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.

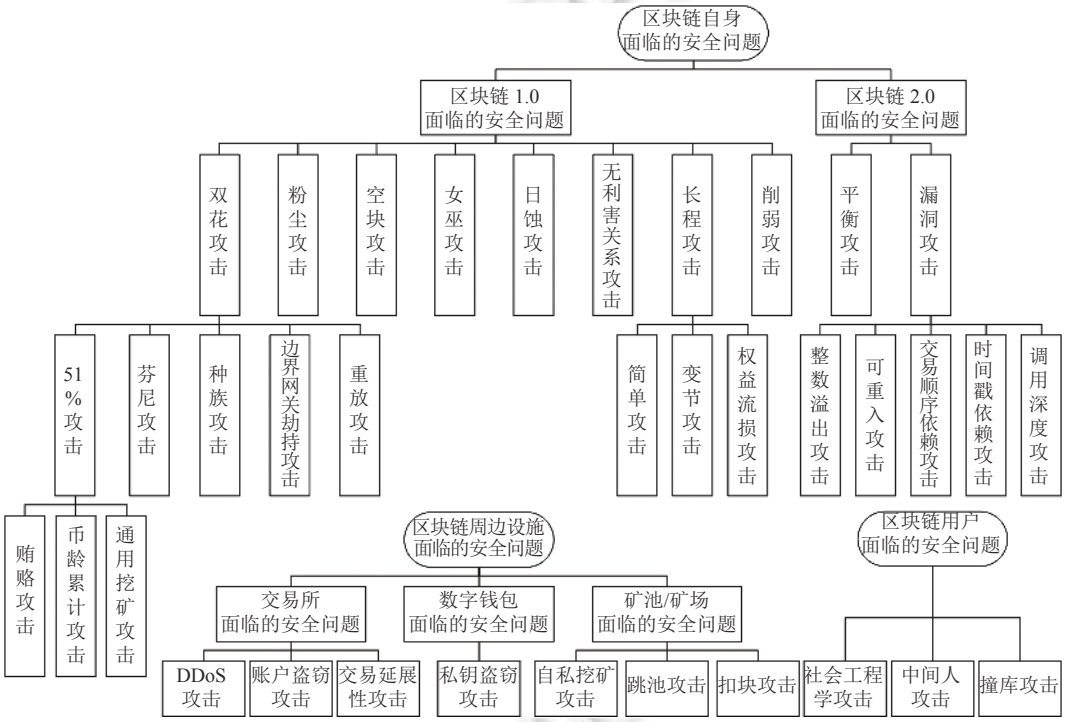

图 1 区块链安全问题总览

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.

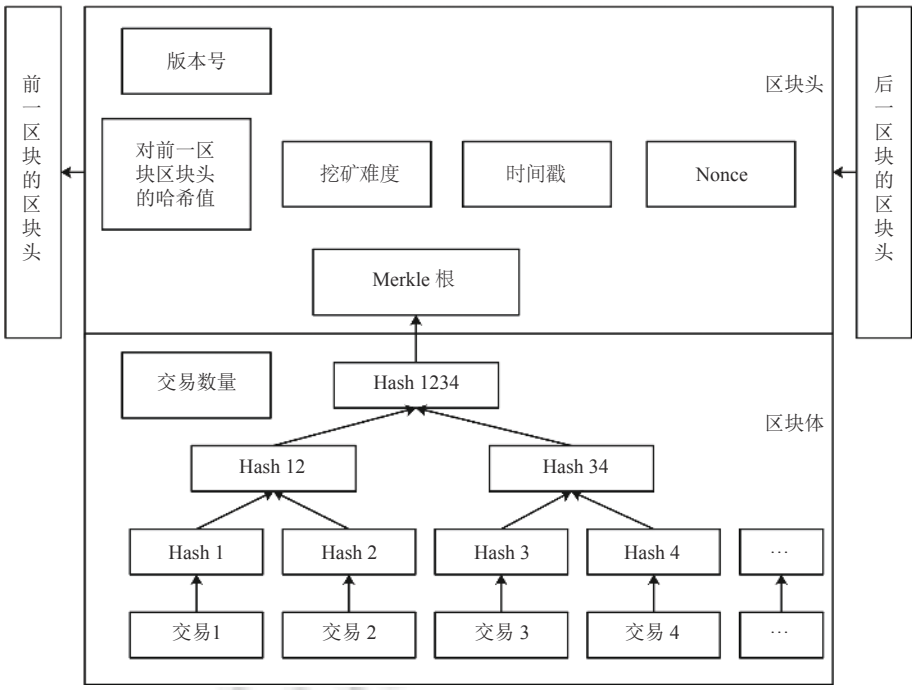

图 2 比特币区块结构

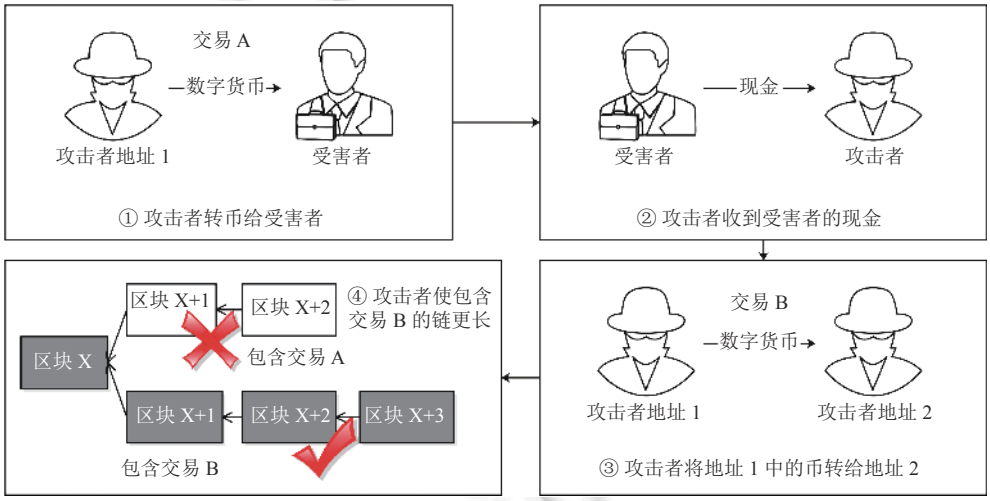

图 3 双花攻击实现流程

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.

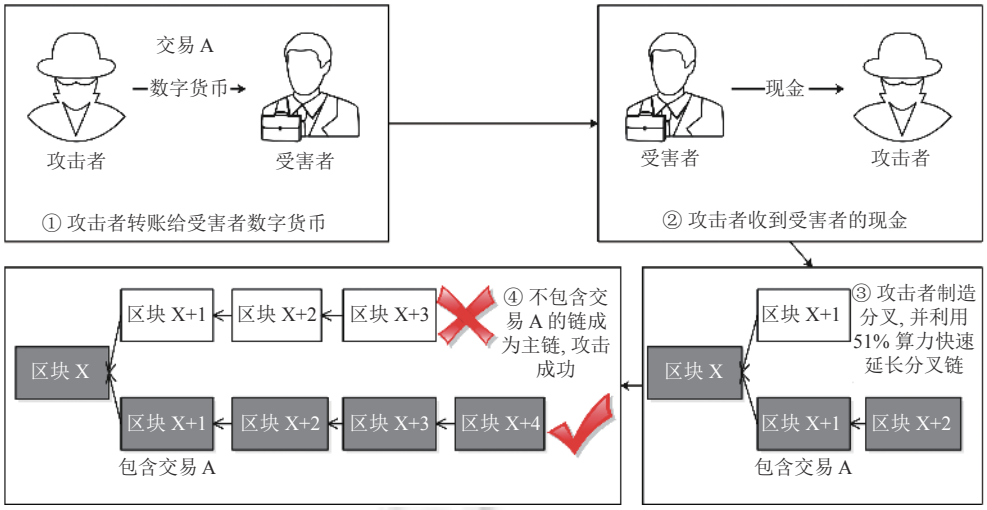

图 4 51% 攻击实现流程

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.

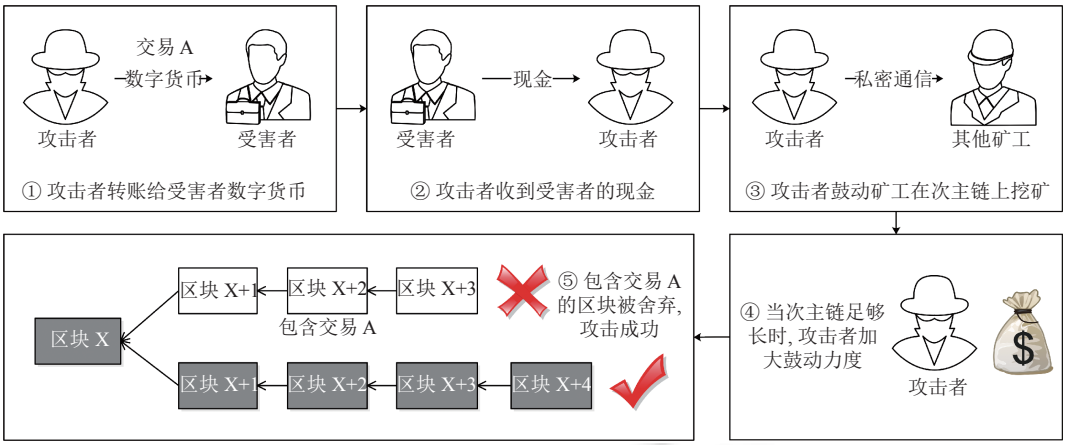

图 5 贿赂攻击实现流程

2) 币龄累计攻击 (coin age accumulation attack)

币龄累计攻击主要实施在基于“PoW+PoS”(工作量证明+权益证明) 混合共识机制的区块链上. 在这种混合共识机制中, 某一地址拥有的数字加密货币越多、持币时间越长, 该地址的挖矿难度就越低, 因此更容易挖到新区块. 根据这种特性, 攻击者在持有一定量的币足够长时间后, 就可以获得接近 51% 算力, 从而发动 51% 攻击[25−27]. 例如, 在点点币 (peercoin) 初始版本中, 其挖矿算法公式为:

$$H\left(H\left(B_{\text{prev}}\right),A,t\right)\leqslant balance(A)\times m\times Age(coins)$$

其中, $H()$ 为某种哈希函数、B_{prev} 为上一个区块的数据、A 为某个账户、t 为时间戳、$balance(A)$ 为账户 A 的余额、m 为某个极小的实数, 其由哈希函数的性质决定、$Age(coins)$ 为币龄.

显然, 攻击者可以利用币龄使得自己更容易发动 51% 攻击[28].

防范方法: 区块链设计者可以对单个地址的持币数量和币龄的最大值进行限制. 当某个地址的币龄已经达到预先设定的最大值时, 系统自动进行清算, 即清空币龄并给予数字货币奖励或是直接停止币龄的增长.

3) 通用挖矿攻击 (general mining attack)

通用挖矿攻击的攻击目标是那些和已有币种的架构和共识相同或相似但还未形成挖矿规模的币种, 尤其是主流币种的山寨分叉币. 由于这些山寨币和某些主流币架构和共识算法相同, 主流币的矿机可以直接用来开采山寨币. 攻击者通过挪用大量主流币矿机, 轻松获得山寨币 51% 算力, 从而进行 51% 攻击, 之后攻击者只需将攻击成果变现, 再返回主流币继续挖矿即可. 由于攻击者只是短期持有山寨币, 因此攻击导致信任崩溃而引起的山寨币贬值对攻击者没有任何影响, 换句话说, 这种通用挖矿攻击对于攻击者而言成本低廉, 极易实施.

防范方法: 区块链设计者在设计新币种时应尽量避免与其他主流区块链的架构和共识算法冲突. 新的币种使用新的共识算法和架构或是在已有算法上进行调整可以有效的减少其他币带来的影响[29].

(2) 芬尼攻击 (finney attack)

芬尼攻击是一种通过控制区块的广播时间来实现双花的攻击, 攻击目标为接受 0 确认的商家[30−32]. 芬尼攻击一般分为 6 步.

① 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 A, 该交易的交易金额为攻击者地址 1 中的数字货币总数;

② 攻击者参与挖矿, 无需 51% 算力, 也最终能在某个时刻挖到包含交易 A 的区块 X;

③ 挖到区块 X 后, 攻击者不立刻进行广播, 先将该区块扣在自己手中;

④ 攻击者发起交易 B, 将地址 1 中的数字货币转账给接受 0 确认的受害者;

⑤ 在交易 B 广播后, 受害者移交等值的财物给攻击者;

⑥ 攻击者拿到财物后立刻广播之前的区块 X, 由于交易 A 先于交易 B, 攻击者转账给受害者的交易 B 会因为

攻击者地址 1 中的币不足而无效, 攻击成功[33].

芬尼攻击的实现流程如图 6 所示.

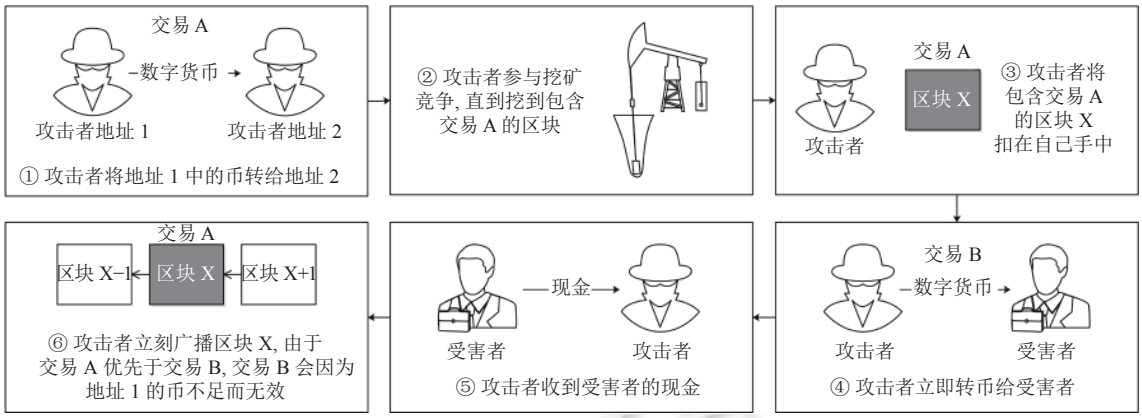

图 6 芬尼攻击实现流程

防范方法: 拒绝 0 确认交付. 在 PoW 共识下, 一般等待 6 个确认就能保证交易在最长链上不会失效.

(3) 种族攻击 (race attack)

种族攻击和芬尼攻击一样, 也是针对接受 0 确认的商家的攻击. 与芬尼攻击不同, 种族攻击主要是通过控制矿工费来实现双花[34,35].

种族攻击一般分为 4 步.

① 攻击者的地址 1 发起一笔转账给接受 0 确认的受害者数字货币的交易 A, 手续费设定为少量;

② 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, 手续费设定为大量;

③ 在交易 A 广播后, 受害者将财物移交给攻击者;

④ 矿工们会优先为手续费高的交易打包, 因此交易 B 先被打包到主链上. 交易 A 则会因为攻击者地址 1 中的币不足而导致失败, 攻击成功[36].

种族攻击的实现流程如图 7 所示.

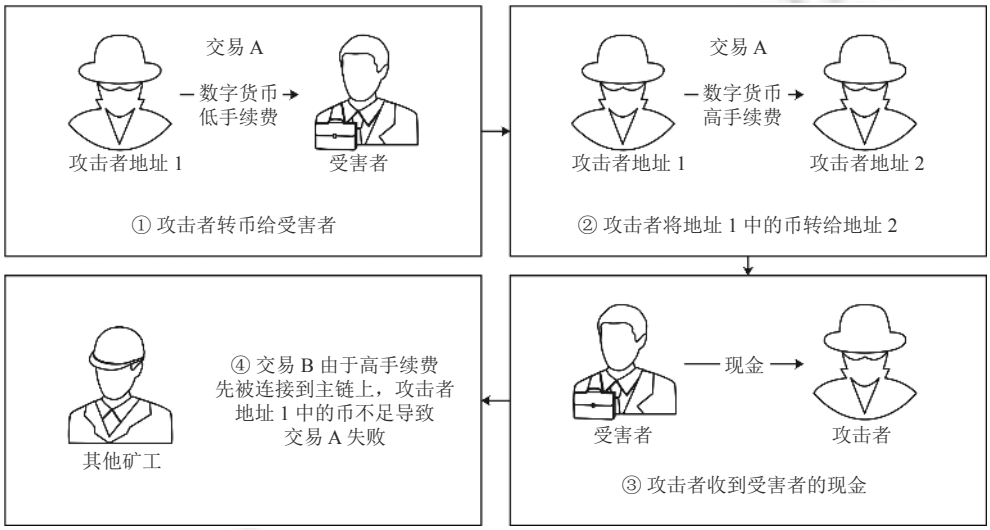

图 7 种族攻击实现流程

防范方法: 区块链商家拒绝 0 确认交付. 在 PoW 共识下, 一般等待 6 个确认就能保证交易在最长链上, 交易几乎不会失效.

