区块链安全监管研究综述

高昊昱[1]，曹春杰[1]，白伊瑞[2]，马琪舜[1]，雷虹[1,3]，孙鸿宇[1]，裴庆祺[4]，芦翔[2]
（1. 海南大学网络空间安全学院，海南 海口 570228；2. 中国科学院信息工程研究所，北京 100864；
3. 云海链控股股份有限公司，海南 澄迈 571924；4. 西安电子科技大学网络与信息安全学院，陕西 西安 710126）

摘　要：区块链是一种安全和可信的新型分布式计算范式，在众多领域得到了广泛应用，但安全问题日渐凸显，监管需求日益迫切。简要介绍区块链生态现状和主要国家的监管政策背景，结合区块链技术和应用架构将相关文献进行划分，从链内、链间和链外 3 个方面分析现有的监管技术及方案的特点。首先将链内监管进一步划分为基础设施层监管、核心功能层监管和用户层监管 3 个层次，并分别详细探讨了各个层次下不同监管技术的优势和不足。随后将链间监管划分为基于“以链治链”思想的监管和跨链安全监管两类，分别简要讨论相关研究的特点，并简要介绍了链外监管的一些代表性案例。最后分析了当前区块链安全监管的共性问题并指出了可能的改进方向以及待监管的新领域，填补区块链监管综述方面的空白，为区块链监管方案设计提供了参考。

关键词：区块链；区块链安全；区块链监管
中图分类号：TP309.2
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025011

Review of blockchain security regulation

GAO Haoyu[1], CAO Chunjie[1], BAI Yirui[2], MA Qishun[1], LEI Hong[1,3], SUN Hongyu[1], PEI Qingqi[4], LU Xiang[2]
1. School of Cyberspace Security, Hainan University, Haikou 570228, China
2. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100864, China
3. SSC Holding Company Ltd, Chengmai 571924, China
4. School of Network and Information Security, Xidian University, Xi’an 710126, China

Abstract: Blockchain is a new distributed computing paradigm characterized by security and trust, widely applied in various fields. However, security issues have become increasingly prominent, and the need for regulation is more urgent. The current state of the blockchain ecosystem and the regulatory policy backgrounds of major countries were briefly introduced. The relevant literature based on blockchain technology and application architecture were categorized and the characteristics of existing regulatory technologies and solutions were analyzed from three aspects: intra-chain regulation, inter-chain regulation, and off-chain regulation. Intra-chain regulation was further divided into three levels: infrastructure layer regulation, core function layer regulation, and user layer regulation. The advantages and disadvantages of different regulatory technologies at each level were discussed in detail. Inter-chain regulation was divided into two categories: regulation based on the “governance by chain” concept and cross-chain security regulation, with a brief discussion of the characteristics of related studies. Then some representative cases of off-chain regulation were introduced. Finally, the common issues in current blockchain security regulation were analyzed with possible improvement directions and new areas in need of regulation. The gap was filled in reviews on blockchain regulation and a reference for the design of blockchain regulatory solutions was provided.

Keywords: blockchain, blockchain security, blockchain regulation

收稿日期：2024–10–09；**修回日期：**2024–11–20
通信作者：雷虹，leihong@hainanu.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2021YFB2700600）；海南大学科研启动基金资助项目（No.KYQD(ZR)-21071）
Foundation Items: The National Key Research and Development Program of China (No.2021YFB2700600), The Research Startup Fund of Hainan University (No.KYQD(ZR)-21071)

0　引言

区块链自诞生以来，其发展阶段已从区块链1.0发展至区块链3.0，其应用领域也从单一支付场景扩展到多个行业，如金融服务、政务法务、供应链管理、身份验证等[1]。区块链1.0聚焦于数字货币，实现了去中心化的价值传输。区块链2.0引入智能合约，标志着链上执行复杂的业务逻辑成为现实。而区块链3.0注重将区块链应用于实际落地场景，实现分布式商业网络[2]。

近年来区块链的快速发展让区块链应用越来越丰富。一批以高性能公链为代表的新兴区块链项目涌现出来，如Solana[3]、Avax[4]、Near、Hedera[5]、Sui[6]等。传统公链（如比特币、以太坊、币安链等）更是承接了海量资金涌入，孵化了各种各样的Web3项目，如去中心化交易所（DEX, decentralized exchange）[7]、去中心化社交与聊天软件[8]、铭文与符文协议、区块链游戏[9]、Web3云服务[10]等[11-16]。

随着区块链技术应用的爆发式增长，其安全问题也随之凸显。区块链底层平台和区块链应用漏洞导致的风险以及各类虚拟资产犯罪行为对区块链安全带来了极大的挑战。根据SlowMist Hacked Statistical数据库统计，自2012年以来全球区块链公开的重大安全事件数量呈逐年递增趋势，如图1所示。区块链相关安全事件主要包括钱包安全事件、恶意挖矿、分布式拒绝服务（DDoS, distributed denial-of-service）攻击、勒索软件、数字货币诈骗、数字货币洗钱、智能合约安全、交易所安全和其他攻击事件9种类别[17-18]。

伴随着频发的区块链安全事件，对区块链加强监管的需求日益迫切。2019年以来，IEEE、ACM、Springer等数据库收录的区块链相关文献虽然高达74 000余篇，但其中直接研究区块链监管的综述却极少。目前国内外与区块链监管相关的综述[19-22]偏重围绕区块链安全或漏洞的检测防御进行分析，或有相关文献分析了某些具体应用场景下的区块链安全[23-29]，但并不涉及区块链监管。

根据区块链技术架构发展现状，本文将其与运行于其上的应用划分为链内基础设施、跨链扩展和去中心化自治社区与应用三层，如图2所示。通过系统梳理区块链监管的研究现状，并在图2所示三层架构的基础上，将现有区块链监管相关文献进行归纳和总结，划分为链内监管、链间监管和链外监管3种类型的监管技术及方案，并分别对每种类型所涉及的文献进行了讨论和比较。本文的主要贡献如下。

1) 将现有监管方案归纳为链内监管、链间监管和链外监管。将链内监管进一步划分为基础设施层监管、核心功能层监管和用户层监管3个层次，并根据相关文献的侧重点对每个层次的监管技术进行细致的分类，讨论其优势和不足。

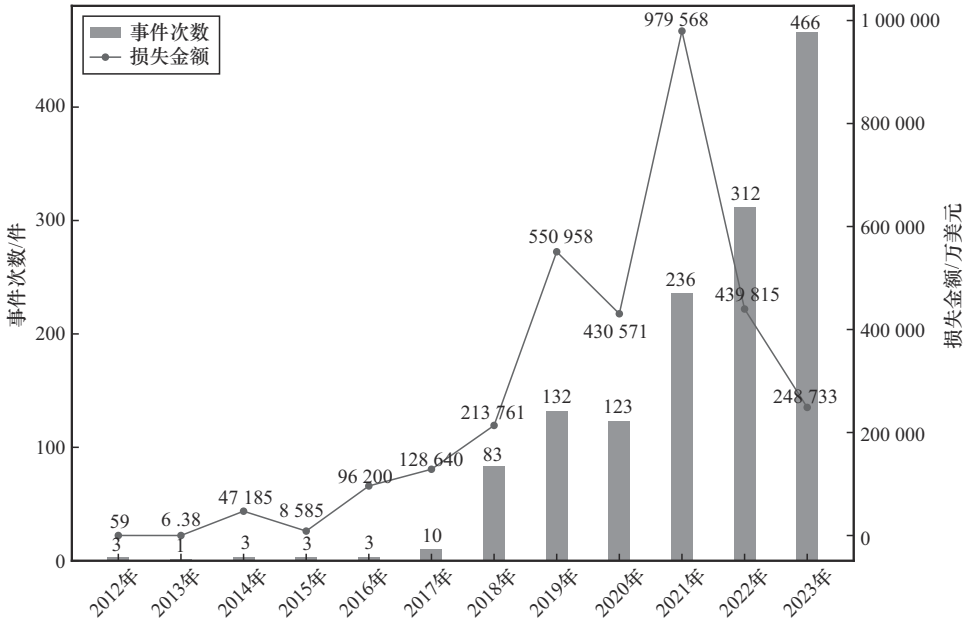

图1　全球区块链公开的重大安全事件

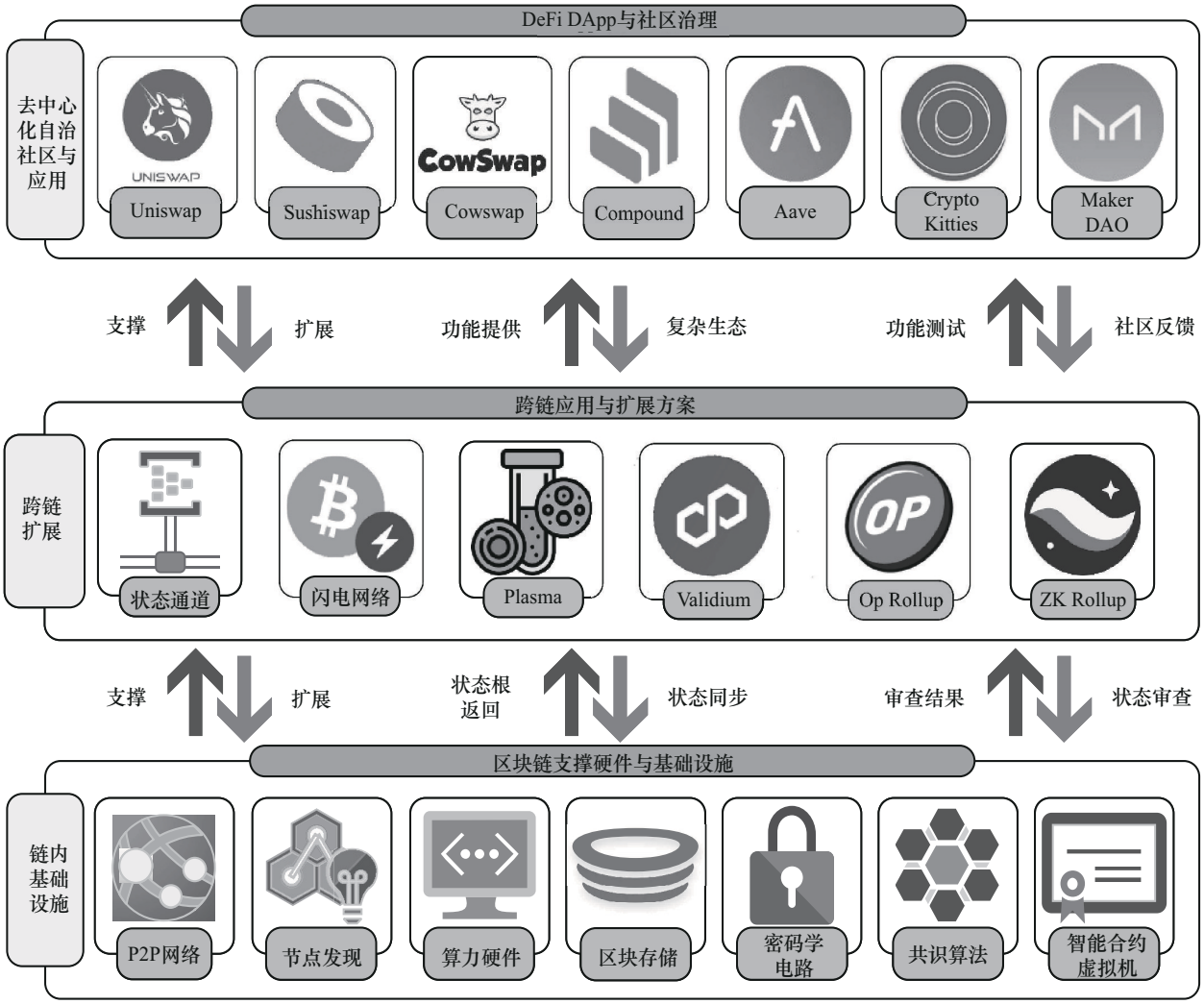

图2　区块链应用三层架构

2) 将链间监管进一步划分为基于“以链治链”思想的监管和跨链安全监管，分析比较相关文献的特点，并简要讨论链外监管的代表性案例。

3) 对现有监管存在的共性问题进行分析并给出可能的改进方向，指出监管应关注以Rollup和去中心化金融（DeFi, decentralized finance）项目等为代表的新兴区块链项目。

1　区块链监管背景

随着区块链技术的深入发展，其应用场景逐渐丰富，各种复杂应用逐渐构成了区块链生态的雏形，这些生态项目承接了海量资金的不断涌入，同时也引起了各国政府和组织的关注。本节简要介绍区块链生态的生态现状和主要国家的代表性区块链监管政策。

1.1　区块链生态现状

在学术界，已有文献提出了区块链生态这一概念[24-30]，经过对相关文献[31-33]的归纳，总结出的区块链生态系统组成如图3所示。图3最下层为支撑发展技术，产生的突破往往会促进区块链技术的革新，通常是密码学、大数据、分布式系统、云和雾计算、去中心化学习等计算机基础学科或技术。最上层的应用领域包括真实世界资产（RWA, real world asset）、电子竞拍、借贷、去中心化金融等多个场景。区块链生态实体由区块链用户、区块链应用提供商、区块链平台服务提供商、区块链基础架构、区块链社区、区块链设备提供商、区块链监管机构和区块链技术咨询提供商八部分构成[34-35]。这些组成部分通过数据和资金相互连接和交互，形成了一个相互依存和相互影响的整体。

