]等技术对待上链数据进行过滤,可以在一定程度上阻止恶意数据被写入区块链.

3 区块链网络层攻击

网络层是区块链技术体系中最基础的技术架构,封装了区块链系统的组网方式、消息传播协议和数据验证机制等要素,使区块链具备了去中心化、不可篡改的技术特性.本节将对 P2P 网络中存在的安全威胁进行剖析.

3.1 针对P2P网络的攻击

P2P 网络主要涉及用户客户端和对等网络结构,攻击者可能针对这两个方面展开如下攻击.

(1) 客户端漏洞(client vulnerability)[51]:尽管现有全节点客户端的底层协议互相兼容,增强了比特币网络的健壮性,但客户端代码中可能存在诸多安全漏洞,并且这些漏洞会随着客户端类型的增加而增加.攻击者可以利用 0day 漏洞扫描等技术扫描客户端中存在的漏洞,然后利用这些漏洞发起各种攻击.2018 年,区块链安全公司 Peck Shield 披露了一个安全漏洞,攻击者可以向以太坊客户端发送特定恶意报文,一旦成功,将导致 2/3 的以太坊节点下线.

(2) 窃听攻击(eavesdropping attack)[52]:攻击者可以通过网络窃听,获取区块链用户节点的网络标识,并将其与 IP 地址关联起来,进而获取用户节点的隐私信息,甚至可以追溯到用户的实际家庭地址.以比特币为例,用户通过连接一组服务器来加入比特币网络,这个初始连接集合就是该用户的唯一入口节点.攻击者可以通过与比特币服务器建立多个连接,以窃听客户端与服务器端的初始连接,获得客户端的 IP 地址.随着交易流经网络,攻击者将窃听得到的 IP 地址与已有的客户端入口节点进行匹配,若成功,则攻击者便可获知交易的来源.

(3) 日蚀攻击(eclipse attack)[53]:攻击者通过特定手段使得目标节点只能获得被操纵的、伪造的网络视图,将其从实际的网络视图中隔离出来,从而妨碍目标节点正常运转,以达成特定的攻击目的.如图 2 所示,攻击者操纵多个对等节点与目标节点保持长时间的传输连接,使其在线链接数达到目标节点的入站连接上限,从而阻止其他合法节点的连接请求.此时,目标节点被攻击者从 P2P 网络中“隔离”出来,导致目标节点无法正常维护区块链账本.

(4) 边界网关协议(border gateway protocol,简称 BGP)劫持攻击[54]:BGP 是因特网的关键组成部分,敌手可以通过劫持 BGP 来实现操纵互联网路由路径的目的.由于区块链是基于互联网来传递信息的,劫持 BGP 可以实现对区块链节点流量的误导和拦截.攻击者一旦接管了节点的流量,就可以通过影响区块链网络的正常运行来破坏共识和交易进程.例如,比特币系统的大部分节点都被托管至几个特定的互联网服务提供商,大约 60%的比特币连接都会通过这些特定服务商,所以攻击者一旦接管了这部分流量,将可以通过 BGP 路由劫持破坏区块链网络的完整性,甚至导致区块链网络瘫痪.

(5) 分割攻击(segmentation attack)[55]:攻击者通过 BGP 劫持攻击将区块链网络划分成两个或多个不相交的网络,此时的区块链会分叉为两条或多条并行支链.攻击者可以在多个支链网络中将同一笔电子货币兑换成现实商品或法币.BGP 劫持攻击停止后,区块链重新统一,以最长的链为主链,其他的链上的交易、奖励等全部失效,攻击者由此获利.

(6) DoS 攻击(denial-of-service attack)[56]:即拒绝服务攻击,攻击者利用大量网络资源攻击计算机系统或网络,使其停止响应甚至崩溃,从而拒绝服务.实际中,用户节点资源通常受限,攻击者只能通过图 3 所示的分布式 DoS 攻击(distributed denial-of-service,简称 DDoS)[57]整合零散网络带宽来实施 DoS 攻击.2017 年 5 月,Poloniex 交易平台遭受了严重的 DDoS 攻击[58],导致比特币价格被锁定在 1 761 美元,用户无法正常执行交易.此外,当区块链网络中的大部分矿工无法盈利时,可能通过拒绝为区块链网络服务而发起 BDoS 攻击(blockchain denial of service,简称 BDoS)[59],导致区块链网络瘫痪.

(7) 交易延迟攻击(transaction delay attack):比特币闪电网络(lightning network)[60]通常使用哈希时间锁定技术[61]来实现安全的资产原子交换,其安全性主要依赖于时间锁定和资金锁定.由于每一笔资金交换都需要通过时间锁定来规定该交易必须在某个时间段内完成.一些恶意节点短时间内建立大量交易,然后故意超时发送,致使网络发生阻塞,影响正常运作.

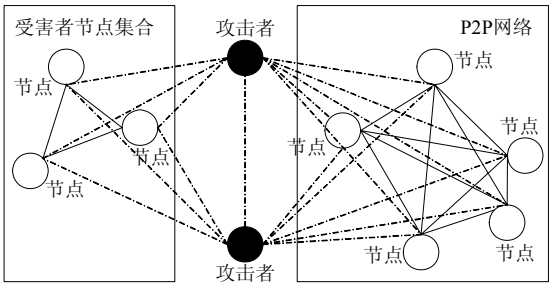


Fig.2 Eclipse attack

图 2 日蚀攻击

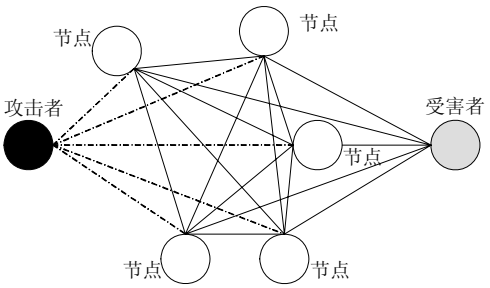


Fig.3 DDoS attack

图 3 DDoS 攻击

3.2 防御策略与方法

网络层攻击的主要攻击目标是区块链底层的 P2P 网络,其共性在于攻击者都是通过扰乱用户的之间的通信,从而达到不同的攻击目的.根据攻击方式的特性,区块链网络层攻击大致可以分为信息窃取类攻击、网络路由劫持类攻击和恶意资源占用类攻击.

(1) 信息窃取类攻击:主要包括客户端代码漏洞和窃听攻击.在针对客户端代码漏洞的攻击场景中,攻击者利用的漏洞可能是预先恶意植入的后门,也可能是开发人员编写错误导致的.理论上,无法完全杜绝类似的漏洞,所以开发商应在软件安全开发生命周期[62]内,通过 Fuzzing[63]、代码审计[64]、逆向漏洞分析[65]、反逆向工程[66]等技术对客户端的安全性进行评估,以缓解类似漏洞带给用户的安全威胁.在窃听攻击场景中,攻击者可以通过网络监听等手段获取用户身份、地址等隐私信息,其关键在于用户的区块链网络标识唯一,攻击者可以将窃听得到的 IP 地址与已有的客户端入口节点进行匹配,从而获得交易数据来源和用户隐私.为了预防窃听攻击,用户应采用混淆的交易方法来打破交易过程中用户唯一标识与 IP 地址之间的一一对应关系.具体地,多个用户可以通过共享唯一网络标识,实现“一对多”或“多对一”的交易,以此混淆用户唯一标识与 IP 地址之间的一一对应关系,使得攻击者无法通过匹配用户标识和 IP 地址来获取用户隐私.此外,在交易数据的传输过程中,应使用可靠的加密算法实现数据的加密传输,防止恶意攻击者对网络节点的信息进行窃取.

(2) 网络路由劫持类攻击:主要包括日蚀攻击、BGP 劫持攻击和分割攻击,它们的攻击原理相似,攻击目标分别为单个节点、节点集合和 P2P 网络.攻击者通过改变节点的网络视图,将目标节点集合从区块链网络中隔离出来,从而达成控制区块链网络的目的.以比特币系统为例,攻击者可以通过这 3 种攻击迫使部分矿工节点“离线”,导致区块链全网实际算力的流失,从而使攻击者的算力在全网总算力中的占比不断上升.当算力超过全网算力的一半时,攻击者可以以远低于原全网 51%的算力发动 51%攻击(详见第 4 节).与通过提升自身算力来实施 51%攻击的方式相比,通过日蚀攻击和 BGP 劫持攻击来提升自身攻击优势的方式更加经济.攻击者之所以可以发起日蚀攻击,其关键在于目标节点无法判断已连接节点的身份.为了预防日蚀攻击,Letz 等人[67]提出了共识信誉机制 BlockQuick.BlockQuick 中的网络节点在接受新产生的区块时,会对矿工的加密签名进行验证,并将该矿工的身份与共识信誉表中已知矿工的身份进行比对.最终,当共识得分大于 50%时,网络节点才会接受该区块;否则,节点察觉出攻击者的日蚀攻击行为并拒绝该区块.而在 BGP 劫持攻击和分割攻击场景中,攻击者主要通过 BGP 路由劫持实现网络视图分割.针对这个问题,研究人员提出了自动实时检测与缓解系统(ARTEMIS)[68],可以在几分钟内帮助服务提供商解决 BGP 劫持问题,使得实时流的公共 BGP 监控服务成为可能.

(3) 恶意资源占用类攻击:DoS,DDoS 攻击属于通过恶意资源占用实现的拒绝服务攻击,目前已经存在很多有效的防御工具,如 DoS 防火墙[69]等.而 BDoS 和交易延迟攻击则属于社会工程学类攻击,解决此类攻击只能通过不断完善激励制度和奖惩制度、优化网络环境等社会工程学手段.

4 区块链共识层攻击

共识层是区块链技术体系的灵魂,主要封装了区块链的各类共识算法,是保证区块链全网节点达成正确共识的关键.本节将从授权共识机制和非授权共识机制两个方面对共识层存在的安全威胁进行分析评估,并尝试给出一些解决思路.

4.1 针对授权共识机制的攻击

授权共识机制是指在授权网络(联盟链、私有链)中,节点须通过身份认证才能加入网络,与其他节点为达成某种共识而共同运行的特定分布式一致性算法.经典的授权共识算法包括拜占庭容错机制(Byzantine fault tolerance,简称 BFT)[70]、实用拜占庭(practical Byzantine fault tolerance,简称 PBFT)[71]以及权威证明算法(proof of authority,简称 PoA)[72]等.BFT 系列共识算法可以在总节点数为 $N=3f+1$、恶意节点数不超过 f 的情况下确保全网节点达成正确的共识(即容错率为 1/3).

(1) 女巫攻击(sybil attack)[26]:泛指网络中攻击者通过操作多个不同身份,以实现特定目标的攻击行为.在区块链网络中,攻击者可能通过发起女巫攻击以实现恶意刷票、刷排名、刷信誉等攻击目的.在 BFT 算法中,假设 A,B,C,D 中点 C 是攻击者,可以获得多个伪装身份 C_1,C_2,C_3,使得攻击者持有的节点数量超过总节点数的 1/3.此时,C 操纵 C,C_1,C_2,C_3 不断发出错误指令,则共有 7 个节点(A,B,C,C_1,C_2,C_3,D)运行 BFT 算法,最终会导致全网达成一个错误的共识.

(2) 克隆攻击(Cloning attack)[73]:在 PoA 系统中,攻击者利用系统中记账节点集合固定的缺点,通过 BGP 劫持、分割攻击等手段将区块链网络视图分为两个,然后克隆得到两个使用相同地址或公私钥对的克隆体,并分别部署至两个视图独立的支链.此时,攻击者可以就同一笔代币在两个网络中进行交易,待交易结束后,攻击者解除路由劫持,区块链网络节点通过最长链或最大权重原则统一区块链主链,攻击者实现了双花攻击.

4.2 针对非授权共识机制的攻击

非授权共识机制是指在非授权网络(公有链)中,节点无需身份认证,即可加入网络与其他节点为达成某种共识而共同运行的特定共识算法.经典非授权共识算法包括工作量证明机制(proof of work,简称 PoW)[12]、权益证明机制(proof of stake,简称 PoS)[28]、信誉证明机制(proof of reputation,简称 PoR)[74]及其衍生算法:委托权益证明机制(delegated proof of stake,简称 DPoS)[75]、评价证明机制(proof of review,简称 PoR)[76]、PoR/PoS 混合共识机制(PoR/PoS-hybrid)[77]等.授权共识算法中,各节点达成共识消耗的是等价的参与权,即节点共识权重相等.而在非授权共识机制中,各节点通过消耗自身持有的“筹码”(PoW 中代表算力 Work,PoS 中代表权益 Stake)竞争记账权,进而达成共识,即节点共识权重不相等.非授权共识机制可以在本轮竞争“总筹码”为 $N=2n+1$、恶意节点持有“筹码”不超过 n 的情况下,确保全网节点达成正确共识(容错率为 1/2).

4.2.1 恶意筹码获取

在非授权的共识机制中,节点持有的“筹码”越多,则其获得记账权的可能性越大.所以节点可能通过傀儡挖矿、贿赂攻击、币龄累计攻击等方式获取“筹码”,以提高自己获得记账权的成功率.

(1) 傀儡挖矿攻击(puppet attack)[39]:攻击者通过植入木马入侵大量网络节点,部署挖矿程序,盗用被入侵主机的电力、算力等资源挖矿获利.2018 年初,上百款《荒野行动》游戏辅助被植入挖矿木马,利用游戏主机显卡的高性能来挖矿获利.同年,攻击者在大量网站的首页植入 Coinhive 平台的门罗币(Monero)的挖矿代码[78],通过网页端盗用网络节点资源挖矿获利,导致该网站用户的系统运行变慢.

(2) 币龄累计攻击(coin age accumulation attack)[28]:在基于“POW+POS”混合共识机制的区块链中,节点持有的“筹码”不仅与其算力有关,还与其持有的币龄有关.持币量越多、持币时间越长,则节点持有的币龄越多.因此,节点可以通过币龄累计攻击来获取更多的“筹码”:买入一定数量代币后,持有足够长时间后,就可以获得足够多的币龄用于竞争记账权.

