

区块链生态共性安全风险综述

高昊昱¹, 曹春杰¹, 徐响¹, 裴庆祺², 芦翔³, 雷虹¹

(1. 海南大学网络空间安全学院(密码学院), 海南 海口 570228;

2. 西安电子科技大学网络与信息安全学院, 陕西 西安 710071; 3. 中国科学院信息工程研究所, 北京 100864)

摘要: 区块链作为一种去信任化的分布式基础架构和新型计算范式, 已经从最初的数字“加密货币”设计演进为广泛应用的技术基础设施, 为数字经济发展和转型提供了新的动能。然而, 这也为区块链技术与应用环境组成的生态带来了众多风险与挑战, 包括区块链自身存在的技术安全风险及其融入现有系统所产生的安全问题。针对这些风险进行深入分析与研究, 对于促进区块链技术与生态的良性发展具有重要意义。对这两类风险进行了全面系统的分析和评估, 总结每种风险的成因、影响和缓解措施, 为现有区块链项目的安全管理和风险控制提供了有力指导。提出了区块链生态安全发展的六大安全目标, 并根据这六大安全目标构建了一个全面、多维度的区块链项目安全评估框架, 旨在推动区块链生态的健康发展, 为构建更加安全、稳定、高效的区块链应用环境提供有力支持。

关键词: 区块链安全; 区块链生态; 风险分析; 区块链治理

中图分类号: TP309.2; TP39

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025015

Survey on blockchain ecosystem common security risk analysis

GAO Haoyu¹, CAO Chunjie¹, XU Xiang¹, PEI Qingqi², LU Xiang³, LEI Hong¹

1. School of Cyberspace Security (School of Cryptology), Hainan University, Haikou 570228, China

2. School of Network and Information Security, Xidian University, Xi'an 710071, China

3. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100864, China

Abstract: Blockchain has been evolved from the initial design of cryptocurrency to a widely applied technological foundation as a decentralized distributed infrastructure and novel computing paradigm, providing new impetus for the development and transformation of the digital economy. However, numerous risks and challenges have also been brought to the ecosystem composed of blockchain technology and application environments, including the technical security risks inherent in blockchain itself and those arising from its integration into existing systems. In-depth analysis and research on these risks have been of great significance for promoting the benign development of

收稿日期: 2024-04-25; 修回日期: 2024-09-13

通信作者: 曹春杰, caochunjie@hainanu.edu.cn

基金项目: 国家重点研发计划(2021YFB2700600); 海南大学科研启动基金(KYQD(ZR)-21071)

Foundation Items: The National Key R&D Program of China (2021YFB2700600), Research Startup Fund of Hainan University (KYQD(ZR)-21071)

引用格式: 高昊昱, 曹春杰, 徐响, 等. 区块链生态共性安全风险综述[J]. 网络与信息安全学报, 2025, 11(2): 1-25.

Citation Format: GAO H Y, CAO C J, XU X, et al. Survey on blockchain ecosystem common security risk analysis[J]. Chinese Journal of Network and Information Security, 2025, 11(2): 1-25.

blockchain technology and ecology. Firstly, a comprehensive and systematic analysis and evaluation of these two types of risks were conducted, with the causes, impacts, and mitigation measures for each risk being summarized, thereby providing strong guidance for security management and risk control of existing blockchain projects. Subsequently, six security objectives for the development of blockchain ecology security were proposed, and based on these objectives, a comprehensive, multi-dimensional blockchain project security assessment framework was constructed, aiming to promote the healthy development of the blockchain ecosystem and provide robust support for building a more secure, stable, and efficient blockchain application environment.

Keywords: blockchain security, blockchain ecosystem, risk analysis, blockchain governance

0 引言

区块链技术是一种去信任化的分布式基础架构和新型计算范式^[1]。随着技术发展,区块链已进入3.0时代,即产业区块链时代,其应用从最初的加密“数字货币”延伸至金融科技、政务民生和社会治理等领域。2020年4月,国家发展和改革委员会将区块链技术纳入“新基建”范畴,成为信息基础设施之一。至2020年年中,注册在商业部门的区块链相关企业数量超过40 000家,仅在2020年的前6个月内就新增了8 129家。区块链的作用毋庸置疑,然而,正如任何技术都有其局限性,区块链亦非无懈可击。从技术角度来看,区块链技术本身不够成熟,存在安全漏洞;从法律角度,区块链的某些特性与当前法律体系存在一定冲突;从经济角度看,区块链性能等原因限制了其在传统场景下的大规模应用。在区块链生态中,风险广泛存在且危险性高,这些风险导致大多数区块链应用方案只存在于理论而不能实际落地,因此,精确抽象区块链生态共性安全风险并给出防范措施,对于区块链产业的健康发展和正确发挥区块链作用至关重要。

总体来说,区块链发展还处于应用探索阶段,分析区块链生态的共性安全风险具有多方面意义。第一,深入分析区块链生态共性安全风险不仅揭示了现有技术的局限,而且能够推动底层技术架构的优化和革新。第二,通过系统化的安全风险分析,可以为区块链技术的标准化和规范化提供依据,还可以为制定相关政策和法规提供技术参数和考量依据,确保区块链技术的应用在一个更加可控和透明的环境中进行。第三,区块链安全性研究的跨学科特性不仅丰富了区块链安全性的研究内容,而且有助于构建一个更加全面

和深入的理论框架,推动相关学科领域的融合与发展。第四,对共性安全风险的认识有助于指导实际应用中的安全性设计和评估。通过对这些共性风险的深入分析,开发者和应用方可以更好地预防和应对安全威胁,提高区块链应用的安全性和可靠性,从而为用户提供更加安全的区块链服务。

本文的主要贡献如下。

1) 系统地叙述了区块链发展历程、应用现状和架构,定义了区块链生态这一概念,对区块链生态安全态势进行了梳理,并对区块链安全事件常见原因进行了讨论。

2) 运用社会技术系统理论思想,从区块链技术安全和业务安全两个维度出发,对区块链生态中存在的共性安全风险进行了全面的评估与详尽的分析。

1 区块链生态与区块链安全风险

1.1 区块链生态

1.1.1 区块链发展历程

区块链技术的历史轨迹贯穿了多个发展阶段:前区块链时代、区块链1.0时代、区块链2.0时代以及当前正处于的区块链3.0时代。在前区块链时代,前人关于密码学的研究为区块链底层加密算法夯实了基础^[2-4];Merkle树(Merkle tree)首次于1980年被提出,后成为比特币等“加密货币”区块验证的基石,为区块链数据的完整性和可靠性验证提供了高效的加密机制^[5];拜占庭将军问题(Byzantine generals problem)于1982年被提出^[6],为理解和设计分布式系统中的共识机制和容错能力奠定了理论基础;1997年出现的HashCash^[7]更是被认为第一代PoW(proof of work)算法;到了1998年,

B-Money^[8]和Bitgold^[9]已经和比特币的特性非常接近。

2008年,中本聪发布了比特币白皮书^[10],正式提出了区块链的概念。白皮书不仅描述了一种去中心化的“数字货币”系统比特币,还详细阐述了其背后的技术原理,即区块链技术。2013年,Vitalik^[11]提出以太坊,以太坊引入了智能合约,进一步扩展了区块链的功能,智能合约可以理解成运行在区块链上的程序,智能合约的出现标志着区块链进入2.0时代。2015年,Linux Foundation推出了Hyperledger项目^[12],区别于公有链(如比特币和以太坊),Hyperledger聚焦于企业级应用,是支持多种区块链技术和框架的开源协作,特别是构建许可链解决方案,要求节点在加入前得到网络的授权,从而适应不同的业务需求和隐私标准。在区块链3.0时代,区块链从原有的金融应用领域扩展到更广泛的行业和社会系统中。区块链发展历程如图1所示。

1.1.2 区块链应用现状

经过十多年的技术与完善,区块链的架构日趋成熟。在我国信息通信研究院对全球范围内的1121项区块链项目统计中,金融领域仍然是区块链技术应用的主要领域,但正逐步向医疗健康、物流、工业互联网等经济社会多个领域拓展。

众多科技巨头的积极参与突显了区块链技术在跨领域融合方面的巨大潜力。

综合以上分析,全球区块链生态呈现广泛且多元,同时显示出各地区在应用焦点和发展速度上的差异。这凸显了深入研究分析区块链生态共性安全风险的必要性。这种风险分析不仅能为理解各地区区块链应用的现状提供视角,也对预测未来发展趋势、制定相应政策和促进国际合作具有重要意义。

1.1.3 区块链层次架构

在区块链技术的演进过程中,传统的6层架构(数据层、网络层、共识层、激励层、合约层和应用层)逐渐呈现出模块淡化的趋势。通过深入分析各层的技术与机制,可以发现,数据层、共识层、激励层以及合约层在交易过程中的界限逐渐模糊,难以进行明确区分。基于对区块链技术本质特性的深入研究,本文将区块链技术的架构简化为如图2所示的3个核心层次:网络层、交易层和应用层。

网络层主要负责构建和维护区块链网络,确保各节点间信息的有效传递,核心要素包括组网方式和数据传播协议。

交易层承载着区块链技术的核心业务逻辑,负责处理所有的交易操作。在这个层面,交易被创建、验证并添加到区块链中。每笔交易都包含

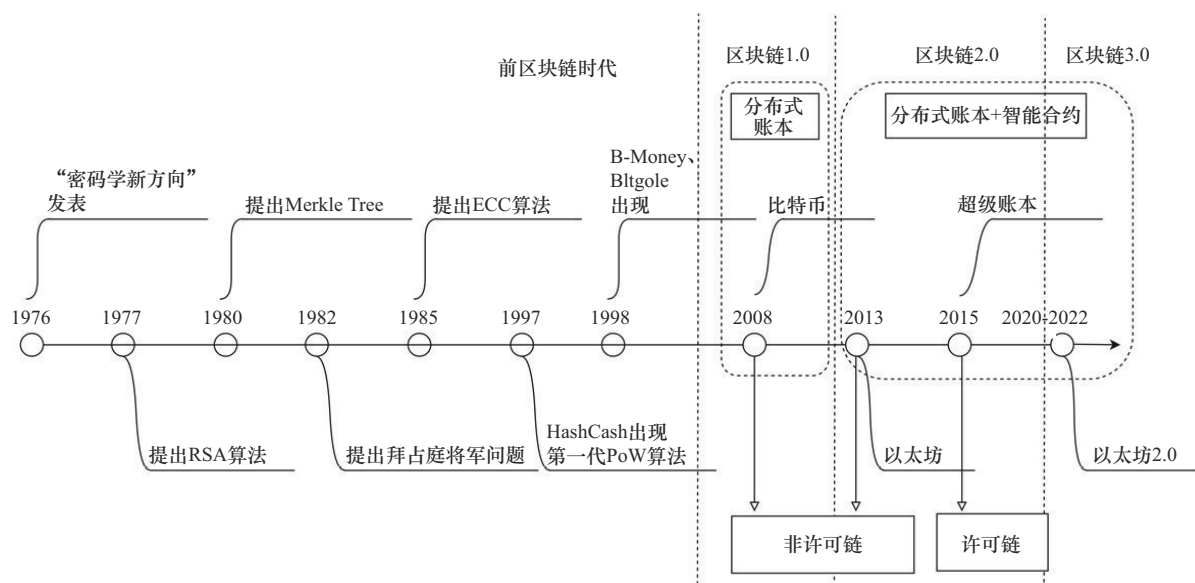


图1 区块链发展历程

Figure 1 Blockchain development history

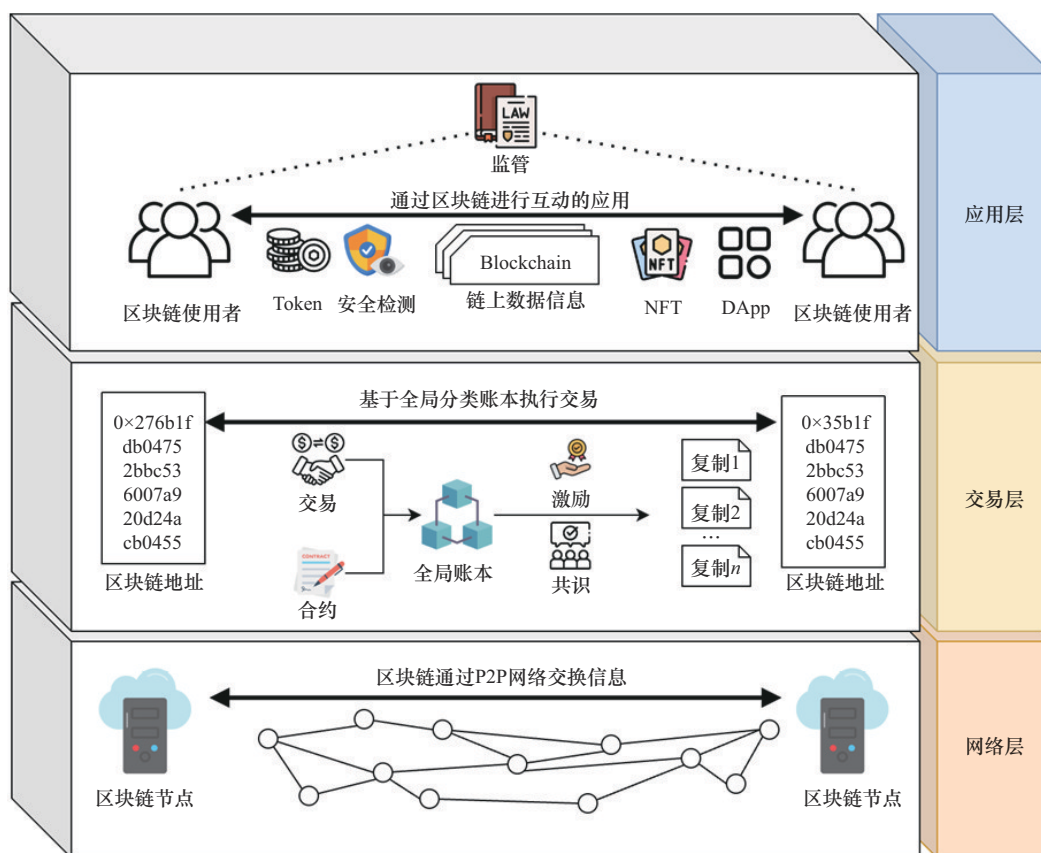


图2 区块链架构

Figure 2 Blockchain architecture

发送方和接收方的地址信息、交易的金额以及一个独特的签名，这个签名证明了交易的有效性。

应用层是架构中的最高层，也是用户与区块链之间的接口，其主要作用是将区块链技术应用于实际商业，为用户提供丰富的功能，帮助他们实现各种任务。

为了缓解区块链的“三元悖论”^[13]困境，业界提出了Layer0、Layer1、Layer2和Layer3层级概念^[14]。Layer0作为最底层的基础设施层，对

