区块链安全问题: 研究现状与展望

韩 璇 [1, 2] 袁 勇 [1, 2] 王飞跃 [1, 3, 4]

摘 要 区块链是比特币底层的核心技术, 展示了在自组织模式下实现大规模协作的巨大潜力, 为解决分布式网络中的一致性问题提供了全新的方法. 随着比特币的广泛流通和去中心化区块链平台的蓬勃发展, 区块链应用也逐渐延伸至金融、物联网等领域, 全球掀起了区块链的研究热潮. 然而, 区块链为无信任的网络环境提供安全保障的同时, 也面临安全和隐私方面的严峻挑战. 本文定义了区块链系统设计追求的安全目标, 从机制漏洞、攻击手段和安全措施三方面对区块链各层级的安全问题进行全面分析, 提出了区块链的平行安全概念框架, 并总结未来区块链安全问题的研究重点. 本文致力于为区块链研究提供有益的安全技术理论支撑与借鉴.

关键词 区块链, 可证明安全, 隐私保护, 安全威胁, 监管

引用格式 韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望. 自动化学报, 2019, **45**(1): 206−225

DOI 10.16383/j.aas.c180710

Security Problems on Blockchain: The State of the Art and Future Trends

HAN Xuan[1, 2] YUAN Yong[1, 2] WANG Fei-Yue[1, 3, 4]

Abstract As the core underlying technology of Bitcoin, blockchain shows the potential of achieving large-scale self-organizing, and provides a new approach to solve the consistency problem in P2P networks. With the widespread circulation of Bitcoin and the rapid development of decentralized blockchain platforms, blockchain has been gradually applied to many fields such as finance and Internet of Things, and related studies have been blooming across the world. Blockchain provides a security architecture in the trustless network environment, however, it also faces serious challenges in security and privacy. In this paper, we defined the security objectives and gave a comprehensive analysis of blockchain security from the aspects of the existing vulnerabilities, attacks and security measures. In addition, we proposed a conceptual framework of parallel security and summarized the key directions of future security research on blockchain. This paper is devoted to providing useful theoretical support and reference for future blockchain researches.

Key words Blockchain, provable security, privacy protection, security threat, supervision

Citation Han Xuan, Yuan Yong, Wang Fei-Yue. Security problems on blockchain: the state of the art and future trends. *Acta Automatica Sinica*, 2019, **45**(1): 206−225

区块链技术起源于比特币[1], 是以比特币为代表的众多数字货币方案的底层核心技术, 最初设计目的是解决电子支付中过度依赖可信第三方的问题. 区块链将哈希函数、Merkle 树、工作量证明 (Proof of work, PoW)[2] 等成熟的技术进行重组, 结合公钥加密、数字签名和零知识证明等密码学技术, 成为一种全新的分布式基础架构和计算范式[3].

区块链极具潜力, 其应用已从最初的数字货币延伸至金融、物联网、智能制造等多个领域, 引起了产业界和政府的广泛关注. 为了推进区块链技术的研究和应用, 国内外先后成立了 R3 CEV、超级账本项目 (Hyperledger) 和中国分布式总账基础协议联盟等区块链联盟, 关注区块链技术的理论创新和应用推广. 各国政府机构也高度关注区块链的发展, 加紧部署区块链发展战略与政策. 2015 年 12 月, 英国政府发布了《分布式账本技术: 超越区块链》[4], 预测区块链将引起新一轮技术变革, 建议加快区块链理论推广与应用开发进程. 我国工信部于 2016 年 10 月发布了《中国区块链技术与应用发展白皮书

收稿日期 2018-10-31 录用日期 2019-01-14
Manuscript received October 31, 2018; accepted January 14, 2019
国家自然科学基金 (71472174, 61533019, 71232006, 61233001, 71702182), 青岛智能产业智库资助
Supported by National Natural Science Foundation of China (71472174, 61533019, 71232006, 61233001, 71702182), Qingdao Think-Tank Foundation on Intelligent Industries
本文责任编委 魏庆来
Recommended by Associate Editor WEI Qing-Lai
1. 中国科学院自动化研究所复杂系统管理与控制国家重点实验室 北京 100190 2. 青岛智能产业技术研究院平行区块链技术创新中心 青岛 266109 3. 国防科学技术大学军事计算实验与平行系统技术中心 长沙 410073 4. 中国科学院大学中国经济与社会安全研究中心 北京 101408
1. The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190 2. Innovation Center for Parallel Blockchain, Qingdao Academy of Intelligent Industries, Qingdao 266109 3. Research Center of Military Computational Experiments and Parallel Systems, National University of Defense Technology, Changsha 410073 4. Center of China Economic and Social Security, The University of Chinese Academy of Sciences, Beijing 101408

(2016)》[5]. 国务院在《“十三五” 国家信息化规划》中将区块链列入战略性前沿科技之一. 同年, 世界经济论坛也对区块链在金融场景下的应用进行预测分析, 认为区块链将在跨境支付、保险、贷款等多方面重塑金融市场基础设施[6].

随着理论研究的深入, 区块链展现出蓬勃生命力的同时, 自身的安全性问题逐渐显露. 针对区块链数字货币应用的安全威胁也呈现高发态势. 各大交易平台被盗事件频发、智能合约漏洞凸显、匿名交易实施犯罪等安全事件更加引发公众对区块链安全性的质疑和对其发展前景的忧虑. 2014 年 2 月 28 日, 曾经世界规模最大的比特币交易平台 Mt.Gox 声称遭受交易延展性攻击 (Transaction malleability attack)[7], 85 万个比特币被盗, 损失估计约 4.67 亿美元, Mt.Gox 最终破产. 2016 年 6 月 17 日, 黑客利用以太坊智能合约漏洞攻击去中心自治组织 (Decentralized autonomous organization, DAO) 的众筹项目 The DAO, 导致 300 多万以太币资产被分离出 The DAO 资金池, 以太坊被迫进行硬分叉弥补损失. 2017 年 5 月 12 日, 比特币勒索病毒 WannaCry 在全球范围内爆发, 百余国家遭到袭击, 其中包括我国部分高校和政府机构网络.

区块链的应用发展迫切地需要系统的安全性研究作为指南. 各国权威机构也将研究重点转向区块链的安全性. 2016 年 12 月, 欧盟网络与信息安全局 ENISA 发布《分布式账本技术与网络安全: 加强金融领域的信息安全》[8], 结合传统网络空间安全问题, 分析了区块链面临的安全技术挑战. 2018 年 1 月, 美国国家标准与技术研究院 NIST 发布了《区块链技术总览》[9], 总结了区块链应用在区块链控制、恶意用户、无信任和用户身份等方面的局限性和概念误区.

区块链发展还处于初级探索阶段, 研究区块链的安全性问题具有多方面的意义. 第一, 研究区块链的安全性有助于促进科学创新. 区块链不是独立而生的技术, 其安全性涉及底层加密方案、分布式一致性、网络系统安全以及经济学激励机制等诸多层面. 区块链的安全性研究给多学科提出了更高的技术要求, 必将促进密码学、分布式、网络安全、博弈论等学科的创新发展. 第二, 研究区块链的安全性有助于加速技术推广. 目前, 理论安全性分析不完备、缺乏代码评估、安全事件频发等不安全因素限制了区块链的发展. 研究安全高效的区块链方案可适用于更多的应用场景, 逐步拓宽的应用实例也将在实践中更好地检验区块链的安全性. 第三, 研究区块链安全性有助于实现可信的可编程社会. 区块链支持的智能合约具有可编程性和自动执行性, 呈现出一定的智能化特征. 研究区块链的安全性, 有助于提高智能合约的安全性和模块化, 简化开发过程, 增强互操作性. 安全的区块链架构和自动执行的智能合约可以从技术上强制合约的执行, 降低违约风险, 构建可信的可编程社会. 第四, 研究区块链的安全性有助于实现可控监管. 区块链的不可篡改性和匿名性为实现监管带来了挑战. 监管机制可以预防、检测系统中的不法行为, 是系统受攻击后的安全修复手段. 分析现有区块链漏洞、潜在攻击和隐私保护机制有利于制定网络监测策略, 设计更高效、安全的监管机制.

本文着眼于区块链技术中的安全问题, 定义了区块链系统设计的安全目标, 梳理了区块链各层级存在的安全隐患, 对现有的安全措施进行对比分析, 提出了用于评估区块链网络攻防策略的平行安全概念框架, 并对未来区块链安全方向的研究重点进行展望, 以期对未来区块链技术的理论研究和应用发展有所助益.

本文的组织结构为: 第 1 节简要介绍区块链的基本概念, 包括比特币区块链的运行原理、区块链的一般定义、特点、分类和面临的安全技术挑战; 第 2 节从安全性和隐私保护两方面给出了区块链的系统级安全性目标; 第 3 节从安全角度剖析区块链的体系架构, 分析区块链各层次存在的安全隐患、潜在的攻击和现有的安全措施; 第 4 节提出区块链上的平行安全概念框架; 第 5 节提出未来区块链在安全方面的重点研究方向; 第 6 节总结全文.

1 区块链概述

2008 年 10 月, 化名为 “中本聪” 的学者在密码学论坛上公开了《比特币: 一种点对点的电子现金系统》一文[1], 提出了利用 PoW 和时间戳机制构造交易区块的链式结构, 剔除了可信第三方, 实现了去中心化的匿名支付. 比特币于 2009 年 1 月上线并发布创世块, 标志着首个基于区块链技术应用的诞生. 根据 BTC.com 网站数据显示, 截至 2018 年 9 月 20 日, 已发行 1 700 余万枚比特币, 总市值超过 1 100 亿美元. 比特币是迄今为止区块链技术最成功的应用, 是众多区块链平台的开发基础, 也是学术界的研究重点. 本节以比特币为例, 简要介绍比特币区块链的工作原理、区块链的定义、特点、分类和面临的安全技术挑战等基本内容.

1.1 比特币的工作原理

比特币运行在 P2P 网络中, 是一种开放的电子现金系统, 允许节点自由加入, 无需通过可信第三方注册认证. 节点使用公钥的哈希值作为自己的数字假名, 也被称为地址, 具备一定的匿名性. 交易是比特币网络中传播和存储的基本数据实体, 常利用数字签名实现代币等数字资产所有权的转移. 交

易不仅要经过验证, 还要在打包成区块后经全网节点达成共识, 才会被记录到比特币的区块链中. 比特币中采用的 PoW 机制保证网络中节点共同维护一份相同的区块链账本. PoW 的实质是求解一个满足部分碰撞的哈希值的原像. 节点竞争完成 PoW 求解的过程被称为挖矿, 这些节点被称为矿工. 矿工通过挖矿来竞争记账权, 即对区块链进行写操作的权限. 矿工挖矿成功后, 可以将打包好的交易区块连接到区块链末尾, 并获得一笔比特币奖励, 以 coinbase 格式保存在区块中. 比特币每产生 2016 个区块, 根据这些区块的生成速率来调整 PoW 的难度, 保证平均 10 分钟生成一个区块. 比特币中首个区块被称为创世块, 也是区块链的头部, 最新链接到区块链上的则为尾部. 挖矿生成区块的过程也是比特币的发行过程. 初始每个区块奖励 50 枚比特币, 每 4 年减半, 直至达到最小的单位聪 (Satoshi, $1\,\text{Satoshi} = 10^{-8}\,\text{BTC}$) 不能再减半为止, 后续挖矿不再发行比特币, 总量约 2 100 万.

