计算机科学与探索
Journal of Frontiers of Computer Science and Technology
1673-9418/2025/19(10)-2559-28
doi: 10.3778/j.issn.1673-9418.2411013

# 区块链恶意交易的层次化研究综述

李嘉乐[1,2],李雷孝[1,2,3+],林　浩[4],杜金泽[4],史建平[5],刘哲旭[1,2]
1. 内蒙古工业大学 数据科学与应用学院,呼和浩特 010080
2. 内蒙古自治区北疆网络空间安全重点实验室,呼和浩特 010080
3. 内蒙古自治区基于大数据的软件服务工程技术研究中心,呼和浩特 010080
4. 天津理工大学 计算机科学与工程学院,天津 300384
5. 鄂尔多斯市市民卡建设有限公司,内蒙古 鄂尔多斯 017099
+ 通信作者 E-mail: llxhappy@126.com

**摘　要:**区块链技术虽在去中心化与安全性上具有显著优势,但其分层架构中潜藏的恶意交易威胁日益复杂化,现有研究多聚焦单一层次的安全分析,缺乏对跨层攻击传导机制的系统性探索。提出包括基础协议层、基础链层、扩展解决方案层、应用层的层次化恶意交易分析框架,深入分析了区块链技术中恶意交易的层次化问题,完整地总结了现有恶意攻击的检测与抵御方法研究进展。对上述四层中的恶意攻击进行综述分析,概述了35种恶意攻击类型的定义及攻击形式,各层级攻击间存在显著的传导效应,协议层的密钥泄露可使应用层的DeFi协议损失扩大数倍;分别介绍了各类攻击的检测方法以及抵御方法,并总结了可以用于抵御该类攻击的相关技术;分析了区块链各层中现存的安全问题,后量子密码学算法在区块链设备中的高功耗问题、确认延迟和低区块出块速度、代理合约模式的复杂性与安全隐患问题和Rollups的状态增长隐患问题,据此提出未来研究的四个方向,后量子密码学的低功耗设计、动态块时间和自适应出块速度、增强代理合约模式的安全性与效率和Verkle树的无状态客户端恒定大小证明方案。

**关键词:**区块链;安全;攻击;漏洞检测
**文献标志码:**A　**中图分类号:**TP309.2

# Review of Hierarchical Research on Malicious Transactions in Blockchain

LI Jiale[1,2], LI Leixiao[1,2,3+], LIN Hao[4], DU Jinze[4], SHI Jianping[5], LIU Zhexu[1,2]
1. College of Data Science and Application, Inner Mongolia University of Technology, Hohhot 010080, China
2. Inner Mongolia Key Laboratory of Beijiang Cyberspace Security, Hohhot 010080, China
3. Inner Mongolia Autonomous Region Software Service Engineering Technology Research Center Based on Big Data, Hohhot 010080, China

**基金项目:**国家自然科学基金(62362055);内蒙古自治区重点研发与成果转化计划项目(2022YFSJ0013,2023YFHH0052);内蒙古自治区高等学校青年科技英才支持计划项目(NJYT22084,NJYT24035);内蒙古自然科学基金(2023MS06008);内蒙古自治区科技成果转化专项资金项目(2020CG0073,2021CG0033);内蒙古自治区直属高校科研项目(JY20220061,JY20230119,JY20230019);鄂尔多斯市重点研发计划(YF20232328);国家重点研发计划(2023YFB2703900)。
This work was supported by the National Natural Science Foundation of China (62362055), the Key Research and Development and Achievement Transformation Programme Projects of Inner Mongolia Autonomous Region (2022YFSJ0013, 2023YFHH0052), the Support Programme for Young Scientific and Technological Talents in Higher Education Institutions in Inner Mongolia Autonomous Region (NJYT22084, NJYT24035), the Natural Science Foundation of Inner Mongolia (2023MS06008), the Special Funds for Transformation of Scientific and Technological Achievements in Inner Mongolia Autonomous Region (2020CG0073, 2021CG0033), the Research Projects of Universities Directly under the Inner Mongolia Autonomous Region (JY20220061, JY20230119, JY20230019), the Ordos Key Research and Development Program Project (YF20232328), and the National Key Research and Development Program of China (2023YFB2703900).
**收稿日期:**2024-11-04　**修回日期:**2025-02-26

中国知网 https://www.cnki.net

4. College of Computer Science and Engineering, Tianjin University of Technology, Tianjin 300384, China
5. Ordos Citizen Card Construction Co., Ltd., Ordos, Inner Mongolia 017099, China

**Abstract:** Although blockchain technology has significant advantages in decentralization and security, the threat of malicious transactions latent in its layered architecture is increasingly complex, and the existing research mostly focuses on the security analysis of a single layer and lacks the systematic exploration of cross-layer attack conduction mechanism. A hierarchical malicious transaction analysis framework including the basic protocol layer, the basic chain layer, the extended solution layer, and the application layer is proposed, which deeply analyzes the hierarchical problem of malicious transactions in blockchain technology, and completely summarizes the research progress of the existing methods for detecting and defending against malicious attacks. Firstly, the malicious attacks in the above four layers are reviewed and analyzed, and the definitions and attack forms of 35 types of malicious attacks are outlined; there is a significant conduction effect between the attacks in each layer, and the key leakage in the protocol layer can expand the loss of the DeFi protocol in the application layer by several times. Secondly, the detection methods of each type of attack as well as the defense methods are introduced respectively, and the relevant technologies that can be used to defend against this type of attack are summarized. Finally, the existing security problems in each layer of the blockchain are analyzed: high power consumption of post-quantum cryptography algorithms in blockchain devices, confirmation delays and low block exit speeds, complexity and security risks of the proxy contract model, and the state growth risks of Rollups. According to this, four directions are proposed for future research: low-power design of post-quantum cryptography, dynamic block time and adaptive block exit speeds, enhancing the security and efficiency of the proxy contract model and Verkle tree constant size proof scheme for stateless clients.
**Key words:** blockchain; security; attacks; vulnerability detection

在进入数字化时代，区块链技术以其独特的去中心化和安全性，成为了金融、供应链管理、医疗等多个领域的核心技术。然而，随着区块链技术的广泛应用，恶意交易行为也日益增多，对区块链系统的安全构成了严重威胁。区块链技术在实际应用中存在技术实施缺陷、预言机风险、智能合约的不可逆性及去中心化风险等问题，导致恶意攻击者可以通过51%攻击、女巫攻击、重入攻击等手段威胁到区块链用户的资产安全，也破坏了区块链系统的信誉。随着区块链技术的不断发展，恶意攻击手段也在不断演变，呈现出更加复杂和隐蔽的特点。

针对区块链技术存在的问题，目前已有诸多相关技术研究进展的总结与分析工作，Saad等人[1]探讨分析了区块链中的各种攻击方式，展示了不同攻击是如何相互联系的，如一个成功的自私挖矿可能会导致区块链分叉，而一个成功的51%攻击能够使攻击者实现双花。Lin等人[2]侧重于对区块链结构、共识机制相关概念的讨论，对公有链、联盟链和私有链进行了区分和描述，讨论了它们的特点和适用场景。Conti等人[3]重点关注区块链的安全和隐私问题，而忽视了提到智能合约的安全问题。Zaghloul等人[4]侧重于比特币的安全和隐私问题而比特币只是区块链生态中的一小部分。Aggarwal等人[5]侧重于从攻击类型的角度对区块链的安全问题进行分类，重点讨论每种攻击类型的特点、原理以及可能的影响。与之相比，Wen等人[6]提供一个系统的视角来审视区块链的安全问题，从数据层、网络层、共识与激励层、合约层和应用层多个层面进行分析，并探讨了针对这些层面的攻击手段和防御策略。根据区块链技术架构的层次性展开的研究能够更清晰地揭示不同层次上的安全问题和攻击手段。这种方法有助于深入理解区块链系统的内在安全机制，并明确如何在不同层面上实施有效的防御策略。此外，区块链的层次化分析也有助于发现区块链中跨层次的安全问题，为构建更为全面的区块链安全防护体系提供理论支持。

本文以区块链四层架构为主体，如图1所示即Layer 0基础协议层、Layer 1基础链层、Layer 2扩展解决方案层和Layer 3应用层，与六层架构相比，两者差异主要体现在架构的简化、扩展性和技术适用性上。四层架构的优势在于它将复杂性更清晰地分层，使得每一层的职责更加明确，从而简化了理解和开发流程。如四层架构中的Layer 2专注于在基础链层（Layer 1）的基础上实现扩展性，解决链上交易处理速度慢、交易费用高等问题。相比之下，六层架构中没有直接体现Layer 2的概念，而是将扩展性与其他功能层（如网络层、共识层）混合在一起。这样做虽然更加细致，但会导致各个层之间的耦合性较强，使得开发者在优化扩展性时需要同时处理底层的共识机制和网络问题，增加了技术实现的复杂性。从

中国知网 https://www.cnki.net

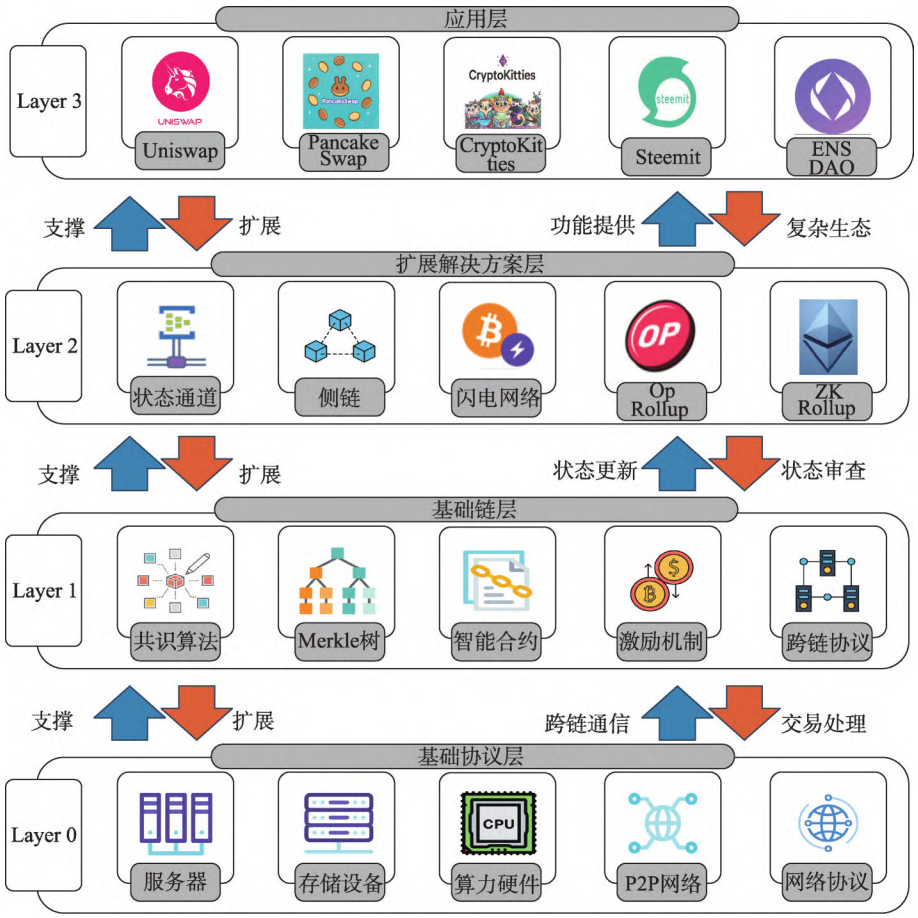


**图1 区块链四层架构图**

Fig.1 Blockchain four-layer architecture diagram

扩展性的角度来看，四层架构更加清晰简洁，减少了层与层之间的耦合性，提高了开发效率，也使得扩展方案可以灵活且快速地部署。

如表1所示，详细列出了区块链四层架构中各层的关键组件，如硬件基础设施、共识机制、智能合约等，以及这些组件在区块链生态中的作用。展示了各部分的研究独立性及其与区块链整体架构的联系，强调了每一部分在实现区块链技术目标中的不可或缺性。并补充了对各层关键技术当前局限性的分析，进一步说明了这些局限性如何导致恶意攻击风险或性能瓶颈，从而突显研究的实践意义与必要性。

## 1 Layer 0基础协议层的恶意交易与攻击

Layer 0作为区块链网络的基础协议层，为整个系统提供了基础支持，包括硬件、网络协议以及通信协议三个部分。

硬件方面，Layer 0依靠服务器、数据中心和网络设备为区块链节点提供运行环境和存储空间，使用固态硬盘(solid-state drive，SSD)和硬盘驱动器(hard disk drive，HDD)存储设备来长期保存区块链数据。

网络协议方面，Layer 0使用传输控制协议/因特网协议(transmission control protocol/Internet protocol，TCP/IP)、边界网关协议(border gateway protocol，BGP)和用户数据报协议(user datagram protocol，UDP)等协议确保节点间通信和数据传输的稳定性。TCP/IP协议确保了节点间通信的连续性[7]，BGP协议优化了网络路由，提高了数据包传输的效率[8]，UDP协议则用于需要快速响应的场景[9]。

通信协议方面，Layer 0采用了点对点网络(peer-to-peer，P2P)和跨链协议。P2P网络允许节点直接通信，维护了网络的去中心化特性。跨链协议则促进了不同区块链网络间的互操作性，允许跨链交易和信息共享。

### 1.1 硬件基础设施上的攻击及相应对策

(1)硬件故障注入

硬件故障注入是指攻击者通过电压波动、时钟干扰、温度变化或物理干预等手段来注入故障，旨在破坏系统功能的行为。电压故障注入通过降低或升高设备的供电电压，导致处理器执行错误的指令或跳过关键指

中国知网 https://www.cnki.net

**表1 区块链架构中各层组件的功能与局限性概述**

Table 1 Overview of functions and limitations of each layer of components in blockchain architecture

| 所在层 | 组件名称 | 组件作用 | 局限性 |
|---|---|---|---|
| Layer 0 | 硬件基础设施 | 硬件基础设施作为区块链系统的物理支撑层，承担着存储、计算和网络通信等关键功能 | 硬件基础设施面临诸多局限性，特别是依赖于集中化的高性能硬件设备、硬件故障、硬件后门等问题，这些都使得区块链网络容易受到攻击 |
| | 网络协议 | 网络协议的主要作用是确保区块链节点之间的通信和数据同步，以保证整个区块链网络的运行、共识以及去中心化性 | 网络协议的局限性主要体现在性能瓶颈、易受DDoS攻击、缺乏隐私保护、节点发现漏洞及可能导致网络分裂和中心化控制，从而增加了被恶意攻击的风险 |
| | 通信协议 | 通信协议是确保去中心化网络中各个节点之间顺畅、可靠和用于新节点能够加入到网络中并同步区块链数据，支持大规模节点的扩展的核心部分 | 通信协议的局限性主要体现在网络带宽和同步性问题、易受日蚀攻击、女巫攻击以及节点发现机制的脆弱性，从而导致区块链容易受到恶意攻击 |
| Layer 1 | 区块链协议 | 区块链协议中的共识机制和数据结构确保了区块链网络的去中心化、安全性和透明性，通过验证交易和区块的合法性、保障数据的不可篡改性，确保区块链网络的稳定运行 | 现有的共识机制和数据结构存在一定局限性，如性能瓶颈、可扩展性问题、能源消耗过大、去中心化度不足等，导致区块链网络面临存储压力和链上数据不可修改性的问题 |
| | 智能合约 | 智能合约是区块链的核心组成部分之一，使区块链能够在去中心化的环境下自动化执行合约条款，避免了中介机构的干预，提升了效率与透明度 | 智能合约存在如漏洞、逻辑设计缺陷、不可更改性、执行成本等问题，这些局限性使得智能合约容易受到攻击或利用，影响区块链的整体安全性和用户信任 |
| | 激励机制 | 激励机制是区块链网络中保证去中心化、安全性和公平性的核心组件。通过奖励节点参与网络的共识和数据验证过程，激励机制促进了网络的安全性、活跃度以及生态系统的长期健康发展 | 激励机制面临着算力集中、资源浪费、去中心化问题、奖励滥用等局限性，这些问题使得区块链容易受到攻击或控制，导致网络的安全性和效率受到威胁 |
| Layer 2 | 状态通道 | 状态通道是Layer 2扩展解决方案中的关键技术之一，旨在提高区块链的交易吞吐量，减少交易延迟，并降低交易成本。通过在链下进行交易，并仅在通道开启和关闭时与区块链进行交互，从而显著提升区块链的扩展性 | 状态通道面临着依赖参与者诚信、资金锁定、链下交易透明性差等局限性，同时多方参与时的复杂性和通道资源的管理问题，也使得其容易受到恶意攻击者的滥用 |
| | 侧链 | 侧链通过提供并行的链上操作和交易处理，显著提升了区块链的可扩展性和交易效率。它使得区块链网络能够支持更多的功能和用例，并允许资产在主链和侧链之间自由流动 | 侧链面临着安全性较弱、去中心化不足、跨链资产转移复杂性等问题，尤其是资产转移过程中容易受到恶意攻击。侧链的技术成熟度和安全性仍然是一个挑战，这使得区块链网络容易受到攻击者的滥用 |
| | Rollups | Rollups通过将计算和交易处理移至链外，并将最终的交易摘要提交到主链，显著提高了区块链的可扩展性和交易吞吐量。能够有效支持智能合约执行，提供高效的去中心化解决方案，并确保与主链的安全性同步 | Rollup面临着依赖于主链的共识和数据完整性、计算复杂性、去中心化程度不完全等问题。这导致Rollups容易受到攻击，造成数据丢失、交易延迟或资产安全问题 |
| Layer 3 | 去中心化金融 | 去中心化金融是基于区块链的一个重要应用层，通过智能合约和去中心化协议提供无需第三方中介的金融服务，增强了金融透明性、安全性、包容性和可接入性 | 去中心化金融面临着智能合约安全漏洞、流动性风险、合规性问题和市场操纵等局限性。这些问题导致平台遭受攻击、资金损失或法律风险，影响其可持续发展 |
| | 去中心化应用 | 去中心化应用部分在整个区块链架构中扮演着关键角色，它们允许开发者构建和部署去中心化应用程序，这些应用程序通过智能合约实现自动化和透明的交易、协议执行以及数据管理 | 当前去中心化应用仍然存在一些局限性，区块链的可扩展性问题限制了去中心化应用在处理大规模数据和用户时的效率。用户体验的复杂性和普及度不足也限制了去中心化应用的广泛应用 |
| | 去中心化自治组织 | 去中心化自治组织是区块链技术的创新应用之一，利用区块链的透明性和不可篡改性，使成员可以通过代币投票等机制实现公平的决策参与，消除传统组织结构中的权力集中问题 | 去中心化自治组织的治理通常依赖代币持有者的投票，但大户持币者可能操纵投票结果，导致权力再次集中。且投票机制可能存在低投票参与率问题，影响决策效率和代表性 |