1.2　区块链监管政策

在学术研究领域之外，区块链在发展过程中受到了各国政府和组织不同程度的关注，部分国家和

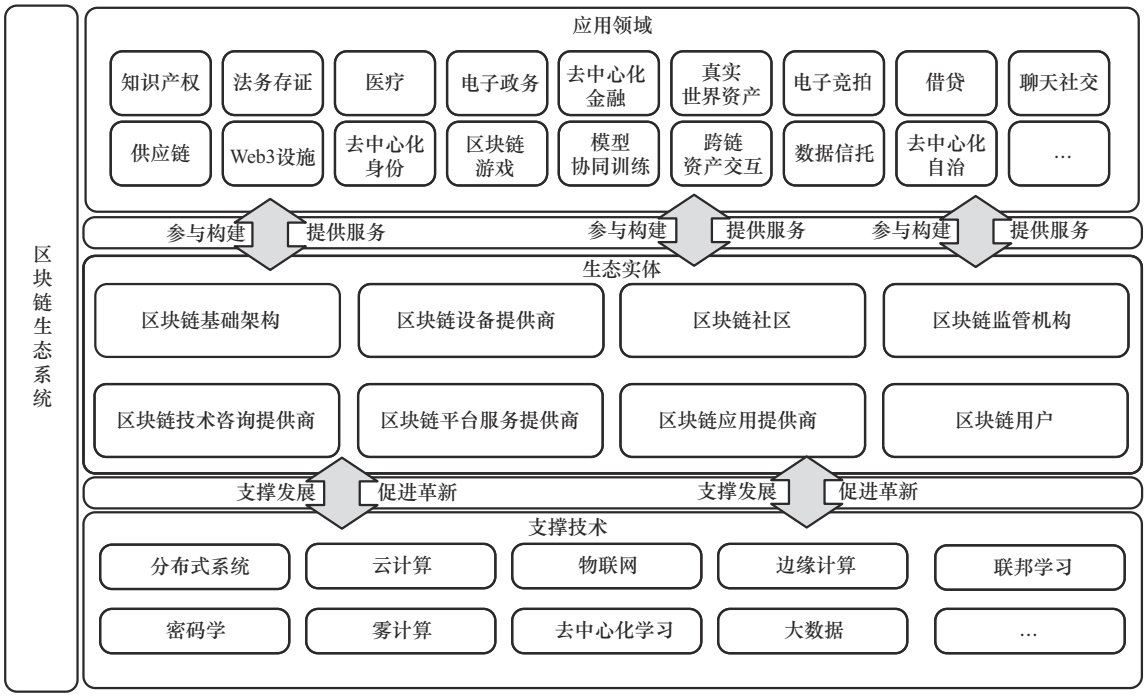

图3　区块链生态系统组成

组织已经开展了体系化和标准化的区块链安全监管工作[36-37]，相关监管政策及监管机构如表1所示。

英国政府首先提出了“监管沙盒”概念[38]。美国制定了针对区块链技术和数字资产的知识产权和税收法规，成立了区块链产业联盟，以推动区块链产业的发展和监管[39]。欧盟委员会制定了“数字金融战略2020”和“区块链战略”，加强数字金融领域的监管和合作。新加坡政府颁布了数字资产税收法案，规定数字资产交易应当缴纳税费[40]。瑞士政府制定了一系列的区块链法规和政策[41]，为区块链企业提供法律保障、指导与监管。我国对于区块链的监管政策主要涉及数字资产交易、首次币发行（ICO, initial coin offering）、数字货币等领域[42]。

我国于2017年9月发布了“关于防范代币发行融资风险的公告”，明确禁止ICO融资活动。同时还加强了对区块链产业的支持和监管，鼓励企业开发更加安全的区块链技术。中国信息通信研究院于2018年发布了“区块链安全白皮书”[43]，从技术

表1　　**部分国家和组织区块链相关监管政策及监管机构**

部分国家和组织	监管政策	监管机构
中国	关于防范比特币风险的通知、关于防范代币发行融资风险的公告、区块链安全白皮书、区块链信息服务管理规定和金融信息服务管理规定	国家互联网信息办公室；中国人民银行数字货币研究所；中国互联网协会区块链专业委员会（SEC）
加拿大	加拿大加密货币税收指南	加拿大税务局（CRA）
法国	加密资产相关监管框架和数字资产服务提供商许可要求和规定	法国金融监管局（AMF）；数字资产发展协会（ADAN）
新加坡	金融科技监管沙盒指南、数字资产税收法案和金融机构行为准则	新加坡金融管理局（MAS）；个人数据保护委员会（PDPC）；新加坡知识产权局（IPOS）
欧盟	数字金融战略、区块链战略、通用数据保护条例和欧盟金融科技行动计划	欧洲证券和市场管理局（ESMA）；欧洲银行管理局（EBA）；欧洲数据保护监督员（EDPS）
日本	数字货币交易法、支付服务法、关于ICO新监管的建议和资产结算法实施令	日本金融厅（FAS）；日本区块链协会（JBA）；日本虚拟货币交易协会（JVCEA）
德国	德国国家区块链战略	联邦金融监管局（BaFin）；联邦数据保护和信息自由专员（BfDI）；金融市场稳定基金（SoFFin）
IMF	加密资产、全球经济中的监管挑战和数字化金融服务的监管框架	国际货币基金组织（IMF）

架构设计角度对区块链监管进行了层级化的风险描述。2019 年，工信部成立了全国区块链和分布式记账技术标准化委员会，系统化地推进标准制定工作，加快了区块链监管体系建立。同年，国家网信办颁布“区块链信息服务管理规定”[44]，该规定是国内第一个由国家机关颁布的专门针对区块链的规范性监管法规文件。

2　区块链监管分类

国内外区块链安全与监管相关综述类研究进展如表 2 所示。文献[20-22,45-49]聚焦于对区块链的数据安全问题和网络安全问题进行研究，不讨论区块链整体的监管。文献[23-25,50-56]侧重于讨论诸如智能合约漏洞与共识算法漏洞等区块链特定领域的安全问题。除表 2 所列综述外，还有文献讨论区块链生态发展情况[26-30,57]，并未讨论区块链安全监管。

表 2　国内外区块链安全与监管相关综述类研究进展

文献	侧重点	是否涉及监管
文献[20-22,45]	区块链安全漏洞攻防与原理分析	不涉及
文献[46-48]	区块链数据安全、网络安全等	涉及不全面
文献[49]	区块链应用研究	不涉及
文献[50-53]	智能合约漏洞检测与修复	不涉及
文献[23-25,55-56]	共识机制安全改进	不涉及

本文将现有区块链监管方案和文献划分为链内监管、链间监管和链外监管，其区块链监管代表性技术发展历程如图 4 所示。链内监管由区块链基础设施层监管、核心功能层监管和用户层监管组成，所涉及文献较多[58-118]，是监管的重点层级。链间监管由基于“以链治链”思想的监管和跨链安全监管 2 类组成[119-131]，链外监管主要涉及去中心化自治组织（DAO, decentralized autonomous organization）和社区，由于跨链技术和链外去中心化治理机制发展历程较短，所涉及文献和监管方案较少[132-137]。从图 4 可以看出，机器学习技术开始越来越多地应用于区块链监管。

2.1　链内监管

本节将链内监管划分为 3 层，分别是基础设施层监管、核心功能层监管和用户层监管。基础设施层的监管技术进一步分为节点关联关系追踪、节点异常行为检测和节点攻击流量检测。核心功能层的监管技术分为异常交易分析与检测、智能合约安全检测、共识机制攻击检测和联盟链穿透式监管。用户层监管主要针对用户，包含用户业务监管和用户账户监管两类监管技术。

2.1.1　基础设施层监管

基础设施层提供了支撑整个区块链系统运行所需的硬件基础组件和运行环境，主要包括存储区块链数据和执行区块链计算任务的计算资源、备份和恢复机制等安全和防护措施，确保节点之间可连接

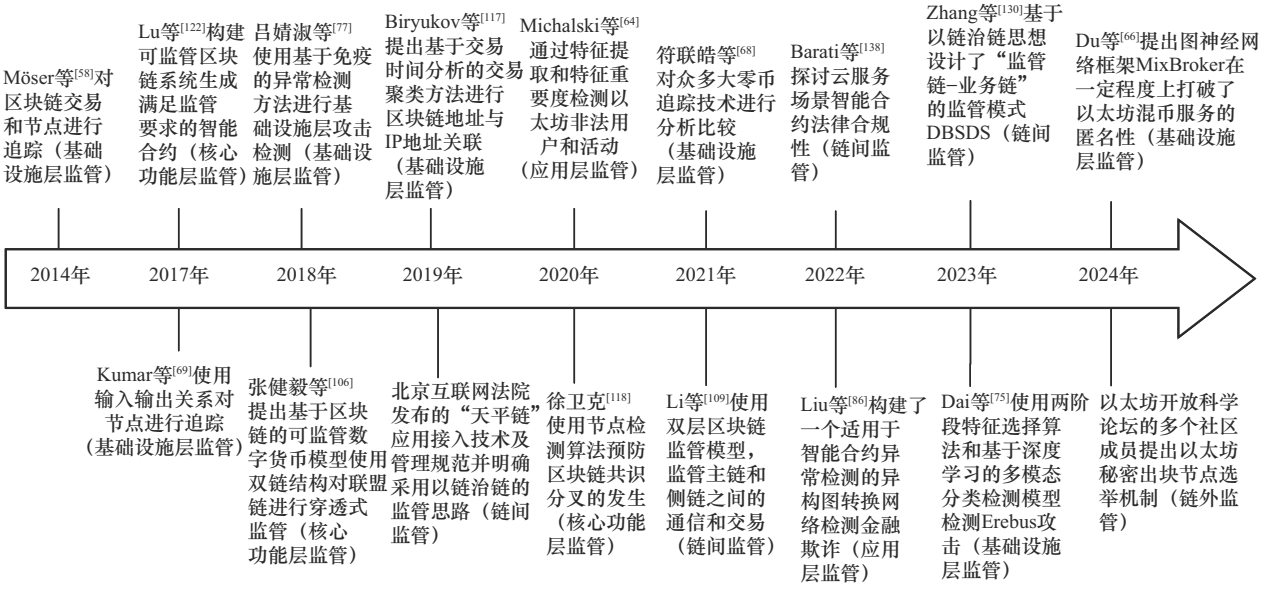

图 4　区块链监管代表性技术发展历程

性和数据传输稳定性的网络基础设施。

2.1.1.1 节点关联关系追踪技术

区块链节点的追踪技术是指通过对区块链网络中节点的网络地址、账户地址和交易等信息进行收集和分析，构建节点之间的关联关系和拓扑结构，从而了解节点之间的连接方式、交互情况、交易行为等特征，实现对区块链的安全监管。节点关联关系追踪技术不影响交易和区块链的最终状态，属于事后监管。

相关研究[58-60]主要利用图分析与日志分析审计、机器学习与聚类分析等技术对区块链交易进行追踪，最终理清区块链节点之间的关系，目前的难点是对强隐私性加密货币交易的追踪。

1) 图分析和日志分析审计。针对文献[58-60]所提基于污染/染色的追踪分析技术在有效性、普适性和效率等方面存在局限性的问题，李致远等[61]提出了一种基于节点影响力的账户余额模型区块链交易追踪方法，利用网络分析和图数据挖掘技术，通过账户余额模型追踪特定目标账户的资金流向，弥补了现有区块链交易追踪研究在普适性和效率方面的缺陷和不足。重点关注共识交易的过程追踪，李杉杉等[62]提出了一种基于自定义日志的Fabric共识交易轨迹追踪方法，利用ELK（Elasticsearch Logstash Kibana）工具链收集与解析Fabric的自定义共识交易日志，通过Spring Boot后端应用处理自定义日志业务逻辑，可以有效追踪到Fabric各节点共识交易的调用轨迹，实现共识交易轨迹的可视化。侧重于节点自动发现，文献[63]提出了一种基于Kademlia协议的节点自动发现机制，构建的路由表可以让网络中的节点在被其他节点发现时逐步加入它们的路由表中，从而实现节点对整个网络的动态感知。

2) 机器学习与聚类分析。使用机器学习方法进行区块链节点追踪可以提高追踪的效率和准确性，机器学习模型可以从大量的数据中学习到模式和规律，帮助识别和分析复杂的节点行为和关系。Michalski等[64]使用监督学习方法分析区块链中节点的特征，通过分析节点在区块链网络中的行为特征来推测节点在区块链中所扮演的角色，如矿工或交易所。虽然本文的目标更加聚焦于定位节点的角色和行为，但其结果可以为节点追踪提供一定的帮助和线索。前向交易追踪是一种用于分析比特币滥用和追踪资金流向的常用技术，即从已知属于网络犯罪活动的一组给定种子地址开始追踪比特币的流动，但其只考虑了向前的交易流动，而没有考虑到向后的交易流动，这意味着在某些情况下可能会错过一些重要的关系和交易信息。为了在分析交易时同时关注输出交易和输入交易，Gomez等[65]提出了双向探索自动化比特币交易追踪技术，通过给定属于网络犯罪活动的种子地址输出一个交易图，并识别出与节点活动以及外部服务和其他网络犯罪活动之间的关系路径。为了防止交易图膨胀，该技术标记数据库与机器学习分类器相结合，快速识别和过滤出属于交易所的地址。从节点对链接预测的角度，Du等[66]提出了图神经网络框架MixBroker，使用原始以太坊混合交易数据构建混币交互图，并从多个角度提取该图中的账户节点特征，以更好地表示混币账户节点的属性。利用图神经网络计算节点之间的相关性概率，从而判断混币账户节点之间的关联关系，一定程度上打破了以太坊混币服务的匿名性。