比特币通过哈希函数将交易区块按时间顺序前后相连, 形成链式结构, 区块链结构如图 1 所示. 每个区块包含交易信息和区块头部两部分. 交易信息是区块的主体部分, 将交易以 Merkle 树结构存储. 最终生成 Merkle 树的根作为交易摘要被记录在区块头部中, 便于交易的验证和查找. 区块头部还记录了区块位置、PoW 参数、时间戳和填充字段等信息. 区块通过保存前驱区块的哈希值来实现区块间的连接关系, 标识自己在区块链中的位置. PoW 参数主要包括比特币采用的 PoW 难度和矿工求解得到的随机数, 用于验证矿工是否挖矿成功. 时间戳表明生成区块时矿工的本地时间. 填充字段内包含当前区块链的版本参数等信息.

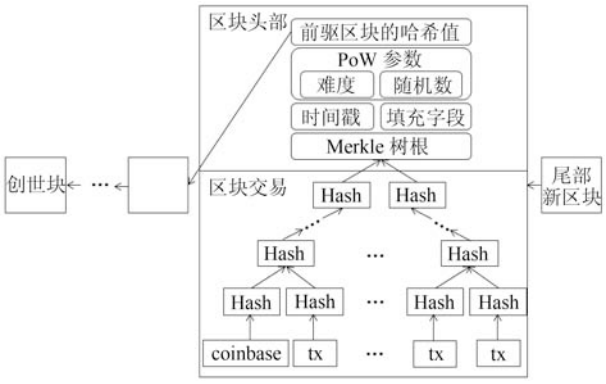

图 1 比特币区块链结构

Fig. 1 Structure of bitcoin blockchain

新用户生成公私钥对和地址后加入比特币网络, 可通过挖矿或者他人转账的方式获得比特币. 用户首先创建并广播交易. 网络中的节点接收交易后, 将该交易转发给相邻的几个节点, 通过泛洪式的传播机制将交易在整个比特币网络中进行传播. 矿工收到交易首先进行验证, 若交易有效, 则保存在自己本地的交易池中, 等待打包成区块; 若交易无效, 则丢弃. 之后, 矿工按照一定规则从交易池中选取交易, 构造 Merkle 树. 然后将当前区块链尾部区块的哈希值、Merkle 树的根和 PoW 难度作为求解 PoW 的输入, 通过穷举的方式得到满足条件的随机数, 填充区块的头部信息. 随后, 矿工将新生成的区块连接到区块链尾部并广播新区块链, 等待网络节点达成共识. 其他矿工收到一个或多个新区块链后, 会对新区块链中的交易、PoW 等进行逐一验证, 并与本地存储的区块链进行对比. 最终, 诚实的矿工将在最长的有效区块链上达成共识, 并在尾部继续挖矿.

1.2 区块链的基本概念

区块链是一种典型的分布式账本技术, 通过共识等多边自治技术手段支持数据验证、共享、计算、存储等功能. 在不同应用场景下, 区块链可以存储并处理不同数据. 为了简化表述, 本文以交易作为区块链存储和处理的数据主体展开介绍.

从区块链的组织结构和运行原理来看, 可以狭义地将区块链视为一种以区块为单位的、按照时间顺序前后相连的单向链式数据结构, 通过共识机制、密码学组件和系统容错等技术保证分布式网络中节点共享数据的一致性和安全性. 从应用角度来看, 区块链是一种集成了密码学算法、分布式网络、共识机制、博弈论等技术的复合分布式网络技术, 利用链式区块结构存储数据, 利用共识机制实现交易的更新和共享, 利用密码学技术保证交易的安全性, 利用自动化脚本代码实现可编程性和自治性, 利用经济学激励机制激发节点自主维护系统稳定, 构成了一种全新的、自治的分布式基础架构与计算范式[3].

如何在分布式网络中实现一致性是区块链技术的核心问题之一. 历经 10 年发展, 区块链先后具备去中心化、可追溯性、不可篡改性、不可伪造性、不可否认性和可编程性等特点.

去中心化是区块链发展伊始最显著的优势. 相比于传统的分布式一致性协议, 区块链大多建立在开放网络中. PoW 等共识机制能有效解决拜占庭将军问题, 允许节点数量扩展, 在部分节点偏离协议执行甚至实施恶意攻击的情况下, 仍能保证一致性. 而大多数 Paxos 系列的分布式一致性算法并不考虑拜占庭将军问题[10−11], 在恶意节点实施主动攻击时, Paxos 算法无法保证消息传输的一致性. 虽然实用的拜占庭容错协议 (Practical Byzantine fault tolerance, PBFT)[12] 等拜占庭一致性算法可以在部分节点实施恶意攻击的情况下保持系统稳定, 但

是这些算法在异步网络中最多支持 1/3 容错, 通信复杂度高, 效率较低, 不适用于允许节点自由加入的开放式网络环境. 去中心化的区块链还可以避免单点失效问题, 系统吞吐量不受单一节点限制. 在 Raft[13]、VR (Viewstamped replication, VR)[14] 等依赖强领导关系的一致性算法中, 如果领导节点宕机或者被攻击者控制, 那么整个系统的安全性和吞吐量都将受到严重影响, 系统的恢复过程也十分复杂. 相比之下, 区块链中 PoW、权益证明 (Proof of stake, PoS)[15] 等共识机制不需要中心节点或特权节点, 在设计上避免了单点失效问题.

区块链结合密码学技术, 可以保证交易的可追溯性、不可篡改性、不可否认性和不可伪造性, 支持数据安全共享和大规模协同计算, 也可实现对用户身份和机密数据的隐私保护, 更适用于需要高隐私性和安全性的分布式应用场景中. 可追溯性是指交易的每次变更都会按照时间顺序记录在区块链上, 前后关联, 可以查询交易从发布源头到最新状态间的整个变更流程. 不可篡改性和不可否认性指交易等数据一经验证达成共识被写入区块链后, 任何人无法对数据进行修改和抵赖. 不可伪造性指任何人无法通过有效手段伪造可通过矿工验证的交易, 更无法伪造整条交易变更记录. 相比传统的中心化数据库, 利用哈希函数的单向性和耐碰撞性、数字签名的防伪认证功能和分布式共识的容错能力, 区块链极大增加了攻击者恶意篡改、伪造和否认数据操作的攻击难度和成本, 有效提升数据的安全性.

以太坊 (Ethereum) 平台上支持的智能合约为区块链增添了可编程属性[16], 将区块链构建成一个可编程的数据共享平台[17]. 具有可编程性的区块链高效地解决了传统合约中依赖中介等第三方维系、合约执行成本高的问题, 降低了合约参与方违约风险和诚实合约方的经济损失.

根据区块链维护过程中是否需要中心节点或者权限优势节点授权, 区块链可以被分为无许可区块链 (Permissionless blockchain) 和许可区块链 (Permissioned blockchain) 两类[18].

无许可区块链是一种完全去中心的分布式账本技术, 允许节点自由加入和退出, 无须通过中心节点注册、认证和授权. 网络节点地位平等, 共享整个区块链账本, 可自由选择是否参与数据验证、挖矿等维护系统稳定的关键环节. 无许可区块链不依赖中心节点提供安全保障, 需要大量网络节点自主参与, 提供数据冗余. 因此, 无许可区块链要具备支持大规模网络和数据扩展的能力, 对共识机制的扩展性、容错能力和效率能耗等方面提出了更高的要求. 一般地, 无许可区块链缺乏身份认证和隐私保护机制, 还需要依靠经济激励机制激励网络节点自发地维护系统, 面临安全隐患多、匿名性弱、激励策略不相容等问题. 无许可区块链适用于完全公开的、全民监督的、全网自治的应用场景中, 如食品安全供应链溯源、知识产权管理等. 比特币就是经典的无许可区块链应用案例, 此类应用也是目前区块链研发的主流. 本文更侧重研究无许可区块链中的安全性问题.

相比于无许可区块链, 许可区块链中存在一个或多个节点具有较高权限, 这些节点可以是可信第三方, 也可能几个高权限节点之间仍然互不信任, 需要协商制定区块链维护规则和访问控制权限, 仅经过相应功能授权的节点才可访问数据、参与系统维护[19], 与区块链去中心化的设计初衷相违背. 许可区块链是一种受限共享分布式账本技术, 具有维护成本低、共识效率高、匿名性强、数据吞吐量大等优势. 但是, 许可区块链往往面临高权限节点易受攻击、信任缺失等问题. 多数许可区块链共识不依赖复杂的计算问题, 计算敏感度低, 降低了攻击者的攻击成本. 许可区块链适用于小范围的、数据交互频繁的组织间或组织内部共享数据服务等应用场景, 如跨行清算、医疗保险理赔等. 英国央行联合伦敦大学提出的法定数字货币框架 RSCoin 方案是典型的许可区块链[20], 由央行作为中心节点负责身份认证、下层节点分组和区块链数据整合等操作, 现已进入实验测试阶段.

1.3 区块链的安全挑战

区块链在数字货币领域的发展如火如荼, 展现出蓬勃生命力的同时, 也面临安全和隐私方面的严峻挑战.

首先, 区块链面临理论模型与实际网络状况相差甚远的安全性分析的挑战[21]. 本质上, 无中心节点的区块链的安全性依赖于大量的数据冗余. 即使攻击者有能力控制某节点进而伪造、篡改、删除该节点的有效数据, 但是要同时对众多网络节点实施攻击是十分困难的. 然而, 在实际区块链网络中, 由于各节点具备的安全防护等级参差不齐, 攻击者可以利用网络拓扑结构, 仅凭少量资源即可成功实施小范围攻击, 破坏系统的安全性与稳定性[22].

其次, 区块链结构复杂, 缺乏系统级安全评估手段. 区块链的发展仍处于初级探索阶段, 它所包含的共识算法、激励机制、智能合约等关键环节的安全性尚待评估, 也缺乏代码评估机制以检测系统漏洞[23]. 区块链建立在对等网络 (Peer to peer, P2P) 中, 与客户端/服务器 (Client/Sever, C/S) 网络系统结构不同, 传统的防火墙、入侵检测等网络安全技术不能完全适用.

