区块链系统安全防护技术研究进展

刘赦迪[1),2)] 杜学绘[1),2)] 王 娜[1),2)] 吴翔宇[1),2)] 单棣斌[1),2)] 乔 蕊[3)]

[1)](战略支援部队信息工程大学 郑州 450001)

[2)](河南省信息安全重点实验室 郑州 450001)

[3)](周口师范学院 河南 周口 466001)

摘 要 区块链是综合运用密码学、共识机制、分布式网络和智能合约等技术所构建的具有安全和可信特征的新型分布式计算范式,在社会、生产、生活等众多领域都得到了广泛应用,对人民生活产生了重大影响.然而,随着区块链技术及应用的蓬勃发展,各种安全问题频发,严重阻碍了区块链的应用和推广.同时,由于区块链技术、框架仍在不断演进之中,研究人员对区块链安全内涵的核心认知和关键特征理解还未统一,存在较大差异,尚未形成一致的区块链安全框架与体系.当前亟需对区块链系统安全技术发展现状进行梳理,为区块链系统所面临的重点安全问题的研究和突破提供参考.本文结合区块链系统技术框架、围绕区块链安全需求,构建了区块链安全技术框架.在此框架下,从区块链密码支撑技术、区块链平台安全技术和区块链风险评估与安全监管 3 个方面系统梳理区块链安全关键技术研究现状,囊括了区块链业务流程和区块链系统技术框架所涉及的主要安全机制.最后总结了区块链系统安全技术有待解决的核心问题和发展趋势.

关键词 区块链安全;安全技术框架;密码支撑;平台安全;安全监管

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2024.00608

Research Progress on Blockchain System Security Technology

LIU Ao-Di[1),2)] DU Xue-Hui[1),2)] WANG Na[1),2)] WU Xiang-Yu[1),2)] SHAN Di-Bin[1),2)] QIAO Rui[3)]

[1)](*Strategic Support Force Information Engineering University, Zhengzhou* 450001)

[2)](*He'nan Province Key Laboratory of Information Security, Zhengzhou* 450001)

[3)](*Zhoukou Normal University, Zhoukou, Henan* 466001)

Abstract Blockchain is a new distributed computing paradigm that integrates cryptography, consensus mechanism, distributed network and smart contract technologies with security and trust characteristics. It has been widely used in many fields such as society, production and life, and has a great impact on people's lives. However, with the vigorous development of blockchain technology and applications, various security problems have seriously hindered the application and promotion of blockchain. Different from traditional information systems, blockchain has distributed, decentralized, high value and other characteristics, but also brings the characteristics of a wide range of security protection and many risk links, which brings new challenges to the application of security technology in the blockchain scenario. Because the blockchain technology and framework are still evolving, researchers' core cognition and key feature understanding of the security connotation of blockchain have not been unified, and there are great differences. A

收稿日期:2023-03-29;在线发布日期:2024-01-03.本课题得到河南省重点研发与推广专项(222102210069)、中原科技创新领军人才项目(224200510003)、国家自然科学基金(62102449)、河南省高校科技创新人才支持计划(23HASTIT029)资助.**刘赦迪**,博士,讲师,主要研究领域为区块链安全.E-mail:ladyexue@163.com.**杜学绘**(通信作者),博士,教授,主要研究领域为网络与信息安全.E-mail:dxh37139@sina.com.**王 娜**,博士,教授,主要研究领域为网络与信息安全.**吴翔宇**,博士研究生,主要研究领域为区块链安全.**单棣斌**,博士,讲师,主要研究领域为网络与信息安全.**乔 蕊**,博士,副教授,主要研究领域为区块链安全.

consistent blockchain security framework and system has not yet been formed. At present, it is urgent to sort out the development status of the security technology of the blockchain system and provide reference for the research and breakthrough of the key security issues faced by the blockchain system. Based on the technical framework of the blockchain system and the security requirements of the blockchain, this paper constructs the technical framework of the blockchain security. Under this framework, the research status of key technologies of blockchain security is systematically reviewed from three aspects: blockchain cryptographic support technology, blockchain platform security technology, and blockchain risk assessment and security supervision, including the main security mechanisms involved in the blockchain business process and blockchain system technology framework. Blockchain cryptographic support technology is mainly to provide cryptographic technology services and call interfaces for blockchain system components, blockchain system users, and blockchain application services. Blockchain cryptographic support technology is the cornerstone of blockchain system security, which mainly solves the security function components in the operation process of the blockchain system and provides confidentiality, integrity, privacy, authentication, and non-repudiation protection for the relevant functional components of the security management operation. It includes the cryptographic algorithm, cryptographic protocol, and cryptographic infrastructure. In addition, in view of the great security threats and challenges brought by quantum computing to cryptography technology, it is also necessary to consider the use of post-quantum cryptography technology in the blockchain to resist quantum attacks. The blockchain platform security technology provides basic blockchain service support for all types of users of blockchain services and is responsible for the actual operation of blockchain system data storage, calculation, transmission, and access. Blockchain platform security technology is the core of blockchain security, which mainly includes five levels of security: storage security, network security, consensus security, application security, and common security services. The first four levels correspond to the data layer, network layer, consensus layer, and application layer of the blockchain basic framework, while common security services run through each layer, and different security services are taken according to different blockchain system types and security needs. Blockchain risk assessment and security supervision are important guarantees for blockchain security. It is mainly responsible for solving the blockchain system itself, blockchain application service security assessment, supervision, governance, norms. Specifically include security risk assessment, security supervision and governance, technical standards and norms. Finally, it summarizes the core problems and development trends of blockchain system security technology.

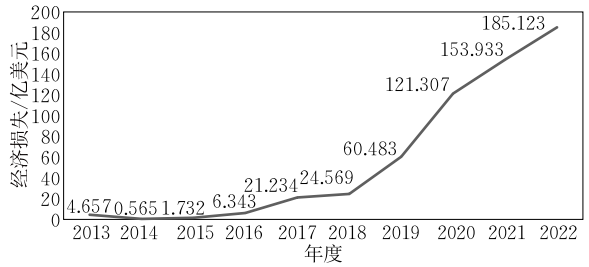
Keywords　blockchain security; security technology framework; cryptography support; platform security; security supervision

1　引　言

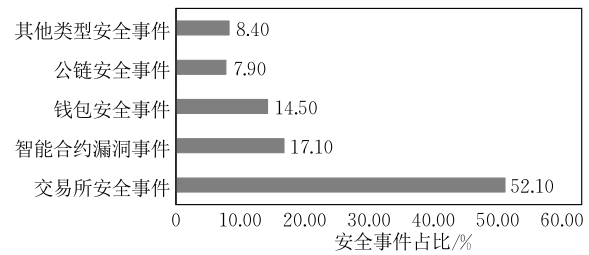
自“区块链”概念于 2008 年在中本聪发表的论文《Bitcoin: A peer-to-peer electronic cash system》中首次提出以来，区块链技术引起了学术界、产业界和各国政府的广泛关注[1]，延伸到数字金融、政务管理、智能制造、物联网、供应链管理等众多领域. 2020 年，Gartner 将实用型区块链列入十大战略科技技术. 全球主要国家也纷纷布局区块链技术产业. 习近平总书记在中央政治局第十八次集体学习时强调“区块链技术的集成应用在新的技术革新和产业变革中起着重要作用”，要求“把区块链作为核心技术自主创新重要突破口加快推动区块链技术和产业创新发展”. 同年，国家发展和改革委员会首次将区块链纳入我国新型基础设施的信息基础设施，更是将区块链行业推动进入了快速发展的新阶段. 2021 年，在《十四五规划纲要》[2]中，首次将区块链纳入国

家五年规划，在“加快数字发展，建设数字中国”篇章中，区块链被列为“十四五”期间七大数字经济重点产业之一，充分体现了党中央、国务院对区块链技术及相关产业发展的高度重视. 同年，工业和信息化部与中央网信办联合发布的《关于加快推动区块链技术应用和产业发展的指导意见》指出“区块链成为建设制造强国和网络强国，发展数字经济，实现国家治理体系和治理能力现代化的重要支撑”.

但区块链在给社会生产、生活方式带来变革同时，安全问题也日益凸显，各类安全事件频发. 2020 年 5 月，意大利交易所 Altsbit 遭受攻击，由于损失巨大导致该交易所于 5 月 8 日宣布关闭；2021 年 7 月，开源比特币支付网络 Bitcoin.org 遭到大规模 DDoS 攻击，无法正常提供服务；同年 8 月，跨链协议 Poly Network 由于函数漏洞遭到网络攻击，带来数亿美元损失；2021 年 10 月，去中心化区块链借贷协议 Compound 试图通过社区提案修补流动性挖矿代币分发合约漏洞时，由于 drip() 函数调用向漏洞合约打入 20 万枚 comp 代币，导致 1.58 亿美元损失风险；同月，以太坊平台 DeFi 协议 Cream Finance 遭受攻击，损失达 1.3 亿美元；2022 年 3 月，Axie Infinity 侧链项目 Ronin Network 受黑客攻击，17.36 万枚 ETH 和 2550 万枚 USDC 被盗，损失达 6.1 亿美元. 上述安全事件表明，加快区块链系统安全支撑技术研究，已成为保障区块链建设和数字经济稳步向前推进的迫切要求. 图 1 展示了近年来公开的区块链安全事件和不同类型安全事件所占比重，从中可以看出区块链安全事件所带来的经济损失巨大、增长显著且攻击类型多样.



(a) 不同年度安全事件损失



(b) 近三年各类安全事件占比

图 1 区块链安全事件统计

不同于传统信息系统，区块链具有分布式、去中心化、高价值等特性，也带来安防范围广、风险环节多的特点，这为安全技术在区块链场景应用带来了新的挑战. 同时，为实现区块链系统的有效运行，还引入了分布式的计算与存储框架. 这些新框架也带来了新的安全威胁. 当前，区块链安全研究仍处于初期，研究人员对区块链安全的核心认知和关键特征还存在差异，理论成果同实际应用要求之间还存在差距，亟待对区块链系统安全技术的发展现状进行系统梳理，为区块链安全重点问题的研究和突破提供参考.

目前国内外在区块链安全细分方向上有一些比较深入的综述，如区块链身份管理、区块链共识机制、区块链数据隐私保护等，但还缺少从区块链系统安全防护视角对区块链系统所涉及的安全防护技术的体系化系统综述研究. 本文结合区块链业务流程和区块链系统技术框架，分析区块链安全关键技术研究进展，在此基础上总结了区块链安全中有待解决的挑战问题和解决思路，探讨了区块链安全的发展趋势. 第 2 节在对区块链安全技术主流分类视角和主要内容总结的基础上，提出一种区块链安全技术框架；在该框架下，第 3 节从密码技术与应用视角梳理了区块链系统中涉及的密码支撑技术；第 4 节则从区块链系统应用支撑视角梳理了区块链平台安全技术；第 5 节综合安全风险评估、安全监管与治理、技术标准与规范 3 个方面梳理了区块链风险评估与安全监管技术；第 6 节分析了区块链安全面临的风险挑战与未来发展趋势；第 7 节对全文进行总结.

2 区块链安全技术框架

建立有效的区块链安全技术框架，能够为区块链系统安全技术研究与部署提供指导. 本节首先对当前有代表性的区块链安全技术分类视角和技术内容进行介绍，在此基础上，提出一种区块链安全技术框架.

2.1 区块链安全技术的分类视角

对区块链所涵盖的安全技术进行合理、系统的分类与组织，是区块链安全技术框架构建的前提与基础. 当前具有代表性的分类视角[3-9]主要包括基于区块链系统技术架构的分类和基于区块链安全风险的分类.

基于区块链系统技术架构的分类方式指按照区块链所涉及不同技术、组件层面进行分类. 例如为了将现有安全体系结构与区块链技术架构相结合，

Leng 等人[3]从信息系统不同层面入手，将 IBM 和 Oracle 安全参考结构映射到区块链技术体系，提出 PDI 框架(Process Data Infrastructure model)，将区块链安全分流程级、数据级以及基础设施级三个层面进行组织构建. 其中，基础设施级安全包括终端设备、网络和节点服务器；流程级安全包括智能合约、实现安全、操作标准和欺诈检测；数据级安全由认证、加密、一致算法、访问控制和密钥管理组成. Homoliak 等人[4]提出一种区块链的安全参考体系结构 SRA，该结构采用类似于 ISO/OSI 的堆叠模型，描述区块链安全和隐私方面性质和层次结构，包含网络层、共识层、复制状态机层以及应用层. Zhang 等人[5]提出一种基于堆栈的模型，该模型由六层组成，分别代表应用、合约、激励、共识、网络和数据层. 基于区块链系统技术架构的分类方式与区块链业务处理流程耦合比较紧密，对建立区块链安全框架具有一定指导意义，但考虑到在区块链应用构建过程中，一些安全技术并非针对特定组件或特定层设计，可能涉及多个系统位置与运行环节，建立区块链安全技术框架并不能完全按照系统组件的方式进行，并且这种方式主要关注系统自身的安全机制，缺乏对区块链系统共性安全、安全监管和内容治理层面的考虑，而这些方面也应是区块链安全的重要组成部分.

基于区块链安全风险的分类方式指按照区块链在不同阶段面临的安全风险或漏洞威胁来进行分类. 例如梅秋丽等人[6]从区块链应用的非技术风险和技术风险两方面角度入手，按数据保护机制、隐私保护机制、密钥管理机制、权限管理机制进行划分. 其中，技术风险主要包括通信网络风险、数据安全风险、密码安全风险、共识机制风险、应用组件风险、用户安全风险等，非技术风险主要包括监管风险、金融风险、法律风险与道德风险等. Saad 等人[7]从攻击面角度入手，按区块链密码结构、分布式体系结构、区块链应用程序上下文三个层面的安全威胁角度分析面向自私挖掘、51%攻击、域名攻击、智能合约攻击、分布式拒绝服务攻击、共识延迟、区块链分叉、孤立和失效块、块吸收、钱包盗窃等攻击场景下应采取的安全防护手段，以减轻攻击和漏洞影响. Chen 等人[8]从漏洞、攻击和防御角度入手，对以太坊系统安全进行分类. Li 等人[9]通过对区块链系统安全风险和真实攻击事件进行分析，提炼出区块链系统安全增强技术. 但基于区块链安全风险的分类方式更像是一种补救式安全技术，难以从系统、体系构建与设计的层面对区块链系统进行全面安全防护与覆盖.

此外，文献[10-14]等区块链系统安全综述性文献对区块链系统安全所需关注的挑战性问题进行了阐述，但没有提出明确的安全技术分类，这些文献在学术研究上具有重要借鉴意义，但在区块链技术框架的构建上指导性较弱. 综上所述，虽然，基于区块链系统技术架构的分类和基于区块链安全风险的分类各有优点，但也存在一定局限性. 第 2.2 节将综合运用这两种安全技术的组织方式，并结合区块链技术参考架构，提出区块链安全技术框架.

2.2　技术框架

2018 年，NIST[15]提出区块链技术概述(NISTIR 8202)，分别从区块链类别、区块链组件、共识模型、分类等技术维度阐述了区块链技术的概念与内涵. 同年，中国电子技术标准化研究院牵头提出区块链和分布式记账技术参考架构，从用户视图和功能视图两个方面对参考架构进行描述，将区块链系统的参与者划分为区块链服务客户、区块链服务提供方以及区块链服务合作方 3 种角色. 其中，区块链服务客户包括服务用户、服务管理者、服务集成者等；区块链服务提供方包括服务运营管理者、服务部署管理者、服务安全和风险管理者等；区块链服务合作方包括服务监管方、服务审计方、服务开发方等. 功能视图涵盖开发、运营、安全、监管和审计四个跨层的功能体系. 因此，本文结合区块链业务流程和区块链系统技术框架组成特点，兼顾存储安全、网络安全、共识安全、应用安全、风险评估与安全监管，提出符合区块链业务特点的安全技术框架，如图 2 所示.

国内金融标准化技术委员会制定了《金融分布式账本技术安全规范》，构建了涵盖基础硬件、基础软件、密码算法、节点通信、账本数据等要素组成的金融分布式账本技术安全体系，该体系倾向于指导金融机构按照合适的安全要求进行区块链系统的部署和维护. 密码行业标准化技术委员会制定的《区块链密码应用技术要求》中提出了基于密码技术支撑环境的密码应用技术架构，描述的主要是区块链各技术层与密码技术的对应关系. 信息安全标准化技术委员会正在制定的《信息安全技术区块链技术安全框架》则侧重于从层次结构与区块链参与角色的安全视角指导基于区块链技术的信息系统进行安全风险防范. 与以上安全技术框架所不同，本文框架将区块链安全技术划分为区块链密码支撑技术、区块

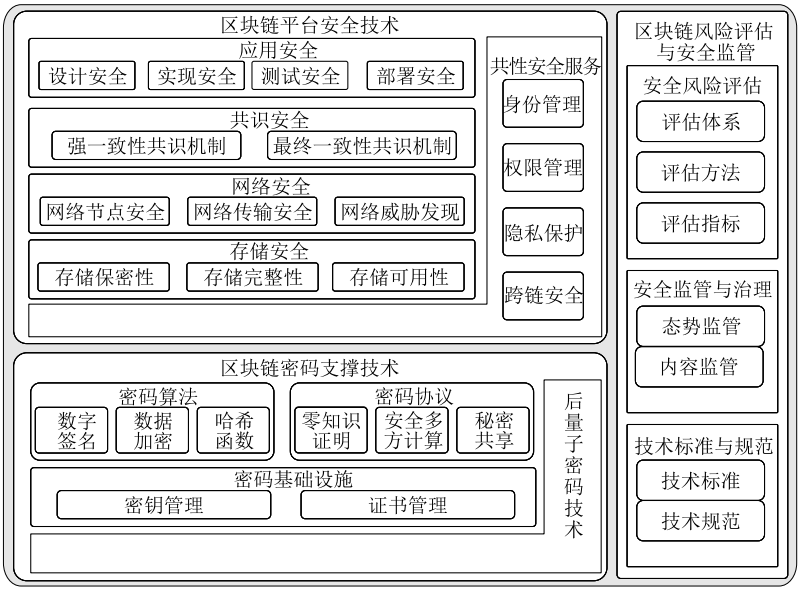


图 2 区块链安全技术框架

链平台安全技术和区块链风险评估与安全监管 3 部分,将框架聚焦于区块链系统各层面所面临的主要安全问题,结合区块链系统技术框架、围绕区块链安全需求,包含一些还未成熟的新兴安全技术,构建的一种区块链安全技术的研究框架,未对区块链系统部署过程的软硬件环境进行过多考虑.在对区块链安全技术进行比较系统学术归纳的同时,更重要的是考虑了区块链安全技术与区块链系统框架间的契合.该框架将区块链安全技术与区块链系统的主要组成部分进行了对应,使得区块链安全需求更加明确,安全技术的服务对象也更加清晰,便于指导区块链安全技术的研究与部署.

区块链密码支撑技术主要是面向区块链系统组件、区块链系统用户、区块链应用服务提供密码技术服务和调用接口.区块链密码支撑技术是区块链系统安全的基石,主要解决区块链系统运行过程中的安全功能组件以及安全管理运行的相关功能组件提供机密性、完整性、隐私性、可认证性和不可否认性保护,具体包括密码算法、密码协议以及密码基础设施.另外,针对量子计算对密码技术带来的极大安全威胁与挑战,还需要在区块链中考虑采用后量子密码技术来抵抗量子攻击.

区块链平台为区块链服务各类用户提供基础区块链的服务支撑,负责区块链系统数据存储、计算、传输、访问等实际运行.区块链平台安全技术是区块链安全的核心,主要包含区块链系统的存储安全、网络安全、共识安全、应用安全、共性安全服务 5 个层面的安全范畴,前 4 个层面分别与区块链基础框架的数据层、网络层、共识层、应用层相对应,而共性安全服务则贯穿于各层,会根据不同区块链系统类型和安全需求采取不同安全服务.

区块链风险评估与安全监管是区块链安全的重要保证,主要负责解决区块链系统自身、区块链应用服务安全评估、监管、治理、规范等一系列问题,具体包括安全风险评估、安全监管与治理、技术标准与规范.

3 区块链密码支撑技术

密码技术在区块链系统中扮演着重要角色,不仅与区块链安全性和效率密切相关,也与区块链实际应用密切相关,是其安全、稳定运行最基础、最核心的安全保障手段[16].从密码技术视角看,多类型密码技术都已在各类区块链平台和服务得到应用.由于密码技术概念广泛、内涵丰富.本节主要介绍区块链密码支撑技术涉及的 4 个方面:密码算法、密码协议、密码基础设施和后量子密码技术.

3.1 密码算法

本节归类区块链系统中常用的密码算法,分析不同算法的特性及应用场景,给出客观评估.

3.1.1 数字签名算法

数字签名算法是基于公钥技术的密码算法,如图 3 所示,区块链中用户使用私钥对交易数据进行数字签名,再由其他区块链节点使用验签算法对交

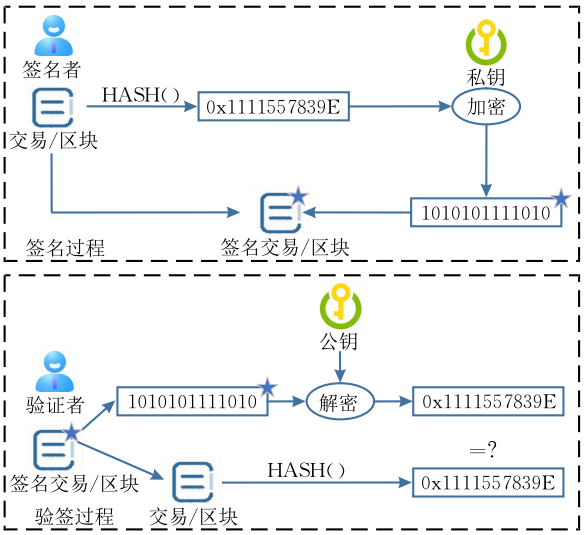


图 3　区块链数字签名与验签

易数据进行验证，防止交易数据篡改和伪造，为区块链提供完整性、可认证性和不可否认性保护. 区块链使用数字签名主要有两方面作用，一是证明消息确实是由数据发送方签名发送，二是用来确定传递消息完整性. 区块链通过不同签名方案能提供不同算法特性，如隐私保护、身份匿名和不可链接性等，所用签名算法包括多重签名、盲签名、环签名、门限签名等.

(1) 多重签名

区块链使用单签名方案时，往往更容易受到攻击，因此存在多重签名安全需求，即一笔交易需要多个私钥签名才能被执行. 当交易需要由来自一组多个参与方签名时，通常采用多重签名算法. 比特币分别利用 CHECKMULTISIG 和 P2SH 机制实现多重签名，CHECKMULTISIG 利用一条语句就能完成多签验证过程，但需要付款人(输出脚本)提供所有收款人公钥. P2SH 只需要向付款人提供一个地址，付款人往该地址支付即可，该地址是收款人 Redeem Script 哈希. 当收款人花费这笔钱时，提供相应 Redeem Script 与收款人数字签名. 若 Redeem Script 执行后，栈顶结果为 TRUE，则表示付款验证通过. Openchain 与 Multichain[17] 均采用 M-of-N 多重签名算法，即使在 $M-1$ 份密钥泄露条件下，依然能够确保区块链资产安全. Maxwell 等人[18] 提出一种基于 Schnorr 的签名方案提高比特币性能和隐私保护能力，支持密码聚合，并在离散对数假设和普通公钥模型下证明其安全性. 针对多重签名存在的性能问题，Boneh 等人[19] 设计短可追责子组多重签名方案，支持签名压缩和公钥聚合，以此来压缩比特币区块链交易数据规模. Han 等人[20] 设计支持多签名为单签名的区块链钱包，采用阈值椭圆曲线数字签名算法实现较高验签性能，并使用布隆过滤器提高交易数据存储效率，确保在暴露参与者信息情况下识别交易参与者. Kansal 等人[21] 采用基于格的多重签名方案来降低区块链通信和存储成本，并在随机预言模型的环短整数解问题上证明是安全的. 综上可知，多重签名具有增加交易安全性、分散信任与控制、支持灵活的多签名控制方案等优势，但也存在增加区块交易时间和复杂度，需要确保多个参与方私钥充分保护管理等方面局限性.