此外，为了提供更高级别的隐私和匿名性保护，一些加密货币采用了环签名、零知识证明、混币等技术手段隐藏交易双方的地址和交易金额，如门罗币[67]、大零币[68]和达世币。尽管这些匿名币可以提供一定程度的匿名性和隐私保护，但并非不可溯源。目前存在6种大零币[68]追踪技术，分别为达南礼物攻击、粉尘攻击、远程侧信道攻击、往返交易攻击、用户行为分析攻击和隐蔽信道攻击，可以用于推断和追踪大零币节点的交易信息。在门罗币[67]技术的追踪领域，目前存在四类主要的追踪方法：基于输入输出关系的追踪[69]（如0-mixin攻击、输出合并攻击、封闭集攻击等）、基于统计规律的追踪（如最新猜测攻击等）、部分公钥已知的追踪（如泛洪攻击、钱包环攻击等）和利用门罗币安全机制漏洞的追踪（如恶意远程节点攻击等）。

2.1.1.2 节点异常行为检测技术

区块链节点可能试图执行恶意操作、攻击网络、钓鱼、篡改数据或进行欺诈行为，节点检测是指通过分析和监测区块链网络中的节点行为，识别可能存在的恶意节点或异常行为，属于事前监管。节点检测的方法多样，目前主要基于流量分析和钓鱼节点检测等方面进行研究。

在流量分析方面，刘国智[70]提出了基于联邦学习和表征学习的异常流量检测算法，并实现了用

于检测区块链网络异常节点的分布式异常流量检测系统，该系统能自动学习流量数据特征，允许参与方动态进出，由智能合约管控全流程。与文献[70]侧重于通过特定算法和系统实现异常检测不同的是，Sanda等[71]采用深度学习卷积神经网络（CNN, convolutional neural network）、K 近邻（KNN, K-nearest neighbor）、决策树和多层感知机（MLP, multi-layer perceptron）算法来确定分类器并预测恶意节点，可以进一步扩展到分析权益证明（PoS, proof of stake）共识上验证节点的异常行为。

在钓鱼节点检测方面，目前检测以太坊网络钓鱼的方法主要关注交易特征和局部网络结构，但在处理边之间的复杂交互和大型图时存在局限性。针对此问题，Zhang 等[72]提出了基于图卷积网络（GCN, graph convolutional network）的以太坊钓鱼节点的检测方法，将复杂交易网络转化为3个简单节点间图，利用GCN生成节点嵌入和全局结构信息来识别钓鱼节点。类似地，Yu 等[73]采用基于消息传递的GCN先构建交易网络，再提取节点信息并分类，以检测钓鱼节点。这两项工作都运用了GCN来检测以太坊的钓鱼节点，且都涉及交易网络的处理和节点信息的利用，解决了当前检测方法在处理复杂交互和大型图时的局限性，提高了检测的效果和准确性。但前者主要侧重于利用GCN生成节点嵌入和全局结构信息来识别钓鱼节点，而后者侧重于先构建交易网络，再提取节点信息并分类。

通过及时识别和应对恶意节点、异常行为和潜在风险，可以增强区块链系统的抗攻击能力，并为各种应用场景提供更可靠的基础设施。然而，节点检测技术仍然面临一些挑战，如检测过程中隐私保护不足、检测效率低下和准确性不高的问题。

2.1.1.3　节点攻击流量检测技术

在基础设施层对区块链节点正常运行危害较大的攻击类型包括Eclipse攻击[74]、Erebus攻击[75]和DDoS攻击[76]，它们的目的是破坏底层网络基础设施的可用性和功能。研究人员基于深度学习对流量数据中的攻击特征进行提取，提出了多种检测方法，研究的焦点围绕如何识别和防范针对区块链基础架构的攻击使其能够稳定、安全地运行。

1) Eclipse攻击检测

Eclipse攻击依赖多节点协作，通过控制目标节点的网络连接，使该目标节点与其他诚实节点隔离，客户端无法区分区块链的规范视图和攻击者提供的视图，该攻击具有隐蔽性和并发性的特点。目前现有的方法大多采用基于自定义行为特征和深度学习[74]、基于免疫的异常检测方法[77]、基于可疑时间戳的检测方法以及利用区块链客户端的通信[78]来检测Eclipse攻击。为了更准确地描述攻击流量的行为特征，Dai等[74]通过定义多层次的流量特征、改进的上采样算法和深度学习模型的结合，利用CNN和双向长短期记忆（Bi-LSTM, bidirectional long short-term memory）网络对Eclipse攻击流量进行深度特征提取，通过引入多头注意力机制将特征提取结果完全整合到混合特征中，有效增强了对日食攻击流量的检测能力。基于检测可疑的区块时间戳是指通过检测新创建的区块之间的时间间隔来判断网络是否被分割，但这种方法需要大约2~3 h才能相对确定客户端是否受到攻击。为了减少平均攻击检测时间，Alangot等[78]提出了比特币客户端通过与互联网上的服务器建立连接来传递交换其区块链视图消息，并且该方法不需要引入任何专用基础设施或对比特币协议和网络进行更改。

2) Erebus攻击检测

Erebus攻击主要针对采用工作量证明（PoW, proof of work）共识的区块链系统。攻击者通过控制大量IP地址形成虚假网络，干扰目标节点的正常运行。针对现有方法中选取检测对象单一、动态攻击目标感知能力弱和对节点资源要求较高的问题，Dai等[75]通过将流量行为特征与基于多模态深度特征学习的路由状态相结合，设计了基于ReliefF_WMRmR的两阶段特征选择算法和基于深度学习的多模态分类检测模型，构建了基于MLP的多模态神经网络，能够有效地检测Erebus攻击，并且检测具有较高的准确性。

3) DDoS攻击检测

在DDoS攻击检测方面，Dai等[76]结合统计和机器学习方法，通过在区块链网络层的节点端捕获流量数据，对预处理的流量进行跨层卷积操作以提取出具有高鲁棒性的攻击流量的抽象特征，并采用改进的随机梯度下降算法对模型的参数进行全局优化以防止训练参数振荡。链路泛洪攻击（LFA, link flooding attack）是一种新型DDoS攻击，利用低速率流量在区块链网络中泛洪一部分目标链路，以阻塞经过这些链路的正常流量，并切断服务器与网络

之间的连接。针对LFA，文献[79]利用长短期记忆网络的时序预测能力检测LFA，但能否通过计算不同流量源的相似性准确识别可疑攻击源，还有待进一步验证。

此外，还可以利用区块链本身具有的可视化服务与工具作为节点关联关系追踪与攻击流量检测的辅助工具。例如，区块链浏览器和Gephi、Cytoscape、Tokenview、BlockAPI等数据分析工具会清晰呈现节点或账户之间的交易关系或数据交互关系。

综上所述，基础设施层监管，区块链节点关联关系追踪与检测技术主要分为两类：一是通过监测区块链网络中节点之间消息传递和交易广播来追踪其活动，监管者可以收集和分析这些数据以了解节点的行为模式、网络拓扑和交易流动；二是利用数据可视化技术，通过区块链节点中的路由表对整个区块链网络进行动态感知，监管者可以直观地观察节点之间的连接关系、交易流向和数据变化。前者对于已定义检测规则的异常行为通过数据分析可以得到较为理想的结果，然而一旦出现新的异常行为，就需要整理新的交易数据集并重新设计检测算法进行计算，适应性较差。后者依赖数据的同步性，必须确保每个节点在某一时刻能够实现数据的一致性。通过动态可视化操作构建知识图谱，可以清晰地发现存在异常行为的地址集群或节点，更容易对该地址集群或节点进行监管。

整体而言，研究人员更倾向于结合多种技术手段，特别是图分析和机器学习，在基础设施层实现更智能化的节点追踪与可视化，以提高区块链监管的效率和节点关系的清晰度。现有研究探讨了如何提高区块链节点的追踪与检测的效率和准确性。一些研究重点关注具体的追踪技术和可视化方法，如基于图数据挖掘、机器学习等技术提高节点追踪的效率。其他研究则探讨了在不同类型的攻击（如Eclipse攻击、DDoS攻击）中如何检测和防御恶意节点的技术手段。这些研究的共同目标是增强区块链网络的安全性和可监管性，形成一个多层次、全面的节点追踪与可视化框架。未来的研究方向可能会集中在提高追踪技术的普适性和效率方面，探索更安全、隐私的追踪技术，以及进一步增强区块链网络的安全性和鲁棒性。

2.1.2 核心功能层监管

核心功能层通常由交易存储、交易处理、智能合约、共识机制等核心组件组成，用于实现区块链的基本功能和特性，为用户层提供了可靠的基础支持，主要监管方法为异常交易分析和检测、智能合约安全检测和共识机制攻击检测。此外，联盟链在核心功能层可实现穿透式监管。

2.1.2.1 异常交易分析和检测

核心功能层监管主要关注区块链上的交易数据和智能合约的执行情况，研究人员提出了多种数据分析方法来分析和检测链上数据。一种常见的方法是基于数据挖掘和机器学习技术识别异常交易和潜在的欺诈行为，监管者可以通过构建模型和算法来分析交易数据的模式和规律，识别出不符合规则的交易行为。另一种方法是利用图论和神经网络分析研究区块链网络中的交易流动和连接关系，通过构建交易图和网络图谱、可视化链上的交易数据之间的关系和连接、识别交易流动、地址之间的交互模式以及资金流动路径，可以发现异常节点、交易路径和集中度，进而评估区块链网络的安全性和稳定性。

1) 基于数据挖掘和机器学习的异常交易分析和检测

目前基于数据挖掘和机器学习对异常交易进行分析的研究主要聚焦于深入挖掘区块链节点交易数据的特征，发现其中的模式与规律，以便更有效地监管区块链网络的交易行为。朱会娟等[80]提出了一种区块链异常交易检测模型，采用残差网络结构ResNet-32，并借助自适应特征融合方法充分挖掘高层抽象特征和原始特征各自的优势，提升区块链异常交易检测性能，这为后续研究提供了模型构建和特征融合的思路。以分析交易动机为切入点，沈蒙等[81]设计了基于动机分析的区块链数字货币异常交易行为识别方法，选取空投糖果和贪婪注资两类异常交易行为作为典型，分别制定了判定规则，还抽象出异常交易模式图，为异常交易行为的分类和模式研究提供了参考。类似地，张晓琦等[82]提出了一种网络表示学习模型DeepWalk-Ba，用于区块链异常交易的特征提取，通过构建地址和实体交易图，联合特征和机器学习进行交易实体识别，并基于交易数据分析提取多粒度交易模式和用户画像，对区块链中的异常交易进行及时可靠的检测。

2) 基于图分析和神经网络的异常交易分析和检测

Wu等[83]针对比特币和以太坊网络设计了2种不同的社区检测方法，分别提出了源于频谱聚类算

法的特定聚类算法和针对图上低等级信号的新型社区检测算法，帮助找到基于用户令牌订阅的用户社区。进一步地，林伟[84]研究了基于区块链技术的虚拟货币异常交易数据检测，并提出了一种基于自定义滑动窗口机制、全连接神经网络和双向门控循环单元的多通道输出特征向量融合的区块链异常交易数据检测模型。为了保护用户隐私安全，降低数据在检测过程中被非法获取或滥用的风险，陈彬杰等[85]提出了一种基于KNN的具有隐私保护功能的区块链异常交易检测方案，记账节点通过使用矩阵乘法对交易数据特征进行随机化，随后云服务器使用KNN对随机化后的交易数据特征进行异常检测。在区块链中智能合约的异常检测方面，Liu等[86]提出了通过以太坊智能合约的交易数据与代码数据来检测欺诈合约，从复杂的智能合约中提取特征，有效识别异常合约，构建了一个适用于智能合约异常检测的异构图转换网络来检测金融欺诈，但能否研发出更精准的特征提取方法提高智能合约异常检测的效率还需要进一步深入探索。

2.1.2.2　智能合约安全检测

智能合约作为区块链技术的核心组成部分，其安全问题备受关注，此领域研究目前较为成熟[53,87-90]，为确保简洁性，本节仅从监管角度对相关文献进行简要讨论。

智能合约漏洞检测方法包括静态分析、动态分析、形式化验证、蜕变测试和基于图神经网络的方法等，这些方法旨在识别智能合约中可能存在的潜在漏洞，如重入攻击、整数溢出、权限问题和时间戳依赖性问题。由于对智能合约的异常检测发生在交易前或交易结束，不影响最终的交易结果，所以这属于事前监管或事后监管。

1) 静态分析

通过对合约代码进行静态扫描和分析，检测潜在的漏洞，常用工具有SmartCheck、Slither等。

2) 动态分析

通过模拟执行合约并监测其行为，发现可能存在的安全问题。ReGuard[91]通过使用模糊测试生成随机且多样化的交易数据，模拟可能的攻击情景，通过记录关键的执行轨迹动态识别智能合约中潜在的重入攻击。

3) 形式化验证

验证智能合约是否符合预期设计属性和安全规范。ZEUS[92]是针对智能合约的自动形式化验证工具，将Solidity源代码转换为LLVM（low level virtual machine）中间语言，并使用XACML（eXtensible access control markup language）设计了5个安全漏洞检测规则，用于在形式化验证过程中确定目标程序的安全性。

4) 蜕变测试

通过生成测试用例并在智能合约中执行，验证测试结果是否符合预期。针对可能出现的安全漏洞，陈锦富等[93]设计了不同的蜕变关系并进行蜕变测试，通过验证源测试用例和后续测试用例之间是否满足蜕变关系，判断智能合约是否存在相关安全漏洞。