(3) 贿赂攻击(the bribing attack)[27]:攻击者通过“恶意悬赏”,鼓励矿工在攻击者指定的支链上进行挖矿,当

支链挖矿投入的“筹码”超过全网总筹码的一半时,攻击者便通过 51%攻击实现双花攻击、历史修复攻击、卖空攻击等.在 PoW 中,贿赂攻击可以看作是一种算力租借方式,被贿赂矿工需要消耗大量算力来挖矿,因此攻击者的攻击成本较高;而在 PoS 共识机制中,被贿赂节点不需要消耗大量算力,以较低成本便可赚取攻击者的悬赏,因此贿赂攻击所需的成本较低,常见于 PoS 系统.

除了通过增加“筹码”提高筹码占比的方法以外,攻击者还可能通过网络层日蚀攻击、BGP 路由劫持、分割攻击(详见第 3 节)等手段迫使大量节点离线,使区块链网络的总算力流失,从而提高自己的记账权竞争筹码占比和记账权竞争的成功率.

4.2.2 51%攻击

一旦存在恶意节点持有的“筹码”超过本轮记账权竞争总“筹码”的一半,则其可以以较大的优势获得记账权,并主导区块链达成特定共识,本文称该攻击为短程 51%攻击;也可以如图 4 所示,利用资源优势计算并生成一条区块链支链,使其长度超过当前主链,并代替成为新的主链,本文称这种攻击为长程 51%攻击.

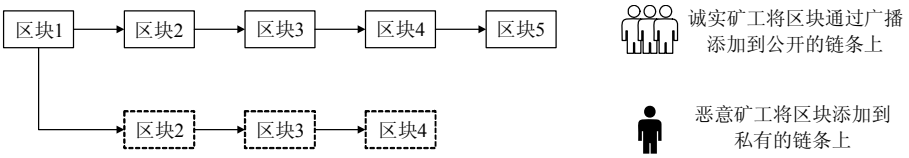


Fig.4 Fork of block chain

图 4 区块链分叉

在实际的区块链网络中,攻击者可能将 51%攻击作为一种子攻击,进而实现以下几类攻击.

(1) 双花攻击(double spending attack)[8]:以比特币系统为例,攻击者在完成交易 A 后,针对 A 花费的代币伪造交易 B,并发动长程 51%攻击,将一条包含交易 B 的支链变成新的主链.如此,攻击者对相同的一组代币实现了“双重花费”.2016 年 8 月,基于以太坊的数字货币 Krypton 遭受了名为“51% Crew”的 51%攻击[79],攻击者通过租用 Nicehash(算力买卖市场)的算力,导致该区块链损失约 21 465KR 的代币.2018 年,比特币黄金社区的一位成员发文称:有人在尝试进行针对交易所的双花攻击,这一攻击造成了千万美元的损失[80],同时引起了人们对于去中心化和 PoW 机制的质疑.

(2) 历史修复攻击(history-revision attack)[40]:在区块链网络中,当攻击者无法持续拥有超过竞争本轮记账权总筹码的一半以上筹码时,攻击者和诚实节点的身份可能发生颠倒,并导致多轮 51%攻击.具体地,当攻击者 A 成功发起 51%攻击将他的支链变为主链时,之前的主链变为支链,诚实节点 B 变为“恶意节点”,A 成为“诚实节点”.一旦 B 获得超过新一轮记账权总筹码的一半时,便可作为“攻击者”发起 51%攻击,将他们的“支链”恢复为主链,此时称 B 发起了历史修复攻击.

(3) 卖空攻击(shot selling attack)[41]:51%攻击会破坏区块链系统,导致其对应的代币贬值.尤其是在 PoS 共识机制下,“聪明”的矿工一般不会对基于 PoS 的区块链系统发动 51%攻击.因为攻击者成功发起 51%攻击,意味着其持有大量代币,而代币贬值将会给攻击者带来巨大的经济损失.但在支持证券信用交易的 PoS 系统中,攻击者可能通过 51%攻击发起卖空攻击来牟取暴利,具体步骤如下.

① 攻击者持有数量为 A 的代币,这些代币的权益需超过本轮投票总权益的一半以上.

② 攻击者通过证券信用交易或金融借贷等手段获得数量为 B 的代币,B 的数量远大于 A.这里的 B 是攻击者所借的证券,攻击结束后,需返还等额的代币给借贷方,如交易所.

③ 攻击者将所借的代币套现,兑换为具备实际价值的经济实体或货币.

④ 攻击者使用双花攻击、传统网络攻击等手段恶意影响区块链网络的正常运作,从而使得基于该区块链的数字货币贬值,此处将贬值率记为 Δ.

⑤ 攻击者回购数量为 B 的代币偿还给借款方,最终获利 $\Delta(B-A)$.

(4) 自私挖矿攻击(selfish mining attack)[81]:与双花攻击不同,自私挖矿攻击是一种利用短程 51%攻击持续

性获取记账权,进而赚取奖励的攻击方式,常见于 PoW 系统中.攻击者通过短程 51%攻击,以较大优势比其他节点先挖到“矿”,暂扣区块并赶在其他节点之前公布出来,以获取记账权并赚取奖励.在延迟公布期间,攻击者沿着之前的区块继续挖矿,以积攒更多的优势,保证他可以连续获得奖励.这种攻击不会破坏比特币的运行机制,但会使其他节点的工作量无效化,浪费了大量的算力.

4.2.3 其他攻击

(1) 无利害关系攻击(nothing at stake attack)[29]:这是一种针对 PoS 共识机制的攻击方式,攻击者可以在区块链产生分叉时,使用权益同时为多个分叉出块,以获取最大化的收益.由于攻击者无需像在 PoW 系统中消耗大量算力,只需进行权益投票便可实现利益最大化,因此也被称为“作恶无成本,好处无限多”的无利害关系问题,这变相地鼓励了区块链分叉的产生.“聪明”的矿工往往采取“在每条分叉上同时挖矿”的最佳策略以获取最大收益,这将导致区块链产生过多分叉,不再是唯一链.全网节点也因此无法达成共识,进而引起双花攻击、非法交易的泛滥.

(2) 预计算攻击(pre-computation attack)[30]:在“PoW+PoS”混合共识机制中,当前区块难度取决于前一区块参数(如哈希值).攻击者可以在生成区块时,通过随机试错法计算并选择一个对自己产生下一区块最有利的参数.通过这种方式,攻击者有更大的优势可以获得下一区块的奖励.

(3) 长距离攻击(long range attack)[82]:PoS 系统中,区块的生成速度比 PoW 快很多,所以攻击者可能尝试通过重写区块链账本,从而实现代币双花等目的.这种攻击和 PoW 中的长程 51%攻击的原理相似,区别在于长距离攻击中,攻击者不用消耗大量算力,便可能伪造出一条新的区块链主链,攻击成本更低,所以带来的安全威胁更大.

4.3 防御策略与方法

共识层攻击的主要攻击目标是影响区块链的共识进程,其共性在于攻击者都是利用共识机制的特点或缺陷来提高自身竞争记账权的成功率,从而使区块链沿着对攻击者有利的方向发展,以实现妨碍网络正常运行、货币双花、最大获利等实际目的.其特性则在于各个攻击的场景、目的、方式的不同.授权共识机制中,攻击者持有的有效节点身份数量是影响共识进程的关键.而在非授权共识机制中,算力、权益等类型的资源才是影响共识进程的关键.同时,攻击者为了获取更多资源,可能采用诸多恶意的筹码获取手段来提升自己竞争记账权的成功率.此外,在一些特殊的系统中,攻击者无需积累“资源”便可实现最大化收益.

在授权共识机制中,攻击者需持有超过全网 1/3 的节点才有可能主导区块链网络达成有利于自己的共识,即攻击者操纵了多个节点身份,发起了女巫攻击.在女巫攻击的场景中,攻击者可能通过伪造等手段获取多个节点身份,也可能通过胁迫、腐化等手段控制多个节点,而其他节点无法检测、判断出攻击者持有节点身份的数量及其之间的内部关系.因此,阻止女巫攻击的关键在于阻止攻击者获取多重身份,可以考虑以下策略.

(1) 采用节点身份验证机制,通过身份验证防止攻击者伪造节点身份.目前,部分私有链采用了 PoA 共识机制,如 Aura[72]、Clique[83]等,该机制通过随机密钥分发与基于公钥体制的认证方式,使得攻击者无法在区块链网络中伪造多个身份,在一定程度上缓解了女巫攻击.

(2) 采用高成本的多身份申请机制,通过提高身份伪造成本缓解女巫攻击.尽管节点身份验证机制可以阻止攻击者伪造身份,但在实际中,这种方式无法满足诚实节点对多节点身份的正常需求.因此,可以考虑在区块链中引入首次申请身份免费、多次申请成本指数式升高的身份申请机制,在满足节点对多身份正常需求的同时,指数式增加攻击者的攻击成本,缓解女巫攻击带来的安全威胁.

理论上,女巫攻击也可以出现在非授权的共识场景中,但由于非授权共识算法中的节点是通过自身持有的“筹码”竞争记账权,多重身份伪造意味着攻击者“筹码”的分流,但“筹码”总量不会发生变化,而攻击者实施女巫攻击不但不能提高自己获得记账权的成功率,反而有可能导致其成功率降低,所以女巫攻击不会对非授权共识机制的共识过程产生实质性影响.

克隆攻击是一种专门针对 PoA 系统的攻击方式,攻击者成功实施克隆攻击的关键,一方面在于 PoA 系统中记账节点集合恒定不变的固有缺陷,另一方面在于攻击者是否能通过 BGP 劫持攻击、分割攻击成功实现网络

分区.因此,解决克隆攻击的关键在于如何阻止攻击者成功实施 BGP 劫持攻击、分割攻击,所以可以考虑采用第 3.2 节中的 ARTEMIS 系统预防攻击者进行网络分区,从源头阻止克隆攻击.然而,ARTEMIS 系统只能在网络发生异常时发现区块链网络是否发生分区,如果攻击者仅对部分关键数据进行管控而不影响其他数据的正常传递,则 ARTEMIS 也无法阻止此类“无特征”的克隆攻击.此时,准备出块的区块链节点可以考虑引入基于权重的节点活性检测方法,主动检测区块链网络是否发生网络分区.具体地,区块链节点可以通过随机取样的方式选取区块链中已有的区块,根据其中包含的交易类型、金额、数量等特征计算出该区块生成者的权重.然后随机选择节点并请求包含其心跳信息和上一区块哈希值在内的活性证明,如果该节点成功证明自身活性,则验证者累计已验证节点的权重,并重复上述操作直至累计权重达到预先设置的阈值;若被选中节点未通过或未参与活性检测,则证明区块链网络发生分区,应立即停止出块.尽管该方法与 ARTEMIS 无法从根本上阻止攻击者在 PoA 系统中实施克隆攻击,但能够在一定程度上预防并缓解克隆攻击来的危害,避免损失.

在非授权共识机制中,攻击者在本轮“记账权”竞争中需持有超过全网 1/2 的“筹码”,才有可能通过 51%攻击主导区块链网络达成有利于自己的共识,进而实现双花攻击、历史修复攻击、卖空攻击等目的.而实际中,攻击者通常很难自己拥有足够的“筹码”来实施 51%攻击,所以可能会通过各种手段获取“筹码”.为了预防 51%攻击,区块链网络应该采取如下策略,阻止攻击者通过傀儡挖矿攻击、贿赂攻击等方法获取“筹码”.

(1) 加强区块链客户端的入侵检测能力,添加防火墙,阻止攻击者通过木马病毒入侵网络节点,盗用受害节点的挖矿资源.

(2) 采用针对“恶意悬赏”的惩罚机制,缓解贿赂攻击带来的危害.全网节点可以对抵制恶意悬赏、恶意攻击达成共识,缴纳保证金并签订智能合约.一旦出现恶意悬赏,则对举报者进行奖励,对恶意节点进行惩罚,没收悬赏金额和保证金,限制其网络交易权限.

(3) 在 PoS 中采用新型的币龄计算方法,限制节点恶意累计币龄的行为.如:点点币通过在币龄计算方法中设置节点持币时间上限的方式,限制了用户所持币龄的上限,在一定程度上阻止了 51%攻击.

(4) 在 PoS 中采用币龄预警、清零机制,预防 51%攻击.在记账权竞争过程中,对节点进行身份认证和权益关联.若发现单节点或关联节点所持权益超过全网一半,则启动预警机制,阻止共识进程,然后清空恶意节点持有的全部币龄,并处罚金.

尽管如此,攻击者还可能存在其他获取“筹码”的途径.为了进一步阻止 51%攻击,以太坊提出了一种计划内置于 PoS 系统客户端的 Casper[84]机制.Casper 机制要求以太坊的矿工锁定一些以太币作为押金,为刚产生的区块担保.如果投注者是诚实的,他们将获得相应的交易费用作为奖励;否则,Casper 将没收大量已投注的以太币作为惩罚.显然,类似 Casper 机制的保证金奖惩机制可以很好地解决一些社会工程学问题,从而预防趋利节点发起的各种攻击.如:在无利害关系攻击场景中,Casper 机制可以惩罚大部分恶意行为,提升了制造恶意分叉的代价,使无利害关系攻击无法为攻击者带来收益.若矿工想参与挖矿,则他必须抵押一定数量的以太币作为押金,保证自己在最长链上挖矿.若该区块被确认上链,则矿工收回保证金并获得一定的奖励.如果其他矿工尝试在多条支链上挖矿来进行无利害关系攻击,则会被没收其在多条支链上的押金,这种概念叫做剑手(slasher)协议[85],即如果矿工在同一个层级的分叉上同时签署了两份承诺,该矿工就会失去区块奖励,甚至被没收押金.

在预计算攻击场景中,攻击者可以通过预计算确定下一区块计算难度的关键在于区块生成算法中,上一区块哈希值与下一区块计算难度的关联性.所以为了预防 PoS 系统中的预计算攻击,应该重新制定区块生成算法.首先,可以考虑打断当前区块链计算难度与前一区块哈希值之间的联系,使得攻击者无法通过预计算控制后续区块的计算难度;其次,也可以考虑增加新的计算元素,使得上一区块的哈希值不再是确定下一区块计算难度的唯一因素.在长距离攻击场景中,区块链网络无法阻止攻击者伪造一条新的区块链主链,但可以通过类似 BlockQuick 的方式,通过增加身份认证、信誉值对比的方式限制全网节点对该链的接受度来预防长距离攻击.