(2) 盲签名

盲签名指消息签名者与发送者是不同实体，签名者对所签署消息是不可见的. 即盲签名实现了签名者对发送者消息进行签名，却不能知道签名消息具体内容. 相当于将文件放入信封，签名者在信封上对文件签名，而不知道文件具体内容. 根据功能不同，盲签名可分为完全盲签名、限制盲签名、公平盲签名、部分盲签名及群盲签名. 盲签名应用于区块链系统，能够提供交易不可链接性和匿名性支持. Valenta 等人[22] 修改比特币混币协议 Mixcoin，利用盲签名保证任何用户输入与输出地址映射对混币服务器匿名不可见. 其中盲签名保护对象是混币用户发送给混币服务器的输出地址，实现保护输入地址和输出地址转移关系目的. Green 等人[23] 利用盲签名构建匿名支付渠道，可在无可信第三方和中心化机制的情况下，大幅减少链上交易的存储空间. Heilman 等人[24] 利用盲签名解决比特币链上链下协同交易过程所面临不信任问题，保证比特币与凭证交易过程匿名性与公平性. 张学旺等人[25] 利用公平盲签名具有的有条件匿名特征，引入可信第三方保管参与方盲因子与用户信息，实现联盟链场景对恶意用户行为的追溯. 但方案存在中心化程度高、安全性较差缺陷，还需配合其他加密方案实现安全增强. 乔康等人[26] 利用椭圆曲线算法构造盲签名替代基于双线性对与 RSA 盲签名算法，结合审计区块链记录混币器行为，实现溯源问责. Fabric2.0 引入 Idemix 方案[27]，签发者利用支持多消息盲签名签发包含用户属性的匿名凭证，用户能够通过零知识证明向验证方选择性地出示与证明其拥有属性的凭证，并保持不向观察者泄漏任何相关信息，实现用户身份匿名性和不可链接性. 综上所述，盲签名能够在保护用户数据隐私同时保证交易的可靠性，但也存在由于无法确认签名的出处和真实性问题，从而对

区块链交易的验证追溯监管机制带来挑战.

(3)环签名

环签名是一种用于解决匿名泄露秘密场景的签名技术.环签名中签名者先通过混淆机制将自身公钥与其它用户公钥构成匿名集合,再对消息签名,也可由集合内成员代表集合创建消息签名.对观察者来说,没有有效手段能够区分签名者来自于匿名集合中具体的用户公钥,也就无法确定签名真实签名者.环签名不同于一般群签名,环签名在构造匿名集合过程无需可信中心和管理者.在区块链网络中,可通过采用环签名实现对签名方的匿名保护.Meiklejohn 等人[28]提出一种以太坊混币服务,利用环签名保护用户身份,实现地址混淆,能够抵抗拒绝服务攻击.门罗币早期使用具有可链接性的环签名算法[29],具有自主混淆能力,能够通过环中由同一签名者生成的两个消息签名来确定这两个消息是由同一签名人产生的.为解决早期门罗币存在利用待定金额可实现身份追踪和匿名集合过小带来的隐私问题[30],后续提出多层环签名方案[31-32],实现密态交易金额成组混淆和确权验证,弥补原方案性能不足,提供更高运算效率与更短环签名长度.针对环签名功能和安全性存在的不足问题,Malavolta 等人[33]提出无随机 oracles 环签名的改进方法.FISCO BCOS 也提供了强匿名性环签名方案用于用户身份隐私保护,但未给出与资产确权、交易流程结合的具体实现方案.孙海锋等人[34]利用环签名算法的强匿名性构造共识节点排序选主算法,提升共识机制的抗自适应攻击能力.综上所述,通过利用环签名机制,参与者能在不泄漏身份的情况下进行交易,保护身份隐私.但是,由于交易过程会允许环内任何人进行签署,存在恶意使用风险且难以监管、调查的问题,需要配套机制进行解决.

(4)门限签名

门限签名[35]是门限秘密共享技术和数字签名技术的结合,由门限值数量约束参与方合作,任意少于门限数量的参与方无法进行签名合谋攻击.如(t,n)门限签名方案中,n 个参与方接收创建签名的共享密钥,需至少 t 个参与方创建消息签名.根据实现方法不同包括基于 RSA 的门限签名、基于 ECDSA 的门限签名、基于 Schnorr 的门限签名及基于 BLS 的门限签名.区块链中门限签名可用于为区块链提供匿名性、增强共识安全性、密钥安全保护及可信预言机选择等领域.Ziegeldorf 等人[36]利用门限签名实现去中心化比特币混币服务 CoinParty,增强了对签名可否认性支持.Dikshit 等人[37]使用基于 ECDSA 的门限签名,用于提供共享控制比特币钱包的安全策略.而基于 ECDSA 的门限签名算法具有较高算法复杂度,一些门限签名围绕 EdDSA 算法展开研究[38-39],如 Libra 项目在生成新账户地址时应用 EdDSA 算法.另外,张文芳等人[40]提出基于门限签名的改进拜占庭容错共识算法,在实现隐私数据隔离保护的同时,提高区块链高并发交易性能.Jian 等人[41]利用 ECDSA 门限签名实现对区块链钱包的安全保护,避免钱包单点故障问题.Soltani 等人[42]利用基于 Schnorr 的门限签名实现去中心化密钥恢复解决方案.唐张颖等人[43]设计基于国密算法 SM2 的门限签名方案,实现钱包私钥的保护.综上所述,门限签名能够提高区块链安全性、防止单点故障的同时,也更好地保护了用户隐私.但需要更多的计算资源和时间来创建签名、增加管理难度.

表 1 对比分析了不同的数字签名算法的应用场景、优势、存在问题,不同算法适用于不同的应用场景和监管要求,需根据应用场景进行适当选择和限制.

表 1 不同数字签名算法

签名算法	应用场景	优 势	存在问题
多重签名	完成交易需要多个私钥共同签名	增加交易安全性、分散信任与控制、支持灵活的多签名控制方案	增加交易时间和复杂度,需确保多参与方私钥充分保护管理
盲签名	在不暴露用户数据的情况下签署交易	保护用户数据隐私的同时能够保证交易的可靠性	由于无法确认签名的出处和真实性对区块链验证机制构成挑战
环签名	不暴露真实签名者实现匿名交易	参与者能在不泄漏身份的情况下进行交易,保护身份隐私	允许环内任何人签署,存在恶意使用风险且难以监管、调查问题
门限签名	利用多个私钥创建一个签名	提高了安全性、防止单点故障的同时,也更好地保护了用户隐私	需要更多的计算资源和时间来创建签名、增加管理难度

3.1.2 数据加密算法

针对不同场景区块链数据加密需求,需利用不同加密原语实现多功能加密支撑,这里主要介绍同态加密、属性加密与可搜索加密三种加密原语.

(1)同态加密

传统加密技术在将数据进行加密的同时,也影响了数据的可用性.如图 4 所示,同态加密[44]支持在不进行数据解密条件下对密文进行计算.解密后,该计算对明文仍然有效.该情况下,用户可以充分利用区块链的鲁棒计算和存储能力,而无需担心隐私

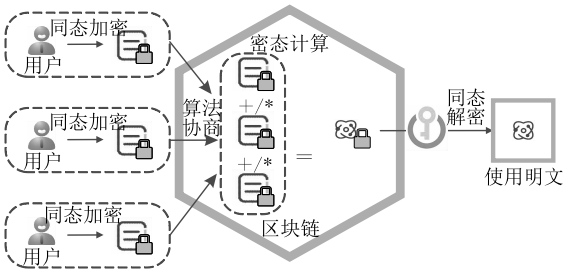


图 4　区块链同态加密模型

泄露，兼顾了区块链的安全性与可用性. 当这一概念与区块链技术结合后，同态加密特性为区块链带来高度安全的新型计算策略.

研究人员将具有加法同态特性或乘法同态特性的 Pedersen、ElGamal 等承诺用于私密数据的保存，并借助发布相应数据哈希值的方式来对其真实性进行承诺[45]. 利用同态加密能够避免在区块链中直接发布数据信息带来的敏感数据泄露风险，实现区块链隐私计算. 如 Kosba 等人[46]提出去中心化智能合约系统 Hawk，利用同态加密实现密态数据运算和智能合约隐私数据保护. Poelstra 等人[47]使用同态加密实现区块链交易信息隐私保护. 针对同态加密易受 IND-CC2 攻击问题，Mattila 等人[48]在区块链中引入两层身份验证机制实现隐私钱包计算保护. 针对以太坊智能合约隐私问题，Bünz 等人[49]提出隐私保护支付机制 Zether，实现账户余额加密保护. 但该机制对加法同态加密的依赖将其功能限制在私有货币转移和有限类私有智能合约，具有较大计算成本. 针对物联网设备的计算资源受限问题，Song 等人[50]将多项式乘法和模幂两种安全外包方案集成到隐理想格的全同态加密中，实现全同态加密外包方案，一定程度上降低终端设备计算负担. Liang 等人[51]结合区块链基于 Paillier 的同态密码系统，实现对电路版权的交易保护. Yaji 等人[52]将 Goldwasser Micali 和 Paillier 加密方案进行对比研究，探索了同态加密在区块链人工智能的应用潜力. Chen 等人[53]将基于格的全同态加密嵌入到以太坊区块链，以构建具有安全和隐私保护能力的可信框架. 还有一些研究[54-55]围绕如何利用同态加密实现分布式数据安全聚合展开研究，但总体来说目前同态加密性能较低，一定程度制约了其在区块链领域的应用. 另外，同态加密仅能解决密文计算隐私问题，私钥并不上链公开，仅依靠同态加密无法在区块链系统上实现公开可验证，还需要与安全多方计算、零知识证明等技术结合使用.

(2) 属性加密

属性加密通过将密文、密钥与属性、策略建立关联，确保不满足访问策略用户无法解密密文，分为基于密钥策略的属性加密(Key Policy Attribute Based Encryption，KP-ABE)与基于密文策略的属性加密(Ciphertext Policy Attribute Based Encryption，CP-ABE). KP-ABE 建立密钥与访问策略、密文与属性集关联. 当密文对应属性集合满足密钥中访问策略时，可成功解密. CP-ABE 建立的则是密文与访问策略、密钥与属性集关联. 当密钥对应属性集满足密文访问策略时，可成功解密. 因此，CP-ABE 将密文与访问策略相对应方式，一般与对称加密结合构造混合加密模式，更适用区块链中数据机密性保护，达到用户按权解密效果，典型的区块链属性加密模型如图 5 所示.

Rahulamathavan 等人[56]在区块链引入去中心化 ABE 方案实现对物联网数据保护，利用多个属性中心为不同矿工和用户颁发属性证书，以有效避免单点故障发生. Wang 等人[57]将 ABE 与基于身份加密 IBE 结合，提高区块链对用户身份和属性的管理能力. Ma 等人[58]提出基于属性的加密算法解决车辆传感器收集数据安全性问题，该算法使用路边单元(RSU)维护区块链. 属性加密将权限管理与加密技术结合，具有灵活度高、扩展性强的特点. 但由于属性加密涉及大量双线性映射计算，故具有较大计算开销. 同时，由于密文长度会随着属性规模增长而动态增加，存在占用存储空间过多问题. 故在计算和存储开销上的优化，也是属性加密在区块链应用的研究重点. 另外，与云计算场景的属性加密不同，区块链系统分布式特性更强，对属性证书的颁发和撤销等流程具有较强分布式管理需求，现有中心的 ABE 方案管理简单，不需要构建复杂信任关系，但对中心可信度要求过高，与区块链分布式需求存在一定冲突，而现有分布式无中心 ABE 研究又存在用户身份在全网公开而带来的隐私泄露风险，需要在安全性与可用性间取得平衡.

(3) 可搜索加密

可搜索加密是一种支持用户无需解密直接在密文状态下进行数据检索的加密技术，满足用户搜索服务的同时，保护其数据的安全和隐私. 如图 6 所示，通过采用区块链支持的可搜索加密将服务器上执行的计算交付到分散透明区块链系统，消除恶意服务器入侵的潜在威胁，增加数据安全性. Feng 等

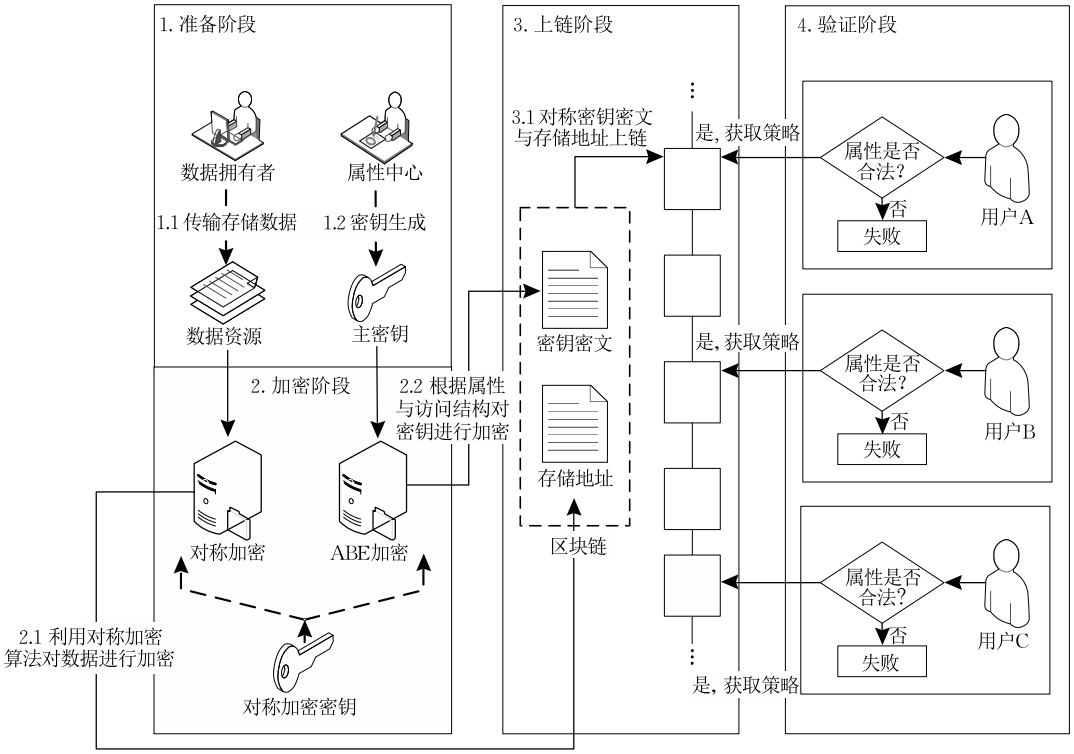


图 5 区块链属性加密模型

人[59]利用可搜索加密快速检索和监督区块链上存储的加密交易信息. Sun 等人[60]利用可搜索加密保证物流区块链上信息安全. 针对可搜索加密面临的公平性问题,Hu 等人[61]利用智能合约监督可搜索加密过程,设计一种对称可搜索加密方案. Li 等人[62]将区块链与可搜索加密结合,构造公平可搜索加密方案. Cai 等人[63]利用智能合约在区块链上记录加密搜索日志,并设计纠纷处理协议,保留加密搜索能力同时,保证服务可靠性. 针对区块链可搜索加密搜索能力提升研究方面,Chen 等人[64]利用布尔表达式在区块链构建搜索索引,具备复杂查询能力. Zhang 等人[65]提出一种联盟链场景下基于多关键字的外包加密数据排序检索方案来实现多云场景下可搜索加密. 针对现有方案在多用户场景效率较低、成本较高问题,Han 等人[66]提出一种支持细粒度访问控制和灵活搜索加密的改进方案,将属性加密与可搜索加密结合,依靠密钥管理服务器进行搜索验证,支持数据拥有者在建立索引后自由脱机,有效降低存储开销. 但目前在区块链可搜索加密研究方面,难以兼顾效率、功能性与安全性.

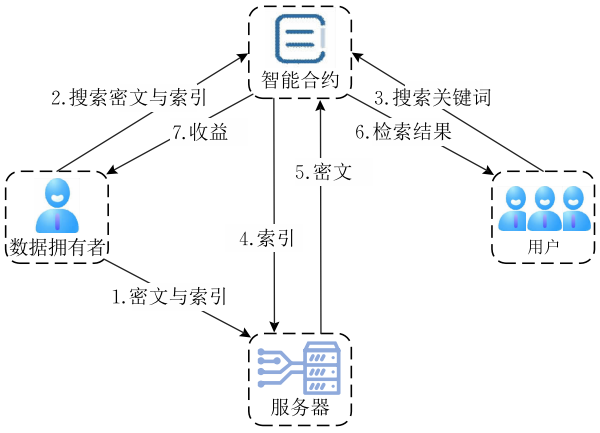


图 6 区块链可搜索加密模型

如表 2 所示,分别对比了三种加密算法的应用场景、优势以及存在问题,三种加密原语可分别应用于链上密文计算、链上密文访问控制以及链上密文检索等场景. 同态加密、属性加密、可搜索加密等加

表 2 不同数据加密算法

方案	应用场景	优 势	存在问题
同态加密	链上数据密文计算	将交易加密和计算操作分离,来保护数据隐私,节省链上数据协同资源和成本	同态加密计算速度较慢,还存在不可知攻击、侧信道攻击等安全隐患,不支持公开可验证
属性加密	链上数据访问控制	只有满足数据密文访问策略用户才能解密获得明文,支持链上数据细粒度可控共享	增加了一定的计算和存储成本,分布式环境下属性证书颁发和撤销难管理,且不支持公开可验证
可搜索加密	链上数据密文检索	支持用户在不泄露明文数据情况下进行数据查询,有选择地从区块链中检索所需要的数据	需要更高的计算和存储代价,对于大数据集的查询效率有所下降,查询方式较为单一,存在关键词猜测攻击风险

密技术的应用能够显著增强区块链系统数据的保密性，但与传统云计算场景下应用上述密码技术不同，区块链系统强调数据的公开可验证，而上述密码技术势必会影响区块链系统数据的可验证性，这就需要控制好数据加密的范围，并利用元数据对密态数据进行描述，能够设计可监管、可验证的新型密钥管理模式解决，满足区块链对数据可验证要求，才能更有力地支撑区块链密态数据管理.

3.1.3　哈希算法

哈希算法能将任意长度输入数据映射为固定长度输出数据. 哈希函数作为区块链数据结构支撑部分，对保证区块链可用性和安全性非常重要. 一些研究围绕区块链哈希算法安全问题，从哈希函数具有的隐藏性和谜题友好性出发，与传统哈希函数安全准则对比，认为对于哈希函数打破隐藏性和谜题友好性比打破原像阻力更难，这表明哈希函数被证明是原像阻力或经密码分析测试，往往足以用于区块链设计. 针对物联网区块链应用场景，Ferreira 等人[67]围绕资源受限的物联网设备对不同类型的哈希算法(MD5、SHA1、SHA224、SHA256、SHA384、SHA512)在平均区块大小、区块验证成功前哈希计算次数以及验证链上 10 个区块所需时间等方面性能进行对比测试，给出指导意见. 区块链不可篡改性在应用过程中为数据安全性带来有力支撑. 但随着区块链技术不断应用，一些研究人员认为区块链不可篡改性在一定程度限制了区块链推广. 由于区块链具有不可篡改性，也导致区块链已发布的问题数据与存在安全漏洞的智能合约无法被编辑. 一些研究提出可编辑区块链概念，利用变色龙哈希函数企图兼顾区块链可编辑和可跟踪能力. Jia 等人[68]提出去中心化变色龙哈希函数，构建可编辑区块链结构，其中密钥由多个区块链节点协同生成，不需任何可信方，结合节点具有的动态性，对变色龙哈希函数进行扩展，以支持阈值编校和主动更新. 当区块链中足够节点批准对链上数据编辑行为时，能够对链上的数据进行修改. 另外，MiMC[69-70]、Poseidon[71]等对零知识证明友好的哈希算法也被应用于区块链领域，可用于实现高效的零知识证明方案，能够显著降低证明生成和验证的计算复杂度. 目前区块链领域哈希函数的研究主要聚焦于提高计算效率、优化存储容量、加强安全性、提高可扩展性等方面的改进与提升，以满足区块链功能性能的不断发展和应用需求.

3.2　密码协议

区块链并非使用单一密码协议，而是将多种协议协同使用，包括零知识证明、安全多方计算、秘密共享协议等.

3.2.1　零知识证明

零知识证明作为一种高级加密原语被用于增加区块链系统的匿名性与隐私性. 零知识证明是证明者向验证者证明其知晓某秘密而又不泄露任何秘密信息的方法，证明过程需满足正确性、完备性和零知识性，是证明者和验证者两方或多方的密码交互协议. 如图 7 所示，根据交互方式不同，分为交互式零知识证明和非交互式零知识证明. 交互式零知识证明指证明者和验证者通过多次交互完成证明. 非交互式零知识证明指证明者和验证者单次交互达到零知识证明效果. 非交互式零知识证明使用门槛低，故区块链大多使用非交互式零知识证明实现身份隐私保护、资产权属标识、权属转移证明，无需透露资产信息.

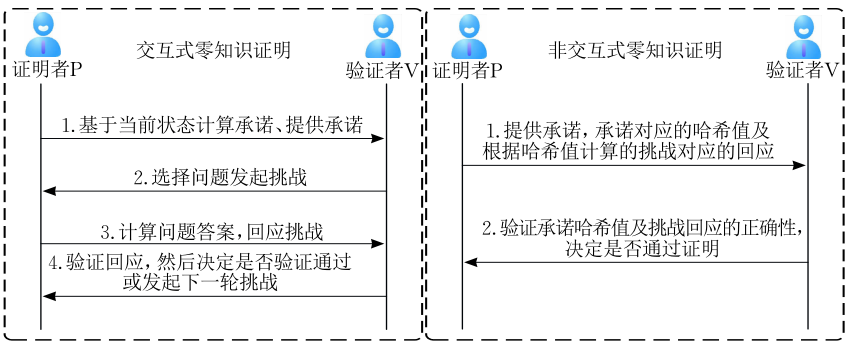


图 7　零知识证明协议

Zerocoin[72]和 Zerocash[73]使用零知识证明确保交易信息不可追踪和不可链接. Zerocoin 是一种比特币去中心化混合和扩展协议，为比特币用户生成等额 Zerocoins，无需第三方混合集. 用户在花费资产时产生记录在区块链的安全承诺，将各自承诺广播和零知识证明，其他用户通过验证区块链记录的证明验证交易. 但该协议存在计算复杂性高、证明尺寸大问题. 为优化计算开销和证明尺寸，Zerocash

对证明进行优化，设计了非交互式零知识证明协议zk-SNARK，用算术电路表示计算条件，以数据作为输入，给出真或假响应，降低证明尺寸和计算复杂度. Quorum 平台[74]也使用 zk-SNARK 实现匿名交易. 但 zk-SNARK 零知识证明前还需对公共参数可信设置，一旦公共参数遭到破坏将减低隐私保护能力. 随后，去可信设置零知识证明算法兴起，如 Ben-Sasson 等人[75]提出无需可信设置零知识证明协议 zk-STARK，对验证方算法复杂度控制到多项式时间级别. Bünz 等人[76]提出非交互式零知识证明协议 BulletProof，借助 Pedersen 承诺实现，支持小尺寸证明且无需可信设置，支持范围证明聚合，生成证明大小与范围区间呈限对数关系，压缩数据空间和交易费用. 同时，新型的零知识证明技术也在不断涌现. Maller 等人[77]提出基于 zk-SNARK 扩展版本协议的 Sonic 方案，虽然还需可信设置，但支持通用连续更新设置，按大小线性伸缩具备更强扩展性. Gabizon 等人[78]提出 Plonk 方案，通过优化算法和数据结构改进 Sonic 方案，将证明时间开销降低 80%. 随后发布的支持递归方案 Halo[79]、Fractal[80]有助于实现证明聚合、扩展证明结构、节约存储空间，提高应用可扩展性. Supersonic 方案[81]则通过移除 Sonic 方案中的可信设置，在计算复杂度高的交易证明场景下更具优势.

常见零知识证明算法对比如表 3 所示.

表 3 不同零知识证明方案对比

方 案	证明生成复杂度	证明验证复杂度	证明尺寸	可信设置
zk-SNARK	$O(n\log N)$	$O(1)$	$O(1)$	是
zk-STARK	$O(n\ \mathrm{ploylog}N)$	$O(\mathrm{ploylog}N)$	$O(\mathrm{ploylog}N)$	否
BulletProof	$O(n\log N)$	$O(N)$	$O(\log N)$	否
Sonic	$O(n\log N)$	$O(1)$	$O(1)$	是

虽然零知识证明应用增强了区块链隐私保护效果，但要封装大量密码单元，存在不少约束，且由于零知识证明生成时间依赖于交易数据，存在通过测量证明生成时间实现侧信道攻击的安全风险.