5) 深度学习

基于智能合约的源代码、操作代码和控制流模式提取特征，并利用深度学习模型（如CNN、RNN和Transformer）训练和预测是否存在安全漏洞。Deng等[94]提出了一种利用深度学习和多模态决策融合的智能合约漏洞检测方法，考虑了智能合约的代码语义和控制结构信息，并通过多模态决策融合方法集成源代码、操作代码和控制流模式。Zhang等[95]提出了一种混合深度学习模型-卷积和双向门控循环单元（CBGRU, convolutional and bi-directional gated recurrent unit），结合了词嵌入方法（Word2Vec、FastText）和深度学习方法（LSTM、GRU、Bi-LSTM、CNN、BiGRU），通过词嵌入方法可以将单词或短语转化为向量表示来捕捉它们之间的语义关系，不同的深度学习模型从不同的角度提取智能合约特征，组合并输入分类器进行智能合约漏洞检测。

智能合约安全是区块链技术中一个重要而复杂的领域。当前已有许多研究致力于智能合约安全性的检测和修复，但大多数漏洞检测工具只能检测单个和旧版本的智能合约漏洞[96]。未来研究应该聚焦于进一步提高检测工具的自动化程度、效率和准确性，将静态分析方法与动态分析方法相结合，以检测多版本智能合约中更多类型的漏洞，从而实现更高的检测准确性。

2.1.2.3　共识机制攻击检测

共识协议是区块链系统中决定交易验证和区块添加的规则集合，一些常见的危害较大的攻击包括双花攻击、51%攻击、自私挖矿攻击和保存攻击

（Saving Attack）等。针对51%攻击和双花攻击开展的研究较为广泛且成熟[97-100]，为确保简洁性，仅对监管影响较大的保存攻击和自私挖矿攻击进行简要讨论。

Saving Attack是一种新型的攻击方式，可以延迟节点达成共识，攻击者在临时共识失败期间“保存”其提议区块的权利，并在网络恢复正常后利用这些权利引发另一次共识失败，这导致区块链性能下降，区块最终确认的时延增加。Otsuki等[101]对各种分叉选择规则进行了Saving Attack的模拟研究，包括最长链规则、GHOST（greedy heaviest-observed sub-tree）、LMD GHOST（latest-message-driven GHOST）和FMD GHOST（fresh-message-driven GHOST）。研究结果表明，Saving Attack对共识有非常大的负面影响，在实验条件下，一个拥有30%投票权的攻击者在保存其区块32分钟后，成功阻止了LMD GHOST共识达成83分钟。

自私挖矿攻击是由少数恶意矿工或矿池利用系统设计的漏洞或潜在弱点，通过不公平的方式获取更多的挖矿奖励。Wang等[102]利用机器学习方法检测区块链中的自私挖矿攻击，采用逻辑回归和全连接神经网络（包含10个隐藏层和每层10个神经元）分别在训练集上训练分类模型，通过学习样本的特征来判断未知样本是否属于自私挖矿攻击，或者属于事后监管方法。

2.1.2.4 联盟链穿透式监管

针对联盟链穿透式监管主要位于核心功能层。穿透式监管是一种从金融领域引入区块链监管中的方法，是指通过监管节点的穿透实现对联盟链上所有节点和交易数据的监管和追溯，以确保联盟链的安全和稳定运行，属于事中监管方法。在联盟链监管中，可将监管逻辑内嵌到核心功能层的组件内，因此穿透式监管可以深入到每个实体进行监管，并对所有交易和信息进行监管和审计。

针对汽车共享充电的各方及交易数据进行监管，刘会霞等[103]提出了一种基于区块链的共享充电桩安全监管方案，构建基于双链的共享充电信任模型，通过认证合约构建交易双方的信任关系，并设计穿透式监管方案，向上核查用户、桩主或运营商的身份，向下核查充电量、充电速度等信息的正确性，对汽车共享充电的各参与方和具体的交易数据进行有效监管。在中国场外期权市场，Zhang等[104]构建了FutureOTC系统，将联盟区块链技术与身份认证和智能合约相结合，同时将行政机构设置为联盟链上的节点并引入穿透式监管，为中国场外期权市场提供了一种去中心化、可靠和智能的解决方案。Wang等[105]提出了一个基于联盟链的非法数据层级拦截方案，通过在应用程序端使用正则化表达式和智能合约分别标记阻止不同影响程度的非法数据，可以有效地监管区块链中的非法数据。不同于以往的单联盟链，张健毅等[106]采用联盟链–公有链双链结构的可监管的数字货币模型，将联盟链作为共识的核心参与者，通过秘密共享方式保证用户交易数据的隐私性，同时以公有链为运行基础，使普通用户可以参与和见证系统的维护。为了实现交易隐私性的全面保障和细粒度的强制监管，霍鑫磊等[107]提出了一种兼具授权监管与隐私保护功能的联盟链方案，包括对联盟链下成员角色划分及变色龙哈希函数、零知识证明等密码技术。文献[106]着重于双链结构和用户参与，而文献[107]侧重于通过技术手段实现全面和精细的监管与隐私保护。

在联盟链的多个应用场景中，研究人员也提出了一些个性化解决方案。在农机调度领域，Yang等[108]提出了一个基于联盟链的农机调度系统，上层监管提高了共识算法的效率和安全性，并允许监督员阻止具有恶意动机的用户，确保系统的安全性，提高农机调度领域数据流的透明度和效率。在建筑工程领域，Li等[109]提出了用于监督离场模块化住宅生产的TABS（two-layer adaptive blockchain-based supervision）模型，实现了适应性私有侧链和主链之间的通信和交易，确保了操作记录的真实性，同时保护了参与者隐私，为建筑工程行业提供了一种无法篡改和隐私保护的监管机制。

此外，可以考虑将监管机构作为一个特权节点接入联盟链，通过追溯和审计分析链上数据以达成穿透式监管的效果，是一个可行的监管方向。

综上所述，核心功能层监管在异常交易检测方面，研究者提出了多种方法来检测和分析区块链上的异常交易，包括基于数据挖掘和机器学习技术的异常交易识别方法，以及利用图论和神经网络分析研究交易流动和连接关系。不同的研究提出了多种模型和算法，例如，朱会娟等[80]使用残差网络结构来提升检测性能，而张晓琦等[82]则通过网络表

示学习模型进行交易实体识别。这些方法虽然在技术细节上有所不同，但共同的目标是提高区块链网络的监管能力，并确保交易行为的合法性。在智能合约安全检测方面，可以看到研究者们在异常交易分析和智能合约安全领域的工作互相参考和借鉴，文献中提到的静态分析、动态分析、形式化验证等方法相互补充，从不同角度来检测智能合约中的潜在漏洞。例如，形式化验证方法通过验证智能合约是否符合设计属性，而动态分析方法则通过模拟智能合约执行来发现安全问题。这些研究共同致力于提高智能合约的安全性，减少潜在漏洞带来的风险。在联盟链监管方面，与公链形成对比的是，由于可以将监管作为基本功能引入核心功能层，或将监管方作为具有监管权限的节点接入，因此联盟链可实现穿透式监管。

2.1.3 用户层监管

用户层提供区块链接口、区块链节点、用户钱包等功能，支持开发者和矿工等角色参与、使用和维护区块链。

2.1.3.1 用户业务监管

用户层用户业务监管主要是针对用户业务方面的，如双重花费、虚假交易、洗钱、庞氏骗局、非法代币发行等。检测此类业务可使用异常交易行为分析与检测方法，异常交易行为指在区块链系统中的参与者表现出与正常交易行为模式不符的行为。针对这些异常交易行为，区块链系统的设计和监管机制需要考虑安全性和合规性，包括识别异常交易行为、监测交易模式、实施合规规则等事后监管方法，以减少和防止异常交易行为的发生。相关研究重点围绕区块链用户的异常交易行为以及相应的监管机制展开讨论，这两者分别对应了区块链用户和区块链监管机构这2个实体。

当前区块链异常交易行为识别方法存在识别目标不明确、处理海量数据效率低以及识别维度单一的问题。针对以上问题，赵泽宁[110]提出了基于启发式地址聚类的增量识别方法和基于交易子图划分的交易行为预测方法，改进了地址聚类算法，通过构建交易图和采用图神经网络提高了预测的准确率。瞿元[111]从宏观的流量数据和微观的交易数据2个层面对比特币中的异常交易行为进行研究，对于宏观流量数据，利用支持向量机和编解码器的组合实现了无监督的异常分析和告警功能。对于微观交易数据，借助演化图卷积网络（GCN）和时间图注意力（TGA, time graph attention）机制进行特征提取，并利用随机森林进行非法交易的异常检测和告警，提供了更为全面的异常检测解决方案。现有的解决方案提高了识别准确率、检测精确性和效率，但能否结合机器学习算法和加密技术增强现有的区块链异常交易行为识别效果和隐私保护功能仍需进一步深入探讨。

2.1.3.2 用户账户监管

私钥是用户访问其账户和资产的关键，黑客可能会攻击用户的钱包，通过伪造身份、诱骗或欺骗用户等手段获取私钥或篡改交易信息，从而窃取资产。以太坊吸引了大量用户和开发者的参与，然而，恶意用户和攻击者也利用以太坊匿名性和开放性的特点进行各种非法活动，如传销、诈骗、洗钱等。研究人员针对以太坊账户提供机器学习、图分析和时间序列分析方法来检测和识别恶意账户，属于事前或事后监管方法。

针对区块链中欺诈账户引发的交易安全问题，周健等[112]提出了一种基于机器学习的欺诈账户检测及特征分析模型，并引入了SHAP值通过链上数据特征分析提供更准确的预测模型。Farrugia等[113]提出了一种检测以太坊非法用户的新方法，通过特征提取和特征重要度分析，并结合XGBoost分类模型在账户层面检测以太坊网络上的非法活动。

梁飞等[114-115]先后提出了基于双曲线图神经卷积网络（LSC-GCN）[114]和基于子空间图聚类（GCN-Clustering）[115]的方法，检测存在恶意行为的以太坊账户。针对现有模型在建立模型的过程中存在数据集中的标签不足导致模型训练不充分和识别效率低的问题，GCN-Clustering将原始节点地址特征转化为含有聚类簇信息的节点特征，利用数据集本身的聚类信息增强节点特征的提取能力，同时用GCN进行监督学习，进一步加强了无监督学习中获取的聚类簇信息在节点特征中的嵌入表达。

石拓等[116]将交易时间信息融入以太坊地址账户特征的模型中，提出了基于时序交易关系的图注意力机制，并改进了传统的注意力网络，使用图注意力机制的系数融合了时间间隔信息、强化间隔时间的因素和考虑时间衰减的影响三部分内容，通过注意力的方式将中心节点与邻居节点进行聚合，可以有效识别存在异常交易行为的以太坊地址。

针对比特币和Dash、Monero、Zcash这3种注重隐私的加密货币的钱包安全，Biryukov等[117]通过手动检查和静态分析工具（如FlowDroid、SmartDec Scanner）扫描和分析钱包，检测钱包在安装方式、权限要求和隐私政策方面存在的安全威胁，提出了基于交易时间分析的交易聚类方法，监听网络流量并试图将攻击者的加密货币地址与IP地址或其他身份信息相关联。

综上所述，针对区块链系统中异常行为（如双重花费、虚假交易、洗钱等）的识别和监管方法，研究人员提出了一系列基于启发式地址聚类、交易子图划分、以太坊庞氏骗局检测等方法，旨在提高异常行为的识别精确度和效率。此外，本节还关注账户安全与监管问题，特别是私钥泄露导致资产被盗的情况。现有研究通过机器学习、图分析和时间序列分析等方法，实现检测和识别恶意账户，提高账户的安全性。随着区块链技术的不断演进和应用范围的不断扩大，未来可以向更加精细化的异常行为检测方法、更有效的账户安全保护策略以及更深入的数据分析和挖掘技术的应用方向发展与研究，以适应日益复杂和多样化的安全威胁。同时，随着监管法规的不断完善和加强，研究人员也需要更加关注区块链系统的合规性，从而确保其在商业和金融领域的可持续发展和广泛应用。

基础设施层、核心功能层、用户层相关的区块链监管技术对比如表3所示，其中×表示未考虑或非方案重点研究内容，√表示方案有所涉及。

2.2 链间监管

链间监管聚焦于不同区块链之间的交互和互操作监管，链间监管核心服务是跨链资产互换、链间通信与数据共享、跨链App操作、智能合约互操作、去中心化身份验证等。链间监管有2种类型，一种是基于“以链治链”的核心思想将监管逻辑部署在监管链上，被监管链与监管链进行数据同步，且监管链可对被监管链进行操作，另一种是对已有的跨链协议进行监管。

2.2.1 基于“以链治链”思想的监管

凯文·沃巴赫等[119]最早在法律领域提出“以链治链”这一概念，陈纯[57]对这一概念进行了进一步深化。“以链治链”技术的基本原理是将一个区块链作为监管链，用来监管另一个区块链，即被监管链。监管方可以在监管链上创建一个智能合约，该合约规定了被监管链上需要遵守的规则和条件。由此引出了一个重要研究方向-区块链“合规”监管，旨在确保区块链交易和活动符合法律法规、规范和标准等合规性要求，这些要求可以是任何类型的规则，如交易限制、防止双重支付、反洗钱等。当被监管链上的某些节点或用户违反了这些规则时，监管方可以通过智能合约在监管链上发起制裁。这种制裁通常会涉及惩罚或惩戒措施，如冻结账户、禁止交易或撤销交易等。