5 区块链合约层攻击

合约层是区块链 2.0 技术体系的重要标志,封装了区块链的各类脚本代码、算法机制和智能合约,使区块链

技术具备了较高的可编程性和实用性.本节将从智能合约和合约虚拟机两方面对区块链合约层存在的安全威胁进行分析,并尝试给出应对策略.

5.1 针对智能合约的攻击

智能合约是区块链 2.0 的标志性技术.图灵完备的区块链网络允许用户在区块链网络上开发并部署特定的代码或应用,但智能合约在编写过程中存在的诸多不足,可能给区块链网络带来以下安全隐患.

(1) 整数溢出漏洞(integer overflow and underflow vulnerability)[86]:智能合约代码中,整数型变量都存在上限或下限,当变量存储的数值超过上限则称为整数上溢,超过下限则称为整数下溢.当一个整数变量发生溢出时,可能会从一个很大的数变成很小的数或者从一个很小的数变成很大的数.利用这个漏洞,攻击者通常通过输入异常参数致使整数溢出,从而达到修改地址指针,实现代码异常调用的目的.2010 年 8 月,由于验证机制中存在大整数溢出漏洞[87],比特币的第 74 638 块出现了一条包含超过 1 844 亿个比特币的交易.2018 年 4 月,BeautyChain(BEC)智能合约中出现了一个灾难性的整数溢出漏洞[88],导致约 10 亿美元的损失.

(2) 时间戳依赖攻击(time-stamp dependency attack)[89]:智能合约的执行大多依赖于当前区块的时间戳,不同的时间戳可能导致智能合约产生不同的执行结果.以抽奖合约为例:假设智能合约需要根据当前时间戳和其他可提前获知变量计算出一个“幸运数”,以确定获奖人员.攻击者则可以在挖矿过程中提前尝试使用不同的时间戳来计算“幸运数”,从而将奖品送给自己想给的获奖者.

(3) 调用深度攻击(call deep attack)[90]:合约虚拟机在运行过程中会为合约相互调用的深度设置一个阈值,即使合约调用不存在任何逻辑问题,但当调用深度超过该阈值后,合约将不再往下执行,即合约调用失败.例如在以太坊虚拟机中,调用深度被限制为 1 024.如果攻击者发起一系列递归调用让栈的深度到达了 1 023,之后再调用目标智能合约的关键函数,就会自动导致这个函数所有的子调用失败.因此,攻击者可以通过控制调用深度,使得某些关键操作无法执行.例如在区块链上实现一个拍卖的智能合约,由于拍卖过程中可能存在多次竞价,需要反复调用合约中的出价函数,攻击者可以恶意刷出价次数.当调用深度达到 1 023 次临界值时竞拍结束,此时调用转账函数就会失败,导致拍卖失败.

(4) 误操作异常攻击(misoperation attack):攻击者通过智能合约 *A* 调用智能合约 *B* 时,*B* 可能因为执行异常而返回合约未执行的状态,若 *A* 不检查 *B* 的结果而继续执行,则将导致 *A* 在 *B* 未执行的情况下完成调用.以 KoET 智能合约[91]为例:网络中各节点可以通过智能合约买卖“以太币国王”称号来获利,支付金额由现任国王来决定.当一个节点想购买“国王”称号时,智能合约 *A* 调用智能合约 *B* 支付赔偿金给现任国王,并指定该节点成为新的国王.如果 *B* 因为操作异常(如调用深度攻击)导致支付失败,而 *A* 在未检查 *B* 执行结果的情况下继续执行,将导致节点在未支付赔偿金的情况下成为新的“国王”,原“国王”同时失去国王称号和赔偿金.

(5) 重入攻击(re-entrancy attacks)[92]:攻击者针对智能合约代码的重入漏洞发起的攻击,可导致两个智能合约发生循环调用.其中最具代表性的是 DAO 攻击[93]:攻击者通过智能合约 *A* 向智能合约 *B* 发起提现请求,*B* 向 *A* 转账并调用 *A* 的回调函数.此时,若 *A* 的回调函数中被攻击者写入操作“合约 *A* 向合约 *B* 发起提现请求”.如此,*A* 再次向 *B* 发起提现请求并重复提现过程,直至提现失败(账户余额不足).2016 年 6 月发生了一起史上最严重的智能合约安全事件——“The DAO”[94],导致价值 6 000 万美元的以太币被盗,迫使以太币硬分叉为以太坊 ETH 和以太经典 ETC.

5.2 针对合约虚拟机的攻击

合约虚拟机是智能合约的调用、执行平台,是区块链技术支持多样化应用的载体,提高了区块链的可扩展性,但仍然可能存在一些安全隐患.

(1) 逃逸漏洞(escape vulnerability)[95]:攻击者在控制一个虚拟机的前提下,通过利用虚拟机和底层监控器(virtual machine monitor,简称 VMM)的交互漏洞,实现对底层 VMM 或其他虚拟机的控制.虚拟机逃逸

后可以在 VMM 层或者管理域中安装后门、执行拒绝服务攻击、窃取其他用户数据,甚至控制其他用户虚拟机等.在区块链系统中,虚拟机在运行代码时会提供一个沙盒环境,一般用户只能在沙盒的限制中执行相应的代码,此类型漏洞会使得攻击者编写的恶意代码在运行该沙盒环境的宿主机上执行,破坏宿主机与沙盒的隔离性.

(2) 逻辑漏洞(logic vulnerability)[96]:逻辑漏洞是指由于程序逻辑不严谨,导致逻辑分支被非正常处理或错误处理的漏洞.虚拟机在发现代码不符合规范时,可能会做一些“容错处理”,并导致一些逻辑问题.最典型的是“以太坊短地址攻击”[97]:在 ERC-20 TOKEN 标准[98]下,攻击者可以输入一个短地址并调用 Transfer 方法提币.EVM 虚拟机在解析合约代码时,会通过末尾填充 0 的方式将短地址补至预期长度.此时,参数编码可能出现逻辑漏洞,导致攻击者获取与交易金额不符的代币.

(3) 资源滥用漏洞(resource-exhaustion vulnerability)[99]:攻击者在虚拟机上部署恶意代码,恶意消耗系统存储资源和计算资源.所以在虚拟机中必须要有相应的限制机制来防止系统的资源被滥用.在以太坊中,智能合约采用了 gas 机制,攻击者想在以太坊虚拟机上做更多操作,需要付出经济代价.

5.3 防御策略与方法

合约层攻击的共性在于,攻击者是尝试通过干扰合约的正常调用来实现不同的攻击目的.其特性在于不同攻击方式的攻击目标和原理不同,攻击者可以利用智能合约的代码漏洞或合约虚拟机的运行漏洞,尝试通过非正常的合约调用,以实现非法获利、破坏区块链网络的目的.

智能合约实质上是由开发者编写并部署在区块链上的一段代码,其中的漏洞可能是由于开发人员编写的代码不符合标准导致的,如整数溢出漏洞、时间戳依赖性、调用深度限制等;也可能是攻击者(开发者)恶意植入的,如重入攻击.所以在智能合约编写过程中,开发人员需考虑到以下几方面.

(1) 养成良好的编程习惯,以严谨的编程逻辑避免智能合约开发过程中出现整数溢出等常见的漏洞.

(2) 针对智能合约的时间戳依赖性,在合约开发过程中应采用多维参数输入、随机参数输入等,避免合约执行结果完全依赖于时间戳,降低合约执行结果的可预测性.

(3) 针对智能合约的调用深度限制,应在智能合约中预先设置预警惩罚机制.当合约调用次数接近上限时,智能合约调用预警合约对用户发出提醒,若用户继续调用合约最终导致合约运行失败,则预警合约调用惩罚合约对最后调用合约的用户进行惩罚.

(4) 针对重入漏洞,应在合约开发过程中设置参数检验机制.当智能合约 A 调用智能合约 B 时,应对 B 返回的参数进行确认,再继续执行.参数检验机制可以阻止攻击者通过在 B 植入漏洞发起重入攻击,也可以阻止攻击者实施误操作异常攻击.

尽管良好的编程习惯和编程策略可以在一定程度上避免智能合约中出现安全漏洞,但仍有一些安全漏洞是不可避免的.所以在部署智能合约时,用户可以采用以下方法避免代码漏洞带来的危害.

(1) 安全评估:在正式部署智能合约前,应对其进行大量安全测试或白盒审计,以评估该合约的安全性.

(2) 采用 Sereum[92],ZEUS[100]等重入攻击防护工具.其中,Sereum 支持多种重入攻击的识别,不仅适用于待部署合约,还可以保护已部署智能合约在重入攻击下的安全性,误报率仅为 0.06%.

此外,合约虚拟机中存在的逃逸漏洞、逻辑漏洞、资源滥用漏洞可能会导致智能合约的异常运行,攻击者可以在发现这些漏洞后,在与其他用户订立智能合约时,利用这些漏洞编写有利于自己的智能合约代码,使得智能合约失去公平性.所以,区块链网络在引入智能合约虚拟机时,应对虚拟机进行系统的代码审计,分析评估其安全性,并将其可能存在的安全漏洞披露出来.而用户在部署智能合约时,除了对合约代码进行常规审计外,也要根据目标合约虚拟机披露的漏洞对代码进行审计,做好双向的智能合约运行环境评估.

6 区块链应用层攻击

应用层是区块链技术的应用载体,为各种业务场景提供解决方案.本节将从挖矿机制和区块链交易两个角度梳理分析区块链应用层存在的安全漏洞和恶意攻击,旨在给出有效的应对策略.

6.1 挖矿场景中的攻击

“挖矿”是维持 PoW 系统正常运转的动力,很多攻击者尝试利用挖矿过程中存在的漏洞获利,这会导致严重的资源浪费,进而降低区块链网络的吞吐量.其中,主要包括针对矿机系统和挖矿机制的恶意攻击.

6.1.1 针对矿机系统的攻击

由于系统代码的闭源特性,用户无法检查矿机的安全性,所以存在诸多安全隐患.

(1) 0day 漏洞攻击(zero-day (0day) vulnerability)[35]:目前,大多数矿机的系统都是通用的,一旦某个矿机系统被发现存在 0day 漏洞,攻击者可以利用该漏洞得到系统控制权限.

(2) 网络渗透攻击(network penetration attack)[101]:攻击者通过利用多种安全漏洞对客户端系统(如钱包客户端、矿机系统、Web 服务系统等)进行持续性渗透,最终获取系统的控制权限,威胁矿机的系统安全.该攻击方式不限制于某一特定漏洞,最终以获取系统权限为目的.

(3) 地址篡改攻击(address tampering attack)[102]:攻击者在攻陷矿机系统之后,通过篡改挖矿奖励接收地址的方式,劫持并盗取原属于目标矿工的挖矿奖励.

6.1.2 针对挖矿机制的攻击

在挖矿过程中,“聪明”的矿工可能利用挖矿机制的一些漏洞做出趋利行为,导致严重的资源浪费.主要包括:

(1) 算力伪造攻击(computational forgery attack)[31]:在比特币系统中,矿池一般通过特定的工作量证明检验算法来检验当前矿工的实际算力.如果算法存在某些漏洞时,“聪明”的矿工可能通过虚报算力来获取更高的奖励,这将严重影响奖励分配的公平性,导致矿池的算力流失.

(2) 扣块攻击(block withholding attack)[32]:也被称为藏块攻击.主要有 3 种形式:第 1 种是矿池下发计算任务后,恶意矿工直接返回一个错误的计算值,然后分得矿池根据算力分发的数字货币奖励;第 2 种是矿工挖出区块后,不向矿池返回,而是私自广播至整个网络,独自获得相应的区块奖励;第 3 种是恶意矿工不会发布自己挖到的区块,导致矿池收益降低.扣块攻击成本较高,恶意矿工获利较少,甚至不获利,所以该攻击常见于矿池恶意竞争的场景中:恶意矿工作为“间谍”加入敌方矿池,在领取敌方矿池奖励的同时,通过浪费敌方矿池的算力资源来获取己方矿池的报酬,实现两方获利.扣块攻击的出现,激化了矿池间的恶意竞争,严重扰乱了正常的挖矿秩序.

(3) 丢弃攻击(drop attack)[33]:攻击者将多个具有良好网络连接的节点置于网络中,这样不但可以方便地获知最新被广播出的区块,也可以比其他节点更加快速地传播目标区块.当攻击者挖出新区块后不会及时公布,直至得知有区块被公布时,攻击者会立即发布自己的区块,并且利用布置好的节点快速地广播到整个网络,使得该合法节点开采的区块被丢弃,从而获取奖励.

(4) 空块攻击(empty block attack)[103]:空块攻击是早期比特币网络中常见的攻击方式,攻击者通过生成空块获取比打包交易区块更快的出块速度,从而以更大的可能性获取出块奖励.空块的产生,意味着比特币网络有 10 分钟处于拒绝服务的状态.偶尔出现空块不会对网络产生太大影响,但短期内出现大量空块,会使交易池中的交易大量滞留,平均交易时间延长.

(5) 通用挖矿攻击(general mining attack)[104]:通用挖矿攻击常见于区块链系统初始化建立的阶段,当该系统与某个已成熟区块链系统采用相同的架构和共识机制时,后者系统中具备大量算力的攻击者可能加入新区块链进行挖矿,以恶意竞争出块奖励.此时容易产生算力集中化问题,甚至当攻击者算力超过新系统全网一半时,可能发起 51%攻击来实现代币双花、历史修复、卖空攻击等攻击目的.

(6) 交易顺序依赖攻击(transaction-ordering dependence attack)[9]:区块链交易场景中,交易的处理顺序不同,则其产生的结果也不相同.例如:当攻击者发布一个奖励丰富的解题智能合约时,攻击者可以监听网络中与之相关的解题交易,并在目标解题交易被验证、打包上链前,发布一个具备高 *Gas* 值的交易,将解题合约的奖励降低为 0.出于最大获利的目的,矿工会优先将高 *Gas* 值的交易打包上链,导致解题者无法获得智能合约中原先声明的奖励.

