第33卷 第1期 Vol.33 No.1 January 2022

ISSN 1000-9825
CODEN RUXUEW

软件学报 Journal of Software

软件学报 Journal of Software

2022 年第 33 卷第 1 期

ISSN 1000-9825

科学出版社

主办

中国科学院软件研究所

中国计算机学会

出版

科学出版社

《软件学报》编委会

(2019 年 1 月~2022 年 12 月)

2013 年全国百强科技期刊　2015 年全国百强科技期刊　中国精品科技期刊　中国计算机学会会刊

软 件 学 报
(Ruanjian Xuebao)

第 33 卷第 1 期
2022 年 1 月

目 次

系统软件与软件工程

开源许可证的选择: 挑战和影响因素 …… 吴　欣　武健宇　周明辉　王志强　杨丽蕴 (1)
自承认技术债的研究: 问题、进展与挑战 …… 郭肇强　刘释然　谭婷婷　李言辉　陈　林　周毓明　徐宝文 (26)
基于神经网络的自动源代码摘要技术综述 …… 宋晓涛　孙海龙 (55)
面向对象程序的上下文敏感指针分析研究 …… 李昊峰　孟海宁　郑恒杰　曹立庆　李　炼 (78)

模式识别与人工智能

自然语言处理中的文本表示研究 …… 赵京胜　宋梦雪　高　祥　朱巧明 (102)
神经结构搜索的研究进展综述 …… 李航宇　王楠楠　朱明瑞　杨　曦　高新波 (129)
大规模图神经网络系统综述 …… 赵　港　王千阁　姚　烽　张岩峰　于　戈 (150)
图分类研究综述 …… 王兆慧　沈华伟　曹　婧　程学旗 (171)
小样本困境下的深度学习图像识别综述 …… 葛轶洲　刘　恒　王　言　徐百乐　周　青　申富饶 (193)

计算机网络与信息安全

域名系统测量研究综述 …… 刘文峰　张　宇　张宏莉　方滨兴 (211)
链下通道路由算法综述 …… 贾林鹏　裴　奇　王　鑫　张瀚文　于　雷　张　珺　孙　毅 (233)
基于网络轨迹的协议逆向技术研究进展 … 王占丰　程　光　马玮骏　张嘉玮　孙中豪　胡　超 (254)
网络行为仿真综述 …… 符永铨　赵　辉　王晓锋　刘红日　安　伦 (274)
基于 RFID 的无源感知机制研究综述 …… 王楚豫　谢　磊　赵彦超　张大庆　叶保留　陆桑璐 (297)

计算机图形学与计算机辅助设计

区块链公链应用的典型安全问题综述 …… 魏松杰　吕伟龙　李莎莎 (324)
基于机器学习的三维场景高度真实感绘制方法综述 …… 赵烨梓　王　璐　徐延宁　曾　峥　葛亮昇　朱君秋　徐子林　赵　钰　孟祥旭 (356)

《软件学报》投稿指南 …… (封三)

期刊基本参数: CN11-2560/TP*1990*m*16*378*zh+en*P*¥70*2022*16*2022-01

Journal of Software Vol.33, No.1 Jan. 2022

Contents

SYSTEM SOFTWARE AND SOFTWARE ENGINEERING

1 Selection of Open Source License: Challenges and Influencing Factors
WU Xin, *WU Jian-Yu*, *ZHOU Ming-Hui*, *WANG Zhi-Qiang*, *YANG Li-Yun*

26 Self-admitted Technical Debt Research: Problem, Progress, and Challenges
GUO Zhao-Qiang, *LIU Shi-Ran*, *TAN Ting-Ting*, *LI Yan-Hui*, *CHEN Lin*, *ZHOU Yu-Ming*, *XU Bao-Wen*

55 Survey on Neural Network-based Automatic Source Code Summarization Technologies
SONG Xiao-Tao, *SUN Hai-Long*

78 Context-sensitive Pointer Analysis for Object-oriented Programs: A Systematic Literature Review
LI Hao-Feng, *MENG Hai-Ning*, *ZHENG Heng-Jie*, *CAO Li-Qing*, *LI Lian*