应于前述架构中的网络层，为整个区块链体系提供坚实的基础支撑。Layer1是建立在Layer0之上的区块链层，它负责维护区块链网络的核心功能。Layer2是通过消除Layer0中的交互来实现的，是一种解决扩展性问题的方案，通过与第三方集成合作来提供更高的扩展性。Layer3为应用层，承载着区块链应用和协议的运行，实现其他应用程序所需的功能。表1展示了Layer层级对比和举例。

在当前复杂多变的区块链生态中，区块链

表1 Layer层级对比和举例

Table 1 Layer comparison and example

层级	定义	主要功能	举例
Layer0	基础设施层	提供区块链底层技术和基础设施	Avalanche、Cosmos、Horizen、Polkadot
Layer1	区块链层	提供主要区块链协议和功能，处理交易和智能合约	以太坊、Polkadot、EOS
Layer2	协议增强层	优化交易速度和费用，提高可扩展性，建立在Layer1主区块链之上	Lightning Network、Rollups、Optimism
Layer3	应用层	开发和运行各种区块链的应用程序和服务	Uniswap、Compound、OpenSea

应用通常不单纯依赖于单一技术，而是倾向于结合多种技术实现更加高效、可靠的区块链应用系统。其中，Layer2可拓展性解决方案尤为突出，成为领域内的重要研究和应用焦点。鉴于这一发展趋势，传统的6层区块链架构分析模型无法全面覆盖新的Layer 2和Layer 3生态，对当前区块链生态的技术细节和安全风险存在盲区。相对而言，采用以Layer0至Layer3为核心的层次结构来分析区块链生态，可以更为精确地定位和评估技术共性安全风险，从而为构建更加安全、稳定的区块链系统提供关键的理论支持和实践指导。

1.1.4 区块链生态格局

传统意义上的生态系统是特定环境内，相互作用的所有生物和环境的统称^[15]，区块链生态系统类似于传统生态系统，这些相互作用的主体不是生物和非生物要素，而是围绕区块链技术展开的多种实体和过程。区块链生态系统指的是一群能够相互作用并与周围世界互动的元素集合，这些元素共同创造一个具有特定特征的环境。也可以将区块链生态系统定义为特定用例下认可的治理结构。这种治理结构为参与者的可接受行为、数据所有权、资金支持、进入和退出标准以及参与者间信息共享的条件提供了定义。区块链生态系统是

一个由不同实体、技术和过程组成的复杂网络，这些要素共同工作以维持区块链平台的健康和增长。

全球区块链技术的应用初步构建了一个如图3所示的多层次生态格局，涵盖了硬件与基础设施、底层技术、上层应用以及安全服务等多个维度。硬件和基础设施是区块链技术稳定运行的基础，为整个区块链生态系统提供了必要的计算能力和硬件支撑。底层技术是这个生态体系的核心所在，它扮演着类似于操作系统的角色，为区块链应用提供了基础的架构和开发平台。这一层面不仅支持了公链、联盟链、私链等多种类型区块链的实现，还通过提供分布式账本、智能合约等关键技术服务，极大地降低了区块链应用的开发难度，加速了应用的部署和落地。上层应用则是这个生态体系与最终用户之间的桥梁，它们以服务 and 解决方案的形式，将区块链技术应用于各个行业和场景。这些应用不仅丰富了区块链技术的应用场景，也为用户带来了更加便捷、高效、安全的体验。安全服务是确保整个生态体系可靠性和稳定性的重要保障。它提供了代码审计、安全监测、安全管理等一系列服务，从源头上保障了区块链系统的安全，为整个生态体系的健康发展提供了有力支撑。整体而言，区块链生态是一个多元化、层次丰富的网络，涉及技术、

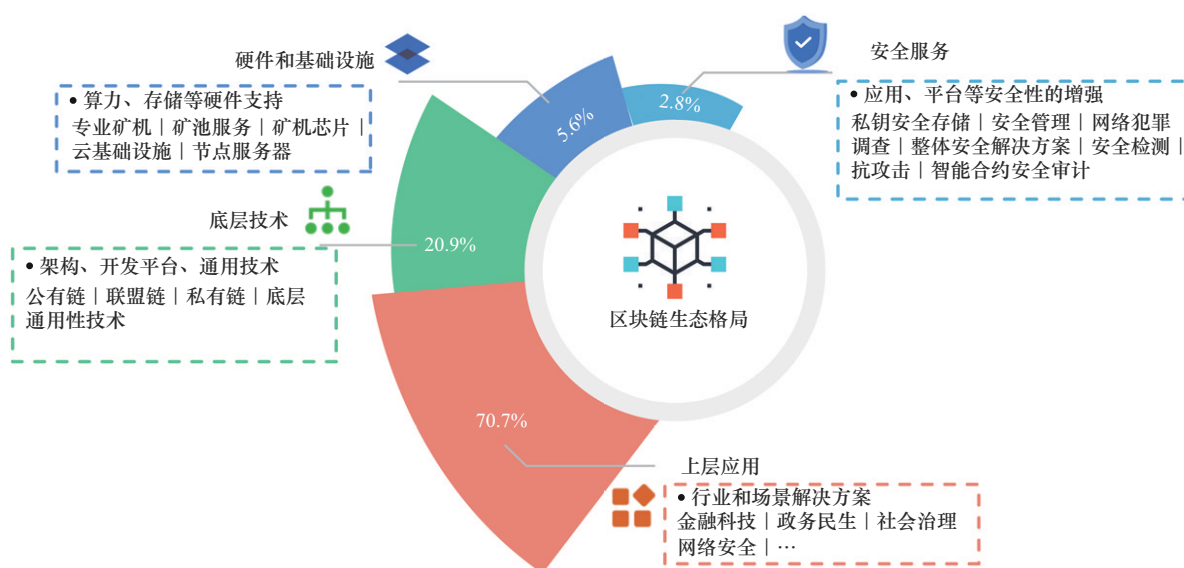


图3 区块链生态格局

Figure 3 Blockchain ecological landscape

市场、法规和社会各个方面,通过各实体和过程的相互作用推动区块链技术的创新与应用。这个系统不断进化,反映了区块链技术与应用的最新发展。

1.2 区块链生态共性安全风险的界定

区块链技术仍处于非金融领域应用的探索阶段,其发展的动态和潜在的应用方向至关重要。为了促进区块链技术与金融科技、政务民生以及社会治理等场景的深度结合,必须对区块链生态中的安全风险有清晰的认识和有效的防范策略。区块链生态安全风险是指区块链技术及其应用过程中可能遇到的各种潜在的安全威胁和漏洞,这些安全风险最终可能导致资产损失、数据泄露、系统瘫痪等严重后果。文献[16]从区块链应用的实际场景出发,探讨了业务层面所面临的安全风险。文献[17]着重从区块链的安全特性出发,分析了在技术发展进程中遭遇的挑战及相关的安全风险。文献[18]从攻击的角度出发,研究了在区块链应用过程中可能遭遇的安全风险。然而,当前对于区块链安全风险的界定大多从信息技术、法律法规和经济成本 3 个不同维度进行,整体对于安全风险的定义与类型划分较为模糊和琐碎。此外,对于技术特性和实际应用之间的分析也存在一定程度的割裂。

以托马斯·休斯为代表的“技术-社会系统”思想强调技术与社会的不可分割性^[19],反对将两者简单割裂。他认为,无论是技术决定论还是技术的社会建构论,都无法全面揭示技术与社会的复杂互动关系。与此同时,社会技术系统理论则认为,组织是一个由社会系统和技术系统相互作用形成的复合体系,其中包括正式组织、非正式组织、技术系统以及成员素质等多个要素^[20]。这一理论特别适用于分析新技术如何融入并影响社会系统,强调社会系统与技术系统之间的紧密关联,技术系统的任何变化都会引发社会系统的相应调整。在区块链生态中,技术系统即区块链技术,社会系统即应用区块链技术的各个场景,以及各个场景中原有的社会环境。区块链技术在应用到社会各应用场景的过程中,不仅通过认证交易商品、

促进脱媒、提升运营效率等方式对商业模式的价值主张、创造、交付、捕获和传播产生深远影响,更在与其他社会要素的重新整合中,触及并改变社会系统的其他多个领域。借助社会技术系统理论提供的观点,可以从技术系统与社会系统的双重视角出发,深入分析区块链生态中存在的共性安全风险。这些风险不仅包括区块链技术系统自身存在的的技术性问题,还涵盖了技术系统升级后社会系统变化所带来的业务层面的风险。这样的分析方式有助于更加全面、深入地了解区块链风险,从而制定更有效的风险管理策略。

2 区块链生态安全态势

据 SlowMist Hacked 统计^[21],从 2012 年开始到 2024 年 2 月,公开的区块链安全事件共 1 459 起,造成了 32 015 275 117.24 亿美元的直接损失,具体数据如图 4 所示。通过对比可以发现,自 2018 年区块链技术大热以来,每年发生的安全事件呈逐年递增趋势,但损失金额却有起伏而且呈下降趋势。

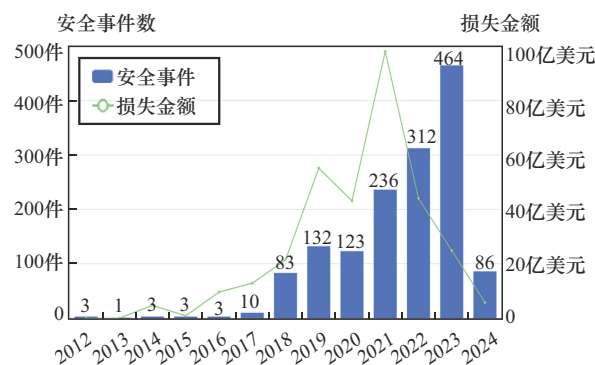


图4 区块链安全事件和损失金额统计

Figure 4 Blockchain security incident and loss amount statistics

造成这些安全事件常见的十大成因如图 5 所示,其中常见原因为卷款跑路,占全部原因的 1/4,就 2023 年由于项目方卷款跑路造成的安全事件共 117 起;其次为智能合约漏洞,2023 年因存在合约漏洞而被攻击的事件有 57 起,损失约为 7 582 万美元,同时合约漏洞利用往往伴随着闪电贷攻击、价格操纵等。2023 年,各赛道项目安全事件的分布及损失如图 6 所示。其中,去中心化金融(decentralized finance, Defi)领域成

为安全事件频发、损失最为严重的领域。据统计，该年度DeFi安全事件总数为282起。紧随其后的是交易平台，作为数字资产交易的主要场所，交易平台负责为用户提供数字资产的存储和管理服务。然而，若交易平台存在安全漏洞或遭受黑客攻击，用户的资产将面临损失或被窃取的风险。

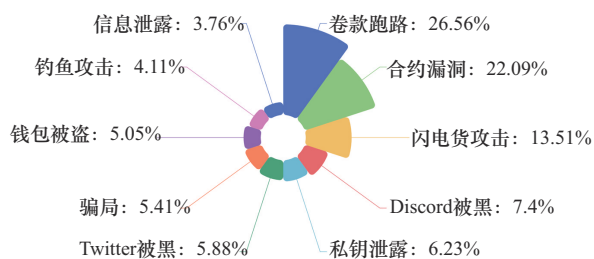


图5 区块链安全事件常见原因

Figure 5 Common causes of blockchain security incidents

通过对区块链生态安全态势进行分析发现，区块链安全事件逐年增加，对区块链生态安全风险的分析和预防迫在眉睫。这一工作不仅可以帮助行业内部人士识别和修复潜在的技术漏洞，还可以提高社区成员对安全实践的认知，进而促进更加稳健的技术发展和应用。此外，这样的分析挖掘能为监管机构提供制定相关政策和监管措施的依据，确保区块链技术的健康、可持续发展，并保护投资者和用户的合法权益。因此，对区块链生态共性安全风险的深入分析不仅是对过去和现状的总结，更是对未来可持续安全策略的关键铺垫。