另外, 计算技术的发展为区块链安全性带来威胁. 随着量子计算的发展, 区块链底层依赖的哈希函

数、公钥加密算法、数字签名、零知识证明等技术的安全性也将受到影响[24].

最后, 完全去中心的匿名区块链系统缺乏有效的监管手段[25], 当攻击者对系统安全性造成威胁、非法用户利用区块链实施违法行为时, 系统无法对攻击者和非法用户进行追责. 一旦攻击成功, 由于区块链的不可篡改性, 非法交易无法撤回, 将给用户造成不可逆转的经济损失. 匿名的区块链平台也将成为犯罪行为滋生、不良内容传播的温巢.

2 区块链的安全目标

根据网络系统的安全需求, 结合区块链的特点, 区块链系统构建的基本安全目标是通过密码学和网络安全等技术手段, 保护区块链系统中的数据安全、共识安全、隐私保护、智能合约安全和内容安全, 各安全目标之间的关系如图 2 所示. 其中, 数据安全是区块链的首要安全目标. 共识安全、智能合约安全、隐私保护和内容安全等安全目标与数据安全联系紧密, 是数据安全目标在区块链各层级中的细化, 也是区块链设计中需要特别考虑的安全要素.

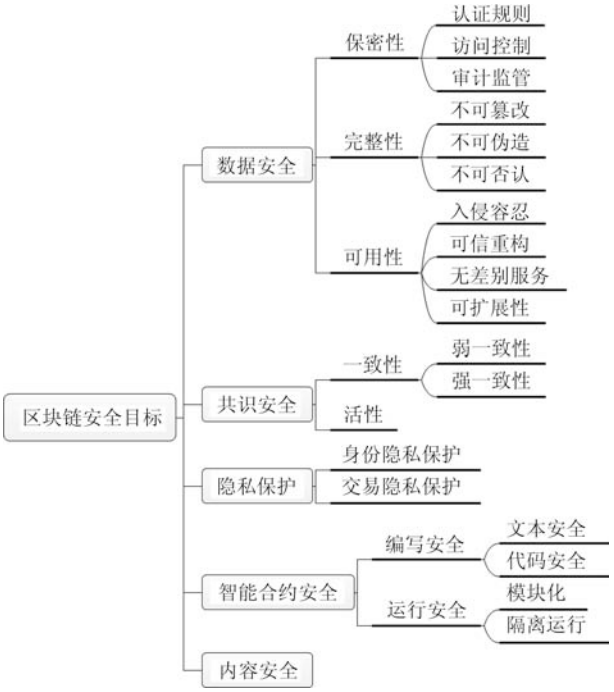

图 2 区块链安全目标

Fig. 2 Security objectives on blockchain

2.1 数据安全

数据安全是区块链的基本安全目标. 区块链作为一种去中心化的存储系统, 需要存储包括交易、用户信息、智能合约代码和执行中间状态等海量数据. 这些数据至关重要, 是区块链安全防护的首要实体. 本文采用 CIA 信息安全三元组来定义区块链的数据安全, 即保密性 (Confidentiality)、完整性 (Integrity) 和可用性 (Availability).

保密性: 规定了不同用户对不同数据的访问控制权限, 仅有权限的用户才可以对数据进行相应的操作, 信息不能被未授权用户知晓和使用, 引申出隐私保护性质. 保密性具体要求区块链设置相应的认证规则、访问控制和审计机制. 认证规则规定了每个节点加入区块链的方式和有效的身份识别方式, 是实现访问控制的基础. 访问控制规定了访问控制的技术方法和每个用户的访问权限. 在无许可区块链中, 如何通过去中心化方式实现有效的访问控制尤为重要. 审计监管是指区块链能够提供有效的安全事件监测、追踪、分析、追责等一整套监管方案.

完整性: 是指区块链中的任何数据不能被未经过授权的用户或者以不可察觉的方式实施伪造、修改、删除等非法操作. 具体指用户发布的交易信息不可篡改、不可伪造; 矿工挖矿成功生成区块获得全网共识后不可篡改、不可伪造; 智能合约的状态变量、中间结果和最终输出不可篡改、不可伪造; 区块链系统中一切行为不可抵赖, 如攻击者无法抵赖自己的双重支付 (Double spending) 攻击行为. 完整性在交易等底层数据层面上往往需要数字签名、哈希函数等密码组件支持. 在共识层面上, 数据完整性的实现则更加依赖共识安全.

可用性: 指数据可以在任何时间被有权限的用户访问和使用. 区块链中的可用性包括四个方面. 首先, 可用性要求区块链具备在遭受攻击时仍然能够继续提供可靠服务的能力, 需要依赖支持容错的共识机制和分布式入侵容忍等技术实现. 其次, 可用性要求当区块链受到攻击导致部分功能受损的情况下, 具备短时间内修复和重构的能力, 需要依赖网络的可信重构等技术实现. 另外, 可用性要求区块链可以提供无差别服务. 即使是新加入网络的节点依旧可以通过有效方式获取正确的区块链数据, 保证新节点的数据安全. 可用性亦指用户的访问数据请求可以在有限时间内得到区块链网络响应, 进一步可引申出可扩展性的含义. 可扩展性是指区块链具有高吞吐量、低响应时延, 即使在网络节点规模庞大或者通信量激增的情况下, 仍能提供稳定的服务.

2.2 共识安全

共识机制是区块链的核心, 共识安全对区块链的数据安全起到重要的支撑作用. 本文引用比特币骨干协议[26] 中定义的一致性 (Consistency) 和活性 (Liveness) 两个安全属性来衡量和评估区块链的共识安全.

一致性: 要求任何已经被记录在区块链上并达成共识的交易都无法更改, 即一旦网络中节点在一

条区块链上达成共识, 那么任意攻击者都无法通过有效手段产生一条区块链分叉, 使得网络中的节点抛弃原区块链, 在新区块链分叉上达成共识. 一致性是共识机制最重要的安全目标. 根据共识机制在达成共识的过程中是否出现短暂分叉, 一致性又分为弱一致性和强一致性. 弱一致性是指在网络节点达成共识的过程中有短暂分叉的出现. 一些情况下, 节点可能会无法立即在两个区块链分叉中做出选择, 形成左右摇摆的情况. 强一致性是指网络中新区块一旦生成, 网络节点即可判断是否对它达成共识, 不会出现阶段性分叉.

活性: 要求诚实节点提交的合法数据终将由全网节点达成共识并被记录在区块链上. 合法数据包括诚实节点提交的合法交易、正确执行的智能合约中间状态变量、结果等. 活性保证了诚实节点能够抵抗拒绝服务攻击, 维护区块链持续可靠运行.

2.3 隐私保护

隐私保护是对用户身份信息等用户不愿公开的敏感信息的保护. 在区块链中, 主要针对用户身份信息和交易信息两部分内容. 因此, 区块链的隐私保护可划分为身份隐私保护和交易隐私保护.

身份隐私保护: 要求用户的身份信息、物理地址、IP 地址与区块链上的用户公钥、地址等公开信息之间是不关联的. 任何未授权节点仅依靠区块链上公开的数据无法获取有关用户身份的任何信息, 也不能通过网络监听、流量分析等网络技术手段对用户交易和身份进行追踪.

交易隐私保护: 要求交易本身的数据信息对非授权节点匿名. 在比特币中特指交易金额、交易的发送方公钥、接收方地址以及交易的购买内容等其他交易信息. 任何未授权节点无法通过有效的技术手段获取交易相关的知识. 在一些需要高隐私保护强度的区块链中, 还要求割裂交易与交易之间的关联性, 即非授权节点无法有效推断两个交易是否具有前后连续性、是否属于同一用户等关联关系.

2.4 智能合约安全

根据智能合约的整个生命周期运作流程, 智能合约安全可以被划分为编写安全和运行安全两部分.

编写安全: 侧重智能合约的文本安全和代码安全两方面. 文本安全是实现智能合约稳定运行的第一步. 智能合约开发人员在编写智能合约之前, 需要根据实际功能设计完善的合约文本, 避免由合约文本错误导致智能合约执行异常甚至出现死锁等情况. 代码安全要求智能合约开发人员使用安全成熟的语言, 严格按照合约文本进行编写, 确保合约代码与合约文本的一致性, 且代码编译后没有漏洞.

运行安全: 涉及智能合约在实际运行过程中的安全保护机制, 是智能合约在不可信的区块链环境中安全运行的重要目标. 运行安全指智能合约在执行过程中一旦出现漏洞甚至被攻击, 不会对节点本地系统设备造成影响, 也不会使调用该合约的其他合约或程序执行异常, 包括模块化和隔离运行两方面. 模块化要求智能合约标准化管理, 具有高内聚低耦合的特点, 可移植, 可通过接口实现智能合约的安全调用. 遭受攻击后的异常结果并不会通过合约调用的方式继续蔓延, 保证了智能合约的可用性. 隔离运行要求智能合约在虚拟机等隔离环境中运行, 不能直接运行在参与区块链的节点本地系统上, 防止运行智能合约的本地操作系统遭受攻击.

2.5 内容安全

内容安全是在数据安全的基础上衍生出来的应用层安全属性, 要求区块链上传播和存储的数据内容符合道德规范和法律要求, 防止不良或非法内容在区块链网络中传播, 保证区块链网络中信息的纯净度. 内容安全的保障重点是加强区块链中信息在传播和存储过程中的控制和管理. 由于区块链具有不可篡改的特点, 一旦非法内容被记录在区块链上, 将很难被修改或撤销, 也将影响公众和政府对区块链应用的态度. 在区块链应用生态中需要网络监测、信息过滤等技术, 保证区块链的内容安全. 例如, 在基于区块链的银行系统中, 需要设置特定的信息内容分析和智能化处理机制来实现了解你的客户 (Know your customer, KYC) 和反洗钱 (Anti money laundering, AML) 等内容监管机制. 此外, 内容安全还需要设置有效的监管机制对已经记录在区块链中的非法内容进行撤销、删除等操作, 维护区块链网络健康发展.

3 区块链的安全性问题

尽管区块链在多领域的应用层出不穷, 但是随着研究的深入和安全事件频发, 区块链在安全性方面的缺陷也逐渐显露. 为了更好地解释区块链体系结构中提供的安全机制和出现的安全问题, 本文采用《区块链技术发展现状与展望》[3] 中提出的数据层、网络层、共识层、激励层、合约层和应用层六层体系架构, 并以此为基础从信息安全的角度对六层体系架构进行重新解释. 每层可细分为基础模块和安全模块两部分, 如图 3 所示. 其中, 基础模块是用于实现该层主要功能的基本组件. 安全模块则是用于保障各层安全性, 为上层提供安全稳定技术支持的安全组件.