(4) 边界网关劫持攻击 (BGP hijacking attack)

边界网关协议 (border gateway protocol) 是一种在 TCP 上运行的自治系统路由协议, 用于生成 IP 数据包转发规则. 攻击者可以利用 BGP 劫持来拦截区块链的网络流量, 阻碍广泛共识的达成[37−40].

边界网关劫持攻击一般分为 4 步:

① 攻击者劫持 BGP, 将区块链网络中的节点划分成多个无法互相通信的分割组, 每个分割组中的节点只能在组内对主链达成共识, 一段时间后区块链产生多条分叉;

② 攻击者分别在各个分叉上花费数字货币, 在各个交易完成后, 攻击者获得多笔现金;

③ 攻击者停止劫持 BGP, 各子组节点之间恢复通信;

④ 全网节点进行共识, 恢复通信后的最长链成为主链, 其他分叉链中的交易被回滚而无效, 攻击成功[41].

边界网关劫持攻击的实现流程如图 8 所示.

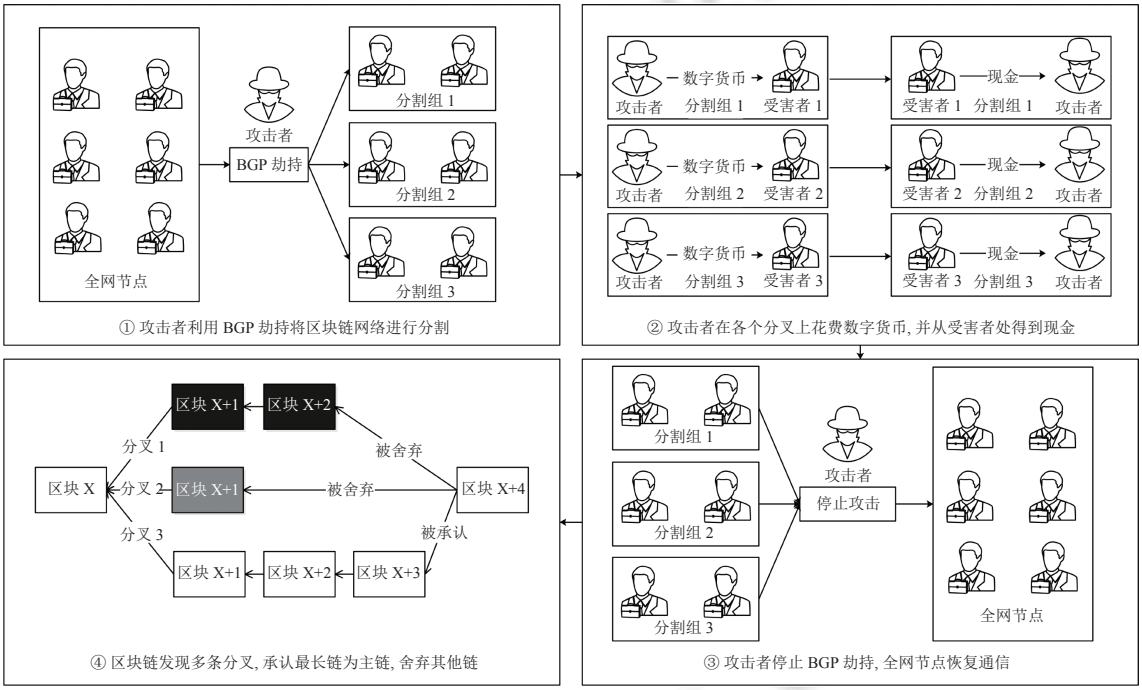

图 8 边界网关劫持攻击实现流程

防范方法: 区块链拥有者可以不使用互联网服务提供商提供的中心化网络, 转而搭建针对区块链专用的去中心化网络, 以减少攻击者仅仅通过劫持少量节点就能对区块链造成巨大影响的可能.

(5) 重放攻击 (replay attack)

软件系统在实际应用中需要升级更新, 区块链也是如此. 但区块链系统内所有节点需要对区块链中的各种协议达成共识, 随着协议的版本更新, 不同节点上运行的协议可能出现差异, 致使其执行的规则不尽相同, 从而导致区块链出现分叉. 分叉主要分为软分叉和硬分叉. 在区块链中, 未升级的节点称为旧节点, 已升级的节点称为新节点. 软分叉是指新节点无法接受旧节点产生的全部或部分区块而产生的临时性分叉, 但由于新节点具有较大的算力, 旧节点产生的区块将没有机会得到认可, 最终新旧节点会对主链问题达成共识. 硬分叉则是指旧节点无法接受新节点产生的全部或部分区块而产生的永久性分叉, 尽管旧节点具备的算力较小, 但新旧节点始终都在维护自己认可的链. 重放攻击往往出现在存在硬分叉的区块链中, 例如 BTC 和 BCC、ETC 和 ETH[42]. 由于硬分叉两条链中

的数据结构、交易格式、地址和私钥算法相同, 所以一条链上的交易数据在另一条链上也有极大可能也是合法的. 攻击者只需抓取一条链上的交易数据, 再复制到另一条链上广播, 即可发动重放攻击[43].

重放攻击一般分为 4 步.

① 假设链 1 和链 2 是某个区块链出现硬分叉后产生的两条链. 攻击者在链 1 中向受害者提出充值数字货币的请求, 并发起一笔向受害者转账的交易 A;

② 一段时间后, 攻击者提出取回该笔数字货币的请求. 受害者同意后, 在链 1 中发起一笔向攻击者转账的交易 B;

③ 攻击者在网络中抓取交易 B 的数据并广播到链 2 上;

④ 由于交易 B 的私钥签名、地址、余额信息等数据在两条链上都合法, 两条链上的矿工都认可这笔交易并将其打包到各自的链上, 最终攻击者在两条链上都获得了受害者的数字货币, 攻击成功[44].

重放攻击的实现流程如图 9 所示.

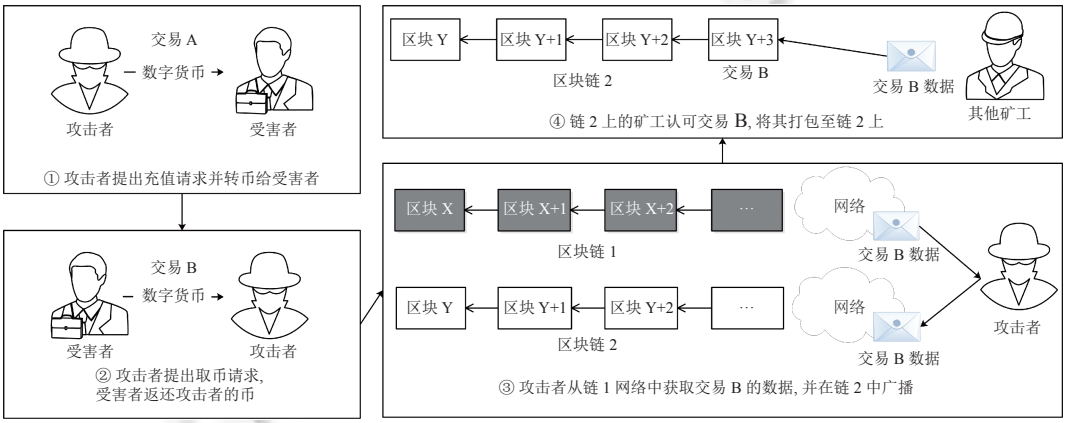

图 9 重放攻击实现流程

防范方法: 区块链设计者可以在区块链产生硬分叉时对分叉链的代码进行适度修改, 使得分叉链和主链之间的交易数据不通用, 从而避免同一笔交易在两条链上都合法.

2.1.2 空块攻击 (empty block attack)

实施空块攻击的攻击者在挖到新区块后, 拒绝将网络中的交易打包到区块. 攻击者挖出的区块中除了挖矿奖励交易外, 没有任何其他交易, 这将导致区块链交易确认时间延长, 区块链活性被降低. 在比特币挖矿的早期, 矿工们还没有加入矿池合作挖矿, 计算随机数和打包交易都需要自己完成, 由于打包空块的速度比打包非空块的速度快, 且出块奖励远大于手续费, 所以矿工们更愿意打包空块来换取出块奖励, 因此导致大量空块产生[45−47].

防范方式: 区块链设计者可以设计共识, 使矿工的收益与块中的交易数目挂钩, 打包的块中的交易越多, 矿工的奖励就越高; 使矿工的挖矿难度与块中的交易数目挂钩, 根据打包的块中的交易数目略微减少矿工的挖矿难度, 使得包含交易多的块更容易被挖出, 从而激励矿工们打包更多的交易.

2.1.3 削弱攻击 (undercutting attack)

PoW 共识中, 矿工的奖励由出块奖励和交易费两部分组成, 且单个区块的出块奖励随时间越来越少. 在 PoW 共识后期, 出块奖励趋近于 0 时, 矿工的奖励仅仅只有交易费部分, 此时, 攻击者为了自己的利益很有可能不在最长链上挖矿, 而是选择制造分叉, 以获得更多的交易费. 这种攻击除了会导致恶意分叉破坏共识, 同时也会因为矿工们出于对利益 (交易费) 和成本 (电费等) 的权衡, 导致交易被恶意堆积, 影响区块链活性[48,49].

削弱攻击原理如图 10 所示.

防范方法: 区块链设计者在设计共识时, 可以永久保留出块奖励, 并将奖励控制在一个合理的范围内. 虽然这样会带来些许通货膨胀, 但可以很大程度上的减少削弱攻击对区块链的影响, 从而带来区块链的稳定.

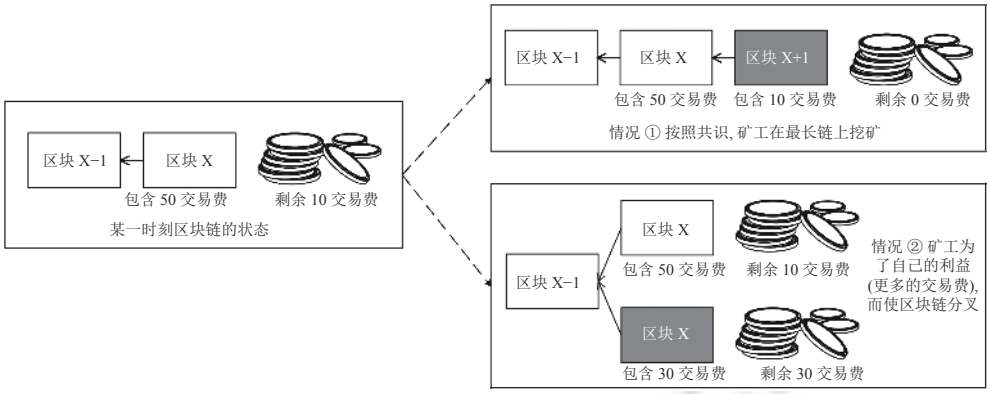

图 10　削弱攻击原理

2.1.4　无利害关系攻击 (nothing at stake attack)

在早期的 PoS (权益证明) 共识机制中, 节点只会因为创建和验证区块得到奖励, 而不会因为任何不当的行为而得到惩罚, 并且在 PoS 共识下, 挖矿不消耗任何资源. 这就导致了当区块链中出现分叉时, 无论这个分叉是偶然出现还是恶意节点故意制造的, 对于其他节点来说, 它们最优的策略是在每一条分叉上都进行挖矿, 这样无论最后哪条链胜出, 它们都会得到奖励. 对于区块链来说, 无利害关系攻击会导致多条分叉并驾齐驱, 链中节点无法对主链达成共识, 极大的影响区块链的可用性[50−53].

无利害关系攻击一般分为 4 步.

① 攻击者故意在主链制造分叉, 或等待主链偶然产生分叉;

② 其他矿工感知到分叉的存在, 按照最优的挖矿策略, 他们会在每一条分叉上进行挖矿;

③ 随着时间的推移, 每条分叉链的长度都有所增加且有很高的概率长度相似, 并且在分叉链长度增长的过程中, 它们有很大的可能产生新分叉;

④ 由于分叉的状态一直持续, 且分叉越来越多, 全网节点无法对主链达成共识, 攻击成功.

无利害关系攻击的实现流程如图 11 所示.

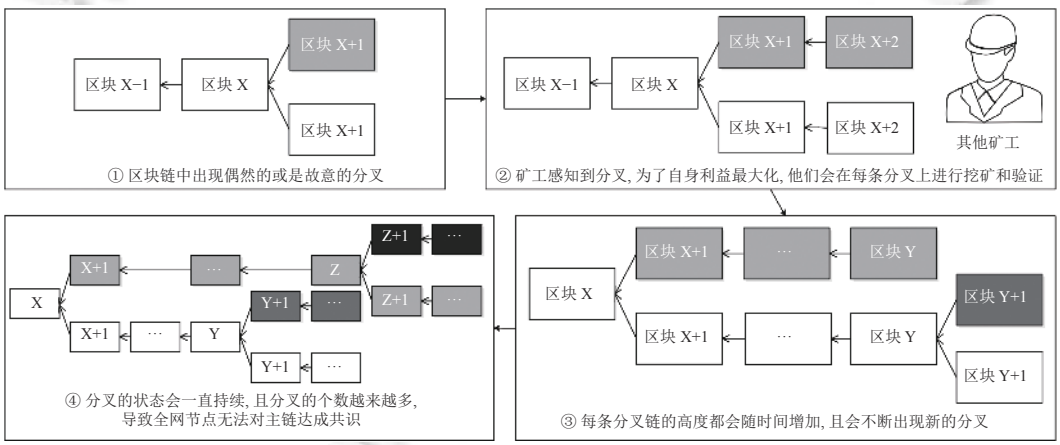

图 11　无利害关系攻击实现流程

防范方法: 区块链设计者将保证金和惩罚措施加入到 PoS 共识中, 防止节点在多条分叉上工作. 节点在创建和验证区块前, 必须缴纳保证金, 当节点在相同高度创建或者验证大于等于两个区块时, 则被认为参与无利害关系攻击, 系统将扣除其保证金[54,55].

2.1.5 长程攻击 (long range attack)

在 PoW 共识中, 如果攻击者要篡改某区块的历史, 需要在这个区块前制造一条分叉链, 并且让其长度超过主链长度. 但由于 PoW 共识的特性, 攻击者制造一条超过主链的分叉链需要大量的算力, 且分叉链长度越长, 分叉链超过主链的难度越高, 这就在导致了在 PoW 共识下, 攻击者只能对短程的区块进行修改; 而在 PoS 共识下, 延长分叉链只需要权益, 即币的数量和币龄, 因此, 攻击者可以较为轻松的篡改成百上千个区块之前的历史区块, 实现长程攻击[56−59]. 长程攻击有 3 种攻击策略.

(1) 简单攻击 (simple attack)

在 PoS 共识的一轮验证周期中, 系统根据每个节点权益的大小, 加权随机挑选验证者. 攻击者若想篡改某一历史区块, 其需要从该区块的父区块位置开始, 制造分叉链并进行秘密验证, 值得注意的是, 由于该分叉链没有公开, 所以除了攻击者验证的块外没有其他验证者验证的块. 为了超越主链长度, 攻击者必须伪造时间戳以便提前生成区块, 一旦分叉链长度超过主链, 攻击者就发布自己的分叉链, 从而达成修改区块历史的目的.

简单攻击的原理如图 12 所示.

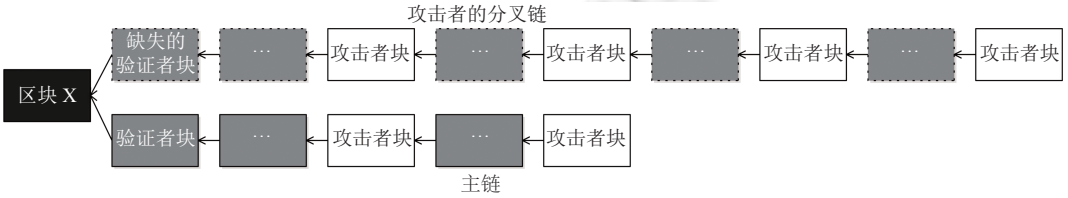

图 12 简单攻击原理

防范方法: 由于此种攻击较为简单, 因此区块链设计者只需在共识中加入时间戳验证机制, 就可以防止攻击者伪造时间戳从而提前生成区块完成攻击; 也可以设置移动检查点 (moving checkpoint), 即仅允许区块链尾端的 X 个区块被重组, 来缩小攻击者可修改历史的区块数目.