3.2.2 安全多方计算

安全多方计算能在互不信任的参与方间不暴露各自秘密数据前提下，实现秘密数据的协同计算. 参与方除获得正确计算结果外，无法获取其它秘密信息，多方计算过程中具有对自身数据绝对控制权. 如图 8 所示，区块链应用安全多方计算能够为分布式多方间数据协作计算过程中的数据安全和隐私保护提供有力支撑，具有输入隐私性、计算正确性及去中心化特征，能在保证数据隐私前提下使用数据，释放数据价值，实现数据可用不可见应用效果. 考虑到区块链计算与存储资源有限，对于数据协同计算常会利用安全多方计算将数据放在链下进行计算，再通过结合其它密码机制来验证相关信息的有效性与可信性. 如 Choudhuri 等人[82]基于可信硬件和以太坊实现了两个基于公平公开账本的多方协议，来对抗不诚实参与方，并发表了该协议无状态版本. Paul 等人[83]通过在该设计中消除 ZK 证明和承诺，有效提高计算效率. 针对区块链安全多方计算所面临的可伸缩性和效率问题，Raman 等人[84-85]提出可验证多方计算构建和压缩方法，解决区块链数据分析应用中的多轮计算验证问题. Luo 等人[86]利用安全多方计算构造选举共识算法，将基于逻辑环选举算法和姚百万算法集成到 DPOS 算法，解决安全多方计算问题. Ashritha 等人[87]利用安全多方计算重构变色龙哈希函数密钥，提高可编辑区块链安全性. 为解决安全多方计算公平性和鲁棒性问题，Gao 等人[88]引入信誉系统来提高方案稳健性. 但在区块链安全多方计算领域，还需克服安全多方计算的效率低、协作难度高的问题，距离通用应用还存在不小差距.

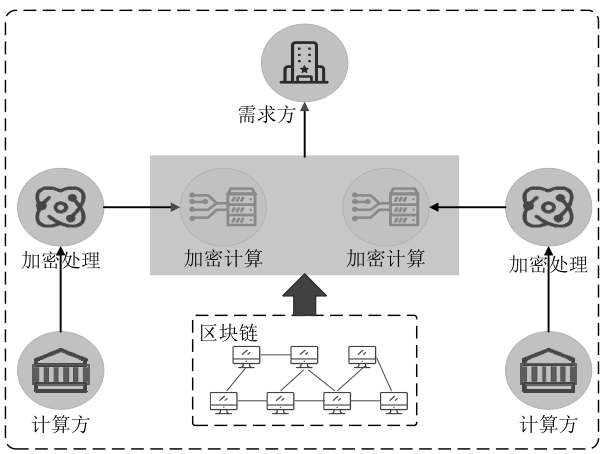


图 8 区块链安全多方计算模型

3.2.3 秘密共享协议

秘密分享是将秘密以适当方式进行分割，分割后每个份额由不同参与者管理，只有足够数目参与者共同合作才能恢复秘密消息，如图 9 所示，其目的是防止秘密过于集中带来的安全隐患，抵抗系统外敌人和系统内用户后台攻击. 秘密共享关键是如何更好地设计秘密分割和恢复方式. 区块链利用秘密共享能够在多方协作中避免秘密信息过于集中带来的安全隐患. 当前的秘密共享协议主要包括 Brickell、Blakley、Shamir、中国剩余定理等. Kim 等人[89]提出面向分布式存储区块链的局部秘密共享方案，利用

具有一个全局秘密和几个局部秘密的分层秘密结构，但该方案显著提高了秘密存储和恢复的通信成本. Biswas 等人[90]提出一种使用区块链的无欺骗(t,n)阈值秘密共享方案，该方案遵循 Shamir 技术，消除 PoW/PoS 共识机制产生的区块链漏洞. 针对区块链中私钥安全回收问题，Li 等人[91]通过可验证秘密共享方式实现联盟链中用户生物识别密钥的安全回收. Chen 等人[92]提出基于门限秘密共享的区块链数据共享查询方案，用于查询数据的秘密元素通过 Blakley 空间平面方程共享，限制了查询者的权限，保证区块链数据查询的安全性. Li 等人[93]提出了一种基于双阈值密钥保护秘密共享的联盟区块链钱包方案. 通过使用秘密共享的方法对用户的钱包私钥进行分割和存储，可以安全有效地保护私钥. Zheng 等人[94]提出了一种基于生成对抗网络(GANs)的密钥秘密共享技术，以解决区块链中存在的安全性低、丢失钥匙难找回及沟通效率低的问题. 在区块链中秘密共享协议主要应用于确保用户钱包安全，抵御钱包攻击. 秘密共享协议能够用于区块链场景中去中心化的密钥管理. 但由于需要进行多次计算和通信，在区块链网络中会带来较高计算和通信成本，且需要依赖于参与者间的信任和合作. 在参与者间存在竞争的交互环境，则难以适用.

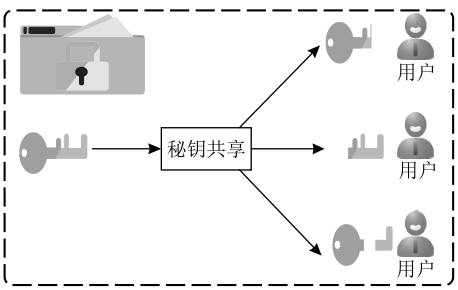


图 9　区块链钱包秘密共享协议

如表 4 所示，分别对比了三种密码协议的应用场景、优势以及存在问题，不同协议适用于不同的应用场景和业务需求，需根据实际场景进行选择.

表 4　不同数据加密算法

方　案	应用场景	优　势	存在问题
零知识证明	交易隐私增加	保证证明信息的安全性和隐私性，防止证明信息被泄露或篡改	需要依赖复杂数学算法和加密技术，具有较高计算开销
安全多方计算	去中心化计算	可在保证多方信息安全和隐私的前提下，实现多方去中心计算任务	需要依赖复杂计算术，具有较高计算开销，且需要依赖参与者间信任合作
秘密共享协议	去中心化密钥管理	通过将敏感信息分散存储，提高信息的安全性与可靠性	多次计算和通信带来较高计算通信成本，参与者存在竞争环境难以适用

3.3　密码基础设施

区块链系统利用密码基础设施来管理密钥与证书，为其密码系统正常运行提供有力支持.

3.3.1　密钥管理

高效安全的密钥管理是区块链系统需要面临的一大挑战. 若攻击者能够通过暴力破解、侧信道攻击、重放攻击、脆弱加密等攻击发现密钥，那么攻击者将能从目标系统窃取任何信息、系统安全性将不复存在. 区块链业务提供者需要对密钥进行严格管理，以防密钥丢失或被非授权访问、使用、泄漏、修改和替换，密钥管理技术涵盖密钥生成、存储、分发、导入导出、使用、备份恢复、归档及销毁等环节[95]. 区块链密钥管理主要对应于区块链钱包(客户端)的密钥管理. 区块链钱包类似于区块链银行账户，要从区块链钱包中使用数字加密货币、转移钱包用户数字资产，钱包所有者需要用其私钥来访问钱包. 当用户使用其合法私钥时，所有者可以访问相应账户，获得该账户对应数字资产使用权. 钱包安全性取决私钥安全. 如果攻击者通过物理手段窃取存储设备、侧信道攻击或黑客攻击等手段窃取钱包私钥，攻击者将能够轻松盗取用户数据资产. 当前密钥管理的密钥存储方式主要包括本地密钥存储、密码保护钱包、离线密钥存储、密码驱动密钥、钱包密钥托管. 不同存储方式如表 5 所示.

表 5　不同密钥管理存储方式

方　式	核心思想	优　点	缺　点
本地密钥存储	密钥存储在设备的本地存储	快速、方便地访问交易密钥	无法抵御恶意软件、设备物理访问和物理损坏
密码保护钱包	密钥由用户创建的密码保护	可以抵抗非法访问存储的密钥	钱包所有者忘记密码，将失去钱包内数字资产
离线密钥存储	私钥存储在 USB 等离线便携载体	避免网络、恶意软件窃取本地密钥	依托硬件载体，降低使用便利性
密码驱动密钥	用户提供密码驱动管理公私钥	降低使用难度，具有抗非法访问密钥能力	若密码强度较弱、存在彩虹表攻击可能
钱包密钥托管	用户密钥依托第三方服务器管理	降低使用难度，可抵抗非法访问本地密钥	钱包的安全是在第三方手中，存在失控风险

针对不同域密钥管理，Pal 等人[96]提出多层架构组密钥管理方案，节点按权限分为上层和下层节点，对每级节点进行组划分，同组节点拥有相同权限，实现分类密钥管理. 针对移动通信密钥安全管理，Jung 等人[97]提出基于分组密钥的安全管理方案，增强现有会话密钥安全方案，克服垂直模型及

SDN 水平模型端到端安全管理局限性. 为简化密钥生命周期管理,Genes-Duran 等人[98]利用中间件将支付区块链费用所需数字签名与授权所需数字签名解耦,用户无需被迫创新钱包保护私钥,提高密钥管理灵活性. 针对区块链高效密钥管理问题,Zhao 等人[99]利用人体传感器网络设计医疗密钥轻量备份和高效恢复方案. 针对钱包密钥安全存储问题,Shbair 等人[100]利用硬件安全模块 HSM 管理以太坊高价值加密密钥. 针对区块链密钥管理系统中的漏洞问题,Tanana[101]根据公开报告描述密钥管理生命周期每个阶段的潜在威胁,然后根据 Azure 区块链工作台和 Azure 密钥库的技术文档评估这些威胁在 Azure 区块链工作台环境中实现的可能性,为密钥管理中对威胁的管控提供支持. Lehto 等人[102]在 Intel Software Guard 扩展飞地生成和维护私钥,通过可信计算环境实现备份密钥与外部存储库间安全存储和恢复. Thota 等人[103]提出安全软件钱包,驻留移动设备,参与区块链网络,可无缝集成企业应用程序. 针对钱包密钥回收问题,Soltani 等人[104]利用自我主权身份验证数字钱包,使用 Shamir 秘密共享方案和 Hyperledger Indy 账本技术提供实用的分散密钥恢复解决方案. Qi 等人[105]将用户生物特征引入密钥管理,利用用户指纹生成私钥,在敏感操作时创建本地指纹特征数据库识别身份. Yeh 等人[106]通过可信执行环境隔离保护用户私钥,生成签名进行双因素认证,确保不会受到泄漏攻击. Kaga 等人[107]通过利用指纹、面部、静脉等生物特征生成短期私钥来创建区块链事务实现区块链中事务可靠验证.

3.3.2 证书管理

大多许可区块链依赖公共密钥基础设施 PKI 进行证书管理,提供身份验证和数据加密等安全服务. 如图10所示,PKI 是公钥密码系统对密钥进行管理的有效机制之一. 区块链可通过 PKI 对参与区块链网络成员进行身份识别与认证. 开源区块链 Fabric 采用支持分层的证书管理结构管理 X.509 格式证书,包括身份注册证书和节点间通信 TLS 证书两类证书,支持 RSA 和 ECDSA 公钥密钥算法,并包含证书根服务器、证书中间服务器,证书中间服务器是具有证书根服务器签名证书的证书服务器节点,用于分散节点与用户的证书颁发过程,减轻根服务器性能压力和暴露机会. 当中间服务器被攻击时,能够最大限度减小影响范围. Corda 则统一由 Doorman 服务管理节点和用户的初始 CA 证书,节点再由该初始 CA 证书创建并签署 TLS 证书和签名证书作为公开或隐私身份. 趣链 Hyperchain 则分别构建了中心化 CA、分布式 CA 两种证书管理体系,中心化 CA 证书管理可由可信机构或自建 CA 实现,分布式 CA 证书管理将证书管理权限转移至联盟链各参与方,由联盟网络节点互相颁发准入证书给其他网络节点,再在建立连接阶段完成证书认证. 另外,还通过构建不同的证书管理分区实现证书分区管理,不同分区可拥有不同的证书体系,分区间不共享证书体系,提高管理灵活性. 但由于区块链系统中的节点与用户动态性强,目前区块链系统证书管理还存在可伸缩性和新成员扩展问题. 为此,Albakri 等人[108]提出一种轻量级基于多项式的密钥管理方案,用于降低许可链背景应用程序证书管理面临的计算开销,增强证书管理的可伸缩性. Gallersdorfer 等人[109]使用绑定到公共已知域名的 TLS 证书来建立新联盟成员身份,使区块链具有更强的成员管理扩展能力.

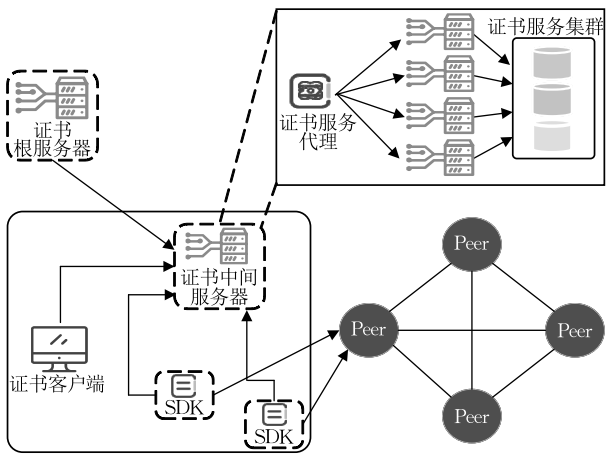


图 10 区块链证书管理

3.4 后量子密码技术

随着量子计算技术不断发展,量子计算机具有的强大并行计算能力,对传统密码算法构成极大安全威胁. Shor[110]提出可解决离散对数问题和因式分解整数问题的量子算法,意味着 RSA、ECDSA、ECDH、DSA 等算法难以有效抵抗量子计算攻击. 同时,量子计算还会降低哈希函数安全性. 量子计算可利用 Grover 算法[111]加速哈希生成,重建整个区块链. 此外,Grover 算法可用于检测散列冲突,在替换区块链中块后,保持区块链完整性. 当前区块链安全性依赖的公钥算法和哈希函数将变得不再安全[112]. 拥有足够强大量子计算机的攻击者能够伪造数字签名,冒充用户窃取数字资产. 为应对量子计算带来的挑战,研究抗量子区块链成为一种趋势,引申出后量子区块链概念[113],重点确保公钥算法和

哈希函数安全. 2022 年，NIST 公布首批四种后量子密码标准算法（CRYSTALS KYBER、CRYSTALS Dilithium、FAL CON 和 SPHINCS＋）. CRYSTALS KYBER 用于保护通过公共网络交换信息的通用加密，其它三种用于数据签名. CRYSTALS Dilithiu 与 FALCON 基于格设计，SPHINCS＋基于散列函数设计.

主流区块链后量子计划已陆续出现，后量子比特币[114]是比特币主区块链的实验分支，采用后量子数字签名方案. 以太坊 3.0 计划采用零知识证明作为抗量子组件. Abelian 项目建议使用基于格的后量子密码系统抵御量子攻击. Corda 项目也在试验后量子算法 SPHINCS. Semmouni 等人[115]提出在 ECDSA 签名中使用 Koblitz 曲线 secp256k1 和 SHA-256 改进比特币系统，实现抗量子攻击. Gao 等人[116]在区块链电子投票协议中利用 Niederreiter 加密系统抵抗量子攻击. 另外，一些研究通过采用量子密码技术，解决区块链抗量子攻击的安全问题. 量子密码[117]基于量子力学基本性质，被证明具有根本安全性，得到广泛关注，涵盖量子密钥分发、量子安全通信、量子秘密共享，量子数字签名和量子公钥密码等. Jogenfors[118]利用量子力学不可克隆定理，提出量子比特币，构建量子比特币协议，但方案效率较低. Kiktenko 等人[119]利用城市光纤网络量子密钥分发实现区块链安全身份认证. Rajan 等人[120]提出一种具有时间量子纠缠的量子区块链，将区块链编码到不同时共存的光子时域状态，与空间纠缠相反，时间纠缠提供量子优势. Gao 等人[121]构造基于贝尔态全量子区块链优化系统安全性，基于量子不可克隆定理，定义新型加密量子货币，采用量子纠缠和 DPoS 机制设计量子区块链来抵抗中间人攻击、双花费攻击、量子攻击等. 总的来说，关于量子区块链研究还不成熟，有很多通信、交互、效率等问题需要解决. 针对区块链的后量子密码系统还面临密钥尺寸较大、签名和哈希长度较大、执行速度慢、计算复杂度和能耗高等问题.

4　区块链平台安全技术

本节介绍平台安全 5 个方面：存储安全、网络安全、共识安全、应用安全以及共性安全服务.

4.1　存储安全

区块链系统的数据存储安全是在区块链密码支撑技术的基础之上建立的，通过综合运用各类密码技术实现覆盖保密性、完整性以及可用性的数据存储安全目标. 由于单一区块链存储能力有限，一般通过采用协同存储模型[122]来提高区块链数据存储性能，如图 11 所示，由中间件来链接区块链节点的链上数据与链下数据库中数据，从而实现数据存储能力提升.

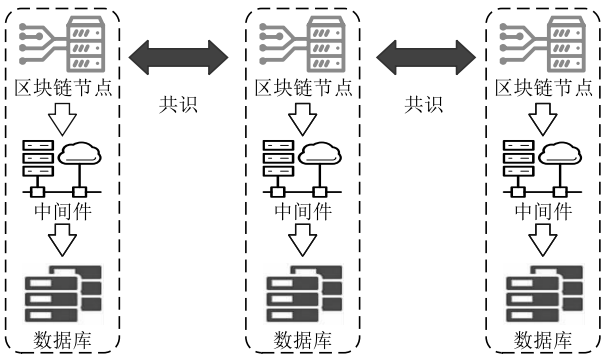


图 11　区块链数据协同存储

为提高数据存储保密性，Zhao 等人[123]提出区块链秘密数据安全保护框架，将包含秘密数据的视频上传区块链网络，利用智能合约操作视频中秘密数据嵌入和提取，并对存储在区块链和数字视频内秘密数据进行验证、跟踪和保护. 针对数据存储的完整性验证问题，Li 等人[124]将轻量级验证标记存储于区块链，使用标签构建 Merkle 哈希树生成证明验证存储数据完整性. He 等人[125]设计一种新的区块链存储结构 T-Merkle 树及其搜索算法，以提高存储利用率并支持块中二进制搜索. 针对区块链直接使用 Merkle 树存储数据结构尺寸较大、难以批量完整性验证问题，Wang 等人[126]采用增量聚合子向量承诺代替 Merkle 树，降低通信消耗. 针对 Merkle 树不能提供非成员证明问题，Wang 等人[127]利用 RSA 构建无 Trapdoor 批量更新密码累加器代替 Merkle 树，支持成员证明和非成员证明. 针对数据完整性审计追责问题，Xie 等人[128]提一种可验证损坏评估方法，允许用户根据数据损坏程度获得补偿. Ren 等人[129]提出区块链与再生编码相结合的混合存储架构，利用再生编码提高数据存储可靠性，利用数据哈希值定期验证机制确保数据完整性.

针对海量数据区块链复制过程系统性能下降影响可用性的问题，Tulkinbekov 等人[130]将区块链数据保存在共享存储中，通过存储集合签名结合区块链事务引用数据，将区块链声明的所有特征保留在单独数据库来兼顾存储安全性与可用性. 针对区块链存储能力受限问题，Ren 等人[131]提出具有指定验证人

的顺序聚合签名方案，以压缩存储空间. Jayabalan 等人[132]将区块链与星际文件系统结合构建患者为中心的数据存储模型，结合 AES-128 和 RSA 4096 多层安全机制保证数据安全. 为提高区块链数据搜索能力、增强数据可用性，Grabis 等人[133]使用用户和设备搜索操作知识库提高数据的检索速度. 针对区块链面临的存储空间占用高、数据灵活性和可用性低、检索效率低、可扩展性差等问题，Han 等人[134]结合链外存储和重复数据删除技术对区块链存储模型优化，减少副链数据冗余，增强数据灵活性，压缩存储空间、提高存储效率，但会带来额外的链上链下通信成本.

综上所述，目前区块链依托各类密码技术在存储保密性上能够达到较高水平，但受限于区块链上珍贵的存储空间，如何高效地构建新型区块链安全存储架构，支持高效数据完整性验证，提高数据存储效率、增强数据搜索能力依然是制约区块链应用于大规模数据应用场景的重要瓶颈.

4.2 网络安全

区块链依靠底层 P2P 网络在节点间传播区块数据，是区块链重要的基础设施. P2P 网络采用去中心化模型，每个设备(也称为对等体)既充当客户端，也充当服务器. 即对等体可向网络上其他对等体发出请求，并平等接收和响应它们的请求，同时扮演客户端和服务器的角色. 不同于传统客户机-服务器模型中，客户机只能够向服务器发送请求，再等待服务器答复. P2P 网络具有容错能力强、整体网络性能高、负载均衡和易于维护特点，但 P2P 网络的安全问题还没有得到充分解决. 区块链通过 P2P 网络进行数据交互，也导致其更容易受到攻击者分散的网络攻击，如拒绝服务攻击、女巫攻击、日蚀攻击、51% 攻击等，如表 6 所示. 区块链系统需要足够强度网络安全技术来维护区块链网络安全，包括网络节点安全、网络传输安全及网络威胁发现.

表 6 区块链常见网络攻击

存储方式	核心思想	防御方案
拒绝服务攻击	利用目标服务缺陷或直接消耗其资源，使其无法提供正常服务	高防服务器、CDN 加速、防火墙、攻击检测和溯源、黑名单机制
女巫攻击	通过操控或模仿多个虚拟身份来进行攻击，干扰系统的正常行为	身份验证机制、信誉机制、工作量机制、节点特征区分
日蚀攻击	节点只能接收由攻击者操纵信息，控制特定节点对网络信息访问	身份验证机制、连接限制、NodeID 更新、节点实时检测
51%攻击	攻击者拥有超过全网50%的算力，便可以发动51%的算力攻击	共识优化、激励机制

4.2.1 网络节点安全

确保网络节点安全的关键是要及时发现区块链网络中的恶意节点. 针对加密货币新节点加入问题，Loe 等人[135]调查了 74 种加密货币的引导节点加入机制，提供了降低加入风险的建议. 针对 P2P 网络恶意节点发现问题，Alanazi 等人[136]提出恶意信任管理器识别协议 MTMI，用于保证 P2P 网络信任管理器匿名性，并为网络中对等体计算和存储信任值，利用公钥基础设施建立信任管理器间安全连接，为网络节点提供可信支持. Prunster 等人[137]通过引入基于硬件的认证机制将 P2P 网络节点标识符绑定到不同物理设备来抵抗女巫和日蚀攻击. 针对节点信任问题，Alhussain 等人[138]提出智能信任管理系统 Trutect，利用神经网络为节点提供可信度度量来检测恶意节点. 针对无线网络节点安全，Ndajah 等人[139]提出基于修改 AODV 路由协议的解决方案，抵抗无线 P2P 网络黑洞攻击. 针对以太坊女巫攻击问题，Eisenbarth 等人[140]提出可疑节点检测撤销机制，构造网络节点监控系统，帮助区块链客户端删除与可疑对等点连接. 针对 Monero 币网络拓扑分析问题，Cao 等人[141]开发网络探索工具来推断网络拓扑结构、大小、节点分布和节点连接，为节点分析提供支撑. 针对开放 P2P 节点资源稀缺性加剧问题，Qu 等人[142]提出非完全合作节点的识别方法和信任路由方案，引入八分域概念，建立信任模型，从直接信任、内部状态和推荐可靠性三个维度分析节点，通过对不同八分域划分识别单个非完全合作节点. 针对 P2P 网络节点公平性问题，Berenjian 等人[143]提出基于激励的安全模型，防止 leecher 对 leecher 交易背叛，并帮助 seed 获得更公平对待. 针对 P2P 僵尸网络攻击问题，Beauchaine 等人[144]提出名为 BotsideP2P 的测试平台，专门用于检测具有内置网络和端点监控的 P2P 僵尸网络. Zhuang 等人[145]提出基于网络流级社区行为分析的改进 PeerHunter 系统来检测 P2P 僵尸网络，利用网络流级别社区行为分析来检测潜在僵尸网络. 针对比特币节点面临的对等连接风险，Tran 等人[146]提出依赖于第三方代理的解决方案，但在比特币点对点系统中存在大约 1 万个潜在脆弱节点，为所有节点提供多个代理存在困难. 针对比特币 P2P 网络中主节点协议安全性与性能评价问题，Sallal 等人[147]提出基于主节点聚类的近端感知扩展协议，评估基于物理邻近性的分组节点安全性，通过分配节点增加物理网络连通性，减少节点间跳数. 综上所述，目前网络恶意节点

检测方面研究已经取得了一定的进展，在较小的网络规模下能够起到较好的防护效果. 但随着区块链网络规模逐渐增大，节点状态动态变化，网络拓扑复杂度将呈现指数增加，检测评估在性能、准确性、实时性上都将面临巨大挑战.