令。时钟故障注入通过改变设备的时钟频率，干扰处理器的正常操作，诱发错误执行。这种方法可以使处理器在错误的时间点执行指令，导致安全检查被绕过。电磁故障注入通过在芯片附近产生强电磁场，干扰其正常工作。这种方法可以影响芯片的电磁抗扰度，导致其产生错误行为。此攻击方式巧妙地利用了硬件本身的脆弱性，导致系统的计算或存储结果产生误差，从而对系统的可靠性和安全性构成威胁。随着硬件故障注入攻击

中国知网 https://www.cnki.net

的演进，攻击者不仅限于破坏系统功能，逐渐开始针对加密算法等关键操作进行攻击。

硬件钱包在区块链中的主要作用是提供一种安全、可靠且方便的方式来存储和管理用户的私钥，确保数字资产的安全，同时支持多种加密货币和交易签名，以及提供备份和恢复功能。2020年Kraken Security Labs对Trezor和KeepKey硬件钱包进行了实验性攻击，发现两者存在相似的硬件设计缺陷。Kraken通过硬件故障注入，绕过硬件钱包的安全保护机制。在实验中，研究团队仅需15 min就成功提取了私钥，如果硬件钱包的用户未设置密码短语，攻击者可完全获取用户的链上加密资产。该研究强调了硬件钱包的安全漏洞可能危及用户私钥的机密性，从而危害了区块链网络中基于私钥的信任机制。私钥泄露后，攻击者可以篡改交易内容，伪造交易签名，从而改变链上的资产状态。这破坏了交易数据的完整性。针对硬件钱包的硬件故障注入攻击，可以通过增强硬件层的加密保护，例如通过使用更加严格的物理安全模块，以及对硬件进行更多的抗攻击设计，如硬件故障注入的检测与防御机制。硬件钱包可以设计为在检测到故障注入时自动销毁私钥或锁定设备。并结合生物识别技术和硬件加密密钥，通过多重身份验证来增强安全性。这样即使私钥被泄露，攻击者仍然难以通过物理设备进行交易。使得区块链用户可以更好地防御此类攻击，确保资产安全。

(2)侧信道攻击

侧信道攻击是一种通过分析设备在运行过程中的物理信号(如时间、功耗、电磁辐射、声波或热量)来推测敏感数据的攻击方式。如图2所示，常见的方法包括时间分析攻击，通过测量设备执行操作所需时间的差异来推断密钥或数据；功耗分析攻击，通过监测设备的功耗波动模式推测其内部操作，分为简单功耗分析和差分功耗分析；电磁泄漏分析，利用设备运行时产生的电磁信号提取信息；声波分析，通过捕获设备运行时的声波频谱模式推断操作流程；以及热分析攻击，通过监测设备表面温度变化推测其内部处理情况。这些方法通过物理侧面信息泄露，绕过加密算法本身，直接威胁设备的安全性。

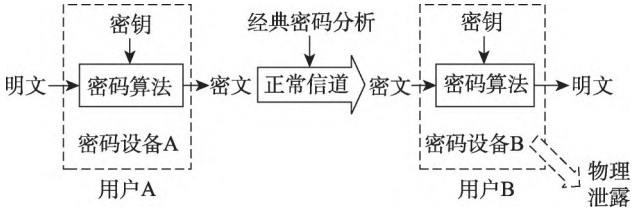


**图2 侧信道攻击流程图**

Fig.2 Side channel attack flowchart

2020年，Tramer等人[10]针对接收者的隐私提出了一般的计时侧信道攻击和流量分析攻击。这些攻击使活跃的远程攻击者能够识别注重隐私的加密货币Zcash或Monero中任何交易的秘密收款人。这些攻击通过利用因实施不同系统组件而泄露的侧信道信息，从而违反了这些加密货币的隐私目标。具体来说，证明了远程用户可以通过测量该用户的P2P节点对某些请求的响应时间，来链接向该用户发送资金的所有交易。时间差异足够大，可以通过WAN远程进行攻击。并进一步研究了计时侧信道对这些加密货币中使用的零知识证明系统的影响。在Zcash的实施中，生成零知识证明的时间取决于秘密交易数据，尤其取决于交易资金的数量。因此，计时侧信道攻击使得攻击者能够利用证明生成时间的微小差异，推测出交易的金额和其他敏感信息，从而破坏了区块链交易的机密性。

为防止计时侧信道攻击，可以通过在生成零知识证明时引入随机化过程，使得每次交易的响应时间无法预测，从而避免通过响应时间推测交易金额。随机化的引入可以大幅度减少侧信道信息的泄露。对于像Zcash和Monero这样的隐私币，可以加强协议层的安全性，包括对零知识证明系统的优化，确保即使存在侧信道攻击，攻击者也无法从计算时间中推测出任何敏感信息。

(3)硬件木马攻击

硬件木马攻击是指攻击者通过修改或篡改硬件设备，植入恶意硬件木马，使其在硬件层面执行未经授权的操作，从而对计算机或网络系统造成安全威胁。这类攻击通常涉及攻击者能够物理接触到硬件设备，或者通过网络访问受感染的设备。

区块链平台Radiant Capital，是一个基于区块链的借贷平台，在2024年遭受了一次毁灭性的黑客攻击，导致损失超过5 000万美元。此事件引发了区块链用户对其智能合约安全性和私钥管理的担忧。Radiant Capital遭黑客攻击的原因是攻击者在多名团队成员的电脑上植入木马程序，诱导硬件钱包签署恶意transferOwnership()操作，将借贷池的控制权转移给攻击者。攻击者随后部署了transferFrom代码，继续从用户的授权账户中窃取资金。此次攻击的复杂程度远超一般攻击，涉及硬件木马程序、硬件钱包拦截软件、智能合约编写、了解组织结构和签名流程等技术。

通过修改智能合约的控制权，攻击者不仅能够窃取资金，还可能影响平台的正常运行。这破坏了区块链系统的数据完整性，因为合约被篡改，交易记录不再可信。针对硬件木马攻击，智能合约的设计应当进行细致的权限管理，通过增加多重授权机制来避免单点故障。

中国知网 https://www.cnki.net

特别是敏感操作如 transferOwnership()应限制权限,避免由单一账户控制,从而防止控制权被滥用。

## 1.2 网络协议上的攻击及相应对策

(1)路由攻击

路由攻击指攻击者将包含错误信息的路由控制包,伪造成合法的信息包,发送到路由终端,干扰正常路由的过程[11]。路由攻击主要包括BGP劫持、中间人(man-in-the-middle,MITM)攻击和路由信息篡改。BGP劫持通过伪造BGP路由公告,将流量重定向至攻击者控制的节点,进而拦截或篡改数据。MITM攻击则在两方通信之间插入自己,拦截并可能篡改通信内容,破坏数据的机密性和完整性。路由信息篡改则通过操控路由协议或改变流量路径,绕过安全防护或泄露敏感信息。这些攻击方法可以威胁区块链网络的安全性、数据完整性和系统的可用性。

Apostolaki等人[12]针对比特币网络所面临的路由攻击进行了详尽分类,主要分为两大类:其一,是通过分割比特币网络为两个互不连通的部分,以破坏其完整性;其二,则是通过延迟区块信息的传播,进而影响全网达成共识的效率。为有效应对上述两类路由攻击,他们提出了短期与长期防御策略。短期措施聚焦于增强网络连接的多样性、审慎分析路由信息、持续监控网络性能、接纳自然的网络连接流失现象,以及精心选择托管服务的位置,这些举措的共同目标在于削弱攻击者对网络的控制力,从而提升比特币网络的整体安全水平。长期防御策略则侧重于加强比特币网络通信的安全性、隐私保护及鲁棒性,具体措施包括比特币连接的加密处理、引入信息验证码机制,以及采用UDP心跳技术。在文献[12]提出的长期策略基础上,Sentana等人[13]提出基于分布式防篡改的联盟区块链系统“BlockJack”,其通过确保区块链与BGP网络间独立性接口同步操作,有效抵御BGP前缀劫持等路由攻击,显著提升网络安全。

2022年亚马逊云计算服务对IP地址突然失去控制后,花了三个多小时才得以重新获得控制权。攻击者利用BGP劫持技术,通过底层互联网协议IP的漏洞控制了约256个IP地址。其中,属于亚马逊运营的AS16509的/24 IP地址块,在8月被错误地指向了英国网络运营商Quickhost的自治系统209243。受影响的IP地址中,44.235.216.69是Celer Bridge加密货币交易所的关键子域bridge-prod2.celer.network的服务器。黑客通过控制该子域,成功从拉脱维亚证书管理机构GoGetSSL获得了TLS证书。利用该证书,黑客在同一域中部署了欺诈性智能合约,并监视正规页面访问。据Coinbase威胁情报团队分析,这些合约从32个账户盗取了234 866.65美元。

(2)拒绝服务攻击

拒绝服务攻击(denial of service,DoS),攻击者通过发送大量带虚假地址的请求,服务器回复后无法收到回传消息,资源无法释放。反复攻击下,服务器因资源耗尽而中断服务[14]。如图3所示,分布式拒绝服务攻击(distributed denial of service attack,DDoS)是DoS攻击的变种形式。DDoS攻击体系包括主攻击机、控制傀儡机、攻击傀儡机和受攻击机。控制傀儡机发布指令,不参与攻击;攻击傀儡机实际发起DDoS攻击[15]。主攻击机控制这两类傀儡机,发送DDoS程序,程序运行时隐蔽性强。傀儡机数量足够时,主攻击机远程发布指令。傀儡机接收指令后,向目标发送大量数据包,消耗资源,易导致服务中断或系统崩溃。

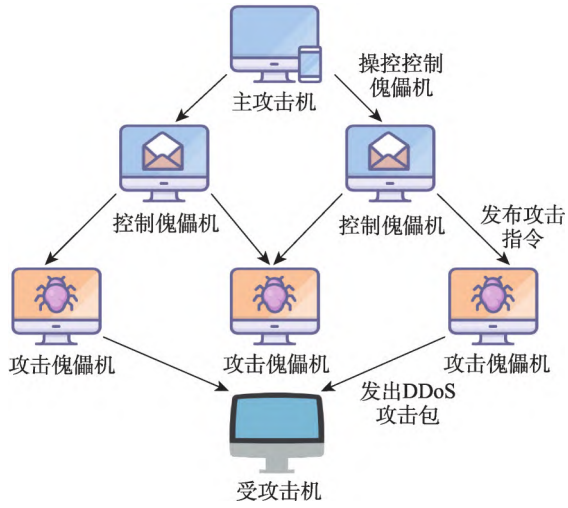


**图3 DDos攻击流程图**

Fig.3 DDoS attack flowchart

防御DoS攻击的首要任务是快速检测和识别攻击源头。基于蚂蚁算法的回溯方法结合流量级信息,实现高效识别DoS攻击的传播路径及源头[16]。引入可验证延迟函数(verifiable delay function,VDF)验证计算任务合法性,具有快速验证和高自由度的特性[17]。结合智能合约和机器学习的方案,通过隐藏服务器在区块链网络中,利用智能合约的不可篡改性和惩罚机制,实时分析并惩戒恶意行为,有效缓解大规模DoS攻击[18]。这套方法体系通过蚂蚁算法回溯、VDF验证和智能合约与机器学习的结合,构成全面高效的DoS检测和防御体系。

相比单个攻击源的DoS攻击,DDoS攻击因其流量特征难以识别、源头分散且多变、攻击模式多样而更难检测。Jia等人[19]提出基于混合集合学习的分布式抗D链检测框架,融合AdaBoost与随机森林,并整合CART与1D3分类器,增强了对DDoS攻击特征的识别能力,提升了检

中国知网 https://www.cnki.net

测系统的鲁棒性和准确性，为后续抵御措施奠定基础。Abou等人[20]创新结合区块链与SDN，提出Cochain-SC方法缓解区块链中的DDoS攻击。该框架通过域内、域间协作机制实现：域内用基于熵和贝叶斯的流量分析方法识别和缓解非法流量，减少资源占用；域间借助区块链智能合约促进不同自治系统安全协作，优化DDoS攻击响应与缓解。

2018年，比特币网络遭遇了一次DDoS攻击，攻击者通过生成大量无效的比特币交易，故意填充交易池，使得矿工和节点的计算和验证能力被大量占用，导致网络的响应速度显著下降。这些无效交易占用了大量网络带宽和节点资源，尤其是在交易验证和区块传播过程中，导致正常的交易数据无法及时处理。长时间的交易延迟可能会影响比特币网络的稳定性，尤其是在网络流量过载时，可能导致更多节点崩溃或断开连接。使得用户和投资者对比特币网络的信任度下降，影响比特币的市场信誉。

（3）DNS攻击

DNS攻击是针对域名系统（domain name system，DNS）的网络攻击，主要包括DNS劫持、DNS放大攻击、DNS缓存污染和域名劫持。DNS劫持通过篡改DNS记录，将用户流量引导至攻击者控制的IP地址，用于窃取信息或散布恶意内容；DNS放大攻击利用开放的DNS解析器，通过伪造请求生成大规模流量，对目标服务器发起DDoS攻击；DNS缓存污染通过向DNS解析器注入伪造的DNS记录，篡改用户的查询结果，引导至恶意网站；域名劫持通过控制域名注册账户修改DNS设置，使合法域名指向攻击者的服务器。这些攻击方式会导致服务中断、数据泄露和用户隐私受损。如图4所示，攻击者发送大量的DNS回应报文到DNS缓存服务器，导致缓存服务器因为处理这些DNS回应报文而耗尽资源，影响正常业务的过程。

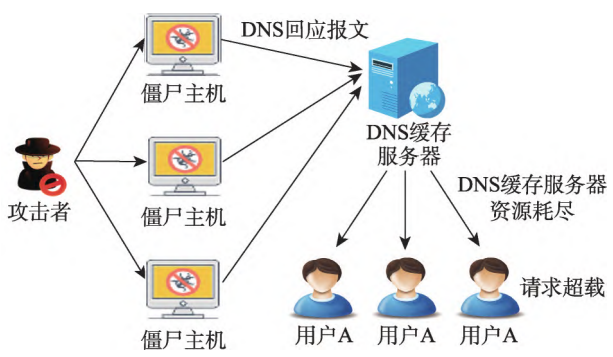


**图4 DNS攻击流程图**

Fig.4 DNS attack flowchart

2024年7月11日，包括Compound Finance和Celer Network在内的多个去中心化金融协议遭遇了DNS劫持攻击。攻击者通过篡改这些平台的DNS记录，将用户重定向至钓鱼网站，试图窃取用户的敏感信息和资金。攻击者主要针对通过Squarespace注册的域名。在从Google Domains迁移至Squarespace的过程中，可能存在的安全漏洞被攻击者利用，导致多因素身份验证被绕过。这使得攻击者能够篡改DNS记录，将用户重定向至恶意网站。虽然Celer Network成功阻止了攻击，但Compound Finance的用户可能在不知情的情况下泄露了敏感信息或资金。从DNS劫持到针对托管服务提供商的社会工程攻击，黑客已经多次证明，许多加密项目中最薄弱的环节不是区块链本身，而是围绕它的传统网络系统。

在针对DNS攻击的防御中，可以使用TLS（transport layer security）/SSL（secure sockets layer）加密等安全协议加强与用户之间的通信安全，防止通信过程中被篡改或监听。同时，去中心化平台可以考虑使用分布式域名系统来增强区块链网络的抗攻击能力。

### 1.3 通信协议上的攻击及相应对策

（1）日蚀攻击

日蚀攻击是针对P2P网络的一种攻击形式，攻击者通过操控网络连接使目标节点仅与恶意节点通信，全面控制其信息访问。并利用僵尸网络篡改节点列表，植入恶意地址，用DDoS攻击迫使目标重启，连接恶意节点，实现双花等目的，破坏区块链系统完整性和可信度。2015年，Heilman等人[21]首次揭示了比特币网络中日蚀攻击的可行性，并通过实验验证了攻击者可以通过控制大量公共IP地址来垄断受害者的网络连接，从而隔离受害者并呈现恶意的区块链视图，该工作不仅展示了日蚀攻击的潜在威胁，还为后续的研究提供了基础。

Xu等人[22]扩展研究至以太坊网络，提出基于随机森林分类算法的日蚀攻击检测模型ETH-EDS，通过收集分析正常和攻击数据包，提取数据包大小、访问频率和时间等特征检测恶意行为。此外，一种不依赖区块链协议更改的轻量级检测方法被提出[23]，利用客户端与互联网服务器间的自然连接，通过八卦协议检测日蚀攻击，允许客户端交换区块链视图信息以检测不一致性。

为解决区块链中的日蚀攻击威胁，提出了一种基于节点间互相评价机制的动态防御模型[24]。通过引入节点间互评机制，结合Kademlia网络协议，对节点的历史行为进行评分，并据此动态调整邻居选择策略。节点在建立连接时优先选择排名更高、行为可信的节点，从而有效降低被恶意节点包围的风险。

（2）女巫攻击

女巫攻击最早是2002年由Douceur[25]在“The Sybil

中国知网 https://www.cnki.net

attack”一文中提出的，他不仅定义了Sybil攻击，还分析了在分布式系统中如何识别和防御这种攻击。如图5所示，攻击者通过单个恶意节点伪造大量虚假节点（Sybil节点）加入网络，这些节点为攻击者夺取网络控制权，干扰查询和返回错误结果。针对区块链网络，其目的旨在削减网络冗余、实施监视或干扰网络正常运作，以及降低网络的整体健壮性。