(2) 变节攻击 (posterior corruption attack)

显然, 简单攻击的攻击效率不高, 攻击者如果想要在相同时间内生成更多的块, 他就需要更多的权益. 除了让自己地址里的权益增加外, 攻击者还可以利用其他地址里的权利, 例如 B 的地址, 哪怕在攻击者进行攻击时 B 地址内的权益已经清空了, 只要 B 的地址内在攻击者需要的历史时刻下有大量的权益, 攻击者在获得该地址的私钥后, 就可以利用自己和 B 的权益进行变节攻击[60].

变节攻击原理如图 13 所示.

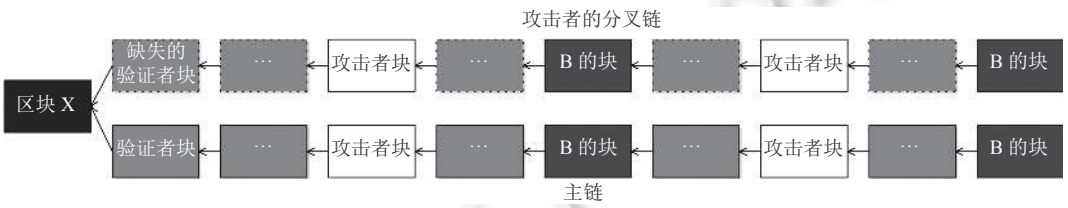

图 13 变节攻击原理

防范方法: 区块链用户可以利用密钥进化技术 (key-evolving cryptography) 和可信执行环境 (trusted execution environments) 来保护自己密钥不被攻击者利用或盗取; 区块链设计者可以设置移动检查点来缩小攻击者可修改历史的区块数目.

(3) 权益流损攻击 (stake bleeding attack)

攻击者若想使自己分叉链的长度更快超越主链, 除了使分叉链更快的出块, 也可以干扰主链的出块速度, 例如当攻击者在主链上被选举为区块验证者时, 其可以放弃该区块的验证以降低主链的出块速度; 同时, 攻击者可以从

主链上复制交易并放在分叉链上广播, 以增加其在分叉链上的权益占比, 从而加快分叉链的出块速度[61−63].

权益流损攻击原理如图 14 所示.

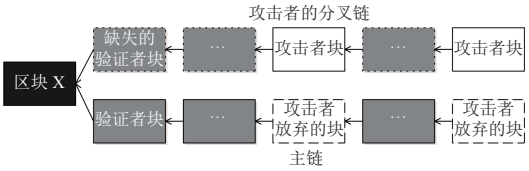

图 14 权益流损攻击原理

防范方法: 区块链设计者可以通过设置移动检查点缩小攻击者可修改历史的区块数目; 也可以利用充裕法则 (plenitude rule) 分析分叉链上自分叉产生时的区块密度变化情况, 实时检测区块链上是否存在权益流损攻击, 以及时做出应对.

2.1.6 粉尘攻击 (dust attack)

粉尘攻击是指用大量交易额极小、毫无价值的垃圾交易占据区块空间, 从而导致正常的交易无法被处理, 造成区块堵塞的攻击. 攻击者通过发起很多交易额极小但手续费较高的交易, 使得矿工优先处理这些交易, 从而达到堵塞区块链的目的; 攻击者也可以利用矿池, 打包无意义的交易, 使得区块链拥堵, 阻碍正常交易被打包[64,65].

防范方式: 区块链设计者指定规则使矿工们达成共识, 不打包交易额极小的交易. 从经济学角度看, 打包更多有意义的交易能够使区块链本身更有价值, 币值也会相应提升, 每个矿工都能从中获利[66].

2.1.7 女巫攻击 (sybil attack)

女巫攻击主要针对的是采用拜占庭容错 (BFT) 协议而非 PoW 机制的区块链. 攻击者通过创建多个身份节点破坏区块链网络的信任基础和冗余策略, 操控区块链选举投票[67−70].

女巫攻击原理如图 15 所示.

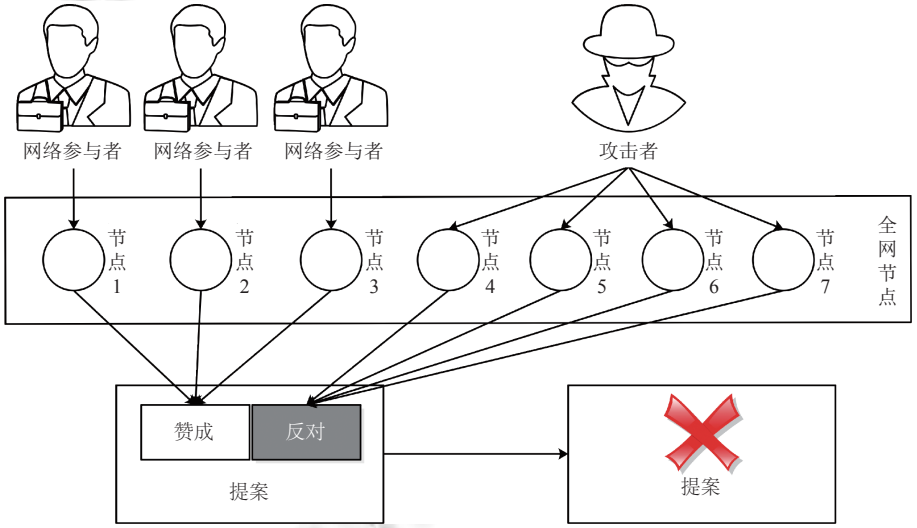

图 15 女巫攻击原理

防范方式: 区块链设计者可以在区块链系统中加入身份认证机制. 只有获得可信的第三方节点或是获得当前网络中大多数可靠节点的认证后, 新的节点才能加入区块链.

2.1.8 日蚀攻击 (eclipse attack)

日蚀攻击是一种由多个傀儡节点发起的针对区块链网络层面的攻击, 攻击者利用傀儡节点修改受害者节点的

节点表并阻止受害者节点接收和发送消息, 从而达到隔离受害者节点的目的. 攻击者通过隔离受害者节点, 征用受害者的挖矿能力进行双花攻击或私自挖矿, 也可以诱使受害者在交易完成前将现金或货物发给攻击者[71−73]. 需要注意的是, 比特币等典型区块链中每个节点拥有两个节点表, NEW TABLE 存储了节点知晓但还未连接过的其他节点 IP; TRIED TABLE 存储了曾经连接过但现在可能没有建立连接的其他节点 IP. 攻击者需要利用傀儡节点 IP 或无效 IP 填满两个节点表, 才能达到隔离节点的目的[74].

日蚀攻击一般分为 3 步.

① 攻击者控制多个傀儡节点向受害者节点进行大量、持续的 TCP 连接, 受害者节点将傀儡节点 IP 存入自己的 TRIED TABLE 中;

② 完成 TCP 连接后, 傀儡节点发送大量无效的 IP 或是其他傀儡节点 IP, 受害者节点将这些 IP 存入自己的 NEW TABLE 中;

③ 攻击者等待受害者节点重启, 重启后, 受害者节点会从两个节点表中选择进行连接的节点, 由于受害者节点的两个表中只有无效节点 IP 和傀儡节点 IP, 因此只能连接上攻击者的傀儡节点. 攻击者完成对受害者节点的隔离, 攻击完成[75−77].

日蚀攻击的实现流程如图 16 所示.

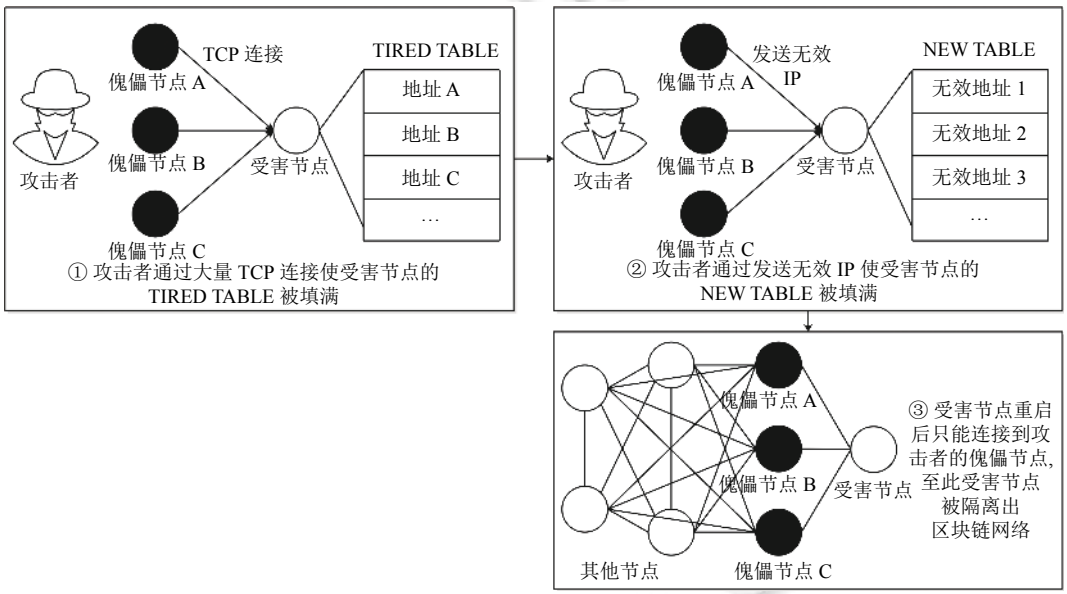

图 16 日蚀攻击实现流程

防范方法: 区块链设计者修改节点连接规则. 利用随机性或是加入噪声的方法使攻击者无法轻松的通过控制受害者节点的节点表发起日蚀攻击; 或是在删除较旧 IP 之前, 先测试该 IP 能否连接上, 只有在连接失败时, 才将此地址从表中删除; 也可以新增两个额外的外部连接, 用于测试新的 IP 是否可以连接, 只有在连接成功时, 才将新地址加入表中, 以此防止攻击者用无效地址填充节点表等.

2.2 区块链 2.0 的安全问题——以以太坊智能合约为例

以太坊作为区块链 2.0 最广为接受的代表, 提供一个可以在区块链上部署、运行智能合约的底层平台, 它采用智能合约—以太虚拟机的架构, 主链代币称为以太币 (ETH).

以太坊智能合约的协商和确认是在区块链存储的应用程序上进行的. 这些合约程序的优点是验证和执行过程去中心化, 但去中心化使得审查非常困难. 智能合约的总体目标是能够满足普通的合约条件, 最小化恶意或意外事件发生的可能性, 并降低成本. 智能合约的运行原理如图 17 所示.

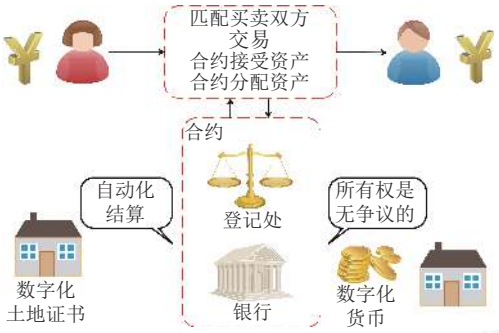

图 17 智能合约运行原理

以太坊虚拟机是以太坊中智能合约的运行环境, 它是以太坊项目中的主要创新点之一. 以太坊虚拟机是图灵完备的 256 位虚拟机, 在给定存储和计算资源的情况下, 以太坊虚拟机能够解决任何可计算的问题[78].

在以太坊上部署智能合约需要花费字节费 Gas. Gas 是以太坊为了防止恶意用户部署无限循环运行的合约, 而要求用户为所部署合约的每一步支付的费用, 智能合约的逻辑越复杂, 花费的 Gas 就越多. Gas 价格是指花费每个 Gas 所需要的以太币的数量, 可由用户自行调整[79].

以太坊智能合约的开发语言是 Solidity 编程语言, Solidity 是一种语法类似 JavaScript 的高级语言. 由于以太坊虚拟机不会额外的对智能合约的执行进行限制, 为了保证安全, 需要智能合约自身具有完整确定性[80,81].

比特币通过引入 PoW 共识来规避少数人的恶意行为, 平均出块时间 10 分钟, 共识中临时性分叉所产生的孤块最终会被抛弃. 而以太坊出块时间缩短至 15 秒, 分叉频繁发生. 因此以太坊在设计中引入了 GHOST 协议, 以权重最高的子树作为合法主链, 同时对产生或发现孤块的矿工予以奖励, 鼓励分叉的及时合并[82].

比特币与以太坊的主链结构和选择方式如图 18 所示, 同样的情况下, 比特币系统将认为 0←1A←2A←3A←4A←5A 为合法主链, 而以太坊系统认为 0←1B←2C←3C←4B 为合法主链.

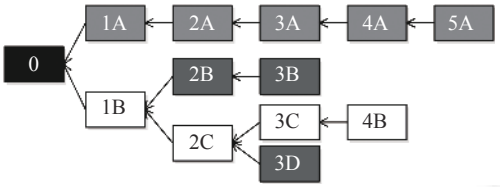

图 18 比特币和以太坊的合法链选择

以太坊也是区块链技术的一种实现, 所以第 2.1 节内的大部分攻击都能在以太坊中实施, 这里不再赘述, 本节将介绍几种特别针对以太坊及其智能合约的攻击, 代表了区块链 2.0 面临的典型安全风险.

2.2.1 平衡攻击 (balance attack)

平衡攻击的目的是阻止新交易被确认. 其利用了以太坊出块时间短的特点, 结合 GHOST 协议对以太坊系统进行破坏. 攻击者将以太坊上的诚实节点分为多个算力均等的子组, 通过延迟多个子组间的网络通讯, 使以太坊产生多条“势均力敌”的分叉. 攻击者使用自身的算力平衡这些分叉间微小的差距, 从而破坏共识机制, 阻止新交易被确认[83−85].

平衡攻击一般分为 4 步.

① 攻击者将诚实矿工隔离成多个算力接近的子组, 确保“自身算力+任意子组算力>任意子组的算力”;

② 攻击者通过延迟子组间的网络通信, 使区块链产生多条分叉, 每个子组都会选择不同子树进行区块打包;

③ 攻击者在每个分叉都进行区块打包, 并将自己打包好的区块隐藏起来, 不进行广播;

④ 攻击者时刻关注每个子组的本地视图, 若在某个子组的本地视图中, 有其他子树的权重要超过该子组原先

选择的子树时, 攻击者将自己已经打包好的区块广播, 以确保多个子组无法就最重子树达成共识.

平衡攻击的实现流程如图 19 所示.

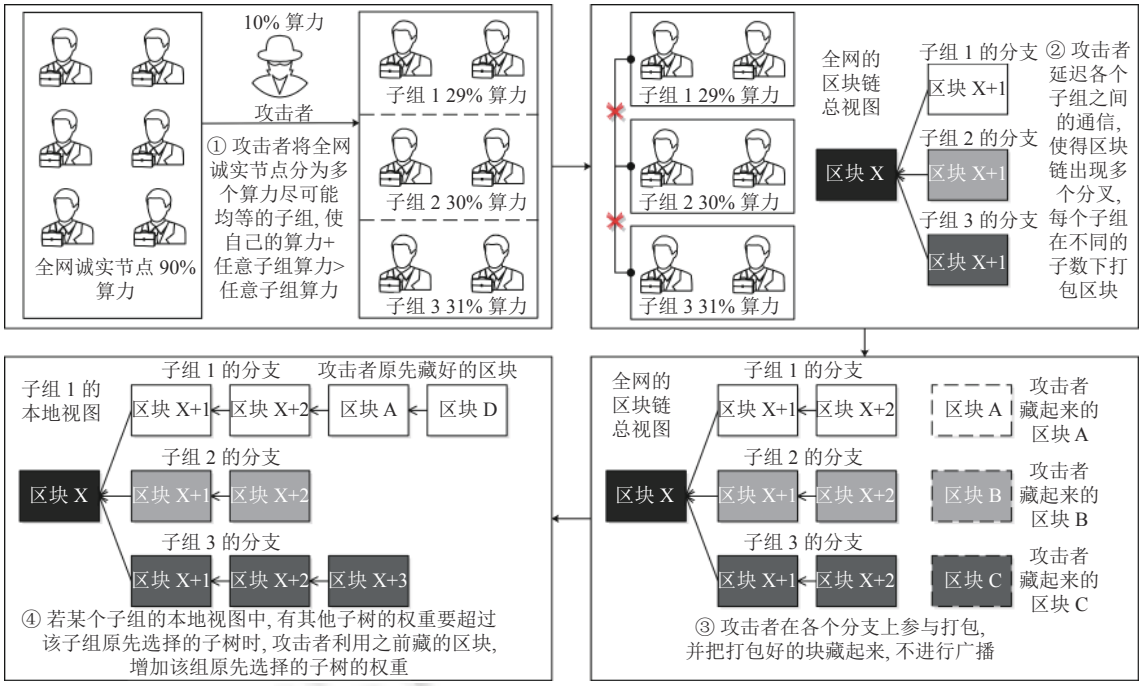

图 19 平衡攻击实现流程

防范方法: 区块链设计者可以加入区块权重机制至 GHOST 协议中, 使不同区块对最重子树共识的影响度不同, 主要有两种方案: 由于攻击者打包好区块后不会立刻广播, 可以设置区块权重与时间成反比, 加大攻击者利用隐藏的区块平衡各个子树权重的难度; 根据系统“历史树图结构”, 实时检测是否受到攻击, 设置检测到攻击前生成的普通区块权重为 1, 检测到攻击后生成的区块中 1/x 个特殊区块的权重为 x (x>>1), 其余特殊区块的权重为 0, 相当于在检测到攻击时提高挖矿的难度, 降低出块速度, 优先保证系统的安全性[86].