4.2.2　网络传输安全

P2P 网络作为区块链主要网络交互协议，在高度敏感的开放网络环境中面临着众多安全威胁，如没有标准化信任机制、缺乏有效安全机制（包括加密、身份验证甚至日志记录），这些威胁将直接对区块链网络传输安全产生直接影响，现有 P2P 网络传输安全研究同样能够提供重要借鉴. Tapsell 等人[148]对比特币网络协议进行分析，发现 Connection handshake，GETHEADERS/HEADERS 和 MEMP-OOL/INV 三种比特币消息交换更易收到欺骗和 DDoS 攻击，可通过在网络消息中引入随机 nonces 提高网络安全性. 为更好地保护 P2P 网络数据传输安全，Musa 等人[149]使用网络监控来管理和保护网络流量，通过包嗅探捕获网络数据分析、检查. 针对传输数据易被篡改污染问题，Ziwich 等人[150]提出基于比较诊断的分布式策略，节点间独立识别和避免污染者，有效对抗内容污染传播. Kumar 等人[151]提出无托管基于身份的签名加密方案 EF-IDSC，用于不可信节点 P2P 点播流安全数据传输，允许对等体使用非对称密钥算法与其他对等体建立会话密钥. 针对拓扑高度影响区块链数据广播速度，导致性能较差，易受双花攻击等问题，Hao 等人[152]构造一种网络传输优化设计，利用 K-Means 算法将邻近对等节点聚集成簇实现地理邻近感知聚类，基于节点属性分类分层拓扑结构，保证网络强连通性和小直径并行生成树广播算法，实现集群内和集群间节点快速数据广播，提高网络性能和安全性. 针对分布式网络数据执行聚类带来的效率和安全挑战，Zhu 等人[153]设计基于同态加密的安全聚合协议和安全分割协议，在不暴露单个对等体隐私情况下实现安全集群计算. 针对在被动窃听者存在情况下鲁棒传输设计问题，Yang 等人[154]通过使人工噪声功率最大化，迷惑被动窃听者，并在有界球形区域为从中继到目的地的信道状态信息错误向量范数和所有中继节点单个功率约束，对用户服从最差信噪比约束. 综上可知，通过多种安全增强技术能够显著提高网络传输的安全性，但对于单个节点来说会带来加大的性能开销，导致交易效率被显著影响. 因此，在实际的区块链应用过程中，建议区分不同敏感程度的安全传输场景，综合评估安全成本-收益，在关键信息传输环节重点应用.

4.2.3　网络威胁发现

异常检测工具在保护网络免受不可预见攻击方面发挥至关重要作用，一般通过自动识别和过滤异常活动实现. 为保证区块链网络可靠和安全，Matsuura 等人[155]提出基于邻域信息的邻居选择方法，使得整个网络块分布变得更快且保持区块链中随机邻居选择性质不变，有效降低日蚀攻击风险. Gaba 等人[156]使用机器学习方法和软件定义网络检测区块链安全攻击，设计以编码器-解码器模型为中心基于异常的网络攻击识别方法. 对于区块链交易面临的网络威胁入侵检测问题，传统入侵检测系统不足以抵御区块链攻击且评估损失时效较长. 根据比特币交易所入侵点不同，Kim 等人[157]描述用户管理服务器入侵、签名服务器入侵、比特币网络入侵三种交易所入侵模型，并提出相应解决方案. 针对异常入侵对区块链的重大威胁，Liang 等人[158]提出基于区块链的协同聚类特征数据融合方法，设计了数据融合数学模型，利用 AI 模型对区块链网络中数据集群进行训练分析，当加权系数和相似度匹配关系遵循标准模式时，可准确协同检测异常入侵行为. 针对采用区块链的物联网系统面临的 DDoS 攻击问题，Kumar 等人[159-160]构造分布式入侵检测系统，利用雾计算检测区块链 IoT 网络中针对矿池的 DDoS 攻击，通过训练随机森林和优化梯度树增强系统对分布式雾节点进行性能评估，对于二进制攻击检测，XGBoost 性能更好，对于多攻击检测，随机森林性能更好. Signorini 等人[161]利用区块链元数据收集潜在恶意活动，允许区块链网络对等体通过共享攻击信息免受日蚀攻击，利用分叉检测防止本地威胁. 针对智能合约网络威胁，Echeberria-Barrio 等人[162]提出基于路径研究的入侵检测系统，用于保护智能合约，监视合约接收事务，生成事务到达路径，从路径信息中提取和分析特征，以保护其免受潜在威胁. Wang 等人[163]提出一种保护以太坊智能合约免受网络威胁入侵检测系统 ContractGuard，将入侵尝试作为异常控制流进行检测，将其嵌入到合约以分析上下文标记无环路径，并在以太坊 gas 性能模型进行优化. Kabla 等人[164]分析入侵检测系统在检测以太坊攻击方面适用性，围绕 DAO 攻击、庞氏骗局、欺诈检测、51% 攻击、缺陷分析、恶意实体、日蚀攻击等攻击行为检测. 针对区块链网络拓扑分析问题，Wang 等人[165]设计一款以太坊网络分析仪

Ethna,利用以太坊 P2P 网络中消息转发协议随机选择特性来测量节点程度分布,并通过网络观察节点计算交易广播延迟和将消息广播到整个 P2P 网络所需跳数,能够为区块链 P2P 网络安全性分析提供网络拓扑支持.针对区块链系统面临 DDOS 攻击问题,Chaganti 等人[166]分别对基于网络的 DDoS 防御方案、基于源的 DDoS 防御方案、基于目的的 DDoS 防御方案及混合 DDoS 防御方案进行分析综述.综上所述,现有区块链系统的网络威胁发现方法主要是利用各类机器学习或深度学习算法构建威胁发现模型,从而实现威胁发现.但该类方法需要有事先标定好的数据集来进行模型训练,对于真实攻击场景中大多是小样本或无样本的威胁攻击场景,其适用性将大大降低.

4.3 共识安全

共识机制[167]是区块链安全、平稳运行的关键技术,对维护网络安全、完整和效率起着至关重要作用,承担着区块链公平正义问题.随着区块链不断发展,呈现出了很多新的场景,对共识机制也提出很多新需求.表 7 是对区块链系统常用共识机制的总结,包含基于工作量证明的共识机制、基于权益证明的共识机制、基于拜占庭容错的共识机制以及混合共识机制,可根据不同的应用场景和安全需求灵活选取合适的共识算法.围绕共识机制的研究较多,但现有共识研究还难以真正意义上突破安全性、去中心化和可扩展性的"不可能三角",在这三个方面中,只能较好地同时满足其中两个,而无法同时满足三个.

表 7 共识机制对比

共识机制	核心思想	优 点	缺 点	应用平台
基于工作量证明的共识机制	通过消耗资源竞争完成特定任务来获得出块权和区块奖励	有效保证节点工作量、增强攻击成本、易于验证	消耗大量资源,造成能源浪费和环境压力,易形成矿池垄断,带来安全问题	Bitcoin、Ethereum、IOTA 等
基于权益证明的共识机制	按参与共识的节点所拥有的权益来投票决定下一个区块的验证节点	具有更高的能源效率和更低的计算要求,能够实现更高的交易吞吐量	存在导致富者更富的情况,导致共识的中心化风险,且质押存在市场风险	Cardano、Snow White、Polkadot 等
基于拜占庭容错的共识机制	通过在主节点、备份节点以及客户端间通过预准备、准备和提交三个步骤确保一致性和安全性	能够满足高性能、高可用性、高容错性需求	增加节点通信流量和计算复杂度,节点越多、性能下降越快	Hyperledger Fabric、Corda 等
混合共识机制	将不同的共识机制结合使用	兼顾不同共识机制的优势,达到高效、安全、灵活的目标	实现要求比较高,需要考虑不同共识机制的安全性和兼容性	Algorand、Hybrid、RapidChain 等

在区块链采用工作量证明作为共识机制情况下,攻击者不能控制超过 50%网络算力.然而,这个 50%阈值只是基于计算能力的分析,对网络和节点行为有隐含和理想假设.Xiao 等人[168]研究表明诸如网络连通性、区块链分叉和挖掘策略等因素能够破坏诚实多数所保证的共识安全.针对共识机制运行公平性和效率问题,Ai 等人[169]提出一种运用连续双拍卖理论的共识激励机制,包括启动阶段、拍卖阶段、完成阶段和确认阶段,以确保交易实时存储.针对比特币和以太坊等主流区块链面临审查攻击问题,Xian 等人[170]对现有 POS 和 POW 算法进行改进,通过引入新消息类型和对验证器进行可疑性评估来识别攻击者.Qiu 等人[171]提出基于动态信誉的区块链共识机制,引入了信誉评估算法,允许信誉值高于阈值的节点申请成为监控节点,在验证器功率过大对区块链网络造成危害情况下,监控验证器行为.为降低 POW 机制对性能的要求,Sui 等人[172]提出基于工作量调整的 POWS 机制,在 POW 共识机制中引入造币概念调整节点挖掘难度,通过计算力和计算量两个因素来动态调整挖掘难度.针对 DAG 区块链系统共识问题,Gai 等人[173]从 DAG 结构中对原始区块进行排序、合并,并重新构建基于单链的区块链系统,通过运行全局排序方案和块合并操作,DAG 可以在新形成块上达成共识.Liu 等人[174]提出基于委托的可伸缩拜占庭假容忍混合共识机制,结合 PoW 和 BFT,实现效率和可伸缩性间的平衡.

不同于公有链,联盟链和私有链倾向于应用基于拜占庭容错的这种确定性共识机制,作为基于工作量和权益证明共识机制的有效替代方案.基于拜占庭容错的共识机制允许两种类型的故障,拜占庭故障和崩溃故障.拜占庭容错共识通过对失败时间和次数限制假设来保证有效性,而终止依赖节点消息广播.Crash-Fault 容错共识在牺牲效率同时,不严格地确保终止和更高吞吐量.Carrara 等人[175]提出基于确认消息广播邻近投票的轻量级共识机制,实现共识成本的降低.针对联盟区块链应用场景,Li

等人[176]提出投票证明机制(Proof of Vote,POV),为网络参与者建立不同安全身份,区块提交和验证由联盟机构投票决定,而不依赖第三方中介或不可控公众意识,提高共识达成速度.针对实用拜占庭容错 PBFT 无法有效激发可靠节点积极性问题,Wang 等人[177]提出信用委托拜占庭容错协议 CDBFT,设计投票奖惩方案及其信用评价方案激发可靠节点积极性,减少异常节点参与.针对区块链监测系统对区块链治理场景跨区块链共识需求,Cheng 等人[178]提出基于智能合约的跨区块链共识机制 PoEC(Proof-of-EndorseContracts),该机制支持被监管区块链通过区块链系统加入治理区块链,而不改变原共识机制,具有低成本、高扩展性和跨区块链等优点.经典区块链共识机制建立在经典密码系统基础上,主要基于计算复杂问题实现.随着计算能力提高,其安全性将受到威胁,存在计算资源浪费、51%攻击、吞吐量低等问题.Wen 等人[179]提出量子区块链共识机制,基于量子隐形传态技术和量子测量随机性设计,具有量子密码学的无条件安全性且不涉及大量计算资源.Li 等人[180]利用量子投票为量子区块链方案提供快速去中心化,构建量子委托权益证明(QDPoS)共识机制,将经典信息初始化为每个单个量子态一部分,这些量子态相互纠缠形成链.

4.4　应用安全

智能合约是实现去中心化区块链应用的核心手段,是表示业务流程可自动执行的程序.它们是可序列化复制的代码和状态对象束.当参与者向区块链添加智能合约时,链中的一个新区块将包含这些智能合约,更新智能合约状态的每个事务也会进入更改后创建的下一个块,具有公开透明、自动执行、安全可靠等特点.为保障区块链应用安全,重点是保障智能合约安全.智能合约生命周期及对应安全问题如图 12 所示,主要涉及设计安全、实现安全、测试安全、部署安全等环节.

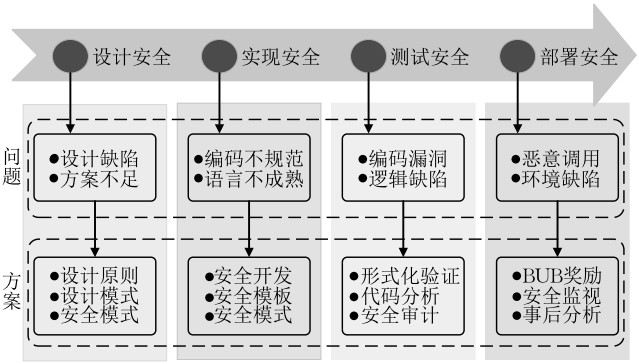


图 12　智能合约生命周期及对应的安全问题

4.4.1　设计安全

智能合约设计安全主要包括设计原则、设计模式、安全建模三个部分,所关注的是如何设计安全的智能合约来避免合约安全问题,安全建模中构建的模型可直接转换为合约实现.在设计原则研究方面,为设计安全的智能合约,文献[181]和文献[182]分别针对 EOS 平台与以太坊平台的合约安全设计原则进行分析,都认为要在智能合约的错误准备、保持更新、保持简洁、彻底测试、清楚特性等方面进行慎重考虑,区别是后者还着重强调合约的安全可重用设计,认为理想的智能合约是模块化的,重用代码而不是重复代码,并要支持可升级组件.在设计模式研究方面,设计模式描述重复出现编码模式的抽象,并给出标准解决方案.Bartoletti 等人[183]以以太坊合约代码样本为例分析,从应用设计角度总结出了 Token、Authorization、Oracle、Randomness、Poll、Time constraint、Termination、Math 以及 Fork Check 9 种常见设计模式,量化不同设计模式在合约中的使用,对设计模式和应用程序领域间相关性研究驱动智能合约领域特定语言编程原语的正确选择,可针对特定模式合约可采用针对性机制改进其安全性.Wohrer 等人[184]从纯安全设计角度提出 Checks Effects Interaction、Emergency Stop、Speed Bump、Rate Limit、Mutex 以及 Balance Limit 6 种设计模式并给出具体代码范例,所提供模式描述了典型安全问题解决方案,可以被 Solidity 开发人员应用以减轻典型攻击场景带来的威胁.针对智能合约开发缺乏标准设计过程的问题,Singh 等人[185]提出自适应安全支持需求工程方法,根据威胁模型、目标模型和服务水平协议安全规范做出决策,在设计阶段针对漏洞和威胁采取预防措施.在安全建模研究方面,为保证合约代码实现和合约需求间语义的一致性,Idelberger 等人[186]认为基于逻辑的智能合约编码在弥合合约实施和法律条文之间的差距方面具有明显的技术优势,因为基于逻辑的智能合约在谈判和争议解决过程中更容易被相关实体理解,提出了将基于逻辑的智能合约与区块链系统结合使用的方案,有效提高安全性,但由于逻辑语言复杂度高、执行效率低,方案部署成本较高.Anastasia 等人[187]引入 VeriSolid 框架,用于正式验证使用基于转换系统的模型指定的合约,该模型具有严格的操作语义,基于模型的方法允许开发人员在抽象的高级别上推理和验证合约行为,从而支持按设计正确原则开发智能合约.为及时发现智能合约设计问题,Ahmadjee 等人[188]提出

基于技术债务的智能合约安全设计漏洞评估方法，使用 CWE 目录分析所识别的安全设计漏洞，并能估计出漏洞后果及其本金和利息，通过调整社区知情评分机制来计算合约活动水平和合约寿命，允许开发人员通过技术债务影响分析和优先级排序专注于解决智能合约漏洞，提高了安全设计问题的可见性. Park 等人[189]使用形式化验证工具 UPPAAL 来证明智能合约系统设计的准确性，实现对合约设计逻辑矛盾和错误的发现.

4.4.2 实现安全

安全实现包括安全开发、安全模板和安全建模三个方面. 前面已经解释了安全性建模. 本节主要讨论安全开发和安全模板. 在安全开发方面，主要关注的是智能合约开发人员如何在合约实现过程避免安全漏洞. OpenZeppelin[190]是安全智能合约开发的安全库，基于 ERC20 和 ERC721 标准实现，提供基于角色的区块链方案控制方案和 SafeMath 安全运算等功能，用于防止合约代码的溢出和下溢问题. 开发可升级以太坊智能合约四种标准技术，分别是 Master Slave、Eternal Storage、Upgradeable storage proxy、Unstructured upgradeable storage proxy. 该工作表明尽管部署的合约代码是不可变的，但只要提前考虑相关安全问题，仍然存在可变通实现方法. 此外，解决特定安全漏洞修复方案也可被视为安全开发一部分. Aragon OSx[191]通过将合约功能权限分配到特定地址来确保只有合法用户能够调用合约. 针对事务还原语句对合约开发安全性影响，Liu 等人[192]通过从智能合约中删除事务还原语句，将改变后合约与原始合约进行比较，分析事务还原语句安全影响，为智能合约开发人员提供适当使用交易还原语句的实用指导. 为避免以太坊合约实现安全漏洞，文献[182]从 External Calls、Force-feeding Ether、Public on-chain Data、Unreliable Participants、Negation of Signed Integers 几方面为开发者提供合约实现开发指导意见. 在安全模板研究方面，针对目前对智能合约研究大多集中在编码安全性上，而缺乏友好工具来为用户设计专门合约编码模板问题，Mao 等人[193]提供了可视化、用户自定义的智能合约设计系统，该系统采用 TF-IDF 和 K-means 算法对智能合约数据集进行领域特征提取，再利用 Char-RNN 实现基本功能代码的自动生成，采用谷歌 Blockly 将代码与 UI 控件链接，为用户设计智能合约提供基本功能模板. Tateishi 等人[194]提出从文档模板和受控自然语言 CNL 自动生成智能合约的技术，能自动化实现从文档模板和 CNL 到一个包括定义合同中条款时间约束和程序模型的映射，并将该模型转换为可执行智能合约. 针对使用自然语言起草智能合约任务问题，Qin 等人[195]探讨了智能合约自然语言和自执行问题，通过支持人类可读、计算机可理解和自执行的基于机器自然语言语义结构 MNL 合约表示方法来重新定义智能合约，通用字典 CoDic 将自然语言转换为通用机器代码，避免各方间歧义. 为帮助开发人员独立于语言或目标区块链平台构建智能合约，Hamdaqa 等人[196]提出增强智能合约参考模型和建模框架 iContract-ML 2.0，将参考模型概念映射到设计参考模型所使用区块链平台，再将其概念映射到以前没有考虑过的新智能合约语言，提供常用功能实现模板，支持生成结构和部署构件，使开发人员能建模和生成可部署到多区块链平台的功能性智能合约代码.

4.4.3 测试安全

由于智能合约部署后很难打补丁，因此有必要在部署前进行足够测试以确保其安全性. 测试安全解决方案可分为形式化验证、代码分析工具和安全审计等方面. 在形式化验证研究方面，形式化验证是验证程序正确性和安全性的数学方法. 智能合约非常适合于形式化验证，因为合约程序规模较小且有时间限制，形式化验证通常在合同代码完成后应用. Abdellatif 等人[197]提出基于智能合约源代码的行为交互优先级框架的智能合约行为强语义建模方法，用一系列运行时验证和模拟引擎模拟行为，以验证安全属性，发现了一些恶意操作. Bhargavan 等人[198]将以太坊智能合约翻译为函数式编程语言 F*，实现程序交互式验证，但该翻译只支持 EVM 字节码片段，而忽略了许多基本结构. Hirai[199]使用 Lem 形式化 EVM 语义，提取交互定理证明器 Isabelle/HOL 来证明智能合约安全属性. 该工作是用于智能合约验证的第一个正式 EVM 定义. 但语义描述只是原始语义的合理近似，不能作为静态分析通用基础. 在代码分析工具研究方面，主要通过代码分析工具来提高代码质量和安全性，Tsankov 等人[200]提出了以太坊智能合约的安全分析器 Securify，通过对合约依赖关系图进行符号化分析，从代码中提取精确语义信息，再检查其遵从性和违反模式，以此证明合约的正确性并发现关键违规行为. Zhou 等人[201]构建一个静态分析工具 SASC，用于生成智能合约的调用关系拓扑图，再进行逻辑风险的检测和定位，并将结果标注在拓扑图上. Jiang 等人[202]提出了一

种模糊器 Contract Fuzzer，使用模糊测试技术发现智能合约漏洞，基于智能合约 ABI 规范生成模糊输入，定义测试 oracle 以检测安全漏洞，测量 EVM 记录智能合约运行时行为，并分析这些日志以报告安全漏洞. Chan 等人[203]提出了一个面向智能合约的模糊测试架构 Fuse，提交待测试智能合约的加密二进制文件或智能合约 URL，分析其控制流信息、合约事务消息和程序状态之间交互，并将该信息传递给漏洞检测模块和模糊测试生成模块实现安全测试. 在安全审计研究方面，如果开发人员自身执行安全审计专业能力不足，可以将审计任务委托给专业机构，由机构将根据发现的安全问题编写合格的审计报告. 理想的审计将是自动和手动代码分析结合. 自动代码分析一般使用静态代码分析工具，如 Oyente 和 Securify 来查找漏洞. 这些工具可为安全审核员节省大量时间，但它们可能会错过一些关键安全漏洞信息. 作为补充，审核员可以检查重点代码，手动分析测试它们是否存在漏洞. 此外，监管机构还需要对智能合约进行公开审计. 公链中智能合约，没有现成源代码，这使得审计具有挑战性. 为此，Zhou 等人[204]提出一种智能合约逆向工程工具 Erays，用于基于 EVM 字节码重构高级伪代码，安全审核员利用 Erays 不仅可以探索以太坊智能合约代码复杂性和代码重用性，还可以发现合约的意图和行为，完成合约的安全审计.

4.4.4　部署安全

即使已经部署并运行了智能合约，区块链用户仍然需要一些措施来发现前一阶段遗漏的合约漏洞，以便在新版本中改进. 由于智能合约很难对漏洞进行修补，因此在智能合约部署后，如何监控智能合约的异常活动并采取相应应对措施是需要提前考虑的问题，鼓励采用一些有效检测和防止智能合约中恶意行为扩散的方法. 这些措施主要包括 BUG 奖励、安全监视和事后分析. 在 BUG 奖励研究方面，尽管部署前测试阶段可以帮助我们找到大多数 BUG，但仍有一些 BUG 难以识别，BUG 奖励程序用于发现深藏不露的 BUG，属于动态分析技术. 在 BUG 奖励计划中，期望获得奖励的黑客通常会在系统运行时发现漏洞. 许多以太坊生态系统支持 BUG 奖励程序提高系统安全性，如 EtherScan 和 Raiden. 然而，BUG 奖励缺乏合理定价原则且存在奖励支付者不进行支付的问题，损害了 BUG 奖励程序运行. 为此，Breidenbach 等人[205]设计 BUG 奖励框架 Hydra，该框架利用一种称为 N-of-N 版本编程 NNVP 的漏洞利用技术，并通过可调整奖励值和承诺来鼓励理性黑客披露合约漏洞，防止漏洞扣留. 在安全监视研究方面，监控分析区块链交易数据可实现漏洞实时发现. 通过分析以太坊合约在运行时的多次调用，Nikolic 等人[206]系统地描述了称为跟踪漏洞的漏洞，实现对 greedy contracts、prodigal contracts 及 suicidal contracts 三种具有追踪漏洞合同的检测，实现 MAIAN 指定跟踪属性推理，通过使用符号分析和验证器，能够发现奇偶校验错误漏洞. Grossman 等人[207]定义了有效的无回调对象 ECF 的概念，通过监视以太坊执行轨迹中的 ECF 对象来识别漏洞. 在事后分析研究方面，随着区块链事务数据量的不断增加，一些数据分析或机器学习的方法可以发现区块链上的攻击或异常活动. Chen 等人[208]提出了一种利用数据挖掘和机器学习方法检测区块链上庞氏骗局的方法，提取智能合约的用户账户和操作代码的特征，建立分类模型来检测作为智能合约实现的潜在庞氏骗局. Chen 等人[209]利用图分析来描述以太坊上的货币转账、智能合约创建和智能合约调用三个主要活动，构建 Money Flow Graph(MFG)、Smart Contract Creation(SCC)和 Smart Invocation Graph(CIG)，利用跨图分析来实现合约攻击取证和运行异常检测，以此检测合约运行状态. 针对某些场景下智能合约的可调整与可更新应用需求，需要对智能合约进行高效的重新编译和重新部署，Li 等人[210]提出了一种新的智能合约体系结构和优化机制 ATOM，设计了一个紧凑的面向应用程序的指令集来描述应用程序操作，从应用程序中构造智能合约的字节码，提供了更经济的更新合约和快速地在指令方面执行合约体系结构支持.

表 8 对比分析了智能合约安全防护相关研究工作，主要从方案分类、方案手段、核心思想等角度描述现有智能合约安全防护在设计安全、实现安全、测试安全、部署安全的代表性工作. 经过分析可知，目前合约设计安全方面大多均需要依靠预设定的模式来指导实现，但现实环境难以预设所有合约的漏洞和威胁模式，还需要进一步抽取出更抽象的安全设计模式强制嵌入到底层开发框架，避免开发人员由于人为因素引入漏洞. 实现与测试安全方面成果较多，综合运用定理证明、符号化分析、模型检测、模糊测试、语法树等技术确保合约逻辑安全，但随着合约系统复杂度增加，可能存在状态空间过大问题，还需在安全性、可用性、可扩展性方面寻求突破. 在部署安全方面，由合约的漏洞难以绝对避免，需要构建有效的合约升级与更新机制来应对动态出现的安全问题.