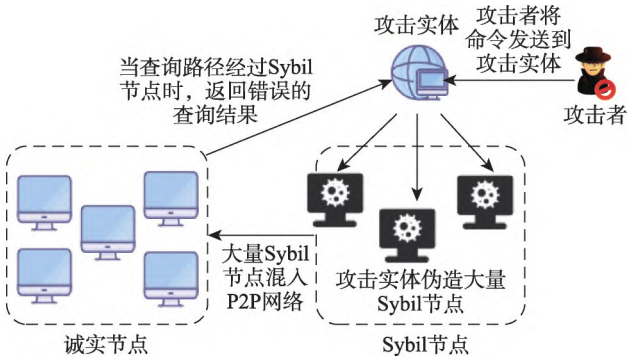


**图5 女巫攻击流程图**

Fig.5 Sybil attack flowchart

在探究女巫攻击对区块链网络系统的挑战时，首要关注共识算法的优化。一种基于实用拜占庭容错算法的反假冒共识机制被提出[26]，引入信誉评价系统，依据节点行为动态分配信任分数，提升对Sybil节点的识别能力。Swathi等人[27]设计针对性防御策略，强调节点间相互监督，关注异常节点，通过加入黑名单遏制女巫攻击。Davis等人[28]提出将女巫攻击作为缓解P2P僵尸网络问题的策略，部署虚假节点渗透僵尸网络，实现多重打击效果。

2022年5月，跨链桥项目Hop Protocol发起了代币空投，将代币总供应量的8%空投给早期用户。空投条件包括达到一定交易量、提供流动性、持有债券、社群活跃参与等。最初符合空投条件的地址大约有43 000个。随后，Hop项目方发起了一项社群举报女巫地址的活动。举报成功者可获得被举报女巫地址原定空投份额的25%作为奖励，从而鼓励用户积极参与揪出女巫地址。最终，约10 000个地址被举报并认定为女巫，取消了空投资格。女巫攻击在区块链领域仍然是一个普遍存在的挑战，并可能针对区块链的共识机制、经济模型和用户隐私，威胁去中心化系统的安全和稳定性。

在本章内容中，分析了区块链Layer 0基础协议层在硬件基础设施、网络协议以及通信协议三大核心领域所面临的潜在安全威胁，并在此基础上系统性地归纳与提出了一系列创新性的防御策略。如表2所示，

**表2 Layer 0恶意攻击类型总结**

Table 2 Layer 0 summary of malicious attack types

| 攻击所在组件 | 攻击名称 | 攻击特征 | 预防措施 | 对区块链的危害性 |
|---|---|---|---|---|
| 硬件基础设施 | 硬件故障注入 | 通过向硬件设备施加异常（如电压、温度等）来引发错误，绕过硬件钱包的安全保护 | 采用物理防篡改设计，增加硬件的抗攻击性，使用硬件加密模块增强安全性 | 破坏私钥的机密性，导致私钥泄露，从而损害资产安全。可能使得硬件钱包失去其原本的安全性 |
| | 侧信道攻击 | 通过分析硬件或软件的物理信息（如电磁辐射、功耗、响应时间等）窃取加密数据 | 加密算法采用随机化技术，增加功耗/响应时间一致性，使用抗侧信道攻击的硬件设计 | 破坏区块链的机密性和完整性，泄露敏感数据如私钥、交易数据，可能导致资金盗窃 |
| | 硬件木马攻击 | 通过恶意程序控制硬件钱包或其他区块链设备，窃取私钥或授权信息 | 加强硬件钱包的物理安全，定期审查硬件钱包的固件，启用多因素身份验证 | 私钥泄露，资金被盗，攻击者可以绕过传统安全机制并完全控制用户账户 |
| 网络协议 | 路由攻击 | 通过操控互联网路由器或BGP协议，重定向区块链网络流量至恶意节点，进行数据窃取或篡改 | 使用BGP监控和验证工具，确保路由表的安全；启用加密通道来加密网络传输 | 数据被篡改、交易被重定向或丢失，可能导致双花攻击、资金丧失以及区块链信任的丧失 |
| | 拒绝服务攻击 | 通过发送大量请求消耗目标系统资源，导致系统崩溃或拒绝服务 | 增加网络的抗攻击能力，如采用负载均衡、流量清洗、内容分发网络等技术；使用DDoS防护服务 | 网络瘫痪、交易延迟、系统不稳定，破坏区块链的可用性，导致用户无法正常访问或提交交易 |
| | DNS攻击 | 通过篡改DNS记录，重定向用户至钓鱼网站，窃取私钥、助记词或其他敏感信息 | 部署域名系统安全扩展来确保DNS数据的安全性，控制DNS请求频率和来源 | 用户信息和资金泄露，破坏区块链应用的信任性；通过伪造网站进行钓鱼，损害区块链的安全性和用户信任 |
| 通信协议 | 日蚀攻击 | 通过操控系统中时间戳或区块生成时间，影响区块链的最终性和共识过程 | 使用不依赖于时间戳的共识机制，增加时间验证和延迟处理，确保交易和区块生成不受时间操控影响 | 影响交易确认时间，可能导致链重组、双花攻击等，破坏区块链的最终性和共识机制 |
| | 女巫攻击 | 通过创建大量虚假身份或节点，控制或影响网络，削弱网络的冗余备份 | 使用机器学习算法检测网络中的异常模式，要求用户证明与身份数量相匹配的资源 | 破坏区块链治理的公正性，影响决策过程，可能导致权力集中和利益不均，影响区块链网络的去中心化特性 |

中国知网 https://www.cnki.net

概述了每种攻击的攻击特征并总结研究人员提出的抵御方法。

## 2 Layer 1基础链层的恶意交易与攻击

Layer 1基础链层(base layer/mainnet)，是区块链技术的核心层，主要负责处理基本的交易和数据存储，并确保整个网络的安全性和去中心化。它由区块链协议、智能合约和激励机制三个关键组件构成。

区块链协议定义了网络的基本规则和运作方式，包括共识机制和数据结构。共识机制是协议的核心，决定了节点如何就交易和区块的有效性达成一致[29]。常见的共识机制包括工作量证明(proof of work，PoW)；权益证明(proof of stake，PoS)；委托权益证明(delegated proof of stake，DPoS)和实用拜占庭容错(practical Byzantine fault tolerance，PBFT)。区块链中以默克尔树为数据结构，是基于默克尔树在数据完整性验证、高效存储，以及支持去中心化系统[30]。

智能合约是一种自动执行交易和逻辑判断，无需第三方即可进行的可信交易[31]。在如以太坊虚拟机的平台上运行，一旦满足预设条件，合约会自动执行。

激励机制是通过奖励积极参与者和惩罚不良行为者[32]。激励网络参与者维护网络，确保生态系统的稳定和持续发展。这三个组件共同确保了区块链网络的安全、透明、不可篡改和可持续性。

### 2.1 区块链协议上的攻击及相应对策

(1)51%攻击

51%攻击是指基于PoW的区块链网络中的一个潜在漏洞，攻击者通过控制超过50%的挖矿能力，可以发起双重支付或撤销交易。如图6所示，攻击者发起两笔交易T1和T2，分别被不同区块确认，形成分叉A和B。攻击者控制大部分算力，使分叉B增长快于A。根据最长链原则，B成为主链，A被遗弃，导致T1交易被撤销。攻击者因此获得现金并保留原代币，实现双重支付。当攻击者控制区块生成权后，可以拒绝任何不利于其利益的交易写入区块链，破坏区块链共识的公平性，使区块链变得中心化或失去公信力。

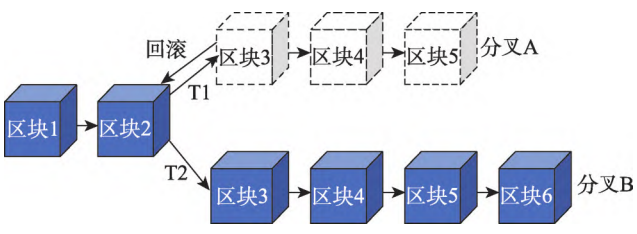


**图6 51%攻击流程图**

Fig.6 51% attack flowchart

在区块链领域，51%攻击的威胁促使研究者们深入探讨并提出了多种防御机制。Garoffolo等人[33]提出“延迟提交区块的惩罚系统”，通过大幅提升攻击成本来消除潜在攻击者优势，惩罚基于区块被隐瞒时间计算。Yang等人[34]提出将矿工历史加权信息与总计算难度结合的技术，通过历史加权信息计算链总难度，增加攻击者资源投入，提高区块链安全性，使51%攻击成本提高两个数量级，增强小型区块链安全性。Aponte-Novoa等人[35]分析比特币和以太坊矿工算力分布，验证算力集中威胁，提出延迟区块发送惩罚系统、基于历史加权难度的挖矿行为研究和使用监督式机器学习算法及算法博弈论等预防措施，从矿工行为角度为防御51%攻击提供实证支持。

2018年发生了以太坊经典(Ethereum classic，ETC)51%攻击，恶意矿工在10 904 146块到10 907 740块之间独立挖出了3 594个区块，生成了一个巨大的分叉。攻击者在独立挖掘“分叉”块时没有向全网发布这些块，所以没有人知道它正在发生。因为这个条分叉链比其他所有矿工建立的链更重，使得矿工们不得不接受这条链，攻击者分叉出的区块链成功变成了主链。本次攻击虽然成功实施，但攻击者并没有得到超额利润回报，但是对ETC这条链的伤害是巨大的，对ETC矿工的信心造成打击，全网总算力可能进一步萎缩。

(2)自私挖矿

自私挖矿是一种矿工通过战略性发布和隐藏区块以此获得更多区块奖励的攻击行为。如图7所示，自私矿工发现新区块后扣留，私自在其上继续挖矿形成分叉A。当A长度超过诚实矿工的分叉B时，A成为有效链，B被抛弃。自私矿工因此独得A上所有区块奖励。自私矿工通过操控区块发布时机，增加自己获得的区块奖励，减少诚实矿工的奖励份额。这种行为破坏了矿工之间的公平竞争，导致区块奖励分配不公。自私挖矿使得大矿池受益更大，小矿工逐渐退出，会导致区块链网络趋于中心化。

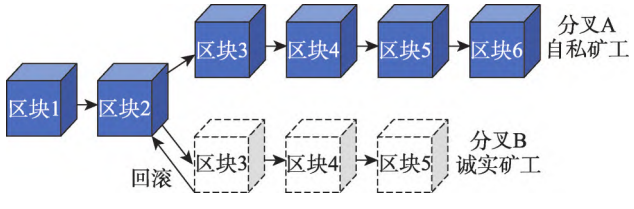


**图7 自私挖矿攻击流程图**

Fig.7 Selfish mining attack flowchart

在区块链技术的研究领域中，自私挖矿的危害是一个备受关注的话题。Eyal等人[36]首次提出了自私挖矿

中国知网 https://www.cnki.net

的概念,分析了在不同情况下自私挖矿策略的收益。并通过构建数学模型和状态机进行的模拟实验证明了在某些条件下,自私挖矿可以为矿工带来更高的收益,从而使得矿工有动机偏离诚实挖矿策略,为后续自私挖矿的研究奠定了理论基础。

继Eyal等人的开创性工作后,Göbel等人[37]探讨了传播延迟下自私挖矿策略对比特币区块链动态的影响,应用简化马尔可夫模型分析不诚实矿工与社区成员对区块链状态认知差异。Yang等人[38]构建新马尔可夫模型,精准捕捉比特币和以太坊网络中矿工行为特征,纳入以太坊特有分叉现象及叔侄区块间距离考量。Madhushanie等人[39]提出防止自私挖矿攻击的机制,通过在区块头添加“BA:区块接受”标志预防攻击,新区块广播前BA标志须为“假”,被广泛接受后方可设为“真”。文献[37]引入了传播延迟,展示了网络性能对自私挖矿的影响。但该模型依然简化了其他复杂因素,如挖矿难度调整或非诚实矿工之间的相互竞争,实际应用可能需要更复杂的优化。文献[38]在文献[37]的基础上提出了更全面的马尔可夫模型,适用于更广泛的区块链环境。但由于纳入了更多的变量和链特性,模型计算复杂度较高,实施和验证的难度也相应增加。文献[39]适用于各种PoW区块链,且对现有协议改动相对较少。BA标志的生效依赖于网络中节点的快速传播和同步,网络延迟或恶意节点可能会干扰该防御机制的效果。

(3)孤块攻击

孤儿区块是一种有效但未纳入最长链的区块,其奖励和费用在最长链上无法使用。在孤块攻击中,攻击者利用强大计算能力快速挖出两个空区块,旨在孤立正常区块,阻止其加入主链。通过链重组使攻击者的链取代主链,从而使合法区块成为孤块,试图破坏区块链的效率、数据完整性和去中心化性。

孤儿区块影响诚实矿工积极性和区块链系统安全性。Chen等人[40]分析孤儿区块产生因素和破坏情况,提出减少网络延迟、共识节点数量和选择合适区块间隔等减少孤儿区块的方法。在此基础上,Jha等人[41]探讨孤块问题,提出增加区块生成时间间隔、动态调整区块大小、构建辅助链等减少孤块风险的方法,并在以太坊环境中验证孤块比率。Solat等人[42]提出ZeroBlock新解决方案,防止比特币孤块攻击,其核心是矿工在一定时间间隔内未发现新区块时生成虚拟“Zeroblock”,无需解决工作量证明,可防止未经授权区块保留。

孤块现象虽然在区块链网络中是正常的,但如果攻击者故意制造孤块会导致矿工的算力浪费,降低网络整体效率。由于实施孤块攻击的成本高且收益不明显,公开的孤块攻击案例较少,但人为操纵孤块也会对区块链网络造成不可忽视的危害。

(4)双花攻击

双花攻击指的是攻击者试图使用同一笔资金在区块链上进行多次支付。在双花攻击中,攻击者通过操控区块链网络的共识或利用系统设计的漏洞,使得一笔交易能够被多次花费。双花攻击有多种变体,其中常见的三种形式是:芬尼攻击、种族攻击和矢量76攻击。芬尼攻击针对区块链未确认交易,由比特币早期开发者Hal Finney提出。芬尼攻击是一种需要攻击者事先挖到一个有效区块的攻击方式,攻击者先在区块链上挖出一个区块但不广播,然后在进行双花交易时广播该区块,导致受害者的交易被拒绝。种族攻击是通过同时发送两笔互相冲突的交易,一笔发送给商家、一笔发送到网络,利用交易确认延迟来实现双花。矢量76攻击结合了芬尼攻击和种族攻击,攻击者利用对未确认交易和区块广播的时间差,通过在私链上预挖区块并发布来进行双花交易。

Masteika等人[43]研究了实体零售中比特币支付的双花攻击风险,提出依赖信誉节点验证交易、设定交易金额限制、监控RBF标志等防御对策,重点在于零确认支付和非托管钱包下的双花攻击,还评估了替代币和二层区块链解决方案。Wang等人[44]进一步深入探讨提出基于区块链的多恶意双花攻击黑名单管理模型,构建黑名单判断策略识别和阻止恶意节点,分析恶意节点联合攻击组合,提出内部恶意游戏概念及联合攻击和去中心化攻击模型,通过数学推导实现技术防御。基于此,Zheng等人[45]提出自适应双花攻击,将其转化为马尔可夫决策过程,用随机动态规划获取最优攻击策略,提醒比特币生态系统双花攻击威胁仍高。这些研究构建了双花攻击全面认识体系,展示了其复杂性、多维性及防御措施的进化。文献[43-45]分别从不同角度研究了双花攻击,文献[43]主要研究零确认支付和非托管钱包下的双花攻击,提出了依赖信誉节点和监控RBF标志的防御措施,该方法易于实施但依赖外部信誉。文献[44]则专注于恶意节点的联合攻击,通过黑名单和博弈模型识别和阻止恶意矿工,能防范大规模恶意联合攻击,但复杂度高。文献[45]提出了自适应双花攻击,利用马尔可夫决策过程计算最优攻击策略,自适应攻击模型揭示了攻击的潜在威胁,但防御需要更强的计算和预测能力。

2021年老牌公链Aeternity(AE)官方证实,他们遭到了双花攻击,此次攻击主要集中在头部交易所和矿池(OKEx、Gate、Binance),损失超过3 900万枚AE代币,价值超500万美元。攻击者首先通过超过半年的时间

中国知网 https://www.cnki.net

积累了2 752万枚AE代币。随后，他们在交易所开设了多个账户，并准备了约2 700万枚AE代币作为接盘资金，同时将USDT等资产充值到这些账户中。接着，攻击者实施了双花攻击，将伪造的AE代币充值到OKEx交易所，并通过自己的账户在交易所内进行交易，将这些伪造的代币卖给自己的小号。通过这种方式，他们将OKEx交易所中的真实AE代币分散提取到各个小号中，并在其他交易所进行抛售。双花攻击大大降低了用户对小型区块链系统的信任，导致用户流失严重。

## 2.2 智能合约上的攻击及相应对策

（1）整数溢出和下溢攻击

整数溢出和下溢攻击针对智能合约中整数处理不当。溢出是整数增加超出范围，当一个整数变量超过其最大存储容量时，值会回绕到最小值。例如，在一个8位无符号整数中，255+1的结果不是256，而是回绕到0。下溢是整数减少低于范围，当一个整数变量低于其最小存储容量时，值会回绕到最大值。例如，在一个8位无符号整数中，0−1的结果不是−1，而是回绕到255。攻击者通过触发这些溢出，可操纵合约逻辑，异常增加自己余额或资产。例如，他们可能使接近最大值的余额溢出变为0，再操作使余额错误地极大增加；或通过下溢使数值从0变为最大值，绕过权限检查。

整数溢出和下溢攻击是智能合约安全的关键问题。Feist等人[46]提出的Slither框架，作为以太坊智能合约的静态分析工具，自动化识别漏洞、优化代码，增强用户理解并辅助审查。其核心优势是中间表示层SlithIR，支持高效数据依赖分析和污点跟踪，在检测整数溢出和下溢漏洞上性能、鲁棒性和准确性超越同类工具。

如图8所示，Wang等人[47]开发了基于机器学习的以太坊智能合约漏洞自动检测模型ContractWard，收集分析49 502个智能合约，利用Oyente工具标记6种漏洞，提取1 619维特征刻画合约静态属性。该模型融合5种机器学习算法与2种采样技术，提升漏洞检测效率和全面性，尤其适合大规模合约批量检测，与Slither框架相比，更侧重自动化和效率。He等人[48]提出基于彩色Petri网（colored Petri net，CPN）的形式化分析方法，严格数字化验证智能合约安全性，为整数溢出和下溢攻击提供深刻理解，通过定义颜色集、设计库所与变迁等构建CPN模型，利用CPN Tools进行模拟与状态空间分析，深度洞察智能合约安全性。

