区块链网络安全研究报告

刘修铭 1)

1) (南开大学网络空间安全学院 天津 中国 300381)

摘 要 本报告对区块链网络的构建方法、基本原理及其潜在的安全漏洞进行了详尽的分析。深入探讨了区块链的核心组成，包括其独特的数据结构、密码学技术和各种共识机制，并详细介绍了区块链系统可能面临的主要安全挑战，如 51%攻击、双花攻击、粉尘攻击、DoS 攻击及套利攻击等。

关键词 区块链技术；网络安全

中图法分类号 TP309

Blockchain Network Security Research Report

LIU Xiu-Ming[1)]

1) (College of Cyberspace Security, Nankai University, Tianjin China 300381)

Abstract This report provides a detailed analysis of the construction methods, fundamental principles, and potential security vulnerabilities of blockchain networks. It delves deeply into the core components of blockchain, including its unique data structure, cryptographic technologies, and various consensus mechanisms, and details the main security challenges that blockchain systems may face, such as 51% attacks, double-spending attacks, dust attacks, DoS attacks, and arbitrage attacks.

Key words blockchain technology; network security

选题

区块链网络安全漏洞分析：通过查找相关文献，了解区块链网络构建的方法、原理，详细分析区块链网络中可能存在的安全漏洞。

1 引言

在当今数字化日益增长的时代，区块链技术以其独特的去中心化特性，提供了一种新的数据管理和交易方式，这种方式在透明性、安全性及不可篡改性等方面展示了巨大的潜力。然而，随着区块链应用的广泛推广，其安全问题也日益突显，成为了研究和实践中不可忽视的一部分。

2 问题与挑战

尽管区块链具有安全优势，但仍面临诸多挑战，如51%攻击的威胁、智能合约漏洞、隐私保护问题以及跨链技术和扩展性问题。这些挑战需通过持续技术创新和严格安全测试解决。

3 区块链介绍

3.1 概述

区块链技术是一种基于块链数据结构来验证和存储数据的分布式基础架构，它通过分布式节点共识算法更新数据，利用密码学保障数据传输和访问安全，同时通过智能合约进行数据编程和操作[1]。

刘修铭，男，2002年生，本科在读，学生，非计算机学会(CCF)会员.E-mail: lxmliu2002@mail.nankai.edu.cn

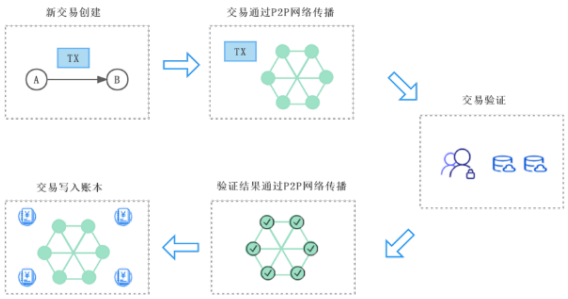

图1 区块链工作流程

3.2 数据结构介绍

区块链的数据结构是一种时间序的链式数据库，每个区块包含前一区块的散列值、时间戳和交易数据，这种结构确保数据难以被篡改。区块由区块头和区块体组成，其中区块头包含诸如版本号、前区块哈希、目标难度值、随机数、Merkle 根和时间戳等信息；区块体则包含交易记录。交易数据通过 Merkle 树进行哈希计算，确保了数据的完整性和安全性[2]。

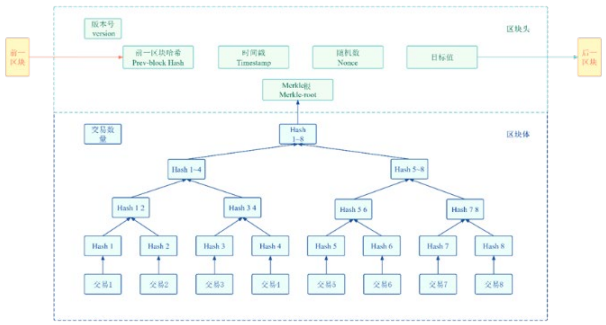

图2 区块链区块结构图

3.3 密码学技术介绍

区块链主要利用哈希算法和非对称加密算法。哈希算法如双 SHA256 用于构建防篡改的链式结构和 Merkle 树，而非对称加密技术则用于信息加密、数字签名和登录认证，确保了数据的安全性和用户的身份验证[3]。