以太坊通过ERC（ethereum request for comments）对智能合约进行规范，从ERC20到ERC1400，实现了从逃避监管向拥抱监管的转变[120]，ERC20只要求提供代币的发行和转移等功能，而ERC1400则规定了发布证券型代币的标准，要求智能合约提供相关法律文件，并在执行转账前进行限制判断，提供对判断结果的可读解释，从而实现在合约层面锁仓、KYC/AML验证、出入账冻结等功能。Libra也在2020年发布了白皮书2.0版本来回应监管疑虑，包含合规性控制（如VASP认证、非托管钱包限制等），使Libra区块链上的所有交易强制执行某些合规性要求。这些措施都是为了提高区块链交易的合规性和透明度，更好地适应监管要求。博雅正链提供了面向监管科技的智能合约编程语言RegLang[121]，根据监管需求设计合约的语法规则和类型系统，监管方可以通过智能合约自动实现穿透式监管，监管对象能够通过监管方公布的监管规则提升自动化合规能力，提高了监管效率和准确性，使监管更加规范化、智能化和数字化。Lu等[122]构建OriginChain系统提供透明的防篡改和可追溯性数据，并自动执行合规检查。该系统生成代表法律协议的智能合约，自动检查和执行服务和条件，并检查是否满足法律法规要求。毛湘科等[123]构建了一个带有监管功能和支持回滚操作的区块链系统，从事前、事中和事后3个不同的阶段实现对区块链上交易的监管。

国内一些企业也积极推动“以链治链”技术实施落地。腾讯安全发布《CCGP跨链治理白皮书》，实现“以链治链”跨链互操作协作。该系统具备强通用性、易扩展性、多方共治、高效、高安全性和留痕可追溯等五大优势特征，覆盖数据广域共享、联合溯源和广域存证三大应用场景，有望推动区块链技术在多个场景的应用落地。北京互联网法院发

表3　区块链监管技术对比

监管层级	监管方法	技术方法	适用链	监管程度	隐私保护
基础设施层	节点关联关系追踪技术	利用ELK追踪Fabric各节点共识交易的调用轨迹[62]	Fabric	强	×
		基于Kademlia协议的节点自动发现机制[63]	公链	强	×
		基于污染/染色的追踪分析方法[58-60]	比特币	中	×
		基于节点影响力的账户余额模型区块链交易追踪方法[61]	以太坊	强	×
		利用机器学习模型从大量数据中学习节点行为和关系的模式和规律,帮助识别和分析复杂的节点行为和关系[64]	公链	中	×
		双向探索自动化比特币交易追踪技术[65]	比特币	强	×
	节点异常行为检测技术	门罗币、大零币和Tornado Cash的追踪技术,图神经网络框架MixBroker判断混币账户节点之间的关联关系[66-69]	门罗币/大零币/以太坊	强	√
		对具有挖矿能力的节点进行分类验证来预防分叉的发生[118]	公链	中	×
		基于联邦学习和基于表征学习的异常流量检测算法以及基于深度学习和多种算法的恶意节点分类和预测[70-71]	Fabric	强	×
		基于消息传递的GCN对节点分类,检测网络钓鱼节点[72-73]	以太坊	强	×
	节点攻击流量检测技术	采用基于自定义行为特征和深度学习、基于免疫的异常检测方法和利用区块链客户端的通信来检测Eclipse攻击[74-78]	比特币	强	×
		将流量行为与基于多模态深度特征学习的路由状态相结合,构建基于MLP的多模态神经网络来检测Erebus攻击[75]	以太坊	强	×
		结合统计和机器学习方法检测DDoS攻击流量[76]	公链	中	×
		利用长短期记忆网络检测链路泛洪攻击[79]	以太坊	强	×
核心功能层	异常交易分析和检测方法	基于动机分析的区块链数字货币异常交易行为识别方法[81]	公链	中	×
		构建地址和实体交易图,联合特征和机器学习进行交易异常检测[82]	公链/联盟链	强	×
		利用残差网络结构和自适应特征融合方法检测异常交易[80]	公链	中	×
		针对比特币和以太坊分别设计源于频谱聚类算法的特定聚类算法和图上低等级信号的新型社区检测算法[83]	比特币/以太坊	中	×
		多通道输出特征向量融合的虚拟货币异常交易数据检测[84]	公链	强	×
		用矩阵乘法对交易数据随机化,再用KNN进行异常检测[85]	公链	中	√
		构建适用智能合约异常检测的异构图转换网络检测金融欺诈[86]	以太坊	强	×
	智能合约安全	使用模糊测试生成随机交易数据,识别智能合约中的重入漏洞[91]	Solidity编写的智能合约	中	×
		针对智能合约的自动形式化验证工具ZEUS[92]		中	√
		设计不同蜕变关系进行测试用例生成,判断智能合约安全漏洞[93]		强	×
		分别使用深度学习和多模态决策融合、混合深度学习模型CBGRU,提取智能合约特征进行智能合约漏洞检测[94-95]		强	×
	共识机制安全	使用模拟研究的方法研究保存攻击对不同分叉选择规则的影响[101]	POS	强	×
		采用逻辑回归和全连接神经网络进行训练检测自私挖矿攻击[102]	比特币	中	×
	联盟链穿透式监管技术	构建基于双链的共享充电信任模型,设计穿透式监管方案[103]	联盟链	强	×
		将行政机构设置为联盟链上的节点来引入穿透式监管[104]	联盟链	强	×
		使用正则表达式和智能合约标记阻止层级非法数据[105]	联盟链	强	×
		联盟链-公有链双链结构的可监管的数字货币模型[106]	联盟链/公链	中	√
		农机调度和建筑工程领域下保护隐私的监管机制[108-109]	联盟链	中	√
		通过对联盟链成员角色划分实现细粒度的强制监管[107]	联盟链	强	√
用户层	用户业务监管	基于启发式地址聚类和基于交易子图划分的方法识别用户异常行为[110]	比特币/以太坊	中	×
		结合支持向量机、编解码器、GCN和随机森林进行无监督的异常分析和告警以及非法交易的异常检测和告警[111]	比特币	中	√
	用户账户监管	基于机器学习和SHAP值的欺诈账户检测模型[112]	以太坊	强	×
		通过特征提取和特征重要度检测以太坊非法用户和活动[113]	以太坊	中	×
		使用LSC-GCN和GCN-Clustering方法检测以太坊恶意账户[114-115]	以太坊	强	×
		基于时序交易关系的图注意力机制结合交易时间信息识别可疑交易行为[116]	以太坊	中	×

布的“天平链”应用接入技术及管理规范[124]，规范了区块链应用接入的技术和流程，提高了电子证据的可信度和效率。该规范涉及接入平台的系统安全性、电子数据合规性和区块链安全性3个方面的要求，推动区块链技术在司法领域的应用。文献[125-128]从物联网、法律和云服务等不同应用场景中探讨智能合约合规验证模型，验证和确认不同环境下智能合约的合规性。

经普杰等[129]提出了一种基于“以链治链”思想的分层跨链监管架构，设计了监管架构中“监管链-业务链”跨链协作的以链治链监管模式，改善了监管行为中心化的集权特性，设计的具有通用性的跨链交互标准数据结构保证了跨链监管过程的通用、安全和高效。Zhang等[130]提出了其链上分层结构、链上和链下混合存储模式、链上监管流程和交易信息可追溯流程，通过事前、事中和事后协同监管，对数据交易的全过程进行多方分层、多维度监管，并利用监管智能合约实现多个监管方的分层监管和事后可追溯（事后监管），能够有效隔离和保护数据交易之间的敏感信息。

我国央行、广东深圳等地方政府已经开始积极采取“以链治链”的方式，利用区块链技术对金融行业进行监管[38]。例如，广东省防控中心利用“金鹰系统”监测疑似非法金融活动企业，对于金融风险的监测与防控效果显著。

以链治链技术可以让监管方通过智能合约对违规节点和用户进行惩罚，有效减少网络攻击和欺诈行为，从而增强了区块链网络的监管和安全性[129]。此外，以链治链技术可以确保监管者随时在监管链上查询被监管链的状态，在任何时候都能够了解网络中发生的一切，提高了区块链网络的透明度和可靠性。以链治链技术可以应用于如今丰富的区块链场景，如金融、物流、医疗等领域，实现更安全和可靠的交易和信息传输。

2.2.2 跨链安全监管

跨链技术是实现链间互联和价值转移的重要技术手段，跨链技术实现了不同区块链之间的互操作性和数据交换，但同时也带来了新的安全风险。

跨链系统的安全性主要取决于原子性、链间信息同步性和网络通道的安全性。鉴于异构区块链在区块结构、共识机制和复杂工作机制方面的多样性，加之跨链技术固有的安全漏洞，如跨链的技术原理与实现机制中的缺陷，这些因素都可能造成安全隐患。此外，若底层区块链的共识算法存在漏洞或被攻破，跨链交互操作的安全性也将受到威胁。公证人机制可能引发共谋攻击和单点故障风险，公证人是负责验证和确认跨链交易的节点，如果公证人之间合谋或某个公证人受到攻击，则整个跨链系统的安全性将受到威胁。哈希锁定机制是一种用于跨链交易的时间约束机制，可能受到时钟漂移和恶意延迟攻击的影响，时钟漂移可能导致锁定时间不准确，而恶意延迟攻击则是利用网络时延来操纵跨链交易的执行顺序。吴迪[131]针对哈希锁定转账延时攻击、中继跨链路由攻击和中继链区块阻塞攻击提出了防护方法，一定程度上加强了跨链系统的安全监管。首先，为了防止哈希锁定转账延时攻击，可以采取扩大时间差的方法，通过扩大Fabric端和ETH端的时间差来增加攻击者进行恶意等待和阻塞网络的难度。然后，可以采取应用链白名单、应用链余额查询和应用链创建时间查询3种防护方法来应对中继跨链路由攻击。最后，通过综合运用设置连接计数脚本和修改网关处理请求顺序这2种方法，可以有效防范中继链区块阻塞攻击。

2.3 链外监管

链外监管是指监管方通过链外机制对被监管链进行监管和管理，这些链外机制包括社区讨论、投票、协商、链下治理、委员会决策等方式。但链外监管存在参与度不足、权力滥用和缺乏透明度等问题[132-133]，需要通过有效的机制和规则来解决。

以太坊The DAO事件[134]和比特币区块大小争论[135]是2个比较典型的链外监管事件，以太坊The DAO事件涉及以太坊智能合约的安全性和治理问题。最终以太坊社区通过链下讨论和投票的方式，决定对以太坊区块链进行硬分叉，以恢复被盗资产，并维护以太坊网络的稳定性。比特币区块大小争论持续了数年，涉及比特币网络的协议更新和扩容等重要事项，但最终的决策是由少数开发者和矿工在链下进行的协商和投票，而大多数比特币用户并未参与或了解这个过程。这种监管不透明和参与度不足的情况，反映了链外监管的一些问题和限制，也引发了对链外监管的探讨和尝试。例如，以太坊开放科研论坛Ethresearch提出的出块节点选举协议Whisk就是由多个社区成员而非以太坊官方人员参与讨论并设计提出。

在实践中，链内监管和链外监管相互结合可以达到更好的监管效果与社区治理效果。EOS[136]是一个基于股份授权证明（DPoS, delegated proof of stake）共识算法的区块链项目，其社区治理机制采用链内链外监管结合的模式。链外监管包括社区讨论、投票和协商等方式，而链内监管通过智能合约等方式来实现。Miyachi 等[137]提出了用于增强医疗信息管理的模块化混合隐私保护框架，结合链内和链外监管 2 种方式设计参考模型，主要通过分布式软件架构实现链内资源与链外资源的交互，从而实现不同类型的医疗数据隐私化管理。

对链内、链间和链外这 3 种监管方式的技术原理、优缺点进行比较，如表 4 所示。

3　区块链监管未来展望

区块链安全监管的挑战与机遇如表 5 所示。对第 3 节中 3 个类别的区块链监管技术进行分析总结可看出，当前区块链监管存在以下 4 个共性问题。

1) 数据关联分析难

区块链交易数据存储在分布式网络中，由于区块链交易的去中心化和匿名性，监管方难以追踪交易参与者的真实身份。例如，在门罗币、达氏币和大零币等隐私公链上，交易参与者的身份和交易细节不公开，监管方难以获取完整的交易信息，从而难以发现和惩罚违规行为，对这些区块链网络中的非法交易和行为监管比较困难。

可能的解决办法是突破链群实体关联与匿名数字身份识别等技术，构建区块链实体-数据-链群三位一体关联式监管，并融合机器学习提取网络层流量数据等非匿名数据的特征，训练针对性的监管大语言模型，但是对于大语言模型在区块链安全监管中的独有算法的安全性也需要纳入考虑，从而保证

表 4　链内、链间和链外监管对比分析

监管方式	技术原理	优点	缺点
链内监管	采用部署节点等较为网络底层的手段加入区块链网络进行流量检测、交易分析和攻击检测	1) 监管生效快:获取链上数据收集较为及时全面,方便结合人工智能进行实时分析; 2) 监管效果好:部署节点的方式可实现一定程度的区块链交易审查	1) 监管成本高:监管方需付出一定的成本部署和维护监管节点,需要高性能计算设备和高网络带宽进行区块链数据和流量分析; 2) 监管隐蔽性差:部署探针类节点的方式容易引起区块链底层网络波动,可能引起监管目标察觉
链间监管[120-123,125-128,138]	将监管规则和条件编码为智能合约并部署在监管链上	1) 自动执行:智能合约的执行是由区块链网络自动完成的,可以保证监管规则的执行不受任何人为因素的影响; 2) 透明度高:监管规则和条件被编码为智能合约,并写入区块链不可变的分布式账本中; 3) 防篡改:智能合约的执行结果被写入区块链不可变的分布式账本中,可以防止被篡改	1) 智能合约自身漏洞:如果智能合约存在漏洞或错误,可能导致监管失败; 2) 执行效率低:智能合约的执行需要消耗大量的计算和存储资源
链外监管[132-135]	监管方通过外部手段对被监管链进行监管	1) 执行效率高:不需要消耗大量的计算和存储资源; 2) 可定制性强:可以根据不同的监管需求进行定制	1) 人为干预:容易受到人为因素的影响,可能导致监管者的不公正行为; 2) 透明度低:链下治理的监管过程不在区块链上,难以保证监管的透明度和可靠性; 3) 易受攻击:需要网络和服务器等基础设施的支持,容易受到恶意攻击的影响