Yam Finance是一个去中心化金融项目，旨在通过弹性供应机制（rebase）来稳定其代币YAM的价格。2020年8月12日，Yam Finance团队发现其智能合约中存在一个简单的数学错误导致了整数溢出，使协议无法正常调整代币供应。该漏洞位于YAM.sol合约的rebase函数中。在执行rebase操作时，代码错误地计算了totalSupply，导致系统保留了过多的代币。错误的代码未能正确更新totalSupply，导致每次rebase都会铸造出超出预期数量的YAM代币。这不仅破坏了代币的供应机制，还使得治理代币的分配出现问题，影响了社区对协议的治理能力。YAM代币价格在漏洞披露后迅速暴跌，24小时内跌幅达99%，对区块链生态系统造成重大损失。

（2）时间戳依赖攻击

时间戳依赖漏洞是智能合约中一个重要的安全问题，源于合约在执行关键逻辑时对区块链上的时间戳的依赖。矿工在创建区块时可以在一定范围内调整时间戳，这种灵活性可能导致预期外的合约行为。具体来说，矿工可能通过操控时间戳来影响依赖其生成的随机数或基于时间的锁定机制，从而可能提前解锁代币或延长锁定期，攻击者通过操控时间戳，影响智能合约的执行条件，这为智能合约的安全性带来了严重威胁。

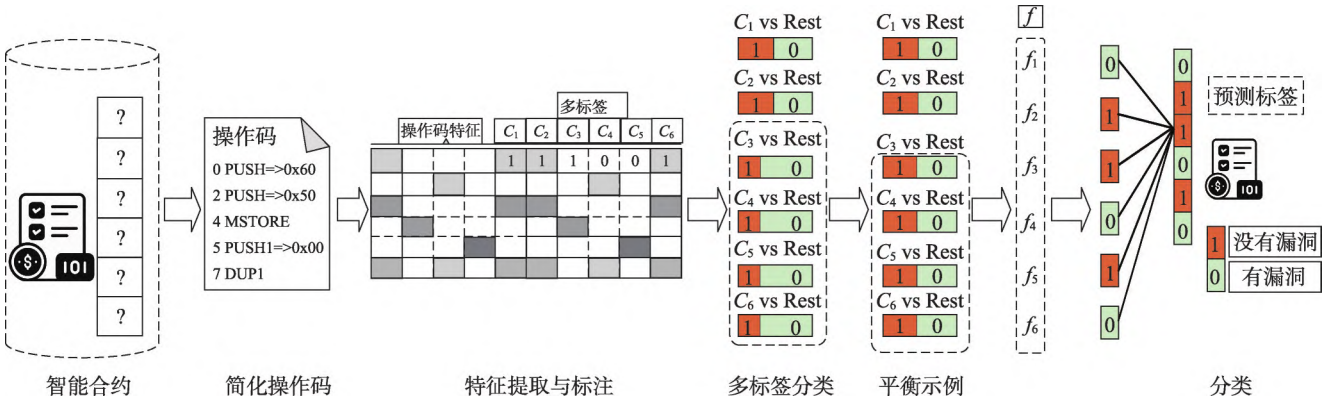


**图8 ContractWard方法检测流程**

Fig.8 ContractWard methods detection process

中国知网 https://www.cnki.net

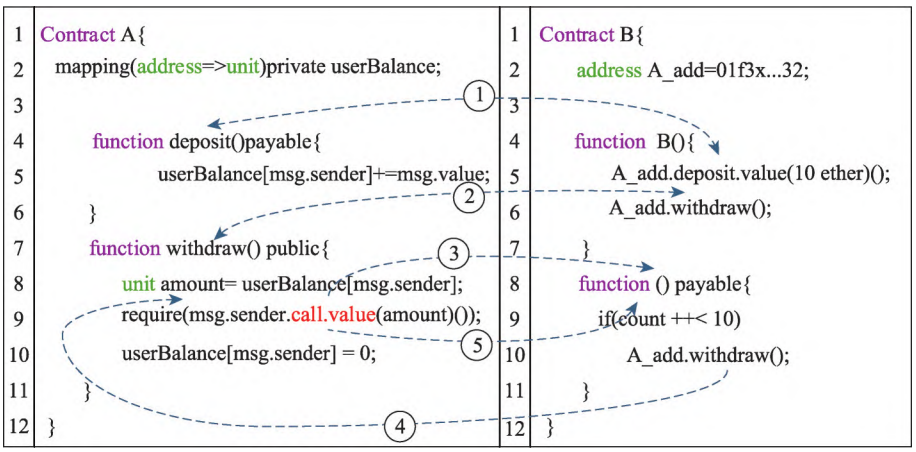


**图9 重入攻击原理图**

Fig.9 Reentry attack schematic

时间戳依赖攻击是智能合约安全的重要课题。Liu等人[49]提出将图神经网络与专家知识结合用于漏洞检测的方法,将智能合约源代码的控制流和数据流语义转换为合约图,利用图神经网络提取图特征并结合安全模式检测漏洞。Zhang等人[50]提出的CBGRU模型,结合不同词嵌入方法和深度学习方法,通过不同模型提取特征进行漏洞检测,在时间戳依赖攻击检测中展现卓越性能,相较于文献[59]的单一图神经网络模型,在多方面提供优势。

Fomo3D是一款基于以太坊的区块链游戏,其设计包含一个空投奖励机制,旨在通过随机性激励玩家参与。Fomo3D的空投奖励依赖于智能合约内生成的“随机数”,由airdrop()函数控制。由于该函数使用了可预测的区块信息(如时间戳)和调用者地址作为随机数种子,攻击者可以通过构造特定的合约,在相同环境内执行相同的随机数计算公式,预测出随机数结果。由于游戏的随机性被破坏,玩家对游戏的公平性产生质疑,使得Fomo3D项目的声誉受到严重影响,由此可见时间戳依赖攻击对智能合约的危害极大。

(3)重入攻击

重入漏洞是一种针对智能合约的严重安全漏洞,攻击者利用智能合约在外部调用期间尚未更新内部状态的时机,反复进行非法操作。如图9所示,合约A的取款函数存在重入漏洞,合约B利用该漏洞窃取资金。首先,攻击者将10以太币存入合约A(步骤1)。然后,攻击者通过调用withdraw函数(步骤2)。当合约A使用call.value向攻击者发送10个以太币时,回退函数将被自动调用(步骤3)。在其回退函数中,攻击者会再次调用withdraw函数(步骤4)。由于攻击者的userBalance尚未设置为0,因此合约A认为攻击者合约中仍有10个以太币,因此再次向攻击者转账10个以太币(步骤5)。取款循环持续9次。最后,攻击方获得100以太币。

作为智能合约安全领域中的一个关键问题,重入攻击一直是研究人员关注的重点。Nikolić等人[51]提出系统化方法表征和检测追踪漏洞,开发MAIAN工具。如图10所示,MAIAN通过插程序间符号分析和具体验证器,精确推理追踪属性,几秒内分析近百万份合约,真实阳性率89%。其分析覆盖合约全生命周期,强调执行痕迹分析,识别多次调用中漏洞合约。虽分析深度和精确度有优势,但处理复杂合约时资源和时间消耗大,需不断更新以适应区块链技术发展。

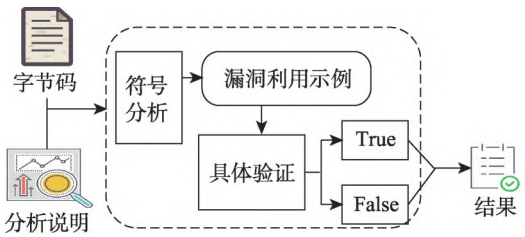


**图10 MAIAN工具检测过程**

Fig.10 MAIAN tool detection process

Rodler等人[52]在Nikolic等人的基础上提出Sereum技术,通过扩展以太坊客户端,引入污点跟踪和攻击检测模块,运行时监控和验证智能合约执行,保护合约免受重入攻击。Sereum在合约执行中跟踪状态变量污点,检测可能导致状态不一致的更新,对关键状态变量添加写入锁,防止重入时非法更新,并实时构造动态调用树检测违规更新。与MAIAN工具相比,Sereum运行时监控对性能影响小,处理大量交易时开销低。

2016年6月17日,以太坊上的去中心化自治组织The DAO遭遇了一次严重的黑客攻击。攻击者利用智

中国知网 https://www.cnki.net

能合约中的重入漏洞，在合约尚未更新余额之前，反复调用提现函数，从而窃取了超过360万枚以太币，约占The DAO总资金的1/3。此次攻击直接引发了以太坊社区的分裂，最终导致以太坊硬分叉，形成了ETH和ETC两条链，削弱了用户对智能合约和区块链项目的信任。

(4)权限控制攻击

权限控制漏洞是智能合约开发中常见的安全问题。通常源于智能合约对关键功能的权限控制不足或缺乏合适的验证逻辑。攻击者可能通过伪造身份、直接调用函数或利用未正确初始化的变量获得超出其权限范围的访问控制，进一步控制合约的核心功能、修改敏感数据或窃取资产。这种攻击方式针对的是权限划分不当、权限验证缺失或逻辑错误的系统，可能导致区块链上的数据被篡改，破坏区块链的数据完整性，削弱用户对智能合约和区块链网络的信任。

Kalra等人[53]提出ZEUS框架，结合抽象解释和符号模型检测验证智能合约安全性，通过静态分析源代码、插入断言语句、转换为LLVM字节码并使用验证器确定违规情况，用户可定义安全策略，相比传统审计，减少了劳动强度和出错概率，但依赖策略定义质量，适用于特定场景。Yang等人[54]引入自然语言处理和机器学习技术提高数据隐私保护效率，研究敏感数据发现、掩码算法推荐及执行，实现智能化掩码中间件，提高隐私数据识别和保护效率，主要适用于隐私保护领域。

2023年4月9日，SushiSwap的RouteProcessor2合约存在权限校验漏洞，攻击者利用该漏洞获利约330万美元。漏洞合约RouteProcessor2未对回调调用者进行是否是uniswapV3 factory部署的V3池检查，只是检查是否是原来lastCalledPool的值，导致了账户授权给RouteProcessor2合约过多尚未使用的资金被盗取。该事件表明，智能合约在权限控制方面的漏洞可能被攻击者利用，导致资金损失。

(5)短地址攻击

短地址攻击是指攻击者利用智能合约对地址参数处理不当的漏洞，通过构造特定的交易数据，使得智能合约无法正确处理地址，从而导致资产被盗或其他恶意操作。通过使用EVM数据自动完成机制来移位和放大第二个参数[55]。这种操作攻击者可以滥用转移函数，非法获取更多的ERC20代币。短地址攻击通常发生在交易中(如在交易所请求提款)。用户在交易所发起合约转让，目标是恶意构建的短地址。如果智能合约没有正确验证地址参数长度，实际转账金额就会因短地址漏洞而急剧增加，导致大量资金被盗。

短地址漏洞的根本原因在于EVM的底层设计缺陷[56]。有效的预防措施包括：在交换层增加以比特为单位的用户输入地址长度验证，或在代码层引入地址长度检查机制，以防止因参数对齐错误而引发的漏洞利用。

2017年这一漏洞曝光后，虽然EVM层并未解决这一问题但各大交易所基本都增加了地址长度校验，web3层也增加了参数格式校验，所以这种攻击在实际应用场景中不会出现。

## 2.3 激励机制上的攻击及相应对策

(1)贿赂攻击

区块链系统用激励机制促参与者诚信，但贿赂攻击是严重威胁。攻击者可以通过多种方法贿赂矿工或验证者来破坏区块链的安全性和完整性。攻击者可以采用直接贿赂的方式，向矿工或验证者支付费用，要求他们验证或拒绝特定交易，或者在区块中包含攻击者构造的交易，以实现双花攻击或阻止竞争对手的交易。攻击者还可以实施隐性贿赂，通过创建一个包含高额手续费的交易，并在条件达成后支付给完成指定行为的矿工或验证者，以此鼓励他们支持攻击链，实现链重组或分叉。在基于投票的治理系统中，攻击者可以利用治理系统贿赂，提供经济激励，诱导持币者或验证者支持特定提案，以实现协议升级、参数调整或其他有利于攻击者的决策。这些贿赂手段都可能对区块链的安全性和去中心化原则造成严重威胁。

Ding等人[57]提出的RIPPB系统通过引入声誉系统和逻辑回归模型改进PBFT协议，增强区块链网络鲁棒性和防御假冒攻击能力，相比传统PBFT，减少节点通信次数，提升信誉度，有效遏制贿赂攻击。Liu等人[58]进一步改进PBFT协议，提出结合多链结构与声誉系统的共识机制，构建双层区块链结构和信誉评估系统，提高交易吞吐量，有效抵御贿赂攻击，但维护成本高，跨链通信安全性至关重要。Sun等人[59]提出贿赂攻击量化分析方法，专注攻击者收益计算，提出精准攻击成本与收益模型，建议设置交易上限和增加确认块数量等策略加强防御。文献[57]提高系统容错能力，但未量化贿赂攻击；文献[58]提升交易吞吐量和安全性，但面临高维护成本和跨链通信安全问题；文献[59]使攻击分析更具现实性和可操作性，但可能忽视其他类型攻击。

2019年，以太坊经典网络曾遭遇贿赂攻击的尝试。攻击者在论坛上公开提议向ETC矿工提供经济激励，鼓励他们支持攻击链，以实现双花攻击。这种行为破坏了ETC网络的共识机制，引发了社区对区块链经济激励模型的质疑。

中国知网 https://www.cnki.net

(2)共谋攻击

共谋攻击是区块链网络的攻击方式,涉及多个攻击者合作,共谋攻击主要包括共谋矿工攻击,即矿工或验证者形成隐秘联盟,集中算力或权益来控制区块生成过程,实施51%攻击操控主链或选择性处理交易;治理共谋,攻击者在链上治理系统中联合大量投票权持有者操控投票结果,推动有利提案或阻止社区利益相关提案;节点联盟攻击,多个节点联合操控网络通信,阻止合法交易广播或制造分叉,破坏网络正常运行并增强对网络的控制力;经济共谋,攻击者与矿工或验证者达成秘密协议,通过经济激励诱导其执行攻击行为,如实现双花攻击或操控交易顺序。共谋攻击主要目标是破坏区块链的激励机制,影响区块链网络公平性、降低安全性和导致激励机制失效。

在密码学与网络安全领域,阈值签名方案与信任模型是抵御复杂攻击、保障系统安全的重要手段。Wang等人[60]提出了一种新的阈值签名方案,通过设计特定多项式方程,使 $t$ 个或更多组成员能代表整个组执行有效阈值签名,但无法构造合法组签名,从而抵抗共谋攻击。Qureshi等人[61]则在FIRE模型基础上,引入多维分散式信任和声誉模型FIRE+,通过构建基于见证者评级的图方法确定节点间可能的共谋行为,并定义多种交互策略检测和预防共谋节点的协作行为,动态适应网络环境变化。这两种方法都致力于抵抗共谋攻击,但Wang等人的方案侧重于密码学原理,安全性高但实现难度大;Qureshi等人的FIRE+模型侧重于网络行为检测和适应性,操作性强,但在面对复杂共谋攻击时可能不如密码学方法直接高效。

2019年1月和2020年8月,以太坊经典网络先后遭受了多次由矿工联合操纵的共谋攻击,攻击者们通过租用算力,获得了ETC网络超过50%的哈希率,以此进行深度链重组,创建了长于合法链的分叉链。实现了双花交易,约21.95万ETC被重复花费。频繁的攻击严重损害ETC网络的激励机制,影响其市场价值和发展前景。

(3)区块扣留攻击

区块扣留攻击(block withholding attack,BWH)是一种针对区块链挖矿池的攻击方式。如图11所示,攻击者通过故意不提交有效区块,破坏矿池的收益分配机制,进而获取不正当的经济利益。区块扣留攻击削弱了挖矿池的整体激励效率。攻击者刻意不提交有效区块,矿池需要更长时间才能挖到新的区块,导致整个矿池的挖矿效率下降,影响了诚实参与者的收益。

Hu等人[62]首次将零确定性策略应用于矿池间BWH攻击分析,将攻击建模为双方博弈游戏,ZD策略者可单方面决定对手收益,使攻击者挖矿池间切换不划算,维

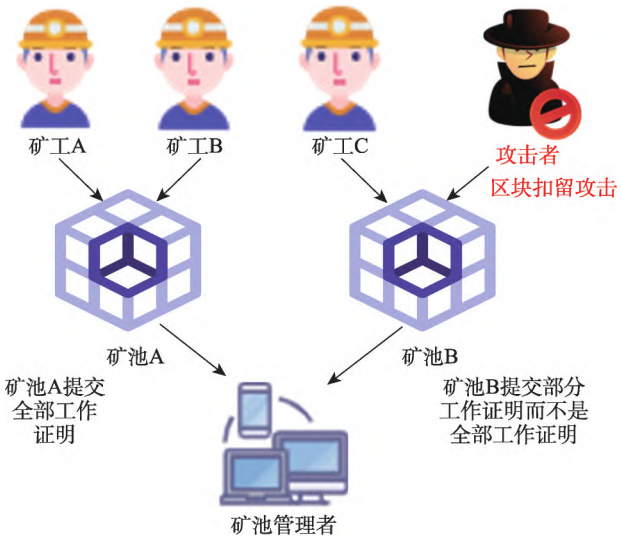


**图11 区块扣留攻击流程图**

Fig.11 Block withholding attack flowchart

护区块链网络稳定性。在此基础上,Liu等人[63]用演化博弈论设计动态博弈模型,通过复制动态方程分析矿池在不同BWH攻击情况下的最优策略,实验表明严格惩罚和高监管下矿池会选择诚实挖矿,低惩罚和低监管下可能会相互发起BWH攻击。Chang等人[64]提出Silent Timestamping防御机制,通过挖矿池管理者强制执行区块排序,迫使攻击者按发现顺序提交份额,削弱BWH攻击动机。文献[62]通过深入的博弈论分析,揭示了攻击者之间的互动和策略选择,但由于ZD策略的理解和实施较为复杂,需要对博弈论有深入的理解并不具备普适性。文献[64] Silent Timestamping为区块扣留攻击提供了一种实际可行的防御机制,不需要网络变化或矿工行为的改变,易于实施。但由于机制依赖于矿池管理者的执行,如果管理者未能正确实施,可能影响防御效果。