PATTERN RECOGNITION AND ARTIFICIAL INTELLIGENCE

102 Research on Text Representation in Natural Language Processing
ZHAO Jing-Sheng, *SONG Meng-Xue*, *GAO Xiang*, *ZHU Qiao-Ming*

129 Recent Advances in Neural Architecture Search: A Survey
LI Hang-Yu, *WANG Nan-Nan*, *ZHU Ming-Rui*, *YANG Xi*, *GAO Xin-Bo*

150 Survey on Large-scale Graph Neural Network Systems
ZHAO Gang, *WANG Qian-Ge*, *YAO Feng*, *ZHANG Yan-Feng*, *YU Ge*

171 Survey on Graph Classification
WANG Zhao-Hui, *SHEN Hua-Wei*, *CAO Qi*, *CHENG Xue-Qi*

193 Survey on Deep Learning Image Recognition in Dilemma of Small Samples
GE Yi-Zhou, *LIU Heng*, *WANG Yan*, *XU Bai-Le*, *ZHOU Qing*, *SHEN Fu-Rao*

COMPUTER NETWORKS AND INFORMATION SECURITY

211 Survey on Domain Name System Measurement Research
LIU Wen-Feng, *ZHANG Yu*, *ZHANG Hong-Li*, *FANG Bin-Xing*

233 Survey on Offchain Channel Routing Algorithm
JIA Lin-Peng, *PEI Qi*, *WANG Xin*, *ZHANG Han-Wen*, *YU Lei*, *ZHANG Jun*, *SUN Yi*

254 Research Progress of Network Protocol Reverse Engineering Technologies Based on Network Trace
WANG Zhan-Feng, *CHENG Guang*, *MA Wei-Jun*, *ZHANG Jia-Wei*, *SUN Zhong-Hao*, *HU Chao*

274 State-of-the-art Survey on Network Behavior Emulation
FU Yong-Quan, *ZHAO Hui*, *WANG Xiao-Feng*, *LIU Hong-Ri*, *AN Lun*

297 Survey on RFID-based Battery-less Sensing
WANG Chu-Yu, *XIE Lei*, *ZHAO Yan-Chao*, *ZHANG Da-Qing*, *YE Bao-Liu*, *LU Sang-Lu*

COMPUTER GRAPHICS AND COMPUTER AIDED DESIGN

324 Overview on Typical Security Problems in Public Blockchain Applications
WEI Song-Jie, *LÜ Wei-Long*, *LI Sha-Sha*

356 State-of-the-art Survey on Photorealistic Rendering of 3D Sences Based on Machine Learning
ZHAO Ye-Zi, *WANG Lu*, *XU Yan-Ning*, *ZENG Zheng*, *GE Liang-Sheng*, *ZHU Jun-Qiu*, *XU Zi-Lin*, *ZHAO Yu*, *MENG Xiang-Xu*

软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2022,33(1):324−355 [doi: 10.13328/j.cnki.jos.006280]

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

区块链公链应用的典型安全问题综述*

魏松杰, 吕伟龙, 李莎莎

(南京理工大学 计算机科学与工程学院, 江苏 南京 210094)

通信作者: 吕伟龙, E-mail: 118106043462@njust.edu.cn

摘　要: 区块链作为互联网金融的颠覆性创新技术, 吸引学术研究和工程应用领域广泛关注, 并被持续推广应用到各种行业领域中. 以公有链为代表的区块链系统具有弱中心化、信任共识、平台开放、系统自治、用户匿名、数据完整等特点, 在缺乏集中可信的分布式场景中实现可信数据管理和价值交易. 但区块链作为新兴信息技术, 由于自身机制和周边设施不够完善、用户安全观念不够成熟等原因, 也面临安全威胁和挑战. 本文首先介绍了区块链技术, 回顾其面临的安全风险; 其次以比特币和以太坊两个典型系统为例, 剖析了针对面向代币交易和应用的区块链系统的各类安全威胁以及应对方法; 接着分析了钱包交易所等区块链周边设施和区块链用户的安全隐患; 最后对文中安全问题进行了分类总结, 提出可行技术线路和防御方法, 展望当前区块链安全的研究热点和发展趋势.