2.2.2 漏洞攻击 (vulnerability attack)

漏洞攻击是以太坊智能合约最主要的安全风险. 以太坊智能合约威胁较高的漏洞有整数溢出漏洞、可重入漏洞、交易顺序依赖问题、时间戳依赖问题、深度调用问题等[87].

(1) 整数溢出攻击 (integer overflow attack)

在程序语言中, 整数类型变量有最大值和最小值, 一旦在运算、转换等过程中超过这个值, 就会出现溢出的情况, 而以太坊智能合约实质上是一种用 Solidity 语言编写的程序代码, 也存在溢出问题. 智能合约中的余额常用无符号整数表示, 在编写智能合约时如果不加注意就会给攻击者可乘之机. 攻击者只需将自己的余额减去一个比该余额大 1 的值, 即可让自己的余额变成最大值[88].

(2) 可重入攻击 (reentrancy attack)

在以太坊中, 当智能合约 A 调用智能合约 B 时, A 会等待 B 的调用结束后再继续运行. 因此攻击者可以在智能合约 A 调用智能合约 B 时, 在 B 被调用的函数中加入回调语句——“使 A 调用 B 的代码”, 从而发起可重入攻击[89].

典型的可重入攻击一般分为 4 步.

① 智能合约 A 向智能合约 B 发出提现请求;

② B 向 A 转账, 并调用 A 的回调函数;

③ A 的回调函数继续提出“A 向 B 发起提现请求”, 两个合约进入互相调用的循环;

④ 当 Gas 用完或是受害者账户余额被耗光时, 攻击结束.

可重入攻击的实现流程如图 20 所示.

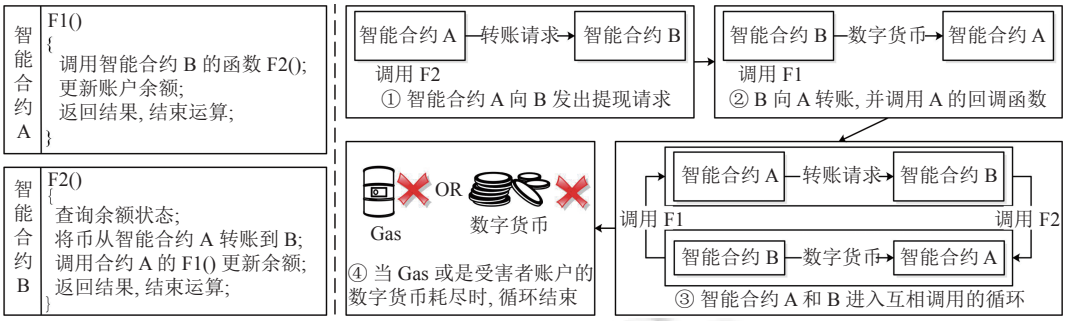

图 20 可重入攻击流程

(3) 交易顺序依赖攻击 (transaction-ordering dependence attack)

在以太坊中, 智能合约的执行结果随当前交易处理顺序的改变而改变. 智能合约被矿工打包到一个区块内需要一定的时间, 攻击者如果在打包完成前监听到网络中智能合约调用, 那么他就可以发布自己的调用或新合约来改变当前的合约状态. 这种攻击方式称为交易顺序依赖攻击[90].

交易顺序依赖攻击一般分为 4 步.

① 攻击者发布一个悬赏合约 A, 悬赏金较高;

② 等待有应征者完成悬赏任务;

③ 在验证节点还未确认悬赏任务成功前, 发布一个将 A 中悬赏金额调低的智能合约 B, 并设置较高的 Gas 费;

④ 验证节点会先验证高费率的智能合约 B, 导致应征者收到的赏金变低, 攻击完成.

交易顺序依赖攻击的实现流程如图 21 所示.

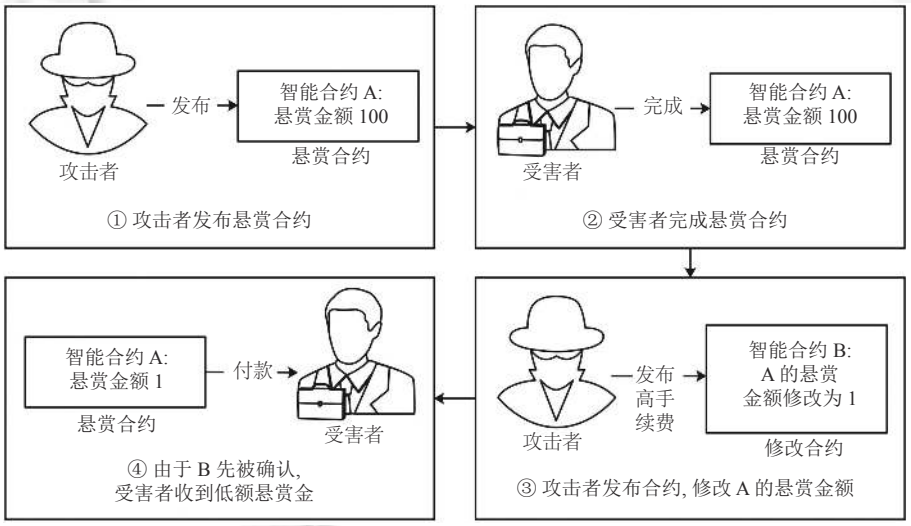

图 21 交易顺序依赖攻击流程

(4) 时间戳依赖攻击 (timestamp dependence attack)

在区块链中, 每个区块都拥有一个时间戳, 而这个时间戳通常是矿工用本地时间设定的. 由于某些智能合约的触发条件依赖于时间戳, 如果攻击者挖到包含该智能合约的区块就可以设定利于自己的时间戳, 从而发动时间戳

依赖攻击[91].

(5) 调用深度攻击 (call depth attack)

调用深度攻击可以让智能合约里的任何调用失败, 即使这些调用是完全正确且可信的. 在合约虚拟机中, 智能合约互相调用的深度会有一个阀值, 一旦调用栈的深度到达阀值, 再调用的函数及其子调用都会失败. 攻击者可以通过控制调用深度, 使得某些如转账、余额清零等关键操作无法进行[92].

防范方式: 对于区块链程序员来说, 养成良好的编程习惯, 理清程序逻辑可以有效的减少漏洞的产生; 对于区块链公司来说, 做好智能合约的安全审计工作, 可以聘请专业的审计公司进行服务, 挖掘智能合约漏洞并进行修复.

3 区块链周边安全问题

正如上文所述, 区块链设计者在设计区块链机制时, 常会出现一些技术漏洞, 给攻击者以可乘之机, 危害区块链系统安全. 但攻击者除了可以利用区块链系统本身设计或实现上的漏洞攻击区块链外, 还可以通过攻击区块链的周边设施, 例如交易所、数字钱包、矿池/矿场等, 来牟取钱财或私利. 这类安全风险并不是由于区块链技术本身的设计缺陷, 或者区块链系统的部署实施, 而是由于区块链应用开发、软件工具、实践过程中缺乏必要的安全考虑或措施所造成的.

下面例举 3 种用于加密货币的区块链周边服务或软硬件周边设施所面临的安全问题.

3.1 交易所面临的安全问题

交易所掌握着众多用户的多种数字加密货币, 是攻击者可以通过较小代价获取极大利益的地方, 交易所被攻击的事件层出不穷[93,94], 主要有以下几种.

3.1.1 分布式拒绝服务攻击 (distributed denial of service attack)

交易所遭遇的拒绝服务攻击多数是分布式拒绝服务 (DDoS) 攻击. 攻击者通过大量傀儡机向目标发送合法的请求以占用大量网络资源, 从而瘫痪目标网络, 使合法用户无法获得服务的响应[95−97]. 分布式拒绝服务攻击一般分为 4 步.

① 攻击者搜集受害交易所网络以及主机的相关情报;

② 攻击者根据收集到情报, 准备一定数量的傀儡机以及适合的攻击手段;

③ 攻击者通过控制所有傀儡机向受害交易所发送海量合法请求, 导致交易所大量的网络资源被占用;

④ 受害交易所最终无法处理海量的请求, 导致网络瘫痪, 其他合法用户的请求无法被响应[98].

分布式拒绝服务攻击的实现流程如图 22 所示.

防范方法: 交易所应做好预警工作, 开启防火墙并实时监控网络中的流量状况; 被 DDoS 攻击时关闭不必要服务的端口并对所有流量进行流量识别, 从而清洗攻击流量.

3.1.2 账户盗窃攻击 (account theft attack)

在区块链交易系统中, 盗窃用户账户是常见攻击之一. 由于交易所是中心化机构, 存放了大量用户的账户信息, 所以对于攻击者而言, 入侵交易所来获得大量账号、密码、私钥等是一种性价比较高的方式[99], 其基本攻击流程如下.

① 攻击者黑进交易所后, 获得大量账号和密码;

② 将账户内的加密货币进行抛售, 以引起大量加密货币下跌;

③ 市场恐慌性抛售后, 攻击者大量买入低价币, 使其币值飞速上涨, 从而场外套现获利.

防范方法: 区块链用户应选择对恶意攻击免疫能力较强的交易系统; 交易所应评估自身基础设施的安全性能, 采取相应安全防御策略; 交易所还可以实时备份数据, 并提高相关人员的安全意识.

3.1.3 交易延展性攻击 (transaction malleability attack)

交易延展性是指在区块链中, 交易 ID (TXID) 在矿工确认之前是可以被修改的. 攻击者可以利用这个特性, 向交易所发动交易延展性攻击[100,101].

交易延展性攻击一般分为 4 步.

① 攻击者将数字货币存入交易所中;

② 攻击者向交易所申请取回数字货币, 交易所同意该申请并在网络中广播向攻击者转币的交易 A;

③ 攻击者截获交易 A, 利用交易延展性修改交易 A 中签名的编码格式得到交易 B, 使得交易 ID 产生变化的同时签名仍有效. 攻击者再将通过交易延展性得到的交易 B 放到网络中广播;

④ 攻击者用交易 A 的交易 ID 向交易所投诉, 声称自己没收到数字货币. 交易所利用交易 A 的交易 ID 查询是否有转账给攻击者的交易. 由于交易 A 被截获, 网络中不存在交易 A, 交易所会误认为转账失败并再次转币给攻击者, 至此, 攻击者会获得两份数字货币.

交易延展性攻击的实现流程如图 23 所示.

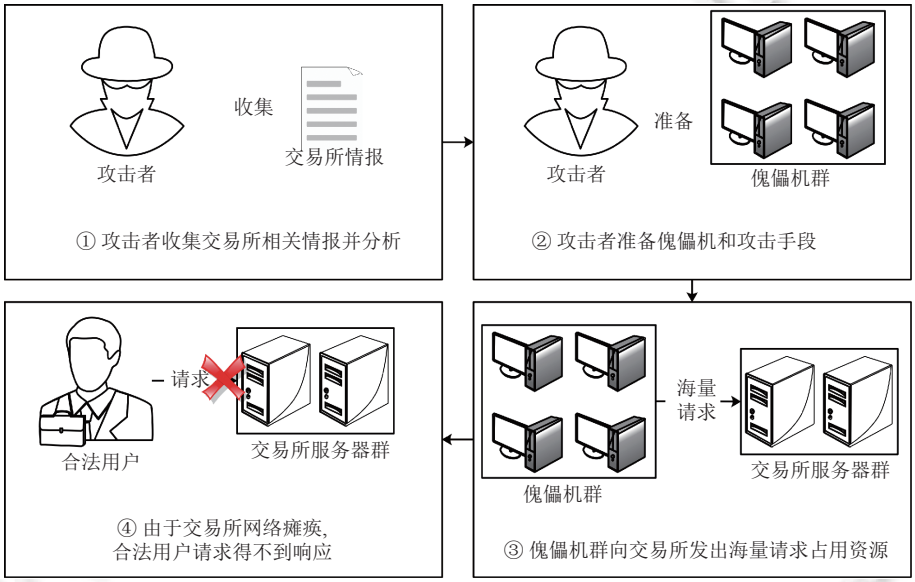

图 22 分布式拒绝服务攻击实现流程

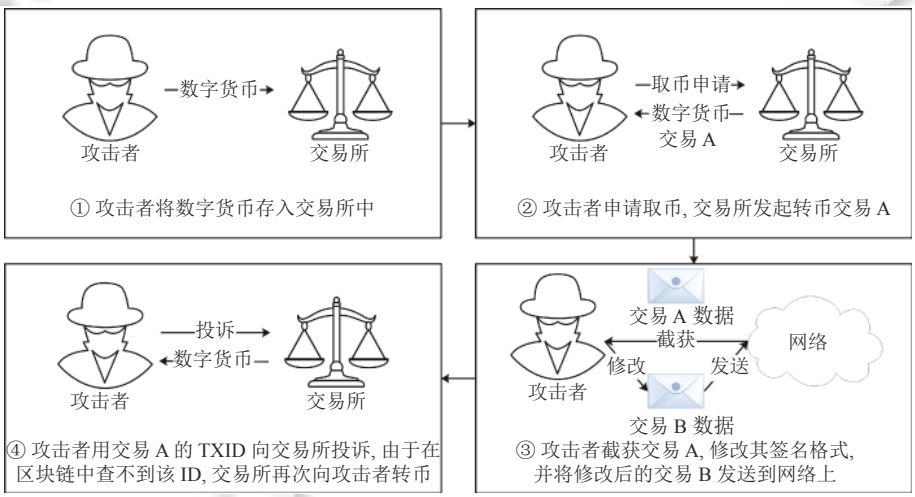

图 23 交易延展性攻击实现流程

防范方式: 区块链设计者可以利用隔离见证技术, 使攻击者无法通过修改签名格式, 在改变 TXID 的情况下不影响签名的合法性[102].

3.2 数字钱包面临的安全问题

加密数字货币的归属权是由一对数字密钥决定的, 某地址与该地址对应的私钥存在一定的数学联系, 拥有私钥的人便能获得对应地址的数字加密货币的处置权. 数字钱包本质上是一种软件, 其存储了区块链上的某些地址以及这些地址对应的私钥. 加密数字货币钱包主要分为在线钱包和离线钱包两种[103].

在线钱包也称热钱包, 是一种在使用的过程中, 必须保持联网状态的钱包, 这类钱包通常以在线钱包和交易平台钱包等形式出现. 在使用在线钱包交易数字加密货币时, 外界可以通过互联网访问到存储私钥的位置, 因此在线钱包容易受到黑客的攻击.

离线钱包也称冷钱包, 是一种一直处于非联网状态的钱包, 这类钱包依靠不联网的硬件设备运行, 外界一般无法通过网络访问到其存储私钥的位置, 因此可以有效避免黑客攻击或中木马病毒等情况造成的损失. 但其也可能因为硬件设计存在问题, 导致漏洞产生, 留下一定的隐患[104].

数字钱包面临的安全问题主要为私钥窃取攻击 (private key theft attack), 攻击者通过黑入联网的在线钱包、篡改官方钱包并诱导用户下载等方式, 获取用户地址私钥, 实现私钥窃取攻击.

防范方式: 大多数情况下, 离线钱包相较在线钱包而言不易受到攻击, 因此区块链用户应使用安全性更高的离线钱包防止攻击者入侵; 数字钱包的设计者不应急于发布硬件产品, 应在产品安全性评估合格后再发售. 另外, 数字钱包的设计者在发布自己软件产品的同时, 应留下软件的散列值, 并督促用户在下载前检查散列值是否与软件匹配, 防止攻击者篡改在线钱包软件.

3.3 矿池/矿场面临的安全问题

矿池/矿场作为 PoW 区块链网络算力的主要来源, 若其自身基础安全防护措施考虑不周, 则会引起高危安全风险. 大规模的矿池/矿场常使用远程管理系统以便管理, 由于这些系统的远程管理机制可能不健全, 或是由于矿池/矿场对远程管理系统不够重视, 使得攻击者利用这些薄弱点, 对矿池/矿场进行攻击. 恶意挖矿策略也是矿池/矿场面临的安全问题之一, 攻击者通过恶意策略抢夺或是单纯的损害诚实矿池/矿场的利益[105].