在以太坊网络的高负载时期,部分矿池被怀疑通过BWH攻击,延缓其广播时间,导致网络出现短暂的区块空缺。这种行为会使得待处理交易的数量增加,进而推高用户为加快交易确认所愿意支付的Gas费用。当Gas费用升高到一定程度后,这些矿池再将扣留的区块广播并打包高费用交易,从而获取更高的交易手续费收入。这种行为严重影响矿池的正常运作,降低诚实矿工信任度。

本章内容综合分析了区块链Layer 1基础链层在面对复杂多变的恶意交易与攻击时所遭遇的挑战,系统性地梳理并分析了现有研究中关于区块链协议、智能合约和激励机制的多种攻击模式及其防御策略。如表3所示,概述了每种攻击的攻击特征并总结研究人员提出的抵御方法。

中国知网 https://www.cnki.net

表3 Layer 1恶意攻击类型总结

Table 3 Layer 1 summary of malicious attack types

| 攻击所在组件 | 攻击名称 | 攻击特征 | 预防措施 | 对区块链的危害性 |
|---|---|---|---|---|
| 区块链协议 | 51%攻击 | 通过控制网络中超过半数的算力时，便能操纵网络，实现双花交易，阻止新交易确认 | 提高网络的总算力，引入惩罚机制增加攻击成本 | 破坏区块链的不可篡改性和数据完整性 |
| | 自私挖矿攻击 | 自私矿工通过隐藏已发现的区块来获取不正当利益 | 提高交易费用减少攻击者利润，引入新的难度调整公式 | 破坏矿工竞争的公平性，延迟交易确认，损害区块链的最终性和可信度 |
| | 孤块攻击 | 通过广播孤立区块，迫使区块链产生分叉并最终丢弃合法区块 | 改进分叉选择规则，改善矿工网络连接，优化区块链的传播协议 | 影响区块链的稳定性，造成链分裂，丢失交易确认，破坏区块链的完整性和最终性 |
| | 双花攻击 | 通过双重使用同一笔资产进行两次支付 | 增加交易确认次数，确保交易不可逆 | 破坏区块链的交易可信性和资金完整性，可能导致用户资金丢失，影响区块链的信任机制 |
| 智能合约 | 整数溢出和下溢攻击 | 利用程序中整数类型的最大值或最小值限制，进行计算操作导致数据类型值异常 | 在设计系统时，明确整数变量的最大值和最小值，并在代码中实施这些限制 | 造成资金错误转移、资产溢出，影响区块链的完整性和智能合约的正确执行 |
| | 时间戳依赖攻击 | 通过操控时间戳来影响合约执行结果，从中获利 | 对时间敏感的操作中引入缓冲期，采用多个区块的时间戳的中位数作为参考 | 影响区块链的交易顺序、最终性和共识过程，破坏区块链的正确性和数据一致性 |
| | 重入攻击 | 通过构造恶意合约，使得在一次交易中可以不断地回调被攻击合约的函数 | 遵循检查-效果-交互模式，通过重入锁防止合约在处理完当前调用之前再次被调用 | 破坏智能合约的逻辑，造成资金盗窃，影响区块链的资产安全性和合约的正确执行 |
| | 权限控制攻击 | 通过各种手段绕过或破坏系统内的权限控制机制，以获得非授权的访问或提升权限 | 通过多重签名钱包管理合约，确保每个用户或合约只拥有完成任务所需最小权限 | 破坏区块链资产的安全性，损害用户的信任 |
| | 短地址攻击 | 通过传递一个较短的地址字符串，导致智能合约错误地解释后续的参数 | 确保接收的地址都具有完整的20字节长度，避免直接在低级汇编中操作地址 | 用户资金可能被误转移，导致资产丢失，破坏区块链资产的安全性 |
| 激励机制 | 贿赂攻击 | 通过贿赂矿工或验证者来诱导他们采取有害于网络的行为 | 提高区块链网络的监管力度和审计频率，增加区块链网络的透明度 | 破坏区块链的去中心化治理机制 |
| | 共谋攻击 | 通过与多方参与者联手操控网络，以获取不正当利益 | 建立信誉系统来评估参与者的行为，设计系统时限制单个参与者或小团体的权力 | 破坏区块链的去中心化特性，导致矿池垄断 |
| | 区块扣留攻击 | 通过不提交有效区块，破坏矿池的收益分配机制，进而获取不正当的经济利益 | 强制矿工按照区块的发现顺序提交份额，引入博弈论策略设计的激励机制 | 导致交易确认延迟，影响区块链的可用性和用户体验，破坏区块链的即时性和可靠性 |

## 3 Layer 2扩展解决方案层的恶意交易与攻击

Layer 2扩展解决方案作为应对Layer 1区块链固有可扩展性挑战的重要策略，集成了多种先进技术框架，包括状态通道、侧链以及Rollups，旨在显著增强区块链网络的交易处理能力和效率，同时确保去中心化和安全性的核心属性不受损害。状态通道机制通过允许用户在链下环境执行交易活动，仅在交易初始化和最终结算阶段与主链进行交互，极大地减少了链上交易的数量，从而提升了系统吞吐量，并实现了近乎即时的交易确认，特别适用于对交易速度有严格要求的应用场景。

侧链作为一种与主链并行运作的独立区块链结构，通过高效的跨链协议与主链实现互操作性，不仅支持多样化的共识机制，还为特定应用提供了高度定制化的运行环境。更重要的是，侧链通过创新的双向锚定机制，实现了资产在主链与侧链之间的安全、无缝转移，进一步拓宽了区块链应用的边界。

Rollups技术则代表了链下计算与链上数据验证相结合的前沿趋势，如图12所示，Rollups通过将大量交易在链下集中处理，并将处理结果压缩至单个区块内提交至主链，显著提高了交易速度和降低了交易成本[65]。其

中国知网 https://www.cnki.net

中，乐观Rollups采取链下执行交易、链上提交结果的模式，并设置挑战期以防止潜在的欺诈行为；而零知识Rollups则运用了先进的零知识证明技术，通过在链上提交加密的证明信息，有效验证了链下交易的真实性和正确性，无需暴露交易细节。

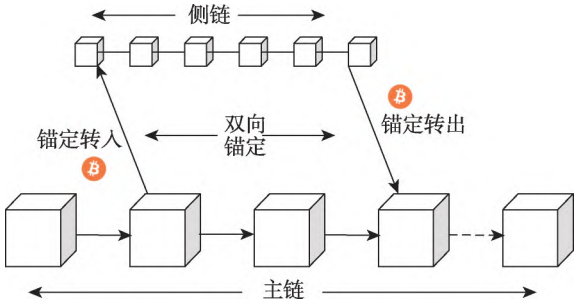


**图12 侧链的广义视图**

Fig.12 Generalized view of side chains

### 3.1 状态通道上的攻击及相应对策

(1)数据可用性攻击

数据可用性攻击(data availability attacks，DAA)影响区块链扩展层，涉及节点恶意提供不完整或错误数据，阻碍数据传播，影响网络正常运行。攻击者可以通过隐藏部分数据，发布一个只包含部分有效数据的区块，导致网络中部分节点无法验证区块数据，进而触发节点间的不一致或分叉。此外，攻击者还可以伪造可用性证明，通过篡改数据证明来欺骗节点接受缺失数据的区块，从而窃取网络资源并破坏数据完整性。数据对区块链的一致性和正确性至关重要，节点需获取全部数据以验证交易和维护系统状态。恶意行为可导致网络问题，如分叉、状态不一致或停滞。在扩展方案如状态通道中，链下计算结果依赖数据可用性，数据不可用将导致错误状态被提交。

为应对区块链数据可用性和完整性挑战，Sheng等人[66]提出ACeD协议解决DAA问题，通过在Merkle树承诺中集成编码理论，确保数据分布式可用性和防篡改性，其创新的编码-分散结构和高效检索协议在应对数据可用性攻击时表现出色，但处理大型区块时编码解码复杂。Mitra等人[67]提出图编码Merkle树结构，用极化编码图提高大型区块应用中的数据可用性，解决了ACeD处理大型区块的问题，具有更好的DAA检测概率、通信成本和编码欺诈证明大小的可行性。

以太坊联合创始人Vitalik Buterin在其文章《区块链验证的哲学》中讨论到数据可用性问题。他指出，如果攻击者能够隐藏区块中的部分数据，无法获取或验证完整数据，轻节点可能接受无效的区块，导致其维护的区块链状态出现错误。当轻节点广泛存在错误状态时，整个网络的可信度和安全性都会受到质疑，用户可能失去对区块链系统的信任。

(2)状态更新欺诈攻击

状态更新欺诈攻击是利用区块链的不可篡改性和状态通道中参与者之间的信任缺陷进行的一种攻击。攻击者可以提交虚假状态更新，将包含错误状态的交易或状态更新提交至主链，企图将无效或恶意状态记录为合法状态，从而窃取资金或操控链上数据。在状态通道中，攻击者可能提交旧版或无效的状态快照，并声称该快照是最新状态，以此恶意回滚状态或窃取通道内的资产。虚假状态更新破坏了区块链上的数据一致性，可能导致智能合约或Layer 2链的运行出现异常。

Dziembowski等人[68]首次提出全面状态通道网络规范，允许在不依赖区块链交互下执行大量交易，通过虚拟通道和中介减少延迟和成本。他们[69]进一步提出支持多方虚拟状态通道的方案，允许无区块链交互创建和关闭通道，扩展应用范围，提高争议解决效率，并提供全面安全模型。Xu等人[70]提出无状态区块链系统SlimChain，采用部分Merkle trie结构更新状态根，通过离链存储和并行处理扩展交易，降低链上负载，减少存储需求和验证复杂度。文献[68-69]通过虚拟通道降低状态更新欺诈风险，但通道结构复杂、依赖中介可能增加协调成本；文献[70]的SlimChain更关注系统可扩展性和安全性。

状态更新欺诈攻击主要在区块链的Layer 2扩展方案中被讨论，由于Layer 2方案在设计时已经考虑了防范此类攻击的机制，实际发生的状态更新欺诈攻击案例较为罕见，随着区块链技术的不断发展和应用场景的增加，新的攻击手段还会层出不穷。因此，对于预防和应对潜在的状态更新欺诈攻击至关重要。

(3)强制退出攻击

强制退出攻击指的是攻击者利用通道协议的设计漏洞，采取单方面行动迫使另一方在不利情况下退出通道。这种攻击通常发生在通道关闭过程中，尤其是缺乏有效的争议解决机制时。在状态通道中，本应双方达成共识后提交最终状态进行结算。然而，攻击者可以伪造退出请求，声称自己拥有某个状态通道或Rollup链上的资产，从而夺取不属于自己的资产，或强迫合法用户重新提交状态证明，增加其Gas成本。攻击者还可以操纵退出过程，通过网络拥塞或操纵验证者，延迟或中断其他用户的退出请求，迫使用户支付更高的Gas费，并破坏系统的退出公平性。频繁的强制退出攻击可能导致区块链系统运行效率下降，影响用户体验。

为了有效抵御强制退出攻击，保护通道参与者的合法权益，可以采用无跳跃客户端规则、经济风险模型和

中国知网 https://www.cnki.net

条件最终化机制等策略。无跳跃客户端规则规定客户端在状态更新时必须遵循顺序原则，禁止连续签署两个更新，防止过时状态被恶意操纵。经济风险模型通过计算成本与收益的平衡点，优化协议设计，抑制强制退出行为。条件最终化机制确保在通道内对象达到预设条件之前，状态不会被最终确定，提高系统对过时状态的反应能力。此外，Coleman等人[71]提出的“惩罚过时状态协议”，在通道关闭或状态更新过程中，对提交过时状态的一方进行惩罚，增加恶意退出的风险成本。

Plasma是一种旨在提高以太坊网络可扩展性和效率的Layer 2解决方案，通过将交易处理转移到链下来实现这一目标。在Plasma协议中，用户可以在子链上自由地进行交易，当需要将资产从子链提取回主链时，可以利用退出机制来实现。由于Plasma协议中，退出请求通常设有挑战期，允许其他用户在此期间对可疑的退出提出挑战。攻击者可能利用用户的疏忽或网络延迟，在挑战期内未被发现，从而成功提取资产。Vitalik Buterin等以太坊核心开发者在技术讨论中提及此类攻击的可能性，并建议Layer 2层方案通过改进挑战机制和提高用户警觉性来防范此类风险。

### 3.2 侧链上的攻击及相应对策

（1）桥接合约攻击

桥接合约是跨链桥的核心部分，用于在不同区块链间转移资产和信息，它在主链和侧链上部署，实现资产安全跨链。工作流程包括资产锁定、目标链上铸造等值代币或解锁发送，以及验证交易有效性。桥接合约攻击是一种通过破坏或操纵跨链桥共识，使合约接受无效交易或阻止解锁，导致用户资产冻结、被盗或区块链互操作性受损的攻击手段，攻击者利用桥接合约中的漏洞，如权限管理不足、逻辑错误或初始化缺陷，以获取桥接合约的控制权，提取锁定资产或操控跨链流程或伪造跨链桥的消息或交易证明，使桥接合约接受无效的交易，从而窃取桥接合约锁定的资产或中断跨链交易。导致侧链上的资金在转移过程中被盗。

为应对桥接合约攻击风险，保障跨链桥稳定运行和用户资产安全，Zhang等人[72]提出Xscope自动化工具检测桥接合约安全漏洞。如图13所示，Xscope有运行时监控和离线分析两种模式，运行时监控检测安全属性并中止恶意请求，离线分析分析历史请求并警告可疑序列。Xie等人[73]提出zkBridge跨链桥接解决方案，利用零知识证明确保桥接正确性，降低链上验证成本，无需额外安全假设，降低桥接资产安全风险。文献[72]的Xscope依赖已知攻击模式识别，实时精准防护已知威胁，但对未知复杂攻击有局限；文献[73]的zkBridge提升安全性和跨链效率，尤其在防范侧链攻击方面出色。

2022年知名区块链游戏Axie Infinity的侧链Ronin Network遭遇了一次重大安全攻击，攻击者通过获取Ronin Network的桥接合约验证节点私钥，伪造交易，从Ronin Bridge中提取了17.36万枚以太币和2 550万枚USDC，总价值约6.15亿美元。此次事件引发了业界对跨链桥和桥接合约安全性的广泛讨论，强调了加强区块链基础设施安全的重要性。

（2）资产锁定攻击

资产锁定攻击是针对区块链和侧链的一种严重威胁，当用户尝试将一个区块链上的资产转移到另一个区块链时，资产原本应在源链上锁定，并在目标链上释放或铸造相应价值的代币。但攻击者会利用桥接合约中的时间锁机制故意延迟或中断交易，或者通过制造网络

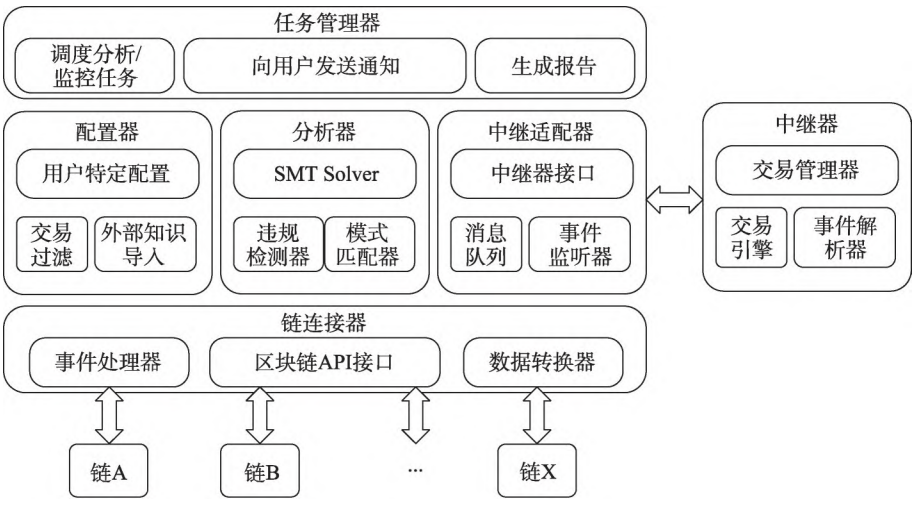


**图13 Xscope结构体系**

Fig.13 Architecture of Xscope

中国知网 https://www.cnki.net

拥堵、发送大量垃圾交易来降低区块链网络处理交易的速度，从而阻止资产按时解锁。这些手段不仅导致用户资产长时间被锁定、无法使用或交易，从而限制了资金流动性，还可能对整个区块链生态系统的稳定性带来重大风险。

在这一背景下，Herlihy[74]在其研究中首次系统地分析了原子跨链交换的理论基础，并提出了一个原子交换协议。该协议通过使用哈希时间锁合约来确保，如果所有参与方都遵循协议，那么所有的资产交换都将顺利进行；反之，如果某些联盟偏离协议，遵循协议的参与方也不会遭受损失。这一研究为跨链交易的安全性提供了理论保障，在源头上有效抵御资产锁定攻击。但文献[74]的研究仅限于强连通的有向图模型，未能涵盖包含序列交换和链下步骤的更一般情况。为了解决这种局限性，Shadab等人[75]提出了一个更为通用的跨链交易协议，即三阶段协议（three-phase protocol，3PP）。该协议不仅适用于强连通的交易图，还能够处理包含序列和链下步骤的交易，即使在交易图不是强连通的情况下。通过引入代表源点和汇点的概念，3PP协议确保了交易的一致性和端到端属性，即如果源点方支付，那么汇点方最终也会得到支付。此外，研究者还开发了一个名为XCHAIN的合成工具，该工具能够根据交易图的高级描述自动生成Solidity智能合约，进一步推动了跨链交易协议的实际应用。

2021年9月，SushiSwap的去中心化代币发行平台MISO遭遇了一次严重的安全事件。攻击者利用SushiSwap的MISO拍卖平台中的一个漏洞，锁定了平台上价值超过300万美元的ETH。项目方被迫与攻击者协商，最终通过回滚和补偿恢复系统。该攻击直接导致平台用户资金受到暂时影响，平台声誉严重受损。