关键词: 区块链; 公链安全; 攻击流程; 防御策略; 共识安全

中图法分类号: TP309

中文引用格式: 魏松杰, 吕伟龙, 李莎莎. 区块链公链应用的典型安全问题综述. 软件学报, 2022, 33(1): 324–355. http://www.jos.org.cn/1000-9825/6280.htm

英文引用格式: Wei SJ, Lü WL, Li SS. Overview on Typical Security Problems in Public Blockchain Applications. Ruan Jian Xue Bao/Journal of Software, 2022, 33(1): 324–355 (in Chinese). http://www.jos.org.cn/1000-9825/6280.htm

Overview on Typical Security Problems in Public Blockchain Applications

WEI Song-Jie, LÜ Wei-Long, LI Sha-Sha

School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract: Originated as Internet financial technology, blockchain is prevailing in many application scenarios and attracting attentions from both academia and industry. Typical blockchain systems are characterized with decentralization, trustworthiness, openness, autonomy, anonymity, and immutability, which brings trustworthiness for data management and value exchange in distributed computation environment without centralized trust authority. However, blockchain is still developing as a continuously evolving new technique. Its mechanisms, peripheral facilities, and user maturity in security are yet to be optimized, resulting in various security threats and frequent security incidents. This paper first overviews the blockchain technology and its potential security vulnerabilities when being used for token transaction and exchange. Then the mostly-seen security problems are enumerated and analyzed with Bitcoin and Ethereum as two sample systems. The security problems encountered by blockchain peripheral facilities and users are presented, and their root causes are probed. Finally, the surveyed problems are categorized and the possible countermeasures or defenses are proposed to address them. Promising research areas and technology evolving directions are briefly covered for the future.

Key words: blockchain; public chain security; attack procedure; defense strategy; consensus security

1 绪　论

1.1 区块链介绍

自中本聪在《比特币: 点对点的电子现金系统》一文中首次提出区块链架构至今, 历经 10 年光阴. 10 年间,

* 基金项目: 国家自然科学基金 (61802186, 61472189); 国家重点研发计划 (2020YFB1804604)
收稿时间: 2020-03-05; 修改时间: 2020-05-07, 2020-11-07; 采用时间: 2020-12-04; jos 在线出版时间: 2021-01-15

区块链技术飞速发展, 广泛应用于各个领域. 从比特币、莱特币等加密货币的区块链 1.0 时代, 到以太坊、超级账本等支持智能合约的平台的区块链 2.0 时代, 再到目前面向去中心化应用 DApp 服务的百花齐放, 区块链经历了数次技术迭代[1,2]. 近些年来, 区块链与金融、农业、能源、公益、医疗等领域深度结合, 市场上出现大量与区块链相关的应用, 众多学者也投身于区块链的研究之中. 区块链技术无疑成为当前最热门的技术之一. 但目前区块链技术和应用方兴未艾, 多数处于试验阶段, 安全漏洞和攻击事件层出不穷, 给用户与区块链服务提供商带来了不小的经济损失, 因此区块链的安全问题受到了各方的广泛关注. 同时, 区块链智能合约一旦在分布式、去中心化网络中部署, 就难以修改, 这种特性一方面防止了数据操纵, 有利于建立起基于广泛分布共识的信任机制; 但另一方面, 当面对安全攻击时, 该特性也阻碍了区块链系统建立起有效的纠正机制, 难以有效及时的挽回损失[3,4].

本文在调研过程中, 发现大多数区块链的安全问题是由于系统自身设计缺陷或是规则漏洞而引起的, 少数区块链安全攻击的对象主要包括交易所、数字钱包、矿池矿场以及区块链用户, 而交易所、数字钱包和矿池矿场可归类为区块链周边设施. 因此本文将所有公有区块链安全问题分为 3 类, 即区块链自身系统、区块链周边设施和区块链用户, 依次在第 2、3、4 节综述并分析它们各自面临的安全问题. 本文重点讨论区块链作为分布式系统应用时面临的安全威胁, 并不涉及对底层通信、P2P 对等网络、加密算法、数据存储等传统系统和网络安全问题的讨论. 全文讨论的安全问题总览如图 1 所示.