(7) 芬尼攻击(Finney attack)[10]:芬尼攻击是扣块攻击的一种衍生攻击,主要发生在支持零确认交易的服

务场景中,可以作为实现双花攻击的跳板.以比特币系统为例,每笔交易被打包后需要经过 6 个区块的确认才能真正上链,这明显无法满足部分服务场景对即时性交易的需求,所以部分商家推出零确认交易服务,即用户在完成交易后无需等待确认便可获取服务,商家则需等待交易数据上链才可以获得相应的费用.攻击者可以利用零确认交易的缺点,实施芬尼攻击:当攻击者挖到包含自己交易 A 的区块时扣留该区块,然后就 A 对应的代币与商家完成零确认交易 B,并在 B 被确认前将包含 A 的区块广播至全网.此时,交易 B 被验证为不合法,攻击者由此实现了双花攻击.与通过 51%攻击实现的双花攻击相比,芬尼攻击的攻击成本远低于基于 51%攻击的双花攻击,因此相对常见.

(8) 种族攻击(race attack)[105]:种族攻击可以看作是一种进阶版的芬尼攻击,可以通过扰乱正常的交易顺序来实现双花攻击.与交易顺序依赖攻击不同的是:交易顺序依赖攻击针对的是智能合约,而种族攻击针对的是支持零确认交易的服务场景.如以太坊中,攻击者在与商家完成零确认交易 A 后,就 A 对应的代币生成一个高 *Gas* 值的交易 B,“聪明”的矿工会优先将 B 打包进区块以获取最大化的利益,导致零确认交易 A 验证失败,而攻击者已经提前获取了相应服务,实现了代币双花.

6.2 区块链交易场景中的攻击

随着部分国家对比特币的认可,出现了很多区块链数字货币、交易平台,形成了一套相对完整的区块链电子货币金融体系.用户节点可以通过交易平台进行资产转换、投资等商业行为,也可以通过钱包账户进行点对点的可信交易.多样的交易平台和用户账户中存在的安全漏洞,严重威胁着区块链用户的资产安全.

6.2.1 针对交易平台的攻击

交易平台是区块链电子货币金融体系中十分重要的一类实体,为区块链用户提供了进行各种商业行为的场所.但由于用户的安全意识不足、系统潜在的安全漏洞等原因,交易平台面临隐私泄露、资产流失的风险.

(1) 弱口令攻击(weak password attack)[106]:实际中,用户可能出于方便记忆等原因,为自己的账户设置了安全级别较低的密码,攻击者通过简单的猜测、穷举等方式,即可获取用户的账户访问权限.

(2) 撞库攻击(credential stuffing attack)[34]:用户由于安全意识不足,可能在不同的网站使用相同的账号和口令.攻击者可以通过钓鱼攻击等手段收集与区块链、金融等相关网站上的用户账号和口令,然后在目标交易平台上使用自动化程序逐个尝试,以获取该平台中用户的账户隐私信息.

(3) 穷举攻击(brute-force attack)[107]:如果网站不对登陆接口做请求限制或者风险控制,攻击者可以针对目标值发送多次测试请求,尝试通过穷举攻击破解某些关键信息.如在短信验证中,若平台不对短信验证码的有效期或验证接口进行限制,攻击者可以轻易对其完成破解.若平台对登陆接口未做请求限制,攻击者可以通过大量的密码字典来暴力破解某个账户的密码.

(4) API 接口攻击(application programming interface,简称 API attack)[108]:用户通常使用私钥 key,通过交易平台中私有的 API 接口来执行一些敏感操作,如交易所新订单的确认、取消等.一旦 API key 泄露,很可能导致用户账户蒙受经济损失.2018 年 3 月,币安网大量用户 API key 泄露[109],攻击者通过泄露的 key 直接操作用户交易,致一万余枚的比特币被用于购买其他币种,造成币市动荡.

(5) 单点登陆漏洞(single sign-on vulnerability)[110]:攻击者可以通过跨站请求伪造、跨站脚本攻击等手段来窃取用户登陆的 Ticket,从而盗取目标用户账户中的资金.2017 年 10 月,OKCoin 旗下交易所出现大量账户被盗情况[111],损失金额超过 1 千万人民币.

6.2.2 针对用户账户的攻击

区块链钱包、交易所账户是用户参与区块链交易的重要工具,保管着大量的用户隐私和资产,是攻击者的主要攻击目标.由于服务场景的多样性和复杂性,用户账户主要面临以下安全威胁.

(1) 钓鱼攻击(phishing attack)[37]:攻击者通过伪造网页、系统、邮件等形式,诱导用户进行一系列交易操作,获取用户的钱包、交易所账户口令,进而盗取用户资产.

(2) 木马劫持攻击(Trojan horse attack)[112]:攻击者可以向用户主机中植入木马病毒,通过按键记录、hook 浏览器的方式来获取其账户和口令,从而盗取目标用户资产.2017 年 8 月,攻击者利用木马病毒

Trickbot 对包括 Coinbase 在内的几家数字货币交易所进行了 Web 注入攻击[113],当受害者购买数字货币时,木马病毒会劫持交易所钱包,并将资金定向至攻击者钱包,最终造成用户损失.

(3) 中间人劫持攻击(man-in-the-middle attack)[114]:目前,多数交易所都采用 HTTPS 协议进行交互,在一定程度上保证了数据安全.但在某些 API 接口的子域名,却未使用 HTTPS.攻击者可以通过在流量中转处劫持网络流量,如路由器、网关等流量出口,从而获取相关信息.

(4) 私钥窃取攻击(private key stealing attack)[115]:用户丢失私钥意味着用户的账户资产全部遗失,因此,用户通常会对钱包的私钥文件进行多次备份,而不安全的备份存放点存在私钥泄露的风险.目前,针对比特币的 wallet.dat 文件广泛出现在互联网中,例如 GitHub、NAS 服务器、Web 服务等互联网可接入的位置.目前,已经有攻击者开始扫描密钥文件,甚至开发相关的木马病毒进行私钥窃取.

(5) 钱包客户端漏洞(wallet client vulnerability):攻击者可能利用钱包软件自身的漏洞实施攻击,进而获取用户隐私和资产.例如:在以太坊多重签名钱包 Parity 中,攻击者可以通过间接调用初始化钱包软件的库函数,将自己更换为受害者钱包的新主人.2017 年 11 月,Parity 钱包出现重大 Bug[116],攻击者利用该 Bug 成为库的主人,然后调用自杀函数报废整个合约库,彻底冻结了 150 多个地址中总计超过 50 万个 ETH,直接导致上亿美元资金被冻结.

(6) 粉尘攻击(dusting attack)[11]:比特币系统中,“聪”是最小的 BTC 单位,通常将 100 聪以内的 BTC 称为粉尘.而且比特币中没有余额的概念,所有合法的交易都可以追溯到前向一个或多个交易的输出,其源头都是挖矿奖励,末尾则是当前未花费的交易输出(unspent transaction output,简称 UTXO).攻击者可以通过向目标用户钱包地址发送“粉尘”来实施粉尘攻击,当用户使用这些“粉尘”交易时,会导致其与用户自有 UTXO 的交易输出发生混合,攻击者可以通过“粉尘”来追踪用户的钱包地址,获取用户的隐私信息,从而勒索、盗取目标用户的资产.

(7) SIM hack[117]:在一些去中心化钱包中,用户需要通过 SIM(subscriber identity module)卡来验证身份的合法性.用户通常在丢失 SIM 卡后向运营商申请“移植”SIM 卡,该服务允许客户将该电话号码转移到新的 SIM 设备中.攻击者可以利用这一漏洞,通过技术手段将受害者的 SIM 卡移植到他们控制的电话上,然后在其电子邮件帐户上启动密码重置流程,验证码会发送到电话号码中.由于攻击者此时控制着 SIM 卡,可以轻易地对受害者账户信息进行篡改,盗取受害者账户中的财产.

(8) 在线钱包窃取(online wallet theft)[118]:目前,很多用户会选择使用在线钱包,这使得个人的资产安全严重依赖于服务商的安全性.2013 年 11 月,比特币在线钱包服务商 Inputs.io 遭受黑客攻击[119],黑客通过电子邮件账号进行入侵,进而劫持代管账号,从中盗取了 4 100 个比特币.

(9) 重放攻击(replay attack)[120]:主要包含单链重放攻击和多链重放攻击.单链重放攻击中,攻击者通常在以太坊等账户余额模型的区块链系统中先发起一笔交易 A(如交易所提现),然后对 A 的时间戳等数据进行修改,获得新的交易 B 并进行广播.因为 B 的私钥签名和公钥加密齐全,所以矿工会在付款方余额足够的情况下将交易 B 打包进新区块.攻击者不断重复便可获取大量资金,直至付款方账户余额不足为止.多链重放攻击通常出现在区块链硬分叉时,此时用户的地址和私钥生成算法相同,所有“一条链上的交易在另一条链上也往往是合法的”,所以攻击者在其中一条链上发起的交易后,可以重新将该交易广播到另一条链上,并得到整个系统的确认.

6.3 防御策略与方法

相比区块链其他层级,应用层攻击的场景更加具体、复杂,所以攻击者的手段也十分多样.因此,区块链应用层面临的安全问题应从实际的服务场景出发,设计合适的防御策略和相关技术.在挖矿场景中,攻击者采用的攻击方式大多具备社会工程学攻击特性,即攻击者会根据矿机漏洞、挖矿机制漏洞采取趋利的挖矿行为, 通过损害矿池或其他矿工利益,实现自身利益的最大化.

针对矿机的系统漏洞,可以尝试以下防御策略.

(1) 开发阶段:开发人员应在开发阶段设定软件安全开发生命周期,建立安全漏洞管理机制,在成品销售

前对矿机系统进行代码审计、性能测试,以预防 0day 漏洞攻击.

(2) 部署阶段:矿工应该在原有的软件防护基础上增加辅助的安全检测技术,如入侵检测、防火墙、蜜罐技术等,进一步预防网络渗透攻击和地址篡改攻击.

此外,攻击者可以利用挖矿机制中存在的漏洞恶意骗取、竞争出块奖励,也可以通过扰乱交易顺序实现双花攻击等.其中,算力伪造攻击和扣块攻击属于恶意骗取矿池出块奖励的攻击行为,可以尝试以下防御策略.

(1) 身份管理机制:矿池应结合保证金奖惩机制(如 Casper 机制)和身份认证机制,对新加入的矿工进行身份认证,要求其缴纳一定的保证金,为其诚实的挖矿行为做保证.

(2) 细粒度的工作量检验算法:矿池应定时更新其使用的工作量检验算法,对以往算法中存在的问题进行背书,作为新算法设计的重要依据.

(3) 合理的绩效制度:矿池应定时对矿工进行绩效考核,奖励表现优秀的矿工,驱逐效率低下的懒惰矿工.对矿池内的矿工行为进行管理和约束,保证矿池公平有序地运行.

(4) 相互监管制度:设置矿工相互监管奖励,一旦矿工因进行算力伪造攻击和扣块攻击而被举报,则矿池奖励举报者,没收恶意矿工的保证金,将其加入黑名单后驱逐出矿池,不再录用.

丢弃攻击、空块攻击、通用挖矿攻击则属于恶意竞争出块奖励攻击行为.丢弃攻击中,攻击者主要依赖于网络资源优势,可以比其他节点更快获取数据上链信息,也可以更快地完成数据打包上链.所以丢弃攻击可以看作是女巫攻击的变种攻击,也可以作为自私挖矿攻击的前置攻击,提高攻击者实施自私挖矿攻击的成功率.为了防止丢弃攻击,区块链网络可以引入身份认证机制,对用户潜在的节点身份进行关联分析,杜绝单个用户通过操纵多个节点获取远高于其他节点的网络优势.在空块攻击场景中,攻击者之所以可以通过生成空块恶意竞争奖励,是因为区块链网络不存在对新区块的有效性验证过程.因此,区块链网络节点只要在获取新区块时执行有效性验证,即可有效缓解阻止空块攻击.通用挖矿攻击则需要特定的场景才可以实施,其关键在于攻击者利用新系统与旧系统之间相同的架构和共识机制导致的矿机(算力)通用问题,通过成熟系统的中算力对新系统实现算力压制,从而恶意竞争出块奖励,甚至实施双花攻击、卖空攻击等恶意行为.因此,新区块链项目必须考虑系统封闭性、专机专用等问题,从根本上杜绝算力通用导致的通用挖矿攻击.

芬尼攻击、种族攻击、交易顺序依赖攻击属于扰乱交易顺序类的攻击方式.芬尼攻击和种族攻击主要针对的是支持零确认交易的服务场景,前者主要利用挖矿便利,攻击者只有在挖到包含自己交易的区块时,才会通过零确认交易扰乱交易秩序,实现代币双花等目的;而后者和交易顺序依赖攻击则是通过提高交易 *Gas* 的方式扰乱交易顺序,进而实现代币双花等目的.这两者的共性在于区块链节点在接受新区块时未验证区块内交易与交易池中的未确认交易是否存在冲突.由于零确认交易可以满足商家的即时性支付需求,所以直接通过禁止零确认交易来阻止芬尼攻击和种族攻击的方式不具备可行性.区块链系统可以考虑开通钱包的子账户来保证零确认交易的安全性,即,用户需要通过专门的子账户才能完成零确认交易操作.此时,零确认交易由矿工单独打包验证,在一定程度上可以避免零确认交易与普通交易的冲突.此外,为了避免攻击者扰乱交易顺序,区块链系统可以要求矿工在打包交易时,通过代币锁定技术缴纳保证金之后再广播新区块.其他节点在接受新区块时,可以就区块内交易在交易池中进行遍历验证:如果通过验证,则接受新区块;否则,该节点可以通过举报矿工恶意行为来获取矿工被锁定的保证金及出块奖励.

在区块链交易场景中,攻击者的最终目的是通过直接或间接手段获取用户节点的账户信息,进而盗取资产,主要存在交易平台和用户账户两个攻击目标.为了保证交易平台中用户的账户隐私,交易平台应采取以下措施.

(1) 引入密码安全等级分析机制.系统可以在用户设置账户密码时,对当前密码的安全性进行实时评级,避免用户使用弱口令,从而预防弱口令攻击.