### 3.3 Rollups上的攻击及相应对策

（1）欺诈证明攻击

欺诈证明攻击是针对乐观Rollups的一种攻击策略，攻击者利用并操纵欺诈证明机制，以破坏系统正常运行。攻击者能够通过提交伪造的欺诈证明，宣称链上某状态有误，进而阻断合法状态的更新并触发状态回滚。同时，攻击者可以利用验证流程中的漏洞，递交不完整或虚假的证明，以此骗取验证奖励并篡改系统状态。在欺诈证明的挑战环节，攻击者可能会抛出虚假挑战，以此延缓或阻断状态确认，致使网络运行受阻，妨碍合法状态的通过。随着区块链交易执行的转移至二层网络，欺诈证明攻击成为了Rollup生态系统中必须面对的安全威胁。

在乐观Rollups中，如Optimism和Arbitrum，采用了一种乐观机制，即除非有验证者提出异议，否则假定二层网络中的聚合器发布的交易数据是有效的[76]。这种机制虽然提高了效率，但也引入了潜在的欺诈风险。欺诈证明攻击发生在验证者检测到聚合器发布的交易数据与实际执行结果不一致时，此时验证者将触发一个争议阶段，以解决潜在的欺诈行为。在Optimism中，欺诈证明通过验证者部署与二层网络相同的智能合约，并提供交易的Merkle证明来验证聚合器发布的数据。如果发现欺诈行为，聚合器将被罚没保证金，利用经济激励机制确保其诚实性。Optimism的验证机制较为直接，依赖主链上的全局争议解决，但处理速度相对较慢。相较于Optimism，Kalodner等人[77]提出的Arbitrum采用了一种更为精细的争议解决机制。在Arbitrum中，争议解决过程通过一个迭代的多轮游戏来识别争议指令，并在主链上执行单步证明。这种方法不仅提高了争议解决的效率，还提供了一定程度的伪隐私性。

Arbitrum团队发现并披露了Optimism的OP Stack中存在的欺诈证明漏洞。该漏洞可能允许攻击者在挑战期内提交恶意交易，绕过欺诈证明机制，导致不正确的状态更新。如果漏洞被利用，攻击者可能在未经适当验证的情况下更改链上状态，影响系统的完整性和用户资产的安全。该研究表明欺诈证明攻击在区块链，特别是Layer 2解决方案中，具有现实威胁。

（2）经济激励攻击

经济激励攻击指攻击者通过操控或破坏Rollups等系统中的经济激励机制，以达到其干扰系统或谋取利益的目的。攻击者通过短期提供大量流动性，操控去中心化金融协议的奖励机制。垄断奖励分配。在奖励减少前迅速撤资，导致市场流动性崩溃。这种攻击的核心在于利用系统对参与者的经济激励来诱导验证者、矿工或其他系统参与者执行有利于攻击者的行为，是Rollups中面临的重要安全风险之一。

经济激励攻击揭示了Rollups等系统中经济激励机制的潜在安全风险。为了应对这些风险，Mamageishvili等人[78]提出了一种混合策略纳什均衡的解决方案。在这个框架下，验证者以一定的概率进行系统状态的检查，而这个概率取决于检查成本、潜在损失以及质押规模。通过调整这些参数，可以在一定程度上降低经济激励攻击的风险。研究者进一步分析了在不同参数设置下，系统的安全性如何变化，并为Rollup协议提供了最优验证者数量和质押规模的建议。这一研究为理解和防御经济激励攻击提供了重要的理论基础和实践指导。然而，目前针对这方面的研究仍较少。未来的研究可以在此基础上，结合金融领域的相关研究，进一步探

中国知网 https://www.cnki.net

索加权质押、动态激励调整等更复杂的激励策略，以更有效地应对不断演变的经济激励安全威胁。

2023年7月，Curve Finance遭遇了一次严重的安全事件，导致其创始人Michael Egorov面临巨额债务和潜在的清算风险。攻击者通过购买大量CRV代币操控Curve的治理，尝试通过不公平的提案增加自身收益。这次攻击对DeFi生态的公平性造成冲击，增加了治理机制中的投票成本。

(3)审查攻击

审查攻击是针对区块链网络中的交易处理的一种攻击方式，它涉及网络中的某些节点如矿工或验证者故意不处理或延迟处理某些交易。对于ZK-Rollup来说，审查攻击的威胁尤其值得关注，因为ZK-Rollup依赖于Layer 1来确认交易的最终性。如果Layer 1上的验证者或矿工进行审查，那么即使交易在Layer 2上已经处理，也可能无法及时或根本无法在Layer 1上得到确认。

Gorzny等人[79]提出了理想状态下的逃生舱，允许用户强制将交易包含在Rollup的状态中。这种机制通常涉及在底层区块链上执行交易，以确保即使Rollup运营商不在线或进行审查，用户的交易也能被处理。并允许用户通过强制交易包含机制提取他们的数字资产。这确保了即使Rollup运营商不合作，用户也能将他们的资产从Rollup中撤出。逃生舱机制确保了即使在面临审查攻击时，用户也能保持对资产的控制权，并能够将他们的资产安全地转移到更可靠的环境之中。

文献[79]提出的逃生舱机制增强了用户对资产的控制权和安全性。即使Rollup运营商不在线或试图进行审查，用户仍可通过底层区块链执行交易，从而确保其资产能够被安全提取。然而，该机制也存在一些缺点。首先，用户可能需要具备一定的技术知识以正确使用逃生舱，增加了操作复杂性。其次，在底层区块链上执行交易可能导致交易费用上升，尤其在高峰期，用户需承担额外的成本。未来研究中可以通过引入多重签名或去中心化自治组织来增强交易的透明性和安全性，进一步提升用户的安全感和信任度。

本章深入探讨了Layer 2技术的核心原理及其在实际中的应用，分析了状态通道、侧链和Rollups这三项关键技术。同时，分析了Layer 2在面对复杂多变的恶意交易和攻击时所面临的挑战，并综述了现有研究中关于状态通道、侧链以及Rollups的多种攻击模式及其相应的防御策略。如表4所示，总结每种攻击的主要特征，并归纳了研究人员提出的针对性防御方法。

**表4 Layer 2恶意攻击类型总结**

Table 4 Layer 2 summary of malicious attack types

| 攻击所在组件 | 攻击名称 | 攻击特征 | 预防措施 | 对区块链的危害性 |
|---|---|---|---|---|
| 状态通道 | 数据可用性攻击 | 通过恶意节点提供不完整或错误数据，破坏区块链的一致性和正确性 | 使用图编码梅克尔树、安装SSL证书并使用HTTPS协议 | 破坏数据的可用性，导致交易延迟或失败，影响区块链网络稳定性和交易处理能力 |
| | 状态更新欺诈攻击 | 提交过期或无效的状态更新以获取不当利益 | 确保状态通道中的状态更新具有时间戳验证和多方共识 | 破坏区块链状态的完整性，影响资产安全性和交易的可信性 |
| | 强制退出攻击 | 利用通道协议漏洞和关闭机制的时限压力，迫使受害者接受不利的结算条件 | 实施健壮的争议解决机制和延长挑战响应时间 | 破坏平台的安全性和可用性，降低用户的信任度 |
| 侧链 | 桥接合约攻击 | 通过破坏跨链桥的共识机制，操纵合约接受无效交易 | 增强桥接合约的安全性，确保跨链交易的共识机制健壮 | 破坏跨链资产转移的安全性，影响区块链网络的可信度和生态系统的稳定性 |
| | 资产锁定攻击 | 通过利用桥接合约的时间锁机制，制造网络拥堵阻止资产在目标链上解锁 | 优化桥接合约逻辑，增强网络交易处理能力，并设置合理的时间锁 | 导致用户资产丧失，影响用户资金的流动性和自由 |
| Rollups | 欺诈证明攻击 | 通过提交虚假证明操纵乐观Rollups的欺诈检测机制，干扰交易流程 | 提高证明难度，实施挑战期验证和采用先进的监控工具 | 破坏区块链交易的真实性和完整性，导致资产丧失、交易错误，影响区块链系统的信任和去中心化特性 |
| | 经济激励攻击 | 通过操纵Rollups系统中的经济激励，诱导系统参与者执行有利于攻击者的行为 | 设计鲁棒的经济模型和激励机制，确保系统参与者的奖励与系统整体利益一致 | 破坏去中心化治理结构，影响区块链的公正性、去中心化和治理透明度 |
| | 审查攻击 | 通过故意忽略或延迟处理特定交易阻碍Layer 2上的交易在Layer 1上得到及时确认 | 实施去中心化的验证者网络，加强监控和惩罚机制 | 影响区块链的交易可用性和流动性，阻碍区块链的正常运行 |

中国知网 https://www.cnki.net

## 4 Layer 3应用层的恶意交易与攻击

Layer 3应用层作为区块链技术的最前沿领域，涵盖了去中心化金融（decentralized finance，DeFi）、去中心化应用（decentralized applications，DApps）以及去中心化自治组织（decentralized autonomous organizations，DAOs），从而推动了区块链在多个行业的实际应用。

DeFi利用区块链和智能合约，提供了传统金融服务的去中心化替代方案。通过去中心化交易所、借贷平台和稳定币等应用，DeFi实现了无需信任的交易、借贷和价值存储。尽管DeFi具有开放性和透明度，但也面临着智能合约漏洞和市场波动等风险。如表5所示，总结了三个平台最受欢迎的五种加密货币去中心化交易场所。

**表5 最受欢迎的加密货币去中心化交易所总结**

Table 5 Summary of most popular cryptocurrency decentralized exchanges

| 平台 | 名称 | 交易总量（2024-01—2024-12） | 市场份额/% | 交易类型 |
|---|---|---|---|---|
| Ethereum | Uniswap v3 | $ 2 640亿 | 33 | Swap |
| | SushiSwap | $ 65亿 | 7 | Swap |
| BSC | PancakeSwap v2 | $ 178.8亿 | 12 | Swap |
| Solana | Raydium | $ 1 246亿 | 30 | Swap |
| | Orca | $ 126.4亿 | 9 | Orderbook |

DApps在区块链上运行，并通过智能合约实现自动化操作，其不可篡改性和去中心化特性确保了安全性和公正性。这些应用已在金融、游戏和社交网络等多个领域展现出广阔的发展前景。

而DAOs则利用智能合约和社区治理机制，实现了组织的自我管理和决策。它们的透明度和社区驱动性引入了一种新型的组织形式。然而，DAOs也面临着治理挑战和合约更新延迟等安全问题。

对Layer 3应用层的探索凸显了区块链技术在多样化应用中的潜力和挑战，同时也为区块链技术的未来发展方向和安全防护措施提供了重要的见解和指导。

### 4.1 去中心化金融中的攻击及相应对策

（1）抢先攻击

抢先攻击是一种在DeFi中频发的利用区块链交易延迟的恶意行为。攻击者通过监控区块链网络中的交易池，获取待确认交易的信息，以确定潜在的高收益交易并识别目标交易的关键参数。接着根据这些信息提交相似但优先级更高的交易，如支付更高的Gas费，从而使攻击者的交易先于目标交易执行，进而改变目标交易的执行结果或使其失败。抢先攻击会导致市场价格短期失真、大额交易成本增加、用户信任下降，还可能引发网区块链络拥堵和交易成本上升，威胁区块链生态系统健康。

Daian等人[80]从理论角度分析去中心化交易所中的抢先攻击问题，提出优先气体拍卖（priority gas auctions，PGAs）和矿工可提取价值概念。Torres等人[81]通过实证研究，对以太坊区块链上的抢先攻击进行大规模数据分析，识别出近20万次攻击事件，攻击者获利超1 841万美元。Kelkar等人[82]定义顺序公平性并提出Aequitas共识协议，通过广播、协议和最终确定三个阶段确保交易顺序公平性。

2024年4月，未经验证的Ember Sword NFT拍卖合约被发现存在抢先漏洞，攻击者通过监控拍卖过程，提前提交更高出价的交易，获取拍品。合法用户的出价被抢先，需要不断提高出价或Gas费，才能竞争拍品。这种行为破坏了拍卖的公平性，增加了其他用户的参与难度，使得用户对区块链的透明性和可靠性产生质疑。

（2）三明治攻击

三明治攻击是抢跑攻击的一种复杂形式，基本步骤包括监控交易池、前置交易、用户交易执行和后置交易。首先，攻击者会监控区块链网络中的内存池，寻找尚未打包进区块的待处理交易。发现目标交易后，攻击者会立即提交一笔高额Gas费用的交易，以确保在目标交易之前被矿工优先打包。随后，目标用户的交易按原计划执行，但由于价格已被前置交易影响，用户的交易将以不利的价格进行。最后，在用户交易之后，攻击者会立即执行一笔反向交易，利用市场价格可能的恢复来获利。

Heimbach等人[83]通过引入博弈论中的三明治游戏来分析三明治攻击，并从攻击者和受害者的角度提供了深入的分析。他们提出了一个简单而有效的算法，帮助交易者设置滑点容忍度，在避免三明治攻击的同时，降低交易失败的风险。该研究为理解三明治攻击的动机和潜在防御策略提供了理论基础，也为后续的技术实现和优化提供了重要的背景信息。在Heimbach的理论分析基础上，Li等人[84]将理论转化为实际的系统改进，提出了一种基于Geth的实时检测系统，用于检测以太坊中的三明治攻击。该系统通过分析交易数据流，能够在区块内进行实时交易分析，快速有效地识别异常模式和潜在的攻击行为。在保持全节点正常运行速度的同时，准确检测区块内的三明治攻击交易。该方法的有效性依赖于准确的数据流分析和系统性能，可能面临实现上的复杂性与挑战。

2024年6月，Solana区块链上发生了一起引人注目的三明治攻击事件，一个被称为“arsc”的MEV机器人在

中国知网 https://www.cnki.net

两个月内通过三明治攻击获利约3 000万美元。在短短20 min内，该机器人进行了494笔交易，盈利约16个SOL，当时约合2 400美元。频繁的三明治攻击导致用户交易成本增加，交易体验下降，该事件引发了区块链社区的强烈不满，呼吁在Solana链上采取措施限制此类行为。

(3)闪电贷攻击

闪电贷攻击是一种新型金融攻击手段，在DeFi生态系统中，闪电贷攻击利用闪电贷的无抵押特性和单交易原子性，攻击者在单个交易中借入大量资金，通过操纵市场价格、利用智能合约漏洞或触发清算机制，执行一系列恶意操作以获取不正当利益。攻击通常包括借入闪电贷、操控市场价格或协议逻辑，实现套利或资产转移，并在交易末尾偿还贷款以完成原子性操作。这种攻击因其复杂性和快速性，能够绕过常规防御，导致DeFi协议资金损失、市场价格异常波动及用户信任受损。

Qin等人[85]首次探讨了交易原子性和闪电贷对DeFi生态系统的影响。通过分析具体的攻击案例，展示了攻击者如何利用闪电贷进行获利，并提出了一个优化问题框架，用于计算攻击参数，可以帮助攻击者或防御者预测和优化攻击策略。区别于Qin等人的理论分析和优化模型构建，Cao等人[86]的研究则提供了一个实际的工具来观察和解释闪电贷攻击的微观过程。提出的Flashot模型，针对每个闪电贷事件提供了一个能够透明地说明智能合约中精确资产流动的标准图表，以直观的方式来展示闪电贷攻击中的资产流动。文献[85-86]有助于后续研究者逐步从基础到高级，全面了解闪电贷攻击的复杂性及其对DeFi生态系统的影响。文献[85]的理论研究虽然提供了攻击参数的优化框架，但忽略了实际环境中的复杂性，如市场动态、流动性限制等，这可能导致理论模型与现实情况之间存在差距。文献[86]提出的Flashot模型在可视化和实时监控方面表现出色，但模型比较依赖准确的数据输入，且在高频交易环境中，实时分析和展示的性能可能会受到限制。

2021年1月，DeFi协议Alpha Homora遭遇了一次严重的闪电贷攻击，攻击者发现Alpha Homora协议中的漏洞，能够在无足够抵押的情况下借出大量sUSD等资产。他们将获取的sUSD作为抵押物，在Iron Bank上借出更多资金。通过重复上述步骤，攻击者多次借贷，最终从Iron Bank中提取了大量资金。频繁的安全事件使用户对DeFi协议的安全性产生质疑，导致用户流失。

## 4.2 去中心化应用中的攻击及相应对策

(1)钓鱼攻击

钓鱼攻击是一种社会工程手段，如图14所示，攻击者常见手段包括伪造与真实平台高度相似的网站或应用程序，通过电子邮件、短信或社交媒体发送虚假信息引导用户点击恶意链接，发布假冒的智能合约或DApp诱导授权，甚至假扮客服或管理员获取用户信任。钓鱼攻击利用用户的信任和安全意识不足，窃取敏感数据并非法访问用户资产，导致资金损失和平台声誉受损。

随着区块链技术发展，以太坊平台钓鱼攻击问题凸显。Chen等人[87]提出基于交易监控的钓鱼攻击检测系统，通过分析交易记录、构建交易图、提取节点特征训练

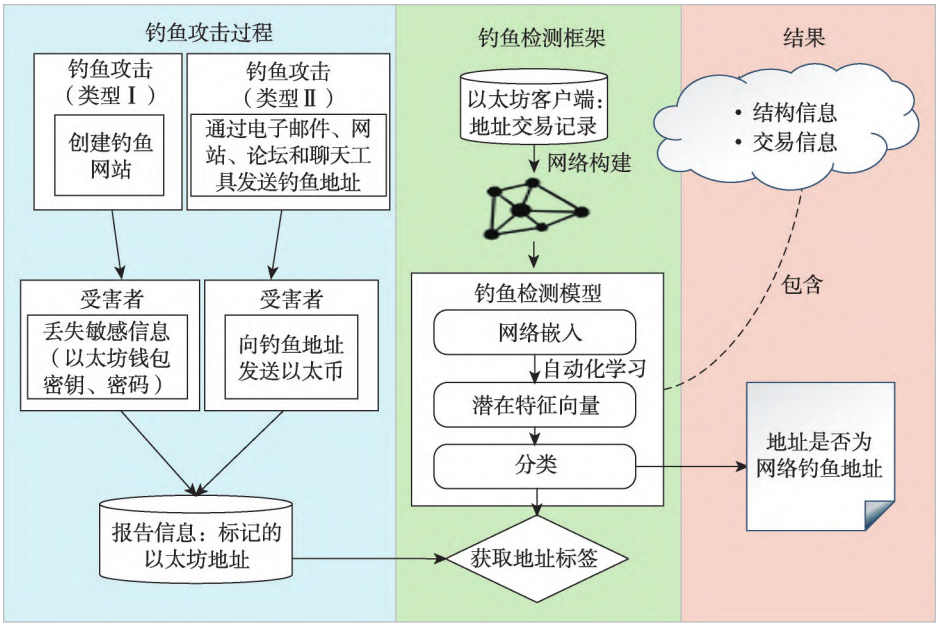


**图14 以太坊中的钓鱼攻击及检测过程**

Fig.14 Phishing attacks and detection process in Ethereum

中国知网 https://www.cnki.net

模型,实时识别钓鱼行为。Wu等人[88]探索网络嵌入技术在钓鱼攻击检测中的应用,提出新方法,提取地址特征并用无监督学习提高检测准确性。该方法爬取标记钓鱼地址,重建交易网络,用trans2vec算法提取特征,再用单类支持向量机(support vector machine,SVM)分类节点。与文献[87]的实时分析方法相比,文献[88]的无监督学习方法在处理数据不平衡、适应数据变化、发现新攻击模式及降低误报等方面优势明显,尤其适用于标签数据难获取或数据分布变化场景。