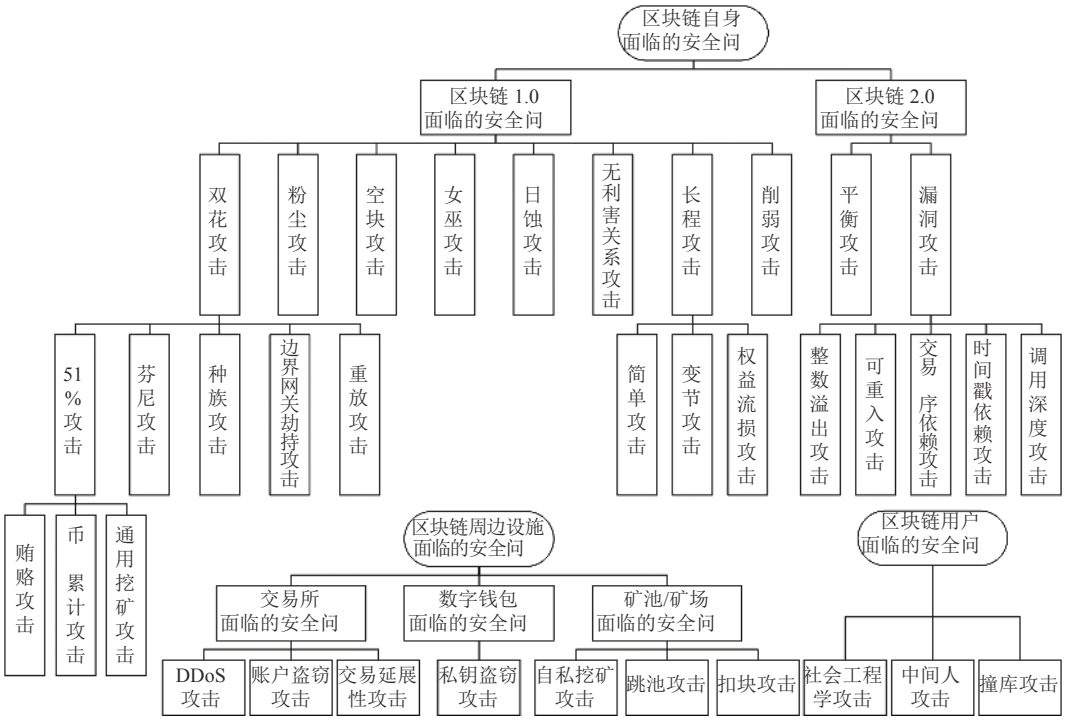

图 1　区块链安全问题总览

1.2　区块链典型安全事件回顾

(1) 2017 年 7 月 Parity 多重签名钱包被盗事件

Parity 是目前使用最广泛的以太坊钱包之一. 本次事件主要是由于智能合约代码编写不严谨导致的, 约有时价 3 000 万美元的 15 万以太币 (ETH) 被盗. 攻击造成了 ETH 从 235 美元暴跌至 196 美元左右. 事后人们逐渐认识到智能合约的编写必须遵守严格的安全规范或模式, 智能合约部署前最好先由专业的机构进行安全审计[5].

(2) 2018 年 11 月 EOS.win 游戏合约遭受随机数攻击事件

EOS 是一种为商用分布式应用 (DApp) 设计的区块链操作系统, EOS.win 是在该平台下实现的竞猜游戏. 在

EOS.win 的智能合约中, 随机数的生成与开奖序号有关, 且智能合约内联调用失败会导致状态信息回滚. 攻击者先是在同一时间控制多个合约账户同时实施小额投注, 以试探随机数生成规律. 在掌握一定规律后, 攻击者再进行多笔大额投注, 以更高的概率赢得奖金并快速套现, 2018 年 11 月 12 日短短一分钟内攻击者获利超过 9 000 个 EOS 币, 导致 EOS.win 参与用户的大量流失. 该事件给 DApp 开发者以警醒——在没有做好充分的安全保障前, 不要轻易上线 DApp, 保护好诚实用户的资金才能更好的留住用户[6].