3 区块链生态技术共性安全风险分析

本节从技术系统的视角，根据不同层级特点，对区块链的Layer0至Layer3层次结构所蕴含的风险进行了全面深入的分析，与社会系统中存在的区块链生态应用共性安全风险形成互补。Layer 0和Layer 1是区块链的底层基础设施层，包括网络节点连接、提供算力的硬件和密码学电路等组件以及运行在其上的区块链共识算法、P2P网络连接协议和智能合约虚拟机，它们为区块链高层应用生态提供了基础设施和底层支持。Layer 2是一种解决Layer 1扩展性问题的方案，其目标是增加吞吐量，降低手续费并减少Layer 1网络拥堵，以太坊众多Rollup方案和其生态是Layer 2的典型代表。Layer 3主要是为开发人员提供工具和框架，从创建和部署去中心化应用程序（decentralized application, DApp），解决了不同区块链之间的互操作性问题，实现了真正的互操作性目标，其代表性生态应用是各种DeFi项目。针对Layer0-1层级，从风险成因、攻击案例、防护措施等多个维度刻画了其共性安全风险；对于Layer2层级，从实现方案原理出发，分析归纳了11个共性安全风险；Layer3最主要且最具代表性的应用是DeFi，因此本文从DeFi应用角度深入探讨Layer3层级共性安全风险。

3.1 Layer0-1 共性安全风险分析

Layer0为区块链基础设施层，Layer1为区块

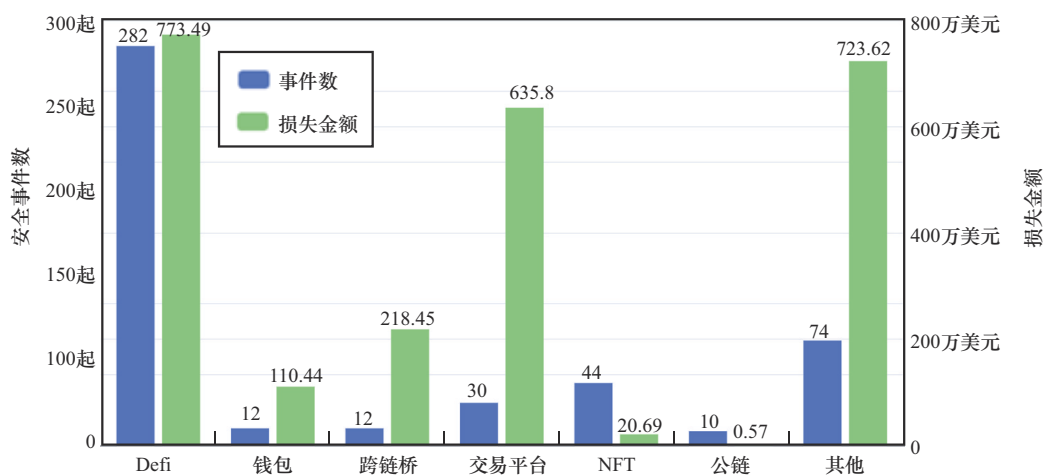


图6 2023年区块链项目安全事件赛道分布

Figure 6 Track distribution of blockchain project security incidents in 2023

链层，两者联系紧密，因此本节进行统一分析。表 2 汇总了区块链生态 Layer0-1 共性安全风险。数字钱包被盗风险涉及 OKcoin 交易所上的账户被盗，Gatecoin、Bitfinex 交易所遭受黑客攻击以及挖矿服务器 Nicehash 被黑客入侵等案例。例如，衡阳“9.15”特大洗钱犯罪集团案犯利用虚

表 2 Layer0-1 共性安全风险总结
Table 2 Summary of common security risks in Layer0-1

风险/攻击	成因	攻击案例	金额/损失	防护措施
51%攻击	PoW 或 PoS 共识算法底层机制 ^[22]	老牌公链 Aeternity 遭到黑客 51% 攻击；Bitcoin Gold (BTG)；Verge (XVG)	损失超过 3 900 万枚 AE 代币；1 800 万美元的 BTG	通过扩大节点规模等方式使得算力尽可能分散
数字钱包被盗	网络钓鱼、交易所被攻击，缺乏有效的安全防护措施而被攻击者实施漏洞攻击	至少 5 名用户在 OKcoin 交易所上的账户在同一时间被盗；香港“数字货币”交易所 Gatecoin 遭受黑客攻击；Bitfinex 交易所攻击；挖矿服务器 Nicehash 被黑客入侵	近 64 万元人民币的比特币和莱特币；200 万美元；45 亿美元；超过 4000 个比特币	增强应用层软件保护等方式在一定程度上加以防范
洗钱、多账户套利	不法分子使用基于密码学保证的强隐私类“加密货币”（如门罗币、达氏币、零币等）进行资产转移，赃款难以追踪	衡阳“9.15”特大洗钱犯罪集团案，犯罪团伙利用虚拟货币交易洗钱	400 亿元	从交易、地址与资产类别等不同维度提供洗钱风险监测与预警，能有效提升各类机构防范与打击虚拟货币洗钱活动的能力 ^[23]
私钥泄露攻击	去中心化特性使得私钥由节点自行保管；不易篡改特性使得用户密钥一旦泄露或丢失就会失去对账户资产的控制	OKX DEX 遭受私钥泄露攻击；用户遗忘私钥	276 万美元；9.3 亿美元（2022 年）	通过第三方机构托管或门限签名技术等方式来确保用户密钥的安全性 ^[24]
DDoS 攻击	攻击者通过超载目标系统的资源，使其无法正常提供服务	OKEx、Bitfinex 等交易所相继遭到 DDoS 攻击；Bitcoin 网络拥堵攻击	交易滞后、交易失败，甚至网络瘫痪	加强对网络攻击流量的监控识别，及时发现并清洗攻击流量；通过 PoW 等方式限制攻击者对节点资源的恶意占用
隐私信息泄露	交易信息公开	Monero 分析攻击：“加密货币”矿机制造商 Canaan 的服务器，窃取了大量的用户数据，包括用户名、电子邮件地址、IP 地址和设备信息 ^[25]	个人隐私泄露	匿名地址、隐私保护协议；对存储和传输的敏感数据进行加密
金融诈骗	区块链滥用、匿名性、创建欺诈性的投资方案、网络钓鱼	Bitconnect 投资平台卷款跑路事件；Octopaul 足球预测区块链平台卷款跑路事件	大量投资者总损失高达 36 亿美元；200 多万人民币	多因素身份验证；选择信誉良好、有安全措施的交易平台进行金融交易；定期监测账户活动，报告可疑/异常活动
智能合约代码漏洞	编程错误、逻辑缺陷或安全审计不足	The DAO 攻击；Parity 冻结；跨链互操作协议 PolyNetwork 遭黑客攻击	360 万个以太币；15.3 万个以太币；价值 6.1 亿美元加密资产被盗	安全审计和代码审查；输入验证和边界检查 ^[26]
量子计算攻击	量子计算机能够在同一时间处理多个状态，使得问题的求解速度大幅加快	基于 Grover 算法和 Shor 算法 ^[27] 的量子计算正对哈希函数和公钥密码算法构成极大的潜在威胁。	暂无	加快预研抗量子计算攻击的后量子密码 PQC 算法 ^[28]
哈希碰撞攻击	基于哈希函数的特性和算法的弱点	MD5 摘要算法碰撞 ^[29] 和 SHA1 摘要算法碰撞 ^[30]	暂无	提高哈希函数设计复杂度对抗攻击；使用开放地址法 ^[31] 、链地址法、再散列函数法

续表

BGP 劫持攻击	恶意操控互联网流量的路由对区块链节点的流量进行误导和拦截	Balancer.fi 遭受 BGP Hijacking 攻击, 访问该网站的链接后, 钱包会遭受钓鱼攻击; 黑客通过 BGP 劫持亚马逊 AWS 256 个 IP	暂无明确数值; 168 万的“加密货币”	建立专门用于区块链的去中心化网络
P2P 网络安全攻击	缺少传统中心化网络中的节点身份认证、网络入侵检测、通信数据验证等安全机制	Sybil 攻击; Eclipse 攻击	暂无	限制未经授权节点接入区块链网络、增加网络异常行为检测、修改节点连接设置等措施解决将面临被攻击风险 ^[32]
整数溢出攻击	数值超出所定义的整数类型范围 ^[33]	黑客攻击了 BEC 的 Token 合约, 通过一个整数溢出安全漏洞将大量 Token 砸向交易所; 黑客通过漏洞制造和抛售了天文数字规模的 SMT Token ^[34]	BEC 的价格几乎归零; SMT 价格崩盘	一方面可使用 OpenZeppelin ^[35] 建立 SafeMath 库进行程序编写; 另一方面可对运算逻辑进行验证
拒绝服务攻击	通过消耗合约资源让用户退出合约	KotET 安全漏洞事件; Govern Mental 合约代币遭到拒绝服务攻击	游戏玩家无论发送多少 ETH 给智能合约都无法成功竞争游戏中的“王位”; 1 100 个 ETH 被困在合约中	引入时间机制使得合约即便执行超时或者操作失败也能够继续执行; 可增设多个 Owner 账户共同治理合约, 必要时可考虑使用多签名请求方式来加强权限控制
无法获取异常攻击	Solidity 语言使得智能合约无法获取被调用合约中出现的异常信息	暂无	暂无	调用低级别函数后需对其返回值进行检查, 以便及时发现异常并进行处理
自私挖矿攻击	攻击者挖到新区块后不立即公布, 继续挖矿直到挖到第二个新区块后公布之前保留的新区块, 浪费诚实矿工的算力获取额外收益 ^[36]	暂无	暂无	文献[37]提出的挖矿难度调整公式加入了孤块数量, 使得自私挖矿不会比诚实挖矿更具优势

拟币交易进行洗钱, 涉及金额达到 400 亿元。为了应对这种风险, 可以提供洗钱风险监测与预警, 有效提升各类机构打击虚拟资产洗钱活动的的能力。

DoS 攻击和隐私信息泄露也是 Layer1 安全风险的一部分。DDoS 攻击是指攻击者通过超载目标系统的资源, 使其无法正常提供服务。隐私信息泄露是指交易信息的公开导致个人隐私泄露^[24], 如 Monero 遭受了分析攻击, 导致个人隐私泄露。

区块链的去中心化特性使得私钥只能由节点自行保管, 一旦私钥泄露或丢失, 用户就会失去对账户资产的控制。例如, OKX DEX 遭受私钥泄露攻击, 导致损失达到 276 万美元。为了确保用户私钥的安全性, 可以通过第三方机构托管或门限签名技术等方式来保护私钥。智能合约漏洞风险包括 The DAO 攻击、Parity 冻结和 Polynet-

work 遭黑客攻击等。此外, 智能合约代码漏洞、P2P 网络安全攻击隐私信息泄露也是安全风险的一部分, 保护用户隐私安全和加强网络安全措施对应对这些风险至关重要。

3.2 Layer2 共性安全风险

Layer2 是针对底层区块链 (Layer1) 扩容的一种链下解决方案, 扩展支付类和扩展智能合约类是目前 Layer2 技术方案的主要方式。根据 Optimism 基金会使用一阶逻辑^[38]对 Layer2 扩展技术的语义建模^[39], 任何 Layer2 的扩展实现, 如支付或状态通道、Validium、侧链、Plasma、Rollup 等都可以被抽象为 OVM (optimism virtual machine), 其特点是与以太坊主链兼容, 除状态通道外均可支持运行以太坊虚拟机 (ethereum virtual machine, EVM)。根据“加密货币”项目市值排行, Layer2 OVM 项目主要是针对以太坊的扩展方案, 如市值排行前 100 的 OVM 项目有

Polygon(Matic)^[40]、Arbitrum^[41]、Optimism^[42]、Metis^[43]、StarkNet^[44]等,关于比特币的 Layer2 上市项目很少,因此本文聚焦于以太坊 Layer2 OVM实现的安全风险分析,Layer2 共性安全风险有以下 11 种。

(1) 交易有效性未验证风险。Layer2 的交易有效性需要由节点或参与方进行验证。状态/支付通道交易的有效性由参与方自行验证,没有仲裁机构对争议进行仲裁,因此交易无效风险较高。对于侧链方案来说,由于侧链方案专门承担验证者角色的节点较少,因此有较高的交易无效风险,同样的情况存在于 Optimism Rollup 和 Plasma。近期取得进展的零知识证明(ZK) Rollup^[45]方案则不存在此风险,ZK Rollup 会在交易改变区块链状态后生成对应的 ZK proof,随后提交到主链上,因此主链上的任何参与方都能访问和验证 Proof 的有效性。

(2) 数据可获得性低的风险。数据可获得性^[46]是 Layer2 特有的属性,Layer2 会将某些必要的数提交到 Layer1 主链上,以备进行争议仲裁或灾备恢复,提交数据内容根据 Layer2 实现方案的不同而有所区别。支付/状态通道只将交易双方最终结算的余额结果提交到主链,中间交易数据不提交,因此这部分数据除交易双方外无法获取,数据可获得性最差。侧链和 Plasma 将区块头和交易的哈希值定期提交到主链上,其数据可获得性略微强于支付通道,但因为它们的交易数据不提交到主链而是自行存储,其数据可获得性仍然较差。Rollup 方案的数据可获得性是 Layer2 实现中最佳的,所有 Rollup 链的交易数据和状态改变的结果都会以压缩的形式提交到 Layer1 主链上,因此 Rollup 可提供最佳的争议仲裁和灾备恢复,数据可获得性最好。