3.3.1 自私挖矿攻击 (selfish mining attack)

自私挖矿攻击是一种针对基于 PoW 共识的区块链的恶意挖矿策略. 实施自私挖矿攻击的恶意矿池在挖到新区块时, 不会立即发布新区块, 而是根据自私挖矿策略决定是发布该块还是继续在自私分叉上挖矿. 当自私分叉长度超过公共链长度时, 若恶意矿池公开分叉链, 则原公共链包含的所有数据将会回滚, 区块链用户将损失回滚部分的数字货币收入, 诚实矿池也将损失原主链上的出块奖励. 自私挖矿攻击同时会导致在诚实矿池中工作的矿工为了获得“超额”的挖矿奖励, 转而加入恶意矿池进行工作, 诚实矿池的算力逐步被蚕食[106−109].

自私挖矿攻击一般分为 3 步.

① 攻击者在最长链上挖矿, 并在合适的时候创建自私分叉;

② 攻击者实时监测网络中新区块的发布情况, 根据最新的发布情况执行对应的策略;

③ 若攻击者挖到新区块, 攻击者则不发布该块而是在该块后继续自私挖矿, 转到步骤②; 若诚实矿池挖到新区块且分叉链长度比主链短, 攻击者则放弃私链, 转到步骤①; 若诚实矿池挖到新区块且分叉链长度和主链相同, 攻击者则立刻发布分叉链, 这种情况下, 攻击者的分叉链仍有一定几率被全网认可, 转到步骤①; 若诚实矿池诚实矿池挖到新区块且分叉链长度−主链长度>1, 攻击者则继续在分叉链上挖矿, 转到②; 若诚实矿池挖到新区块且分叉链长度−主链长度=1, 攻击者则立刻发布分叉链, 转到步骤①[110].

自私挖矿攻击的实现流程如图 24 所示.

防范方式: 改进挖矿规则. 当矿工收到两个及以上的相同长度的分支时, 他必须传播所有分支并随机选择一个分支, 在其后继续挖矿, 从而增大恶意矿池进行自私挖矿的成本[111].

3.3.2 跳池攻击 (pool hopping attack)

矿池聚集了众多矿工的算力, 在矿池中, 一般根据算力大小给矿池内参与挖矿的矿工结算收益, 结算模式有很多, 例如 Proportional 模式、PPS 模式、PPLNS 模式等. 如果矿池使用的是 Proportional 模式付给矿工报酬, 矿工

很有可能为了自己的利益向矿池发动跳池攻击. 在 Proportional 模式下, 从矿池挖到上个区块到挖到当前区块的时间被称为一个挖矿周期, 每个矿工的区块奖励与一个挖矿周期内其有效工作量证明 (share) 所占全部有效工作量的百分比成正比. 因此矿工们收益最高的策略是当当前挖矿周期长度到达一个阀值后, 跳槽到另一个才发现新区块、挖矿周期较短的矿池重新开始挖矿[112−115].

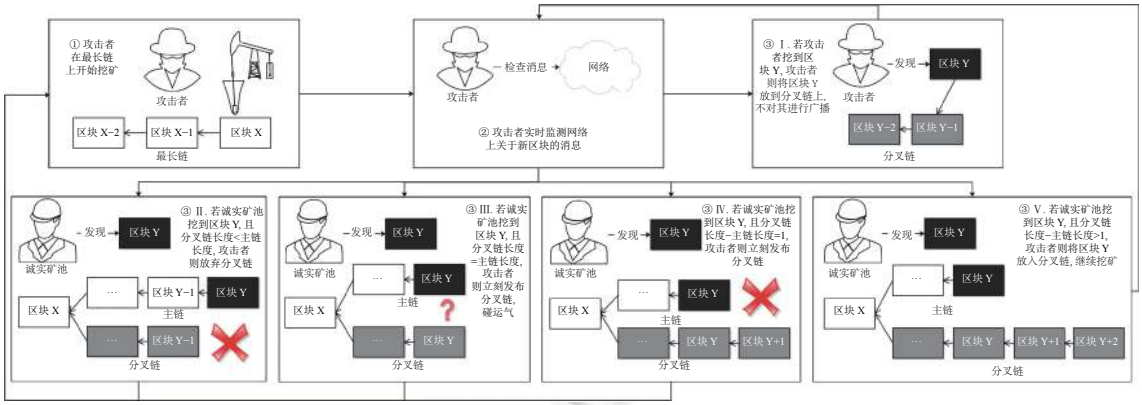

图 24　自私挖矿攻击实现流程

防范方式: 矿池应采用更优的收益结算模式, 如 PPS 模式或 PPLNS 模式, 防止矿工为了自身利益最大化, 进行跳池攻击.

3.3.3　扣块攻击 (withholding block attack)

扣块攻击是指恶意矿工在挖到新区块后不向矿池提交, 而是直接丢弃该区块, 从而减少矿池收入的攻击. 这种攻击同时损害了恶意矿工和矿池的利益, 但矿池损失的要比恶意矿工损失的更多. 扣块攻击并不是完全无利可图的, 如果矿池是按 PPS 模式, 即:

矿工的收益=矿池用于奖励矿工的总币量×某个矿工提供的算力/当前网络难度.

付给矿工报酬, 恶意矿工即使不提交区块也可以领到一定报酬; 如果矿池是按 PPLNS 模式, 即:

矿工的收益=矿池用于奖励矿工的总币量×出块时该名矿工提交的有效工作量证明在总有效提交中占比.

付给矿工报酬, 矿池的竞争对手可以通过派出恶意矿工加入该矿池进行扣块攻击, 使该矿池整体收益下降, 从而促使受害者矿池的矿工跳槽到新矿池工作[116−118].

防范方式: 矿池可以偶尔向手下的矿工进行突击检查, 提供解决方案已知的任务, 诱使恶意矿工落入陷阱并找出他们[119]; 或是更改挖矿算法使得矿工无法验证得到的有效工作量证明 (share) 是否是符合区块解, 从而无法将精确挑选出符合区块解的答案, 将其丢弃.

4　区块链用户面临的安全问题

攻击者除了可以攻击区块链自身与区块链周边设施外, 还可以攻击区块链用户. 但与区块链自身机制与区块链周边设施不同的是, 区块链设计者没有在用户层面设计过多复杂的机制, 因此区块链用户所遇的安全问题通常为网络安全领域中的通用攻击. 以下介绍 3 种用户面临的典型安全问题.

4.1　社会工程学攻击 (social engineering attack)

近些年来, 社会工程学攻击[120,121]开始流行起来. 欺诈者通过冒充官方人员或权威人士, 向区块链用户索取一定量的数字加密货币, 甚至直接索要私钥. 区块链用户如果不及时确认对方身份就极易上当受骗, 因而遭受损失.

防范方法: 用户应在透露重要信息前及时确认对方身份; 同时应当妥善保管私钥, 切勿将私钥透露给其他人, 谨防欺诈.

4.2 中间人攻击 (man-in-the-middle attack)

中间人攻击是一种较为传统的网络攻击手段, 攻击者能够在通信双方毫不知情的情况下, 通过拦截网络通信数据, 对数据进行嗅探和篡改[122,123]. 区块链本身对中间人攻击具有一定的免疫力, 但在数字货币场外交易中——例如在场外交易平台中进行货币交易, 中间人攻击仍是一种可行的攻击方式. 中间人攻击一般分为 6 步.

① 受害者发出与卖家进行交易的申请, 攻击者截获受害者的通信数据;

② 攻击者将受害者通信数据里的公钥换成自己的公钥并发给卖家;

③ 卖家同意交易, 并把自己区块链中的地址等交易信息发送给受害者;

④ 攻击者截获卖家发出的通信数据, 并把收款地址改成自己区块链中的地址, 并用受害者公钥加密, 再把篡改后的通信数据给受害者;

⑤ 受害者收到攻击者篡改后的通信数据后, 将数字货币转至攻击者的地址;

⑥ 攻击者收到了受害者的数字货币, 但卖家没收到, 因此交易失败. 受害者白白损失了该笔数字货币.

中间人攻击的实现流程如图 25 所示.

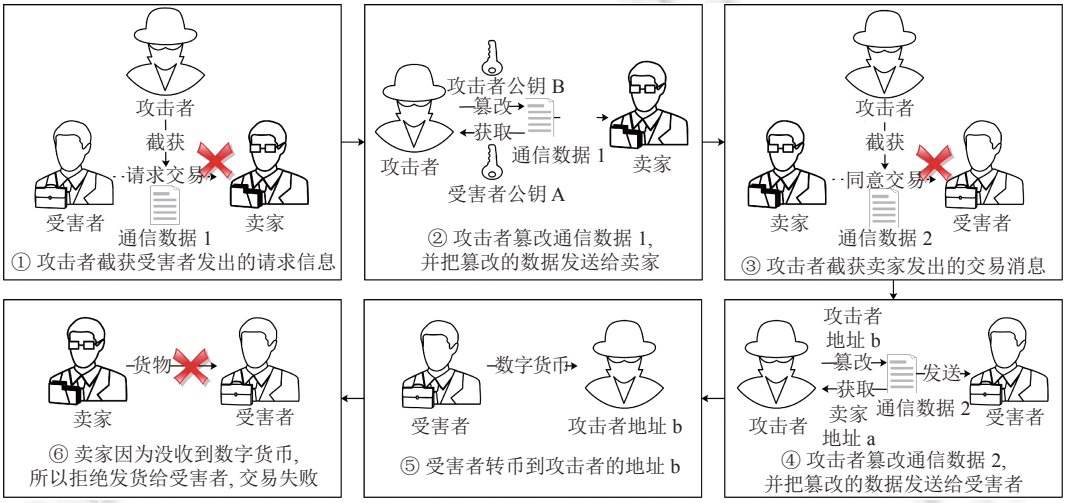

图 25 中间人攻击实现流程

防范方式: 用户应在通信过程中引入数字证书技术. 用户可以通过可靠的数字证书认证机构认证对方身份, 确保自己是在和正确的通信者进行消息交换, 防止攻击者拦截并篡改消息[124].

4.3 撞库攻击 (credential stuffing attack)

安全意识不高的用户常常会在其他网站使用与交易平台相同或相似的账户密码. 一旦这些账户密码被泄露或者被窃取, 攻击者就可以利用这些账号和密码, 在区块链交易平台上进行撞库攻击[125].

撞库攻击一般分为 4 步.

① 拖库: 攻击者搜寻受害网站, 通过社会工程手段 (收买管理员、钓鱼等) 或者技术手段 (Web 漏洞、服务器漏洞、配置错误等) 取得该网站的访问权限;

② 洗库: 攻击者对受害网站的数据库进行信息筛选, 得到所需数据, 若数据库中的数据被加密则使用破解技术破解;

③ 撞库: 攻击者对得到的数据进行整理, 选择出账户密码数据;

④ 尝试: 攻击者用得到的账户和密码在区块链交易平台上进行尝试, 同时利用这些账户和密码为攻击其他网站做准备, 转到①[126].

撞库攻击的实现流程如图 26 所示.

防范方式: 用户不应在多个网站上设置同一个密码; 对于重要的账户, 要使用高强度的密码防止被破解; 不要将密码保存在公共设备上, 防止被泄露.

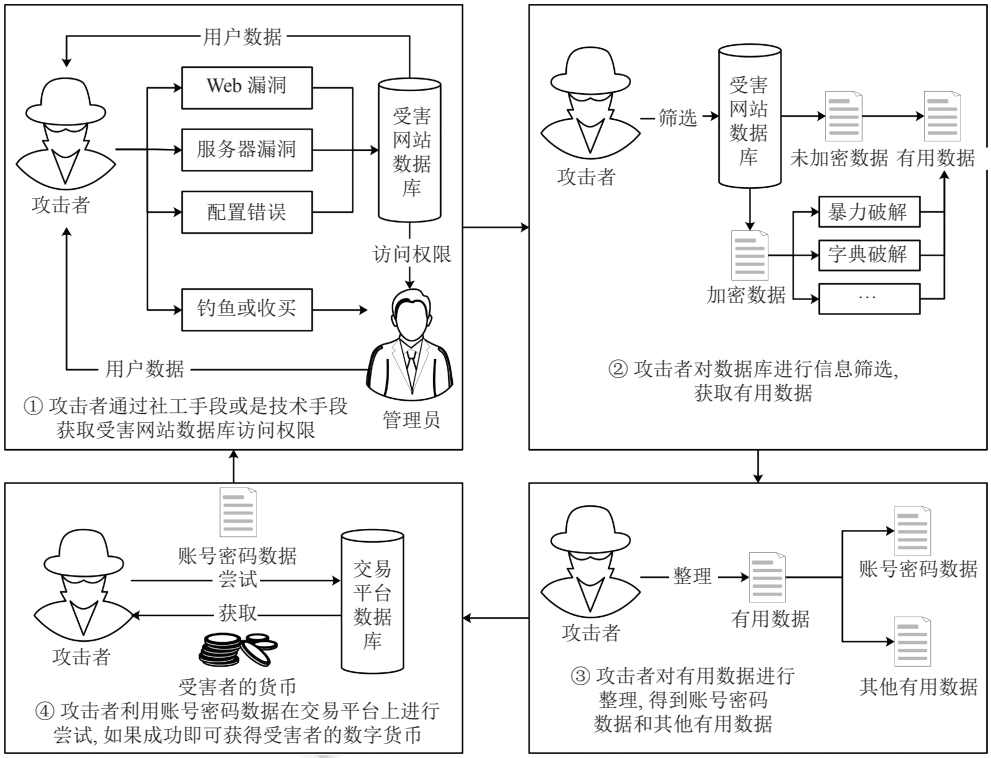

图 26 撞库攻击实现流程

5 区块链安全问题分类与总结

针对区块链技术在数字货币交易等应用领域, 前文介绍了多种典型的安全问题和攻击方法, 本节将对这些问题按照区块链系统的层次架构进行分类并总结.

5.1 区块链层次架构介绍

一个典型的区块链系统一般分为 6 层, 从上到下分别为应用层、合约层、激励层、共识层、网络层、数据层, 如图 27 所示. 每层各司其职又互相协作, 最终实现一个去中心化的协作系统和信任机制.

(1) 数据层: 数据层描述了区块链的数据结构与相关的加密技术, 实现数据的去中心化存储、完整性与合法性校验、可追溯性与不可篡改性保证等功能.

(2) 网络层: 网络层主要通过分布式组网机制、数据传播机制、数据验证机制, 搭建区块链网络中各个节点之间信息交流的桥梁.

(3) 共识层: 共识层采用了各种共识算法, 例如工作量证明 (PoW)、权益证明 (PoS)、股份授权证明 (DPoS) 等, 使区块链系统中的高度分散的节点能够快速且正确地针对区块数据的有效性达成共识.

(4) 激励层: 激励层为区块链提供了激励措施, 使各个节点实现自身利益最大化的个体理性行为与保障区块链系统安全有效的总体目标相一致.

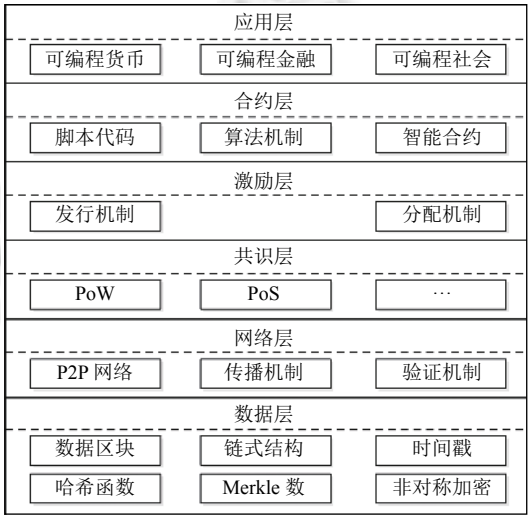

图 27 区块链应用系统的层次结构

(5) 合约层: 合约层封装了区块链的各类脚本代码、算法和智能合约, 是灵活编程和操作区块链系统的基础.

(6) 应用层: 应用层封装了区块链的各种应用场景和案例, 支持数字货币交易、去中心化应用等 (DApp), 实现可编程货币、可编程金融、可编程社会[127].

5.2 安全问题分类

下面对本文所述全部 36 种安全问题综合区块链基本架构进行分类, 并分析每种攻击所依赖的共识以及攻击实施难度, 区块链安全问题分类如表 1 所示. 需要说明的是, 在表中, 若某层级被勾选, 则说明该攻击会使该层级的某些功能失效或出错. 例如, 边界网关劫持攻击通过拦截区块链网络流量, 阻止广泛共识的达成, 由于其破坏了网络层的节点通信能力, 同时也破坏了共识层的共识过程, 因此网络层和共识层被勾选; 空块攻击通过拒绝打包交易到区块中, 用不合法的手段获得更多的出块奖励, 由于其既破坏了激励规则又阻碍了区块链记录合法交易, 因此数据层和激励层被勾选.