(3) 2019 年 1 月 ETC 遭受 51% 攻击事件

在全球最大的智能合约漏洞事件 The DAO[7]发生后, 以太坊分裂成 ETC 和 ETH 两大阵营. 2019 年 1 月 7 日, 多家机构和交易所接连预警和确认, 加密数字货币 ETC 遭遇 51% 攻击, 造成 54 200 个 ETC、约 27 万美元的损失. 此次攻击产生的根本原因是 ETC 市值缩水, 网络算力降低, 攻击者通过短期租用算力的方式获得共识主导能力. 这次事件给所有基于工作量证明共识机制的区块链敲响了警钟——虽然在一般的攻击场景中, 51% 攻击的成本高、收益率低, 但对于小规模区块链系统来说, 攻击者可以通过租借、挪用算力的方式, 短瞬间获得大量算力, 从而进行 51% 攻击.

2 区块链自身安全问题

2.1 区块链 1.0 的安全问题——以比特币为例

本文中区块链 1.0 的安全问题, 主要是指以比特币为代表的数字加密货币区块链系统的安全风险和漏洞, 这类区块链通常只能进行与转账、汇款和数字化支付相关的操作, 缺少智能合约的部署运行能力. 有些区块链攻击虽然从时间上来说, 是在区块链 2.0 时期被提出的, 但由于其主要是在数字加密货币区块链中实施的, 因此也被分类在区块链 1.0 的安全问题中.

需要指出的是, 本文虽然结合区块链技术的发展过程, 将攻击分为 1.0 时代、2.0 时代等, 但以以太坊等为代表的区块链 2.0 技术完全基于最初区块链的“分布式系统+P2P 网络+密码学”基础架构发展而成, 只是在共识机制、节点管理、智能合约、算法选择等方面进行了扩展和创新. 因此本节所讨论的安全问题, 实际上也适用于 2.0 时代中采用同样设计或者具有同样漏洞的区块链系统.

本节将以比特币为例, 逐一例举这类攻击的攻击形式, 分析其攻击原理, 总结可能的防范方法.

比特币是一种采用区块链架构的加密数字货币, 比特币使用 P2P 网络众多节点组成的分布式账本进行确认与记账操作, 并用密码学技术进行加密, 以确保货币流通各个环节的安全性[8]. 比特币架构中, 每一个区块包含区块头和区块体两部分. 区块头包含数据和父区块地址, 区块体主要包含交易详情和交易计数. 比特币引入了工作量证明 (PoW) 工作机制、UTXO 和 Merkletree 等数据结构、SHA-256 椭圆曲线加密算法, 以确保攻击者需要面临极高难度才能对比特币区块链进行破解[9].

比特币的区块结构如图 2 所示.

比特币作为区块链的第一个应用, 其将 P2P 动态组网、基于密码学的分布式账本、共识机制等成熟技术进行组合, 保证了比特币系统的可用性、机密性和完整性. 但比特币并非完美, 有些设定反而给系统带来了安全隐患[10,11]. 下面依次介绍典型攻击及其防范方法.

2.1.1 双花攻击 (double spending attack)

双花攻击, 顾名思义就是将同一笔数字货币花费多次的攻击[12−14]. 双花攻击包含以下 4 个步骤.

① 攻击者的地址 1 发起一笔向受害者转账数字货币的交易 A;

② 受害者在交易 A 收到足够多的确认后, 认可交易 A, 并向攻击者转账现金或是发送商品;

③ 攻击者的地址 1 发起一笔向其地址 2 转账数字货币的交易 B, 该交易的交易金额为攻击者地址 1 中的数字货币总数, 由于交易 A 与交易 B 冲突, 因此区块链产生分叉;

④ 攻击者运用各种手段, 使包含交易 B 的链的长度超过包含交易 A 的链, 根据最长链原则, 交易 B 被认为有效, 而交易 A 被认为无效, 攻击者攻击成功[15].