(2) 交易平台应在用户登录账号时进行人机识别,在一定程度上缓解撞库攻击.而用户也应该注意避免多网站的密码通用问题,可以考虑对账户进行安全等级评估,相同安全等级的账户采用相同的密码,这样既可以缓解撞库攻击,也能避免账户密码过多给用户带来的密码管理问题.

(3) 通过限制目标账户的登陆频率和限制单节点的访问请求频率,从被访问端和访问端两个方向限制攻

击者的攻击能力,可以有效预防穷举攻击.

(4) 启用 API 调用接口认证机制,合理管理交易平台的 API 接口,预防 API 接口攻击.

(5) 提高开发工程师的安全素养,在一些敏感系统里单独实现一些额外的认证机制,避免单点登陆漏洞.

此外,用户在日常交易中应该提高个人的安全意识,采取相应的安全措施,避免在交易过程中泄露了个人账户的隐私数据,具体需要从以下几方面考虑.

(1) 培养好安全意识,提高对危险网站、邮件的辨识能力,预防钓鱼攻击.

(2) 构建全面的系统安全防护体系,安装防火墙等安全软件,预防木马劫持攻击.

(3) 利用安全的路由协议对区块链网络实现全方位覆盖,预防中间人劫持攻击.

(4) 实现离线的密钥管理,预防攻击者对在线密钥存储中的私钥窃取.

(5) 利用代码审计、逆向漏洞分析、反逆向工程等技术对钱包客户端代码的安全性进行评估.

(6) 在使用数字货币钱包时,对一些来源不明的小额资金“粉尘”进行标记并禁用,预防粉尘攻击.

(7) 使用专门的零钱包存储该用户持有的“粉尘”级资产,其中既包含攻击者发送的“粉尘”,也可能包含用户自身交易产生的小额资金.为了资产安全,该零钱包中的资金专用于隐私性不高的交易.

在针对认证机制漏洞的 SIM hack 攻击场景中,攻击者主要是利用服务商提供的“账户找回”服务中的安全隐患来成功获取目标账户.因为基于手机、邮件的二次验证并不是完全安全的方法,因此服务商应尝试使用采取 2FA 等具备更高安全性的有更高级别安全设置的服务.2FA 是基于时间、历史长度、实物,例如信用卡、SMS 手机、令牌、指纹等自然变量结合一定的加密算法组合出的一组动态密码,一般每 60s 刷新一次.这种方法不容易被破解,相对较安全.

理论上,基于 UTXO 结构的区块链系统可以抵抗重放攻击,因为转账是基于每一笔 UTXO 进行的原子级别操作,不存在一笔 UTXO 被重复扣除的情况.但是在类似以太坊的账户结构中,交易是通过余额判断合法性的,只要余额足够就可以进行重复扣款转账,一笔交易的信息进行多次广播的重放攻击是可行的.交易延展性攻击和重放攻击非常相似,它们都是对交易所发起的攻击方式,但重放攻击主要针对区块链硬分叉的情况,而交易延展性攻击讲究的是区块标识的可变性.

此外,基于 Hyperledger Fabric 的区块链也可以抵抗重放攻击,该框架中采用 Endorser 节点对客户端提交的交易预案进行身份验证,若交易信息异常,则系统终止操作,这种方式可以有效阻止重放攻击.以太坊的账户结构中存在一个参数 *Nonce*,该参数的值等于从这个账户中发出交易的数量.当交易完成验证后,发送者账户中的 *Nonce* 值会自动增加 1.当矿工验证一笔交易是否合法的时候,矿工会对比交易包含的 *Nonce* 值,并与该交易的发送者账户中的 *Nonce* 值进行比较,相等才算作合法交易,并对该交易打包出块.单链重放攻击无法修改发送者账户的数值,因此当接受到重复交易时,矿工会直接判定它无效,从而阻止了单链重放攻击.面对多链重放攻击时,可以参考以太零开发团队的做法,建立一个交易锁.当一笔交易发起时,交易锁将被广播到整个区块链网络.此时,交易锁会锁定交易关联的数字资产.交易在主节点验证期间,原交易资产被锁定无法使用,以此达到抵御多链重放攻击的目的.

7 区块链攻击簇与安全防御体系

区块链网络中,攻击者可能通过单个区块链攻击,也可能通过包含多种攻击的区块链攻击簇来实现最大化获利的目的.如表 1 所示,本文对这些区块链攻击方式进行了整理和分析,梳理了各种攻击方式之间的潜在联系.此外,很多攻击方式不只局限于前文所述的攻击目标(场景)和攻击目的.攻击场景不同,实施方式多样,带来的安全威胁也不尽相同.为了更好地预防这些攻击,本节进一步研究了区块链攻击簇的基本原理,整理出了本文涉及的区块链攻击方式中所有潜在的攻击簇(如图 5 所示),并尝试构建出了一个较为全面的区块链安全防御体系.

Table 1 Summary of block-chain attacks

表 1 区块链攻击总结

分类			攻击方式	主要攻击目标	主要攻击目的	潜在前置(子)攻击	潜在后续攻击	攻击难度
数据层攻击	数据隐私窃取		碰撞攻击	Hash 函数	破坏系统安全	–	卖空攻击	高
			后门攻击	密码学算法		–	卖空攻击	高
			量子攻击	密码学工具		–	卖空攻击	高
			交易特征分析	交易数据	获取用户隐私	窃听攻击,中间人劫持攻击	粉尘攻击	低
	恶意数据攻击		交易延展性攻击	交易数据	代币双花	–	双花攻击	较低
			恶意信息攻击	区块数据	破坏网络环境	–	–	低
网络层攻击	针对P2P网络的攻击		客户端漏洞	网络节点	获取节点控制权	0day 漏洞攻击	木马劫持攻击、窃听攻击	较低
			窃听攻击		获取用户隐私	客户端漏洞	交易特征分析	低
			日蚀攻击		隔离目标节点	BGP 劫持攻击、女巫攻击	51%攻击	中
			BGP 劫持攻击	区块链网络	分割网络	–	分割攻击,日蚀攻击	中
			分割攻击			BGP 劫持攻击	双花攻击,克隆攻击	中
			DoS 攻击		拒绝服务	–	卖空攻击	高
			DDoS 攻击			木马劫持	卖空攻击	中
			BDoS 攻击			–	卖空攻击	低
			交易延迟攻击		影响交易进程	–	–	低
共识层攻击	针对授权共识机制的攻击		女巫攻击	BFT,PBFT	妨碍共识	私钥窃取攻击	日蚀攻击	较低
			克隆攻击	PoA	代币双花	分割攻击	双花攻击	较高
	针对非授权共识机制的攻击	恶意筹码获取	傀儡挖矿攻击	客户端资源	获取筹码	木马劫持攻击、网络渗透攻击	51%攻击	较高
			币龄累计攻击	PoS,DpoS,PoW/PoS		–	51%攻击	较高
			贿赂攻击	PoW,PoS,DPoS		–	51%攻击	较高
		51%攻击	双花攻击	PoW,PoS	代币双花	51%攻击、分割攻击等	卖空攻击	高
			历史修复攻击	PoW,PoS,DPoS	代币双花、回滚交易	51%攻击	卖空攻击	高
			卖空攻击	PoS	期货倒卖获利	DoS/DDoS 攻击、双花攻击等	–	高
			自私挖矿攻击	PoW	恶意竞争出块奖励	51%攻击、丢弃攻击等	–	高
		其他攻击	无利害关系攻击	PoS		–	–	低
			预计算攻击	PoS		–	自私挖矿攻击	低
			长距离攻击	PoS	代币双花	–	双花攻击	中
合约层攻击	针对智能合约的攻击		整数溢出漏洞	合约代码	恶意篡改变量	–	–	低
			时间戳依赖攻击		预测合约结果	–	–	低
			调用深度攻击	合约调用	恶意调用获利	–	误操作异常攻击	低
			误操作异常攻击			调用深度攻击	–	低
			重入攻击			–	–	低
	针对合约虚拟机的攻击		逃逸漏洞	合约运行	恶意运行获利	–	木马劫持攻击	低
			逻辑漏洞			–	–	较低
			资源滥用漏洞	虚拟机硬件资源	浪费系统资源	–	–	低
应用层攻击	挖矿场景中的攻击	针对矿机系统的攻击	0day 漏洞攻击	应用程序或系统	入侵矿机系统	–	客户端漏洞	低
			网络渗透攻击	网络系统		木马劫持攻击、钓鱼攻击等	篡改攻击、傀儡挖矿攻击	较低
			地址篡改攻击	区块链交易	篡改奖励地址	木马劫持攻击、网络渗透攻击	–	中

Table 1 Summary of block-chain attacks (Continued)

表 1 区块链攻击总结(续)

分类			攻击方式	主要攻击目标	主要攻击目的	潜在前置(子)攻击	潜在后续攻击	攻击难度
应用层攻击	挖矿场景中的攻击	针对挖矿机制的攻击	算力伪造攻击	矿池	骗取联合挖矿奖励	–	–	低
			扣块攻击			–	芬尼攻击	低
			丢弃攻击	诚实矿工	恶意竞争出块奖励	–	自私挖矿攻击	低
			空块攻击	诚实矿工		–	–	低
			通用挖矿攻击	初始化区块链系统		–	51%攻击	较高
			交易顺序依赖攻击	区块链交易	扰乱交易顺序	–	芬尼攻击、种族攻击	较低
			芬尼攻击	零确认交易场景	代币双花	扣块攻击、交易依赖攻击	双花攻击	较低
			种族攻击	零确认交易场景	代币双花	交易顺序依赖攻击	双花攻击	较低
	区块链交易场景中的攻击	针对交易平台的攻击	弱口令攻击	用户账户	获取账户控制权	–	网络渗透、在线钱包窃取	低
			撞库攻击			–		较低
			穷举攻击			–		低
			单点登录漏洞			–	网络渗透	低
			API 接口攻击			–		低
		针对用户账户的攻击	钓鱼攻击	账户隐私		–	木马劫持攻击、SIM hack 等	低
			中间人劫持攻击			–	SIM hack、交易特征分析等	低
			木马劫持攻击			钓鱼攻击、逃逸漏洞等	私钥窃取、傀儡挖矿攻击等	较低
			私钥窃取攻击			木马劫持攻击	女巫攻击	中
			钱包客户端漏洞			0day 漏洞攻击	私钥窃取	低
			粉尘攻击		获取账户资产	交易特征分析	–	较低
			SIM hack	账户控制权		钓鱼攻击、中间人劫持攻击等	在线钱包账号窃取	较低
			在线钱包窃取			SIM hack 等	–	中
			重放攻击	账户资产		–	–	低

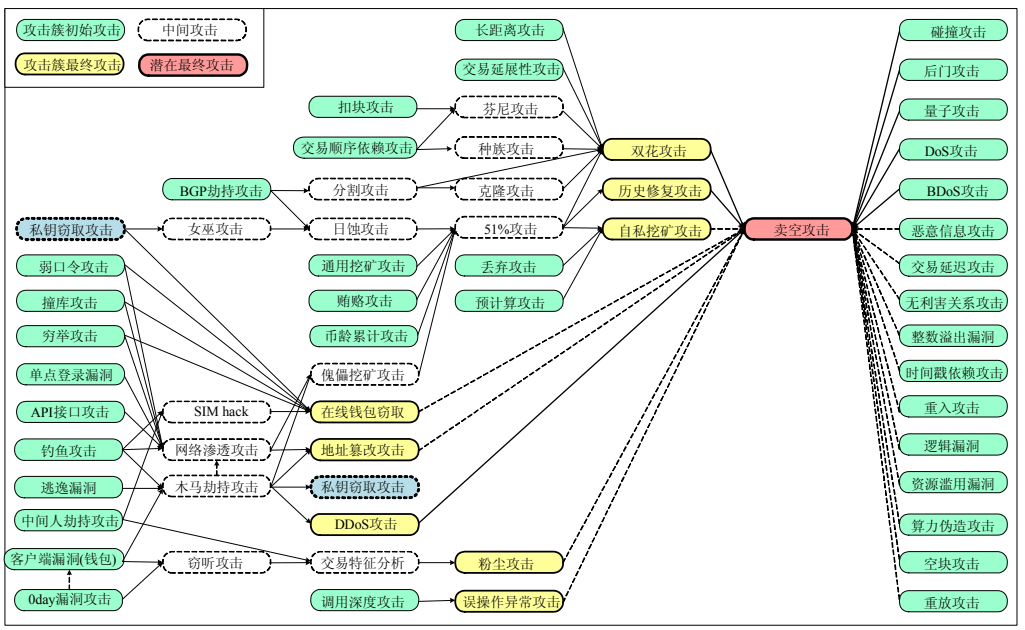


Fig.5 Associations view between block-chain attacks

图 5 区块链攻击关联视图

7.1 区块链攻击簇

区块链的技术特性和安全性,是人们考量区块链技术实用性的两个重要指标.理论上,任何区块链攻击造成的危害达到一定程度时,均可导致区块链网络产生动荡,使其中流通的代币面临贬值风险.尤其是在支持证券信用交易的区块链网络中,攻击者可以通过卖空攻击倒卖期货产品获利.因此,本节将从卖空攻击出发,对所有可能导致代币贬值的安全因素进行溯源分析,探究导致区块链网络安全问题的根本原因.

在支持证券信用交易的区块链网络中,本文涉及的所有区块链攻击均为卖空攻击的前置攻击,即所有攻击方式构成一个卖空攻击簇.前置攻击的安全威胁越大,则其导致的代币贬值率Δ越大,卖空收益$\Delta(B-A)$也越大.如图 5 所示,部分攻击方式(图 5 虚线箭头标识)需要造成大规模的网络损失才有能帮助攻击者实现最大化的卖空获利,而一些攻击方式(图 5 实线箭头标识)则可以轻易帮助攻击者实现最大化的卖空获利.此外,卖空攻击的直接前置攻击可能是单个攻击(图 5 右侧),也可能是攻击簇(图 5 左侧).其中,碰撞攻击、后门攻击、量子攻击属于区块链数据层攻击,严重威胁了区块链底层数据的安全性.一旦攻击者通过这些攻击实现卖空攻击,则将导致区块链系统崩溃,由此实现最大化的卖空获利(Δ=1).攻击者也可以通过 DoS 系列攻击(DDoS,BDoS)使区块链网络瘫痪,从而获取较大的代币贬值率,实现最大化的卖空获利.