(3) 数据不一致风险。所有 Layer2 实现方案因涉及与主链进行部分状态同步的问题,都有数据不一致的风险。支付通道的数据不一致风险因其与 Layer1 主链状态或数据同步最少而最高,侧链和 Plasma 次之,Rollup 因其将交易和状态信息都提交到主链上而将数据不一致风险降到了最低。

(4) 虚假交易风险。支付通道的结算需要所

有参与方共同确认才会进行,因此参与的交易方越多,伪造交易的风险越低。侧链和 Plasma 都因其数据可获得性差,存在伪造交易的风险。负责提交区块头到主链的节点可以虚构一个不存在的交易并提交到主链,同时此节点不把交易数据广播给 Layer2 中的其他节点和用户,导致交易的有效性无法被任何一方验证。Rollup 则不存在这个问题,原因是节点在提交交易结果的同时必须提交压缩的交易数据,若只有交易结果没有交易数据,则交易无效。

(5) 资产双花风险。支付通道中的所有交易在主链上最终确定,所以双花风险很低。其他 layer2 实现方案都有可能遭受双花攻击,攻击能否成功取决于子链与主链进行状态同步的速度和时间间隔,与主链的同步速度越快,越不容易产生双花攻击的风险。

(6) 资产无法结算风险。支付通道需要参与方共同确认才可以关闭,若有一方或多方共谋恶意阻止通道关闭,则支付通道无法关闭,导致用户资金无法完成结算而退出。用户进行资产结算退出侧链时,如果侧链的验证者(或矿工)不诚实或有恶意,他们可能会拒绝执行或处理正当的退出请求。另外一种情况是用户在退出侧链时,需要提交证明他们在侧链上的资产所有权的证据。如果侧链的数据不可用或者损坏,用户可能无法生成这样的证据,从而无法退出,造成这种情况的原因是侧链数据可用性差。

(7) 中心化程度与抗审查性^[47]。除了支付通道以外,其他 Layer2 扩展方案都存在中心化程度高的问题,这些扩展方案的出块节点一般由项目方运营,项目方为了节省运营成本和提高 Layer2 性能,往往只运行单一节点,一旦项目方节点故障,则 Layer2 可用性将大打折扣,且抗审查性也很弱。

(8) 验证者腐化或被贿赂风险。支付通道无第三方验证者,因此不存在这个问题。其他 Layer2 方案因其中心化特性都存在这个风险。近期有项目方如 Metis 提出了去中心化的 Layer2,只要质押一定数量的代币,任何人都能成为 Layer2 的出块或排序节点。

(9) 主链重组风险^[48]。这个风险是由

Layer2 锚定的 Layer1 主链重组导致的，如主链发生短暂的分叉，Layer2 提交的状态信息在主链其中一个分叉上，当主链消除分叉后，Layer2 可能需要重新提交状态信息。对于 Rollup 实现来说，其不只需要重新提交交易结果和世界状态，还需要重新提交压缩的交易数据，而其他 Layer2 实现方案则只需要重新提交区块头或者交易哈希。

(10) 资产永久锁定风险。这个风险所有 Layer2 实现方案都具有，这是因为用户在将资产转移到 Layer2 前需要将它们锁定到 Layer2 实现方案项目方提供的资产锁定智能合约中，若 Layer2 出现问题，则可能导致用户资产无法解锁或结算。

(11) 资产退出结算延迟。Layer2 还有一个实现中的缺陷是资产退出，Layer2 回到 Layer1 时结算无法立即完成，需要设定一定的挑战期限（通常为数天）进行合法性校验，若期限内无人提出证明交易不合法的欺诈证明，则通过挑战期。需要立即结算的场景或者需要 Layer2 和 Layer1 高速状态同步的 DApp 因此受限。近期，StarkNet 推出的 ZK Rollup 方案则自带有效性 ZK 证明^[49]，没有挑战期，可以快速结算。

Layer2 共性安全风险总结如表 3 所示。其中

主链重组风险无法避免，必须设计相应的缓解措施，这是以太坊主链因 PoS 机制经常出现暂时性的分叉导致的，在主链完成最终分片升级以前会一直存在。主链重组风险原理如图 7 所示。

如图 7 所示，Layer 2 链的状态信息需通过同步节点（排序器）提交到位于 Layer 1 主链的状态同步智能合约中永久保存。位于 Layer 2 的区块数据 ABC 已打包到 Layer 1 区块并且记录在 Layer 1 的状态同步智能合约中，这些 Layer 1 区块已得到足够多的确认并且位于最长合法链，而 Layer 2 区块 D 的状态虽然已完成同步，但所同步的区块位于 Layer 1 的暂时性分叉 1 中，这个分叉不在最长合法链中，最终会被回滚，对于 Layer 2 来说，发生了一次主链回滚事件，导致本来已同步状态的 Layer 2 区块变成未同步状态。

以上 Layer 2 安全风险根本上是 OVM 中心化架构本身的天然缺陷导致的。Layer 1 因其可扩展性差必然需要 Layer 2 进行扩容，而 Layer 2 因其与 Layer 1 主链的锚定关系导致其采用类 OVM 的实现方式，Layer 2 风险缓解方式如下：

- 1) 消除排序器中心化；
- 2) 排序器与区块提出者角色分离；
- 3) 采用非交互式验证器；

表 3 Layer2 共性安全风险总结
Table 3 Summary of common security risks in Layer2

OVM 方案	安全风险											Layer2 项目
	交易有效性未验证风险	数据可获得性	数据不一致风险	虚假交易风险	资产双花风险	资产无法结算风险	中心化程度	验证者腐化/贿赂	主链重组	抗审查	资产永久锁定	
状态/支付通道 ^[50]	高 (P2P 验证)	(差) 参与方自行存储	高 (链下数据争议)	反比于参与方数量	低 (主链结算)	高	低	无	低	强	可能	Connex ^[51] 、Celer ^[52] 、Petrin ^[53] 、Counterfactual ^[54] 、Interledger ^[55]
Sidechains (侧链) ^[56]	较高 (验证者节点数量少)	(较差) 侧链存储	高 (侧链数据与主链不同步)	高 (验证节点作恶)	取决于数据同步速度和时间	中等 (侧链与主链锚定机制不完善)	取决于实现	高	低	取决于节点数量	可能	Polygon、xDai ^[57] 、SKALE Network ^[58]
Rollups ^[59-60]	较高 (验证者节点数量少)	(强) 链上存储	低	低 (主链最终确定)	取决于数据同步速度和时间	低 (退出过程中可能出现争议)	高	高	高	弱	可能	Optimism、Arbitrum、StarkNet
Plasma ^[61]	较高 (验证者节点数量少)	(较差) Plasma 链存储	高 (Plasma 链数据与主链不同步)	高 (验证节点作恶)	取决于数据同步速度和时间	高 (退出失败或延迟)	取决于实现	高	低	取决于节点数量	可能	Kyber Network ^[62] 、Loom Network ^[63] 、OmiseGO ^[64]

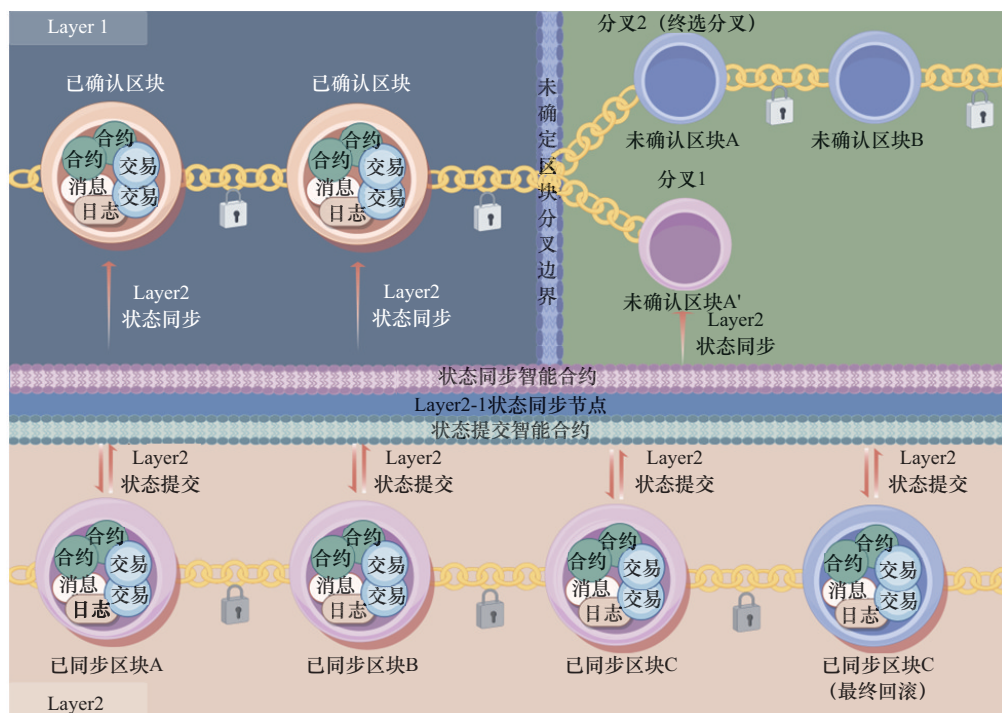


图7 主链重组风险原理

Figure 7 Main chain reorganization risk principle

- 4) 针对主链重组风险设计状态备份机制;
- 5) 采用去中心化社区治理方式, 减少对项目方的决策依赖;
- 6) 采用兼容EVM的异构高性能Layer 2链。

3.3 Layer3 共性安全风险分析

Layer3层为Layer2上的应用层, 其共性安全风险如表4所示, 主要有MEV (miner/maximal extractable value) 攻击风险、闪电贷攻击风险、Rug Pull攻击风险、吸血鬼攻击风险、预言机攻击风险等。

(1) MEV攻击: 矿工/验证者最大化可提取价值^[65]是指矿工(或验证者)在打包区块时, 通过改变交易顺序以获取额外的收益。MEV攻击可通过多种方式实现: 前置攻击、后置攻击、三明治攻击^[66]、损失与再平衡攻击(loss versus rebalancing, LVR)^[67]。其中, 三明治攻击通过在受害者交易前后进行操作, 即前置和后置攻击结合, 巧妙实现了低风险套取利润。三明治攻击如图8所示, 一般步骤如下。

- 1) 攻击者在内存池中不断搜索潜在的受害者交易。
- 2) 攻击者将这个交易组合顺序发给矿工/验

证者, 进行竞价确定交易位置, 出价最高者的组合顺序确定为最终交易执行顺序。

3) 矿工/验证者成功出块, 交易得到确认后攻击者通过智能合约将出价金额转给矿工/验证者。至此完成一次三明治攻击, 攻击者继续搜索下一个潜在受害者交易。

在文献[68]所描述的案例中, 攻击者通过在受害者交易前插入一笔前置交易, 在受害者交易后追加一笔后置交易。在这一过程中, 攻击者仅使用4.4个WETH作为初始资金, 却赚取了34.7个WETH, 成功发起了一次三明治攻击并最终获利9.6万美元。出现MEV攻击的主要原因是去中心化交易所(decentralized exchange, DEX)采用的自动做市商(automated market maker, AMM)协议存在设计缺陷。此类自动做市商通常采用恒定乘积函数来维护交易对的流动性, 即式(1):

$$X_1 \cdot X_2 = K1 \quad (1)$$

其中, $X_1 \cdot X_2$ 分别表示两种代币的储备量。在不考虑交易费用的情况下, 交易前后储备量乘积保持不变, 始终为 X_T 。由于恒定函数的特性, 在

表4 Layer3 共性安全风险总结
Table 4 Summary of common security risks in Layer3

风险	风险成因	风险是否可持续	攻击案例	财产损失	缓解措施
MEV 攻击	交易执行顺序可以被操纵，并获取额外利润	是	黑客持续通过三明治攻击捆绑受害者交易	每次三明治攻击平均造成上百美元的损失，最高损失可达10万美元	尽可能地将大宗交易拆分为许多小交易；设置自动滑动容差；建立MEV拍卖平台
闪电贷攻击	无抵押借入大量资金，操纵市场，获得巨额利润	是	Harvest Finance 在 Curve 中的储备资产价格被黑客操纵	攻击者以远低于储备资产价值的价格购买这些资产，最终获利3 400 万美元	自动检测价格操纵攻击
Rug Pull	投资项目管理者在收取投资者资金后放弃项目，使投资者获得无价值资产	否	Arbix Finance 被攻击者引诱购买没有价值的资产	攻击者从金库中榨干了约1 000 万美元的用户资产	投资者应谨慎行事，并在投资前始终确认项目的可信度；持续跟踪投资项目的审计信息
吸血鬼攻击	激励一个平台的流动性提供商将他们的 LP 代币入股到一个新平台，从而窃取该平台的流动性	否	Sushi 发布吸血鬼游戏，鼓励 Uniswap 的流动性提供商将其 LP 代币存入 Sushi	最终 Sushi 从 Uniswap 提取了约8 300 万美元的流动性	对协议代码库应用限制性许可证
预言机攻击	部分借贷平台通过唯一价格预言机获取外部市场价格。如果外部市场被攻击者操纵，抵押品价值被严重错估，从而低价买入或高价抵押，最终获取利润。与闪电贷组合使用	是	黑客操纵 SushiSwap INV-WETH 池的 INV 价格，使得 Inverse Finance 使用 SushiSwap 作为价格预言机时，INV 价格被严重夸大	攻击者抵押 1 700 个 INV（实际价值约 6.44 万美元），借出总价值约 1 560 万美元的资产	使用时间加权平均价格预言机；聚合来自多个独立数据提供商的价格数据