2024年12月,Ledger硬件钱包用户遭遇钓鱼诈骗,攻击者伪造了Ledger的支持电子邮件,声称公司发生了数据泄露事件,并要求用户验证其恢复短语。这些欺诈邮件实际上是通过邮件营销平台发送的,邮件中的链接指向了伪装成Ledger官方网站的钓鱼网站。当用户在这些钓鱼网站上输入其种子短语后,攻击者便能够完全控制用户的钱包,并将资金转移走。

(2)依赖性攻击

依赖性攻击是一种针对软件开发中使用的外部库或第三方依赖项的攻击。应用层中的DApps通常依赖开源库、智能合约模板和其他第三方组件来实现功能。攻击者通过篡改区块链项目中使用的外部依赖如在第三方库、模块或插件中,植入恶意代码来实现攻击。常见方法包括篡改已存在的依赖包、发布与合法依赖名称相似的恶意包、获取依赖维护权后发布恶意更新,或利用依赖版本冲突破坏系统功能。攻击者通过这些方式窃取敏感数据、操控智能合约或破坏系统功能,导致用户资产被盗、服务中断或生态系统信任受损。

Birsan[89]研究发现npm、pip和gem等包管理生态系统存在依赖混淆攻击。若公司私有仓库的内部包名与公共仓库包名相同,攻击者可上传同名恶意包至公共仓库执行恶意代码,Birsan借此成功入侵多家知名公司。为防御此攻击,未来研究可集中于严格依赖管理策略,包括实施严格包版本控制、维护依赖列表、利用包签名验证真实性及定期自动化安全扫描。

在去中心化交易所中,依赖性漏洞可能导致严重的安全问题。2024年7月,去中心化AI项目Bittensor遭遇攻击,一些用户的钱包被盗,损失约800万美元。研究人员分析,此次攻击可能是由于恶意的Bittensor软件包被上传到Python的PyPi软件包管理器,用户在不知情的情况下下载并使用了该恶意软件包,导致私钥泄露和资金被盗。

### 4.3 去中心化自治组织中的攻击及相应对策

(1)治理攻击

治理攻击是一种针对DAO的恶意行为,通过操纵或滥用治理机制以获取非法利益。攻击巧妙利用了DAO的开放与去中心化特性,通过投票权操纵,即攻击者通过大量收购治理代币临时掌控投票权,强行推动有利于自身的提案;恶意提案,即提出表面合理却暗藏恶意的提案,诱使DAO成员在未经深思熟虑的情况下予以通过;以及贿赂投票,即通过直接或间接的经济利益诱惑DAO成员支持特定提案。这些攻击行为不仅严重损害DAO本身,还可能波及整个区块链生态系统,引发市场动荡。

随着区块链技术发展,以太坊平台治理攻击问题凸显,威胁去中心化金融生态系统安全。Mehar等人[90]深入分析DAO攻击事件,回顾DAO创建、攻击过程及以太坊社区反应,引发对区块链不可篡改性和“代码即法律”原则的反思,揭示治理攻击机制和风险。Wang等人[91]提出五层参考模型描述DAO架构,通过交易图谱和级联特征提取技术,结合轻量级梯度提升机的双采样集成算法,开发实时监控和预警治理攻击的系统,提高检测准确性和鲁棒性。

2020年10月,MakerDAO经历了一次治理攻击事件,部分大户利用投票权提议分配高额奖励给自己,导致治理机制受到质疑。当治理制度无法平衡参与者的权利和义务时,治理权利便会流向操控者手中,使得区块链网络的去中心化特性被削弱,影响区块链生态系统的长期发展。

(2)合约审查延迟攻击

合约审查延迟攻击是针对DAO的一种恶意策略,攻击者通过大量提交无实质性内容或极端复杂的提案,蓄意扰乱DAO的正常提案审议流程。迫使DAO的核心管理层及社区成员将时间与资源耗费在处理这些无效或偏离主题的提案上,进而严重滞后了关键合约的审查进度。当DAO内发现核心合约存在安全漏洞时,该攻击可能故意阻碍针对漏洞修复的提案获得及时通过,使系统持续处于易受攻击的状态,加剧了安全风险。

为应对DAO无法迅速响应安全威胁或市场动态导致治理代币价值受损、动摇市场信心的问题,有效防范和应对合约审查延迟攻击至关重要。Rikken等人[92]提出一个多层次的区块链治理框架,涵盖基础设施层、应用层、公司层和机构层,强调各层次治理挑战的相互关联性,指出某层面治理决策可能显著影响其他层面。为应对合约审查延迟攻击,他们在智能合约编写中引入互斥锁机制,防止攻击者利用合约重新进入实施攻击。但该框架在实际应用中可能面临治理决策协调复杂性及不同利益方潜在冲突,互斥锁使用也可能降低合约执行灵活性、增加合约复杂性,引发性能问题。

中国知网 https://www.cnki.net

本节内容分析了区块链Layer 3应用层在去中心化金融、去中心化应用及去中心化自治组织所面临的潜在安全威胁,并在此基础之上,系统性地整合与归纳了现有研究中的防御策略。如表6所示,针对应用层遭受的各类攻击,概述了各种攻击的攻击特征,并总结了研究人员提出的相应抵御方法。

## 5 挑战与未来展望

### 5.1 问题与挑战

当前区块链四层架构的研究与应用已取得显著进展。然而,随着区块链技术在不同领域的广泛应用,其架构规模不断扩大,功能和逻辑日益复杂化,所面临的挑战也愈加多样化。这种复杂性不仅增加了各层之间的相互依赖和协调难度,还在硬件、共识机制、智能合约等多方面带来了诸多安全性挑战。

后量子密码学算法在区块链设备中的高功耗问题。区块链设备中已经开始引入后量子密码学算法,以应对未来量子计算带来的安全威胁。这些算法在区块链节点、智能合约、区块链钱包和共识机制中得到了广泛应用,确保了区块链系统的安全性和效率。随着技术的不断发展,后量子密码学算法将在区块链设备中发挥越来越重要的作用。但由于后量子密码学算法通常比传统加密算法计算复杂度更高,如基于格的系统中采样与多项式运算能耗较高,显著增加资源受限设备的功耗,需优化以降低能耗。这些算法还通常需要更大的密钥和签名尺寸,增加了存储需求,对存储空间有限的区块链设备构成挑战,需优化存储管理以减少开销。

确认延迟和低区块出块速度。部分共识机制存在着交易确认速度缓慢的问题。以工作量证明(PoW)机制为例,交易需历经多个区块的逐一确认,才能被视为真正不可篡改。然而,这一冗长的区块确认流程,为攻击者提供了可乘之机。他们可能在这段时间内,针对同一资产在不同交易中进行重复操作,并企图在主链上散布虚假交易信息,或是构建出更长的替代链条,从而大大增加了双花攻击的风险与可行性。研究人员通过改进共识机制算法以解决确认延迟和低区块出块速度的问题,但也引入了一些新的问题,如改进的共识算法通常更复杂,涉及更多参数和机制,增加了实现和维护的难度,与现有的区块链基础设施不兼容等问题。

代理合约模式的复杂性与安全隐患。在智能合约的升级机制中,代理合约模式被广泛采用,通过将逻辑合约和数据合约分离来实现可升级性。代理合约作为用户的交互入口,负责将调用请求转发至逻辑合约,而逻辑合约的升级无需影响数据合约的状态。然而,代理

**表6 Layer 3恶意攻击类型总结**

Table 6 Layer 3 summary of malicious attack types

| 攻击所在组件 | 攻击名称 | 攻击特征 | 预防措施 | 对区块链的危害性 |
|---|---|---|---|---|
| 去中心化金融 | 抢先攻击 | 攻击者监控内存池,发现有利交易,便提交类似交易并支付更高费用以确保优先处理 | 提高交易的隐私性,实施交易排序算法,增加交易费用的不确定性 | 导致用户的交易失败或以不利价格执行,影响区块链交易的效率和公平性 |
| | 三明治攻击 | 在用户交易前后提交两笔交易,通过控制价格差异从中获利,用户的交易以不利价格执行 | 限制Gas费用,避免低流动性池,小额交易 | 导致用户遭遇不公价格执行,损害区块链平台的透明度和市场效率 |
| | 闪电贷攻击 | 攻击者通过借入大量资金,在同一笔交易中利用这些资金进行市场操纵或其他恶意操作,然后归还借款,从而获得利润 | 使用可靠的价格预言机,限制交易量,引入时间锁定机制,引入滑点保护机制 | 破坏市场稳定性,导致资产价格剧烈波动,可能导致大量资金被窃取 |
| 去中心化应用 | 钓鱼攻击 | 攻击者通过伪装成可信赖的实体,诱骗用户提供敏感信息如用户名、密码、信用卡详情等 | 启用双因素认证,使用强密码,警惕可疑邮件和链接 | 破坏区块链的机密性和完整性,影响平台信誉,可能导致平台用户流失 |
| | 依赖性攻击 | 攻击者发布或更新含恶意代码的库,开发者一旦集成,恶意代码即被执行,导致私钥被盗、交易篡改 | 隔离关键系统,建立安全依赖策略,设计高可用性和冗余系统 | 破坏智能合约的执行逻辑,导致智能合约功能异常或资产损失,影响区块链平台的安全性和可用性 |
| 去中心化自治组织 | 治理攻击 | 攻击者通过操纵治理提案的投票过程,或者利用治理规则中的漏洞来实现对协议控制权的非法获取 | 强化治理规则,提高社区成员参与度,建立紧急响应机制 | 破坏区块链的去中心化特性,影响治理决策的公正性,可能导致区块链平台治理机制失效或不公平的决策 |
| | 合约审查延迟攻击 | 攻击者利用合约审查交易执行顺序的漏洞,通过构造一系列交易,使得自己的交易在审查过程中被优先处理 | 限制交易的频率,增加交易的复杂度,检查交易的返回值,优化交易池的管理机制 | 导致交易执行延迟,影响市场稳定性和区块链的运行效率 |

中国知网 https://www.cnki.net

合约模式的引入也带来了额外的系统复杂性，增加了开发、审计和调试的难度，同时还可能引发安全隐患，如调用上下文丢失或恶意逻辑合约的替换问题。因此，未来研究需要探索一种高效安全的代理合约模式，既满足智能合约的升级需求，又能有效降低系统复杂性。

Rollups的状态增长隐患。状态增长问题是区块链网络中节点必须持续存储和管理的数据量不断增加的现象。随着状态持续增长，查询指定状态片段的时间会变得更长。这是因为当前merkle patricia trie会在满足“节点只有一个子节点”的条件时使用“快捷方式”，如果状态越来越满，可用的“快捷方式”也就会越来越少，从而影响状态访问效率。

## 5.2 未来展望

针对区块链四层架构中现阶段的不足，通过总结已有研究成果，本文提出了在该领域未来可能的研究方向和发展趋势。

后量子密码学的低功耗设计。选择适合区块链设备的后量子密码学算法是实现低功耗设计的第一步。对于资源极其有限的区块链设备，可以使用轻量级的哈希签名方案，如XMSS或SPHINCS+的简化版本。对于资源较多的区块链设备，可以使用更复杂的后量子密码学算法，如Kyber或Dilithium，再对其进行适当的优化。选择合适的算法参数，以在安全性和效率之间取得平衡，并简化算法的某些步骤，减少不必要的计算。同时，利用专用硬件加速器来提高后量子密码学算法的执行效率，从而降低功耗。如，使用现场可编程门阵列或专用集成电路来实现后量子密码学算法的硬件加速。这些硬件可以高效执行复杂的数学运算，减少CPU的负担，从而降低功耗。使用低功耗的逻辑门和存储单元，可以优化电源管理策略，确保硬件在不使用时进入低功耗模式。

动态块时间和自适应出块速度。传统工作量证明（PoW）系统通常采用固定的出块时间，如比特币的10 min，但这种机制在应对网络交易量和算力波动等变化时显得不足。未来可以探索通过引入强化学习中的Q-Learning算法，可以动态调整出块时间，提高系统适应性和效率。Q-Learning通过交互学习“状态-动作”对的价值函数，在特定状态下选择最优动作。在PoW系统中，状态可以定义为网络交易量、算力波动、区块大小等，动作则为调整出块时间的策略。算法通过状态感知与动作选择、合理的奖励机制设计以及Q值函数的持续优化，逐步学会最优调整策略。在高交易量时缩短出块时间以缓解拥堵，在算力波动时延长出块时间以减少资源浪费。借助Q-Learning的自适应能力，PoW系统能在长期运行中不断优化策略，实现更智能的动态调整方案，突破传统固定机制的局限性，为区块链技术开辟新的发展方向。

增强代理合约模式的安全性与效率。代理合约模式的复杂性和潜在安全隐患需要通过优化设计和改进应用加以解决。首先需要对架构进行改进设计，通过减少冗余逻辑、采用高效的调用转发机制以及简化合约路径，可以显著提升调用效率和整体性能。同时，引入存储分层设计能够有效降低状态访问的资源消耗，从而增强系统的运行效率。此外，形式化验证工具的使用是保障安全性的核心措施，包括验证调用上下文的完整性、预防逻辑替换攻击，以及确保逻辑与数据合约行为一致性。结合模拟多种攻击场景的方式，可以在早期识别并修复潜在漏洞，从而进一步提升安全性。为了降低开发与调试的复杂性，开发模块化的代理合约模板以及直观的框架与工具链至关重要。这些工具不仅能简化开发者的工作流程，还可以通过一键部署与升级功能提升操作效率。通过这些优化措施，代理合约模式将在性能与安全性上取得平衡，为智能合约的持续创新和发展提供可靠的技术支持。

Verkle树的无状态客户端恒定大小证明方案。在以太坊等区块链系统中，Verkle树的引入为实现无状态客户端提供了一种创新方案。这种方案的核心在于无需客户端存储整个状态数据库即可验证区块的完整性和合法性。Verkle树通过向量承诺技术取代传统的哈希函数，显著优化了证明的大小。无论树的宽度如何增加，Verkle树的证明大小始终保持恒定，从而降低了验证过程对带宽和存储资源的需求。这一特性对于扩展区块链系统的可用性具有重要意义，使得资源受限的设备（如轻节点或移动终端）也能高效参与网络验证。未来的研究可以进一步探索优化Verkle树在实际应用中的性能，通过优化树结构的节点更新算法，如开发更加高效的增量更新方法，仅对发生变化的节点进行选择性修改，而无需重新计算整棵树。此外，结合缓存机制，通过存储和复用高频访问节点的中间状态，可以显著减少重复计算带来的资源消耗。探索新的承诺方案或混合模型，降低更新过程中承诺生成和验证的计算复杂度，也将进一步提高效率。在实际部署中，开发自动化工具链以简化Verkle树的动态管理，能够帮助节点快速适应变化的区块链环境。这些优化策略不仅有助于提升Verkle树的更新效率，还能推动无状态区块链技术的广泛应用，为区块链网络的扩展性和易用性提供更强大的支持。

中国知网 https://www.cnki.net

## 6 结束语

区块链技术作为一项颠覆性创新，以其独特的去中心化特性和不可篡改的数据结构，为金融交易、供应链管理、版权保护等众多领域带来了革命性的变革。然而，随着区块链技术的广泛应用，伴随而来的安全问题也日益凸显，尤其是区块链平台的漏洞和攻击手段层出不穷，严重威胁着系统的整体安全性。因此，区块链安全防护技术，特别是针对恶意交易和潜在漏洞的检测技术，已经成为学术界和工业界研究的热点。本文系统地回顾了区块链安全领域的研究进展，探索了该领域的研究现状、研究不足以及未来趋势。希望本文能帮助未来研究者更好地理解和应对区块链技术在不同层次上可能遇到的恶意交易和攻击。

## 参考文献：


[1] SAAD M, SPAULDING J, NJILLA L, et al. Exploring the attack surface of blockchain: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1977-2008.

[2] LIN I C, LIAO T C. A survey of blockchain security issues and challenges[J]. International Journal of Network Security, 2017, 19(5): 653-659.

[3] CONTI M, KUMAR E S, LAL C, et al. A survey on security and privacy issues of Bitcoin[J]. IEEE Communications Surveys & Tutorials, 2018, 20(4): 3416-3452.

[4] ZAGHLOUL E, LI T T, MUTKA M W, et al. Bitcoin and blockchain: security and privacy[J]. IEEE Internet of Things Journal, 2020, 7(10): 10288-10313.

[5] AGGARWAL S, KUMAR N. Attacks on blockchain[J]. Advances in Computers, 2021, 121: 399-410.

[6] WEN Y J, LU F Y, LIU Y F, et al. Attacks and countermeasures on blockchains: a survey from layering perspective[J]. Computer Networks, 2021, 191: 107978.

[7] CERF V, KAHN R. A protocol for packet network intercommunication[J]. IEEE Transactions on Communications, 1974, 22(5): 637-648.

[8] 王群, 李馥娟, 倪雪莉, 等. 域间路由安全增强及区块链技术的应用研究[J]. 计算机科学与探索, 2024, 18(12): 3144-3174.
WANG Q, LI F J, NI X L, et al. Research on blockchain-based inter-domain routing security enhancement[J]. Journal of Frontiers of Computer Science and Technology, 2024, 18 (12): 3144-3174.

[9] POSTEL J. RFC768: User datagram protocol[S]. Internet Society, 1980: 1-3.