表 8 智能合约安全防护相关研究工作

分 类	手 段	代表性工作	核心思想
设计安全	设计原则	Security Guidelines[181]	错误准备、保持更新、保持简洁、彻底测试、清楚特性
		General Philosophy[182]	错误准备、保持更新、保持简洁、彻底测试、清楚特性、重用安全
	设计模式	Empirical Analysis[183]	代币、授权、预言机、随机性、投票、时间约束、终止、数学、分叉检查
		Security Patterns[184]	检查-效果-交互、功能紧急停止、敏感任务减慢、速率限制、资源互斥、余额限制
		SRE_BBC[185]	事务排序依赖、时间戳依赖、异常处理、可重入处理
	安全模式	Idelberger[186]	利用基于逻辑合约编码替代基于过程性合约编码，保证实现和需求间语义一致性
		Anastasia[187]	将合约转化为有限状态机，利用形式化验证检查合约行为是否满足设计要求属性
		Ahmadjee[188]	将漏洞映射至通用缺陷列表 CWE，识别设计漏洞，利用技术债务估算漏洞后果
		Park[189]	利用时序逻辑表达合约需求属性，并利用定时计算树逻辑 TCTL 对模型进行验证
实现安全	安全开发	OpenZeppelin[190]	提供基于角色的权限控制方案和 SafeMath 安全运算等功能，防止合约代码溢出问题
		Aragon OSx[191]	提供自主访问控制权限控制方案，使用 Mythril 和 Soylent 等工具审核合约内容
		Liu 等人[192]	描述以太坊智能合约中的交易恢复语句，辅助开发人员安全利用事务恢复语句开发
	安全模板	Mao 等人[193]	采用 Char-RNN 模型生成合约基本功能代码，并将生成的代码嵌入到用户界面块
		Tateishi 等人[194]	利用文档模板和受控自然语言 CNL 自动化生成可执行的智能合约
		Qin 等人[195]	利用通用字典 CoDic 将自然语言合约转换为通用机器代码，避免各方间歧义
		Hamdaqa 等人[196]	提供常用功能实现模板，建模和生成可部署到多区块链平台功能性智能合约代码
测试安全	形式化验证	Abdellatif 等人[197]	利用行为交互优先级 BIP 对合约行为进行语义建模，验证安全属性，发现恶意操作
		Bhargavan 等人[198]	将智能合约源码和 EVM 字节码翻译为函数式编程语言 F * 进行程序交互式验证
		Hirai 等人[199]	用 Lem 形式化智能合约语义，利用交互定理证明器 Isabelle/HOL 证明合约安全属性
	代码分析	Tsankov 等人[200]	对合约依赖关系图进行符号化分析，提取精确语义信息，检查其遵从性和违反模式
		Jiang 等人[202]	基于智能合约 ABI 规范生成模糊输入，定义 oracle 使用模糊测试技术检测安全漏洞
	安全审计	Zhou 等人[204]	逆向工程将 EVM 字节码重构为高级伪代码，发现合约意图和行为，完成安全审计
部署安全	BUG 奖励	Breidenbach 等人[205]	利用 N-of-N 版本编程漏洞利用技术、可调整奖励值和承诺鼓励理性黑客披露漏洞
	安全监视	Nikolic 等人[206]	实现对 greedy contracts、prodigal contracts 及 suicidal contracts 三种追踪漏洞合同检测
		Grossman 等人[207]	通过监视以太坊执行轨迹中的有效无回调对象 ECF 来识别合约漏洞
	事后分析	Chen 等人[208]	提取合约用户账户和操作代码特征，建立分类模型检测智能合约实现的庞氏骗局
		Chen 等人[209]	利用跨图分析实现合约攻击取证和运行异常检测，以此检测合约运行状态
		Li 等人[210]	利用指令集描述程序操作、构造合约字节码，对合约进行高效重新编译和重新部署

4.5 共性安全服务

共性安全服务是为区块链系统提供一系列基础安全服务的集合，涵盖身份管理、权限管理、隐私保护以及跨链安全等服务.

4.5.1 身份管理

区块链系统在提供分布式、去中心化应用服务同时，需要对区块链交互的各参与实体身份进行有效管理. 在中心化服务中，数据统一由可信中心机构进行集中化管理. 而在分布式的区块链中，为实现分布式管理目标，需将交互数据在网络进行公开，并在特定节点间利用共识机制对数据校验，达成数据一致性，故区块链需要实现安全、高效身份管理，满足区块链参与实体身份标识、身份认证和身份隐藏需求，身份管理技术脉络如图 13 所示.

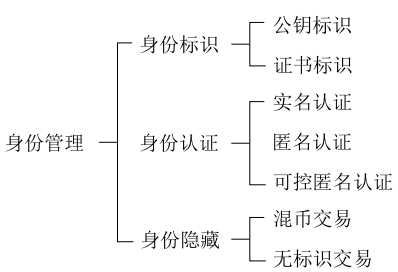


图 13 身份管理技术脉络

(1) 身份标识

身份标识是用于标识区块链系统中参与实体身份的机制，主要利用公钥密码技术进行实现. 公链一般使用公钥进行身份标识，如比特币利用椭圆曲线密码算法生成实体身份标识，该标识被称为比特币地址，长度 160 bit，利用 SHA256 和 RIPEMD160 对实体公钥进行两次哈希计算得到，利用该标识实现对链上数据资产标定与确权. 与比特币不同，以太坊平台采用 Keccak256 生成实体地址，门罗币则通过生成两对公钥-私钥对进行实体身份标识，利用密钥派生机制实现多密钥管理. 在联盟链一般使用证书标识身份，提供更强监管能力，如 Hyperledger Fabric、Corda 通过 X.509 证书实现实体身份标识.

(2) 身份认证

身份认证是综合利用第 3.1.1 节中数字签名算法来确认区块链中参与实体身份的机制，验证实体是否具有相应数据操作、访问权限，涵盖有实名认证、匿名认证、可控匿名认证. 由于公链更加强调对参与实体身份的隐私保护，一般为实体用户提供匿名身份认证，在整个身份管理交互中没有第三方可信机构参与，没有身份准入机制且身份掌握在实体自身手中. 而在联盟链场景更加强调对实体身份有

效监管，如 Fabric、趣链、Corda、FISCO BCOS 等区块链使用 CA 机构颁发证书作为标识、利用实体私钥签名验证实体身份，实现强监管条件实名身份认证. 针对实名身份认证带来的隐私泄露问题，又引发围绕可控匿名认证机制的研究. 在可控匿名认证机制中，对联盟链监管方来说能识别出实体用户真实身份，而普通参与实体无法识别其它用户真实身份. 如 Fabric0.6 提出基于两级安全证书体系的可控匿名认证方案，其中证书体系由注册证书 ECert 和交易证书 TCert 共同组成，注册证书 ECert 为实名证书，再由注册证书 ECert 派生出交易证书 TCert，达到前台匿名、后台可监管身份管理需求. 交互过程使用不同 TCert 证书，故对普通观察者无法发现用户身份. 但该方案存在证书规模大、证书可链接性等问题，为此 Fabric2.0 采用 Idemix 机制，利用盲签名和零知识证明实现可控匿名认证，保证身份验证过程无需暴露身份信息. FISCO BCOS 引入群签名机制实现可控匿名认证，采用支持群成员撤销和短签名特性的 BBS 04 方案，联盟链监督方能通过签名恢复实体证书.

(3) 身份隐藏

在身份隐藏研究方面，简单匿名认证只能保证区块链实体身份弱匿名性，通过交易数据关联分析能分析出用户身份特征，难以保证区块链参与实体真正身份隐私，故引入身份隐藏实现区块链数据交互过程身份信息保护，主流身份隐藏技术包括混币交易和无标识交易技术. 混币交易技术通过将多个交易汇聚在一起，使得外部观察者无法确定真正的交易发起人和接收人，如 Mixcoin 协议、CoinShuffle 方案. 为提高混币方案交互效率，还可采用 DC-net (Dining Cryptographer net)改善加密货币的匿名性能. 无标识交易则利用零知识证明防止他人收集和利用交易信息. 文献[211]结合区块链系统交易模型特点对身份管理技术进行了较为系统的综述，故本文不对技术细节进行过度阐述.

综上所述，现有区块链身份管理技术随着密码技术的不断发展，呈现百花齐放的发展状态. 但现有研究大多集中在对单一区块链系统的身份管理研究，缺乏对跨链、链上链下协同等跨安全域场景下身份兼容性方面的研究，且如何有效提高身份管理便捷性、身份信息存储安全性也是研究重点.

4.5.2　权限管理

权限管理用于为区块链用户授予相应资源访问或操作的权限，如图 14 所示，按对区块链各层级影响范围为维度对权限进行划分，可分为链级权限、合约权限、账号权限及节点权限.

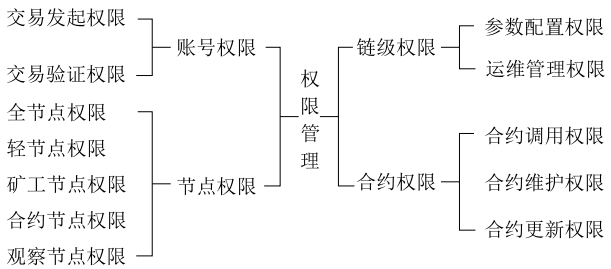


图 14　区块链权限类型

(1) 链级权限

链级权限指对整个区块链平台运行带来影响的相关权限，受该权限保护的区块链资源一般在区块链创世时就稳定存在于区块链，其访问需受到足够强度保护，否则容易带来系统功能性故障，对整个区块链产生破坏，如区块链需要所有参与节点保持一致参数配置集合、对区块链部署运维人员的权限管理等. 由于公有链面向应用场景是完全去中心化网络用户，故公有链一般无需设置对区块链部署运维人员的权限管理机制，但需各节点具备自身区块链系统参数配置权限管理能力. 而在联盟链和私有链许可链场景，面向组织、机构用户存在对部署运维人员实现统一权限管控需求，提高区块链安全性. 如 PlatONE 链采用基于角色访问控制模型来实现对链级权限管理，将系统角色分为系统管理者、合约部署者、链管理者及节点管理者等角色，按节点管理、合约管理、数据管理等业务功能为资源实现区块链业务权限管控. Hyperchain 链同样采用基于角色访问控制模型，包括链级管理员、节点管理员、合约管理员及普通用户，通过联盟自治框架 CAF、节点级访问控制等方式，实现多层级管理和限制，为系统及账本数据管理提供全方位安全保障. 合约权限是指对区块链智能合约对应业务接口调用资源权限，受该权限保护资源包括智能合约维护与调用，限制用户对智能合约代码更新、智能合约状态变更以及智能合约代码维护.

(2) 合约权限

在合约权限管理中，可利用特定代表相应智能合约的标识符，利用黑名单或白名单机制来对相应合约用户提供接口级整体保护. XuperChain 链提出基于访问控制列表 ACL 合约权限管理方法，用于对合约方法读写做控制，包括系统合约和用户合约. 如果把合约账号当作股份制公司，那么 ACL 便是公司

股东投票机制，ACL 可规定合约账号背后各“股东”账号权重，只有当“股东”签名权重之和大于设定阈值时操作才会生效. 另外，在编写智能合约时，可通过指定合约函数可见性来控制什么函数可以被哪类用户实现调用. 通过该方式可有效实现对智能合约关键部分代码函数访问控制. Rust 智能合约可利用 pub fn、fn 以及 pub(crate) fn 合约属性分别实现可外部调用与仅能内部调用合约接口. FISCO BCOS 引入“合约粒度”权限治理，用户不仅可管理“区块链”和“合约”维度权限，还可通过设置“白名单”和“黑名单”策略来管理具体合约中函数方法调用权限.

(3) 账号权限

账号权限指在区块链账本主体，除智能合约一般还包括区块链账号. 账号权限核心是保护区块链账本账号，使其不被随意使用，既包含交易发起方验证，又包含发起方是否有权向交易接收方发起操作验证. 该权限管理主要是通过前文所总结的密码技术，实现对交易行为权限控制. 另外，还有一类研究从保护账号对应链上数据可访问性角色实现权限管控，如结合区块链与属性加密机构实现对链上数据资源的细粒度访问控制，利用 ABE 来表达授权逻辑语义，灵活定义数据删除和编辑访问控制策略. 链级参数、合约接口以及系统账号是上述三种类型权限保护对象，这三类保护对象皆为区块链系统层面全局权限概念，在不同区块链节点上以一致化形式部署运行.

(4) 节点权限

节点权限指区块链中作为参与者单节点在与区块链服务进行交互中被受控访问的接口资源权限. 理论上一个区块链中的节点只需要满足特定协议，可用不同方式来实现，也可对客户端提供不同接口. 节点权限所保护资源对象就是实现区块链节点协议服务器端对其客户端暴露接口，确保接口不可被随意访问，如蚂蚁链利用访问密钥 AccessKey 实现对区块链接口调用权限管理，当程序在调用蚂蚁区块链平台、蚂蚁区块链产品 OpenAPI 或调用功能扩展 SPI 接口时，需要在程序中配置一组约定好有权限的访问密钥 AccessKey，才能实现访问.

综上所述，现有权限管理已能够从不同层面为区块链系统提供权限支持. 但现有方法大多为静态权限管理方法，随着区块链应用规模不断增长，存在权限控制不够灵活、动态权限管理效率低下、权限泄露风险难发现、跨链访问权限兼容性弱等问题，可结合属性、风险、信任等要素，进一步扩展权限管理能力.

4.5.3 隐私保护

为了达成共识，区块链节点需公开链上交易信息，这给用户带来严重隐私问题. 区块链隐私标准定义[212]是指仅与个人利益相关且不需要强制公开的个人信息及个人领域. 隐私主体是自然人，客体是个人信息和个人领域，内容指特定个人对信息和领域的秘而不宣，不愿第三方探知和干涉的事实和行为. 区块链系统隐私主要涉及链上数据隐私、网络交互隐私.

在链上数据隐私研究方面，主要包括在区块链系统中与用户个人相关的数据信息，包含交易数据、账户信息、用户身份、智能合约等. 第 4.5.1 节提及的身份隐藏技术是实现用户交易、身份隐私保护的重要手段. 另外，通过综合利用零知识证明、差分隐私、环签名、盲签名、同态加密、安全多方计算等密码学技术与手段也可有效对链上隐私信息进行保护，同时兼顾链上数据的隐私保护与可验证性，在第 3 节区块链密码支撑技术部分对相关方法有详细介绍. 文献[213]从区块链交易内容隐藏、隐藏交易验证和隐藏交易监管三个方面对区块链交易内容隐私保护技术进行了较为全面的综述.

在网络交互隐私研究方面，在开放网络环境中攻击者能够利用远程旁路攻击来探测交易内容及用户身份信息，破坏交易匿名性、不可连接性. 同时，攻击者可通过控制区块链节点利用网络扫描技术、拓扑探测技术等获取网络信息用于攻击. 现有研究主要利用网络信息隐藏技术保护区块链系统网络层信息匿名性和隐蔽性，避免攻击者将 IP 地址与链上交易建立关联. 常用方法包括可信第三方转化、混合网络、洋葱路由、大蒜路由等机制在网络交互方间实现加密信息传输. 另外，为实现网络交互隐私数据的保护，研究人员还提出通道隔离机制来保证数据仅对通道内节点可见，如闪电网络技术、雷电网络技术、多通道隔离技术等. 闪电网络是建立在比特币网络上的第二层支付协议. 由于闪电网络支持链下交易，利用链下网络通道实现高频小额度交易，区块链上不记录完整交易信息，它提高了比特币平台的吞吐量，扩展了比特币网络的可扩展性和隐私保护能力. 雷电网络是建立在以太坊网络上的第二层支付协议，其链下交易机制与通道机制与比特币闪电网络原理类似. 多通道隔离技术将区块链中不同节点归

属到不同网络交互通道之中，每个通道独立维护一套完整区块链账本，利用身份管理和权限管理机制来控制实现对通道的访问控制，不同的通道之间无法进行网络的直接交互，从而有效地保护通道内部网络交互数据的隐私安全. 但无论是闪电网络、雷电网络还是多通道隔离技术，底层交互都比较复杂，应用的难度成本较高，难以进行完备的安全性分析，可能存在潜在的安全风险.

另外，为扩展区块链计算隐私保护性能，将可信计算与区块链结合是重要研究方向[214-216]. 如图 15 所示，将敏感计算部分从区块链移动至可信执行环境，区块链进行链上非隐私交易计算，可信执行环境进行隐私交易计算方式提高计算的隐私安全.

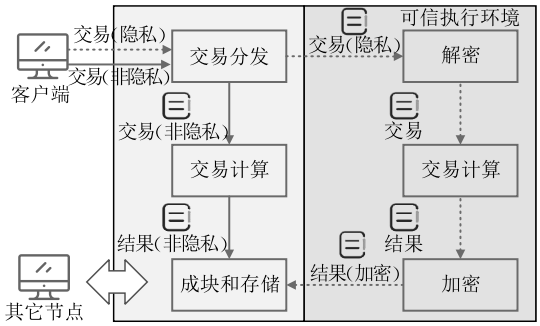


图 15　基于可信执行环境的区块链隐私保护

还有一些研究[217]利用专用硬件保证区块链关键隐私计算环境安全. 但目前总的来看将敏感计算操作从区块链转移到 TEE 并非没有问题，目前的 TEE 硬件平台内存有限，而区块链数据库的内存较大. 这种内存限制使得在 TEE 中运行完整的区块链软件不切实际、成本过高. 而若仅利用 TEE 进行关键的计算环节，则在 TEE 内部运行的程序还需要依赖可信区域之外的软件从区块链数据库中获取数据，该过程势必会进行额外的外部通信，带来额外隐私计算风险. 如何兼顾区块链与 TEE 协同的安全性与可用性，还需不断深入研究.

4.5.4　跨链安全

随着不同区块链技术不断演进，公有链、联盟链及私有链等多类型区块链大量共存，由于各区块链存在独立性，在不同链间实现价值交换和信息交互面临较大挑战，价值和数据孤岛现象凸显. 跨链技术是打通同构链或异构链，实现不同类型区块链互联互通的技术方法，能有效提高区块链系统性能，是扩展和连接区块链的桥梁，其安全性是不容忽视的重要问题. 如表 9 所示，目前主流跨链技术[218]包括公证人机制、侧链/中继、哈希锁定.

表 9　跨链技术对比

方　案	原　理	优　势	不　足
公证人机制	公证人作为不同区块链间信任中介审验跨链交易	具有较高安全性和可靠性	公证人处存在安全和性能瓶颈
侧链/中继	跨链交易在主链和侧链之间进行转移处理	单侧链模式实现跨链交易高效、降低交易时间和费用	需跨链多签、技术实现复杂，当涉及多侧链，中继过程复杂耗时
哈希锁定	跨链交易信息通过哈希锁定链上	跨链资产交换安全、隐私且效率高	不适用复杂的跨链交易，应用场景受限

在区块链间进行安全互操作最简单方法是使用公证人方案[219]. 公证人模式中，受信任个人或团体被用来向一个区块链宣布另一个区块链上发生的行为，并确保该声明正确. 这些组既可自动侦听和响应事件，也可在请求事件时侦听和响应事件. 如 Ripple 提出跨链价值传输技术 InterLedger 协议，允许不同区块链间通过第三方公证处作为中介来实现货币兑换，利用密钥算法为不同区块链和第三方公证处间建立资金托管关系，当所有跨链操作参与方达成一致性共识时，交易才能顺利、安全执行，降低了跨链交互门槛，具有较高安全性和可靠性，但公证人处存在安全和性能瓶颈.

侧链/中继模式中侧链不是专指特定区块链，而是指所有遵守侧链协议的区块链，是相对区块链主链的概念. 侧链是一种协议，允许数字资产从区块链主链安全转移到其他区块链，也可从其他区块链安全转移回主链. 侧链目的是实现双向楔入，使数字资产可在主链和侧链间传输. 侧链协议意味数字资产不仅可在主链流通，还可在其他链上流通. 侧链/中继模式本质特征是注重区块链结构和一致性特性. 一般来说，主链不知道侧链存在，但侧链一定知道主链的存在，双链不知道中继存在，但中继一定知道双链存在. 如 Pegged Sidechains、Plasma、Minimal Viable Plasma、Plasma Cash、Loom 等. Guo 等人[220]提出一种安全多侧链系统，通过同时转移资产来提高吞吐量，并通过实现防火墙属性来保证资产在多链转移的安全性. Gai 等人[221]提出基于 BFT 的侧链框架 Cumulus，利用一种名为等待证明(Proof-of-Wait)的新型加密分拣算法，公平地选择侧链节点，以高效和分散方式与主链进行通信，设计了两步提取协议，确保可安全收集资产回到主链，而不依赖于 BFT 委员会. Garoffolo 等人[222]提出一种类似比特币的区块链系统结构，侧链节点直接观察主链，而主链节点只观察来自侧链维护者经过加密验证的证

书，允许在不知道内部结构情况下创建和通信不同类型侧链. 单侧链模式实现跨链交易高效、降低交易时间和费用，但需跨链多签、技术实现复杂，当涉及多侧链，中继过程复杂耗时.

哈希锁定是设置不同链间互操作的触发器，通常使用公开随机数哈希. 它起源于比特币闪电网络，关键技术是可撤销序列到期合约 RSMC 和哈希时间锁合约 HTLC. 如 Alice 和 Bob 间可达成一个协议来锁定 Alice 拥有 BTC，在时间 T 前，如果 Bob 可给 Alice 展示一个合适 R，使 R 哈希值等于之前约定值，Bob 则可得到该 BTC；若时间 T 时，Bob 不能提供正确 R，该 BTC 自动解冻返回 Alice. 哈希锁的使用可以实现跨区块链资产交换，但不能实现跨链资产转移，也不能实现跨链契约，应用场景较为受限. Sun 等人[223]将公证人方案与哈希锁定结合，引入奖惩机制避免恶意公证人带来的安全威胁，提高容错能力. Dai 等人[224]提出基于改进哈希锁的跨区块链多跳交易模型，设计一种公证多重签名方案，解决传统模型缺乏信任的问题，并基于有向图的环检测方法设计跨区块链多跳交易环，实现跨区块链安全交易. Deng 等人[225]结合侧链技术和哈希锁定技术，建立了一个新的区块链作为第三方交易平台，从而保证不同区块链之间的信任传递. 哈希锁定模式下跨链资产交换安全、隐私且效率高，但不适用复杂的跨链交易，应用场景比较受限.

5 区块链风险评估与安全监管

5.1 安全风险评估

为保障各应用领域区块链安全质量，区块链正式上线运行前需进行全面安全风险评估，对区块链安全风险进行全方位、立体式评估、分析，确保区块链安全可靠. 由于区块链系统复杂性，其安全风险评估与分析需采取比传统系统更全面视角. 为避免区块链潜在风险，最有效方法是对其进行严格安全评估，特别是政府部门使用区块链作为国家基础设施，需满足更高安全要求. 常用的区块链系统安全风险评估方法如表 10 所示.