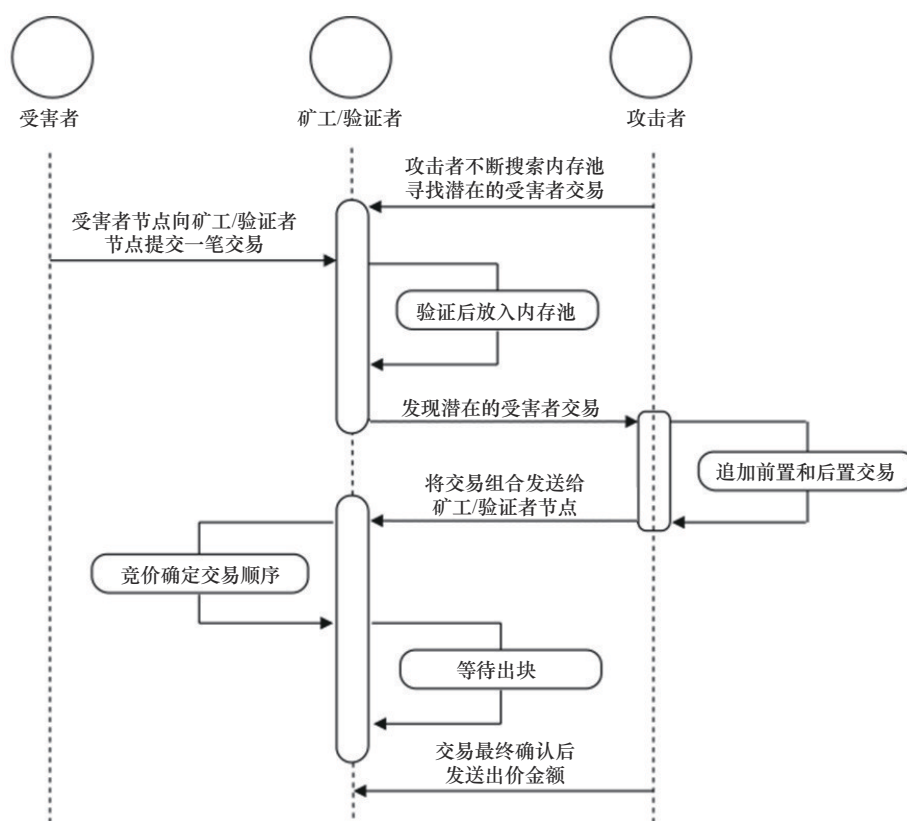


图8 三明治攻击

Figure 8 Sandwich attack

AMM上交易存在滑点问题,即用户实际成交价格不等于用户的预期价格。例如,一个用户想要用 p 个代币2换取代币1,假设能够换取 q 个代币1,交易将遵循式(2)执行。

$$(X_1 - q)(X_2 + p) = X_1 \cdot X_2 \quad (2)$$

可化简为式(3):

$$q = \frac{pX_1}{p + X_2} \quad (3)$$

最后可变换为式(4):

$$\frac{q}{p} \neq \frac{X_1}{X_2} \quad (4)$$

正是滑点问题的存在,攻击者才有从三明治攻击中获利的可能。针对MEV攻击,有多种缓解措施,Patrick等^[69]通过订单拆分的方法,将大宗交易拆分为多个小交易,避免三明治攻击盈利机会的出现;Xavier等^[70]设计了一种可验证的交易排序规则,允许矿工/验证者通过操纵交易顺序获利,但是被操纵的交易不会因排序变更出现额外的损失;Heimbach等^[71]设计了一个博弈论模型,通过受害者和攻击者的角度分析三明治攻击,提供了一种设置滑动容差的算法来避免三明治攻击

的发生,最后分析表明,其算法优于Uniswap的恒定容差算法;Chemaya等^[72]在之前研究的基础上提出了自动滑动容差的算法,Uniswap v3已经从恒定滑动更改为自动滑动^[73];文献[74]重新设计了AMM机制,提出了一种基于时间加权平均的做市商(time-weighted average market maker, TWAMM)机制,也是将大宗交易通过其算法拆分为多个小型交易;Daian等^[75]提出了MEV拍卖平台,旨在建立提取MEV的规范秩序。

(2) 闪电贷攻击:攻击者可以通过闪电贷平台无抵押地借入大量资金^[76],操纵市场从而达到获取利润的目的。闪电贷攻击如图9所示,一般分为4步。

- 1) 攻击者通过闪电贷平台无抵押借入大量代币。
- 2) 攻击者利用借入的代币在DEX或其他交易平台上进行大量买入或卖出,操纵目标代币的价格。
- 3) 通过价格操纵,攻击者可能会对一些抵押贷款平台进行预言机攻击,使其高估或低估抵押品的价值,以高价抵押或低价收购代币获取利润。
- 4) 在完成所有交易并获取利润后,攻击者立即归还闪电贷。

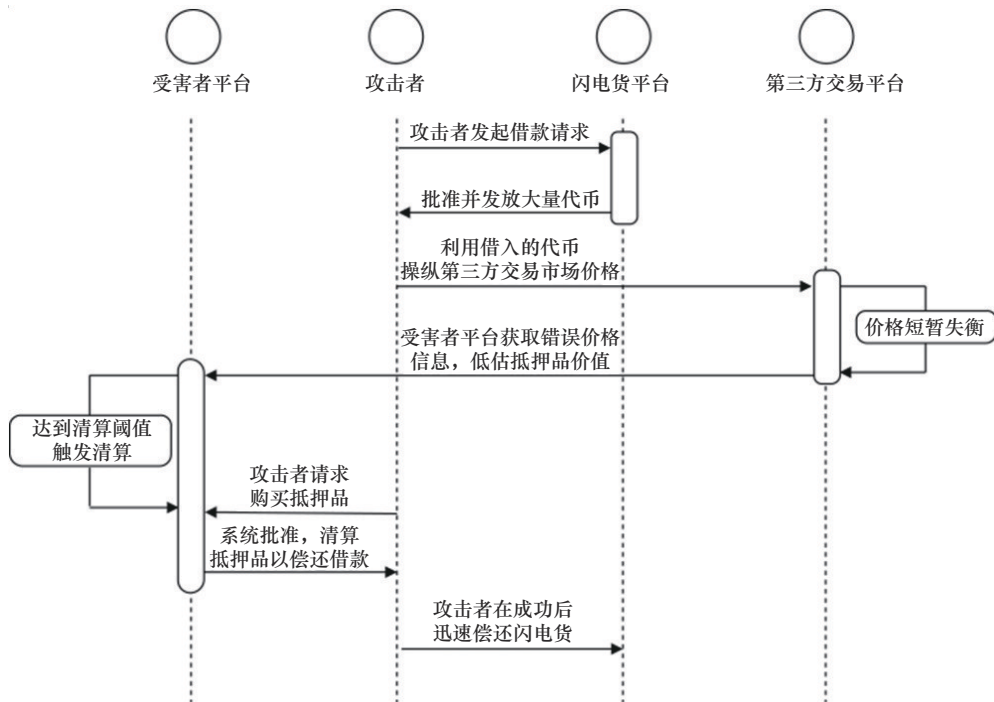


图9 闪电贷攻击

Figure 9 Flash loan attack

例如，攻击者通过闪电贷暂时操纵了 Harvest Finance 在 Curve 中持有的储备价值^[77]，压低了 Harvest 上 USDT 和 USDC 的价格，使攻击者能够以远低于其价值的价格购买这些代币，并偿还闪电贷，最终获利 3 400 万美元。

针对闪电贷攻击已经有相关研究，Qing 等^[78]提出了自动检测价格操纵攻击的方法，并在以太坊的前 14 50 万个区块上进行了实验评估，检测到了约 180 次攻击，准确率约为 78.9%；Cao 等^[79]设计了 Flashot 工具，能够在每个 Flashloan 事件中以标准化图表精确地说明资产流。

(3) Rug Pull 风险：Rug Pull 是指项目管理者在收取投资者资金后放弃项目，给投资者留下无价值的资产^[80]。进行这种骗局的一种方法是引诱收益农场协议购买没有价值的资产，然后将该资产换成 ETH 或另一种有价值的资产。例如 Arbix Finance^[81]，在没有任何先进攻击技术的情况下，攻击者直接从金库中榨干了约 1 000 万美元的用户资产。为了防止 Rug Pull，投资者应谨慎行事，并在投资前始终确认项目的可信度^[82]。此外，持续跟踪投资项目的审计信息，使投资者能够快速识别风险并采取适当措施，从而减少损失。

(4) 吸血鬼攻击：吸血鬼攻击^[83]是一种策略，其第一步是诱导平台的流动性提供商将他们的 LP 代币（代表提供的流动性数量）投资到一个新平台。当新平台成功吸引足够的流动性后，吸血鬼攻击进入第二阶段，即把质押的 LP 代币转移到新平台。通过这一手段，新平台能够利用转移的流动性为其自动化做市商服务，不仅窃取原有平台的流动性，还夺走其交易量和用户。以 SushiSwap 为例，Uniswap 的流动性提供商将 LP 代币抵押在 SushiSwap 上，以换取额外的 Sushi 代币奖励^[84]。在 SushiSwap 的吸血鬼攻击事件之后，Uniswap 采取了法律手段进行反击，如对协议代码库实施限制性许可证。

(5) 预言机攻击：由于部分贷款平台将去中心化交易所作为唯一价格预言机，攻击者通过闪电贷短时间内获取大量资金，利用 DEX 滑动机制，扭曲两种代币之间的相对价格，若攻击者操纵价格使得贷款平台的抵押品价格被严重低估，

则能够以远低于其价值的价格购买这些抵押品，最终实现盈利目的；相反，若抵押品价格被严重高估，则攻击者抵押资产，以远超出其价值的价格借出大量资金，同样获取大量利润。例如，一名攻击者在 SushiSwap INV-WETH 池中将 500 个 ETH 换成 1 700 个 INV，从而操纵 INV 的价格，使 INV 的价格上涨了约 50 倍，引导贷款平台 Inverse Finance 使用 SushiSwap 作为价格预言机，预言机返回的 INV 价格被夸大^[85]。

预言机攻击可以通过时间加权平均价格预言机（time weighted average price, TWAP）^[86]来解决，但是这种解决方案只能确保价格不会在同一区块内被操纵。目前比较主流的方案是聚合来自多个独立数据提供商的价格数据，确保价格不容易被操纵^[87]。

4 区块链生态业务安全风险分析

区块链生态业务安全风险通常是区块链技术改变了原有传统业务模式和逻辑所带来的，其业务安全风险分类如图 10 所示，具体可以进一步细化为业务数据安全风险、业务应用安全风险和业务监管安全风险 3 个维度。

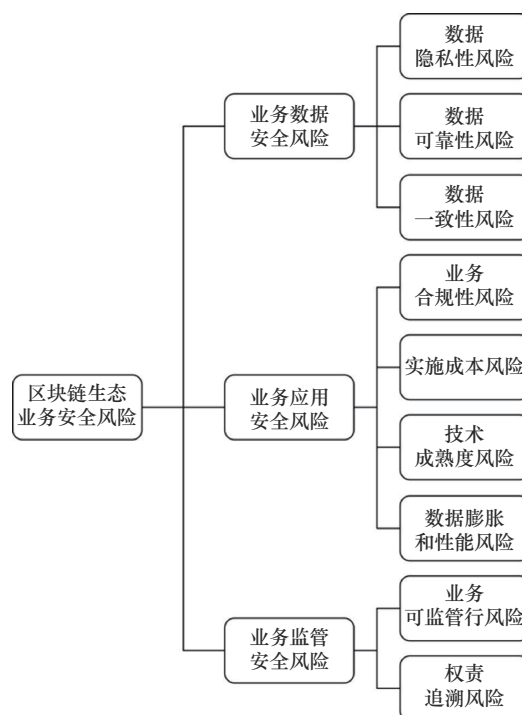


图 10 区块链生态业务安全风险分类
Figure 10 Refined classification of security risks in blockchain ecological business

4.1 业务数据安全风险

业务数据安全风险主要源于区块链的固有特性或技术缺陷在某些应用场景中的放大效应。这不仅限制了区块链技术在实际应用中的广度、深度与长久性,而且可能给经济和社会带来损失。区块链生态业务数据风险具体包括数据隐私性风险、数据可靠性风险以及数据一致性风险。对这 3 种风险的评估如表 5 所示。

4.1.1 数据隐私性风险

区块链生态中的隐私问题主要涉及交易隐私和用户身份信息隐私。用户身份信息隐私表示区块链账户背后的实体身份信息;交易隐私是指区块链中各种账户交易信息。尽管区块链技术因其透明性而受到推崇,增强了系统的信任度,但这一特性可能导致用户交易和身份数据的潜在暴露,引发隐私问题。例如,攻击者能够通过长期监测链上交易的元数据,掌握链上任何账户地址的行为动态,并“追溯”出交易背后的现实参与方。此外,通过大数据分析,攻击者还可能轻易找到用户的公钥,并进一步结合公开的交易时间、交易内容以及交易者信息,从而确定公钥的实际所有者。区块链底层技术依托于非对称加密和哈希算法等密码学加密算法,确保只有密钥持有者能