此外,完整的攻击簇也可以作为卖空攻击的前置攻击,其中包括:

(1) 双花攻击簇.如图 5 所示,双花攻击簇主要存在 7 种潜在的双花攻击前置攻击方式,其中包括 2 种攻击簇初始攻击:长距离攻击和交易延展性攻击;还包括 5 种中间攻击:芬尼攻击、种族攻击、分割攻击、克隆攻击和 51%攻击,主要涉及扣块攻击、BGP 劫持攻击、通用挖矿攻击、贿赂攻击、币龄累计攻击等 16 种攻击簇初始攻击.这些攻击方式可以在具体服务场景中,使攻击者生成的无效交易(代币已支出或待支出)合法化,从而达成“代币双花”的最大获利目的.

(2) 历史修复攻击簇.历史修复攻击实质上是通过多轮 51%攻击实现交易回滚、历史修复的攻击方式,所以其潜在的前置攻击方式只有 1 种中间攻击:51%攻击,涉及通用挖矿攻击、贿赂攻击、币龄累计攻击等 12 种攻击簇初始攻击.这些攻击方式侧重于帮助攻击者获取超过全网一半的记账权竞争资源,攻击者可以通过恶意竞争记账权实施 51%攻击,从而实现交易回滚、历史修复的攻击目的.

(3) 自私挖矿攻击簇.主要包括 3 种潜在的前置攻击方式,其中包括 2 种攻击簇初始攻击:丢弃攻击和预计算攻击以及 1 种中间攻击:51%攻击,涉及通用挖矿攻击、贿赂攻击、币龄累计攻击等 12 攻击簇初始攻击.这些攻击方式侧重于帮助攻击者积累并保持恶意竞争挖矿奖励的优势.这 3 种前置攻击的结合使用,不仅可以帮助攻击者恶意竞争挖矿奖励,还可以帮助攻击者积累优势,使其可以连续获得区块奖励.其中,51%攻击可以帮助攻击者建立前期的攻击优势,而丢弃攻击和预计算攻击则可以帮助攻击者实现最大化的获利.如果攻击者无法拥有足够的网络资源来实现网络监听和快速的数据传播,则其无法保证攻击者总是可以在其他节点之前将自己的区块公布至全网.一旦攻击者自私挖矿失败、连胜中断,则其不仅无法继续获取出块奖励,还会失去自己前期通过 51%攻击和预计算攻击积累的全部攻击优势.因此,实现丢弃攻击是提高自私挖矿攻击可行性的关键.

(4) 在线钱包窃取攻击簇.主要包含 5 种潜在的前置攻击方式,其中包括 3 种攻击簇初始攻击:弱口令攻击、撞库攻击、穷举攻击以及 2 种中间攻击:私钥窃取攻击和 SIM hack 攻击,涉及钓鱼攻击、逃逸漏洞、客户端漏洞、0day 漏洞攻击等 4 种攻击簇初始攻击.这些攻击方式侧重于帮助攻击者获取用户的账户隐私,攻击者通过劫持用户账户来盗取账户资金.

(5) 地址篡改攻击簇.地址篡改攻击可以分为奖励地址篡改和收款地址篡改两种,其攻击原理基本一致,潜在的前置攻击方式包括 2 种中间攻击:网络渗透攻击和木马劫持攻击,主要涉及弱口令攻击、撞库攻击、穷举攻击、单点登录漏洞等 9 种攻击簇初始攻击.这些攻击方式侧重于帮助攻击者获取交易所、矿机系统等区块链网络实体的系统漏洞,攻击者可以根据这些漏洞进行地址篡改,劫持并盗取攻击目标的入账资金.

(6) DDoS 攻击簇.DDoS 攻击的核心思想是:攻击者通过一些网络手段,整合零散的网络资源来攻击区块

链网络,导致网络瘫痪拒绝服务.DDoS 攻击簇的潜在前置攻击方式包含 1 种中间攻击:木马劫持攻击,涉及 4 种攻击簇初始攻击:钓鱼攻击、逃逸漏洞、客户端漏洞、0day 漏洞攻击.这些攻击簇初始攻击旨在帮助攻击者获取用户节点的控制权,攻击者通过这种方式控制大量的用户节点,即可获取足够的网络资源来实施 DDoS 攻击,从而实现期货卖空获利等潜在攻击目的.

(7) 粉尘攻击簇.粉尘攻击是攻击者追踪目标用户钱包、账户,从而盗取用户账户资产的攻击方式.这种攻击簇的潜在前置攻击方式主要包括 2 种中间攻击:窃听攻击和交易特征分析,涉及 3 种初始攻击:中间人劫持攻击、钱包客户端漏洞和 0day 漏洞攻击.攻击者可以利用这些初始攻击发动中间攻击来获取用户钱包、账户信息,从而间接实现盗取用户钱包、账户余额的攻击目的.

(8) 误操作异常攻击簇.主要包括 1 种潜在前置攻击:调用深度攻击,旨在帮助攻击者在智能合约运行的场景中,根据合约调用次数受限的特点实现误操作,从而获利.

综上所述,卖空攻击簇主要涉及 37 种初始攻击,这些攻击方式反映了区块链网络最底层的安全漏洞和威胁.因此,构建区块链安全防御体系的关键,是在区块链系统模型设计阶段解决这些初始攻击所依赖的安全漏洞,从根本上缓解、甚至解决区块链系统面临的诸多安全问题.

7.2 区块链安全防御体系

区块链安全防御体系的构建,仅依靠简单堆砌现有攻击解决方案是显然不够的,并且很多解决方案只能在一定程度上缓解相应攻击方式带来的危害,这降低了区块链网络的安全性上限.因此,构建区块链安全防御体系,应当从现有的攻击方式出发,逆向追溯并解决所有的潜在前置攻击,从根本上缓解或解决这些区块链攻击.同时,结合现有的一些区块链安全技术,进一步解决遗留的安全问题.本节将在攻击关联分析的基础上,通过设计区块链底层系统模型,从源头解决上述 37 种初始攻击依赖的安全漏洞和技术缺陷;同时,结合已有的区块链上层安全防御技术,为区块链网络提供追加式的安全保护,以此构建出较为全面的区块链安全防御体系.

7.2.1 区块链底层模型设计

区块链系统模型设计的合理性,往往决定着区块链网络的安全性和实用性.如:密码学工具的安全性决定着区块链数据的安全性,共识机制的方案特性决定着区块链网络交易的吞吐量和安全性等.因此,构建区块链安全防御体系的关键在于设计出一个合理、安全、逻辑紧密的系统模型.根据卖空攻击簇涉及的 37 种初始攻击的特性,本文将从以下几个层面出发设计区块链系统模型.

(1) 底层技术安全:包括密码学工具的安全性、P2P 网络的安全性,可从以下几点考虑.

① 严格评估待选密码学工具的安全性,避免采用被植入后门的密码学工具,以阻止攻击者发起的碰撞攻击、后门攻击和交易延展性攻击.

② 提高系统对多种密码学工具的兼容性,以满足用户在多样化服务场景中的安全性需求.

③ 根据实际安全需求选择备用的密码学工具作为应急预案,以应对量子攻击、密码算法破解等安全事件带来的安全威胁,提高系统稳健性.

④ 设计并部署数据过滤模型和数据上链协议,避免攻击者通过恶意信息攻击破坏区块链网络环境.

(2) 运行机制安全:科学合理的区块链运行机制是保证区块链网络良好运行的关键,所以在构建区块链系统时,开发者应尝试引入科学合理的挖矿机制、共识机制和交易机制.

① 公平的挖矿机制:系统应在矿工的客户端内置 Casper 协议,利用惩罚措施阻止恶意矿工通过无利害关系攻击和空块攻击实现最大化收益.在矿池挖矿的场景中,矿池应采用矿工算力监测和工作量检验算法并行的方式,评估矿工工作量的合理性,以此杜绝矿工通过算力伪造攻击和扣块攻击获取额外奖励的可能性.通过这些方法,可以在一定程度上保证矿工的平均盈利,避免矿工因无法盈利而发起 BDoS 攻击.

② 安全的共识机制:由于构造的差异性,不同共识机制所具备的优势和缺陷也不尽相同.为了保证全网节点竞争记账权的公平性,应从以下几点考虑.

(a) 针对授权共识机制中存在的女巫攻击,区块链系统需要引入身份验证机制对网络节点进行

身份验证和身份关联分析,对申请多个身份的用户征收费用,提高攻击者通过申请多个身份实施女巫攻击的攻击成本,在一定程度上缓解女巫攻击.

(b) 在 PoS 系统中,币龄累计攻击为攻击者提升自身记账权竞争的成功率提供了可能,而币龄的定义是 PoS 系统运行的基础,所以废除币龄定义方式的解决方案不具备可行性.因此,PoS 区块链系统应该引入币龄预警、清零机制(详见第 4.3 节)作为补充,通过对用户节点所持币龄的上限进行限制,从而缓解币龄累计攻击带来的安全威胁.

(c) 在 PoW+PoS 系统中,应对区块计算方式进行调正,避免当前区块的哈希值单独且直接影响下一区块的生成难度,从而阻止预计算攻击.

(d) 新区块链系统应避免使用与已有系统相同的架构和共识算法,尽可能通过专机专用的方式避免算力通用的问题,从根本上解决通用挖矿攻击.若无法避免,则该系统应在客户端内置 Casper 协议,以此缓解通用挖矿攻击带来的安全威胁.

(e) 设计新共识算法时,可以考虑引入如信用、评分等机制,以支持基于非代币的 Casper 协议,解决代币类 Casper 协议中用户因为缴纳保证金过多而影响正常交易的问题,在不影响用户交易的情况下,预防各种社会工程学攻击.

③ 有序的交易机制:在区块链网络中,应结合基于信誉等非代币系统的奖惩机制规范用户节点的交易行为.以基于信誉系统的奖惩机制为例,攻击者可能通过恶意悬赏的方式贿赂矿工沿着指定的方向挖矿,也可能通过提高交易 *Gas* 值的方式促使矿工提前打包指定交易.因此,针对贿赂攻击和交易顺序依赖攻击中的恶意悬赏,矿工可以搜集证据并举报攻击者.一旦成功,举报者可以获得全部的悬赏金和定量的信誉值提升,攻击者悬赏交易作废,信誉值降低,直至无法参与区块链交易.此外,矿工也可以通过举报实施交易延迟攻击和重放攻击的攻击者来获取更高的信誉值,缓解用户恶意交易行为带来的安全隐患.

(3) 设备系统安全:区块链网络涉及诸多设备,如互联网终端、合约虚拟机、矿机等.尽管这些设备用途不同,但面临的安全威胁大多一致,所以可以采用以下方法来保证区块链设备的系统安全性.

① 避免使用可能存在单点登陆漏洞、逃逸漏洞等软件漏洞的设备和客户端软件.开发商应在产品开发阶段使用规范的编程逻辑开发相关软件,并在出厂销售前对产品的安全性进行全方位的测试与评估.用户节点在使用相关产品时,也应对其进行安全性评估,避免使用存在安全问题的产品.

② 为设备构建安全的防御层.首先,使用 DoS 攻击防火墙,保证设备系统在 DoS 攻击下的可用性和稳健性;其次,合理管理系统 API 接口,实现细粒度的访问控制,预防 API 接口攻击.同时限制单位时间内其他节点的访问频率和 API 接口(数据)的被访问频率,从访问者和被访问者两个角度实现对穷举攻击的全面防御.

(4) 智能合约安全:智能合约的安全隐患主要包括合约代码漏洞和合约调用漏洞.

① 首先,开发者在编写智能合约时应注重严谨的编程逻辑,避免合约代码出现整数溢出、时间戳依赖等常见代码漏洞(详见第 5.3 节).在部署智能合约前,用户应对智能合约进行代码审计,评估智能合约的安全性.

② 其次,对于合约调用类攻击(调用深度攻击、重入攻击),开发者可以在编写智能合约时对合约的调用次数进行限制,例如设置智能合约调用次数超过限定深度时,智能合约按照前一次的参数输入运行,避免智能合约由于超限的调用次数导致的合约调用失败.

③ 此外,在合约进行调用时应严格执行返回参数验证的过程,从而预防重入攻击和由调用深度攻击导致的误操作异常攻击.

(5) 用户行为安全:用户在区块链网络中的不良行为习惯可能导致其面临隐私信息泄露和资产被盗的风险,因此,健全的用户行为规范是区块链安全防御体系的重要一环.首先,用户节点在设置账户口令时应避免使用弱口令,同时避免在多个网站使用相同的账号和口令,预防攻击者发起的弱口令攻击和撞

库攻击.此外,在日常的区块链网络活动中应提高个人安全意识,忽略来历不明的邮件和网址,避免落入攻击者为实施钓鱼攻击和中间人劫持攻击而设置的陷阱.

7.2.2 区块链上层技术兼容

区块链的底层模型设计旨在从源头缓解甚至解决 37 种初始攻击依赖的安全漏洞,但仍可能遗留下很多安全问题.本节在此基础上,通过兼容一些区块链上层技术进一步完善本文的区块链安全防御体系.

(1) 基于智能合约的 Casper 奖惩协议:尽管以太坊引入的 Casper 机制可以通过惩罚恶意节点的方式来阻止攻击者借助运行机制漏洞来获取最大化利益的“擦边球”行为,如挖矿场景中的无利害关系攻击、空块攻击和算力伪造攻击等,然而其内置 Casper 协议于 PoS 系统客户端的做法限制了 Casper 机制的扩展性和灵活性,无法满足多样的服务需求.而独立的 Casper 机制则需要一个高权限的可信管理者,这与区块链去中心化的思想相悖.智能合约技术的出现,为解决 Casper 机制的应用问题提供了思路.区块链系统在初始化阶段可以提供基于智能合约的 Casper 奖惩协议模板,全网节点可以在参与公共活动(如挖矿、投票等)时初始化并加入特定的 Casper 智能合约,通过奖励举报者、惩罚被举报恶意节点的方式,保证活动的公平性和有序性.