区块链作为一种多学科交叉的复合新技术在各层次都面临理论和实践上的安全性威胁, 如图 4 所

示. 虽然, 针对区块链各层级的安全措施相继出现, 但还处于初级探索阶段, 尚不完善. 一些安全技术可能会引入新的问题.

图 3 区块链体系架构

Fig. 3 The basic framework of blockchain

3.1 数据层

数据层既规定了交易、区块、链式结构在内的狭义区块链的数据结构和存储形式等基本模块, 也包括了关于用户身份、地址的密钥管理机制以及区块链所需的其他密码学组件等安全模块, 是实现其他五层功能的基础. 综合数据层各组件特点, 数据层面临着量子计算威胁、密钥管理不当、交易关联性紧密和密码组件代码漏洞等安全性问题.

3.1.1 量子计算威胁

区块链数据层中的交易和区块实体都涉及到公钥加密、数字签名、哈希函数等多种密码学组件. 为了满足更高的隐私保护需求, 一些区块链方案还需要环签名、零知识证明等隐私保护技术. 这些密码学组件的安全性直接影响到区块链数据层的安全性. 短期来看, 数学理论、密码学解析和计算技术的发展不会对一些已经形成标准的密码算法构成威胁. 但是随着量子计算的兴起, 现有的密码算法将面临安全性降低甚至被攻破的危险. NIST 发布的后量子密码报告[27] 中给出了大规模量子计算机对一些密码算法安全性造成的影响, 如表 1 所示.

尽管现阶段量子计算的研究成果还不能对区块链中的密码算法构成威胁, 但是从长远看, 区块链的发展势必要引入可以抵抗量子攻击的加密系统. 美国 NIST 于 2018 年 4 月召开后量子密码算法标准会议, 在全球范围内召集抗量子攻击的公钥加密算法. 一些研究也利用基于格的后量子签名等算法替代比特币中对应的密码组件[28]. 随着量子密码的兴起, 俄罗斯量子中心 (Russian quantum center, RQC) 正积极研究首个依赖量子加密技术实现分布式数据存储和验证的量子区块链.

表 1 量子计算对一般密码算法的影响[27]

Table 1 Impact of quantum computing on common cryptographic algorithms[27]

密码算法	类型	功能	安全性影响
AES	对称密码	加密	攻击难度减半
SHA-2, SHA-3	–	哈希函数	攻击难度减半
RSA	公钥密码	加密	攻破
ECDSA, ECDH	公钥密码	签名, 密钥交换	攻破
DSA	公钥密码	签名, 密钥交换	攻破

3.1.2 密钥管理不当

区块链在金融领域的应用往往涉及数字资产交易, 直接关系到用户的个人利益, 也容易成为贪心攻击者的攻击目标. 现代密码体制的安全是基于密钥的安全. 然而, 区块链应用普遍缺乏有效的密钥管理技术. 因使用、存储不当导致的密钥泄露和丢失都给比特币用户带来巨大利益损失. 例如, 为了方便记忆, 用户常选用有实际意义的字符串作为密钥, 有利于攻击者实施字典攻击 (Dictionary attack); 采用硬件存储密钥也容易遭受侧信道攻击 (Side channel attack). 尤其是在无许可区块链中, 没有中心节点参与为密钥管理方案设计增加了难度. 区块链的不可篡改性也使得密钥一旦丢失或被盗, 用户将遭受不可逆转的经济损失, 亟需合理的密钥管理机制.

目前, 区块链应用中的主流密钥管理方法包括本地存储、离线存储、托管钱包和门限钱包. 本地存储将密钥直接或经加密后存储在本地设备上, 容易被恶意读取, 物理设备损坏时也无法恢复. 离线存储将密钥保存在离线的物理存储介质中, 防止恶意软件攻击. 但是使用时仍然需要联网, 无法完全避免恶意软件入侵. 区块链还可以利用第三方托管钱包服务器为用户提供密钥托管服务. 但是, 托管钱包破坏了区块链的去中心化. 托管钱包可能恶意窃取用户密钥, 存在后门攻击和单点失效问题. 托管服务器作为中心节点也容易成为攻击目标. 一旦被攻破, 大量密钥失窃将会造成严重的损失. 门限钱包利用门限加密技术将密钥分散存储在多个设备中, 使用密钥时需要多个设备参与. 即使某个设备被攻击, 攻击者仍然无法恢复出完整的密钥, 也不影响用户的使用. 但是这种方案在设计上存在一定困难, 算法复杂度高, 且不可扩展. 密钥保护秘密分享 (Password-protected secret sharing, PPSS) 是一种线上的门限钱包方案[29], 是今后区块链实现安全密钥管理的主流研究方向.

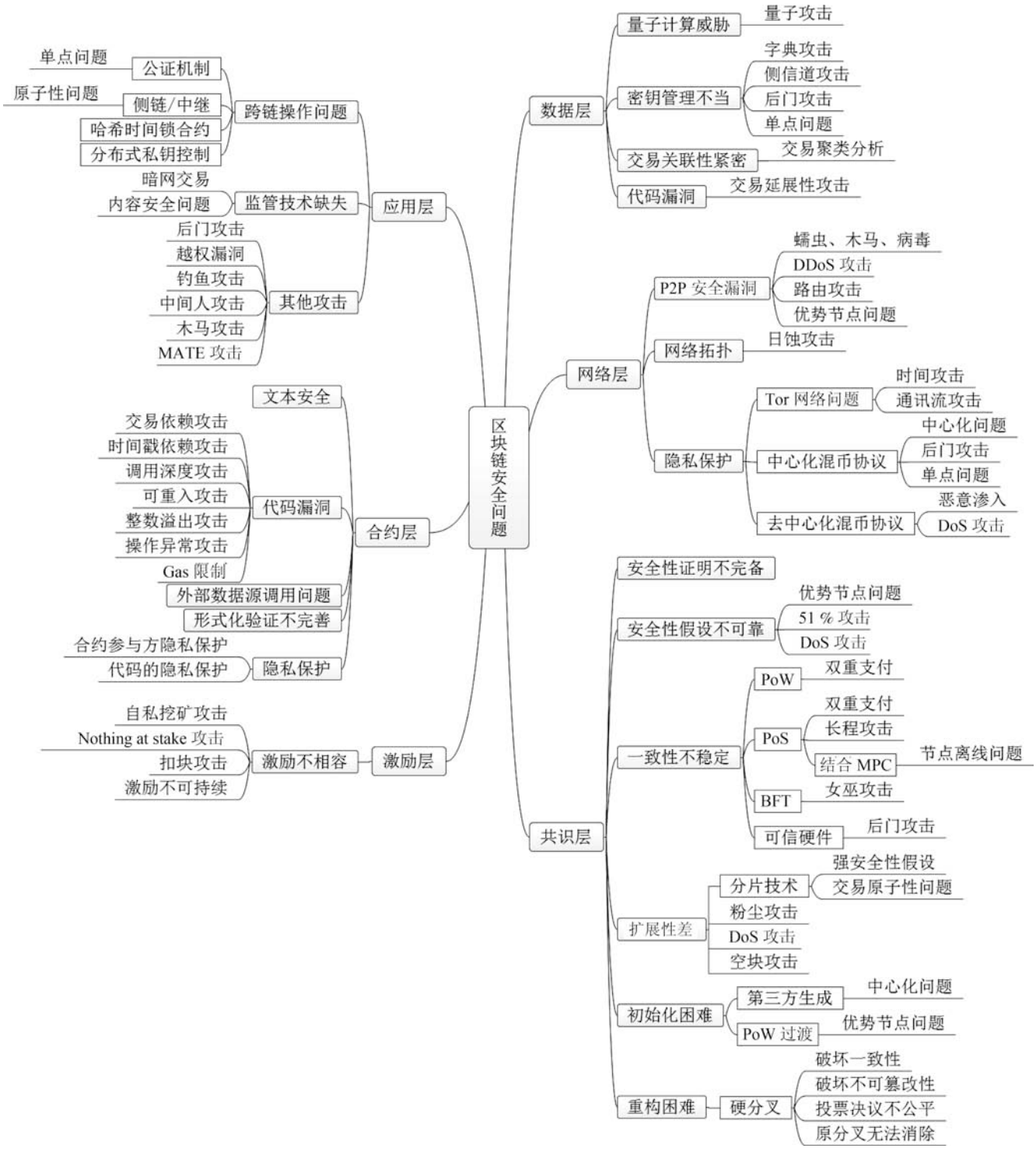

图 4　区块链的安全问题

Fig. 4　Security threats on blockchain

3.1.3　交易关联紧密

基于区块链的数字货币平台大多使用数字假名, 允许用户拥有多个假名, 但是这种方式仅能提供较弱的用户身份的匿名性, 交易之间的关联性和交易金额等信息均公开在区块链上. 一旦用户的一个地址暴露, 该用户的所有公钥地址都可能被推断出来. 通过交易图谱分析和交易聚类分析[30] 也可以根据交易的统计特性推断出交易所有者的真实身份.

为了提高攻击者利用交易之间的拓扑结构推测用户身份的难度, 数据层利用零知识证明、环签名

等密码学技术来实现交易的混淆. 2013 年, Saberhagen 利用环签名和隐蔽地址技术构造了匿名电子现金 CryptoNote 协议[31], 将实际交易发送方身份隐藏在一系列公钥中, 后发展成门罗币 (Monero)[32] 的核心协议. 然而, 环签名方案面临攻击者可伪造环签名实施构陷等安全问题. 环签名的扩展性差、签名长度长也影响其在区块链中的应用. 2013 年, Miers 等利用零知识证明技术设计了匿名代币 Zerocoin[33], 可以将比特币兑换成 Zerocoin 后进行匿名交易, 实现对用户身份的隐私保护, 但是不能隐藏交易金额, 支付效率低. 2014 年, Sasson 等在 Zerocoin 的基础上利用简洁非交互零知识证明 (Zero-knowledge succinct non-interactive arguments of knowledge, zk-SNARK)[34] 构造了匿名支付协议 Zerocash[35], 实现了对交易双方身份和交易金额的隐私保护, 是零币 (ZCash) 的核心协议. zk-SNARK 技术具备抗量子攻击能力, 备受学术界关注. 但是, zk-SNARK 技术尚不成熟, 存在效率瓶颈, 生成证明的过程复杂, 且证据占据空间过大, 不适用存储空间有限的区块链系统.