访问数据。私钥的个人管理也存在风险,一旦私钥遗失或受到恶意软件攻击,相关数据可能永久无法访问或面临泄露风险。随着量子计算发展和密码分析技术的进步,实用的密码体制存在安全威胁,未来被破解的可能性很大,量子计算对密码学体制的影响如表 6 所示。尽管哈希算法(如 SHA 256),以其强大的抗碰撞性被视为相对安全,但不可否认的是,对于对哈希算法的碰撞攻击^[88]以及针对 Merkle-Damgard 散列函数(在区块链中被广泛使用的 SHA.256 也是此类算法)的长度扩展攻击^[89]仍然存在。此外,由于区块链技术的业务拓展和广泛应用,接入节点数量将呈指数级增长。然而,这也将带来隐私泄露风险的成倍增长。

4.1.2 数据可靠性风险

2019 年, Synthetix 的一个喂价渠道上传了错误的韩元价格,报价比真实汇率高出近千倍,一个交易机器人因此获得超过 10 亿美元的利润^[90]。区块链的核心优势在于其数据不易篡改性,但这一特性同时引出了一系列的数据可靠性问题。数据可靠性是指数据的完整性和准确性,衡量数据在不同时间段内和来源的一致性和无误性^[91]。区块链数据可靠性风险主要有以下 3 方面。

表 5 业务数据安全风险评估
Table 5 Business data security risk assessment

业务数据风险	含义	发生场景	潜在影响	影响范围	发生概率	风险优先级
数据隐私性风险	个人身份信息或交易数据未经授权而被获取、使用或泄露	交易追踪和分析、身份信息关联识别、量子计算机破解密码体制、私有泄露或遗失	个人隐私泄露、商业秘密泄露、经济损失	广	高	高优先级
数据可靠性风险	链上数据失真、数据完整性被破坏	数据源错误、私钥安全受损、智能合约缺陷	经济损失、信任下降	广	中	高优先级
数据一致性风险	不同节点上的数据无法保持一致性	网络分割、共识机制故障、交易确认延迟、区块链分叉	交易无效化、双重支付、网络分裂	广	低	高优先级

表 6 量子计算对密码学体制的影响
Table 6 The impact of quantum computing on cryptography

加密算法	类型	作用	安全基础	安全性威胁
AES	对称密码	加密	—	攻击难度减半
SHA256	哈希函数	数据指纹	—	攻击难度减半
RSA	非对称密码	签名、密钥交换	大整数分解	可被完全破解
ECDSA、ECDH	非对称密码	签名、密钥交换	椭圆曲线离散对称	可被完全破解
DSA	非对称密码	签名、密钥交换	离散对称	可被完全破解

首先, 区块链技术的一大优势在于它能够确保链上数据的完整性。然而, 这种机制也存在一个不可忽视的局限性: 当数据源本身就存在失真或错误时, 这些不准确的数据也会被记录在区块链上。在此情况下, 区块链只能维持这些失真的链上数据, 并且无法纠正或更改错误数据。与专门用于代币交易的区块链系统不同, 区块链在各类业务场景的应用主要是为了将各类信息上链, 而这些信息的验证比交易的验证复杂得多。当前市场上缺乏能够有效检测信息内容是否合法的工具^[92]。

其次, 区块链技术的去中心化存储和私钥分布式存储特性, 虽然在一定程度上提高了数据的安全性, 但存在潜在的安全风险。黑客若成功获取私钥, 便可能进行非法操作, 导致数据的完整性受到破坏。区块链的数据安全性在很大程度上依赖于私钥的安全。如果私钥泄露或被盗, 那么该安全机制就会失去作用。

最后, 智能合约核心本质为一段代码程序, 通过自动化执行代码实现契约的缔结与履行。然而, 如果智能合约代码在设计和编写过程中存在疏漏或错误, 就可能引发一系列风险。这些风险包括但不限于数据记录错误、恶意篡改的风险, 甚至可能导致整个系统发生故障, 产生严重的负面影响。历史上的The DAO被攻击事件是一个深刻的教训。一旦错误的信息被存在链上, 它将迅速扩散至整个网络, 进而对所有用户构成威胁, 甚至可能带来严重的经济损失或风险。

4.1.3 数据一致性风险

一致性问题分布式领域最基础、最重要的问题, 也是研究热点^[93]。区块链中的数据一致性是指整个区块链网络中所有节点上的数据是一致的。区块链数据不一致将影响区块链应用的可靠性、稳定性和安全性, 如在代币系统中, 可能导致已确认的交易被撤销, 或者相同的资产被多次支付(双重支付)。造成数据一致性风险的主要原因如下。

网络分割: 如果区块链网络中的节点被分割成互不通信的子网, 每个子网内的节点可能会形成各自不同的区块链视图, 从而导致数据一致性问题。

共识机制故障: 区块链依靠共识机制来确保网络中的所有节点都同意数据的当前状态。如果共识机制出现故障, 如在某些节点未能正确执行或存在恶意节点试图破坏共识过程, 那么数据一致性也会受到影响。

交易确认延迟: 在一些区块链系统中, 交易需要被网络中的大多数节点确认后才会被认为最终确定。如果网络通信存在延迟, 或者有大量交易需要处理, 这可能导致交易确认被延迟, 从而影响数据一致性。

软硬分叉: 区块链网络中的软分叉或硬分叉可能导致数据一致性问题。分叉发生时, 网络中的节点可能会暂时或永久地在不同的链上继续记录交易, 直至分叉解决损失。

4.2 业务应用安全风险

业务应用安全风险指区块链技术应用后对原有业务运行规则变革带来的风险, 包括业务合规性风险、实施成本风险、技术成熟度风险、数据膨胀和性能风险。对这4种风险的评估如表7所示。

4.2.1 业务合规性风险

2019年, Libra遭遇了全球监管机构的审查, 以确定其业务运营是否合规^[94]。业务合规性是指在遵循相关法律、政策和行业标准的前提下进行企业或个人业务活动的过程^[95]。虽然区块链技术在提升业务效率、降低运营成本等方面展现出显著优势, 但其固有特性也给业务合规性带来了新的挑战。首先, 区块链的去中心化属性排除了单一实体对系统的控制, 这在提高系统抗脆弱性的同时, 为监管机构监督确保各参与方遵守相关法律法规带来了挑战。特别是在涉及跨法律辖区的场景中, 缺乏中央监管实体使得实施统一的合规标准更加困难。其次, 尽管区块链可以提供高度的数据透明度, 但其匿名性或伪匿名性特点可能被用于逃避监管或从事非法活动。此外, 区块链技术的不易篡改性确保了数据的持久性和不变性, 这在很多应用场景中是一个优势。然而, 当出现数据录入错误或需符合如GDPR之类的数据保护法规要求时, 不易篡改性可能转变为合规难题。这一特点在防止数据篡改的同时限制了对非法

表 7 业务应用安全风险评估

Table 7 Business application security risk assessment

业务应用风险	含义	发生场景	潜在影响	影响范围	发生概率	风险优先级
业务合规性风险	区块链应用在设计时可能违反相关的法律、政策和行业标准	跨法律辖区、利用匿名性从事非法活动、链上错误信息无法更正	法律违规、商誉损失、业务中断	中等	较高	高优先级
实施成本风险	应用区块链过程中的高额成本问题	技术研发与升级、系统整合、运营维护、能源消耗	项目延期或失败、财务压力、投资回报率低	中等	较高	较高优先级
技术成熟度风险	区块链技术存在潜在的技术不足或缺陷，可能影响系统的可靠性、安全性和性能	跨领域应用、系统升级、新技术引入	系统故障、安全漏洞、投资风险	中等	较高	较高优先级
数据膨胀和性能风险	区块链不易篡改带来的数据只增不减问题	所有应用区块链技术的场景	存储与维护成本增加、查询性能降低	大	随时间增加	较低优先级

或错误信息的更正能力。最后，区块链的跨境特性带来了法律管辖权的复杂性，不同国家和地区对区块链的监管态度和法规存在差异，可能导致企业在多法域中经营时面临法律适用和管辖权冲突的合规风险。

4.2.2 实施成本风险

区块链技术作为一种前沿技术，为不同行业带来了创新的机遇，但与此同时，其应用实施伴随着诸多挑战和成本问题。当前，区块链技术在市场中的认知并没有达到很高的程度，技术的整合所需成本也很高。区块链基础架构本身还在不断发展和优化中，若基础技术存在缺陷，则难以确保最终应用的安全性，可能导致实际运营中出现难以预测的问题。特别是，在区块链技术替代传统中心化系统的过程中，尽管长期看来可以带来效率提升和成本降低，但短期内所需承担的更新和过渡成本可能对许多组织来说难以承受。目前，设计一款成熟的区块链应用程序并非易事。多种因素（如隐私保护、可扩展性以及互操作性等）在一定程度上限制了这些方案的实际运用。同时，在实际运行的区块链中，存在算力消耗大的问题，如基于区块链的 EHR 需要消耗大量的计算能力，并需要大量的时间来执行任务，实现成本和能源消耗成为许多企业面临的关键挑战之一。在实际应用中，区块链解决方案往往需要与现有业务流程和系统集成，这可能引发兼容性问题 and 额外的成本。在现实场景中，各种业务难以权衡，在最终的功能指标上，实际的区块链应用

甚至不如传统中心化应用。区块链的可拓展性问题也影响了其在大规模应用场景中的部署和业务拓展。

4.2.3 技术成熟度风险

尽管区块链经历了一段相对较长的发展，但区块链技术的成熟度在很多方面还有待提高，包括底层链技术的设计、研发和改进，以及性能和容量上的短板，还有相关从业人员不足等问题。此外，区块链技术在非金融领域尚处于应用探索阶段，相应相关配套系统和上层 DApp 开发在应用过程中可能面临安全漏洞的风险，如运行环境、交互页面和移动端支持等。

区块链技术正在快速发展和迭代中，许多新的特性、协议和优化持续被引入。尽管这种快速迭代有助于技术进步，但同时意味着现有的解决方案可能迅速过时，企业和开发者需要不断跟进最新技术，增加了应用开发和维护的复杂性。为了降低技术成熟度所带来的风险，关键措施包括加大对区块链底层技术的投入、推动技术标准化，以及强化专业人才培养。同时，开发区块链应用时应采用灵活的架构，确保系统可适应技术更新。此外，必须对区块链系统进行全面的安全评估和定期的技术审查，确保能够应对新出现的安全威胁。建立应急响应机制也至关重要，以保障在面对技术故障或安全事件时能迅速采取行动，维护系统稳定和数据安全。

4.2.4 数据膨胀和性能风险

区块链技术以其分布式存储特性提升了网络

透明度和数据不易篡改性，但这带来了数据膨胀的挑战。随着区块链的持续运行，存储需求不断攀升，尤其是全节点需保存全部历史数据，导致运营成本上升和处理效率下降。同时，新节点的数据同步时间延长，复杂化了数据管理任务，提高了技术维护要求。加密猫（Crypto Kitties）在2017年的流行是一个突出实例，它导致以太坊网络的交易拥堵、处理时长增加及燃料费用上升^[96]。此外，数据量增长还可能引发性能问题，尤其在需要处理大量并发访问的场景下，如政务应用，可能导致网络拥堵和延迟。区块链的性能，尤其是交易处理速度，受共识机制和网络带宽限制，现有机制（如PoW）虽性能稳定但处理速度缓慢，而较新的机制（如PoS）虽处理速度快但可能牺牲一定程度去中心化。

4.3 业务监管安全风险

业务监管安全风险是从宏观层面考察区块链技术加入对既有法律体系造成冲击与不稳定所带来的风险，包括业务可监管性风险和权责追溯风险。对这两种风险的评估如表8所示。

4.3.1 业务可监管性风险

区块链与各类应用场景的结合为社会发展开启了新纪元，为各行业带来了前所未有的变革与机遇，但也伴随着一系列新的问题形式，这要求当前监管机构推动革新，提供更加多元化和精细化的监管策略。传统的监管政策在面对区块链技术所催生的复杂金融活动时，显得力不从心。监管层在全面评估区块链技术对企业、机构、用户及整个社会的风险时遇到了极大的挑战，现有的统一监管制度难以适应多样化的应用场景。

目前，监管机构面临着两大主要困境^[97]。首先，监管规则无法跟上区块链技术的快速迭代与创新，导致监管滞后于市场实践，无法及时有效地规范区块链业务活动。其次，区块链的去中

心化特性与现有中心化的监管模式之间存在本质矛盾。区块链技术通过去中心化的方式实现了数据的安全与透明，但同时使得监管机构难以获取必要的数据进行风险监测和评估，这无疑增加了监管的难度。

鉴于区块链技术的独特性，监管机构在收集和分析网络运行数据方面面临着巨大的挑战。这种技术特性导致对区块链技术的风险评估变得尤为困难，因为监管机构在评估区块链业务的风险程度时，缺乏必要的的数据支撑。这种数据不足的情况进一步增加了风险识别与防范工作的复杂性。在基于区块链的解决方案中，监管机构的角色变得更为关键和复杂，需要更加审慎和全面地考虑各种风险因素。由于区块链技术的新兴性和不确定性，监管机构在界定其法律边界和监管环境时面临着巨大的挑战。当一个新的交易在区块链网络中发生时，监管机构往往难以明确界定相关利益方的法律义务和管辖权。因此，区块链技术与现行法律法规之间的不匹配也是一个不容忽视的问题，并且世界各国对于区块链的态度不一致，很难有唯一的标准来约束这些基于区块链的方案。同时，传统监管体系中的很多法律法规本身就是不完善的，这使得在区块链技术的赋能下，监管工作变得更加复杂和艰巨。