表 1 区块链安全问题分类

安全问题	被攻击的区块链层级						依赖哪种特定共识	实施难度
	数据层	网络层	共识层	激励层	合约层	应用层		
双花攻击	√	√	√	√	—	—	不限	较低
51%攻击	—	—	√	—	—	—	PoW	较高
贿赂攻击	—	—	√	√	—	—	PoW	较低
币龄累计攻击	—	—	√	—	—	—	PoW+PoS	较低
通用挖矿攻击	—	—	√	—	—	—	PoW	低
芬尼攻击	—	√	√	—	—	—	不限	较低
种族攻击	—	—	√	√	—	—	不限	较低
边界网关劫持攻击	—	√	√	—	—	—	不限	较高
重放攻击	√	—	—	—	—	—	不限	较低
空块攻击	√	—	—	√	—	—	PoW	低
削弱攻击	√	—	√	—	—	—	PoW	低
无利害关系攻击	—	—	√	—	—	—	PoS	低
长程攻击	√	—	√	—	—	—	PoS	较高
简单攻击	—	—	√	—	—	—	PoS	低
变节攻击	—	—	√	—	—	—	PoS	较高
权益流损攻击	√	—	√	—	—	—	PoS	较高
粉尘攻击	√	—	—	√	—	—	不限	较低
女巫攻击	—	—	√	—	—	—	BFT	较低
日蚀攻击	—	√	—	—	—	—	不限	高
平衡攻击	√	√	√	—	—	—	PoW	高
漏洞攻击	—	—	—	—	√	—	不限	较低
整数溢出攻击	—	—	—	—	√	—	不限	低
可重入攻击	—	—	—	—	√	—	不限	低
交易顺序依赖攻击	—	—	—	—	√	—	不限	较低
时间戳依赖攻击	—	—	—	—	√	—	不限	较低
调用深度攻击	—	—	—	—	√	—	不限	低
DDoS攻击	—	√	—	—	—	√	不限	较低
账户盗窃攻击	—	—	—	—	—	√	不限	较低
交易延展性攻击	√	—	—	—	—	—	不限	较低
私钥窃取攻击	—	—	—	—	—	√	不限	低
自私挖矿攻击	—	—	—	√	—	—	PoW	较高
跳池攻击	—	—	—	√	—	—	PoW	较低
扣块攻击	—	—	—	√	—	—	PoW	低
社会工程学攻击	—	—	—	—	—	√	不限	低

根据安全问题分布图 28, 不难发现, 大多数攻击针对的是区块链的共识层, 因此设计一种漏洞较少、安全性较高的共识机制是区块链安全领域的研究重点; 另外, 大部分区块链攻击具有通用性, 其执行不依赖于特定的共识机制, 即在大部分区块链应用系统中均能实施. 因此, 区块链的设计者们可以参考本文所述防范方法, 或是借鉴其他设计者的经验教训, 从而设计出安全可靠的区块链系统. 除了通用的攻击方式外, 针对 PoW 共识机制的区块链攻击较多, 这是由于 PoW 作为当前最主流区块链共识算法, 被深入研究并频繁实践. 研究针对 PoW 共识的攻击对攻击者而言收益较高, 但这不代表其他共识算法足够安全, 区块链的拥有者和用户仍需要保持一定警惕性, 制定合理的应急策略, 以便在遭遇攻击时尽可能的减少损失.

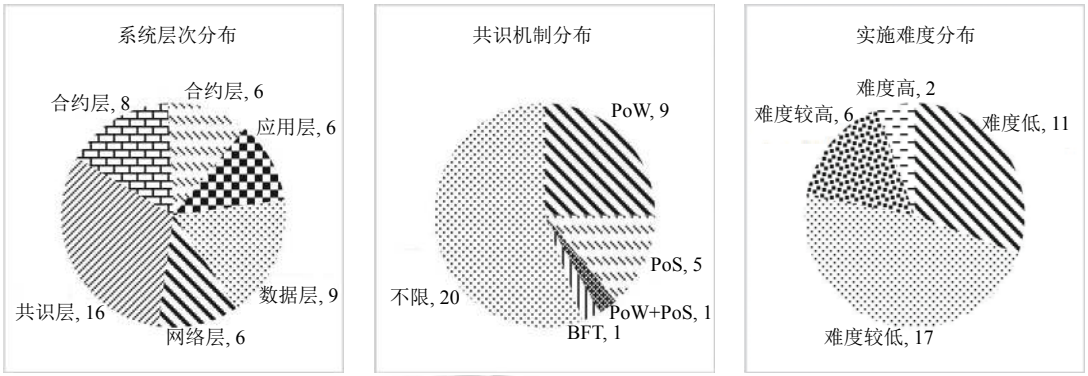

图 28　区块链应用系统的安全问题分布

为了粗略评估各攻击的安全风险程度, 本文将攻击实施难度分为四类. 难度低代表成功实施该类攻击几乎不需要攻击者投入成本, 也不依赖苛刻的时机, 可行性较高. 如通用挖矿攻击, 攻击者只需要从主流币处调来矿机, 并花费少量电费, 就可以对山寨币进行攻击. 再例如整数溢出攻击、调用深度攻击, 攻击者只需知晓智能合约的整数范围、调用深度, 并花费少量交易费, 就可以轻松的发起攻击. 难度较低代表成功实施该类攻击需要攻击者投入一定的成本或是需要等待特定的时机, 可行性适中. 如贿赂攻击、币龄累积攻击, 攻击者需要投入一定的成本用于贿赂矿工或是进行币龄积累, 才能成功完成攻击. 再例如时间戳依赖攻击、交易延展性攻击, 攻击者需要监听或者拦截到特定的交易, 才能成功实施攻击. 难度较高代表成功实施该类攻击需要攻击者投入大量成本或是需要等待较为苛刻的时机, 可行性较低. 如 51% 攻击, 攻击者需要全网超过 51% 的算力才能成功完成攻击, 想要在大型链中获得 51% 算力, 需要投入大量的成本. 再例如, 自私挖矿攻击, 攻击者首先需要一定算力, 同时也需要连续挖到几个区块后, 才能成功实施攻击. 难度高代表成功实施该类攻击需要攻击者投入极大成本并且需要苛刻的时机, 难以实施. 如日蚀攻击, 攻击者需要大量傀儡机尝试与受害节点进行连接, 从而恶意填充受害节点的节点表, 该步骤时间较长, 并且需要等待受害节点自己重启, 这种重启不受攻击者控制, 可控性差. 再例如平衡攻击, 攻击者首先需要知晓全网节点的网络状态, 并将所有诚实节点划分成多个算力几乎均等的子组, 并切断各个子组间的通信, 到该步骤为止已经需要相当大的成本了, 之后还需要不断监控各个子组的本地视图, 并在必要的时刻将自己已经挖好的区块广播, 在此过程中, 各个子组间的通信仍要被切断, 因此, 该攻击的实施难度非常高.

5.3　当前研究方向与最新进展

由于区块链仍处于发展状态, 自身机制、周边设施、用户安全意识都不够成熟, 基础架构的每个层次都易受到攻击. 当前, 世界各地的研究者从攻防两侧提出了很多有用的攻击、防御策略, 本节将以区块链架构的 6 个层次为划分, 分别介绍当前区块链安全方向的研究方向与最新进展, 供读者参考.

(1) 数据层

① 应对量子计算的挑战: 现阶段大多数区块链底层的加密算法是椭圆曲线算法, 但椭圆曲线算法不是一种抗量子攻击算法, 易受到未来的量子攻击的威胁. Shahid 等人提出了一种新的一次性签名 (OTS) 算法, 该算法对量子计算有一定的抵抗性, 且与现有的所有 OTS 方案相比, 该方案的密钥和签名大小都是最小的[128].

② 保护隐私: 区块链上的智能合约允许节点们在没有可信第三方参与或监督的情况下进行可信交易, 但由于智能合约内可能存在隐私信息, 且智能合约需要在参与节点上运行, 这会导致某节点的隐私被其他节点知晓. 在数字加密货币区块链中常使用零知识证明技术以保证用户使用数字货币时不透露自己的身份, 但零知识证明技术仍存在一些问题, 例如只能保证 2 个当事方参与交易却不泄露自己的隐私信息. Wan 等人提出了一种用于认证数据的零知识证明方案, 它将零知识证明技术与数字签名技术有效结合, 保证了智能合约的数据保密性和真实性[129]. Harris 等人提出了一种基于共识的秘密共享协议, 该协议允许多个当事方参与交易, 并且不会泄露任何个人隐私信息[130].

(2) 网络层

网络入侵检测系统: 入侵检测系统常通过自动识别并过滤异常活动, 来保护网络和系统免受意外攻击, 以增强网络的安全性. 在区块链中, 大量攻击是通过网络层攻击区块链本身, 如日蚀攻击, 分割攻击等. 为此 Signorini 等人设计了一种针对于区块链系统的异常检测工具, 它允许区块链网络的对等节点通过共享历史的攻击信息来抵御日蚀攻击[131].

(3) 共识层

① 避免互操作场景下中的双花攻击: 双花攻击是区块链中非常典型的攻击之一, 单一区块链中的双花攻击已经被深入研究过, 但在跨链技术日渐成熟的现在, 交易常常由多个区块链协作完成, 这种互操作场景下的双花攻击研究较少. Sai 等人提出使用中立的观察者来监视跨多个链的交易, 并设计了一种协议消除互操作场景下的双花攻击[132].

② 研究双花攻击的变种攻击: 传统的双花攻击有 51% 攻击、贿赂攻击、种族攻击等, 大量学者已经对这些攻击进行过研究, 但双花攻击仍存在新的变种. Zhang 等人介绍了一种新的联合攻击形式——基于女巫攻击的比特币双花攻击, 并提出了两种解决该攻击的防御方案[133].

(4) 激励层

① 避免跳池攻击: 跳池攻击是一种矿工通过寻找并采用最佳的跳槽策略, 使得自己利益最大化的过程, 现在较为流行的矿池收益结算模式是 PPLNS, 但这种模式仍存在一些问题. Zolotavkin 等人利用博弈论模型分析了 PPLNS 结算模式下的跳池攻击, 并给出了避免跳池攻击的方案[134].

② 扣块攻击的最优策略与解决方案: 在矿池间的竞争中, 扣块攻击是较为常见的破坏手段, 使用多少算力攻击其他矿池能带来最大的收益成为恶意矿池所面临的一个重要决策问题. Qin 等人提出了恶意矿池最佳扣块策略, 并给出了攻击成功条件[135]. Kaci 等人提出了一种新的区块链架构, 用于管理矿池、矿工的信誉, 该架构允许矿池接受可信的矿工, 矿工也可以对矿池进行评估, 从而建立起矿池和矿工之间的信任, 减少扣块攻击出现的可能[136].

(5) 合约层

① 智能合约漏洞检测: 智能合约经常由于程序员的不良编程习惯和疏忽大意, 产生一些安全漏洞. 攻击者如果找到这些漏洞就可以对使用这些合约的受害者进行攻击. Gao 等人提出了一种自学习智能合约特性的方案, 该方案可进行合约重复代码检测、合约错误检测和合约验证[137]. Wang 等人提出了一种基于机器学习的智能合约漏洞检测方法, 该方法从智能合约的简化操作代码中提取二元特征, 并利用五种机器学习算法和两种采样算法构建了漏洞检测模型[138]. Samreen 等人提出了一个动、静态分析相结合的智能合约检测框架, 来检测 Etalum 中的可重入漏洞[139].

② 智能合约代码修复: 现有的智能合约安全分析工具侧重于漏洞检测, 但很少考虑智能合约代码的修复问题. Zhang 等人提出了一种智能合约代码自动修复系统, 该系统可以对智能合约字节码进行修正, 并帮助开发者发布智能合约[140].

(6) 应用层

为金融安全提供可靠的调查模型. 由于区块链消除了交易对可信第三方的需求同时具有匿名性, 某些不法分子会利用基于区块链的数字加密货币进行洗钱等违法操作. Wu 等人提出了一种基于扩展的安全 Petri 网的比特币交易网络分析方法, 该方法利用 Petri 网的结构特征和动态语义来定义比特币交易的静态与动态特征, 用于分析和

查找与非法交易相关的可疑地址[141].

总体而言, 近些年国内外学者针对区块链各个层级的研究都取得了丰硕的研究成果. 从研究趋势上看, 针对数据层、共识层和合约层的研究数量不断上升, 逐渐成为当前区块链安全领域的研究重点. 根据区块链应用需求和现有的研究成果, 本文认为在区块链安全领域, 未来研究将向隐私安全、智能合约安全和跨链技术安全 3 个方向发展.

隐私安全: 当前区块链隐私安全方向的研究重点是为用户提供一套隐私保护方案. 现有方案主要利用零知识证明、安全多方计算、同态加密等技术, 在区块链账本公开透明的前提下增加匿名性, 最大程度地确保区块链用户的个人隐私安全. 一方面, 零知识证明等技术的引入, 为区块链系统添加了额外的操作流程和步骤, 势必会带来不小的时空代价, 导致区块链的可用性和可拓展性大大降低; 另一方面, 匿名程度的上升必然会使违规交易追踪与监管面临严峻的挑战. 因此, 如何在匿名性与交易性能、匿名性与监管难度间取得合理平衡将成为区块链隐私安全领域的研究重点.

智能合约安全: 当前智能合约安全的研究重点主要为智能合约漏洞检测与修复. 现有的漏洞检测方案可以针对智能合约中的简单漏洞进行检测并提供审计报告, 部分降低了智能合约开发者出错的可能和人工审计成本. 但由于智能合约版本更新换代较快, 各个平台采用的智能合约底层框架不尽相同, 现有方案很难为所有平台所有版本的智能合约提供漏洞检测服务, 因此设计一种通用性强的智能合约漏洞检测工具是未来研究方向之一. 除了漏洞检测, 未来还可以通过研究标准化的智能合约编写工具以及智能合约漏洞自动修复工具来减少智能合约的安全风险. 另外, 站在智能合约设计者的角度, 为预防在复杂合约的编程过程中可能出现的安全漏洞以及因此而带来的风险, 设计一种“图灵完备”的安全脚本智能合约语言也是可以考虑的方案之一.

跨链技术安全: 跨链技术作为增加区块链可拓展性和解决不同公链/侧链之间交易困难问题的核心技术, 愈发被工业级和学术界重视. 现有关于跨链技术的研究大多停留在如何更好的实现跨链交互上, 很少考虑到跨链技术带来的潜在安全威胁. 跨链场景下的攻击模型以及防御方案将是未来的研究方向之一. 未来研究者们可以从区块链传统攻击模型在跨链场景下的新实现以及针对跨链场景的新攻击模型两个方面考虑, 逐步完善跨链技术的安全性.

6 结 语

区块链技术自问世以来, 不断演化发展, 一直作为学术研究、企业应用、政府监管、民间投资的热点和争议而存在. 目前方案成熟、效果明显、应用广泛的区块链应用领域还当属数字货币交易. 由于区块链技术问世较晚、还处于技术的快速迭代完善时期, 其面临的安全风险和威胁攻击多种多样, 针对区块链公链应用的安全事件频繁发生. 本文首先回顾了近几年发生的针对典型的区块链数据服务、交易平台的安全事件; 接着, 列举并分析了区块链自身机制、区块链周边设施、区块链用户所面临的 36 种安全问题, 同时给出了每种安全风险的有效防范策略建议; 最后结合区块链系统层次结构, 对本文提及的安全问题进行分类并做出总结. 希望能给区块链安全的研究者、技术创新应用者、区块链开发者提供研究参考资料和安全评估视野, 促进区块链的健康发展.

References:

[1] Crosby M, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: Beyond Bitcoin. Applied Innovation Review, 2016, 2: 6–19.

[2] Liu AD, Du XH, Wang N, Li SZ. Research progress of blockchain technology and its application in information security. Ruan Jian Xue Bao/Journal of Software, 2018, 29(7): 2092–2115 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[3] Lin IC, Liao TC. A survey of blockchain security issues and challenges. International Journal of Network Security, 2017, 19(5): 653–659. [doi: 10.6633/IJNS.201709.19(5).01]

[4] Gao WC, Hatcher WG, Yu W. A survey of blockchain: Techniques, applications, and challenges. In: Proc. of the 27th Int'l Conf. on Computer Communication and Networks. Hangzhou: IEEE, 2018. 1–11. [doi: 10.1109/ICCCN.2018.8487348]

[5] Destefanis G, Marchesi M, Ortu M, Tonelli R, Bracciali A, Hierons R. Smart contracts vulnerabilities: A call for blockchain software engineering? In: Proc. of 2018 Int'l Workshop on Blockchain Oriented Software Engineering. Campobasso: IEEE, 2018. 19–25. [doi: 10.1109/IWBOSE.2018.8327567]

[6] Huang YH, Wang HY, Wu L, Tyson G, Luo XP, Zhang R, Liu XZ, Huang G, Jiang XX. Characterizing eosio blockchain. arXiv: 2002.05369, 2020.