(2) 基于 ARTEMIS 的网络异常监测技术:为了应对网络层存在的 BGP 路由劫持攻击和分割攻击,在区块链系统中部署 ARTEMIS 系统是十分必要的.该系统可以在几分钟内帮助服务提供商解决 BGP 劫持的问题,为实现实时的 BGP 劫持监控及应急响应提供可能.然而,ARTEMIS 系统仅对造成网络异常的 BGP 路由劫持攻击和分割攻击具备较高的识别率,而对攻击者通过选择性管控流量发起的 BGP 路由劫持攻击和分割攻击无效.因此,区块链节点在出块时,可以通过第 4.3 节所述的基于权重的节点活性检测方法检查网络是否发生分区现象,此处不再赘述.通过部署由 ARTEMIS 技术和基于权重的节点活性检测方法组成的网络异常监测技术,可以很好地解决网络层存在的安全隐患及其潜在的后置攻击(如克隆攻击),保证区块链网络的正常运行.

(3) 集成式的代码评估模型:为了应对 0day 漏洞攻击、逻辑漏洞等代码漏洞问题,保证区块链网络设备和智能合约的代码安全,系统开发者应尝试构建出一套完整全面的代码评估模型,合理兼容现有包括 Fuzzing、代码审计、逆向漏洞分析、反逆向工程等在内的代码监测评估技术.在此基础上,可以引入机器学习等技术实现全方位的漏洞扫描与风险预测,进一步提升代码评估模型的效率与准确性,保证区块链网络中的代码安全.

7.3 区块链攻防技术发展态势

目前,区块链网络中发生的安全事件以网络层、合约层和应用层攻击为主,其中,网络层攻击多为传统网络中的常见安全问题,这是由当前区块链网络基于传统网络的现状导致的.因此,传统网络中的安全防御技术也可以用于解决区块链网络层攻击.所以,本文的区块链安全防御体系可以通过不断兼容传统网络中已有或新兴的安全防御技术,来保证区块链网络的安全运行.此外,合约层攻击和应用层攻击大多是由代码漏洞、客户端漏洞和用户社会行为漏洞导致的,这些最底层的漏洞是无法完全避免的,所以本文的区块链安全防御体系旨在不断完善区块链底层模型设计,通过科学合理的制度不断规范用户的行为,以此减少安全漏洞.同时,在技术兼容方面,区块链安全防御体系可以通过不断兼容新型的漏洞检测方法或策略来完善自身集成式的代码评估模型,以此保证区块链系统的健壮性.

值得注意的是:目前已发生的区块链安全事件大多只会影响区块链网络的正常运行,但无法从根本上摧毁区块链系统,这是因为区块链的底层技术和合理运行机制在一定程度上保证了区块链系统的安全性.一旦数据层和共识层中的大多数攻击,如碰撞攻击、量子攻击、51%攻击等目前仅理论上可行的区块链攻击具备实际发生的条件,则区块链系统无疑面临着崩溃的风险.因此,构建区块链安全防御体系需要在保证当前系统安全的同时,通过技术预研增强防御体系自身的稳健性.本文构建的区块链安全防御体系在底层模型设计阶段便要求开发者提高系统对多种密码学工具的兼容性,以满足用户在多样化服务场景中的安全性需求.同时,根据实际安全需求选择备用的密码学工具作为应急预案,以应对量子攻击、密码算法破解等安全事件带来的安全威胁.此外,

本文提出的区块链安全防御体系在上层技术兼容方面同样对新兴的安全防御技术提供了较高的兼容性,因此具备良好的可扩展性,可以为大多数区块链系统提供安全、可靠的持续性防御.

区块链技术的理论研究目前处于 2.0 甚至 3.0 阶段,而应用与推广将在未来很长的一段时间里处于 1.0 至 2.0 的过渡阶段,这种预研优势是保证区块链技术在区块链攻防博弈中持续发展的根本.随着区块链技术的不断推广与应用,多样、复杂的应用场景将使区块链技术面临着更加严峻的安全威胁,而区块链攻击技术势必会关注区块链具体应用场景中由于技术低耦合性导致的安全漏洞.此外,云计算、边缘计算、物联网等新兴技术体系与区块链技术的融合发展,势必成为一种颇具前景的区块链发展模式,而各种技术的短板及技术体系之间的耦合程度仍将成为攻击者的攻击目标.最后,服务场景和技术架构的复杂化,可能为攻击者实现 51%攻击、双花攻击等提供一条新的攻击序列.针对这些潜在的安全威胁,通过维护区块链攻击关联视图来准确评估系统安全性,结合“底层模型设计+上层技术兼容”提供安全防御的模式,将成为区块链安全防御技术的主流.尤其是在技术兼容方面,态势感知、溯源追踪、机器学习等新兴技术的应用,将大大提升区块链系统安全防御体系的网络监管和预警能力,为实现快速的攻击检测与追踪溯源提供了可能.

8 总结与展望

区块链凭借其多元融合架构赋予的去中心化、去信任化、不可篡改等技术特性,成为了一种具有里程碑意义的新一代互联网技术,为解决传统中心化服务架构中的信任问题、安全问题提供了一种新的解决思路.因此,区块链技术具备十分重要的科研价值和良好的应用前景.关于区块链的研究甚至一度上升至国家发展战略层面,而安全问题更是区块链研究的重中之重.本文从区块链层级架构和攻击关联分析两个维度出发,首先对现有 60 种区块链攻击方式的攻击原理和防御策略展开研究;然后,通过探究这些攻击之间的潜在联系,归纳出了完整的卖空攻击簇及其 8 个子攻击簇;最后,逆向溯源这些攻击簇涉及的 37 种攻击簇初始攻击,从根本上给出了缓解或解决相应区块链攻击的策略,奠定了区块链安全防御体系的基础.同时,结合现有的安全方案,给出了解决遗留安全问题的防御策略,构建出了相对完整的区块链安全防御体系.

区块链的去中心化结构特性,使其具备了与云计算等中心化服务相同的发展前景,这意味着区块链技术在未来不仅会被用来解决中心化服务架构中的信任问题和安全问题,还会出现在更多的去中心化服务场景中.而在未来的一段时间中,区块链技术的发展将侧重于多服务架构融合的场景,愈加复杂的服务场景将给区块链技术带来更加严峻的安全挑战.因此,针对具体情况进行具体分析,构建支持防御策略动态更新的区块链安全防御体系,是保证区块链技术快速发展的必由之路.

References:

[1] Pawel S, Daniël R, Ivan H, Siwei S. StrongChain: Transparent and collaborative proof-of-work consensus. In: Proc. of the USENIX Security. 2020. 819−836.

[2] Yu HF, Ivica N, Ruomu H, Prateek S. OHIE: Blockchain scaling made simple. In: Proc. of the IEEE S&P. 2020. 90−105.

[3] Liu ZT, Xiang YX, Shi J, Gao P, Wang HY, Xiao XS, Wen BH, Hu YC. HyperService: Interoperability and programmability across heterogeneous blockchains. In: Proc. of the CCS. 2019. 549−566.

[4] George B, Brian NL. Bobtail: Improved blockchain security with low-variance mining. In: Proc. of the NDSS. 2020. https://dx.doi.org/10.14722/ndss.2020.23095

[5] Si XM, Xu MX, Yuan C. Survey on security of blockchain. Journal of Cryptologic Research, 2018,5(5):8−19 (in Chinese with English abstract).

[6] PeckShield. A report on anti money laundering (AML) for digital asset in 2019 (in Chinese). https://m.dapptotal.com/reports/PeckShield_AML_Research_Report_final

[7] Eric B. The Economic Limits of Bitcoin and the Blockchain. National Bureau of Economic Research, Inc., 2018.

[8] Karame G, Androulaki E, Capkun S. Double-spending fast payments in Bitcoin. In: Proc. of the ACM Conf. on Computer and Communications Security. 2012. 906−917.

[9] Orda A, Rottenstreich O. Enforcing fairness in blockchain transaction ordering. In: Proc. of the IEEE ICBC. 2019. 368−375.

[10] Bitcoin Stack Exchange. What is a Finney attack? 2020. https://bitcoin.stackexchange.com/questions/4942/what-is-a-finney-attack

[11] Yuan C. Defense scheme during hard bifurcation in block chain. Modern Computer, 2019(9):3−7,13 (in Chinese with English abstract).

[12] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2020. https://bitcoin.org/bitcoin.pdf

[13] Ma A, Pan X, Wu L, Guo JF, Huang QW. A survey of the basic technology and application of block chain. Journal of Information Security Research, 2017,3(11):968−980 (in Chinese with English abstract).

[14] Liu YZ, Liu JW, Zhang ZY, Xu TG, Yu H. Overview on blockchain consensus mechanisms. Journal of Cryptologic Research, 2019, 6(4):395−432 (in Chinese with English abstract).

[15] Huang JF, Liu J. Survey on blockchain research. Journal of Beijing University of Posts and Telecommunications, 2018,41(2):1−8 (in Chinese with English abstract).

[16] He HW, Yan A, Chen ZH. A survey of smart contract technology and application based on blockchain. Journal of Computer Research and Development, 2018,55(11):2452−2466 (in Chinese with English abstract).

[17] Ethereum. Ethereum official site. 2020. https://ethereum.org

[18] Melanie S. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015.

[19] R3 CEV. R3 official site. 2020. https://www.r3.com

[20] China Ledger. China ledger official site. 2020. http://www.chinaledger.com

[21] Cisco. Cisco official site. 2020. https://www.cisco.com

[22] Hyperledger. Hyperledger official site. 2020. https://www.hyperledger.org

[23] Katz J, Lindell Y. Introduction to Modern Cryptography. 2nd ed., Chapman and Hall/CRC, 2014.

[24] Berndt S, Liśkiewicz M. Algorithm substitution attacks from a steganographic perspective. In: Proc. of the CCS. 2017. 1649−1660.

[25] Decker C, Wattenhofer R. Bitcoin transaction malleability and MtGox. In: Proc. of the ESORICS. 2014. 313−326.

[26] Douceur JR. The Sybil attack. In: Proc. of the IPTPS. 2002. 251−260.

[27] Bonneau J. Why buy when you can rent? Bribery attacks on Bitcoin-style consensus. In: Proc. of the Financial Cryptography and Data Security (FC). 2016. 19−26.

[28] King S, Nadal S. PPCoin: Peer-to-peer crypto-currency with proof-of-stake. 2012. http://people.cs.georgetown.edu/~clay/classes/fall2017/835/papers/peercoin-paper.pdf

[29] Houy N. It will cost you nothing to 'kill' a proof-of-stake crypto-currency. 2014. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393940

[30] CryptoWiki. Proof-of-work system. 2020. http://cryptowiki.net/index.php?title=Proof-of-work_system

[31] 360 Core Security. Hacker forged computational power to steal multiple digital currencies (in Chinese). https://blogs.360.cn/post/

[32] Bag S, Ruj S, Sakurai K. Bitcoin block withholding attack: Analysis and mitigation. IEEE Trans. on Information Forensics and Security, 2017,12(8):1967−1978.

[33] Narayanan A, Bonneau J, Felten EW, Miller A, Goldfeder S, Clark J. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016.

[34] Thomas K, Pullman J, Yeo K, Raghunathan A, Kelley PG, Invernizzi L, Benko B, Pietraszek T, Patel S, Boneh D, Bursztein E. Protecting accounts from credential stuffing with password breach alerting. In: Proc. of the USENIX Security. 2019. 1556−1571.

[35] Bilge L, Dumitras T. Investigating zero-day attacks. 2013. https://www.usenix.org/system/files/login/articles/02_bilge_6-13_online.pdf

[36] Anderson R. Secuirty Engineering: A Guide to Building Dependable Distributed Systems. 2nd ed., Wiley Publishing, Inc., 2008.

[37] Hadnagy C. Social Engineering: The Art of Human Hacking. John Wiley&Sons, 2010.

[38] Jin C, Wang XY, Tan HY. Dynamic attack tree and its applications on Trojan horse detection. In: Proc. of the Multimedia and Information Technology (MMIT). 2010. 56−59.

[39] Grustniy L. Rakhni Trojan: To encrypt and to mine. 2018. https://www.kaspersky.com/blog/rakhni-miner-cryptor/22988/

[40] Barber S, Boyen X, Shi E, Uzun E. Bitter to better-how to make Bitcoin a better currency. In: Proc. of the Financial Cryptography and Data Security (FC). 2012. 399−414.

[41] Lee S, Kim S. Short selling attack: A self-destructive but profitable 51% attack on PoS blockchains. IACR Cryptology ePrint Archive, 2020-019, 2020.

[42] Santis AD, Micali S, Persiano G. Non-interactive zero-knowledge proof systems. In: Proc. of the CRYPTO. 1987. 52−72.

[43] Schwennesen B. Elliptic curve cryptography and government backdoors. 2016. https://services.math.duke.edu/~bray/Courses/89s-MOU/2016/Papers/BAS_Paper3_EllipticCurveCryptography.pdf

[44] Aggarwal D, Brennen GK, Lee T, Santha M, Tomamichel M. Quantum attacks on Bitcoin, and how to protect against them. Ledger, 2018,3:68−90.

[45] Awan MK, Cortesi A. Blockchain transaction analysis using dominant sets. In: Proc. of the Computer Information Systems and Industrial Management (CISIM). 2017. 229−239.

[46] Androulaki E, Karame GO, Roeschlin M, Scherer T, Capkun S. Evaluating user privacy in Bitcoin. In: Proc. of the Financial Cryptography and Data Security (FC). 2013. 34−51.

[47] Fuji R, Usuzaki S, Aburada K, Yamaba H, Katayama T, Park M, Shiratori N, Okazaki N. Investigation on sharing signatures of suspected malware files using blockchain technology. In: Proc. of the Int'l MultiConf. of Engineers and Computer Scientists (IMECS). 2019. 94−99.

[48] Zcash. Zcash official site. 2020. https://z.cash

[49] Wuille P. Segregated witness and its impact on scalability. 2020. http://diyhpl.us/wiki/transcripts/scalingbitcoin/hong-kong/segregated-witness-and-its-impact-on-scalability/

[50] Géron A. Hands-on Machine Learning with Scikit-learn, Keras, and TensorFlow. 2nd ed., O'Reilly Media, Inc., 2019.