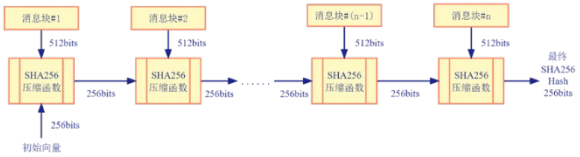

图3 双SHA256哈希函数

区块链的共识机制解决了数据一致性和安全性问题，包括 PoW、PoS、DPoS 和 PBFT 等算法，各有优势和适用场景，它们共同保障了分布式账本的正确性和不可篡改性[4]。

表1 共识机制比较

参数	PoW	PoS	DPoS	PBFT
中心化程度	完全去中心化	完全去中心化	部分去中心化	部分去中心化
节点准入许可	不需要	不需要	不需要	需要
接入节点数	不限	不限	不限	受限
出块时间	>500s	<100s	<100s	<10s
吞吐量（TPS）	<10	<1000	>1000	<2000
可扩展性	强	强	强	弱
主要资源占用	算力（电能）	权益、代币	权益、代币	带宽（通信）
是否分叉	易分叉	易分叉	不易分叉	无分叉
最终一致性	无最终性	无最终性	无最终性	有最终性
安全保障	1/2以上 算力可信	1/2以上 stake可信	1/2以上 股权可信	2/3以上 节点可信
优点	实现简单，攻击难度大	耗费资源少	共识效率高，吞吐量大	可以忍受总数1/3的作恶节点
缺点	耗费资源过多	易受权益粉碎攻击	去中心化程度不足	节点增多时效率降低
应用场景	公有链的初期阶段	公有链的中期阶段	共识节点少，公有链	有作恶节点，联盟链

以太坊作为区块链 2.0 的代表，引入了智能合约技术，支持定制应用并通过智能合约与区块链交互，可用于广泛的应用场景和高效的数据交互。

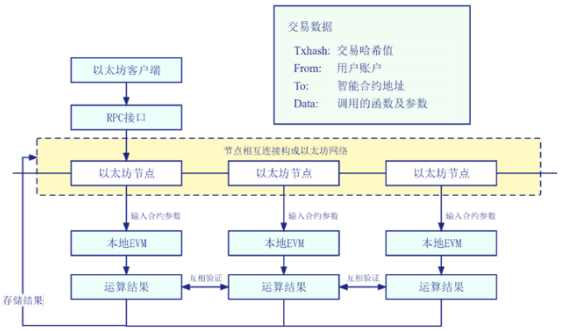

图4 智能合约执行流程图

4 区块链安全性

4.1 综述

区块链系统构建的基本安全目标是通过密码学和网络安全等技术手段，保护区块链系统中的数据安全、共识安全、隐私保护、智能合约安全和内容安全，各安全目标之间的关系如图所示。

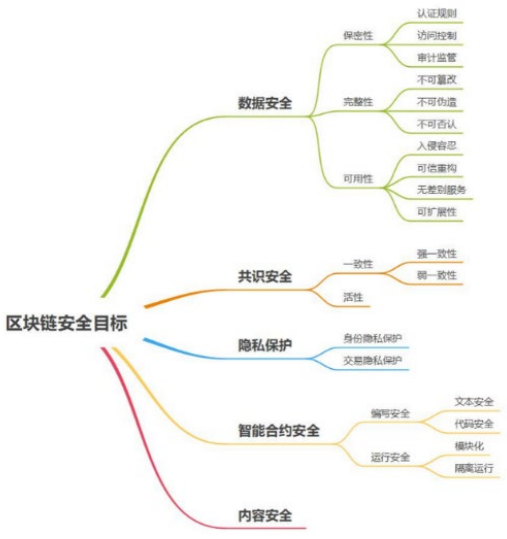

图5 区块链安全目标关系图

4.2 区块链存在的安全漏洞[1]

4.2.1 51%攻击

51%攻击允许控制者通过超过一半的哈希率操纵 PoW 区块链交易，实施双花。攻击者可以逆转交易，重复使用已花费的加密货币，当其链长度超过主链时，便成为有效链[5]。