[7] Mehar MI, Shier CL, Giambattista A, Gong E, Fletcher G, Sanayhie R, Kim HM, Laskowski M. Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. Journal of Cases on Information Technology (JCIT), 2019, 21(1): 19–32. [doi: 10.4018/JCIT.2019010102]

[8] Zou J, Zhang HN, Tang Y, Li L, Liu TX, Chen H. Blockchain Technical Guidelines. Beijing: China Machine Press, 2016. 109–219 (in Chinese).

[9] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin White Paper, 2008.

[10] Tomov YK. Bitcoin: Evolution of blockchain technology. In: Proc. of the 2019 IEEE XXVIII Int'l Scientific Conf. Electronics. Sozopol: IEEE, 2019. 1–4. [doi: 10.1109/ET.2019.8878322]

[11] Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA, Felten EW. Sok: Research perspectives and challenges for Bitcoin and cryptocurrencies. In: Proc. of the 2015 IEEE Symp. on Security and Privacy. San Jose: IEEE, 2015. 104–121. [doi: 10.1109/SP.2015.14]

[12] Shalini S, Santhi H. A survey on various attacks in Bitcoin and cryptocurrency. In: Proc. of the 2019 Int'l Conf. on Communication and Signal Processing. Chennai: IEEE, 2019. 220–224. [doi: 10.1109/ICCSP.2019.8697996]

[13] Jang J, Lee HN. Profitable double-spending attacks. Applied Sciences, 2020, 10(23): 8477. [doi: 10.3390/app10238477]

[14] Pérez-Solà C, Delgado-Segura S, Navarro-Arribas G, Herrera-Joancomartí J. Double-spending prevention for Bitcoin zero-confirmation Trans.. Int'l Journal of Information Security, 2019, 18(4): 451–463. [doi: 10.1007/s10207-018-0422-4]

[15] Rosenfeld M. Analysis of hashrate-based double spending. arXiv: 1402.2009, 2014.

[16] Houy N. It will cost you nothing to 'kill' a proof-of-stake crypto-currency. Economics Bulletin, 2014, 34(2): 1038–1044. [doi: 10.2139/ssrn.2393940]

[17] Shanaev S, Shuraeva A, Vasenin M, Kuznetsov M. Cryptocurrency value and 51% attacks: Evidence from event studies. The Journal of Alternative Investments, 2019, 22(3): 65–77. [doi: 10.2139/ssrn.3290016]

[18] Liu ZY, Luong NC, Wang WB, Niyato D, Wang P, Liang YC, Kim DI. A survey on blockchain: A game theoretical perspective. IEEE Access, 2019, 7: 47615–47643. [doi: 10.1109/ACCESS.2019.2909924]

[19] Yang XL, Chen Y, Chen XH. Effective scheme against 51% attack on proof-of-work blockchain with history weighted information. In: Proc. of 2019 IEEE Int'l Conf. on Blockchain. Atlanta: IEEE, 2019. 261–265. [doi: 10.1109/Blockchain.2019.00041]

[20] Li XQ, Jiang P, Chen T, Luo XP, Wen QY. A survey on the security of blockchain systems. Future Generation Computer Systems, 2020, 107: 841–853. [doi: 10.1016/j.future.2017.08.020]

[21] Bentov I, Gabizon A, Mizrahi A. Cryptocurrencies without proof of work. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Christ Church: Springer, 2016. 142–157. [doi: 10.1007/978-3-662-53357-4_10]

[22] Bonneau J. Why buy when you can rent? In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Christ Church: Springer, 2016. 19–26. [doi: 10.1007/978-3-662-53357-4_2]

[23] Gao S, Li ZC, Peng Z, Xiao B. Power adjusting and bribery racing: Novel mining attacks in the Bitcoin system. In: Proc. of the 2019 ACM SIGSAC Conf. on Computer and Communications Security. London: ACM, 2019. 833–850. [doi: 10.1145/3319535.3354203]

[24] Kothapalli A, Cordi C. 2016. A bribery framework using smartcontracts.

[25] Vasin P. Blackcoin's Proof-of-Stake Protocol v2. 2014. https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[26] Averin A, Averina O. Review of blockchain technology vulnerabilities and blockchain-System attacks. In: Proc. of 2019 Int'l Multi-Conf. on Industrial Engineering and Modern Technologies. Vladivostok: IEEE, 2019. 1–6. [doi: 10.1109/FarEastCon.2019.8934243]

[27] Niya SR, Stiller B. BAZO: A proof-of-stake (PoS) based blockchain. Technical Report, Zurich: University of Zurich, 2019.

[28] Bachmann S. Proof of stake for Bazo [Bachelor Thesis]. Zurich: University of Zurich, 2018.

[29] Shrivas MK, Dean TY, Brunda SS. The disruptive blockchain security threats and threat categorization. In: Proc. of the 1st Int'l Conf. on Power, Control and Computing Technologies. Raipur: IEEE, 2020. 327–338.[doi: 10.1109/ICPC2T48082.2020.9071475]

[30] Georgiadis E, Zeilberger D. A combinatorial-probabilistic analysis of Bitcoin attacks. Journal of Difference Equations and Applications, 2019, 25(1): 56–63. [doi: 10.1080/10236198.2018.1555247]

[31] Grunspan C, Pérez-Marco R. On profitability of Nakamoto double spend. Probability in the Engineering and Informational Sciences, 2021: 1–15. [doi: 10.1017/S026996482100005X]

[32] Kaushik A, Choudhary A, Ektare C, Thomas D, Akram S. Blockchain—literature survey. In: Proc. of the 2nd IEEE Int'l Conf. on

Recent Trends in Electronics, Information & Communication Technology. Bangalore: IEEE, 2017. 2145–2148.[doi: 10.1109/RTEICT.2017.8256979]

[33] Joshi J, Mathew R. A survey on attacks of bitcoin. In: Proc. of the Int'l Conf. on Computer Networks, Big data and IoT. Cham: Springer, 2018. 953–959. [doi: 10.1007/978-3-030-24643-3_113]

[34] Lei M. Exploiting Bitcoin's topology for double-spend attacks [Bachelor Thesis]. Zürich: ETH Zürich, 2015.

[35] Maroufi M, Abdolee R, Tazekand BM. On the convergence of blockchain and Internet of Things (IoT) technologies. arXiv: 1904.01936, 2019.

[36] Bajaj AS, Tyagi L, Arora P. Blockchain and decentralized applications. BTP Report, New Delhi: Indraprastha Institute of Information Technology, 2018.

[37] Ekparinya P, Gramoli V, Jourjon G. Double-spending risk quantification in private, consortium and public Ethereum blockchains. arXiv: 1805.05004, 2018.

[38] Nguyen TSL, Jourjon G, Potop-Butucaru M, Thai KL. Impact of network delays on Hyperledger Fabric. In: Proc. of the IEEE INFOCOM 2019-IEEE Conf. on Computer Communications Workshops. Paris: IEEE, 2019. 222–227. [doi: 10.1109/INFCOMW.2019.8845168]

[39] Saad M, Cook V, Nguyen L, Thai MT, Mohaisen A. Partitioning attacks on Bitcoin: Colliding space, time, and logic. In: Proc. of 2019 IEEE 39th Int'l Conf on Distributed Computing Systems. Dallas: IEEE, 2019. 1175–1187. [doi: 10.1109/ICDCS.2019.00119]

[40] Tran M, Choi I, Moon GJ, Vu AV, Kang MS. A stealthier partitioning attack against Bitcoin peer-to-peer network. In: Proc. of the 2020 IEEE Symp. on Security and Privacy. San Francisco: IEEE, 2020. 496–511. [doi: 10.1109/SP40000.2020.00027]

[41] Apostolaki M, Zohar A, Vanbever L. Hijacking Bitcoin: Routing attacks on cryptocurrencies. In: Proc. of the 2017 IEEE Symp. on Security and Privacy. San Jose: IEEE, 2017. 375–392.[doi: 10.1109/SP.2017.29]

[42] Wang J, Chen GL. Overview on blockchain fork in bitcoin. Communications Technology, 2018, 51(1): 149−155 (in Chinese with English abstract). [doi: 10.3969/j.issn.1002-0802.2018.01.027]

[43] Dasgupta D, Shrein JM, Gupta KD. A survey of blockchain from security perspective. Journal of Banking and Financial Technology, 2019, 3(1): 1–17. [doi: 10.1007/s42786-018-00002-6]

[44] McCorry P, Heilman E, Miller A. Atomically trading with roger: Gambling on the success of a hardfork. In: Garcia-Alfaro J, Navarro-Arribas G, Hartenstein H, Herrera-Joancomartí J, eds. Data Privacy Management, Cryptocurrencies and Blockchain Technology. Cham: Springer, 2017. 334–353. [doi: 10.1007/978-3-319-67816-0_19]

[45] Eyal I, Gencer AE, Sirer EG, Van Renesse R. Bitcoin-NG: A scalable blockchain protocol. In: Proc. of the 13th USENIX Symp. on Networked Systems Design and Implementation. Berkeley: USENIX, 2016. 45–59.

[46] Eskandari S, Moosavi S, Clark J. SoK: Transparent dishonesty: Front-running attacks on blockchain. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Cham: Springer, 2019. 170–189. [doi: 10.1007/978-3-030-43725-1_13]

[47] Sina A. Investigating the Bitcoin blockchain through the analysis of empty blocks [MS. Thesis]. Venice: Università Ca'Foscari Venezia, 2019.

[48] Zhou DL, Ruan N, Jia WJ. A robust throughput scheme for Bitcoin network without block reward. In: Proc. of the 21st IEEE Int'l Conf. on High Performance Computing and Communications; the 17th IEEE Int'l Conf. on Smart City; the 5th IEEE Int'l Conf. on Data Science and Systems. Zhangjiajie: IEEE, 2019. 706–713. [doi: 10.1109/HPCC/SmartCity/DSS.2019.00105]

[49] Mannan GS. Security of blockchain: An investigation and analysis of mining attacks on Bitcoin [MS. Thesis]. Edgbaston: University of Birmingham, 2017.

[50] Nguyen CT, Hoang DT, Nguyen DN, Niyato D, Nguyen HT, Dutkiewicz E. Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. IEEE Access, 2019, 7: 85727–85745. [doi: 10.1109/ACCESS.2019.2925010]

[51] Saleh F. Blockchain without waste: Proof-of-stake. Review of Financial Studies, 2021, 34: 1156–1190. [doi: 10.2139/ssrn.3183935]

[52] Gupta S, Sadoghi M. Blockchain transaction processing. In: Sakr S, Zomaya A, eds. Encyclopedia of Big Data Technologies. Cham: Springer, 2019. [doi: 10.1007/978-3-319-63962-8_333-1]

[53] Daian P, Pass R, Shi E. Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake. In: Proc. of the 23rd Int'l Conf. on Financial Cryptography and Data Security. Cham: Springer, 2019. 23–41. [doi: 10.1007/978-3-030-32101-7_2]

[54] Baliga A. Understanding blockchain consensus models. Persistent Systems, 2017, 2017(4): 1–14.

[55] Jain A, Arora S, Shukla Y, Patil T, Sawant-Patil S. Proof of stake with casper the friendly finality gadget protocol for fair validation consensus in Ethereum. Int'l Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2018, 3(3): 291–298.

[56] Cohen B, Pietrzak K. The Chia network blockchain. Chia Network White Paper, 2019.

[57] Fanti G, Kogan L, Oh S, Ruan K, Viswanath P, Wang GR. Compounding of wealth in proof-of-stake cryptocurrencies. In: Proc. of the 23rd Int'l Conf. on Financial Cryptography and Data Security. Cham: Springer, 2019. 42–61. [doi: 10.1007/978-3-030-32101-7_3]

[58] Sayeed S, Marco-Gisbert H. Assessing blockchain consensus and security mechanisms against the 51% attack. Applied Sciences, 2019, 9(9): 1788. [doi: 10.3390/app9091788]

[59] Roelen E, Modeneis T. A Technical Description of the Smilo Platform. Rotterdam, Netherlands: Smilo Foundation, 2019.

[60] Deirmentzoglou E, Papakyriakopoulos G, Patsakis C. A survey on long-range attacks for proof of stake protocols. IEEE Access, 2019, 7: 28712–28725. [doi: 10.1109/ACCESS.2019.2901858]

[61] AlMallohi IAI, Alotaibi ASM, Alghafees R, Azam F, Khan ZS. Multivariable based checkpoints to mitigate the long range attack in proof-of-stake based blockchains. In: Proc. of the 3rd Int'l Conf. on High Performance Compilation, Computing and Communications. Xi'an: ACM, 2019. 118–122. [doi: 10.1145/3318265.3318289]

[62] Zhang S, Lee JH. Eclipse-based stake-bleeding attacks in PoS blockchain systems. In: Proc. of the 2019 ACM Int'l Symp. on Blockchain and Secure Critical Infrastructure. Auckland: ACM, 2019. 67–72. [doi: 10.1145/3327960.3332391]

[63] Homoliak I, Venugopalan S, Hum Q, Szalachowski P. A security reference architecture for blockchains. In: Proc. of the 2019 IEEE Int'l Conf. on Blockchain. Atlanta: IEEE, 2019. 390–397. [doi: 10.1109/Blockchain.2019.00060]

[64] Saad M, Njilla L, Kamhoua C, Kim J, Nyang D, Mohaisen A. Mempool optimization for defending against DDoS attacks in PoW-based blockchain systems. In: Proc. of the 2019 IEEE Int'l Conf. on Blockchain and Cryptocurrency. Seoul: IEEE, 2019. 285–292. [doi: 10.1109/BLOC.2019.8751476]

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

[66] Bradbury D. The problem with Bitcoin. Computer Fraud & Security, 2013, 2013(11): 5–8. [doi: 10.1016/S1361-3723(13)70101-5]

[67] Douceur JR. The Sybil attack. In: Proc. of the 1st Int'l Workshop on Peer-to-Peer Systems. Cambridge: Springer, 2002. 251–260. [doi: 10.1007/3-540-45748-8_24]

[68] Dinger J, Hartenstein H. Defending the Sybil attack in P2P networks: Taxonomy, challenges, and a proposal for self-registration. In: Proc. of the 1st Int'l Conf. on Availability, Reliability and Security. Vienna: IEEE, 2006. 756–763. [doi: 10.1109/ARES.2006.45]

[69] Swathi P, Modi C, Patel D. Preventing Sybil attack in blockchain using distributed behavior monitoring of miners. In: Proc. of the 10th Int'l Conf. on Computing, Communication and Networking Technologies. Kanpur: IEEE, 2019. 1–6. [doi: 10.1109/ICCCNT45670.2019.8944507]

[70] Rahmadika S, Ramdania DR, Harika M. A blockchain approach for the future renewable energy transaction. Journal of Physics: Conf. Series, 2019, 1175(1): 012122. [doi: 10.1088/1742-6596/1175/1/012122]

[71] Wüst K, Gervais A. Ethereum eclipse attacks. ETH Zurich, 2016.

[72] Wang SL, Wang CY, Hu Q. Corking by forking: Vulnerability analysis of blockchain. In: Proc. of the IEEE INFOCOM 2019-IEEE Conf. on Computer Communications. Paris: IEEE, 2019. 829–837. [doi: 10.1109/INFOCOM.2019.8737490]

[73] Aoki Y, Shudo K. Proximity neighbor selection in blockchain networks. In: Proc. of the 2019 IEEE Int'l Conf. on Blockchain. Atlanta: IEEE, 2019. 52–58. [doi: 10.1109/Blockchain.2019.00016]

[74] Heilman E, Kendler A, Zohar A, Goldberg S. Eclipse attacks on Bitcoin's peer-to-peer network. In: Proc. of the 24th USENIX Security Symp. Washington: USENIX, 2015. 129–144.