3.1.4 代码漏洞

一些密码组件在编译的过程中也可能存在缺陷和漏洞. 交易延展性攻击[36] 就是一种针对数据层代码漏洞实施的攻击, 利用比特币使用数字签名构造的交易在编译过程中的延展性, 常被用于针对比特币交易平台进行攻击. 攻击者首先向交易平台请求取款. 随后, 交易平台创建一笔交易支付给攻击者一笔比特币. 当监听到这笔交易时, 攻击者对这笔交易的签名部分进行字符串填充或者采用其他编码方式编码, 但不破坏签名本身, 签名仍然有效. 然后, 攻击者根据更改后的交易重新生成 TXID 标识符来伪造一笔新的交易, 将伪造的交易广播到网络中. 网络中的矿工会有一定概率率先将伪造交易写入区块链, 使得原有效交易被判为双重支付[37], 导致交易平台认为原交易并未被矿工验证通过, 不得不产生一笔新交易再一次支付给攻击者. 攻击一旦成功, 攻击者就会获得双倍的比特币. 部分研究尝试通过修改 TXID 的结构来应对交易的延展性攻击[38].

3.2 网络层

网络层的核心是确保区块链节点的合法加入和有效通信, 具体包括区块链的组网模式、节点之间的通信模式、扩展网络以及必要的匿名网络通信技术. 区块链采用 P2P 联网通信方式, 过程不依赖可信第三方, 通过 P2P 网络的路由查询结构, 在全球范围内的网络节点之间建立连接. 根据节点是否包含全部数据, 区块链网络中的节点又可分为全节点和轻节点两类. 全节点存储了包括交易集合、密钥管理规定的节点公钥和地址、区块链账本、网络路由等所有数据. 轻节点则仅存储区块哈希值等区块链账本中的部分信息, 通过随机协议, 与其他节点建立数据传入和传出连接. 全节点和轻节点之间的通讯形成了区块链中常见的去中心化网络拓扑结构. 除主网络之外, 根据功能的不同, 网络中还会形成扩展网络. 如比特币中小算力矿工会选择加入矿池形成中心化矿池网络, 采用 Stratum 协议[39] 与矿池通信, 共同完成挖矿任务. 网络层还需要匿名网络通信技术提供匿名通信等安全保障.

网络层包含多种网络技术, 技术本身的安全问题必然会对区块链网络层带来安全风险. 总的来说, 网络层的安全问题主要包括 P2P 网络的安全问题、网络拓扑被用于攻击以及网络层面的隐私保护问题.

3.2.1 P2P 网络安全漏洞

P2P 网络为对等网络环境中的节点提供一种分布式、自组织的连接模式, 缺少身份认证、数据验证、网络安全管理等机制. 攻击者可以自由发布非法内容, 传播蠕虫、木马、病毒, 甚至实施分布式拒绝服务攻击 (Distributed denial of service, DDoS)、路由攻击等, 具有不易检测、传播迅速等特点. 由于 P2P 网络采用不同于 C/S 网络的对等工作模式, 无法使用防火墙、入侵检测等技术进行有针对性的防护, 网络中的节点更易遭受攻击. 另外, P2P 网络中节点也不是完全平等的. 节点的权限会因加入网络的先后顺序而有所差异. 越先加入网络的节点占据的资源越多, 越可能限制新加入节点享有的数据资源和操作权限. 因此, 在 P2P 网络上建立的区块链也会存在各节点享有资源和权限不均等的情况, 轻节点容易受到全节点的限制.

3.2.2 节点的网络拓扑

节点的网络拓扑结构会为攻击者寻找攻击目标并实施攻击创造便利. 攻击者可以采用主动式注入报文或者被动式监听路由间传输的数据包来监测网络拓扑结构, 很容易获得目标节点的路由信息并控制其邻居节点, 进而实施攻击. 日蚀攻击 (Eclipse attack)[16] 就是攻击者利用节点间的拓扑关系实现网络隔离的一种典型攻击方式. 其基本思想是攻击者通过网络拓扑控制目标节点的数据传入传出节点, 限制目标节点与外界的数据交互, 甚至将目标节点与区块链主网络隔离, 使目标节点仅能接收到攻击者传输的消息, 导致目标节点保存的区块链视图与主网区块链视图不一致, 破坏局部的一致性. 日蚀攻击可作为其他攻击的基础[40]. 当网络出现阶段性区块链分叉竞赛时, 攻击者利用日蚀攻击迫使目标节点将计算资源浪费在无效的区块链上. 攻击者还可以针对算力优势节点实施日蚀攻击, 实现算力的分

离, 影响挖矿奖励的分配, 降低网络中的有效算力, 进一步降低自私挖矿 (Selfish mining) 和双重支付等攻击的难度.

3.2.3 隐私保护问题

数据层的隐私保护技术利用密码学技术从数据结构角度为区块链中用户与交易提供了基本的隐私保护, 却无法避免交易在网络传输中与用户 IP 地址之间的关联性. 用户创建交易并打包成 IP 数据包, 经过网络路由间传输至整个区块链网络. 攻击者可以利用监听并追踪 IP 地址的方式推测出交易之间、交易与公钥地址之间的关系, 破坏了区块链追求的隐私保护目标.

著名的洋葱网络 Tor[41] 是比特币中应用最广泛的匿名通信系统, 融合了洋葱代理、网络拓扑、加密等技术, 防止攻击者通过监听、流量分析等手段追踪交易的用户身份, 在一定程度上阻断了数据包与节点 IP 地址之间的关联性. 为了提高网络层的隐私保护, 一些节点采用 Tor 网络通讯系统来隐藏数据包的源 IP 地址. 然而, Tor 网络技术尚不完善, 理论上的威胁模型较弱, 仅能抵御非全局的主动攻击和被动攻击. 即使通信双方均使用 Tor 网络进行匿名传输, 攻击者仍然可以通过时间攻击和通讯流攻击检测网络中数据流的通信延迟、洋葱代理之间数据包的相关性, 判断数据包的匿名路径, 进而追踪到用户的 IP 地址.

网络层还为数字货币领域中的匿名支付提供了混币技术支持. 混币技术是指网络中的不同用户由中心节点组织或者自发地形成短暂的混币网络, 以混淆交易的方式保证攻击者难以根据混币后的交易推测出真实交易双方的对应关系, 实现匿名支付.

混币技术包括中心化混币和去中心化混币两类. 中心化混币由第三方服务器来执行交易混淆的过程. 用户需要将交易代币发送到第三方账户上, 经服务器多次交易最终发送给交易接收方. 中心化混币破坏了区块链的去中心化特点, 存在第三方设置后门窃取代币、单点失效等问题. 为了防止第三方恶意泄露混币过程, Bonneau 等于 2014 年提出 Mixcoin 混币协议[42], 引入审计机制监管第三方. 2015 年, Valenta 等使用盲签名技术对 Mixcoin 协议进行优化, 防止第三方泄露混币过程[43]. 然而, 中心化混币提供的隐私保护强度与混币次数有关, 普遍存在混币成本高、效率低等问题.

去中心化混币通过用户自发的将多个交易混合产生一笔新的交易, 对代币按原交易进行再分配, 从而实现匿名支付. 2013 年, Maxwell 提出的 Coinjoin 协议是最早的去中心化混币方案[44]. 2014 年, Ruffing 等对 Coinjoin 协议进行改进, 提出一种名为 CoinShuffle 的交易洗牌协议[45]. 2015 年, Ziegeldorf 等利用安全多方计算构造了允许部分节点失效甚至实施恶意操作的 CoinParty 混币协议[46]. 去中心化混币技术规避了中心化混币协议单点失效和成本高等问题, 操作简单, 在数字货币领域中有广泛应用. 但是去中心化混币存在恶意渗入, 混币成员恶意泄露混币过程的问题, 无法抵御 DoS 攻击, 无法兼顾效率和隐私保护需求.

3.3 共识层

共识层是区块链架构的核心, 主要规定了区块链的共识机制, 确保各节点在网络层提供的网络环境和通信模式中可以共享同一份有效的区块链视图 (View). 区块链的最大创新在于共识层支持的共识机制提供了一种剔除可信第三方的可信数据共享机制, 为上层应用提供安全的账本支持[47]. 共识层致力于设计高安全性、高效率、低能耗的共识机制, 根据采用的基础协议不同, 可以划分为 5 大系列, 包括 PoW、PoS、拜占庭容错协议 (Byzantine fault tolerance, BFT)、分片技术、可信硬件.

良好的共识机制有助于提高区块链系统的性能效率, 提供强有力的安全性保障, 支持功能复杂的应用场景, 促进区块链技术的拓展与延伸. 区块链上的共识机制发展尚不完善, 普遍存在安全性证明不完备、安全性假设不可靠、扩展性差、一致性不稳定、初始化和重构难等问题. 不同类型的共识机制还面临不同的攻击威胁.

3.3.1 安全性证明不完备

共识机制在安全性建模时需要考虑网络时序性、节点数量拓展、在线离线切换、算力或权益的动态分布、共识难度变更、区块链增长速率等多变量因素. 由于共识机制下层的网络环境复杂, 新的共识机制不断涌现, 传统的可证明安全框架无法完全适用于区块链. 共识机制的安全性面临建模困难、安全性证明不完备的问题.

2015 年, Garay 等为 PoW 构建了安全模型, 并在静态同步网络模型中分析了比特币的安全性[26]. Kiayias 等在此基础上引入区块产生速率作为共识机制安全性分析的一项因素[48]. Sompoinsky 等在同一时期研究了网络延迟对 PoW 安全性的影响[49]. Pass 等于 2017 年从网络延迟和 PoW 难度之间的关系入手, 对 PoW 进行可证明安全分析[50]. Kiayias 等也在一系列 PoW 可证明安全成果的基础上, 提出了同步网络中 PoS 的安全模型和证明方法[51]. 现阶段对共识机制的可证明安全研究大多集中在 PoW 和 PoS 两类共识机制中, 缺乏一般性. 研究中往往仅考虑单一变量, 对多变量模型下的共识机制的安全性分析还不成熟. 复杂的网络环境也为

共识机制的安全性分析带来挑战.

3.3.2 安全性假设不可靠

现代密码体制的安全性评估依赖计算复杂性理论, 常用可证明安全理论将密码体制的安全性归约到某个公开的数学困难问题上, 如椭圆曲线上的离散对数问题. 然而, 采用 PoW 和 PoS 的共识机制的安全性假设并不依赖计算困难问题, 而是依赖所有的诚实节点所拥有的算力或者权益占多数这类看似合理的假设. 这些安全性假设在实际应用中很容易被打破. 以采用 PoW 的比特币为例, 根据 BTC.com 2018 年 10 月发布的矿池算力分布, 如果排名前四的矿池合谋, 形成具有绝对算力优势的超级节点, 总算力约占全网算力的 56.5 %, 直接打破 PoW 的安全性假设. 矿池合谋可实施 51 % 攻击, 甚至有针对性地实施 DoS 攻击, 阻止交易的验证和记录, 破坏共识机制的活性.