4.3.2 权责追溯风险

在区块链生态中，权责追溯面临多重风险，尤其体现在匿名性与责任归属、分布式架构、交易不可逆性以及智能合约的自动执行等方面。首先，区块链的匿名性或伪匿名性虽然保护了用户隐私，却给追踪交易背后真实身份带来难题，特别是在处理非法交易或安全漏洞时，确定责任主体异常复杂。其次，区块链去中心化和分布式特点导致数据和资产管理责任分散于众多节点，使得在没有清晰监管和责任界定机制的情况下，责

表8 业务监管安全风险评估

Table 8 Business regulatory security risk assessment

业务监管风险	含义	发生场景	潜在影响	影响范围	发生概率	风险优先级
业务可监管性风险	传统监管模式难以适用区块链应用	跨境交易、去中心化金融、智能合约执行	监管真空、非法活动、法律冲突	广	高	高优先级
权责追溯风险	无法准确确定和追踪交易参与者身份和行为责任	非法交易处理定责、智能合约错误定责	信任缺失、法律责任难界定、经济损失	中等	较高	高优先级

任追溯变得更加困难。此外，一旦区块链上的交易被确认，其不可逆特性对于错误或欺诈交易的纠正构成挑战，需要在遵循区块链原则的同时，寻找有效的纠纷解决途径。智能合约虽然提高了执行效率，但可能因漏洞或设计缺陷引发错误行为，加剧责任归属的不确定性。面对区块链的权责追溯风险，关键缓解措施包括加强身份验证以平衡匿名性与责任追溯的需求，明确节点责任以促进有效的责任划分，以及开发交易可逆性机制和强化智能合约的安全审计。这些措施不仅针对区块链技术的匿名性和分布式特性所带来的挑战，还解决了交易不可逆性和智能合约自动执行可能引发的责任归属问题，从而提升了区块链系统的可追溯性和整体安全性。

5 讨论

5.1 区块链生态安全目标

本节根据区块链生态存在的共性安全风险归纳出了六大核心安全目标：数据安全、共识安全、合约安全、私钥安全、系统安全和监管安全。这些安全目标共同构筑了区块链安全体系的坚实基础，对于保障区块链项目的稳定运行具有至关重要的意义。

数据安全目标的核心在于保障区块链中存储和传输数据的机密性、完整性和可用性，防止任何未经授权的访问、泄露或篡改。共识安全目标则强调区块链网络中所有参与者对数据状态能够达成高度一致的共识。合约安全目标主要关注智

能合约的安全性，防止因合约漏洞或设计缺陷导致的安全事件。私钥安全目标旨在确保私钥的安全存储和使用，防止私钥泄露或被恶意攻击者窃取。系统安全目标则关注区块链技术本身架构、节点以及通信协议等的安全性。监管安全目标在于确保区块链技术和应用遵守相关法规和行业标准，以促进行业的健康发展。

通过结合这六大安全目标，本文构建了一套全面且多维的区块链生态安全目标框架，如表9所示。此外，本文还构建了一个如表10所示的区块链项目三级度量标准，该标准根据ISO 27005和ISO 31000标准改编而成^[98]。在对一个区块链项目进行安全评估时，可以从六大安全目标出发，针对每个安全目标的评估指标对区块链项目进行评分，最后通过权重计算出综合评分，从而评估出该项目的安全等级和风险程度。这一标准为区块链风险管理提供一个系统的评级机制，有助于确保区块链技术的健康、稳定发展，并推动其在社会系统中的广泛应用和深度融合。

5.2 展望

随着区块链技术的快速发展，其在各个行业的应用前景广阔，但安全仍然是至关重要的考量。

在数据安全领域，随着数据价值的不断提升和隐私保护意识的增强，区块链技术将更加注重数据的加密和隐私保护。新型加密技术（如零知识证明、同态加密等）将得到更广泛的应用，以确保数据的机密性、完整性和可用性，从而构建

表9 区块链生态安全目标框架

Table 9 Blockchain ecological security objective framework

安全目标	关联风险	评估指标	缓解措施
数据安全	数据隐私性风险、数据可靠性风险	数据保密性、数据完整性、数据可用性	实施数据加密、访问控制、备份和恢复机制
共识安全	数据一致性风险	活性、一致性	采用稳定可靠的共识算法，优化网络响应和处理速度
合约安全	数据可靠性风险	编写安全、运行安全	进行智能合约审计，采用形式化验证和漏洞检测工具
私钥安全	数据隐私性风险、数据可靠性风险	使用安全、保管安全	引入硬件钱包、多重签名、密钥管理方案
系统安全	数据隐私性风险、实施成本风险、技术成熟度风险、数据膨胀和性能风险	系统架构安全、通信安全	采用分层架构、安全协议、性能优化和监控机制
监管安全	业务合规风险、业务可监管风险、权责追溯风险	合规性审查、监管透明性	增强法规遵循、引入第三方审计、建立法律顾问团队

表 10 区块链项目三级度量标准
Table 10 Three-level metrics for blockchain projects

安全 评分	安全 等级	安全目标					
		数据安全	共识安全	合约安全	私钥安全	系统安全	监管安全
0-60	低危	数据加密和访问控制措施较为完善，能够基本保证数据保密性、完整性和可用性	共识机制稳定，基本无一致性问题，活性较高	合约代码审计清晰，编写和运行安全，潜在漏洞极少，风险可控	私钥管理严密，极小概率的安全威胁，基本保证私钥使用和保管安全	系统架构和协议设计健全，需进一步强化防御措施	法规遵循良好，合规性风险极低，监管透明度好
60-80	中危	基本数据加密措施，存在潜在的未授权访问风险，无法完全保证数据保密性、完整性和可用性	共识机制较稳定，偶有一致性问题但能快速恢复，共识活性一般	合约代码未经完全审计，存在已知的小漏洞，无法完全保证编写和运行安全	基本私钥存储和管理安全措施，存在被窃风险，无法完全保证私钥使用和保管安全	系统架构和协议设计较为安全，存在已知安全问题	存在部分合规性漏洞，需要改进以提升监管透明度和合规性
80-100	高危	数据安全机制薄弱，高风险的未授权访问和数据泄露	共识机制出现严重问题，难以保证数据一致性	合约存在严重漏洞，未进行安全审计，风险高	私钥安全机制薄弱，极高的被窃或丢失风险	系统存在严重安全缺陷，需紧急采取补救措施	法规标准不符，面临严重合规问题

更加安全的数据环境。在共识安全方面，随着网络规模的扩大，高效稳定的共识机制成为关键。拜占庭容错、DAG 技术等新型共识算法将不断优化，确保网络在大规模、高并发场景下依然能够保持活性、一致性和安全性，降低分叉和延迟风险。智能合约作为区块链技术的重要应用之一，其安全性也将得到更多关注。随着智能合约应用场景的不断拓展，对合约代码的审计和测试将变得更加重要。形式化验证、自动化测试工具等技术手段将得到进一步应用，以确保智能合约的正确性和安全性，避免潜在的安全风险。私钥作为区块链安全的关键环节，其管理也将成为未来发展的重要方向。随着用户对私钥安全意识的提升，更加安全、便捷的私钥管理方案将不断涌现。多因素认证、生物识别技术、去中心化身份验证系统等新型技术将应用于私钥管理，提高私钥的安全性和易用性。此外，随着区块链技术的广泛应用并与其他技术的融合，系统安全将面临更多挑战。区块链技术将需要更加注重链上与链下系统的安全整合，以及与其他技术的安全协同。安全的 API 设计、可信的执行环境、跨链安全等将成为研究的重点，以确保整个系统的安全性和稳定性。在监管环境方面，随着区块链技术的普及和应用领域的拓展，相关法规和监管政策也将不断完善。区块链项目需要在遵守法规的前提下进行设计和运营，确保合规性成为项目成功的关键要素。透明的治理机制、合规的数据处理以及清晰的责任追溯将成为区块链项目的基本要求，以提升技术的社会认可度和应用范围。

总体来说，未来区块链技术的发展将更加注重安全性，通过加强数据安全、共识安全、智能合约安全、私钥管理以及系统安全等方面的研究和应用，推动区块链生态的健康发展。同时，随着法规和监管政策的完善，区块链技术将在更加合规和规范的环境下得到广泛应用，为各行各业带来更加安全、高效和可靠的解决方案。

6 结束语

本文聚焦于区块链生态安全，结合社会技术系统理论对区块链生态共性安全风险进行了深入的界定和分类。将区块链共性安全风险划分为技术安全风险和业务安全风险，技术安全风险从 Layer0-Layer3 的分层结构角度分析每层技术本身和相应方案存在的风险和安全隐患；业务风险则从社会系统视角出发，分析由于技术系统革新所带来的风险和挑战。本文通过对每种风险进行详细分析和评估，总结风险成因、影响和缓解措施，为区块链生态的安全管理提供了有益参考。

参考文献：

- [1] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.
- [2] DIFFIE W, HELLMAN M E. New directions in cryptography[M]. Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman. 2022: 365-390.
- [3] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications

- of the ACM, 1978, 21(2): 120-126.
- [4] KOBLITZ N. Elliptic curve cryptosystems[J]. *Mathematics of Computation*, 1987, 48(177): 203-209.
- [5] MERKLE R C. A digital signature based on a conventional encryption function[C]//Conference on the Theory and Application of Cryptographic Techniques. Berlin Heidelberg: Springer, 1987: 369-378.
- [6] 马永仁. 区块链技术原理及应用[M]. 北京: 中国铁道出版社, 2019: 24.
- MA Y R. Principles and applications of blockchain technology[M]. Beijing: China Railway Press, 2019: 24.
- [7] BACK A. Hashcash-a denial of service counter-measure[R]. 2002.
- [8] DAI W. B-Money[EB].
- [9] SZABO N. Bitgold[EB].
- [10] WRIGHT C S. Bitcoin: a peer-to-peer electronic cash system[J]. *SSRN Electronic Journal*, 2008: 21260.
- [11] VITALIK B. Ethereum white paper[J]. *GitHub Repository*, 2013, 1: 22-23.
- [12] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[EB]. arxiv preprint arxiv: 1801.10228, 2018.
- [13] 季乃礼, 兰金奕. 三元悖论视角下的区块链信任与社会治理研究[J]. *山东科技大学学报(社会科学版)*, 2020, 22(5): 87-97.
- JI N L, LAN J Y. Research on blockchain trust and social governance from the perspective of trilemma[J]. *Journal of Shandong University of Science and Technology(Social Sciences)*, 2020, 22(5): 87-97.
- [14] REBELLOET AL. G. A. F. A survey on block-chain scalability: from hardware to layer-two protocols[J]. *IEEE Communications Surveys & Tutorials*, 2024, 26(4): 2411-2458.
- [15] ZHOU H, XU Y, DAI H B, et al. Recovery of ecosystem productivity in China due to the clean air action plan[J]. *Nature Geoscience*, 2024: 1-7.
- [16] IQBAL M, MATULEVIČIUS R. Blockchain-based application security risks: a systematic literature review[M]. *Lecture Notes in Business Information Processing*. Cham: Springer International Publishing, 2019: 176-188.
- [17] 张滨. 区块链安全风险研究[J]. *电信工程技术与标准化*, 2017, 30(11): 1-5.
- ZHANG B. Security risk study of blockchain[J]. *Telecom Engineering Technics and Standardization*, 2017, 30(11): 1-5.
- [18] LI X Q, JIANG P, CHEN T, et al. A survey on the security of blockchain systems[J]. *Future Generation Computer Systems*, 2020, 107: 841-853.
- [19] 杨海红, 邱惠丽, 李正风. 托马斯·休斯“技术-社会系统”思想探微[J]. *自然辩证法研究*, 2020, 36(8): 26-30, 43.
- YANG H H, QIU H L, LI Z F. Exploration on Thomas P. Hughes' thought on “technical-social system” [J]. *Studies in Dialectics of Nature*, 2020, 36(8): 26-30, 43.
- [20] COOPER R, FOSTER M. Sociotechnical systems[J]. *American Psychologist*, 1971, 26(5): 467.
- [21] SlowMist Hacked. SlowMist zone[EB].
- [22] 刘敖迪, 杜学绘, 王娜, 等. 区块链系统安全防护技术研究进展[J]. *计算机学报*, 2024, 47(3): 608-646.
- LIU A D, DU X H, WANG N, et al. Research progress on blockchain system security technology[J]. *Chinese Journal of Computers*, 2024, 47(3): 608-646.
- [23] SULTAN N, MOHAMED N, MARTIN M, et al. Virtual currencies and money laundering: existing and prospects for jurisdictions that comprehensively prohibited virtual currencies like Pakistan[J]. *Journal of Money Laundering Control*, 2024, 27(2): 395-412.
- [24] 刘海鸥, 周颖玉, 周鑫, 等. 区块链隐私威胁及保护机制研究综述[J]. *计算机集成制造系统*, 2023, 29(7): 2292-2312.
- LIU H O, ZHOU Y Y, ZHOU X, et al. Review on privacy threats and protection mechanisms for blockchain technology[J]. *Computer Integrated Manufacturing Systems*, 2023, 29(7): 2292-2312.
- [25] ZHANG R, XUE R, LIU L. Security and privacy on blockchain[J]. *ACM Computing Surveys*, 2020, 52(3): 1-34.
- [26] 崔展齐, 杨慧文, 陈翔, 等. 智能合约安全漏洞检测研究进展[J]. *软件学报*, 2024, 35(5): 2235-2267.
- CUI Z Q, YANG H W, CHEN X, et al. Research progress of security vulnerability detection of smart contracts[J]. *Journal of Software*, 2024, 35(5): 2235-2267.
- [27] 王永利, 徐秋亮. 量子计算与量子密码的原理及研究进展综述[J]. *计算机研究与发展*, 2020, 57(10): 2015-2026.
- WANG Y L, XU Q L. Principle and research progress of quantum computation and quantum cryptography[J]. *Journal of Computer Research and Development*, 2020, 57(10): 2015-2026.
- [28] 沈传年. 区块链安全问题研究综述[J]. *计算机工程与科学*, 2024, 46(1): 46-62.
- SHEN C N. Review on security issues of blockchains[J]. *Computer Engineering & Science*, 2024, 46(1): 46-62.
- [29] WANG X, FENG D, LAI X, et al. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD[J]. *Cryptology ePrint Archive*, 2004.
- [30] STEVENS M. New collision attacks on SHA-1 based on optimal joint local-collision analysis[M]//*Lecture Notes in Computer Science*. Berlin Heidelberg: Springer, 2013: 245-261.
- [31] 张伟, 许海洋, 周百顺. 多进程共享的高效哈希表[J]. *计算机工程与设计*, 2017, 38(5): 1190-1195.
- ZHANG W, XU H Y, ZHOU B S. Efficient hash table supporting multi-process sharing[J]. *Computer Engineering and Design*, 2017, 38(5): 1190-1195.
- [32] 倪雪莉, 马卓, 王群. 区块链P2P网络及安全研究[J]. *计算机工程与应用*, 2024, 60(5): 17-29.
- NI X L, MA Z, WANG Q. Research on blockchain P2P network and its security[J]. *Computer Engineering and Applications*, 2024, 60(5): 17-29.
- [33] DUAN L, SUN Y Y, ZHANG K J, et al. Multiple-layer security threats on the ethereum blockchain and their countermeasures[J]. *Security and Communication Networks*, 2022, 2022: 5307697.
- [34] 田国华, 胡云瀚, 陈晓峰. 区块链系统攻击与防御技术研究进展[J]. *软件学报*, 2021, 32(5): 1495-1525.