Morganti 等人[226]利用收集的区块链漏洞和安全事故信息，构建威胁列表基于 NIST SP-800-30 方法对区块链系统进行定性的安全风险评估，让使用者和设计者对区块链系统存在的风险有一个清晰的认识. 叶聪聪等人[227]提出根据区块链结构来评估

表 10 安全风险评估方法对比

评估方法	评估依据
文献[226]	区块链漏洞、安全事故信息构建的威胁列表
文献[227]	区块链结构到达稳定状态的攻击状态的概率
文献[228]	区块链威胁、漏洞对资产管理和业务运行影响
文献[229]	区块链系统的技术组合体系和算力
文献[230]	区块链系统的匿名性
文献[4]	区块链系统的分层体系架构
文献[231]	区块链系统的加密技术标准
文献[232]	区块链软件容错、资源控制、备份恢复、审计等
文献[233]	区块链核心机制、认证加密、安全运维管理
文献[234]	区块链技术、数据、应用、运营

和检测安全性的方法，通过模拟区块链运行过程中诚实矿工和攻击者行为，分析不同状态 51%攻击成功的概率，当概率达到某一阈值时，将向区块链系统用户发送提醒，通过延长交易确认时间来降低攻击风险. Gourisetti 等人[228]提出基于经验范式的网络安全漏洞缓解框架 CyFEr，将区块链脆弱性评估问题转化为多标准决策分析 MCDA 问题，利用等级权重方法评估给定区块链应用或用例中区块链节点和网络安全态势. 秦超霞等人[229]提出区块链安全风险评估方法，根据区块链技术体系架构建立区块链可信计算基，结合层次分析和配对比较的安全敏感性分析方法，为各安全风险影响因素分配权重，从技术架构和算力两方面量化区块链安全风险. 针对区块链匿名性评估问题，Lu 等人[230]提出基于贝叶斯网络的匿名性评估模型 AABN，采用精确推理和近似推理方法对 MIX 匿名网络匿名性进行定量评价，并对 MIX 匿名网络在不同输出策略匿名性进行评估实验. Homoliak 等人[4]提出区块链安全参考体系结构 SRA，采用类似于 ISO/OSI 的堆叠模型，描述各种安全和隐私方面性质和层次结构，包含区块链的网络层、共识层、复制状态机层以及应用层，通过将 SRA 结构嵌入威胁-风险评估标准 ISO/IEC 15408 来实现对区块链的安全风险评估. 根据现行联邦信息安全管理法案 FISMA 要求，联邦 IT 项目和使用的区块链平台需满足美国国家标准技术研究院 NIST 的加密标准. Howard 等人[231]从加密标准是否符合安全标准角度对 Ethereum、Hyperledger Fabric、R3's Corda 及 Multichain 四种区块链进行安全风险评估. 一些组织和团体已启动区块链评估规范的开发，如中国区块链评估联盟 CBEA 推出《区块链及分布式账本信息系统分级评估规范》. 但上述工程并未将分级保护标准应用于区块链安全评价规范的制定. Wang 等人[232]以中国等级保护 2.0 三级标准为例，提出区块链通用安全评价规则，以确

保区块链能满足国家作为关键基础设施建设的需求.从区块链点对点网络、分布式账本、智能合约系统和共识机制等核心技术角度提出和分析评估要求和具体实施建议,并对比特币、以太坊和 Hyperledger 等主要平台评估结果汇总和分析.结果显示,目前区块链在软件容错、资源控制、备份与恢复等方面已能满足评估项目要求,但在安全审计、访问控制、识别与认证、数据完整性等方面还需进行改进,以满足国家安全、经济发展和人类生活等重要领域要求.Mallah 等人[235]提出将区块链技术风险与应用生态风险相结合的风险评估方法,依据漏洞信息确定其优化级,分析漏洞被成功利用概率和对网络影响来估计漏洞风险,通过突出显示代表最大累积风险的攻击媒介来揭示可作为安全设计部署的适当对策,以避免网络攻击.针对区块链基础设施面临的安全风险,魏亮等人[233]构造包含区块链基础设施核心机制、传统认证加密、安全运维管理 3 个大安全领域、14 类安全评估指标的风险评估体系,综合评估区块链基础设施安全风险应对能力.何宝宏等人[234]将区块链安全风险划分为技术、数据、应用以及运营四个维度进行考虑分析.

5.2　安全监管与治理

区块链安全风险既来自于区块链技术自身的安全缺陷,也来自于相关数据、业务、流程、应用缺乏有效监管.由于区块链是一种“只增不删”的共享总账系统,链上存储的数据信息具有不可篡改、无法替换、难以删除的特性.特别是公有链平台由于没有准入机制,数据上链权限面向所有用户开放,用户可向区块链写入任意信息,并借助区块链网络实现快速传播,该情况容易造成敏感、违法信息上链传播,为社会治理带来安全隐患.随着公有链功能扩展和用户数量增加,非法数据内容的写入滥用已成为各公有链共性问题,该行为带来问题主要包括侵犯版权、恶意软件传播、侵犯隐私、传播政治敏感内容、传播有害信息等.

如表 11 所示,区块链安全监管与治理包括区块链态势监管和区块链内容治理两个维度.区块链态势监管主要用于监控区块链系统运行的整个态势信息.针对去中心化数字加密货币可监管性带来的困难,张健毅等人[236-237]提出了一种可监管数字货币模型,采用双链结构设计,联盟链作为共识核心参与收集确认交易,决定系统状态,加密存储完整交易信息.联盟链参与者通过秘密共享保证用户交易数据隐私性,也可通过投票完成对交易内容解密,来实现可控匿名.Xue 等人[238]提出兼具隐私和监管功能的区块链交易模型,使用概率加密实现对区块链交易真实身份的隐藏,使用承诺方案和零知识证明技术实现对交易隐私保护,保证交易合法性验证.监管机构使用加密技术可在不存储用户信息情况下对区块链交易进行监管,大大减轻存储、计算和密钥管理压力,且不依赖特定共识机制,可作为独立模块使用.Xiao 等人[239]提出加密货币混合服务 RBSmix,通过盲签名防止攻击者链接输入和输出地址,通过阈值秘密共享算法、加密技术和监管团队,结合投票思想,跟踪非法地址资金来源.Li 等人[240]提出基于可追溯两层身份结构的区块链交易原型,将基于个人 CA 身份与匿名地址结合,在不集中保存交易数据情况进行申诉,在保护隐私同时可对交易进行监管,并通过链下交易确认协议,建立基于智能合约的链上监管机构.Li 等人[241]将 ElGamal 加密和零知识证明结合,保证审计票据真实性,使监管机构在不打开承诺情况下,实现对交易隐私数据可靠监管,并采用多基分解方法提高监控器解密效率,兼顾区块链安全性和可审计性.区块链内容治理主要用于链上错误、恶意、违规数据的治理.针对可编辑区块链问题,Marsalek 等人[242]提出可校正区块链体系结构,使用共识强制投票机制,对数据更正请求进行分散决策,应用更正信息存储在第二链中,确保仍可成功验证已更正链,支持任意数据校正.Ateniese 等人[243]利用变色龙哈希函数代替区块链哈希函数实现可编辑区块链,它允许在给定 Secret Trapdoor 信息情况下有效确定哈希碰撞,从而在不改变外部哈希函数和不破坏哈希链路完整性的条件下实现区块链数据的物理修改.但该方法只是进行区块链级的修改,在修改过程中要完整替换整个待修改区块,存在修改粒度较粗、缺乏对内容有效验证以及可控性隐患.Politou 等人[244]提出一种可变交易区块链的数据修改机制,支持交易级粒度的修改,但并不真正修改区块链上的物理数据,本质是追加新数据,在后续区块链生成新活跃交易,但该方式由于并未真正更改链上数据,故没有办法清除链上的有害信息.Deuber 等人[245]采用基于共识的投票机制实现链上数据修改,当收集足够多选票时,在链上执行操作,利用双哈希链结构确保区块间链式结构完整性,并为编校后的区块链提供公共可验证性和问责性.另外,为了实现区块链内容治理,还可采用数据过滤技术来避免虚假、敏感和有害等不良信息上链,如基于文本检测的数据过滤、基于经济成本的数据过滤

等[246].还可通过将加密数据上链,仅向授权用户和应用开放解密密码或利用链上链下相结合的数据管理技术,实现链上数据可控管理.

表 11 区块链安全监管与治理方法

类型	方 法	核心思想
区块链	以链治链	用区块链技术治理区块链及应用
态势	链上链下协同	用链下决策机制提供链上紧急管理能力
监管	交易追溯分析	追溯区块链交易行为、发现非法交易
区块链	共识治理	基于共识的投票机制实现链上数据修改
内容	变色龙哈希	利用变色龙哈希实现可编辑区块链
治理	数据过滤	非法文本、图像、视频检测发现技术

5.3 技术标准与规范

区块链在金融、政务、能源、物联网等领域均有广泛应用前景,但在技术实现和标准规范方面还存在许多不完善之处,需进一步探索完善区块链安全技术标准与规范.表 12 为区块链安全在国际标准化研究领域的相关工作.2020 年,国际标准化组织 ISO 发布《区块链和分布式账本技术 隐私和个人可识别信息保护考虑》[247]明确区块链中涉及个人隐私保护的技术规范,指导隐私风险缓解实践.发布《区块链和分布式分类账技术 数字资产保管人的安全管理》[248]对用户安全管理要求进行规范.ISO 立项《区块链和分布式账本技术 智能合约安全良好实践和问题概述》[249],对智能合约的安全开发实践进行指导.2019 年,国际电信联盟 ITU 发布首个区块链安全标准《分布式账本技术的安全威胁》[250],从攻击目标、手段、影响及可能性维度为区块链安全实践提供指导.随后发布《云计算区块链即服务的功能需求》[251],同步开展区块链即服务安全标准制定工作,涉及威胁分析、安全防范等内容.同时,ITU 对区块链安全服务参考框架、安全测评、安全保障等领域相关标准均已立项,用于描述分布式账本技术各类安全、测评以及保障要求,指导各类安全隐患应对方法.

表 12 区块链安全国际技术标准与规范工作

时间	组织	标准名称
2019	ITU	分布式账本技术的安全威胁
2020	ISO	区块链和分布式账本技术隐私和个人可识别信息保护考虑
2020	ISO	区块链和分布式分类账技术数字资产保管人的安全管理
2020	ISO	区块链和分布式账本技术智能合约安全良好实践和问题概述
2020	ITU	云计算区块链即服务的功能需求
2020	ITU	智能合约安全管理要求
2020	ITU	使用分布式账本技术进行分散身份管理的安全指南
2020	ITU	分布式账本技术的安全框架
2021	ITU	分布式账本技术的安全保证
2023	ITU	区块链即服务(BaaS)安全性指南

表 13 为区块链安全在国内标准研究领域的相关工作.2023 年,全国信息安全标准化技术委员会发布了《信息安全技术区块链信息服务安全规范》[252]、《信息安全技术区块链技术安全框架》[252-253]2 个国家标准.区块链信息服务安全规范对围绕区块链上信息内容传播中安全风险隐患,对区块链信息服务提出安全要求和测试评估方法,适用于区块链信息服务提供者建立健全相应信息安全机制,并配备相应的技术保障措施,开展区块链信息服务安全建设,也适用于对区块链信息服务安全评估.区块链技术安全框架围绕区块链技术所面临的安全风险,分为区块链密码支撑、安全功能组件、安全管理运行和区块链角色四部分制定了技术安全标准框架.2020 年,工业和信息化部发布《区块链技术架构安全要求》[254],规范区块链在共识、合约、账本等技术方面安全要求.随后,全国区块链和分布式记账技术标准化技术委员会相继开展《区块链和分布式记账技术 参考架构》[255]、《区块链和分布式记账技术 物流追踪服务应用指南》[256]、《区块链和分布式记账技术 系统测试规范》[257]、《区块链和分布式记账技术 应用程序接口 中间件技术指南》[258]、《区块链和分布式记账技术 智能合约生命周期管理技术规范》[259]等标准研制,均涉及区块链安全防护和检测相关内容.同时,与区块链安全相关的行业标准也陆续发布,中国通信标准化协会出台《电信网和互联网区块链基础设施安全防护要求》[260]、《区块链技术架构安全要求》[261],规范区块链基础设施安全开发运营.但总体来说,区块链技术目前尚未成熟,技术不断演化,许多安全概念与规范还未形成有效共识,技术标准与规范工作整体滞后,需不断完善.

表 13 区块链安全国内技术标准与规范工作

时间	组 织	标准名称
2019	陕西省市场监督管理局	区块链安全测评指标体系
2020	工业和信息化部	区块链技术架构安全要求
2020	中国通信标准化协会	区块链技术架构安全要求
2020	金融标准化技术委员会	金融分布式账本技术安全规范
2021	信息安全标委会	区块链信息服务安全规范
2021	信息安全标委会	区块链技术安全框架
2022	上海市市场监督管理局	区块链技术安全通用要求
2022	密码行业标委会	区块链密码应用技术要求

6 研究挑战与展望

6.1 区块链安全面临的主要挑战

区块链安全性研究不单单是技术性的,还需要综合考虑业务、组织和操作等相关管理问题.区块链

安全面临的重大挑战主要体现在以下 4 个方面：

(1)区块链密码支撑研究任重道远：区块链系统中密码技术的重要性不言而喻，是区块链核心安全机制，用于保护安全性、完整性、可靠性. 随着区块链逐渐演化为一种分布式的计算范式，需要依靠密码技术实现愈加复杂的功能，密码技术研究需要结合区块链涌现的新特点不断地适应演化，如密文计算、密文检索、隐私保护、身份验证、共识机制等均需要其支持. 涉及的密码技术也越来越复杂，需要大量额外的计算和存储资源来实现，在实现区块链系统时迫切需要综合考虑资源的使用和成本效益，以确保方案的可持续性、可扩展性，设计更加适用于区块链的专用优化算法. 同时，由于区块链系统的匿名性和去中心化特点使得法规和监管方面的问题日益突显，密码技术需要在保证安全性的前提下提高系统的可监管性.

(2)区块链网络运行机制存在漏洞：区块链是技术的集成创新，与集中式网络架构不同，区块链不依赖单一网络中心存储、处理数据，带来避免单点故障、提高抗打击能力的优势. 但其安全防护是系统工程，涉及多节点、多方面安全因素共同影响. 需通过互相配合、各司其职来共同维护分布式区块链运行的安全与稳定. 在不同技术层面，广泛存在算法漏洞、协议漏洞、实现漏洞、使用漏洞及系统漏洞等多种类型安全漏洞，攻击者通过利用这些安全漏洞能够破坏区块链安全性、完整性与可用性，颠覆区块链所构建的信任基石. 另外，由于为了在分布式区块链环境下不同节点间达到存储和计算一致性共识，区块链网络的所有数据都会向所有参与节点公开，对于攻击者也可通过网络交互获取链上数据、通过攻击薄弱节点漏洞窃取链上执行情况，带来安全问题，极大地限制了区块链的使用范围和应用领域.

(3)链上链下的可信交互风险加重：区块链系统凭借其共识机制和密码学相关技术能够保证链上数据的真实性和可靠性，但若仅仅将区块链当作一个孤立运行的信息系统，而不与其它信息系统或数据源进行联通，将难以在现实的环境下真实发挥区块链的效能，但目前研究缺乏对链下数据源的安全保障机制. 一旦不可信的数据源接入区块链系统，并提供上链数据支持，将会给整个区块链系统带来严重的数据安全隐患. 故需要对链外数据进行可靠的数据源认证、数据格式转换、数据清洗等一系列可信数据处理后才能上链，有效避免链下数据的篡改和伪造风险，如何有效的保障上链数据的正确性、隐私性是区块链安全技术发展的重要挑战.

(4)区块链安全监管面临严峻挑战：区块链系统结构与运行方式决定了区块链上存储的数据信息难以通过传统的方式进行篡改，加之区块链系统具有一定匿名性，各类违法有害信息一旦被写入区块链，不但可以借助区块链系统实现传播且难以清除、修改，带来了违法有害信息的监管难题. 同时，基于区块链技术实现的数字加密货币为黑市交易、勒索病毒、贩毒洗钱等违法犯罪活动提供了一条资金交付通道，同时也存在损害各国的金融主权，影响金融市场的稳定，增加了政府、金融机构的监管难度.

6.2　区块链安全技术的研究展望

(1)区块链密码技术方向

密码技术是区块链安全与稳定运行最基础、最核心保障手段. 但区块链系统所处的是一种分布式网络环境，需要建立面向区块链环境分布式密码算法的密钥管理机制，设计具有可证明安全性的分布式数字签名算法，为用户、节点参与区块链交互提供身份支持. 另外，对于区块链系统所需的隐私保护需求也需要利用密码技术提供支撑，可研究安全高效的环签名、属性加密、代理重加密、多重签名等密码技术设计理论，结合区块链应用保护链上数据存储隐私，可研究同态密码、新型杂凑函数、零知识证明等新型密码技术的设计应用实现链上数据计算隐私保护. 同时，区块链系统随着节点规模的增大、性能要求的增高，需要设计配套的安全高效的分布式密钥协商协议，确保密钥协商安全. 随着量子计算技术的不断发展，对区块链密码系统带来巨大安全威胁和长期使用的安全挑战，需要围绕具有抗量子计算能力的区块链密码技术，抵抗在数据加密、数字签名等方面存在的量子攻击，设计具备抗量子攻击能力的身份认证、安全通信、安全共识协议，且需要考虑抗量子密码算法的安全高效实现与区块链系统传统密码体系向抗量子密码技术系统迁移的解决方案.

(2)网络安全防护技术方向

区块链依靠底层的对等网络在节点之间传播区块数据、达成一致共识. 但目前在区块链系统中还存在“三元悖论”，即安全性、去中心化、可扩展性三种特性难以很好兼备，导致区块链系统在网络上存在性能瓶颈、安全瓶颈. 为更好兼顾区块链系统和应用的安全可信和执行效率，需要设计区块链网络安全架构，确保区块链系统具备较强故障容错性，通过构建新型区块链网络拓扑结构、设计高效数据通信与转发算法，提高对各类网络攻击、安全漏洞的防御能

力,增强底层网络的安全性、可靠性、高效性.针对区块链面临的拒绝服务攻击、女巫攻击、日蚀攻击等网络攻击问题,需要建立对常见网络攻击的安全防护机制,结合真实源地址验证,防止伪造地址攻击,利用入侵检测、安全审计等技术实现对网络攻击的追责溯源机制.另外,当前共识机制安全性还缺乏理论证明,需要针对单链、多链、跨链等不同类型区块链和应用场景,设计定制化、灵活性高、扩展性强的高性能可证明安全共识机制,支持动态节点能够在复杂网络环境下达成共识,构建共识协议安全模型,实现网络异步/半同步及大规模节点环境中同时保障安全性及活性的高性能共识算法和低负载容错网络架构.

(3)链上链下可信协同方向

区块链可保证链上数据在多个参与方间的安全可信流通,但无法确保上链数据来源真实性、完整性,且区块链链上存储资源与计算资源受限,现实应用场景中链上业务运转离不开链下支持,链上链下可信交互成为了"卡脖子"问题.为了确保链上数据链下来源、计算结果真实性,需要研究实现数据可信上链技术,可以将区块链与可信执行环境相结合,利用链上链下的互相验证来保障链下代码和数据计算结果的安全可信,构建高效数据采集环境安全检测机制,链下数据完整性验证机制.同时,为保证区块链智能合约链外输入的真实性,需要研究安全、高效的预言机实现方法,支持预言机的可信动态评估、可信预言机选择和链外输入验证.为了增加区块链系统安全存储能力,研究多模态数据多种类节点链上链相结合的轻量化安全存储方法,实现低时延高吞吐数据管理、支持多模态数据溯源、复杂数据安全检索、多源数据安全共享与协同计算.针对当前区块链系统链上智能合约编程语言发展不够成熟的现状,需要针对区块链平台的特点,不断完善、实现简洁安全的智能合约编程语言,支持合约代码安全性验证分析,实现安全可信的智能合约执行引擎.

(4)安全监管与治理方向

为了保证区块链行业健康发展,加强对区块链及其应用的安全监管研究已经成为行业共识,区块链的安全监管应该涵盖对区块链系统的态势监管和区块链内容监管.为了实现对区块链系统的安全态势监管,需要研究区块链节点的追踪与可视化方法、低时延高安全自适应可监管的链上链下网络通信方案,构建区块链全节点的网络图谱,支持监控链内、链间、跨链节点的运行状态、探测发现异常节点与异常行为.同时,在特定应用场景下能够实现穿透式的区块链监管,结合相应技术实现可监管场景下的数据隐私保护,构建对监管友好的交易隐私保护机制,支持在保护交易参与方身份和交易内容等敏感信息的同时,实现对异常链上交易的识别、追踪与溯源,支持可验可查可监管但敏感数据不上链、隐私数据不泄露场景.为了实现对区块链系统的内容监管,需要区块链系统具备对上链前数据内容的监管审查与上链后数据内容的控制治理能力,可通过设计特定的数据内容快速检测发现与预警技术,及时发现违规信息并通过配合相应安全受控的数据回滚机制来实现不同应用场景、不同类型区块链的分级、分类数据内容治理与管控.

7 总 结

区块链作为一种具有去中心化、公开透明、不可篡改等特征,用于构建新型网络信任关系的重要信息技术,对助力数字经济发展、重塑数据价值流通具有重大意义,由于区块链系统作为数据、资产的载体具备巨大的价值极易成为恶意攻击者的重点攻击目标,传统安全技术难以适用分布式区块链技术架构,针对区块链系统的安全技术研究已刻不容缓.本文在结合区块链业务流程和区块链系统技术框架组成特点基础上,提出一种符合区块链业务特点的安全技术框架,从区块链密码支撑技术、区块链平台安全技术以及区块链风险评估与安全监管 3 个方面总结了区块链安全技术的研究进展,以期对区块链安全研究工作提供启发与借鉴.

致 谢 在此,我们向对本文的工作给予支持和宝贵建议的评审老师和同行表示衷心的感谢!

参 考 文 献

[1] Zavolokina L, Zani N, Schwabe G. Designing for trust in blockchain platforms. IEEE Transactions on Engineering Management, 2023, 70(3): 849-863

[2] Central Government of the People's Republic of China. The 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Outline of the Vision Goals to 2035. 2021(in Chinese)
(中华人民共和国中央人民政府. 中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要. 2021)

[3] Leng J W, Zhou M, Zhao J L, et al. Blockchain security: A survey of techniques and research directions. IEEE Transactions on Services Computing, 2022, 15(4): 2490-2510

[4] Homoliak I, Venugopalan S, Reijsbergen D, et al. The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. IEEE Communications Surveys and Tutorials, 2021, 23(1): 341-390

[5] Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Computing Surveys, 2019, 52(3): Article 51

[6] Mei Qiu-Li, Gong Zi-Hong, Liu Shang-Yan, et al. Research on security mechanism of blockchain platform. Journal of Information Security Research, 2020, 6(1): 25-36(in Chinese)
(梅秋丽，龚自洪，刘尚焱等. 区块链平台安全机制研究. 信息安全研究，2020，6(1)：25-36)

[7] Saad M, Spaulding J, Njilla L, et al. Exploring the attack surface of blockchain: A systematic overview. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1977-2008

[8] Chen H S, Pendleton M, Njilla L, et al. A survey on Ethereum systems security: Vulnerabilities, attacks, and defenses. ACM Computing Surveys, 2020, 53(3): 1-43

[9] Li X, Jiang P, Chen T, et al. A survey on the security of blockchain systems. Future Generation Computer Systems, 2020, 107: 841-853

[10] Wang W, Hoang D T, Hu P, et al. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access, 2019, 7: 22328-22370

[11] Conti M, Kumar E S, Lal C, et al. A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials, 2018, 20(4): 3416-3452

[12] Bhushan B, Sinha P, Sagayam K M, et al. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. Computers & Electrical Engineering, 2021, 90: 106897

[13] Cheng J R, Xie L Y, Tang X Y, et al. A survey of security threats and defense on blockchain. Multimedia Tools and Applications, 2021, 80(20): 30623-30652

[14] Altaf A, Iqbal F, Latif R, et al. A survey of blockchain technology: Architecture, applied domains, platforms, and security threats. Social Science Computer Review, 2023, 41(5): 1941-1962

[15] Yaga D, Mell P, Roby N, et al. Blockchain technology overview. National Institute of Standards and Technology, USA: Technical Report NISTIR 8202, 2018

[16] Wang L, Shen X, Li J, et al. Cryptographic primitives in blockchains. Journal of Network and Computer Applications, 2019, 127: 43-58

[17] Casino F, Dasaklis T K, Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 2019, 36: 55-81

[18] Maxwell G, Poelstra A, Seurin Y, et al. Simple schnorr multi-signatures with applications to Bitcoin. Designs, Codes and Cryptography, 2019, 87(9): 2139-2164

[19] Boneh D, Drijvers M, Neven G. Compact multi-signatures for smaller blockchains//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany, 2018: 435-464

[20] Han J, Song M, Eom H, et al. An efficient multi-signature wallet in blockchain using bloom filter//Proceedings of the 36th Annual ACM Symposium on Applied Computing. 2021: 273-281

[21] Kansal M, Singh A K, Dutta R. Efficient multi-signature scheme using lattice. The Computer Journal, 2022, 65(9): 2421-2429

[22] Valenta L, Rowan B. Blindcoin: Blinded, accountable mixes for Bitcoin. Financial Cryptography and Data Security: FC 2015. San Juan, USA, 2015: 112-126

[23] Green M, Miers I. Bolt: Anonymous payment channels for decentralized currencies//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 473-489

[24] Heilman E, Baldimtsi F, Goldberg S. Blindly signed contracts: Anonymous on-blockchain and off-blockchain Bitcoin transactions//Proceedings of the International Conference on Financial Cryptography and Data Security. Christ Church, New Zealand, 2016: 43-60

[25] Zhang Xue-Wang, Li Zhi-Hong, Lin Jin-Zhao. Privacy protection schema based on fair blind signature and hierarchical encryption for consortium blockchain. Journal on Communications, 2022, 43(8): 131-141(in Chinese)
(张学旺，黎志鸿，林金朝. 基于公平盲签名和分级加密的联盟链隐私保护方案. 通信学报，2022，43(8)：131-141)