3.3.3 一致性不稳定

如何保证共识机制可以持续稳定地实现一致性是目前共识层的研究重点. 一致性是衡量共识机制安全性强弱的重要性质. PoW 和部分 PoS 共识方案在达成共识的过程中需要等待后续区块生成才能判断之前的区块是否被大多数节点认可, 会出现短暂的分叉, 仅实现弱一致性. 类似 PoA[52]、2-Hop[53] 等采用 PoW 和 PoS 相结合的共识机制也存在短暂分叉的情况.

为了解决 PoW 和 PoS 系列共识方案存在的弱一致性问题, 2017 年, Kiayias 等将 PoS 与安全多方计算 (Multi-party computation, MPC) 结合, 提出了 Ouroboros 区块链共识方案[51], 增强了 PoS 的一致性, 但要求节点持续在线, 无法保证新节点的安全加入. Gilad 等利用 PoS 实现密码抽签算法并结合拜占庭容错协议, 提出了 Algorand 方案[54], 仅能在理想情况下以极高的概率保持一致性.

然而, 在实际应用中, 节点通过共识机制完成一致性的效果受网络影响严重. 当网络同步性较差, 即使网络中没有恶意节点进行主动攻击, 共识机制也无法稳定保持强一致性. 如果网络中存在攻击者利用网络层节点拓扑结构隔离网络, 形成网络分区, 那么将很容易产生短暂的区块链分叉, 破坏一致性.

针对共识机制一致性的攻击有双重支付攻击和长程攻击 (Long-range attack). 双重支付攻击是破坏共识机制一致性的典型攻击方式, 是数字货币方案设计中需要解决的首要安全性问题. 在比特币中, 双重支付攻击的目的是重复花费自己已经使用过的一笔比特币. 在一般区块链中, 双重支付攻击是指攻击者企图在区块链上记录一笔与现有区块链上的交易相违背的无效交易. 常用的方法是产生一条更长的区块链分叉, 使包含原交易的区块链被大多数矿工丢弃. 长程攻击是 PoS 中潜在的攻击行为. 由于 PoS 中矿工挖矿需要付出的代价极低, 具有权益优势的节点有可能从创世块开始产生一条完全不同的区块链分叉, 即为长程攻击.

目前, 区块链共识机制的安全性需要依赖良好的网络环境、严格受限的敌手能力和强安全性假设, 在实际应用中很难确保稳定的一致性. 即使消逝时间证明 (Proof of elapsed time, PoET)[55] 和运气证明 (Proof of luck, PoL)[56] 利用可信硬件提供随机性, 保证共识机制的一致性不受网络状况影响. 但是如果硬件中设置后门, 整个区块链将被完全控制.

3.3.4 扩展性差

可扩展性是区块链共识机制研究关注的重要属性, 是区块链可用性必不可少的一部分[57]. 比特币 PoW 平均每 10 分钟产生一个区块, 且区块内包含的交易数量有限, 交易吞吐量低, 扩展性差. 一些研究通过引入分片技术来提高 PoW 的可扩展性. 分片技术的思想是将网络中的节点进行有效分组, 从而实现多组数据验证和记录的并行操作. 分片技术的关键在于设计合理的分片方式, 支持周期性轮换和新旧节点更替, 同时还要兼顾跨分片交易的原子性问题. Elastico 协议是区块链上首个基于分片思想的共识机制[58], 利用 PoW 对网络中的节点进行分组, 不同分组并行处理不同的数据, 再由特定一组进行打包记录. Omniledger 利用随机数生成算法 RandHound 协议和基于可验证随机函数的抽签算法实现定期分组, 并提出利用锁定交易的方式处理跨分片交易[59]. 此外, 英国央行提出的法定数字货币框架 RSCoin 方案[25] 也在许可区块链中采用分片技术提高区块链的扩展性.

目前, 如何提高区块链共识机制的可扩展性仍然是一个主流研究方向. 分片技术虽然从理论上解决了 PoW 扩展性差的问题, 却引入了跨链交易原子性问题, 需要强安全假设, 降低了区块链的安全性. 另外, 区块链上的共识机制还面临粉尘攻击、交易的 DoS 攻击和空块攻击等. 粉尘攻击指攻击者发布大量小额交易, 增加区块链网络负载, 占据矿工交易池硬盘空间, 造成大量交易排队等待验证的情况, 进而对网络中其他有意义的交易进行 DoS 攻击, 影响共识效率和系统吞吐量. 空块攻击则是矿工为了尽快解决 PoW 问题, 仅填充区块头部, 而不验证打包任何交易, 从而在竞争挖矿过程中能够更快地发布区块并获得区块奖励. 虽然空块攻击不影响区块链的有效性, 却拖慢了交易验证和记录的效率, 加剧了 PoW 等共识机制扩展性差的问题.

3.3.5 初始化难问题

大量研究关注共识机制实现一致性的过程, 往往忽略了区块链的初始化问题, 即如何在 P2P 网络中保证创世块的安全生成. 区块链的初始化直接关系到后续共识机制的执行过程是否安全可靠, 是保证共识机制稳定可靠的前提. 区块链一直面临初始化困难的问题.

目前, 区块链的初始化有两种方式, 一种是依赖第三方产生创世块, 另一种由现有的、成熟的区块链自然过渡得到新区块链的创世块. 依赖第三方初始化违背了区块链去中心化的设计初衷, 无法适用于 P2P 网络中的无许可区块链方案, 也无法确保第三方生成的创世块的随机性与安全性, 可能会左右后续区块的生成. 依赖成熟的基于 PoW 区块链过渡产生创世块的方式增加了初始化的复杂性. 用于初始化的 PoW 潜在的不安全因素将直接影响创世块的安全性和后续区块的生成. 例如将 PoW 作为以账户余额为权益的 PoS 区块链的初始化, 根据已有的 PoW 区块链中的账户余额分布来产生 PoS 区块链的创世块. 攻击者可以预先通过存款、转账等方式产生权益优势节点, 以很高的概率获得产生创世块的记账权. 另外, 初始化过程需要 PoW 提供随机性. 在 PoW 区块链中具有较高算力的节点也可以产生一个有利于自己的 PoW 区块, 从而提升自己获得 PoS 创世块记账权的概率.

3.3.6 重构困难问题

共识机制赋予了区块链不可篡改性, 提升了系统的可信度, 但是也增加了区块链重构的难度. 一旦出现共识机制的安全性假设被打破、数据层密码组件被攻破、代码漏洞被利用等严重威胁区块链安全性的攻击, 在缺少可信第三方或者外界干预的情况下, 区块链无法有效实现灾难恢复, 无法自动恢复到被攻击之前的安全状态. 无效数据或违法操作被写入区块链并执行, 将对用户造成不可弥补的损失, 甚至影响整个区块链的后续运行.

硬分叉是目前区块链唯一可行的重构方式. 2016 年 The DAO 事件发生之后, 有 89% 以太坊成员投票支持采用硬分叉的方式进行重构, 自受攻击位置之前的区块后创建一条区块链分叉, 强制退回被窃取的以太币. 但是, 硬分叉重构存在很多局限性. 首先, 硬分叉直接破坏了共识机制的一致性和不可篡改性的本质特点, 区块链可信度会受到影响. 其次, 判断是否需要进行硬分叉重构的投票方式不一定公平, 投票成员可能会支持更有利于自己的决定. 最后, 硬分叉后网络中存在新旧两条区块链分叉, 旧区块链分叉无法被彻底消除. 由于包含恶意交易的区块中还包含一些合法交易, 硬分叉的过程必然会对这些合法交易的交易双方造成利益损失.

3.4 激励层

在无许可区块链中, 激励层与共识层相互依存, 共同维护区块链系统的安全性与稳定性. 共识机制设计直接影响激励实体的选取和激励分配策略. 相应地, 激励机制设计是否合理也关系到共识机制的安全性和区块链的稳定性. 网络中的节点参与交易验证和区块生成的目的是为了获得更高的奖励. 驱利的节点可能会在这一过程中采取一些不利于区块链系统维护的策略来提高自己的收益, 甚至对区块链的安全性构成威胁. 因此, 激励层还需要策略性行为检测和动态的奖励机制优化.

激励层需要解决的主要问题是经济学上的激励不相容问题, 具体指参与维护区块链的矿工不会实施危害安全性的恶意攻击, 但是会以自身利益最大化来指导自己的挖矿策略. 这种策略与区块链整体利益形成冲突, 破坏区块链系统效率和稳定性, 包括自私挖矿攻击[60]、Nothing at stake 攻击、扣块攻击 (Withholding attack)[61] 和激励不可持续问题.

3.4.1 自私挖矿攻击与 Nothing at stake 攻击

在理想情况下, 基于 PoW 的区块链中节点能够获得的区块奖励期望与他所拥有的计算资源成正比. 而在实际比特币区块生成中, 一些节点可能会在自己成功完成 PoW 产生区块后, 有策略地广播自己的区块, 以获得高于自己所拥有的计算资源比例的奖励收益, 即实施自私挖矿攻击. 自私挖矿攻击是 Eyal 等于 2013 年提出的一种针对 PoW 的攻击行为, 不易检测和预防. 理论上, 基于 PoW 和 PoS 的无许可区块链系统都可能遭到自私挖矿攻击, 对共识机制的安全性和激励机制的公平性造成严重威胁.

自私挖矿包含多种挖矿策略, 最典型的是当某 PoW 区块链矿工成功生成一个区块后不立即广播, 而是在这个新区块后继续挖矿. 当监测到网络中产生一个新区块时, 自私挖矿节点才公开自己的区块, 形成区块链分叉竞赛. 如果自私挖矿节点可以抢先产生两个连续的区块, 不仅可以成功获得区块奖励, 还能消耗掉另一个分叉区块所包含的工作量. 即使自私挖矿节点没能成功产生连续的两个区块, 仍然可能形成长度为 1 的分叉, 将网络算力进行分离, 降低网络中的有效算力. Eyal 等的研究表明, 当网络中的节点随机选择区块链分叉进行拓展时, 拥有 1/3 算力的自私挖矿节点即可获得 1/2 区块奖励期望, 直接破坏激励机制的公平性, 对 PoW 的安全性假设造成威胁, 也影响区块链的扩展性, 降低了区块链的效率.

与自私挖矿类似, Nothing at stake 攻击是针对 PoS 激励机制的一种攻击. 由于 PoS 中节点生成区

块的成本较低, 当出现区块链分叉时, 为了利益最大化, 矿工的最佳策略是在两个区块链分叉后均进行挖矿. 这就使得发起区块链分叉的恶意攻击极容易成功, 增加了区块链分叉和双重支付的概率.