双花攻击的实现流程如图 3 所示.

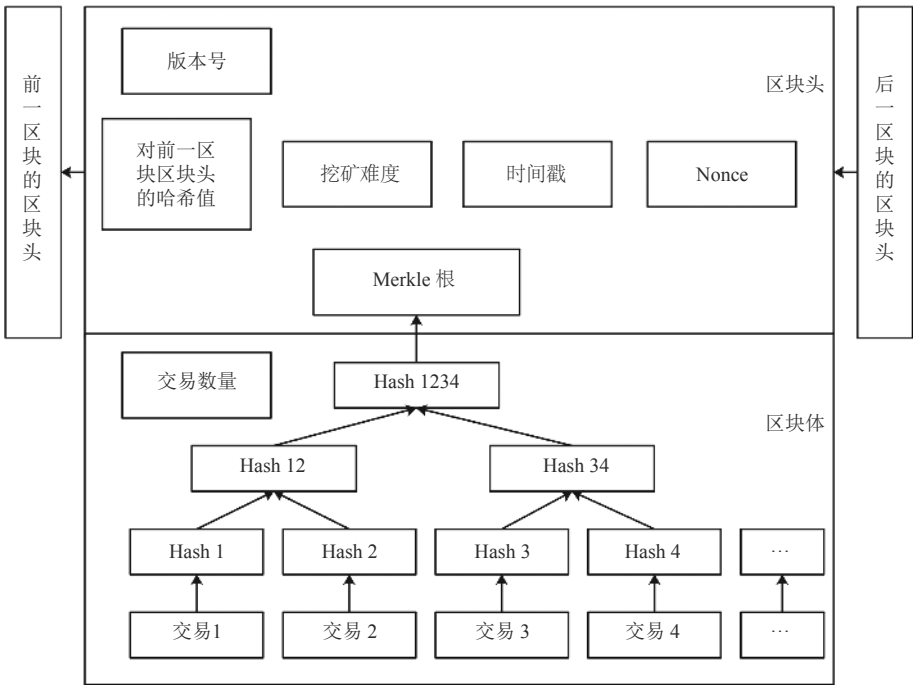

图 2　比特币区块结构

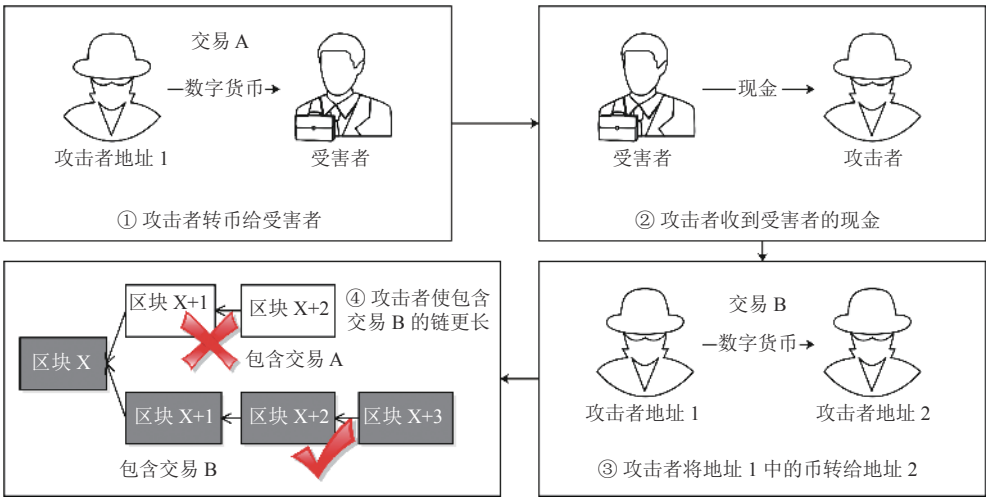

图 3　双花攻击实现流程

双花攻击具体有以下 5 种攻击实施方式.