[26] Qiao Kang, Tang Hong-Bo, You Wei, et al. Efficient and safe auditable mixed-coin service scheme based on blind signature. Chinese Journal of Network and Information Security, 2020, 6(4): 23-36(in Chinese)
(乔康，汤红波，游伟等. 高效安全的可审计盲混币服务方案. 网络与信息安全学报，2020，6(4)：23-36)

[27] Camenisch J, Drijvers M, Lehmann A. Anonymous attestation using the strong diffie hellman assumption revisited//Proceedings of the Trust and Trustworthy Computing: 9th International Conference. Vienna, Austria, 2016: 1-20

[28] Meiklejohn S, Mercer R. Möbius: Trustless tumbling for transaction privacy. Proceedings on Privacy Enhancing Technologies, 2018, 2018(2): 105-121

[29] Fujisaki E, Suzuki K. Traceable ring signature//Proceedings of the International Workshop on Public Key Cryptography. Beijing, China, 2007: 181-200

[30] Möser M, Soska K, Heilman E, et al. An empirical analysis of traceability in the Monero blockchain. Proceedings on Privacy Enhancing Technologies, 2018, 2018(3): 143-163

[31] Noether S, Mackenzie A, Lab T. Ring confidential transactions. Ledger, 2016, 2016(1): 1-18

[32] Sun S F, Au M H, Liu J K, et al. RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero//Proceedings of the 22nd European Symposium on Research in Computer Security. Oslo, Norway, 2017: 456-474

[33] Malavolta G, Schröder D. Efficient ring signatures in the standard model//Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security. Hong Kong, China, 2017: 128-157

[34] Sun Hai-Feng, Zhang Wen-Fang, Wang Xiao-Min, et al. A robust Byzantine fault-tolerant consensus algorithm against adaptive attack. Acta Automatica Sinica, 2023, 49(7): 1471-1482(in Chinese)
(孙海锋，张文芳，王小敏等. 基于门限和环签名的抗自适应攻击拜占庭容错共识算法. 自动化学报，2023，49(7)：1471-1482)

[35] Tu Bin-Bin, Chen Yu. A survey of threshold cryptosystems. Journal of Cryptologic Research, 2020, 7(1): 1-14(in Chinese)
(涂彬彬，陈宇. 门限密码系统综述. 密码学报，2020，7(1)：1-14)

[36] Ziegeldorf J H, Grossmann F, Henze M, et al. CoinParty: Secure multi-party mixing of Bitcoins//Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. Texas, USA, 2015: 75-86

[37] Dikshit P, Singh K. Efficient weighted threshold ECDSA for securing bitcoin wallet. Asia Security and Privacy. Surat, India, 2017: 1-9

[38] Bisheh-Niasar M, Azarderakhsh R, Mozaffari-Kermani M. Cryptographic accelerators for digital signature based on Ed25519. IEEE Transactions on Very Large Scale Integration Systems, 2021, 29(7): 1297-1305

[39] Feng Q, He D, Luo M, et al. Practical secure two-party EdDSA signature generation with key protection and applications in cryptocurrency//Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications. Guangzhou, China, 2020: 137-147

[40] Zhang Wen-Fang, Sun Hai-Feng, Zhang Yan-Duan, et al. A consensus algorithm for consortium chain with tree based master-slave multi-chain architecture. Acta Electronica Sinica, 2022, 50(2): 257-266(in Chinese)
(张文芳，孙海锋，张晏端等. 基于树形结构构造的联盟链主从多链共识算法. 电子学报，2022，50(2)：257-266)

[41] Jian Z, Ran Q, Liyan S. Securing blockchain wallets efficiently based on threshold ECDSA scheme without trusted center//Proceedings of the Asia-Pacific Conference on Communications Technology and Computer Science. Shenyang, China, 2021: 47-51

[42] Soltani R, Nguyen U, An A. Practical key recovery model for self-sovereign identity based digital wallets//Proceedings of the International Conference on Dependable, Autonomic and Secure Computing. Fukuoka, Japan, 2019: 320-325

[43] Tang Zhang-Ying, Wang Zhi-Wei. A threshold SM2 signature scheme. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2022, (4): 1-11(in Chinese)
(唐张颖，王志伟. 门限 SM2 签名方案. 南京邮电大学学报(自然科学版)，2022，(4)：1-11)

[44] Alharbi A, Zamzami H, Samkri E. Survey on homomorphic encryption and address of new trend. International Journal of Advanced Computer Science and Applications, 2020, 11(7): 618-626

[45] Pedersen T P. Non-interactive and information-theoretic secure verifiable secret sharing//Proceedings of the Advances in Cryptology. California, USA, 1992: 129-140

[46] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts//Proceedings of the IEEE Symposium on Security and Privacy. San Jose, USA, 2016: 839-858

[47] Poelstra A, Back A, Friedenbach M, et al. Confidential assets//Proceedings of the International Conference on Financial Cryptography and Data Security. Amsterdam, Netherlands, 2018: 43-63

[48] Mattila V, Rahman Ahbab M, Dwivedi P, et al. Homomorphic encryption in 5ire Blockchain. International Journal of Social Sciences and Man-Agement Review, 2022, 5(2): 264-276

[49] Bünz B, Agrawal S, Zamani M, et al. Zether: Towards privacy in a smart contract world//Proceedings of the Financial Cryptography and Data Security. Kota Kinabalu, Malaysia, 2020: 423-443

[50] Song M Y, Sang Y P, Zeng Y Y, et al. Blockchain-based secure outsourcing of polynomial multiplication and its application in fully homomorphic encryption//Proceedings of the Security and Communication Networks, 2021, 2021: 1-14

[51] Liang W, Zhang D, Lei X, et al. Circuit copyright blockchain: Blockchain-based homomorphic encryption for IP circuit protection. IEEE Transactions on Emerging Topics in Computing, 2021, 9(3): 1410-1420

[52] Yaji S, Bangera K, Neelima B, et al. Privacy preserving in blockchain based on partial homomorphic encryption system for AI applications//Proceedings of the 25th IEEE International Conference on High Performance Computing, Data and Analytics (HiPC). Bengaluru, India, 2018: 81-85

[53] Chen P C, Kuo T H, Wu J L. A study of the applicability of ideal lattice-based fully homomorphic encryption scheme to ethereum blockchain. IEEE Systems Journal, 2021, 15(2): 1528-1539

[54] Regueiro C, Seco I, De Diego S, et al. Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption. Information Processing & Management, 2021, 58(6): 1-17

[55] Jia B, Zhang X S, Liu J W, et al. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IoT. IEEE Transactions on Industrial Informatics, 2022, 18(6): 4049-4058

[56] Rahulamathavan Y, Phan R C W, Rajarajan M, et al. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption//Proceedings of the IEEE International Conference on Advanced Networks and Telecommunications Systems. Bhubaneswar, India, 2017: 1-6

[57] Wang H, Song Y J. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. Journal of Medical Systems, 2018, 42(8): 152

[58] Ma J, Li T, Cui J, et al. Attribute-based secure announcement sharing among vehicles using blockchain. IEEE Internet of Things Journal, 2021, 8(13): 10873-10883

[59] Feng T, Pei H M, Ma R, et al. Blockchain data privacy access control based on searchable attribute encryption. Computers Materials & Continua, 2021, 66(1): 871-884

[60] Sun Y B, Li X F, Lv F R, et al. Research on logistics information blockchain data query algorithm based on searchable encryption. IEEE Access, 2021, 9: 20968-20976

[61] Hu S, Cai C, Wang Q, et al. Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization //Proceedings of the International Conference on Computer Communications. Hawaii, USA, 2018: 792-800

[62] Li H G, Tian H B, Zhang F G, et al. Blockchain-based searchable symmetric encryption scheme. Computers & Electrical Engineering, 2019, 73: 32-45

[63] Cai C, Weng J, Yuan X, et al. Enabling reliable keyword search in encrypted decentralized storage with fairness. IEEE Transactions on Dependable and Secure Computing, 2021, 18(1): 131-144

[64] Chen L X, Lee W K, Chang C C, et al. Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Systems, 2019, 95: 420-429

[65] Zhang C, Fu S J, Ao W J. A blockchain based searchable encryption scheme for multiple cloud storage//Proceedings of the International Symposium on Cyberspace Safety and Security. Guangzhou, China, 2019: 585-600

[66] Han J J, Li Z Y, Liu J, et al. Attribute-based access control meets blockchain-enabled searchable encryption: A flexible and privacy-preserving framework for multi-user search. Electronics, 2022, 11(16): 1-22

[67] Ferreira J, Zhygulskyy M, Antunes M, et al. Performance of hash functions in blockchain applied to IoT devices// Proceedings of the Iberian Conference on Information Systems and Technologies. Coimbra, Portugal, 2019

[68] Jia M, Chen J, He K, et al. Redactable blockchain from decentralized chameleon hash functions. IEEE Transactions on Information Forensics and Security, 2022, 17: 2771-2783

[69] Albrecht M, Grassi L, Rechberger C, et al. MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Hanoi, Vietnam, 2016: 191-219

[70] Cui J M, Hu K, Wang M Q, et al. On the field-based division property: Applications to MiMC//Proceedings of the Annual International Conference on the Theory and Application of Cryptology and Information Security. Taipei, China, 2022: 241-270

[71] Grassi L, Khovratovich D, Rechberger C, et al. POSEIDON: A new hash function for zero-knowledge proof systems. USENIX Security Symposium. Electr Network, 2021: 519-535

[72] Miers I, Garman C, Green M, et al. Zerocoin: Anonymous distributed E-Cash from Bitcoin//Proceedings of the IEEE Symposium on Security and Privacy. San Francisco, USA, 2013: 397-411

[73] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized anonymous payments from Bitcoin//Proceedings of the IEEE Symposium on Security and Privacy. San Jose, USA, 2014: 459-474

[74] Polge J, Robert J, Le Traon Y. Permissioned blockchain frameworks in the industry: A comparison. ICT Express, 2021, 7(2): 229-233

[75] Ben-Sasson E, Bentov I, Horesh Y, Riabzev M. Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptology ePrint Archive, 2018, 2018(46): 46-129

[76] Bünz B, Bootle J, Boneh D, et al. Bulletproofs: Short proofs for confidential transactions and more//Proceedings of the IEEE Symposium on Security and Privacy (SP). San Francisco, USA, 2018: 315-334

[77] Maller M, Bowe S, Kohlweiss M, et al. Sonic: Zero-knowledge SNARKs from Linear-size universal and updatable structured reference strings//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. London, UK, 2019: 2111-2128

[78] Gabizon A, Williamson Z J, Ciobotaru O. PLONK: Permutations over Lagrange-bases for oecumenical noninteractive arguments of knowledge. Cryptology ePrint Archive, 2019, 2019(953): 1-34

[79] Bowe S, Grigg J, Hopwood D. Recursive proof composition without a trusted setup. Cryptology ePrint Archive, 2019, 2019(1023): 1-31

[80] Chiesa A, Ojha D, Spooner N. FRACTAL: Post-quantum and transparent recursive proofs from holography//Proceedings of the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Zagreb, Croatia, 2020: 769-793

[81] Bünz B, Fisch B, Szepieniec A. Transparent SNARKs from DARK compilers//Proceedings of the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Zagreb, Croatia, 2020: 677-706

[82] Choudhuri A R, Green M, Jain A, et al. Fairness in an unfair world: Fair multipartycomputation from public bulletin boards//Proceedings of the 24th ACM-SIGSAC Conference on Computer and Communications Security. Dallas Texas USA, 2017: 719-736

[83] Paul S, Shrivastava A. Efficient fair multiparty protocols using blockchain and trusted hardware//Proceedings of the International Conference on Cryptology and Information Security in Latin America. Santiago de Chile, Chile, 2019: 301-320

[84] Raman R K, Varshney K R, Vaculin R, et al. Constructing and compressing frames in blockchain-based verifiable multiparty computation//Proceedings of the 44th IEEE International Conference on Acoustics, Speech and Signal Processing. Brighton, UK, 2019: 7500-7504

[85] Raman R K, Vaculin R, Hind M, et al. A scalable blockchain approach for trusted computation and verifiable simulation in multi-party collaborations//Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency. Seoul, Korea, 2019: 277-284

[86] Luo Y H, Deng X S, Wu Y L, et al. MPC-DPOS: An efficient consensus algorithm based on secure multi-party computation//Proceedings of the International Conference on Blockchain Technology and Applications. Xi'an, China, 2019: 105-112

[87] Ashritha K, Sindhu M, Lakshmy K V, et al. Redactable blockchain using enhanced chameleon hash function//Proceedings of the International Conference on Advanced Computing and Communication Systems. Coimbatore, India, 2019: 323-328

[88] Gao H M, Ma Z F, Luo S S, et al. BFR-MPC: A blockchain-based fair and robust multi-party computation scheme. IEEE Access, 2019, 7: 110439-110450

[89] Kim Y, Raman R K, Kim Y S, et al. Efficient local secret sharing for distributed blockchain systems. IEEE Communications Letters, 2019, 23(2): 282-285

[90] Biswas A K, Dasgupta M, Ray S, et al. A probable cheating-free (t,n) threshold secret sharing scheme with enhanced blockchain. Computers & Electrical Engineering, 2022, 100: 107925

[91] Li G J, You L, Hu G R, et al. Recoverable private key scheme for consortium blockchain based on verifiable secret sharing. KSII Transactions on Internet and Information Systems, 2021, 15(8): 2865-2878

[92] Chen L, Zhang X, Sun Z X. Blockchain data sharing query scheme based on threshold secret sharing. Security and Communication Networks, 2022, 2022:1-13

[93] Li G J, You L. A consortium blockchain wallet scheme based on dual-threshold key sharing. Symmetry-Basel, 2021, 13(8): 1444

[94] Zheng W B, Wang K F, Wang F Y. GAN-based key secret-sharing scheme in blockchain. IEEE Transactions on Cybernetics, 2021, 51(1): 393-404

[95] Brunner C, Eibl G, Frohlich P, et al. Who stores the private key? An exploratory study about user preferences of key management for blockchain-based applications//Proceedings of the International Conference on Information Systems Security and Privacy. Electr Network, 2021: 23-32

[96] Pal O, Alam B, Thakur V, et al. Key management for blockchain technology. ICT Express, 2021, 7(1): 76-80

[97] Jung Y, Peradilla M, Agulto R. Packet key-based end-to-end security management on a blockchain control plane. Sensors, 2019, 19(10): 1-16

[98] Genes-Duran R, Yarleque-Ruesta D, Belles-Munoz M, et al. An architecture for easy onboarding and key life-cycle management in blockchain applications. IEEE Access, 2020, 8: 115005-115016

[99] Zhao H W, Bai P D, Peng Y, et al. Efficient key management scheme for health blockchain. Caai Transactions on Intelligence Technology, 2018, 3(2): 114-118

[100] Shbair W M, Gavrilov E, State R, et al. HSM-based key management solution for ethereum blockchain//Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency. Virtual Conference, Australia, 2021: 1-3

[101] Tanana D. Vulnerability analysis of azure blockchain workbench key management system//Proceedings of the International Symposium Problems of Redundancy in Information and Control Systems. Moscow, Russian Federation, 2023: 138-141

[102] Lehto N, Halunen K, Latvala O M, et al. CryptoVault-A secure hardware wallet for decentralized key management//Proceedings of the IEEE International Conference on Omni-Layer Intelligent Systems. 2021: 137-140

[103] Thota A R, Upadhyay P, Kulkarni S, et al. Software wallet based secure participation in hyperledger fabric networks//Proceedings of the International Conference on Communication Systems and NETworks. Bangalore, India, 2020: 1-6

[104] Soltani R, Nguyen U T, An A J, et al. Practical key recovery model for self-sovereign identity based digital wallets//Proceedings of the IEEE 17th International Conference on Dependable, Autonom and Secure Comp. Fukuoka, Japan, 2019: 320-325

[105] Qi Y A, Fu Y, Wang T, et al. Pftom: A blockchain based on fingerprint//Proceedings of the Chinese Automation Congress. Shanghai, China, 2020: 5338-5344

[106] Yeh L Y, Hsu W H, Huang J L, et al. Integrating cellphone-based hardware wallet with visional certificate verification system//Proceedings of the IEEE Global Communications Conference. Electr Network, 2020: 1-6

[107] Kaga Y, Fujio M, Naganuma K, et al. A secure and practical signature scheme for blockchain based on biometrics//Proceedings of the International Conference on Information Security Practice and Experience. Melbourne, Australia, 2017: 877-891

[108] Albakri A, Harn L, Maddumala M, et al. Polynomial-based lightweight key management in a permissioned blockchain//Proceedings of the IEEE Conference on Communications and Network Security. Washington, USA, 2019: 1-9

[109] Gallersdorfer U, Strugala J N, Matthes F. Efficient onboarding and management of members in permissioned blockchain networks utilizing TLS certificates. Frontiers in Blockchain, 2021, 4: 739431

[110] Shor P W. Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 1999, 41(2): 303-332

[111] Grover L K. A fast quantum mechanical algorithm for database search//Proceedings of the 28th Annual ACM Symposium on Theory of Computing. Philadelphia, USA, 1996: 212-219

[112] Fedorov A, Kiktenko E, Lvovsky A. Quantum computers put blockchain security at risk. Nature, 2018, 563: 465-467

[113] Fernández-Caramès T M, Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access, 2020, 8: 21091-21116

[114] Semmouni M C, Nitaj A, Belkasmi M. Bitcoin security with post quantum cryptography. Networked Systems, 2019: 281-288

[115] Semmouni M C, Nitaj A, Belkasmi M. Bitcoin security with post quantum cryptography//Proceedings of the Networked Systems: 7th International Conference. Marrakech, Morocco, 2019: 281-288

[116] Gao S, Zheng D, Guo R, et al. An anti-quantum e-voting protocol in blockchain with audit function. IEEE Access, 2019, 7: 115304-115316

[117] Yin J, Li Y-H, Shengkai L, et al. Entanglement-based secure quantum cryptography over 1120 kilometres. Nature, 2020, 582: 1-5

[118] Jogenfors J. Quantum Bitcoin: An anonymous, distributed, and secure currency secured by the no-cloning theorem of quantum mechanics//Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency. Seoul, Korea, 2019: 245-252

[119] Kiktenko E, Pozhar N, Anufriev M, et al. Quantum-secured blockchain. Quantum Science and Technology, 2017, 3(3): 035004

[120] Rajan D, Visser M. Quantum blockchain using entanglement in time. Quantum Reports, 2019, 1(1): 3-11

[121] Gao Y-L, Chen X-B, Xu G, et al. A novel quantum blockchain scheme base on quantum entanglement and DPoS. Quantum Information Processing, 2020, 19(12): 420

[122] Wei Q, Li B Z, Chang W L, et al. A survey of blockchain data management systems. ACM Transactions on Embedded Computing Systems, 2022, 21(3): 1-28

[123] Zhao H G, Liu Y X, Wang Y H, et al. Hiding data into blockchain-based digital video for security protection//Proceedings of the 3rd International Conference on Smart BlockChain. Zhengzhou, China, 2020: 23-28

[124] Li J X, Wu J G, Jiang G Y, et al. Blockchain-based public auditing for big data in cloud storage. Information Processing & Management, 2020, 57(6): 102382

[125] He K, Shi J, Huang C, et al. Blockchain based data integrity verification for cloud storage with T-Merkle tree//Proceedings of the Algorithms and Architectures for Parallel Processing: 20th International Conference. New York City, USA, 2020: 65-80

[126] Wang J, Chen J H, Ren Y J, et al. Data security storage mechanism based on blockchain industrial Internet of Things. Computers & Industrial Engineering, 2022, 164: 107903

[127] Wang J, Chen W C, Wang L, et al. Blockchain-Based data storage mechanism for industrial Internet of Things. Intelligent Automation and Soft Computing, 2020, 26(5): 1157-1172

[128] Xie M, Yu Y, Chen R A, et al. Accountable outsourcing data storage atop blockchain. Computer Standards & Interfaces, 2022, 82: 103628

[129] Ren Y J, Leng Y, Cheng Y P, et al. Secure data storage based on blockchain and coding in edge computing. Mathematical Biosciences and Engineering, 2019, 16(4): 1874-1892

[130] Tulkinbekov K, Kim D H. Storing blockchain data in public storage//Proceedings of the 12th International Conference on Ubiquitous and Future Networks. Electr Network, 2021: 299-301

[131] Ren Y J, Leng Y, Zhu F J, et al. Data storage mechanism based on blockchain with privacy protection in wireless body area network. Sensors, 2019, 19(10): 2395

[132] Jayabalan J, Jeyanthi N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. Journal of Parallel and Distributed Computing, 2022, 164: 152-167

[133] Grabis J, Stankovski V, Zarins R, et al. Blockchain enabled distributed storage and sharing of personal data assets//Proceedings of the 36th IEEE International Conference on Data Engineering. 2020: 11-17

[134] Han H, Wan W N, Zhang J Q, et al. A scalable double-chain storage module for blockchain. Computers Materials & Continua, 2022, 73(2): 2651-2662

[135] Loe A F, Quaglia E A. You shall not join: A measurement study of cryptocurrency peer-to-peer bootstrapping techniques //Proceedings of the ACM Conference on Computer and Communications Security. London, UK, 2019: 2231-2247

[136] Alanazi A A. Malicious Trust Managers Identification (MTMI) in peer to peer networks. International Journal of Computer Science and Network Security, 2021, 21(9): 91-98

[137] Prunster B, Fasllija E, Mocher D. Master of puppets: Trusting silicon in the fight for practical security in fully decentralized peer-to-peer networks//Proceedings of the 16th International Joint Conference on E-Business and Telecommunications. Prague, Czech Republic, 2019: 252-259

[138] Alhussain A, Kurdi H, Altoaimy L. Managing trust and detecting malicious groups in peer-to-peer IoT networks. Sensors, 2021, 21(13): 4484

[139] Ndajah P, Matine A O, Hounkonnou M N. Black hole attack prevention in wireless peer-to-peer networks: A new strategy. International Journal of Wireless Information Networks, 2019, 26(1): 48-60

[140] Eisenbarth J P, Cholez T, Perrin O. Ethereum's peer-to-peer network monitoring and sybil attack prevention. Journal of Network and Systems Management, 2022, 30(4): 65

[141] Cao T, Yu J S, Decouchant J, et al. Exploring the Monero peer-to-peer network//Proceedings of the 24th International Conference on Financial Cryptography and Data Security. Kota Kinabalu, Malaysia, 2020: 578-594

[142] Qu D P, Zhang J K, Hou Z H, et al. A trust routing scheme based on identification of non-complete cooperative nodes in mobile peer-to-peer networks//Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Guangzhou, China, 2020: 22-29

[143] Berenjian S, Hajizadeh S, Atani R E, et al. An incentive security model to provide fairness for peer-to-peer networks//Proceedings of the IEEE Conference on Application, Information and Network Security. Penang, Malaysia, 2019: 71-76

[144] Beauchaine A, Collins O, Yun M. BotsideP2P: A peer-to-peer botnet testbed//Proceedings of the 12th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference. Electr Network, 2021: 236-242

[145] Zhuang D, Chang J M. Enhanced PeerHunter: Detecting peer-to-peer botnets through network-flow level community

behavior analysis. IEEE Transactions on Information Forensics and Security, 2019, 14(6): 1485-1500

[146] Tran M, Choi I, Moon G J, et al. A stealthier partitioning attack against Bitcoin peer-to-peer network//Proceedings of the IEEE Symposium on Security and Privacy. 2020: 894-909

[147] Sallal M, Owenson G, Adda M, et al. Security and performance evaluation of master node protocol in the Bitcoin peer-to-peer network//Proceedings of the IEEE Symposium on Computers and Communications. Rennes, France, 2020: 980-985

[148] Tapsell J, Akram R N, Markantonakis K, et al. An evaluation of the security of the Bitcoin peer-to-peer network//Proceedings of the IEEE International Congress on Cybermatics. Halifax, Canada, 2018: 1057-1062

[149] Musa A, Abubakar A, Gimba U A, et al. An investigation into peer-to-peer network security using wireshark//Proceedings of the International Conference on Electronics, Computer and Computation. Halifax, Canada, 2019: 1-6

[150] Ziwich R P, Duarte E P, Silveira G P. Distributed mitigation of content pollution in peer-to-peer video streaming networks. IET Communications, 2020, 14(11): 1760-1768

[151] Kumar M, Chand S. SecP2PVoD: A secure peer-to-peer video-on-demand system against pollution attack and untrusted service provider. Multimedia Tools and Applications, 2020, 79(9): 6163-6190

[152] Hao W F, Zeng J J, Dai X H, et al. BlockP2P: Enabling fast blockchain broadcast with scalable peer-to-peer network topology//Proceedings of the International Conference on Green, Pervasive and Cloud Computing. Uberlandia, Brazil, 2019: 223-237

[153] Zhu Y W, Li X X. Privacy-preserving *k*-means clustering with local synchronization in peer-to-peer networks. Peer-to-Peer Networking and Applications, 2020, 13(6): 2272-2284