3.4.2 扣块攻击

矿池降低了个体参与挖矿的成本, 人人都可参与维护区块链获得奖励收益. 矿池也将节点集结起来形成算力或权益优势节点, 威胁共识机制的安全性假设. 矿池间的博弈也对区块链安全性、效率产生巨大影响. 一些矿池为了获得更高的奖励会利用目标矿池的奖励分配策略来实施扣块攻击, 通过委派部分矿工加入到目标矿池贡献无效的工作量, 分得目标矿池的奖励, 追求矿池整体获得更高的奖励. 扣块攻击对采用 PPS (Pay-per-share) 模式、PPLNS (Pay per last N shares) 模式和 PROP (PROPortionately) 奖励分配方式的目标矿池的攻击效果明显, 且不易检测[62]. 为了获得更高的长远收益, 矿池会纷纷实施扣块攻击. 扣块攻击与自私挖矿攻击类似, 在一定程度上削减了网络中的有效算力, 降低了系统吞吐量, 造成交易验证延迟甚至网络拥塞的情况, 影响区块链的可扩展性.

3.4.3 不可持续问题

比特币等数字货币的激励机制包含区块奖励和交易费两部分, 其中占矿工节点主要收益的区块奖励普遍呈现逐渐减少直至降为 0 的趋势. 随着区块奖励的降低, 这些区块链必将完全依赖交易费驱动系统, 面临不可持续的问题. 2016 年, Carlsten 等研究了在仅依赖交易费来激励节点的极端情况下区块链的稳定性[63]. Carlsten 等认为仅依赖交易费奖励难以避免形成公地悲剧, 产生大量区块链分叉, 影响区块链的安全性和效率. 攻击者利用节点都想获得更高收益的心理产生区块链分叉, 仅打包部分交易, 给后续的区块预留了大量交易费奖励. 其他节点为了利益最大化必然会在剩余交易费较多的区块链分叉后面进行拓展, 而丢弃预先到达的区块链. 为此, 一些研究人员建议持续发行代币来维护系统稳定. 但是, 持续代币发行会出现通货膨胀. 长此以往, 区块奖励将不再具有吸引力.

此外, 多数激励机制仅奖励成功生成区块的节点, 对其他诚实参与共识协议的节点不予以奖励. 激励机制无法客观评估各节点维护系统所贡献的工作量权重, 对危害区块链安全性的攻击行为也不予以经济惩罚, 奖励分配缺乏公平性与合理性.

3.5 合约层

智能合约是合约层的核心, 是一种可自动执行的数字化协议, 包含相关代码和数据集, 部署在区块链上, 也是可按照预设合约条款自动执行的计算机程序. 智能合约最早由 Nick Szabo 提出, 后经以太坊重新定义, 并建立完整的开发架构. 围绕智能合约, 合约层还包括智能合约的运行机制、编写语言、沙盒环境和测试网络. 运行机制描述了智能合约的执行规则. 编写语言包括以太坊平台提供的 Solidity、Serpent、LLL 等图灵完备语言和 Fabric 使用的 Go、Java 等高级编写语言. 沙盒环境是一种新型的恶意代码检测和防治技术, 为用户提供一种相对安全的虚拟运算环境. 以太坊以以太坊虚拟机 (Ethereum virtual machine, EVM) 为智能合约提供沙盒环境. 此外, 为了保证智能合约的安全性, 用户编写智能合约后还需要在测试网络上进行测试.

以太坊是最早的开源智能合约开发平台[11]. 本节主要围绕以太坊梳理智能合约的安全问题. 虽然以太坊为智能合约编写提供了一些模板和测试环境, 但是由于智能合约代码开源、涉及数字资产转移, 一旦代码漏洞被利用, 会造成不可逆转的损失. 除智能合约创建者在设计业务逻辑时的文本安全问题以外, 合约层还面临智能合约代码漏洞、外部数据源调用、缺乏形式化验证、难实现隐私保护等问题.

3.5.1 代码漏洞

由于以太坊采用自制的脚本语言编写智能合约, 尚不成熟, 难以避免出现漏洞. 根据智能合约漏洞研究[64−65] 总结, 常见的智能合约中的代码漏洞和执行过程中存在的攻击如下:

1) 交易依赖攻击: 智能合约执行过程中的每次操作都需要以交易的形式发布状态变量的变更信息, 不同的交易顺序可能会触发不同的状态, 导致不同的输出结果. 这种智能合约问题被称为交易顺序依赖. 恶意的矿工甚至故意改变交易执行顺序, 操纵智能合约的执行.

2) 时间戳依赖攻击: 一些智能合约执行过程中需要时间戳来提供随机性, 或者作为某些操作的触发条件. 而网络中节点的本地时间戳略有偏差, 攻击者可以通过设置区块的时间戳来左右智能合约的执行, 使结果对自己更有利.

3) 调用栈深度攻击: 以太坊 EVM 设置调用栈深度为 1 024, 攻击者可以先迭代调用合约 1 023 次再发布交易触发该合约, 故意突破调用栈深度限制, 使得合约执行异常.

4) 可重入攻击: 当一个合约调用另一个合约时, 当前执行进程就会停下来等待调用结束, 这就产生了一个中间状态. 攻击者利用中间状态, 在合约未执行结束时再次调用合约, 实施可重入攻击. 著名的 The DAO 事件就是攻击者实施可重入攻击, 不断重复地递归调用 withdrawblance 函数, 取出本该被清

零的以太坊账户余额, 窃取大量以太币.

5) 整数溢出攻击: 智能合约中规定了整数的范围, 难以避免变量、中间计算结果越界, 导致整数溢出. 程序中仅保存异常结果, 影响智能合约的执行.

6) 操作异常攻击: 智能合约的执行可能需要调用其他合约, 缺少被调用合约的状态验证或返回值验证将会对智能合约的执行带来潜在威胁. 部分被调用合约执行异常, 异常结果可能会传递到调用合约上, 影响调用合约的执行.

7) Gas 限制: 以太坊规定了交易消耗的 Gas 上限, 如果超过则交易失效. 如果 Gas 消耗设计不合理, 则会被攻击者利用实施 DoS 攻击. Extcodesize 和 Suicide 是 DoS 攻击者反复执行降低 Gas 操作的攻击实例, 最终导致以太坊交易处理速度缓慢, 浪费了大量交易池硬盘存储资源.

3.5.2 外部数据源调用问题

区块链最初的设计是为了在无可信第三方的情况下实现安全支付, 仅能对区块链上的数据进行操作. 区块链和智能合约迫切地需要通过可信技术访问外部数据, 建立与外部数字世界的连接. 预言机作为可信实体成为了连接智能合约和 Web API 之间的桥梁, 却引入了安全问题. TLSnotary 和 Town-Crier 方案[66] 利用超文本传输协议安全 HTTPS 协议访问外部数据, 是一种提供加密可检查信息的预言机. 但是它们不能保证不同节点访问的数据的一致性与真实性, 也无法避免数据提供网站恶意变更数据或被攻击引起单点失效问题. Augur 方案[67] 通过设置惩罚机制, 要求特定用户在特定时间返回结果, 否则将面临罚款, 但并没有为用户提供随意接入系统的接口, 限制了预言机的可用性.

3.5.3 形式化验证不完善

以太坊提供的 EVM 具有错综复杂的语义, Solidity 语言尚不成熟, 暴露出来的安全问题直接危害智能合约的执行和用户的个人数字资产, 需要形式化验证和程序分析工具对智能合约代码和执行过程进行分析.

目前, 已有一些针对智能合约形式化验证的工具出现. Oyente 提供了一系列针对 EVM 漏洞检测的启发式引擎驱动. Hevm 以一种交互式修复漏洞模式允许智能合约逐步地执行操作码. Manticore 是一种符号化的执行引擎, 包括 EVM 在内的多种模式, 支持具体程序方案、符号化执行驱动和断言检测等. REMIX 是一种基于浏览器的智能合约编写和漏洞修补的 IDE JavaScript 应用, 内嵌的静态分析工具可以针对已知的预定义漏洞进行检测. F* 是一种用于程序验证的通用函数式编程工具[68], 支持验证工具的自动执行和基于依赖类型证明的表达, 可以对实际智能合约的语义正确性和运行过程的安全性进行验证. 但是, 现有的形式化验证和程序分析工具多是针对已知漏洞的检测和验证. 未来的研究将更加关注现有的智能合约的反模式, 构造动态检测的程序分析工具.

3.5.4 隐私保护问题

以太坊、超级账本项目都是开源的智能合约平台, 上面支持的智能合约普遍都是公开的. 智能合约常涉及多用户的参与, 执行也需要用户提供经济激励, 用户的账户信息、交易、智能合约的状态变量等信息都公开于整个网络中, 亟需增加隐私保护机制.

与数据层相似, 密码学技术也可以为提高智能合约隐私保护特性提供强有力的技术保障. 其中, 零知识证明可以隐藏用户身份和交易内包含的知识. Hawk[69] 在仅支持匿名交易的 Zerocash 协议的基础上进行扩展, 利用零知识证明技术和安全多方计算实现了具有隐私保护的智能合约编写框架, 保证交易和合约参与方身份对合约以外的人匿名, 但是仍然存在合约代码隐私性的问题. 同态加密技术也被视为增强智能合约隐私保护的新兴技术, 可以为智能合约提供可信执行环境.

然而, 引入隐私保护机制必然会增加智能合约执行难度, 用户也需要付出更多经济激励成本. 一些需要高保密性、功能复杂的应用场景给智能合约的设计和编写提出了挑战. 密码学技术在实际应用中也具有局限性. 零知识证明系统和同态加密方案构造困难、效率低、占用区块链存储空间, 不适用小成本、时效性要求高的智能合约, 是目前制约智能合约隐私保护发展的主要因素.

3.6 应用层

区块链在金融、供应链、能源等多领域具有广泛的应用场景[70−71]. 虽然在不同的应用场景下, 应用层需要反映不同的区块链的业务功能, 在设计上略显差异. 但是, 应用层作为直接与用户交互的区块链层级, 在架构设计上还具有一定的共同点. 一般地, 应用层需要具备 API 接口、跨链异构和监管技术. 从当前区块链应用发展来看, 应用层设计面临跨链操作难、监管技术缺失和应用层攻击等问题.

3.6.1 跨链操作难

面对数量众多的异构区块链应用, 亟需跨链技术将它们连接起来, 构建互联、互通、互信的区块链应用网络. 去中心化的区块链无法像传统网络系统通过中心节点实现互通, 如何实现去中心化区块链平台间的连接、解决跨链操作的原子性问题是跨链技术面临的最大挑战.

区块链研发人员意识到跨链技术的重要性, 先

后使用公证机制、侧链或中继网络、哈希时间锁合约 (Hash time lock contract, HTLC) 和分布式私钥控制等技术实现异构区块链互联.