(1) 51% 攻击 (51% Attack)

51% 攻击是一种在掌握绝对算力优势的情况下, 把已经花出的数字货币重新收回或多次利用的攻击方式, 主要针对基于工作量证明 (PoW) 共识机制的区块链[16−18].

51% 攻击一般分为 4 步.

① 攻击者发起一笔交易 A, 将一定量的数字加密货币转账给受害者;

② 受害者在交易 A 收到足够多的确认后, 认可交易 A, 并向攻击者移交等值的财物;

③ 攻击者在拿到财物后, 从交易 A 之前区块开始制造分叉, 利用>51% 的算力优势在该分叉链上进行挖矿;

④ 当分叉链长度超过原主链时, 根据最长链原则成为新主链, 原主链上的交易 A 无效, 攻击成功[19].

51% 攻击的实现流程如图 4 所示.

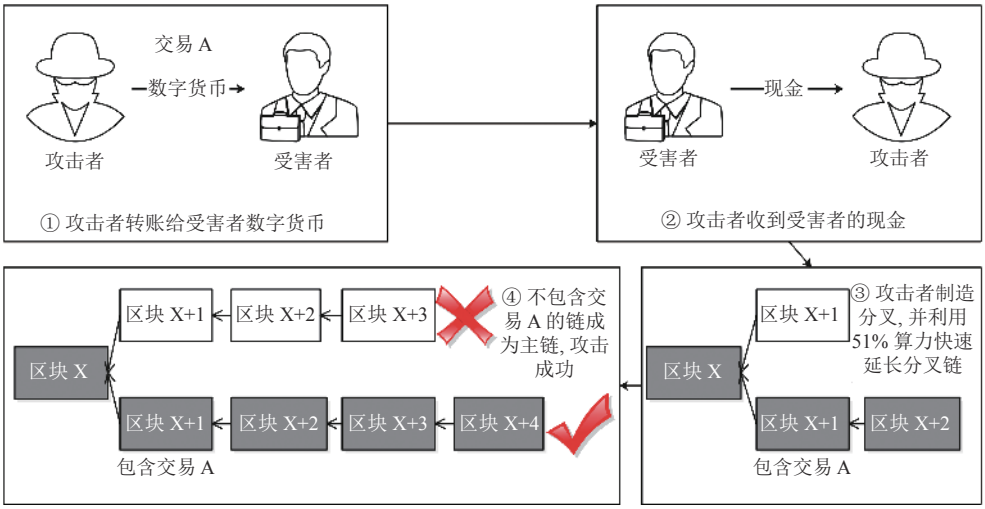

图 4 51% 攻击实现流程

由于 PoW 共识机制的特性, 理论上无法通过技术层面阻止 51% 攻击的产生. 因此在设计比特币系统时, 中本聪利用经济学原理来减少 51% 攻击出现的可能——获得全网算力优势的代价极度昂贵, 而花费极高成本实施的双花攻击会造成信任崩溃, 使得数字货币严重贬值, 这对于攻击者而言得不偿失[9]. 相反, 在拥有 51% 算力的情况下, 进行诚实挖矿所获得的收益要更多[20].

防范方法: 保持算力分散. 51% 攻击能够成功实施的根本原因是算力过分集中, 在 PoW 共识机制下只要存在算力中心化, 所有区块链都无法完全避免 51% 攻击.

虽然实施 51% 攻击的成本极高, 攻击者缺乏经济层面的动机, 但实际生活中 51% 攻击还是有可能发生的. 在小型山寨币中, 获得全网算力优势的代价相对较小, 攻击者可以在实施 51% 攻击后, 退出系统快速变现, 从而牟取暴利.

为了降低攻击难度或者节省成本, 攻击者有以下 3 种低成本的 51% 攻击方法.

1) 贿赂攻击 (bribe attack)

贿赂攻击是一种在非协作选择模型上 (比如无信任基础区块链) 的攻击, 攻击者通过额外经济奖励收购挖矿算力, 使得自己所掌握的算力短期内超过 51%, 从而对区块链进行 51% 攻击[21−23].