[51] Estehghari S, Desmedt Y. Exploiting the client vulnerabilities in Internet E-voting systems: Hacking Helios 2.0 as an example. EVT/WOTE, 2010,10:1−9.

[52] Dai HN, Wang H, Xiao H, Li XR, Wang Q. On eavesdropping attacks in wireless networks. In: Proc. of the 2016 IEEE Int'l Conf. on Computational Science and Engineering (CSE). IEEE, 2016. 138−141.

[53] Heilman E, Kendler A, Zohar A, Goldberg S. Eclipse attacks on Bitcoin's peer-to-peer network. In: Proc. of the USENIX Security. 2015. 129−144.

[54] Apostolaki M, Zohar A, Vanbever L. Hijacking Bitcoin: Routing attacks on cryptocurrencies. In: Proc. of the IEEE S&P. 2017. 375−392.

[55] Sun YX, Edmundson A, Vanbever L, Li O. RAPTOR: Routing attacks on privacy in Tor. In: Proc. of the USENIX Security. 2015. 271−286.

[56] Elleithy KM, Blagovic D, Wang C, Sideleau P. Denial of service attack techniques: Analysis, implementation and comparison. Journal of Systemics, Cybernetics, and Informatics, 2005,3(1):66−71.

[57] Saad M, Thai MT, Mohaisen A. POSTER: Deterring DDoS attacks on blockchain-based cryptocurrencies through mempool optimization. In: Proc. of the ASIACCS. 2018. 809−811.

[58] Cointelegraph. Bitcoin exchange poloniex under severe DDoS attack again, users outraged. 2017. https://cointelegraph.com/news/bitcoin-exchange-poloniex-under-severe-ddos-attack-again-users-outraged

[59] Mirkin M, Ji Y, Pang J, Klages-Mundt A, Eyal I, Juels A. BDoS: Blockchain denial-of-service attacks. arXiv Preprint arXiv:1912.07497, 2019.

[60] Wikipedia. Lightning network. 2020. https://en.wikipedia.org/wiki/Lightning_Network

[61] Sun GZ, Wang JT, Gu Y. Security threat analysis of blockchain technology. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2019,39(5):48−62 (in Chinese with English abstract).

[62] Microsoft. Microsoft security development lifecycle (SDL). 2020. https://www.microsoft.com/en-us/securityengineering/sdl/

[63] Sutton M, Greene A, Amini P. Fuzzing: Brute Force Vulnerability Discovery. Addison-Wesley Professional, 2007.

[64] Dowd M, McDonald J, Schuh J. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Addison-Wesley Professional, 2006.

[65] Klein T. A Bug Hunter's Diary. No Starch Press, 2011.

[66] Roundy KA, Miller BP. Binary-code obfuscations in prevalent packer tools. ACM Computing Surveys, 2013,46(1):1−32.

[67] Dominic L. BlockQuick: Super-light client protocol for blockchain validation on constrained devices. IACR Cryptology ePrint Archive, 2019-579, 2019.

[68] Sermpezis P, Kotronis V, Gigis P, Dimitropoulos X, Cicalese D, King A, Dainotti A. ARTEMIS: Neutralizing BGP hijacking within a minute. IEEE/ACM Trans. on Networking, 2018,26(6):2471−2486.

[69] Amadi EC, Eheduru GE, Eze FU, Ikerionwu C, Okafor KC. Anti-DDoS firewall: A zero-sum mitigation game model for distributed denial of service attack using linear programming. In: Proc. of the 2017 IEEE Int'l Conf. on Knowledge-based Engineering and Innovation (KBEI). IEEE, 2017. 27−36.

[70] Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans. on Programming Languages and Systems (TOPLAS), 1982,4(3):382−401.

[71] Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proc. of the USENIX Symp. on Operating Systems Design and Implementation (OSDI). 1999. 173−186.

[72] Microsoft. Ethereum proof-of-authority on azure. 2018. https://azure.microsoft.com/en-us/blog/ethereum-proof-of-authority-on-azure

[73] Ekparinya P, Gramoli V, Jourjon G. The attack of the clones against proof-of-authority. In: Proc. of the NDSS. 2020. https://dx.doi.org/10.14722/ndss.2020.24082

[74] Bitconch. A newly distributed Web protocol based on an innovative proof reputation (PoR) consensus algorithm. 2020. https://bitconch.io/download/BRWhitePaperEn.pdf

[75] Grigg I. EOS—An introduction. 2020. https://eos.io/documents/EOS_An_Introduction.pdf

[76] Zaccagni Z, Dantu R. Proof of review (PoR): A new consensus protocol for deriving trustworthiness of reputation through reviews. IACR Cryptology ePrint Archive, 2020-475, 2020.

[77] Leonard K. A PoR/PoS-hybrid blockchain: Proof of reputation with nakamoto fallback. IACR Cryptology ePrint Archive, 2020-381, 2020.

[78] Krebsonsecurity. Who and what is coinhive? 2018. https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/

[79] Redman J. Small Ethereum clones getting attacked by mysterious '51 Crew'. 2016. https://news.bitcoin.com/ethereum-clones-susceptible-51-attacks/

[80] Paganini P. Bitcoin gold hit by double-spend attack, exchanges lose over $18 million. 2018. https://securityaffairs.co/wordpress/72878/hacking/bitcoin-gold-double-spend.html

[81] Grunspan C, Pérez-Marco R. On profitability of selfish mining. arXiv Preprint arXiv:1805.08281, 2018.

[82] Kwon J. Tendermint: Consensus without mining. 2014. https://pdfs.semanticscholar.org/df62/a45f50aac8890453b6991ea115e996c1646e.pdf

[83] Szilágyi P. EIP 225: Clique proof-of-authority consensus protocol. 2020. https://eips.ethereum.org/EIPS/eip-225

[84] Buterin V, Griffith V. Casper the friendly finality Gadget. arXiv Preprint arXiv:1710.09437, 2017.

[85] Buterin V. Slasher: A punitive proof-of-stake algorithm. 2014. https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/

[86] Anley C, Heasman J, Lindner F, Richarte G. The Shellcoder's Handbook: Discovering and Exploiting Security Holes. 2nd ed., Wiley Publishing, Inc., 2007.

[87] Bitcoinwiki. Value overflow incident. 2016. https://en.bitcoin.it/wiki/Value_overflow_incident

[88] Hessenauer S. Batch overflow bug on Ethereum ERC20 token contracts and SafeMath. 2018. https://blog.matryx.ai/batch-overflow-bug-on-ethereum-erc20-token-contracts-and-safemath-f9ebcc137434

[89] Alharby M, Moorsel AV. Blockchain based smart contracts: A systematic mapping study. In: Proc. of the Int'l Conf. on Artificial Intelligence and Soft Computing. 2017. 125−140.

[90] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts SoK. In: Proc. of the Int'l Conf. on Principles of Security and Trust. 2017. 164−186.

[91] Kieran E. KoET (king of the ether throne). 2020. https://github.com/kieranelby/KingOfTheEtherThrone

[92] Rodler M, Li WT, Karame GO, Davi L. Sereum: Protecting existing smart contracts against re-entrancy attacks. In: Proc. of the NDSS. 2019. https://dx.doi.org/10.14722/ndss.2019.23413

[93] Fang WD, Zhang WX, Pan T, Chen W, Yang Y. Cyber security in blockchain: Threats and countermeasures. Journal of Cyber Security, 2018,3(2):87−104 (in Chinese with English abstract).

[94] Wikipedia. The DAO. 2020. https://en.wikipedia.org/wiki/Decentralized_autonomous_organization

[95] Zhao HQ, Zhang YY, Yang K, Kim T. Breaking turtles all the way down: An exploitation chain to break out of VMware ESXi. In: Proc. of the USENIX Security. 2019. 1−9.

[96] Xu Y, Li WX, Wang DY. Web security attack and defense: A practical guide to penetration testing. Beijing: Publishing House of Electronics Industry, 2018 (in Chinese).

[97] Chen HS, Pendleton M, Njilla L, Xu SH. A survey on Ethereum systems security: Vulnerabilities, attacks and defenses. ACM Computing Surveys, 2020,53(3):1−43.

[98] Vogelsteller F, Buterin V. EIP 20: ERC-20 token standard. 2015. https://eips.ethereum.org/EIPS/eip-20

[99] Daniel P, Benjamin L. Broken metre: Attacking resource metering in EVM. In: Proc. of the NDSS. 2020. https://dx.doi.org/10.14722/ndss.2020.24267

[100] Kalra S, Goel S, Dhawan M, Sharma S. ZEUS: Analyzing safety of smart contracts. In: Proc. of the NDSS. 2018. http://dx.doi.org/10.14722/ndss.2018.23082

[101] Weidman G. Penetration Testing: A Hands-on Introduction to Hacking. No Starch Press, 2014.

[102] Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Computing Surveys, 2019,52(3):1−34.

[103] McCorry P, Hicks A, Meiklejohn S. Smart contracts for bribing miners. In: Proc. of the Financial Cryptography and Data Security (FC). 2018. 3−18.

[104] Charlie H, Squir RL. Automating attack discovery on blockchain incentive mechanisms with deep reinforcement learning. arXiv Preprint arXiv:1912.01798, 2019.

[105] Dasgupta D. A survey of blockchain from security perspective. Journal of Banking and Financial Technology, 2019,3:1−17.

[106] Weber JE, Guster D, Safonov P, Schmidt MB. Weak password security: An empirical study. Information Security Journal: A Global Perspective, 2008,17:45−54.

[107] Wu YM, Cao P, Withers A, Kalbarczyk ZT, Iyer RK. Mining threat intelligence from billion-scale SSH brute-force attacks. In: Proc. of the NDSS. 2020. https://dx.doi.org/10.14722/diss.2020.23007

[108] Anderson R. Security Engineering. 2nd ed., Wiley Publishing, Inc., 2008.

[109] Whittaker Z, Shu C. Binance says more than $40 million in Bitcoin stolen in ‘large scale’ hack. 2019. https://techcrunch.com/2019/05/07/binance-breach/

[110] Ghasemisharif M, Ramesh A, Checkoway S, Kanich C, Polakis J. O single sign-off, where art thou? An empirical analysis of single sign-on account hijacking and session management on the Web. In: Proc. of the USENIX Security. 2018. 1475−1492.

[111] Gao A. Chinese Bitcoin exchange OKEx hacked for $3 Mln, police not interested. 2017. https://cointelegraph.com/news/chinese-bitcoin-exchange-okex-hacked-for-3-mln-police-not-interested

[112] Jin C, Wang XY, Tan HY. Dynamic attack tree and its applications on Trojan horse detection. In: Proc. of the Int’l Conf. on Multimedia and Information Technology. 2010. 56−59.

[113] Cimpanu C. Banking Trojan now targets coinbase users, not just banking portals. 2017. https://www.bleepingcomputer.com/news/security/banking-trojan-now-targets-coinbase-users-not-just-banking-portals/

[114] Karapanos N, Capkun S. On the effective prevention of TLS man-in-the-middle attacks in Web applications. In: Proc. of the USENIX Security. 2014. 671−686.

[115] MacKenzie P, Reiter MK. Networked cryptographic devices resilient to capture. In: Proc. of the IEEE S&P. 2001. 12−25.

[116] Schroeder S. Wallet bug freezes more than $150 million worth of Ethereum. 2017. https://mashable.com/2017/11/08/ethereum-parity-bug/

[117] Kelso CE. $45,000,000 worth of BCH & BTC claimed stolen in SIM attack: Doubts linger about veracity. 2020. https://coinspice.io/news/45000000-worth-of-bch-btc-claimed-stolen-in-sim-attack-doubts-linger-about-veracity/

[118] Bamert T, Decker C, Wattenhofer R, Welten S. Bluewallet: The secure bitcoin wallet. In: Proc. of the Int’l Workshop on Security and Trust Management. 2014. 65−80.

[119] Sullivan B. Hackers steal 4,100 Bitcoins from Inputs.io. 2013. https://www.cbronline.com/news/hackers-steal-4100-bitcoins-from-inputsio/

[120] Saad M, Spaulding J, Njilla L, Kamhoua C, Shetty S, Nyang D, Mohaisen A. Exploring the attack surface of blockchain: A systematic overview. arXiv Preprint arXiv:1904.03487, 2019.

附中文参考文献:

[5] 斯雪明,徐蜜雪,苑超.区块链安全研究综述.密码学报,2018,5(5):8−19.

[6] 派盾.2019 年度数字资产反洗钱(AML)研究报告.2020.

[11] 袁超.区块链中硬分叉期间的防御方案.现代计算机,2019(9):3−7,13.

[13] 马昂,潘晓,吴雷,郭景峰,黄倩文.区块链技术基础及应用研究综述.信息安全研究,2017,3(11):968−980.

[14] 刘懿中,刘建伟,张宗洋,徐同阁,喻辉.区块链共识机制研究综述.密码学报,2019,6(4):395−432.

[15] 黄俊飞,刘杰.区块链技术研究综述.北京邮电大学学报,2018,41(2):1−8.

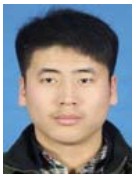
[16] 贺海武,延安,陈泽华.基于区块链的智能合约技术与应用综述.计算机研究与发展,2018,55(11):2452−2466.

[31] 360 核心安全.黑客伪造算力盗取多种数字货币. https://blogs.360.cn/post/黑客伪造算力盗取多种数字货币.html

[61] 孙国梓,王纪涛,谷宇.区块链技术安全威胁分析.南京邮电大学学报(自然科学版),2019,39(5):48−62.

[93] 房卫东,张武雄,潘涛,陈伟,杨旸.区块链的网络安全:威胁与对策.信息安全学报,2018,3(2):87−104.

[96] 徐焱,李文轩,王东亚.Web 安全攻防:渗透测试实战指南.北京:电子工业出版社,2018.



田国华(1993－),男,博士生,主要研究领域为区块链,云计算,信息安全.

胡云瀚(1997－),男,硕士生,主要研究领域为区块链,信息安全.

陈晓峰(1976－),男,博士,教授,博士生导师,CCF 专业会员,主要研究领域为公钥密码学,云计算安全,数据安全,区块链.