[154] Yang D M, Li H J, Ren B Q, et al. Robust security transmission design for multi-user peer-to-peer wireless relay networks. International Journal of Distributed Sensor Networks, 2022, 18(6): 1-15

[155] Matsuura H, Goto Y, Sao H. Region-based neighbor selection in blockchain networks//Proceedings of the 4th IEEE International Conference on Blockchain. 2021: 21-28

[156] Gaba S, Budhiraja I, Makkar A, et al. Machine learning for detecting security attacks on blockchain using software defined networking//Proceedings of the IEEE International Conference on Communications. Seoul, Korea, 2022: 260-264

[157] Kim S, Kim B, Kim H J, et al. Intrusion detection and mitigation system using blockchain analysis for bitcoin exchange//Proceedings of the International Conference on Cloud Computing and Internet of Things. Singapore, 2018: 40-44

[158] Liang W, Xiao L J, Zhang K, et al. Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems. IEEE Internet of Things Journal, 2022, 9(16): 14741-14751

[159] Kumar R, Kumar P, Tripathi R, et al. A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. Journal of Parallel and Distributed Computing, 2022, 164: 55-68

[160] Kumar P, Kumar R, Gupta G P, et al. A distributed framework for detecting DDoS attacks in smart contract-based blockchain-IoT systems by leveraging fog computing. Transactions on Emerging Telecommunications Technologies, 2021, 32(6): e4112

[161] Signorini M, Pontecorvi M, Kanoun W, et al. BAD: A blockchain anomaly detection solution. IEEE Access, 2020, 8: 173481-173490

[162] Echeberria-Barrio X, Zola F, Segurola-Gil L, et al. SmartWarden: Automated intrusion detection system for smart contracts//Proceedings of the 3rd Conference on Blockchain Research and Applications for Innovative Networks and Services. Paris, France, 2021: 51-52

[163] Wang X M, He J H, Xie Z J, et al. ContractGuard: Defend Ethereum smart contracts with embedded intrusion detection. IEEE Transactions on Services Computing, 2020, 13(2): 314-328

[164] Kabla A H H, Anbar M, Manickam S, et al. Applicability of intrusion detection system on Ethereum attacks: A comprehensive review. IEEE Access, 2022, 10: 71632-71655

[165] Wang T T, Zhao C H, Yang Q, et al. Ethna: Analyzing the underlying peer-to-peer network of Ethereum blockchain. IEEE Transactions on Network Science and Engineering, 2021, 8(3): 2131-2146

[166] Chaganti R, Boppana R V, Ravi V, et al. A comprehensive review of denial of service attacks in blockchain ecosystem and Open Challenges. IEEE Access, 2022, 10: 96538-96555

[167] Liu Yi-Zhong, Liu Jian-Wei, Zhang Zong-Yang, et al. Overview on blockchain consensus mechanisms. Journal of Cryptologic Research, 2019, 6(4): 395-432(in Chinese)
(刘懿中，刘建伟，张宗洋等. 区块链共识机制研究综述. 密码学报，2019，6(4)：395-432)

[168] Xiao Y, Zhang N, Lou W J, et al. Modeling the impact of network connectivity on consensus security of proof-of-work blockchain//Proceedings of the 39th IEEE International Conference on Computer Communications. 2020: 1648-1657

[169] Ai Z P, Liu Y, Wang X W, et al. ABC: An auction-based blockchain consensus-incentive mechanism//Proceedings of the 26th IEEE International Conference on Parallel and Distributed Systems. 2020: 609-616

[170] Xian X B, Zhou Y, Guo Y R, et al. Improved consensus mechanisms against censorship attacks//Proceedings of the IEEE International Conference on Industrial Cyber Physical Systems. Taipei, China, 2019: 718-723

[171] Qiu X F, Qin Z, Wan W N, et al. A dynamic reputation-based consensus mechanism for blockchain. Computers Materials & Continua, 2022, 73(2): 2577-2589

[172] Sui K L, Yang C Z, Li Z H. Research on consensus mechanism for anti-mining concentration//Proceedings of the 7th International Conference on Communications, Signal Processing, and Systems. Dalian, China, 2018: 483-492

[173] Gai K K, Hu Z Y, Zhu L H, et al. Blockchain meets DAG: A blockDAG consensus mechanism//Proceedings of the International Conference on Algorithms and Architectures for Parallel Processing. New York, USA, 2020: 110-125

[174] Liu Y, Ai Z P, Tian M M, et al. DSBFT: A delegation based scalable Byzantine false tolerance consensus mechanism //Proceedings of the 20th International Conference on Algorithms and Architectures for Parallel Processing. New York, USA, 2020: 426-440

[175] Carrara G R, Mattos D M F, De Albuquerque C V N, et al. Vicinity-based consensus: A fast in-neighborhood convergence consensus mechanism for blockchain. IEEE Global Communications Conference. Madrid, Spain, 2021: 1-6

[176] Li K J, Li H, Hou H X, et al. Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain//Proceedings of the 19th IEEE International Conference on High Performance Computing and Communications. Bangkok, Thailand, 2017: 466-473

[177] Wang Y H, Cai S B, Lin C L, et al. Study of blockchains's consensus mechanism based on credit. IEEE Access, 2019, 7: 10224-10231

[178] Cheng J R, Zhang Y, Yuan Y M, et al. PoEC: A cross-blockchain consensus mechanism for governing blockchain by blockchain. Computers Materials & Continua, 2022, 73(1): 1385-1402

[179] Wen X J, Chen Y Z, Zhang W, et al. Blockchain consensus mechanism based on quantum teleportation. Mathematics, 2022, 10(14): 2385

[180] Li Q, Wu J J, Quan J Y, et al. Efficient quantum blockchain with a consensus mechanism QDPoS. IEEE Transactions on Information Forensics and Security, 2022, 17: 3264-3276

[181] Security guidelines [Online]. Available: https://github.com/slowmist/eos-smart-contract-security-bestpractices/blob/master/README_EN.md#security-guidelines

[182] Ethereum smart contract security best practices: General philosophy[Online]. Available: https://consensys.github.io/smart-contract-best-practices/general_philosophy/

[183] Bartoletti M, Pompianu L. An empirical analysis of smart contracts: Platforms, applications, and design patterns//Proceedings of the Financial Cryptography and Data Security. Sliema, Malta, 2017: 494-509

[184] Wohrer M, Zdun U. Smart contracts: Security patterns in the ethereum ecosystem and solidity//Proceedings of the 2018 International Workshop on Blockchain Oriented Software Engineering. Campobasso, Italy, 2018: 2-8

[185] Singh I, Lee S W. SRE_BBC: A self-Adaptive security enabled requirements engineering approach for SLA smart contracts in blockchain-based cloud systems. Sensors, 2022, 22(10): 3903

[186] Idelberger F, Governatori G, Riveret R, et al. Evaluation of logic-based smart contracts for blockchain systems//Proceedings of the Rule Technologies. Research, Tools, and Applications: The 10th International Symposium. New York, USA, 2016: 167-183

[187] Mavridou A, Laszka A, Stachtiari E, et al. VeriSolid: Correct-by-design smart contracts for ethereum. Financial Cryptography and Data Security. ST Kitts, Nevi, 2019: 446-465

[188] Ahmadjee S, Mera-Gomez C, Bahsoon R, et al. Assessing smart contracts security technical debts//Proceedings of the 4th IEEE/ACM International Conference on Technical Debt. 2021: 6-15

[189] Park W S, Lee H, Choi J Y, et al. Formal modeling of smart contract-based trading system//Proceedings of the 23rd International Conference on Advanced Communications Technology. Electr Network, 2021: 48-52

[190] OpenZeppelin. Available: https://openzeppelin.org

[191] Aragon OSx. https://devs.aragon.org/docs/osx/how-it-works/core/permissions/

[192] Liu L, Wei L L, Zhang W Q, et al. Characterizing transaction-reverting statements in Ethereum smart contracts//Proceedings of the 36th IEEE/ACM International Conference on Automated Software Engineering. Electr Network, 2021: 630-641

[193] Mao D H, Wang F, Wang Y L, et al. Visual and user-defined smart contract designing system based on automatic coding. IEEE Access, 2019, 7: 73131-73143

[194] Tateishi T, Yoshihama S, Sato N, et al. Automatic smart contract generation using controlled natural language and template. IBM Journal of Research and Development, 2019, 63(2): 1-6

[195] Qin P, Guo J Z, Shen B Q, et al. Towards self-automatable and unambiguous smart contracts: Machine natural language //Proceedings of the 16th IEEE International Conference on E-Business Engineering. Shanghai, China, 2019: 479-491

[196] Hamdaqa M, Met L, Qasse I. A domain-specific language for modeling and deploying smart contracts onto multiple blockchain platforms. Information and Software Technology, 2022, 144: 106762

[197] Abdellatif T, Brousmiche K-L. Formal verification of smart contracts based on users and blockchain behaviors models//Proceedings of the IFIP NTMS International Workshop on Blockchains and Smart Contracts. Paris, France, 2018: 1-5

[198] Bhargavan K, Delignat-Lavaud A, Fournet C, et al. Formal verification of smart contracts: Short paper//Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security. Vienna, Austria, 2016: 91-96

[199] Hirai Y. Defining the Ethereum virtual machine for interactive theorem provers//Proceedings of the Financial Cryptography and Data Security: FC 2017 International Workshops. Sliema, Malta, 2017: 520-535

[200] Tsankov P, Dan A, Drachsler-Cohen D, et al. Securify: Practical security analysis of smart contracts//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada, 2018: 67-82

[201] Zhou E, Hua S, Pi B F, et al. Security assurance for smart contract//Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security. Paris, France, 2018: 1-5

[202] Jiang B, Liu Y, Chan W K. ContractFuzzer: Fuzzing smart contracts for vulnerability detection//Proceedings of the 33rd IEEE/ACM International Conference on Automated Software Engineering. Montpellier, France, 2018: 259-269

[203] Chan W K, Jiang B. Fuse: An architecture for smart contract fuzz testing service//Proceedings of the 25th Asia-Pacific Software Engineering Conference. Nara, Japan, 2018: 707-708

[204] Zhou Y, Kumar D, Bakshi S, et al. Erays: Reverse engineering ethereum's opaque smart contracts//Proceedings of the 27th USENIX Conference on Security Symposium. Baltimore, USA, 2018: 1371-1385

[205] Breidenbach L, Daian P, Tramèr F, et al. Enter the hydra: Towards principled bug bounties and exploit-resistant smart contracts//Proceedings of the 27th USENIX Conference on Security Symposium. Baltimore, USA, 2018: 1335-1352

[206] Nikolic I, Kolluri A, Sergey I, et al. Finding the greedy, prodigal, and suicidal contracts at scale//Proceedings of the 34th Annual Computer Security Applications Conference. San Juan, USA, 2018: 653-663

[207] Grossman S, Abraham I, Golan-Gueta G, et al. Online detection of effectively callback free objects with applications to smart contracts. ACM Programming Languages, 2017, 2: Article 48

[208] Chen W, Zheng Z, Cui J, et al. Detecting ponzi schemes on Ethereum: Towards healthier blockchain technology//Proceedings of the 2018 World Wide Web Conference. Lyon, France, 2018: 1409-1418

[209] Chen T, Li Z, Zhu Y, et al. Understanding Ethereum via graph analysis. ACM Transactions on Internet Technology, 2020, 20(2): 1-32

[210] Li T, Fang Y Z, Jian Z L, et al. ATOM: Architectural support and optimization mechanism for smart contract fast update and execution in blockchain-based IoT. IEEE Internet of Things Journal, 2022, 9(11): 7959-7971

[211] Yao Qian, Zhang Da-Wei. Survey on identity management in blockchain. Journal of Software, 2021, 32(7): 2260-2286(in Chinese)
(姚前, 张大伟. 区块链系统中身份管理技术研究综述. 软件学报, 2021, 32(7): 2260-2286)

[212] Wang Chen-Xu, Cheng Jia-Cheng, Sang Xin-Xin, et al. Data privacy-preserving for blockchain: State of the art and trends. Journal of Computer Research and Development, 2021, 58(10): 2099-2119(in Chinese)
(王晨旭, 程加成, 桑新欣等. 区块链数据隐私保护: 研究现状与展望. 计算机研究与发展, 2021, 58(10): 2099-2119)

[213] Yao Shuang, Zhang Da-Wei, Li Yong, et al. A survey on privacy protection of transaction content in blockchain. Journal of Cryptologic Research, 2022, 9(4): 596-618(in Chinese)
(姚爽, 张大伟, 李勇等. 区块链交易内容隐私保护技术研究综述. 密码学报, 2022, 9(4): 596-618)

[214] Hardin T, Kotz D, Soc I C. Amanuensis: Provenance, privacy, and permission in TEE-enabled blockchain data systems//Proceedings of the 42nd IEEE International Conference on Distributed Computing Systems. Bologna, Italy, 2022: 144-156

[215] Maddali L P, Thakur M S D, Vigneswaran R, et al. VeriBlock: A novel blockchain framework based on verifiable computing and trusted execution environment//Proceedings of the International Conference on COMmunication Systems and NETworkS. Bangalore, India, 2020: 1-6

[216] Hardjono T, Smith N. Decentralized trusted computing base for blockchain infrastructure security. Frontiers in Blockchain, 2019, 2: 24

[217] Santos J M V, Pascua J E V, Tiglao N M C. Hardware-accelerated blockchain-based authentication for the Internet of Things//Proceedings of the 14th European-Alliance-for-Innovation(EAI) International Wireless Internet Conference. Electr Network, 2021: 283-295

[218] Li Fang, Li Zhuo-Ran, Zhao He. Research on the progress in cross-chain technology of blockchains. Journal of Software, 2019, 30(6): 1649-1660(in Chinese)
(李芳, 李卓然, 赵赫. 区块链跨链技术进展研究. 软件学报, 2019, 30(6): 1649-1660)

[219] Scheid E J, Kiechl P, Franco M, et al. Security and standardization of a notary-based blockchain interoperability API//Proceedings of the 3rd IEEE International Conference on Blockchain Computing and Applications. Electr Network, 2021: 42-48

[220] Guo J N, Gai K K, Zhu L H, et al. An approach of secure two-way-pegged multi-sidechain//Proceedings of the 19th International Conference on Algorithms and Architectures for Parallel Processing. Melbourne, Australia, 2019: 551-564

[221] Gai F Y, Niu J Y, Tabatabaee S A, et al. Cumulus: A secure BFT-based sidechain for off-chain scaling//Proceedings of the 29th IEEE/ACM International Symposium on Quality of Service. Electr Network, 2021: 1-6

[222] Garoffolo A, Kaidalov D, Oliynykov R, et al. Zendoo: A zk-SNARK verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains//Proceedings of the 40th IEEE International Conference on Distributed Computing Systems. Electr Network, 2020: 1257-1262

[223] Sun Y Y, Yi L Y, Duan L, et al. A decentralized cross-chain service protocol based on notary schemes and hash-locking//Proceedings of the IEEE International Conference on Services Computing. Barcelona, Spain, 2022: 152-157

[224] Dai B R, Jiang S M, Li C, et al. A multi-hop cross-blockchain transaction model based on improved hash-locking. International Journal of Computational Science and Engineering, 2021, 24(6): 610-620

[225] Deng L P, Chen H, Zeng J, et al. Research on cross-chain technology based on sidechain and hash-locking//Proceedings of the 2nd International Conference on Edge Computing. Seattle, USA, 2018: 144-151

[226] Morganti G, Schiavone E, Bondavalli A. Risk assessment of blockchain technology//Proceedings of the 2018 Eighth Latin-American Symposium on Dependable Computing. Foz do Iguacu, Brazil, 2018: 87-96

[227] Ye Cong-Cong, Li Guo-Qiang, Cai Hong-Ming, et al. Security detection model of blockchain. Journal of Software, 2018, 29(5): 1348-1359(in Chinese)
(叶聪聪，李国强，蔡鸿明等. 区块链的安全检测模型. 软件学报，2018，29(5)：1348-1359)

[228] Gourisetti N G, Mylrea M, Patangia H. Application of rank-weight methods to blockchain cybersecurity vulnerability assessment framework//Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference. Las Vegas, USA, 2019: 0206-0213

[229] Qin Chao-Xia, Guo Bing, Shen Yan, et al. Security risk assessment model of blockchain. Acta Electronica Sinica, 2021, 49(1): 117-124(in Chinese)
(秦超霞，郭兵，沈艳等. 区块链的安全风险评估模型. 电子学报，2021，49(1)：117-124)

[230] Lu T B, Yan R, Lei M, et al. AABN: Anonymity assessment model based on Bayesian network with application to blockchain. China Communications, 2019, 16(6): 55-68

[231] Howard J P, Vachino M E. Blockchain compliance with federal cryptographic information-processing standards. IEEE Security & Privacy, 2020, 18(1): 65-70

[232] Wang D, Zhu Y, Zhang Y, et al. Security assessment of blockchain in Chinese classified protection of cybersecurity. IEEE Access, 2020, 8: 203440-203456

[233] Wei Liang, Zha Xuan. Blockchain infrastructure security risk and evaluation exploration. Information and Communications Technology and Policy, 2020, (2): 10-13(in Chinese)
(魏亮，查选. 区块链基础设施安全风险及评估探索. 信息通信技术与政策，2020，(2)：10-13)

[234] He Bao-Hong, Kang Chen, Zhang Yi-Hui. Blockchain security risks and regulatory practices. Information Security in China, 2021, (3): 43-47(in Chinese)
(何宝宏，康宸，张奕卉. 区块链安全风险及其监管实践. 中国信息安全，2021，(3)：43-47)

[235] Mallah R A, López D, Farooq B. Cyber-security risk assessment framework for blockchains in smart mobility. IEEE Open Journal of Intelligent Transportation Systems, 2021, 2: 294-311

[236] Zhang Jian-Yi, Wang Zhi-Qiang, Xu Zhi-Li, et al. A regulatable digital currency model based on blockchain. Journal of Computer Research and Development, 2018, 55(10): 2219-2232(in Chinese)
(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. 计算机研究与发展，2018，55(10)：2219-2232)

[237] Zhang J Y, Li P J, Xu Z L, et al. Gemini-Chain: A regulatable digital currency model based on blockchain//Proceedings of the 39th IEEE International Conference on Computer Communications. Electr Network, 2020: 760-765

[238] Xue Z Y, Wang M, Zhang Q Y, et al. A regulatable blockchain transaction model with privacy protection. International Journal of Computational Intelligence Systems, 2021, 14(1): 1642-1652

[239] Xiao R Y, Sun G Z, Yang J L, et al. RBSmix: A regulatable privacy-preserving method for cryptocurrency. Wireless Communications & Mobile Computing, 2022, 2022: 1-14

[240] Li H B, Xie T, Xie J, et al. A decentrlized trading model based on public blockchain with regulatable bi-tierred Identities//Proceedings of the 19th IEEE International Symposium on Parallel and Distributed Processing with Applications. New York, USA, 2021: 1189-1198

[241] Li Y F, Chen Y L, Li T, et al. A regulatable data privacy protection scheme for energy transactions based on consortium blockchain. Security and Communication Networks, 2021, 2021: 1-11

[242] Marsalek A, Zefferer T, Soc I C. A correctable public blockchain//Proceedings of the 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications Rotorua. New Zealand, 2019: 554-561

[243] Ateniese G, Magri B, Venturi D, et al. Redactable blockchain-or-rewriting history in Bitcoin and Friends//Proceedings of the 2nd IEEE European Symposium on Security and Privacy. Paris, France, 2017: 111-126

[244] Politou E, Casino F, Alepis E, et al. Blockchain mutability: Challenges and proposed solutions. IEEE Transactions on Emerging Topics in Computing, 2021, 9(4): 1972-1986

[245] Deuber D, Magri B, Thyagarajan S A K, et al. Redactable blockchain in the permissionless setting//Proceedings of the 40th IEEE Symposium on Security and Privacy. San Francisco, USA, 2019: 124-138

[246] Yuan Yong, Wang Fei-Yue. Editable blockchain: Models, techniques and methods. Acta Automatica Sinica, 2020, 46(5): 831-846(in Chinese)
(袁勇，王飞跃. 可编辑区块链：模型、技术与方法. 自动化学报，2020，46(5)：831-846)

[247] ISO. ISO/TR 23244: 2020 Blockchain and distributed ledger technologies—privacy and personally identifiable information protection considerations. 2020

[248] ISO. ISO/TR 23576:2020 Blockchain and distributed ledger technologies—security management of digital asset custodians. 2020

[249] ISO. ISO/WD TR 23642 Blockchain and distributed ledger technologies-overview of smart contract security good practice and issues. 2021

[250] ITU-T. X.1401: Security threats of distributed ledger technology. 2019

[251] ITU-T. Cloud computing-functional requirements for blockchain as a service. 2020

[252] National Information Security Standardization Technical Committee. Information security technology—security specification for blockchain information service. 2023(in Chinese)

(全国信息安全标准化技术委员会. 信息安全技术 区块链信息服务安全规范. 2023)

[253] National Information Security Standardization Technical Committee. Information security technology—security framework for blockchain technology. 2023(in Chinese)
(全国信息安全标准化技术委员会. 信息安全技术 区块链技术安全框架. 2023)

[254] Ministry of Industry and Information Technology. Blockchain technology architecture security requirements. 2020(in Chinese)
(工业和信息化部. 区块链技术架构安全要求. 2020)

[255] Ministry of Industry and Information Technology. Blockchain and distributed ledger technology—reference architecture. 2023(in Chinese)
(全国区块链和分布式记账技术标准化技术委员会. 区块链和分布式记账技术 参考架构. 2023)

[256] Ministry of Industry and Information Technology. Blockchain and distributed ledger technology—guidelines for applications of logistic tracking services. 2022(in Chinese)
(全国区块链和分布式记账技术标准化技术委员会. 区块链和分布式记账技术 物流追踪服务应用指南. 2022)

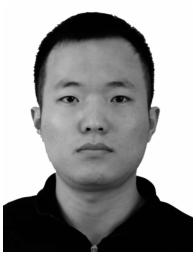
[257] Ministry of Industry and Information Technology. Blockchain and distributed ledger technology-System testing specification. 2021(in Chinese)
(全国区块链和分布式记账技术标准化技术委员会. 区块链和分布式记账技术 系统测试规范. 2021)

[258] Ministry of Industry and Information Technology. Blockchain and distributed ledger technology-application interface-technical guidelines of middleware. 2021(in Chinese)
(全国区块链和分布式记账技术标准化技术委员会. 区块链和分布式记账技术 应用程序接口 中间件技术指南. 2021)

[259] Ministry of Industry and Information Technology. Blockchain and distributed ledger technology-technical specification of smart contract lifecycle management. 2020(in Chinese)
(全国区块链和分布式记账技术标准化技术委员会. 区块链和分布式记账技术 智能合约生命周期管理技术规范. 2020)

[260] China Communication Standardization Association. Telecommunications networks and internet blockchain infrastructure security requirements. 2022(in Chinese)
(中国通信标准化协会. 电信网和互联网区块链基础设施安全防护要求. 2022)

[261] China Communication Standardization Association. Blockchain technology architecture security requirements. 2020(in Chinese)
(中国通信标准化协会. 区块链技术架构安全要求. 2020)



LIU Ao-Di, Ph. D., lecturer. His current research interests focus on blockchain security.

DU Xue-Hui, Ph. D., professor. Her current research interests focus on network and information security.

WANG Na, Ph. D., professor. Her current research interests focus on network and information security.

WU Xiang-Yu, Ph. D. candidate. His current research interests focus on blockchain security.

SHAN Di-Bin, Ph. D., lecturer. His current research interests focus on network and information security.

QIAO Rui, Ph. D., associate professor. Her current research interests focus on blockchain security.

Background

As an important information technology with characteristics of the decentralization, openness and transparency, and immutable, blockchain is used to build a new network trust relationship. Blockchain is of the great significance in facilitating the development of the digital economy and reshaping the pattern of the value circulation. However, due to the huge value of the blockchain as the carrier of the data and assets, it is easy to become the key target of the malicious attackers, and traditional security technology is difficult to apply the distributed blockchain technology architecture. Therefore, the security technology research of the blockchain is urgent. Based on the characteristics of the blockchain business process and the blockchain system technical framework, this paper proposes a security technical framework that conforms to the characteristics of the the blockchain business. In addition, the research progress of the blockchain security technology is summarized from three aspects: blockchain cryptographic support technology, blockchain platform security technology, and blockchain risk assessment and security supervision, to provide inspiration and reference for the research work of blockchain security.

This work is supported by the Key Research and Development and Promotion Program of Henan Province (No. 222102210069), the Zhongyuan Science and Technology Innovation Leading Talent Project (No. 224200510003), the National Natural Science Foundation of China (No. 62102449) and the Henan University Science and Technology Innovation Talent Support Plan (No. 23HASTIT029).