表 5　区块链安全监管的挑战与机遇

挑战	机遇
数据关联分析难	需考虑突破链群实体关联与匿名数字身份识别等技术,构建区块链实体-数据-链群三位一体关联式监管,融合机器学习提取网络层流量数据等非匿名数据的特征,训练针对性的监管大语言模型
业务合规监管考虑少	应考虑链上业务与安全漏洞风险协同监管,应针对业务和技术风险分别设计专门的监管方案或系统
跨链协作监管能力低	利用波卡插槽拍卖、跨链 HUB 等跨链协议进行以链治链监管
监管成本高	参与区块链社区事项投票与决策,发挥监管效力的同时平衡监管成本

监管技术本身的安全性。一个典型的针对大语言模型的攻击方式是命令注入，攻击者可以通过巧妙构造输入，使模型执行期望之外的行为。如果基于大语言模型的区块链监管接口被滥用，即使有输入规范，攻击者仍可能使用命令注入利用监管接口的权限导致损害或干扰被监管的区块链应用的正常运行。

2) 业务合规监管考虑少

现有监管方案偏向于利用技术手段监管某一具体的漏洞或风险，忽略了监管目标业务本身的合规安全风险，可能导致监管漏洞的存在。现有的监管方法和技术只适用于某些特定的区块链网络[80-81,84,113]，通用性较差，应考虑链上业务与安全漏洞风险协同监管，针对业务和技术风险分别设计专门的监管方案或系统。

3) 跨链协作监管能力低

区块链跨链协议发展已较为成熟，出现了多种跨链项目。跨链也不再局限于仅涉及两条区块链，而是出现了以波卡链为代表的多链协作互联的复杂跨链场景。对此，相应的区块链监管研究还不够深入和充分，需要考虑建立跨链监管互操作机制[139]或多链协同监管机制，如利用波卡链的插槽拍卖机制将监管逻辑嵌入得到的插槽中，监管连接插槽的区块链应用。

4) 监管成本高

由于运行监管方案或系统需外部持续投入资源，监管成本将只增不减，无法做到监管自行维持。例如，节点检测和攻击检测技术需要长期维护所需网络设施或部署节点收集区块链P2P层流量。异常交易分析和智能合约安全需投入大量计算资源训练所需机器学习模型以完成检测或识别。节点追踪技术需要进行大量数据分析。穿透式监管则需要投入大量软件资源以满足监管所需要求。

可能的平衡监管成本的方式是，区块链监管方作为区块链社区的一员，可作为去中心化自治组织的成员对事项进行提议与投票，这些过程产生的收益可用于降低监管成本。因此，能否基于区块链生态模型并结合监管成本，使用博弈论对监管有效性与监管收益进行量化建模，从而进一步分析监管对于区块链生态发展的具体作用是一个有待探索的方向。

随着区块链技术的深入发展，现已出现多种旨在解决现有公链可扩展性问题的Rollup[140]项目，如Arbitrum[141]、Optimism[142]等，以及采用新记账结构或分片的高性能公链，如Kaspa[143]、Near[144]等，传统的监管技术对其适用性有待深入检验。此外，去中心化交易所的出现促进了去中心化金融生态的繁荣，对去中心化交易所的监管将是区块链安全监管的一个重点领域。监管方应关注如下几个新兴区块链项目，如表6所示。

对这些新兴区块链项目的监管，可行的监管手段如下。

1) 监管时应考虑利用去中心化自治组织实现监管。比如，非许可链的去中心化社区本身就对项目具有治理权和投票权，这些社区参与门槛不高，不失为监管的一大有效途径。

2) 应将监管范围扩展到各种Rollup方案和DeFi项目，并根据其底层实现机制进行针对性监管，以此增加监管覆盖面。

3) 应关注比特币新生态，并进行针对性监管。近期出现以Ordinals和Sats为代表的铭文生态、以Runes为代表的符文生态和比特币智能合约虚拟机，未来监管方应留意这些新兴区块链项目。

4 结束语

区块链的快速发展带来了日渐严重的安全问题，也让区块链安全监管成为领域内的研究重点之一。本文将区块链生态现状进行了分析归纳并简要

表6 新兴区块链项目

监管领域	监管目标	监管难点	可能的平衡监管成本的方式
Rollup	Arbitrum、Optimism等Layer 2扩展网络	1) 与主链状态相对隔离，主链监管手段不适用；2) 排序器节点抗审查	1) 成为排序器节点获取状态提交收益；2) 成为验证节点获取验证收益
去中心化金融	DEX、借贷协议、NFT等	缺乏KYC认证、交易抗审查	成为订单填充者获取市场信息，并获取交易费收益
比特币新生态	铭文/符文协议、比特币智能合约虚拟机等	协议去中心化、智能合约虚拟机抗审查	去中心化社区投票与决策

阐述区块链监管的国内外政策背景，根据当前区块链技术和其上应用的特点给出了链内基础设施、跨链扩展和链外去中心化自治社区与应用的三层划分，并依据此划分将现有的监管技术及方案归纳为链内监管、链间监管和链外监管 3 个方面进行了系统的分析和比较，重点讨论了链内监管的基础设施层、核心功能层和用户层监管的相关文献并进行了特点比较，简要讨论了链间和链外监管的代表性方案，并将链内、链间和链外 3 种监管方案进行了总结对比，最后指出了当前区块链安全监管的共性问题和可能的改进方向以及未来监管方应该留意的新兴区块链项目。

参考文献:

[1] CHOI T M, SIQIN T. Blockchain in logistics and production from blockchain 1.0 to blockchain 5.0: an intra-inter-organizational framework[J]. Transportation Research Part E: Logistics and Transportation Review, 2022, 160: 102653.

[2] ALIEF R N, PUTRA M A P, GOHIL A, et al. FLB2: layer 2 blockchain implementation scheme on federated learning technique[C]//Proceedings of the 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). Piscataway: IEEE Press, 2023: 846-850.

[3] PIERRO G A, TONELLI R. Can solana be the solution to the blockchain scalability problem? [C]//Proceedings of the 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER). Piscataway: IEEE Press, 2022: 1219-1226.

[4] ROCKET T, YIN M F, SEKNIQI K, et al. Scalable and probabilistic leaderless BFT consensus through metastability[J]. arXiv Preprint, arXiv: 1906.08936, 2019.

[5] TANG Y, YAN J W, CHAKRABORTY C, et al. Hedera: a permissionless and scalable hybrid blockchain consensus algorithm in multiaccess edge computing for IoT[J]. IEEE Internet of Things Journal, 2023, 10(24): 21187-21202.

[6] FITZI M, WANG X C, KANNAN S, et al. Minotaur: multi-resource blockchain consensus[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2022: 1095-1108.

[7] JAYAPAL C, M J, S N R. An insight into NFTs, stablecoins and DEXs in blockchain[C]//Proceedings of the 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). Piscataway: IEEE Press, 2023: 1-6.

[8] DEVMANE M A. D-space: a decentralized social media app[C]//Proceedings of the 2023 2nd International Conference on Edge Computing and Applications (ICECAA). Piscataway: IEEE Press, 2023: 809-814.

[9] BREIKI H A. Trust evolution game in blockchain[C]//Proceedings of the 2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA). Piscataway: IEEE Press, 2022: 1-4.

[10] KARANJAI R, XU L, DIALLO N, et al. DeFaaS: decentralized function-as-a-service for emerging dApps and Web3[C]//Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). Piscataway: IEEE Press, 2023: 1-3.

[11] GABRIEL T, CORNEL-CRISTIAN A, ARHIP-CALIN M, et al. Cloud storage. A comparison between centralized solutions versus decentralized cloud storage solutions using blockchain technology[C]//Proceedings of the 2019 54th International Universities Power Engineering Conference (UPEC). Piscataway: IEEE Press, 2019: 1-5.

[12] ZHONG Z S, WEI S R, XU Y T, et al. SilkViser: a visual explorer of blockchain-based cryptocurrency transaction data[C]//Proceedings of the 2020 IEEE Conference on Visual Analytics Science and Technology (VAST). Piscataway: IEEE Press, 2020: 95-106.

[13] SABLE N P, RATHOD V U, SABLE R, et al. The secure E-wallet powered by blockchain and distributed ledger technology[C]//Proceedings of the 2022 IEEE Pune Section International Conference (PuneCon). Piscataway: IEEE Press, 2022: 1-5.

[14] ARAB G A, COGLIATTI J I, URQUIZÓ P, et al. Development of a blockchain-based Web3 application for CO_2 absortion right management[C]//Proceedings of the 2023 IEEE International Humanitarian Technology Conference (IHTC). Piscataway: IEEE Press, 2023: 1-4.

[15] CUI W P, SUN Y X, ZHOU J R, et al. Understanding the blockchain ecosystem with analysis of decentralized applications: an empirical study[C]//Proceedings of the 2021 the 5th International Conference on Management Engineering, Software Engineering and Service Sciences. New York: ACM Press, 2021: 38-44.

[16] SUN J, SADDIK A E, CAI W. Smart contract as a service: a paradigm of reusing smart contract in web3 ecosystem[J]. IEEE Consumer Electronics Magazine, 2024, 14(1): 46-55..

[17] RAIKWAR M, GLIGOROSKI D. Aggregation in blockchain ecosystem[C]//Proceedings of the 2021 Eighth International Conference on Software Defined Systems (SDS). Piscataway: IEEE Press, 2021: 138-143.

[18] 董伟良, 刘哲, 刘逵, 等. 智能合约漏洞检测技术综述[J]. 软件学报, 2024, 35(1): 38-62.
DONG W L, LIU Z, LIU K, et al. Survey on vulnerability detection technology of smart contracts[J]. Journal of Software, 2024, 35(1): 38-62.

[19] 魏松杰, 吕伟龙, 李莎莎. 区块链公链应用的典型安全问题综述[J]. 软件学报, 2022, 33(1): 324-355.
WEI S J, LÜ W L, LI S S. Overview on typical security problems in public blockchain applications[J]. Journal of Software, 2022, 33(1): 324-355.

[20] 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.

[21] 刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展[J]. 计算机学报, 2021, 44(1): 1-27.
LIU M D, CHEN Z N, SHI Y J, et al. Research progress of blockchain in data security[J]. Chinese Journal of Computers, 2021, 44(1): 1-27.

[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] ZHOU S S, LI K, XIAO L J, et al. A systematic review of consensus mechanisms in blockchain[J]. Mathematics, 2023, 11(10): 2248.

[24] XU J, WANG C, JIA X H. A survey of blockchain consensus protocols[J]. ACM Computing Surveys, 2023, 55(13): 1-35.

[25] CHOO K R, OZCAN S, DEHGHANTANHA A, et al. Editorial: blockchain ecosystem: technological and management opportunities and challenges[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 982-987.

[26] KHANG A, CHOWDHURY S, SHARMA S. The data-driven blockchain ecosystem: fundamentals, applications, and emerging technologies[M]. Boca Raton: CRC Press, 2022.

[27] RIASANOW T, BURCKHARDT F, SETZKE D S, et al. The generic blockchain ecosystem and its strategic implications[C]//Proceedings of the 24th Americas Conference of Information Systems. Piscataway: IEEE Press, 2018. 1-10.

[28] REHMAN M H U, SALAH K, DAMIANI E, et al. Trust in blockchain cryptocurrency ecosystem[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1196-1212.

[29] STAFFORD T F, TREIBLMAIER H. Characteristics of a blockchain ecosystem for secure and sharable electronic medical records[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1340-1362.

[30] KABASHKIN I. Risk modelling of blockchain ecosystem[C]//International Conference on Network and System Security. Berlin: Springer, 2017: 59-70.

[31] YOO S. A study on blockchain ecosystem[J]. The Journal of the Institute of Webcasting, Internet and Telecommunication, 2018, 18: 1-9.

[32] KIM J W. Analysis of blockchain ecosystem and suggestions for improvement[J]. Journal of Information and Communication Convergence Engineering, 2021, 19(1): 8-15.

[33] RAIKWAR M, GLIGOROSKI D. DoS attacks on blockchain ecosystem[C]//European Conference on Parallel Processing. Berlin: Springer, 2022: 230-242.

[34] ZHANG H, YI J B, WANG Q. Research on the collaborative evolution of blockchain industry ecosystems in terms of value co-creation[J]. Sustainability, 2021, 13(21): 11567.

[35] PAPADONIKOLAKI E, TEZEL A, YITMEN I, et al. Blockchain innovation ecosystems orchestration in construction[J]. Industrial Management & Data Systems, 2023, 123(2): 672-694.

[36] 张伟, 董伟, 张丰麒, 等. 德国区块链技术在金融科技领域中的应用、监管思路及对我国的启示[J]. 国际金融, 2019(9): 76-80.
ZHANG W, DONG W, ZHANG F Q, et al. The application of German blockchain technology in the field of financial science and technology, its supervision ideas and its enlightenment to China[J]. International Finance, 2019(9): 76-80.