- TIAN G H, HU Y H, CHEN X F. Research progress on attack and defense techniques in block-chain system[J]. *Journal of Software*, 2021, 32(5): 1495-1525.
- [35] OpenZeppelin. OpenZeppelin contracts[EB].
- [36] NAYAK K, KUMAR S, MILLER A, et al. Stubborn mining: generalizing selfish mining and combining with an eclipse attack[C]//*Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P)*. Piscataway: IEEE Press, 2016: 305-320.
- [37] GRUNSPAN C, PÉREZ-MARCO R. On profitability of selfish mining[EB]. arXiv preprint arXiv: 1805.08281, 2018.
- [38] BARWISE J. An introduction to first-order logic[M]//*Studies in Logic and the Foundations of Mathematics*. Amsterdam: Elsevier, 1977: 5-46.
- [39] Optimism. Introducing the OVM[EB].
- [40] SUJATHA E, KUMAR G N, VIKAS N V, et al. Decentralized portfolio tracking application on A polygon layer 2 blockchain[C]//*Proceedings of the 2023 International Conference on Networking and Communications (ICNWC)*. Piscataway: IEEE Press, 2023: 1-5.
- [41] KALODNER H, GOLDFEDER S, CHEN X, et al. Arbitrum: scalable, private smart contracts[C]//*Proceedings of the 27th USENIX Security Symposium (USENIX Security 18)*. 2018: 1353-1370.
- [42] YE Z, MISRA U, CHENG J J, et al. Specular: towards secure, trust-minimized optimistic blockchain execution[EB]. arXiv preprint arXiv: 2212.05219, 2022.
- [43] KAUR G, GANDHI C. Scalability in blockchain: challenges and solutions[M]. USA: Academic Press, 2020: 373-406.
- [44] THIBAULT L T, SARRY T, HAFID A S. Blockchain scaling using rollups: a comprehensive survey[J]. *IEEE Access*, 2022, 10: 93039-93054.
- [45] HARISHANKAR M, AKESTORIDIS D G, IYER S V, et al. Plasma go: a scalable sidechain protocol for flexible payment mechanisms in blockchain-based marketplaces[EB]. arXiv preprint arXiv: 2003.06197, 2020.
- [46] LAVAU T, DETCHART J, LACAN J, et al. Modular zk-rollup on-demand[J]. *Journal of Network and Computer Applications*, 2023, 217: 103678.
- [47] HE S L, TANG Q, WU C Q, et al. Decentralizing IoT management systems using blockchain for censorship resistance[J]. *IEEE Transactions on Industrial Informatics*, 2020, 16(1): 715-727.
- [48] AVERIN A, AVERINA O. Review of blockchain technology vulnerabilities and blockchain-system attacks[C]//*Proceedings of the 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*. Piscataway: IEEE Press, 2019: 1-6.
- [49] ČAPKO D, VUKMIROVIĆ S, NEDIĆ N. State of the art of zero-knowledge proofs in blockchain[C]//*Proceedings of the 2022 30th Telecommunications Forum (TELFOR)*. Piscataway: IEEE Press, 2022: 1-4.
- [50] SIVARAMAN V, VENKATAKRISHNAN S B, RUAN K, et al. High throughput cryptocurrency routing in payment channel networks[C]//*Proceedings of the 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*. 2020: 777-796.
- [51] Connex Network. What is connex[EB].
- [52] DONG M, LIANG Q, LI X, et al. Celer network: Bring internet scale to every blockchain[J]. arXiv preprint arXiv: 1810.00037, 2018.
- [53] DZIEMBOWSKI S, ECKEY L, FAUST S, et al. Perun: Virtual payment hubs over cryptocurrencies[C]//*2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019: 106-123.
- [54] COUNTERFACTUAL. The Official Website of Counterfactual[EB].
- [55] THOMAS S, SCHWARTZ E. A protocol for interledger payments [EB].
- [56] SINGH A, CLICK K, PARIZI R M, et al. Sidechain technologies in blockchain networks: an examination and state-of-the-art review[J]. *Journal of Network and Computer Applications*, 2020, 149: 102471.
- [57] GNOSIS. Whitepaper[EB].
- [58] SKALE Network. The SKALE network: an ethereum interoperable elastic blockchain network[EB].
- [59] KOEGLA, MEGHJIZ, PELLEGRINO D, et al. Attacks on rollups[C]//*Proceedings of the 4th International Workshop on Distributed Infrastructure for the Common Good*. New York: ACM, 2023: 25-30.
- [60] MAMAGISHVILI A, FELTEN E W. Incentive schemes for rollup validators[M]. *Lecture Notes in Operations Research*. Cham: Springer Nature Switzerland, 2023: 48-61.
- [61] DZIEMBOWSKI S, FABIAŃSKI G, FAUST S, et al. Lower bounds for off-chain protocols: exploring the limits of plasma[J]. *Cryptology ePrint Archive*, 2020.
- [62] Kyber Network. KyberNetwork: a trustless decentralized exchange and payment service [EB].
- [63] Loom Network. Loom network lightpaper[EB].
- [64] OMG Network. OmiseGO: decentralized exchange and payments [EB].
- [65] QIN K H, ZHOU L Y, GERVAIS A. Quantifying Blockchain Extractable Value: How dark is the forest? [C]//*Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP)*. Piscataway: IEEE Press, 2022: 198-214.
- [66] YANG S, ZHANG F, HUANG K, et al. SoK: MEV countermeasures: theory and practice[EB]. arXiv preprint arXiv: 2212.05111, 2022.
- [67] MILIONIS J, MOALLEMI C C, ROUGHGARDEN T, et al. Automated market making and loss-versus-rebalancing[EB]. arxiv preprint arxiv: 2208.06046, 2022.
- [68] EigenPhi. Arbitrage transaction detail[EB].
- [69] PATRICK Z, NADAHALLI T, WATTENHOFER Y W R. Analyzing and preventing sandwich attacks in ethereum[J]. *ETH Zürich*, 2021: 1-29.
- [70] XAVIER FERREIRA M V, PARKES D C. Credible decentralized exchange design via verifiable sequencing rules[C]//*Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. New York: ACM, 2023: 723-736.
- [71] 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.
- [72] CHEMAYA N, LIU D Y, MCLAUGHLIN R, et al. The power of default: measuring the effect of slippage tolerance in decentralized exchanges[J]. SSRN Electronic Journal, 2023.
- [73] ADAMSH, ZINSMEISTER N, SALEMM, et al. Uniswap v3 core[R]. 2021.
- [74] WHITE D, MCCARTHY D, ADAMS H. TWAMM[EB].
- [75] DAIAN P, GOLDFEDER S, KELL T, et al. Flash boys 2.0: front-running in decentralized exchanges, miner extractable value, and consensus instability[C]//Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2020: 910-927.
- [76] WANG D, WU S, LIN Z, et al. Towards a first step to understand flash loan and its applications in defi ecosystem[C]//Proceedings of the 2023 IEEE 43rd International Conference on Distributed Computing Systems (ICDCS). IEEE, 2023: 154-165.
- [77] ROBERT S R. "Engineering Error" Led to \$34 Million DeFi Hack, Harvest Finance Says[EB].
- [78] QING X, HUANG Z R, DOU W S, et al. Detecting flash loan based attacks in ethereum[C]//Proceedings of the 2023 IEEE 43rd International Conference on Distributed Computing Systems (ICDCS). Piscataway: IEEE Press, 2023: 154-165.
- [79] CAO Y X, ZOU C, CHENG X. Flashot: a snapshot of flash loan attack on DeFi ecosystem[EB]. arXiv preprint arXiv: 2102.00626, 2021.
- [80] XU J H, FENG Y B. Reap the harvest on blockchain: a survey of yield farming protocols[J]. IEEE Transactions on Network and Service Management, 2023, 20(1): 858-869.
- [81] GUNDERMAN D. Suspected cryptocurrency "rug pull" nets actors \$10 million[EB].
- [82] XIA P C, WANG H Y, GAO B Y, et al. Trade or trick?[C]//Proceedings of the ACM on Measurement and Analysis of Computing Systems, 2021, 5(3): 1-26.
- [83] XU J H, PARUCH K, COUSAERT S, et al. SoK: decentralized exchanges (DEX) with automated market maker (AMM) protocols[J]. ACM Computing Surveys, 2023, 55(11): 1-50.
- [84] DALE B. SushiSwap will withdraw up to \$830M from uniswap today: why it matters for DeFi[EB].
- [85] REDSTONE ORACLES. Oracle attacks #1-inverse finance, \$15M stolen[EB].
- [86] MACKINGA T, NADAHALLI T, WATTENHOFER R. TWAP oracle attacks: easier done than said[C]//Proceedings of the 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). Piscataway: IEEE Press, 2022: 1-8.
- [87] SMARTCONTENT. TWAP Oracles vs chainlink price feeds: a comparative analysis[EB].
- [88] WANG X Y, YU H B. How to break MD5 and other hash functions[M]. Lecture Notes in Computer Science. Berlin Heidelberg: Springer, 2005: 19-35.
- [89] CORON J S, DODIS Y, MALINAUD C, et al. Merkle-damgård revisited: how to construct a hash function[M]. Lecture Notes in Computer Science. Berlin Heidelberg: Springer, 2005: 430-448.
- [90] 姚前, 陈永伟. Web 3.0: 下一代互联网的变革与挑战[M]. 北京: 中信出版社, 2022.
- YAO Q, CHEN Y W. Web 3.0: the changes and challenges of the next generation Internet[M]. Beijing: CITIC Press, 2022.
- [91] RABCAN J, RUSNAK P, ZAITSEVA E, et al. Analysis of aata reliability based on Importance analysis[C]//Proceedings of the 2019 International Conference on Information and Digital Technologies (IDT). Piscataway: IEEE Press, 2019: 402-408.
- [92] CAI X Q, DENG Y. The principle and core technology of blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 84-131.
- [93] 韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望[J]. 自动化学报, 2019, 45(1): 206-225.
- HAN X, YUAN Y, WANG F Y. Security problems on blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2019, 45(1): 206-225.
- [94] MAZUMDAR S. Facebook's libra faces EU antitrust [EB].
- [95] Veritas. Navigating regulatory compliance[EB].
- [96] SERADA A. Why is cryptokitties (not) gambling[C]//Proceedings of the 15th International Conference on the Foundations of Digital Games. Piscataway: IEEE Press, 2020: 1-4.
- [97] YU G, NIE T Z, LI X H, et al. The challenge and prospect of distributed data management techniques in blockchain systems[J]. Chinese Journal of Computers, 2019, 42: 1-27.
- [98] STALLINGS W, BROWN L. Computer security: Principles and practice[EB].

[作者简介]



高昊昱 (1994-), 男, 山西太原人, 海南大学博士生, 主要研究方向为区块链、可信计算。



曹春杰 (1977-), 男, 陕西西安人, 博士, 海南大学教授、博士生导师, 主要研究方向为无线网络安全、区块链、人工智能安全。



徐响（1999-），男，湖北鄂州人，海南大学硕士生，主要研究方向为区块链、数字身份。



芦翔（1982-），男，山东烟台人，博士，中国科学院信息工程研究所副研究员，主要研究方向为区块链安全监管、物联网密码工程与应用。



裴庆祺（1975-），男，广西百色人，博士，西安电子科技大学教授、博士生导师，主要研究方向为信息安全、电子商务/电子政务安全。



雷虹（1984-），男，湖南常德人，博士，海南大学教授、博士生导师，主要研究方向为区块链、可信执行环境、隐私计算。