[75] Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S. On the security and performance of proof of work blockchains. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. Vienna: ACM, 2016. 3–16. [doi: 10.1145/2976749.2978341]

[76] Wang K, Kim HS. FastChain: Scaling blockchain system with informed neighbor selection. In: Proc. of 2019 IEEE Int'l Conf. on Blockchain. Atlanta: IEEE, 2019. 376–383. [doi: 10.1109/Blockchain.2019.00058]

[77] Ajayi O, Cherian M, Saadawi T. Secured cyber-attack signatures distribution using blockchain technology. In: Proc. of 2019 IEEE Int'l Conf. on Computational Science and Engineering (CSE) and IEEE Int'l Conf. on Embedded and Ubiquitous Computing (EUC). New York: IEEE, 2019. 482–488. [doi: 10.1109/CSE/EUC.2019.00095]

[78] Qian WN, Shao QF, Zhu YC, Jin CQ, Zhou AY. Research problems and methods in blockchain and trusted data management. Ruan Jian Xue Bao/Journal of Software, 2018, 29(1): 150–159 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5434.htm [doi: 10.13328/j.cnki.jos.005434]

[79] Canessane RA, Srinivasan N, Beuria A, Singh A, Kumar BM. Decentralised applications using Ethereum blockchain. In: Proc. of the 5th Int'l Conf. on Science Technology Engineering and Mathematics. Chennai: IEEE, 2019. 14–15. [doi: 10.1109/ICONSTEM.2019.8918887]

[80] Buterin V. A next-generation smart contract and decentralized application platform. Ethereum White Paper, 2014, 3(37): 1–36.
[81] Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014, 151: 1–32.
[82] Vujičić D, Jagodić D, Ranđić S. Blockchain technology, Bitcoin, and Ethereum: A brief overview. In: Proc. of the 17th Int'l Symp. INFOTEH-JAHORINA. East Sarajevo: IEEE, 2018. 1–6. [doi: 10.1109/INFOTEH.2018.8345547]
[83] Wei PW, Yuan Q, Zheng YL. Security of the blockchain against long delay attack. In: Proc. of the 24th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Brisbane: Springer, 2018. 250–275. [doi: 10.1007/978-3-030-03332-3_10]
[84] Gramoli V. From blockchain consensus back to byzantine consensus. Future Generation Computer Systems, 2020, 107: 760–769. [doi: 10.1016/j.future.2017.09.023]
[85] Natoli C, Gramoli V. The balance attack against proof-of-work blockchains: The R3 testbed as an example. arXiv: 1612.09426, 2016.
[86] Natoli C, Gramoli V. The balance attack or why forkable blockchains are ill-suited for consortium. In: Proc. of the 47th Annual IEEE/IFIP Int'l Conf. on Dependable Systems and Networks. Denver: IEEE, 2017. 579–590. [doi: 10.1109/DSN.2017.44]
[87] Gupta BC. Analysis of Ethereum smart contracts-A security perspective [MS. Thesis]. Kanpur: Indian Institute of Technology Kanpur, 2019.
[88] Grech N, Kong M, Jurisevic A, Brent L, Scholz B, Smaragdakis Y. MadMax: Surviving out-of-gas conditions in Ethereum smart contracts. Proc. of the ACM on Programming Languages, 2018, 2(OOPSLA): 116. [doi: 10.1145/3276486]
[89] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on Ethereum smart contracts (SOK). In: Proc. of the 6th Int'l Conf. on Principles of Security and Trust. Uppsala: Springer, 2017. 164–186. [doi: 10.1007/978-3-662-54455-6_8]
[90] Luu L, Chu DH, Olickel H, Saxena P, Hobor A. Making smart contracts smarter. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. Vienna: ACM, 2016. 254–269. [doi: 10.1145/2976749.2978309]
[91] Wang S, Yuan Y, Wang X, Li JJ, Qin R, Wang FY. An overview of smart contract: Architecture, applications, and future trends. In: Proc. of the 2018 IEEE Intelligent Vehicles Symp. Changshu: IEEE, 2018. 108–113. [doi: 10.1109/IVS.2018.8500488]
[92] Delmolino K, Arnett M, Kosba A, Miller A, Shi E. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In: Proc. of the 2016 Int'l Conf. on Financial Cryptography and Data Security. Berlin: Springer, 2016. 79–94. [doi: 10.1007/978-3-662-53357-4_6]
[93] Decker C, Guthrie J, Seidel J, Wattenhofer R. Making Bitcoin exchanges transparent. In: Proc. of the 20th European Symp. on Research in Computer Security. Vienna: Springer, 2015. 561–576. [doi: 10.1007/978-3-319-24177-7_28]
[94] Chuen DLK. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. London: Academic Press, 2015. 5–185. [doi: 10.3905/jwm.2015.18.2.096]
[95] Vasek M, Thornton M, Moore T. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In: Proc. of the 2014 Int'l Conf. on Financial Cryptography and Data Security. Christ Church: Springer, 2014. 57–71. [doi: 10.1007/978-3-662-44774-1_5]
[96] Huynh TT, Nguyen TD, Tan H. A survey on security and privacy issues of blockchain technology. In: Proc. of the 2019 Int'l Conf. on System Science and Engineering. Dong Hoi: IEEE, 2019. 362–367. [doi: 10.1109/ICSSE.2019.8823094]
[97] Feng Q, He DB, Zeadally S, Khan MK, Kumar N. A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, 2019, 126: 45–58. [doi: 10.1016/j.jnca.2018.10.020]
[98] Naoumov N, Ross K. Exploiting P2P systems for DDoS attacks. In: Proc. of the 1st Int'l Conf. on Scalable Information Systems. Hong Kong: ACM, 2006. 47–52. [doi: 10.1145/1146847.1146894]
[99] Moore T. The promise and perils of digital currencies. Int'l Journal of Critical Infrastructure Protection, 2013, 6(3−4): 147–149. [doi: 10.1016/j.ijcip.2013.08.002]
[100] Zhao YL. Practical aggregate signature from general elliptic curves, and applications to blockchain. In: Proc. of the 2019 ACM Asia Conf. on Computer and Communications Security. Auckland: ACM, 2019. 529–538. [doi: 10.1145/3321705.3329826]
[101] Decker C, Wattenhofer R. Bitcoin transaction malleability and MtGox. In: Proc. of the 19th European Symp. on Research in Computer Security. Wroclaw: Springer, 2014. 313–326. [doi: 10.1007/978-3-319-11212-1_18]
[102] Zhao YL. Aggregation of gamma-signatures and applications to Bitcoin. Cryptology ePrint Archive, 2018.
[103] Vyas CA, Lunagaria M. Security concerns and issues for bitcoin. In: IJCA Proc. on National Conf. cum Workshop on Bioinformatics and Computational Biology. 2014. 10–12.
[104] Gennaro R, Goldfeder S, Narayanan A. Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security. In: Proc. of the 14th Int'l Conf. on Applied Cryptography and Network Security. Guildford: Springer, 2016. 156–174. [doi: 10.1007/978-3-319-39555-5_9]
[105] Lewenberg Y, Bachrach Y, Sompolinsky Y, Zohar A, Rosenschein JS. Bitcoin mining pools: A cooperative game theoretic analysis. In: Proc. of the 2015 Int'l Conf. on Autonomous Agents and Multiagent Systems. Istanbul: Int'l Foundation for Autonomous Agents and

Multiagent Systems, 2015. 919–927.
[106] Sapirshtein A, Sompolinsky Y, Zohar A. Optimal selfish mining strategies in Bitcoin. In: Proc. of the 20th Int'l Conf. on Financial Cryptography and Data Security. Christ Church: Springer, 2016. 515–532. [doi: 10.1007/978-3-662-54970-4_30]
[107] Courtois NT, Bahack L. On subversive miner strategies and block withholding attack in Bitcoin digital currency. arXiv: 1402.1718, 2014.
[108] Saad M, Njilla L, Kamhoua C, Mohaisen A. Countering selfish mining in blockchains. In: Proc. of the 2019 Int'l Conf. on Computing, Networking and Communications. Honolulu: IEEE, 2019. 360–364. [doi: 10.1109/ICCNC.2019.8685577]
[109] Grunspan C, Pérez-Marco R. Bitcoin selfish mining and dyck words. arXiv: 1902.01513, 2019.
[110] Bai QL, Zhou XY, Wang X, Xu YD, Wang X, Kong QS. A deep dive into blockchain selfish mining. In: ICC 2019–2019 IEEE Int'l Conf. on Communications. Shanghai: IEEE, 2019. 1–6. [doi: 10.1109/ICC.2019.8761240]
[111] Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. In: Proc. of the 18th Int'l Conf. on Financial Cryptography and Data Security. Christ Church: Springer, 2014. 436–454. [doi: 10.1007/978-3-662-45472-5_28]
[112] Qin R, Yuan Y, Wang S, Wang FY. Economic issues in Bitcoin mining and blockchain research. In: Proc. of the 2018 IEEE Intelligent Vehicles Symp. (IV). Changshu: IEEE, 2018. 268–273. [doi: 10.1109/IVS.2018.8500377]
[113] Liu KY, Ohsawa Y. Auction based rewards distribution method in pool mining. In: Proc. of the 2019 Int'l Electronics Communication Conf.. Okinawa: ACM, 2019. 103–110. [doi: 10.1145/3343147.3343162]
[114] Singh SK, Salim MM, Cho M, Cha J, Pan Y, Park JH. Smart contract-based pool hopping attack prevention for blockchain networks. Symmetry, 2019, 11(7): 941. [doi: 10.3390/sym11070941]
[115] Shi HW, Wang SL, Hu Q, Cheng XZ, Zhang JS, Yu JG. Hopping-proof and fee-free pooled mining in blockchain. arXiv: 1912.11575, 2019.
[116] 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. [doi: 10.1109/TIFS.2016.2623588]
[117] Chang SY, Park Y, Wuthier S, Chen CW. Uncle-block attack: Blockchain mining threat beyond block withholding for rational and uncooperative miners. In: Proc. of the 17th Int'l Conf. on Applied Cryptography and Network Security. Bogota: Springer, 2019. 241–258. [doi: 10.1007/978-3-030-21568-2_12]
[118] Vokerla RR, Shanmugam B, Azam S, Karim A, De Boer F, Jonkman M, Faisal F. An overview of blockchain applications and attacks. In: Proc. of the 2019 Int'l Conf. on Vision Towards Emerging Trends in Communication and Networking. Vellore: IEEE, 2019. 1–6. [doi: 10.1109/ViTECoN.2019.8899450]
[119] Rosenfeld M. Analysis of Bitcoin pooled mining reward systems. arXiv: 1112.4980, 2011.
[120] Barber S, Boyen X, Shi E, Uzun E. Bitter to better—How to make Bitcoin a better currency. In: Proc. of the 16th Int'l Conf. on Financial Cryptography and Data Security. Kralendijk: Springer, 2012. 399–414. [doi: 10.1007/978-3-642-32946-3_29]
[121] Canelón J, Huerta E, Incera J, Ryan T. A cybersecurity control framework for blockchain ecosystems. The Int'l Journal of Digital Accounting Research, 2019, 19: 103–144. [doi: 10.4192/1577-8517-v19_5]
[122] Stephen R, Alex A. A review on blockchain security. IOP Conference Series: Materials Science and Engineering, 2018, 396: 012030. [doi: 10.1088/1757-899X/396/1/012030]
[123] Herbert J, Litchfield A. A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology. In: Proc. of the 38th Australasian Computer Science Conf. (ACSC 2015). Sydney: CRPIT, 2015. 27–30.
[124] Gangan S. A review of man-in-the-middle attacks. arXiv: 1504.02115, 2015.
[125] Wang KC, Reiter MK. How to end password reuse on the web. In: Network and Distributed Systems Security. San Diego: NDSS, 2019.
[126] Glazier W, Dhiman M. Automation attacks at scale-credential exploitation. 2017.
[127] Yuan Y, Wang FY. Blockchain and cryptocurrencies: Model, techniques, and applications. IEEE Trans. on Systems, Man, and Cybernetics: Systems, 2018, 48(9): 1421–1428. [doi: 10.1109/TSMC.2018.2854904]
[128] Shahid F, Ahmad I, Imran M, Shoaib M. Novel one time signatures (NOTS): A compact post-quantum digital signature scheme. IEEE Access, 2020, 8: 15895–15906. [doi: 10.1109/ACCESS.2020.2966259]
[129] Wan ZG, Guan ZS, Zhou Y, Ren K. zk-AuthFeed: How to feed authenticated data into smart contract with zero knowledge. In: Proc. of the 2019 IEEE Int'l Conf. on Blockchain. Atlanta: IEEE, 2019. 83–90. [doi: 10.1109/Blockchain.2019.00020]
[130] Harris CG. Consensus-based secret sharing in blockchain smart contracts. In: Proc. of the 2019 Int'l Workshop on Big Data and Information Security. Bali: IEEE, 2019. 79–84. [doi: 10.1109/IWBIS.2019.8935853]
[131] Signorini M, Pontecorvi M, Kanoun W, Di Pietro R. ADvISE: Anomaly detection tool for blockchain systEms. In: Proc. of the 2018 IEEE World Congress on Services. San Francisco: IEEE, 2018. 65–66. [doi: 10.1109/SERVICES.2018.00046]

[132] Sai K, Tipper D. Disincentivizing double spend attacks across interoperable blockchains. In: Proc. of the 1st IEEE Int'l Conf. on Trust, Privacy and Security in Intelligent Systems and Applications. Los Angeles: IEEE, 2019. 36–45. [doi: 10.1109/TPS-ISA48467.2019.00014]

[133] Zhang SJ, Lee JH. Mitigations on sybil-based double-spend attacks in Bitcoin. IEEE Consumer Electronics Magazine, 2020. [doi: 10.1109/MCE.2020.2988031]

[134] Zolotavkin Y, Garcia J. Incentives for stable mining in pay per last N shares pools. In: Proc. of the 2019 IFIP Networking Conf. (IFIP Networking). Warsaw: IEEE, 2019. 1–9. [doi: 10.23919/IFIPNetworking.2019.8816835]

[135] Qin R, Yuan Y, Wang FY. Optimal block withholding strategies for blockchain mining pools. IEEE Trans. on Computational Social Systems, 2020, 7(3): 709–717. [doi: 10.1109/TCSS.2020.2991097]

[136] Kaci A, Rachedi A. PoolCoin: Toward a distributed trust model for miners' reputation management in blockchain. In: Proc. of the 17th IEEE Annual Consumer Communications & Networking Conf. (CCNC). Las Vegas: IEEE, 2020. 1–6. [doi: 10.1109/CCNC46108.2020.9045608]

[137] Gao ZP, Jiang LX, Xia X, Lo D, Grundy J. Checking smart contracts with structural code embedding. IEEE Trans. on Software Engineering, 2020. [doi: 10.1109/TSE.2020.2971482]

[138] Wang W, Song JJ, Xu GQ, Li YD, Wang H, Su CH. ContractWard: Automated vulnerability detection models for Ethereum smart contracts. IEEE Trans. on Network Science and Engineering, 2020. [doi: 10.1109/TNSE.2020.2968505]

[139] Samreen NF, Alalfi MH. Reentrancy vulnerability identification in Ethereum smart contracts. In: Proc. of the 2020 IEEE Int'l Workshop on Blockchain Oriented Software Engineering. London: IEEE, 2020. 22–29. [doi: 10.1109/IWBOSE50093.2020.9050260]

[140] Zhang YY, Ma SQ, Li JR, Li KL, Nepal S, Gu DW. SMARTSHIELD: Automatic smart contract protection made easy. In: Proc. of the 27th IEEE Int'l Conf. on Software Analysis, Evolution and Reengineering. London: IEEE, 2020. 23–34.[doi: 10.1109/SANER48275.2020.9054825]

[141] Wu Y, Tao F, Liu L, Gu JY, Panneerselvam J, Zhu RB, Shahzad MN. A Bitcoin transaction network analytic method for future blockchain forensic investigation. IEEE Trans. on Network Science and Engineering, 2020. [doi: 10.1109/TNSE.2020.2970113]

附中文参考文献:

[2] 刘敖迪, 杜学绘, 王娜, 李少卓. 区块链技术及其在信息安全领域的研究进展. 软件学报, 2018, 29(7): 2092–2115. http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[8] 邹均, 张海宁, 唐屹, 李磊, 刘天喜, 陈晖. 区块链技术指南. 北京: 机械工业出版社, 2016. 109–219.

[42] 王健, 陈恭亮. 比特币区块链分叉研究. 通信技术, 2018, 51(1): 149–155. [doi: 10.3969/j.issn.1002-0802.2018.01.027]

[78] 钱卫宁, 邵奇峰, 朱燕超, 金澈清, 周傲英. 区块链与可信数据管理: 问题与方法. 软件学报, 2018, 29(1): 150–159. http://www.jos.org.cn/1000-9825/5434.htm [doi: 10.13328/j.cnki.jos.005434]

魏松杰(1977－), 男, 博士, 副教授, CCF 高级会员, 主要研究领域为网络安全, 区块链技术.

李莎莎(1997－), 女, 硕士, 主要研究领域为分布式系统, 任务调度.

吕伟龙(1996－), 男, 硕士, CCF 学生会员, 主要研究领域为区块链技术, 密码学, 网络安全.