贿赂攻击一般分为 5 步.

① 攻击者发起一笔交易 A, 将一定量的数字加密货币转账给受害者;

② 受害者在交易 A 收到足够多的确认后, 认可交易 A, 并向攻击者移交等值的财物;

③ 攻击者在网络中宣称将提供额外奖励给在目前相对较长但不包含交易 A 的次主链上工作的矿工, 以鼓动其他矿工违背共识, 在非主链上进行工作;

④ 当次主链足够长时, 攻击者通过加大奖励力度, 促使次主链的长度在短时间内超过原主链的长度;

⑤ 当次主链成功超越原主链长度后, 次主链成为最长链, 根据共识, 其他矿工承认次主链为新主链, 原主链中的交易 A 因为回滚而无效[24].

贿赂攻击的实现流程如图 5 所示.

防范方法: 可以在区块链挖矿机制设计中引入保证金和惩罚措施. 当矿工做出不利于区块链的决策时, 会受到处罚并失去抵押在链上的保证金. 这种惩罚措施变相提高了攻击者的贿赂成本, 使得贿赂攻击更难发生.

《软件学报》2022 年出版专刊/专题

发表期数	专刊/专题名称	特约编辑
2022 年第 3 期	数据库系统新型技术	李国良,于戈,杨俊,范举
2022 年第 4 期	面向开放场景的鲁棒机器学习研究	陈恩红,李宇峰,邹权
2022 年第 5 期	领域软件工程	汤恩义,江贺,陈俊洁,李必信,唐滨
2022 年第 6 期	系统软件安全	杨珉,张超,宋富,张源
2022 年第 6 期	定理证明理论与应用	曹钦翔,詹博华,赵永望
2022 年第 7 期	智能系统的分析和验证	明仲,张立军,秦胜潮
2022 年第 8 期	形式化方法与应用	陈立前,孙猛
2022 年第 9 期	融合媒体环境下的媒体内容分析与信息服务技术	汪萌,张勇东,俞俊,张伟
2022 年第 10 期	智慧信息系统新技术	邢春晓,王鑫,张勇,于戈

登录软件学报网站: http://www.jos.org.cn 免费下载专刊/专题全文.

软 件 学 报
Ruanjian Xuebao
(月刊, 1990 年创刊)
第 33 卷 第 1 期 2022 年 1 月

Journal of Software
(monthly)
(Started in 1990)
Vol.33 No.1 Jan. 2022

主管单位	中国科学院
主办单位	中国科学院软件研究所 中国计算机学会
主 编	赵 琛
编 辑	《软件学报》编辑部 (北京 8718 信箱 邮编 100190) 电话: 010-62562563, E-mail: jos@iscas.ac.cn http://www.jos.org.cn
编辑部主任	方 梅
出 版	科 学 出 版 社 (北京东黄城根北街 16 号 邮编 100717)
印 刷	北京宝昌彩色印刷有限公司
总发行处	中国邮政集团公司北京市报刊发行局
订 购 处	全国各地邮局
国外总发行	中国国际图书贸易总公司 (北京 399 信箱 邮编 100044)

Sponsored by the Chinese Academy of Sciences
Published by Institute of Software, The Chinese Academy of Sciences (ISCAS) and China Computer Federation
Editor-in-Chief: ZHAO Chen
Edited by Editorial Board of Journal of Software
(P.O.Box 8718, Beijing 100190, P.R.China)
Tel: 8610-62562563, E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Distributed by Science Press (16 Donghuangchenggen North Street, Beijing 100717, China)
Printed by Beijing Baochang Color Printing Co., Ltd
Generally Distributed by Beijing Bureau for Distribution of Newspapers and Journals
Domestically Distributed by All Local Post Offices in China
Overseas Distributed by China International Book Trading Corporation (P.O.Box 399, Beijing 100044, China)

ISSN 1000-9825
CN 11-2560/TP
国内邮发代号: 82-367
国外发行代号: M4628

定价: 70.00 元

公 开 发 行