[37] 杨东, 陈哲立. 虚拟货币立法: 日本经验与对中国的启示[J]. 证券市场导报, 2018(2): 69-78.
YANG D, CHEN Z L. Virtual currency legislation: experience of Japan and inspiration to China[J]. Securities Market Herald, 2018(2): 69-78.

[38] 刘宗媛, 黄忠义, 孟雪. 中外区块链监管政策对比分析[J]. 网络空间安全, 2020, 11(6): 19-24.
LIU Z Y, HUANG Z Y, MENG X. Application of blockchain in the field of digital rights[J]. Cyberspace Security, 2020, 11(6): 19-24.

[39] 邓建鹏. 美国区块链监管机制及启示[J]. 中国经济报告, 2019(1): 125-130.
DENG J P. Blockchain regulatory mechanism and enlightenment in United States[J]. China Policy Review, 2019(1): 125-130.

[40] 邓建鹏. 新加坡的区块链监管政策及其评议[J]. 复旦大学法律评论, 2020(1): 59-72.
DENG J P. Singapore's blockchain regulatory policy and its review[J]. Fudan University Law Review, 2020(1): 59-72.

[41] 皮六一, 薛中文. 加密资产交易监管安排及国际实践[J]. 证券市场导报, 2019(7): 4-12.
PI L Y, XUE Z W. Regulation arrangement and international practice of crypto-asset transactions[J]. Securities Market Herald, 2019(7): 4-12.

[42] 邹萍, 李艳东, 王肖, 等. 区块链监管的现状与展望[J]. 网络空间安全, 2019, 10(6): 51-56.
ZOU P, LI Y D, WANG X, et al. The status quo and future trends of blockchain regulation[J]. Cyberspace Security, 2019, 10(6): 51-56.

[43] 洪学海, 汪洋, 廖方宇. 区块链安全监管技术研究综述[J]. 中国科学基金, 2020, 34(1): 18-24.
HONG X H, WANG Y, LIAO F Y. Review on the technology research of blockchain security supervision[J]. Bulletin of National Natural Science Foundation of China, 2020, 34(1): 18-24.

[44] 王利朋, 关志, 李青山, 等. 区块链数据安全服务综述[J]. 软件学报, 2023, 34(1): 1-32.
WANG L P, GUAN Z, LI Q S, et al. Survey on blockchain-based security services[J]. Journal of Software, 2023, 34(1): 1-32.

[45] 刘汉卿, 阮娜. 区块链中攻击方式的研究[J]. 计算机学报, 2021, 44(4): 786-805.
LIU H Q, RUAN N. A survey on attacking strategies in blockchain[J]. Chinese Journal of Computers, 2021, 44(4): 786-805.

[46] 于戈, 聂铁铮, 李晓华, 等. 区块链系统中的分布式数据管理技术: 挑战与展望[J]. 计算机学报, 2021, 44(1): 28-54.
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, 2021, 44(1): 28-54.

[47] 徐恪, 凌思通, 李琦, 等. 基于区块链的网络安全体系结构与关键技术研究进展[J]. 计算机学报, 2021, 44(1): 55-83.
XU K, LING S T, LI Q, et al. Research progress of network security architecture and key technologies based on blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 55-83.

[48] 秦超霞, 郭兵, 沈艳, 等. 区块链的安全风险评估模型[J]. 电子学报, 2021, 49(1): 117-124.
QIN C X, GUO B, SHEN Y, et al. Security risk assessment model of blockchain[J]. Acta Electronica Sinica, 2021, 49(1): 117-124.

[49] 钱鹏, 刘振广, 何钦铭, 等. 智能合约安全漏洞检测技术研究综述[J]. 软件学报, 2022, 33(8): 3059-3085.
QIAN P, LIU Z G, HE Q M, et al. Smart contract vulnerability detection technique: a survey[J]. Journal of Software, 2022, 33(8): 3059-3085.

[50] 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.

[51] JIANG F, CHAO K L, XIAO J M, et al. Enhancing smart-contract security through machine learning: a survey of approaches and techniques[J]. Electronics, 2023, 12(9): 2046.

[52] WU H G, PENG Y B, HE Y Q, et al. A review of deep learning-based vulnerability detection tools for Ethernet smart contracts[J]. Computer Modeling in Engineering & Sciences, 2024, 140(1): 77-108.

[53] CHU H T, ZHANG P C, DONG H, et al. A survey on smart contract vulnerabilities: data sources, detection and repair[J]. Information and Software Technology, 2023, 159: 107221.

[54] 陈锦富, 冯乔伟, 蔡赛华, 等. 基于形式化方法的区块链系统漏洞检测模型[J]. 软件学报, 2024, 35(9): 4193-4217.
CHEN J F, FENG Q W, CAI S H, et al. Vulnerability detection model for blockchain systems based on formal method[J]. Journal of Software, 2024, 35(9): 4193-4217.

[55] WANG Y, GOU G P, LIU C, et al. Survey of security supervision on blockchain from the perspective of technology[J]. Journal of Information Security and Applications, 2021, 60: 102859.

[56] 叶聪聪, 李国强, 蔡鸿明, 等. 区块链的安全检测模型[J]. 软件学报, 2018, 29(5): 1348-1359.
YE C C, LI G Q, CAI H M, et al. Security detection model of blockchain[J]. Journal of Software, 2018, 29(5): 1348-1359.

[57] 陈纯. 联盟区块链关键技术与区块链的监管挑战[R]. 2019.
CHEN C. Key technologies of consortium blockchain and regulatory challenges of blockchain[R]. 2019.

[58] MÖSER M, BÖHME R, BREUKER D. Towards risk scoring of Bitcoin transactions[C]//Financial Cryptography and Data Security. Berlin: Springer, 2014: 16-32.

[59] ANDERSON R. Making Bitcoin legal (transcript of discussion)[C]// Security Protocols XXVI. Berlin: Springer, 2018: 254-265.

[60] TOVANICH N, CAZABET R. Pattern analysis of money flows in the Bitcoin blockchain[C]//International Conference on Complex Networks and Their Applications. Berlin: Springer, 2023: 443-455.

[61] 李致远, 徐丙磊, 周颖仪. 基于节点影响力的区块链匿名交易追踪方法[J]. 计算机科学, 2024, 51(7): 422-429.
LI Z Y, XU B L, ZHOU Y Y. Blockchain anonymous transaction tracking method based on node influence[J]. Computer Science, 2024, 51(7): 422-429.

[62] 李杉杉, 王岩泽, 邹英龙, 等. 基于自定义日志的Fabric的共识交易轨迹可视化追踪方法[J]. 计算机应用, 2022, 42(11): 3421-3428.
LI S S, WANG Y Z, ZOU Y L, et al. Consensus transaction trajectory visualization tracking method for Fabric based on custom logs[J]. Journal of Computer Applications, 2022, 42(11): 3421-3428.

[63] ZHENG L W, HELU X H, LI M H, et al. Automatic discovery mechanism of blockchain nodes based on the kademlia algorithm[C]//International Conference on Artificial Intelligence and Security. Berlin: Springer, 2019: 605-616.

[64] MICHALSKI R, DZIUBAŁTOWSKA D, MACEK P. Revealing the character of nodes in a blockchain with supervised learning[J]. IEEE Access, 2020, 8: 109639-109647.

[65] GOMEZ G, MORENO-SANCHEZ P, CABALLERO J. Watch your back: identifying cybercrime financial relationships in Bitcoin through back-and-forth exploration[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2022: 1291-1305.

[66] DU H B, CHE Z, SHEN M, et al. Breaking the anonymity of ethereum mixing services using graph feature learning[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 616-631.

[67] 林定康, 颜嘉麒, 巴•楠登, 等. 门罗币匿名及追踪技术综述[J]. 计算机应用, 2022, 42(1): 148-156.
LIN D K, YAN J Q, LANDENG B, et al. Survey of anonymity and tracking technology in monero[J]. Journal of Computer Applications, 2022, 42(1): 148-156.

[68] 符朕皓, 林定康, 姜皓晨, 等. 大零币匿名技术及追踪技术综述[J]. 计算机科学, 2021, 48(11): 62-71.
FU Z H, LIN D K, JIANG H C, et al. Survey of anonymous and tracking technology in zerocash[J]. Computer Science, 2021, 48(11): 62-71.

[69] KUMAR A, FISCHER C, TOPLE S, et al. A traceability analysis of monero's blockchain[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2017: 153-173.

[70] 刘国智. 基于联邦学习的异常流量监测方法研究与实现[D]. 北京: 北京邮电大学, 2021.
LIU G Z. Research and implementation of abnormal traffic monitoring method based on federated learning[D]. Beijing: Beijing University of Posts and Telecommunications, 2021.

[71] SANDA O, PAVLIDIS M, SERAJ S, et al. Long-range attack detection on permissionless blockchains using deep learning[J]. Expert Systems with Applications, 2023, 218: 119606.

[72] ZHANG Z, HE T, CHEN K, et al. Phishing node detection in ethereum transaction network using graph convolutional networks[J]. Applied Sciences, 2023, 13(11): 6430.

[73] YU T, CHEN X M, XU Z, et al. MP-GCN: a phishing nodes detection approach via graph convolution network for ethereum[J]. Applied Sciences, 2022.

[74] DAI Q Y, ZHANG B, DONG S Q. Eclipse attack detection for blockchain network layer based on deep feature extraction[J]. Wireless Communications and Mobile Computing, 2022, 2022(1): 1451813.

[75] DAI Q Y, ZHANG B, XU K Y, et al. An Erebus attack detection method oriented to blockchain network layer[J]. Computers, Materials & Continua, 2023, 75(3): 5395-5431.

[76] DAI Q Y, ZHANG B, DONG S Q. A DDoS-attack detection method oriented to the blockchain network layer[J]. Security and Communication Networks, 2022, 2022: 5692820.

[77] 吕婧淑, 杨培, 陈文, 等. 基于免疫的区块链eclipse攻击的异常检测[J]. 计算机科学, 2018, 45(2): 8-14.
LYU J S, YANG P, CHEN W, et al. Abnormal detection of eclipse attacks on blockchain based on immunity[J]. Computer Science, 2018, 45(2): 8-14.

[78] 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.

[79] 曹琬廅. 基于区块链的可信链路泛洪攻击检测方法研究[D]. 合肥: 中国科学技术大学, 2022.
CAO W(J/Q). Research on detection method of trusted link flooding attack based on blockchain[D]. Hefei: University of Science and Technology of China, 2022.

[80] 朱会娟, 陈锦富, 李致远, 等. 基于多特征自适应融合的区块链异常交易检测方法[J]. 通信学报, 2021, 42(5): 41-50.
ZHU H J, CHEN J F, LI Z Y, et al. Block-chain abnormal transaction detection method based on adaptive multi-feature fusion[J]. Journal on Communications, 2021, 42(5): 41-50.

[81] 沈蒙, 桑安琪, 祝烈煌, 等. 基于动机分析的区块链数字货币异常交易行为识别方法[J]. 计算机学报, 2021, 44(1): 193-208.

SHEN M, SANG A Q, ZHU L H, et al. Abnormal transaction behavior recognition based on motivation analysis in blockchain digital currency[J]. Chinese Journal of Computers, 2021, 44(1): 193-208.

[82] 张晓琦, 白雪, 李光松, 等. 基于网络表示学习的区块链异常交易检测[J]. 网络安全与数据治理, 2022, 41(10): 11-20.
ZHANG X Q, BAI X, LI G S, et al. Blockchain abnormal transaction detection based on network representation learning[J]. Cyber Security and Data Governance, 2022, 41(10): 11-20.

[83] WU S X, WU Z X, CHEN S H, et al. Community detection in blockchain social networks[J]. Journal of Communications and Information Networks, 2021, 6(1): 59-71.

[84] 林伟. 基于多特征融合的区块链异常交易检测[J]. 信息网络安全, 2022(10): 24-30.
LIN W. Detection of abnormal transactions in blockchain based on multi feature fusion[J]. Netinfo Security, 2022(10): 24-30.

[85] 陈彬杰, 魏福山, 顾纯祥. 基于KNN的具有隐私保护功能的区块链异常交易检测[J]. 信息网络安全, 2022, 22(3): 78-84.
CHEN B J, WEI F S, GU C X. Blockchain abnormal transaction detection with privacy-preserving based on KNN[J]. Netinfo Security, 2022, 22(3): 78-84.

[86] LIU L, TSAI W T, BHUIYAN M Z A, et al. Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum[J]. Future Generation Computer Systems, 2022, 128: 158-166.

[87] HE D J, DENG Z, ZHANG Y X, et al. Smart contract vulnerability analysis and security audit[J]. IEEE Network, 2020, 34(5): 276-282.

[88] VACCA A, SORBO A D, VISAGGIO C A, et al. A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges[J]. Journal of Systems and Software, 2021, 174: 110891.

[89] CHEN H S, PENDLETON M, NJILLA L, et al. A survey on ethereum systems security: vulnerabilities, attacks, and defenses[J]. ACM Computing Surveys, 2020, 53(3): 1-43.

[90] KANNENGIEßER N, LINS S, SANDER C, et al. Challenges and common solutions in smart contract development[J]. IEEE Transactions on Software Engineering, 2022, 48(11): 4291-4318.

[91] LIU C, LIU H, CAO Z, et al. ReGuard: finding reentrancy bugs in smart contracts[C]//Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings. New York: ACM Press, 2018: 65-68.