[10] TRAMÈR F, BONEH D, PATERSON K. Remote side-channel attacks on anonymous transactions[C]//Proceedings of the 29th USENIX Security Symposium, 2020: 2739-2756.

[11] MITSEVA A, PANCHENKO A, ENGEL T. The state of affairs in BGP security: a survey of attacks and defenses[J]. Computer Communications, 2018, 124: 45-60.

[12] APOSTOLAKI M, ZOHAR A, VANBEVER L. Hijacking Bitcoin: routing attacks on cryptocurrencies[C]//Proceedings of the 2017 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2017: 375-392.

[13] SENTANA I, IKRAM M, KAAFAR M. BlockJack: towards improved prevention of IP prefix hijacking attacks in inter-domain routing via blockchain[C]//Proceedings of the 18th International Conference on Security and Cryptography, 2021: 674-679.

[14] ZLOMISLIĆ V, FERTALJ K, SRUK V. Denial of service attacks, defences and research challenges[J]. Cluster Computing, 2017, 20(1): 661-671.

[15] ZARGAR S T, JOSHI J, TIPPER D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks[J]. IEEE Communications Surveys & Tutorials, 2013, 15(4): 2046-2069.

[16] LAI G H, CHEN C M, JENG B C, et al. Ant-based IP traceback[J]. Expert Systems with Applications, 2008, 34(4): 3071-3080.

[17] RAIKWAR M, GLIGOROSKI D. DoS attacks on blockchain ecosystem[C]//Proceedings of the European Conference on Parallel Processing. Cham: Springer, 2021: 230-242.

[18] FANG L M, ZHAO B, LI Y, et al. Countermeasure based on smart contracts and AI against DoS/DDoS attack in 5G circumstances[J]. IEEE Network, 2020, 34(6): 54-61.

[19] JIA B, LIANG Y Q. Anti-D chain: a lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain[J]. China Communications, 2020, 17(9): 11-24.

[20] ABOU EL HOUDA Z, HAFID A S, KHOUKHI L. Cochain-SC: an intra-and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract[J]. IEEE Access, 2019, 7: 98893-98907.

[21] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse attacks on Bitcoin's peer-to-peer network[C]//Proceedings of the 24th USENIX Security Symposium, 2015: 129-144.

[22] XU G Q, GUO B J, SU C H, et al. Am I eclipsed? A smart detector of eclipse attacks for Ethereum[J]. Computers & Security, 2020, 88: 101604.

[23] ALANGOT B, REIJSBERGEN D, VENUGOPALAN S, et al. Decentralized and lightweight approach to detect eclipse attacks on proof of work blockchains[J]. IEEE Transactions on Network and Service Management, 2021, 18(2): 1659-1672.

[24] VINTA S R, PATEL S A, SAMEEN A Z, et al. Dynamic defense model against eclipse attacks in proof-of-work blockchain systems[J]. Procedia Computer Science, 2024, 235: 1202-1212.

[25] DOUCEUR J R. The Sybil attack[C]//Proceedings of the


中国知网 https://www.cnki.net

International Workshop on Peer-to-Peer Systems. Berlin, Heidelberg: Springer, 2002: 251-260.

[26] WANG Y T, TAN M S. Defense against Sybil attack in blockchain based on improved consensus algorithm[C]// Proceedings of the 2023 IEEE International Conference on Control, Electronics and Computer Technology. Piscataway: IEEE, 2023: 986-989.

[27] SWATHI P, MODI C, PATEL D. Preventing Sybil attack in blockchain using distributed behavior monitoring of miners [C]//Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies. Piscataway: IEEE, 2019: 1-6.

[28] DAVIS C R, FERNANDEZ J M, NEVILLE S, et al. Sybil attacks as a mitigation strategy against the storm botnet[C]// Proceedings of the 2008 3rd International Conference on Malicious and Unwanted Software. Piscataway: IEEE, 2008: 32-40.

[29] 王群, 李馥娟, 王振力, 等. 区块链原理及关键技术[J]. 计算机科学与探索, 2020, 14(10): 1621-1643.
WANG Q, LI F J, WANG Z L, et al. Principle and core technology of blockchain[J]. Journal of Frontiers of Computer Science and Technology, 2020, 14(10): 1621-1643.

[30] MERKLE R C. Protocols for public key cryptosystems[C]// Proceedings of the 1980 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 1980: 122.

[31] 刘哲旭, 李雷孝, 刘东江, 等. 智能合约漏洞检测与修复研究综述[J]. 计算机科学与探索, 2025, 19(4): 854-876.
LIU Z X, LI L X, LIU D J, et al. Review of smart contract vulnerability detection and repair research[J]. Journal of Frontiers of Computer Science and Technology, 2025, 19(4): 854-876.

[32] BUTERIN V. A next-generation smart contract and decentralized application platform[J]. Ethereum White Paper, 2014, 3(37): 1-36.

[33] GAROFFOLO A, STABILINI P, VIGLIONE R, et al. A penalty system for delayed block submission[J]. Horizen, 2018: 1-7.

[34] YANG X L, CHEN Y, CHEN X H. Effective scheme against 51% attack on proof-of-work blockchain with history weighted information[C]//Proceedings of the 2019 IEEE International Conference on Blockchain. Piscataway: IEEE, 2019: 261-265.

[35] APONTE-NOVOA F A, OROZCO A L S, VILLANUEVA-POLANCO R, et al. The 51% attack on blockchains: a mining behavior study[J]. IEEE Access, 2021, 9: 140549-140564.

[36] EYAL I, SIRER E G. Majority is not enough[J]. Communications of the ACM, 2018, 61(7): 95-102.

[37] GÖBEL J, KEELER H P, KRZESINSKI A E, et al. Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay[J]. Performance Evaluation, 2016, 104: 23-41.

[38] YANG R K, CHANG X L, MIŠIĆ J, et al. Assessing blockchain selfish mining in an imperfect network: honest and selfish miner views[J]. Computers & Security, 2020, 97: 101956.

[39] MADHUSHANIE N, VIDANAGAMACHCHI S, ARACHCHILAGE N. BA-flag: a self-prevention mechanism of selfish mining attacks in blockchain technology[J]. International Journal of Information Security, 2024, 23(4): 2783-2792.

[40] CHEN Y G, YANG L, TIAN L W. A study of orphan blocks in public blockchain[C]//Proceedings of the 2022 IEEE 2nd International Conference on Data Science and Computer Application. Piscataway: IEEE, 2022: 220-223.

[41] JHA B, DAS B. The study of the issues related to orphan blocks[C]//Proceedings of International Conference on Computational Intelligence, Data Science and Cloud Computing. Singapore: Springer, 2022: 355-363.

[42] SOLAT S, POTOP-BUTUCARU M. Brief announcement: zeroblock: timestamp-free prevention of block-withholding attack in Bitcoin[C]//Proceedings of the 19th International Symposium on Stabilization, Safety, and Security of Distributed Systems. Cham: Springer, 2017: 356-360.

[43] MASTEIKA S, REBŽDYS E, DRIAUNYS K, et al. Bitcoin double-spending risk and countermeasures at physical retail locations[J]. International Journal of Information Management, 2024, 79: 102727.

[44] WANG J L, LIU Q, SONG B Y. Blockchain-based multi-malicious double-spending attack blacklist management model [J]. The Journal of Supercomputing, 2022, 78(12): 14726-14755.

[45] ZHENG J, HUANG H W, LI C L, et al. Revisiting double-spending attacks on the Bitcoin blockchain: new findings [C]//Proceedings of the 2021 IEEE/ACM 29th International Symposium on Quality of Service. Piscataway: IEEE, 2021: 1-6.

[46] FEIST J, GRIECO G, GROCE A. Slither: a static analysis framework for smart contracts[C]//Proceedings of the 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain. Piscataway: IEEE, 2019: 8-15.

[47] WANG W, SONG J J, XU G Q, et al. ContractWard: automated vulnerability detection models for ethereum smart contracts[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(2): 1133-1144.

[48] HE Y Q, DONG H J, WU H G, et al. Formal analysis of reentrancy vulnerabilities in smart contract based on CPN [J]. Electronics, 2023, 12(10): 2152.

[49] LIU Z G, QIAN P, WANG X Y, et al. Combining graph neural networks with expert knowledge for smart contract vulnerability detection[J]. IEEE Transactions on Knowledge and Data Engineering, 2021, 35(2): 1296-1310.

[50] ZHANG L J, CHEN W J, WANG W Z, et al. CBGRU: a detection method of smart contract vulnerability based on a

中国知网 https://www.cnki.net

hybrid model[J]. Sensors, 2022, 22(9): 3577.
[51] NIKOLIĆ I, KOLLURI A, SERGEY I, et al. Finding the greedy, prodigal, and suicidal contracts at scale[C]//Proceedings of the 34th Annual Computer Security Applications Conference. New York: ACM, 2018: 653-663.
[52] RODLER M, LI W, KARAME G O, et al. Sereum: protecting existing smart contracts against re-entrancy attacks[EB/OL]. [2024-10-04]. https://arxiv.org/abs/1812.05934.
[53] KALRA S, GOEL S, DHAWAN M, et al. ZEUS: analyzing safety of smart contracts[C]//Proceedings of the 2018 Network and Distributed System Security Symposium, 2018: 1-12.
[54] YANG H, HUANG L Q, LUO C F, et al. Research on intelligent security protection of privacy data in government cyberspace[C]//Proceedings of the 2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics. Piscataway: IEEE, 2020: 284-288.
[55] XU Y J, HU G R, YOU L, et al. A novel machine learning-based analysis model for smart contract vulnerability[J]. Security and Communication Networks, 2021, 2021(1): 5798033.
[56] JIAO T Y, XU Z Y, QI M F, et al. A survey of ethereum smart contract security: attacks and detection[J]. Distributed Ledger Technologies: Research and Practice, 2024, 3(3): 1-28.
[57] DING M, HE H, QIAO R, et al. RIPPB: a robust and improved PBFT protocol for blockchain[C]//Proceedings of the 2022 IEEE 17th Conference on Industrial Electronics and Applications. Piscataway: IEEE, 2022: 384-389.
[58] 刘昊哲, 李莎莎, 吕伟龙, 等. 基于信誉度的主从多链区块链共识机制[J]. 南京理工大学学报, 2020, 44(3): 325-331.
LIU H Z, LI S S, LV W L, et al. Master-slave multiple-blockchain consensus based on credibility[J]. Journal of Nanjing University of Science and Technology, 2020, 44(3): 325-331.
[59] SUN H Y, RUAN N, SU C H. How to model the bribery attack: a practical quantification method in blockchain[C]//Proceedings of the 25th European Symposium on Research in Computer Security. Cham: Springer, 2020: 569-589.
[60] WANG J, CAI Y Q, HE J Y. A new threshold signature scheme to withstand the conspiracy attack[C]//Proceedings of the 2010 International Conference on Computational Intelligence and Security. Piscataway: IEEE, 2010: 343-346.
[61] QURESHI B, MIN G Y, KOUVATSOS D. Countering the collusion attack with a multidimensional decentralized trust and reputation model in disconnected MANETs[J]. Multimedia Tools and Applications, 2013, 66(2): 303-323.
[62] HU Q, WANG S L, CHENG X Z. A game theoretic analysis on block withholding attacks using the zero-determinant strategy[C]//Proceedings of the 2019 IEEE/ACM 27th International Symposium on Quality of Service. Piscataway: IEEE, 2019: 1-10.
[63] LIU X, HUANG Z, WANG Q, et al. An evolutionary game theory-based method to mitigate block withholding attack in blockchain system[J]. Electronics, 2023, 12(13): 2808.
[64] CHANG S Y, PARK Y. Silent timestamping for blockchain mining pool security[C]//Proceedings of the 2019 International Conference on Computing, Networking and Communications. Piscataway: IEEE, 2019: 1-5.
[65] SCHAFFNER T. Scaling public blockchains[D]. Basel: University of Basel, 2021.
[66] SHENG P, XUE B, KANNAN S, et al. ACeD: scalable data availability oracle[C]//Proceedings of the 25th International Conference on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2021: 299-318.
[67] MITRA D, TAUZ L, DOLECEK L. Graph coded merkle tree: mitigating data availability attacks in blockchain systems using informed design of polar factor graphs[J]. IEEE Journal on Selected Areas in Information Theory, 2023, 4: 434-452.
[68] DZIEMBOWSKI S, FAUST S, HOSTÁKOVÁ K. General state channel networks[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2018: 949-966.
[69] DZIEMBOWSKI S, ECKEY L, FAUST S, et al. Multi-party virtual state channels[C]//Proceedings of the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer, 2019: 625-656.
[70] XU C, ZHANG C, XU J, et al. SlimChain: scaling blockchain transactions through off-chain storage and parallel processing [J]. Proceedings of the VLDB Endowment, 2021, 14(11): 2314-2326.
[71] COLEMAN J, HORNE L, LI X J. Counterfactual: generalized state channels[EB/OL]. [2024-10-04]. http://l4.ventures/papers/statechannels.pdf.
[72] ZHANG J S, GAO J B, LI Y, et al. Xscope: hunting for cross-chain bridge attacks[C]//Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering. New York: ACM, 2022: 1-4.
[73] XIE T C, ZHANG J H, CHENG Z R, et al. zkBridge: trustless cross-chain bridges made practical[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2022: 3003-3017.
[74] HERLIHY M. Atomic cross-chain swaps[C]//Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing. New York: ACM, 2018: 245-254.
[75] SHADAB N, HOUSHMAND F, LESANI M. Cross-chain transactions[C]//Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency. Piscataway: IEEE, 2020: 1-9.
[76] THIBAULT L T, SARRY T, HAFID A S. Blockchain scaling using rollups: a comprehensive survey[J]. IEEE Access, 2022, 10: 93039-93054.
[77] KALODNER H, GOLDFEDER S, CHEN X, et al. Arbitrum: scalable, private smart contracts[C]//Proceedings of the 27th USENIX Security Symposium, 2018: 1353-1370.

中国知网 https://www.cnki.net

[78] MAMAGEISHVILI A, FELTEN E W. Incentive schemes for rollup validators[C]//Proceedings of the 4th International Conference on Mathematical Research for Blockchain Economy. Cham: Springer, 2023: 48-61.
[79] GORZNY J, LIN P A, DERKA M. Ideal properties of rollup escape hatches[C]//Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good. New York: ACM, 2022: 7-12.
[80] DAIAN P, GOLDFEDER S, KELL T, et al. Flash boys 2.0: frontrunning, transaction reordering, and consensus instability in decentralized exchanges[EB/OL]. [2024-10-04]. https://arxiv.org/abs/1904.05234.
[81] TORRES C F, CAMINO R. Frontrunner jones and the raiders of the dark forest: an empirical study of frontrunning on the Ethereum block- chain[C]//Proceedings of the 30th USENIX Security Symposium, 2021: 1343-1359.
[82] KELKAR M, ZHANG F, GOLDFEDER S, et al. Order-fairness for Byzantine consensus[C]//Proceedings of the 40th Annual International Cryptology Conference. Cham: Springer, 2020: 451-480.
[83] HEIMBACH L, WATTENHOFER R. Eliminating sandwich attacks with the help of game theory[C]//Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security. New York: ACM, 2022: 153-167.
[84] LI D Z, ZHANG K J, WANG L, et al. A Geth-based real-time detection system for sandwich attacks in Ethereum[J]. Discover Computing, 2024, 27(1): 11.
[85] QIN K H, ZHOU L Y, LIVSHITS B, et al. Attacking the DeFi ecosystem with flash loans for fun and profit[C]//Proceedings of the 25th International Conference on Financial Cryptography and Data Security. Cham: Springer, 2021: 3-32.
[86] CAO Y, ZOU C, CHENG X. Flashot: a snapshot of flash loan attack on DeFi ecosystem[EB/OL]. [2024-10-04]. https://arxiv.org/abs/2102.00626.
[87] CHEN W L, GUO X F, CHEN Z G, et al. Phishing scam detection on ethereum: towards financial security for blockchain ecosystem[C]//Proceedings of the 29th International Joint Conference on Artificial Intelligence, 2020: 4506-4512.
[88] WU J J, YUAN Q, LIN D, et al. Who are the phishers? phishing scam detection on ethereum via network embedding[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52(2): 1156-1166.
[89] BIRSAN A. Dependency confusion: how I hacked into apple, Microsoft and dozens of other companies[EB/OL]. [2024-10-04]. https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610.
[90] MEHAR M I, SHIER C L, GIAMBATTISTA A, et al. Understanding a revolutionary and flawed grand experiment in blockchain[J]. Journal of Cases on Information Technology, 2019, 21(1): 19-32.
[91] WANG S, DING W W, LI J J, et al. Decentralized autonomous organizations: concept, model, and applications[J]. IEEE Transactions on Computational Social Systems, 2019, 6(5): 870-878.
[92] RIKKEN O, JANSSEN M, KWEE Z. Governance challenges of blockchain and decentralized autonomous organizations [J]. Information Polity, 2019, 24(4): 397-417.

**李嘉乐**(2000—),男,内蒙古鄂尔多斯人,硕士研究生,主要研究方向为区块链技术、智能合约等。
**LI Jiale**, born in 2000, M.S. candidate. His research interests include blockchain technology, smart contract, etc.

**李雷孝**(1978—),男,山东成武人,博士,教授,主要研究方向为数据分析与数据挖掘、网络空间安全、区块链技术等。
**LI Leixiao**, born in 1978, Ph.D., professor. His research interests include data analysis and data mining, cyberspace security, block chain technology, etc.

**林浩**(1995—),男,天津人,博士研究生,主要研究方向为数据挖掘、人格检测、区块链技术。
**LIN Hao**, born in 1995, Ph.D. candidate. His research interests include data mining, personality testing and blockchain technology.

**杜金泽**(1998—),男,山西太原人,博士研究生,主要研究方向为区块链技术、隐蔽信道构建和分析等。
**DU Jinze**, born in 1998, Ph.D. candidate. His research interests include blockchain technology, construction and analysis of covert channels, etc.

**史建平**(1982—),男,内蒙古鄂尔多斯人,主要研究方向为计算机应用技术、数据分析等。
**SHI Jianping**, born in 1982. His research interests include computer application technology, data analysis, etc.

**刘哲旭**(1996—),男,山东淄博人,硕士研究生,主要研究方向为区块链技术、机器学习等。
**LIU Zhexu**, born in 1996, M.S. candidate. His research interests include blockchain technology, machine learning, etc.

中国知网 https://www.cnki.net