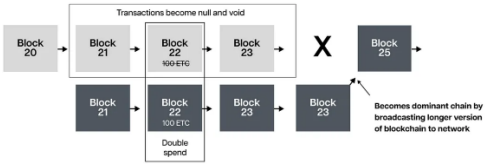

图6 51%攻击示意图

在 2018 年，Bitcoin Gold 遭遇多次 51%攻击，攻击者通过租用算力实现双重支付，损失超过 1800 万美元。2019 年，Ethereum Classic 也遭受类似攻击，导致重大财产损失。这些事件揭示了加密货币网络在面对可租用算力时的安全脆弱性，即使是知名的区块链也可能遭受重大安全威胁。

为防止 51%攻击，可增加网络哈希率，使用 PoS 或 DPoS 共识算法，提高大额交易确认数，并部署网络监听与警告系统监测异常算力集中。这些措施可增强区块链的安全性和抵抗攻击的能力。

4.2.2 double-spending 攻击

双花攻击利用数字货币的特性多次使用同一笔资金。常见手法包括 Race Attack、Finney Attack、Vector76 Attack 及 51%攻击，通过控制矿工费、区块广播时间或算力，攻击者回滚交易以重复使用资金[6]。

2019 年 1 月，ETC 遭受 51%攻击，慢雾预警，攻击者利用租借算力实施 12 次 double-spending 攻击，盗取约 110 万美元。所幸在社区努力下，攻击者一周后归还所得。

为防御 double-spending 攻击，区块链可以借助的措施有：提高交易确认次数、使用中心化验证机制加快交易审核、部署网络监控工具检测异常、实行交易锁定防资金重用、为大额交易加入多重签名等二次验证措施。

4.2.3 粉尘攻击

粉尘攻击通过向私人钱包发送微量代币追踪交易，侵犯用户匿名性。黑客利用粉尘追踪用户地址，可能威胁要求赎金。此攻击也可引发比特币网络拥堵，通过分析混合的交易输出，黑客可获得用户身份信息[7]。

2019 年共发生超 8 起公链被攻击事件，在 8 月 9 日，黑客向莱特币发起“粉尘攻击”，受影响的地址达 294582 个。

为防止粉尘攻击，可采取包括粉尘转换服务、使用 VPN 隐藏身份、标记小额不明转账以避免使用、将大额资产转移到新的 HD 钱包隔离风险、忽略含备忘标签的可疑小额支付等措施进行处理。

4.2.4 Dos 攻击

拒绝服务攻击（DoS）通过使目标系统过载或崩溃，阻断合法用户的访问权限。常见的攻击形式包括缓冲区溢出、ICMP flood（亦称“死亡之 Ping”）、SYN flood 攻击，以及难以追踪的分布式拒绝服务攻击（DDoS），后者通过多个源点发起，更为难以防御[8]。

第一例公认的 DoS 攻击发生于 2000 年 2 月，当时一名 15 岁的加拿大黑客利用该方法攻击了亚马逊和 eBay 的网络服务器。自那以后，DoS 攻击越来越多地被用于针对各行各业的目标进行破坏。

区块链网络防御 DoS 攻击的措施包括增增加节点的冗余性、限制请求的速率、采用 DoS 防护服务、实施端点过滤、异步处理请求、加强节点的安全配置、采用多样化的共识机制以及建立应急响应计划等。这些策略的联合使用可以显著提高网络的抵抗力和安全性。

4.2.5 套利攻击

区块链套利攻击利用市场不一致或智能合约漏洞获利。常见类型包括简单市场套利、跨协议套利、时间差套利、闪电贷套利和操纵预言机的 Oracle 套利。这些策略在 DeFi 平台上尤为常见，套利者利用交互差异和延迟获得利益[9]。

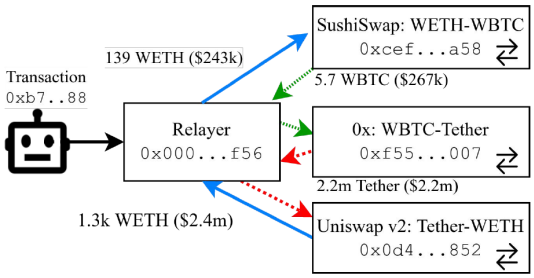

图7 套利攻击示意图[9]