[92] KALRA S, GOEL S, DHAWAN M, et al. ZEUS: analyzing safety of smart contracts[C]//Proceedings 2018 Network and Distributed System Security Symposium. Piscataway: IEEE Press, 2018: 1-12.

[93] 陈锦富, 王震鑫, 蔡赛华, 等. 基于蜕变测试的区块链智能合约漏洞检测方法[J]. 通信学报, 2023, 44(10): 164-176.
CHEN J F, WANG Z X, CAI S H, et al. Vulnerability detection method for blockchain smart contracts based on metamorphic testing[J]. Journal on Communications, 2023, 44(10): 164-176.

[94] DENG W C, WEI H C, HUANG T, et al. Smart contract vulnerability detection based on deep learning and multimodal decision fusion[J]. Sensors, 2023, 23(16): 7246.

[95] ZHANG L J, CHEN W J, WANG W Z, et al. CBGRU: a detection method of smart contract vulnerability based on a hybrid model[J]. Sensors, 2022, 22(9): 3577.

[96] HE D J, WU R, LI X J, et al. Detection of vulnerabilities of blockchain smart contracts[J]. IEEE Internet of Things Journal, 2023, 10(14): 12178-12185.

[97] RAMEZAN G, LEUNG C. Analysis of proof-of-work-based blockchains under an adaptive double-spend attack[J]. IEEE Transactions on Industrial Informatics, 2020, 16(11): 7035-7045.

[98] ZHENG J, HUANG H W, ZHENG Z B, et al. Adaptive double-spending attacks on PoW-based blockchains[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(3): 1098-1110.

[99] 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.

[100] CHULERTTIYAWONG D, JAMALIPOUR A. Sybil attack detection in Internet of flying things-IoFT: a machine learning approach[J]. IEEE Internet of Things Journal, 2023, 10(14): 12854-12866.

[101] OTSUKI K, NAKAMURA R, SHUDO K. Impact of saving attacks on blockchain consensus[J]. IEEE Access, 2021, 9: 133011-133022.

[102] WANG Z J, LV Q Z, LU Z B, et al. ForkDec: accurate detection for selfish mining attacks[J]. Security and Communication Networks, 2021, 2021(1): 5959698.

[103] 刘会霞, 李玲玲. 基于区块链的共享充电桩安全监管方案[J]. 计算机应用研究, 2022, 39(5): 1319-1323, 1348.
LIU H X, LI L L. Security supervision scheme of shared charging pile based on blockchain[J]. Application Research of Computers, 2022, 39(5): 1319-1323, 1348.

[104] ZHANG Q, GAO J, QIN Q Q, et al. FutureOTC: an intelligent decentralized OTC option trading and E-contract signing system[C]// Blockchain Technology and Application. Berlin: Springer, 2020: 17-30.

[105] WANG X Q, ZHANG K, DING Y, et al. An illegal data supervision scheme for the consortium blockchain[C]//Blockchain Technology and Application. Berlin: Springer, 2022: 100-115.

[106] 张健毅, 王志强, 徐治理, 等. 基于区块链的可监管数字货币模型[J]. 计算机研究与发展, 2018, 55(10): 2219-2232.
ZHANG J Y, WANG Z Q, XU Z L, et al. A regulatable digital currency model based on blockchain[J]. Journal of Computer Research and Development, 2018, 55(10): 2219-2232.

[107] 霍鑫磊, 龙宇, 谷大武. 一种基于联盟链的兼具授权监管与隐私保护方案[J]. 小型微型计算机系统, 2023, 44(3): 589-595.
HUO X L, LONG Y, GU D W. Privacy protection and authorization supervision scheme based on consortium chain[J]. Journal of Chinese Computer Systems, 2023, 44(3): 589-595.

[108] YANG H T, XIONG S M, FRIMPONG S A, et al. A consortium blockchain-based agricultural machinery scheduling system[J]. Sensors, 2020, 20(9): 2643.

[109] LI X, WU L, ZHAO R, et al. Two-layer adaptive blockchain-based supervision model for off-site modular housing production[J]. Computers in Industry, 2021, 128: 103437.

[110] 赵泽宁. 区块链异常交易行为识别关键技术研究[D]. 天津: 天津理工大学, 2023.
ZHAO Z N. Research on key technologies of blockchain abnormal trading behavior identification[D]. Tianjin: Tianjin University of Technology, 2023.

[111] 瞿元. 比特币异常行为检测系统的研究与设计[D]. 成都: 电子科技大学, 2021.

QU Y. Research and design of Bitcoin abnormal behavior detection system[D]. Chengdu: University of Electronic Science and Technology of China, 2021.

[112] 周健, 张杰, 闫石. 基于链上数据的区块链欺诈账户检测研究[J]. 计算机应用研究, 2022, 39(4): 992-997.
ZHOU J, ZHANG J, YAN S. Research on blockchain fraud account detection based on data on chain[J]. Application Research of Computers, 2022, 39(4): 992-997.

[113] FARRUGIA S, ELLUL J, AZZOPARDI G. Detection of illicit accounts over the ethereum blockchain[J]. Expert Systems with Applications, 2020, 150: 113318.

[114] 梁飞, 卫兰, 林文成. 基于子空间图聚类检测以太坊恶意账户的方法[J]. 信息安全研究, 2023, 9(E1):68-71.
LIANG F, WEI L, LIN W C. A method for detecting malicious Ethereum accounts based on subspace graph clustering [J]. Journal of Information Security Research, 2023, 9(E1): 68-71.

[115] 梁飞, 马立, 翟宝宇, 等. 基于双曲空间图神经卷积网络检测以太坊恶意账户的技术[J]. 网信军民融合, 2022(9): 48-52.
LIANG F, MA L, ZHAI B Y, et al. Detection of malicious accounts in ethereum based on hyperbolic space graph neural convolution network[J]. Civil-Military Integration on Cyberspace, 2022(9): 48-52.

[116] 石拓, 梁飞, 尚钢川, 等. 基于时序交易图注意力神经网络的以太坊恶意账户检测[J]. 信息网络安全, 2022, 22(10): 69-75.
SHI T, LIANG F, SHANG G C, et al. Detection of malicious ethereum account based on time series transaction and graph attention neural network[J]. Netinfo Security, 2022, 22(10): 69-75.

[117] BIRYUKOV A, TIKHOMIROV S. Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash[J]. Pervasive and Mobile Computing, 2019, 59: 101030.

[118] 徐卫克. 预防区块链分叉的节点检测算法[J]. 电子技术与软件工程, 2020(3): 186-187.
XU W K. Node detection algorithm for preventing blockchain bifurcation[J]. Electronic Technology & Software Engineering, 2020(3): 186-187.

[119] 凯文•沃巴赫, 林少伟. 信任, 但需要验证: 论区块链为何需要法律[J]. 东方法学, 2018(4): 83-115.
WERBACH K, LIN S W. Trust, but verify: why the blockchain needs the law[J]. Oriental Law, 2018(4): 83-115.

[120] 孔浩东. 非同质化通证的法律性质研究[J]. 网络安全技术与应用, 2022(9): 141-143.
KONG H D. Study on the legal nature of non-homogeneous general certificate[J]. Network Security Technology & Application, 2022(9): 141-143.

[121] 高健博, 张家硕, 李青山, 等. RegLang: 一种面向监管的智能合约编程语言[J]. 计算机科学, 2022, 49(6): 462-468.
GAO J B, ZHANG J S, LI Q S, et al. RegLang: a smart contract programming language for regulation[J]. Computer Science, 2022, 49(6): 462-468.

[122] LU Q H, XU X W. Adaptable blockchain-based systems: a case study for product traceability[J]. IEEE Software, 2017, 34(6): 21-27.

[123] 毛湘科, 李超, 郝濛婷, 等. 一种全方位监管的区块链系统设计与实现[J]. 计算机与数字工程, 2023, 51(1): 81-85, 92.
MAO X K, LI C, HAO Y T, et al. A blockchain system design and implementation for all-round supervision[J]. Computer & Digital Engineering, 2023, 51(1): 81-85, 92.

[124] 张雅宁, 吴品才. 北京互联网法院“天平链”建设及启示: 兼论区块链技术对电子档案真实性维护的可行性[J]. 档案与建设, 2022(10): 63-65.
ZHANG Y N, WU P C. The construction of “balance chain” in Beijing Internet court and its enlightenment: also on the feasibility of blockchain technology to maintain the authenticity of electronic files[J]. Archives & Construction, 2022(10): 63-65.

[125] AMATO F, COZZOLINO G, MOSCATO F, et al. A model for verification and validation of law compliance of smart contracts in IoT environment[J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7752-7759.

[126] PARVIZIMOSAED A, SHARIFI S, AMYOT D, et al. Subcontracting, assignment, and substitution for legal contracts in symboleo[C]// Conceptual Modeling. Berlin: Springer, 2020: 271-285.

[127] MOLINA-JIMENEZ C, SFYRAKIS I, SOLAIMAN E, et al. Implementation of smart contracts using hybrid architectures with on and off-blockchain components[C]//Proceedings of the 2018 IEEE 8th International Symposium on Cloud and Service Computing (SC2). Piscataway: IEEE Press, 2018: 83-90.

[128] PARVIZIMOSAED A, BASHARI M, KIAN A R, et al. Compliance checking for transactive energy contracts using smart contracts[C]// Proceedings of the 2020 IEEE PES Transactive Energy Systems Conference (TESC). Piscataway: IEEE Press, 2020: 1-5.

[129] 经普杰, 王良民, 董学文, 等. 分层跨链结构: 一种面向区块链系统监管的可行架构[J]. 通信学报, 2023, 44(3): 93-104.
JING P J, WANG L M, DONG X W, et al. CHA: cross-chain based hierarchical architecture for practicable blockchain regulatory[J]. Journal on Communications, 2023, 44(3): 93-104.

[130] ZHANG Y Q, MA Z F, LUO S S, et al. DBSDS: a dual-blockchain security data sharing model with supervision and privacy-protection[J]. Concurrency and Computation: Practice and Experience, 2023, 35(21): e7706.

[131] 吴迪. 针对跨链体系的多场景攻击与防御方法研究[D]. 北京: 北京交通大学, 2022.
WU D. Research on multi-scenario attack and defense method for cross-chain system[D]. Beijing: Beijing Jiaotong University, 2022.

[132] BRINKMANN M, HEINE M. Can blockchain leverage for new public governance: a conceptual analysis on process level[C]//Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance. New York: ACM Press, 2019: 338-341.

[133] DURSUN T, ÜSTÜNDAĞ B B. A novel framework for policy based on-chain governance of blockchain networks[J]. Information Processing & Management, 2021, 58(4): 102556.

[134] DIROSE S, MANSOURI M. Comparison and analysis of governance mechanisms employed by blockchain-based distributed autonomous organizations[C]//Proceedings of the 2018 13th Annual Conference on System of Systems Engineering (SoSE). Piscataway: IEEE Press, 2018: 195-202.

[135] USHIDA R, ANGEL J. Regulatory considerations on centralized aspects of DeFi managed by DAOs[C]//Financial Cryptography and Data Security. Berlin: Springer, 2021: 21-36.

[136] MONCADA R, FERRO E, FAVENZA A, et al. Next generation blockchain-based financial services[C]//Euro-Par 2020: Parallel Pro-

cessing Workshops. Berlin: Springer, 2021: 30-41.
[137] MIYACHI K, MACKEY T K. hOCBS: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design[J]. Information Processing & Management, 2021, 58(3): 102535.
[138] BARATI M, RANA O. Tracking GDPR compliance in cloud-based service delivery[J]. IEEE Transactions on Services Computing, 2022, 15(3): 1498-1511.
[139] 杨东.“依法治链”与“以链治链”: 区块链技术监管的结合之道[R]. 2019.
YANG D. “Rule of law by chain” and “Chain-based governance”: the integration path of blockchain technology regulation [R]. 2019.
[140] 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 Press, 2022: 7-12.
[141] KALODNER H A, GOLDFEDER S, CHEN X Q, et al. Arbitrum: scalable, private smart contracts[C]//27th USENIX Security Symposium. Berkeley: USENIX Association, 2018: 1353-1370.
[142] GONÇALVES J P D B, VILLAÇA R D S. A new consensus mechanism for blockchained federated learning systems using optimistic rollups[C]//Proceedings of the 2024 IEEE International Conference on Blockchain. Piscataway: IEEE Press, 2024: 406-411.
[143] SOMPOLINSKY Y, WYBORSKI S, ZOHAR A. PHANTOM GHOSTDAG: a scalable generalization of nakamoto consensus: September 2, 2021[C]//Proceedings of the 3rd ACM Conference on Advances in Financial Technologies. New York: ACM Press, 2021: 57-70.
[144] SNEHLATA, SHUKLA P, SINGH A K, et al. An intelligent blockchain-oriented digital voting system using NEAR protocol[J]. SN Computer Science, 2023, 4(5): 643.

[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、可信计算等。

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、人工智能安全等。

白伊瑞（1999– ），女，山西临汾人，中国科学院信息工程研究所博士生，主要研究方向为区块链、可信数字身份、大模型安全等。

马琪舜（2000– ），男，河南周口人，海南大学硕士生，主要研究方向为区块链、去中心化金融安全等。

雷虹（1984– ），男，湖南澧县人，博士，海南大学教授、博士生导师，主要研究方向为网络空间安全、可信执行环境、区块链技术、智能传感器等。

孙鸿宇（1993– ），男，陕西渭南人，博士，海南大学讲师，主要研究方向为内核安全、人工智能安全、人工智能应用与安全等。

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/电子政务安全等。

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、硕士生导师，主要研究方向为区块链安全监管、物联网密码工程与应用等。