例如，攻击者曾利用 WUSDMaster 合约的 stake 函数漏洞，通过 1:1 兑换 BSC_USDT 与 WUSD 并

1 https://github.com/slowmist/Cryptocurrency-Security-Audit-Guide/blob/main/Blockchain-Common-Vulnerability-List_CN.md 网站中详细列举了区块链面临的漏洞攻击，篇幅原因，此处选择较为重要的五个攻击作为展示。

同时执行 swap 操作，导致 WaultSwapPair 池中代币失衡，实现套利。该攻击导致 370 枚 BEP_ETH 被盗，并通过 Anyswap 转移，损失约 93 万美元。

确保智能合约进行严格的安全审计，使用多源预言机以增强数据的准确性，限制交易速度并引入滑点以减少套利利润，采用复杂的价格更新机制，以及监控并限制大额闪电贷，这些措施有助于维护市场的公正性和系统的安全。

5 结语

区块链技术作为分布式账本技术的核心，正处于快速发展阶段。尽管 PoW、PoS、DPoS 和 PBFT 等不同共识机制在提升交易效率和降低成本方面各具优势，但它们也面临特有的安全挑战。例如，PoW 易受 51%攻击威胁，PoS 和 DPoS 可能导致资本更加集中，而 PBFT 在网络分裂情况下表现不佳。针对这些漏洞，未来研究应聚焦于开发更健壮、适应性强的共识机制，并加强区块链的隐私保护与抗攻击能力。

此外，随着量子计算和人工智能技术的发展，区块链的安全性面临新挑战。未来研究应探索如何将这些技术融入区块链架构中，以提高其安全性和效率。通过跨学科合作与创新，区块链技术能够突破现有限制，在金融、医疗、供应链等领域发挥更大作用，为其长远发展和广泛应用奠定坚实基础。

参 考 文 献

[1] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain. ACM Comput. Surv. 52, 3, Article 51 (May 2020), 34 pages. https://doi.org/10.1145/3316481

[2] 曾诗钦,霍如,黄韬,刘江,汪硕,冯伟.区块链技术研究综述：原理、进展与应用[J] .通信学报,2020,41(01):134-151

[3] 王化群,吴涛.区块链中的密码学技术[J] .南京邮电大学学报(自然科学版),2017,37(06):61-67

[4] 靳世雄,张潇丹,葛敬国,史洪彬,孙毅,李鸣,林业明,姚忠将.区块链共识算法研究综述[J] .信息安全学报,2021,6(02):85-100

[5] C. Ye, G. Li, H. Cai, Y. Gu and A. Fukuda, "Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting," 2018 5th International Conference on Dependable Systems and Their Applications (DSA), Dalian, China, 2018, pp. 15-24, doi: 10.1109/DSA.2018.00015.

[6] M. Iqbal and R. Matulevičius, "Exploring Sybil and Double-Spending Risks in Blockchain Systems," in IEEE Access, vol. 9, pp. 76153-76177, 2021, doi: 10.1109/ACCESS.2021.3081998.

[7] F. A. AlShlawi, N. K. AlSa'awi, W. Y. Bin Saleem and A. Ara, "DUST-MASK: A Framework for Preventing Bitcoin's Dust Attacks," 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2020, pp. 1-6, doi: 10.1109/ICCAIS48893.2020.9096763.

[8] Raikwar, M., Gligoroski, D. (2022). DoS Attacks on Blockchain Ecosystem. In: Chaves, R., et al. Euro-Par 2021: Parallel Processing Workshops. Euro-Par 2021. Lecture Notes in Computer Science, vol 13098. Springer, Cham. https://doi.org/10.1007/978-3-031-06156-1_19

[9] McLaughlin, Robert, Christopher Kruegel, and Giovanni Vigna. "A large scale study of the ethereum arbitrage ecosystem." 32nd USENIX Security Symposium (USENIX Security 23). 2023.

Background

Blockchain technology, with its decentralized nature, has revolutionized data storage and transactions, and is widely applied in fields such as finance and supply chain management. However, as its applications expand, so too do its security challenges, including 51% attacks and smart contract vulnerabilities. Thus, enhancing blockchain security to counter these threats is crucial. This report will explore these security challenges and potential countermeasures in depth.