1) 公证机制: 通过中间节点资金托管的方式保证安全支付. 2015 年, Ripple 团队提出 Interledger 协议[72], 通过一个或多个第三方连接器账户进行资金托管, 形成跨链交易路径, 可以保证两个异构区块链之间的代币兑换, 却面临单点问题.

2) 侧链或中继网络: 将侧链或中继区块链作为异构区块链间的中介网络, 典型代表有 Cosmos 和 Polkadot 方案. Cosmos 是 Tendermint 团队开发的区块链互联网络, 通过主干网上的中继器将异构的区块链子网进行互联, 从而实现各数字资产交易, 是价值互联网的代表. Polkadot 利用中继区块链网络实现了以太坊与其他区块链之间的跨链通信, 不仅支持代币兑换, 也尝试构建通用的跨链通信技术.

3) 哈希时间锁合约: 要求只有在规定时间内给出正确的哈希值原像的节点才可以使用这笔被锁定的代币. 在闪电网络中, 若两个节点之间没有建立通道, 则可以通过哈希时间锁进行安全的链下交易.

4) 分布式私钥控制: 通过安全多方计算或者门限密钥分享等方式实现对账户资产的锁定与解锁.

目前, 跨链技术的发展还处于初级阶段, 需要大量理论研究和实验测试支撑. 跨链技术研究还多限于金融领域的代币兑换和跨境支付, 要实现异构区块链通信还有待进一步研究.

3.6.2 监管技术缺失

比特币和以太坊先后出现的暗网交易、勒索病毒、数字资产被盗等安全事件引起了社会各界对区块链平台监管缺失问题的广泛讨论. 监管技术的目标是对于非法行为的检测、追踪和追责, 从而保证区块链平台的内容安全. 然而, 区块链去中心化、不可篡改、匿名等特点却增加了监管机制设置的难度.

比特币作为目前最成熟、市场占有率最高的区块链数字货币应用, 自然而然成为监管技术研究的主要场景[19]. 部分研究提出通过政府设立专门的执法机构或者数字货币交易平台等第三方对比特币地址进行追踪, 对非法交易进行定位. 另一个研究方向是放弃比特币的匿名性以降低实施监管的难度, 或者牺牲去中心化特点构造多中心化的替代方案, 各中心具有不同的监管权限, 共同实现对区块链的监管. 这些监管方案或多或少都牺牲了区块链的优势特点, 方案的可行性还有待评估. 一些第三方企业和科研机构也专注设计区块链监管技术, 为政府执法机关提供比特币网络犯罪监控支持, 如美国的 Chaianalysis 公司、加拿大的 BIG (Blockchain Intelligence Group) 公司和桑迪亚国家实验室等.

现有的研究成果很难从根本上对比特币上出现的洗钱、黑市交易、勒索等违法犯罪行为进行有效的防范、分析和追责. 虽然已经开发出一些比特币去匿名化工具, 已有的网络数据分析和监管方案普遍采用 “一刀切” 的监管技术手段, 危害正常使用比特币进行合法交易的诚实用户的隐私. 与跨链技术研究现状相似, 比特币上现有的监管技术不一定适用于其他区块链应用平台, 如何实现既保护诚实用户隐私又监控非法用户行为的可控监管技术将长久地成为区块链应用发展需要突破的关键技术.

3.6.3 其他攻击

理想情况下, 用户可以直接通过区块链应用层提供的功能接口来调用相应的区块链服务. 然而, 多数应用还需要依赖第三方中介机构和区块链服务供应商. 这就为攻击者从应用层进行攻击创造了条件. 例如, 用户使用比特币钱包供应商提供的密钥管理服务时, 就面临后门攻击和密钥泄露的风险. 在应用层开发过程中同样存在代码漏洞问题, 尤其在第三方平台介入的应用场景下, 更容易出现越权漏洞风险. 钓鱼攻击、中间人攻击、木马劫持等传统网络攻击手段也会对上层区块链应用构成威胁. 另外, 在有多方参与的区块链应用中, 攻击者可以在个人权限范围内控制应用软件或硬件, 实施 MATE 攻击 (Man-at-the-end attack)[73], 违反应用层协议规定或行业规范, 恶意泄露或篡改用户信息, 破坏数据的保密性与完整性. 在应用层的设计上还需要充分考虑组织管理上的人员安全, 增强应用层的软件保护.

4 区块链的平行安全

区块链的平行安全理论是在区块链生态环境中利用平行智能理论和 ACP 方法 (Artificial systems + Computational experiments + Parallel execution, 人工系统 + 计算实验 + 平行执行)[74−75] 实现区块链的安全决策. 平行安全理论通过形式化地描述区块链安全相关的共识算法、节点状态、网络环境、激励机制等核心要素的静态特征与动态行为来构建人工区块链系统, 根据区块链上已发现的攻击以及尚未发现但理论上潜在的攻击, 利用计算实验对不同区块链应用场景进行不同的人工攻击实验, 从容错能力、节点行为策略、响应时延、交易吞吐量等多维度评估区块链的抗攻击能力, 并寻求区块链的最优安全防御策略. 人工区块链系统还需要与实际区块链系统进行虚实交互与闭环反馈, 用人工攻击实验结果辅助实际区块链系统实现决策寻优与平行调谐. 本质上, 区块链的平行安全系统就是以人工区块链系统作为 “计算实验室”, 利用不同攻击策略下的人工区块链系统试错实验与理性慎思, 实现真

实区块链系统在遭受安全威胁时的实时管理与决策.

区块链的平行安全理论框架如图 5 所示, 其核心思想是基于 ACP 方法来实现区块链系统建模、攻击模拟实验与辅助决策, 即: 利用人工系统 (A) 方法对实际区块链系统建模, 能够反映实际系统的运行状态; 利用计算实验 (C) 方法, 在人工系统中进行不同的人工攻击实验、分析和评估, 从而掌握对应实际区块链系统在各种攻击下的演化规律与应对措施, 形成完善的 “情景 - 应对” 知识库; 利用平行执行 (P) 方法, 通过人工系统和实际系统在相同攻击下的平行执行与协同演化, 实现对实际区块链系统的学习与培训、实验与评估、管理与控制.

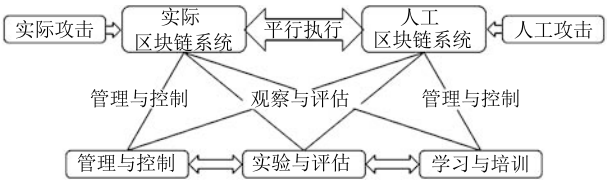

图 5　区块链的平行安全框架

Fig. 5　A framework of parallel security on blockchain

区块链的平行安全系统可以实现区块链安全决策最优化, 准确高效地解决区块链系统在实际运行中遇到的安全威胁. 然而, 平行安全更多地是一种指引性安全攻防范式, 其落地实施还需要逐步解决区块链复杂生态系统的整体建模、攻击模拟、区块链的计算实验与智能解析、人工系统与实际系统的双向引导与协同演化等问题.

5　未来区块链安全方面研究重点

区块链的创新性在于实现了分布式共识, 其上运行的智能合约也可实现丰富的业务功能, 具有重要的研究价值和广阔的应用前景. 尽管区块链的理论研究和应用发展日新月异, 但是目前区块链体系架构中的各个层面均存在安全缺陷, 还需要在共识机制、隐私保护、监管机制、跨链技术等方面进一步研究探索.

5.1　打破 “不可能三角”

共识机制是保证区块链数据一致性的关键, 也是影响区块链系统性能效率的主要环节, 在区块链出现至今的发展历程中, 一直都是学术界和产业界关注的焦点. 虽然共识机制的研究取得了一些成果, 但是依然面临去中心化、安全性和可扩展性三者不可兼顾的问题.

PoW 是最早应用在区块链上的共识机制, 一直存在效率低、能耗高等问题. 低能耗的 PoS 共识方案面临易分叉的安全问题. 有相对完善证明体系的 BFT 协议不支持大规模节点扩展, 网络开销较大. 分片技术提高系统效率的同时也造成安全性弱的问题. 利用可信硬件实现共识会有后门风险. 如何打破 “不可能三角” 僵局, 兼顾去中心化、安全性和可扩展性是区块链共识机制发展要解决的重要问题.

5.2　隐私保护与可控监管

隐私保护和监管机制都是未来区块链安全方面需要重点研究的方向.

隐私保护在开放式网络环境中必不可少. 在区块链体系架构中, 隐私保护涉及数据层、网络层、合约层和应用层, 依赖零知识证明、同态加密等密码学技术、混币技术、Tor 网络等匿名网络通讯技术, 实现对交易数据、用户身份、智能合约和用户行为信息的保护. 各种技术在实际应用过程中都存在局限性. 未来区块链隐私保护的发展既要依赖具有高安全性、高效率的密码方案, 也要关注用户身份、交易信息、合约代码等多方面的隐私保护.

监管机制是区块链世界与现实社会组织结构之间重要的衔接点, 有助于拓宽区块链的应用范围, 为区块链应用平台提供纯净健康的网络环境, 是区块链应用层架构不可或缺的组件. 未来区块链上的监管机制设计将从政策规定和技术工具两个层面并行发展, 关注区块链的内容安全. 国家要加强制定不同领域区块链应用的合法操作规则和必要的政策约束. 企业需要根据具体应用设置适用的政策制度, 如银行必要的 KYC 和 AML 政策. 政策规定的制定有利于明确违法行为范畴和技术层面的设计目标. 技术层面上将更关注去中心化区块链平台上监管技术的设计和实现, 研究智能化内容抽取、分析、处理技术和分布式网络预警技术.

在未来区块链发展中, 如何兼顾隐私保护和监管至关重要. 监管机制一方面要从预防、检测、追踪、追责等方面处理区块链网络中的违法数据, 另一方面也要保护合法用户的隐私信息, 在隐私保护与监管这一对矛盾体中寻求平衡, 建立保护诚实用户隐私、追踪非法用户信息的可控监管体系.

5.3　区块链互联

为了丰富区块链的功能、完善区块链生态、实现区块链价值最大化, 区块链与外部数字世界、物理世界和异构区块链之间的互联将成为未来发展趋势. 在实现区块链互联的过程中会面临诸多安全问题, 也将成为未来区块链安全方向的研究重点.

区块链应用大多针对数字货币, 数据流动也仅限于区块链内部, 形成数据孤岛. 为了使区块链上数据多元化, 支持更多功能, 区块链不可避免要引入外部数据源, 实现与外部数字世界的互联. 预言机是目前实现区块链与外部数字世界安全互联的主流研究

方向. 在与外部数字世界互联时, 区块链的去中心化与外部数据源的中心化运营形成对立. 如何保证由第三方服务器提供的数据源真实可信, 是区块链与外部数字世界互联要解决的核心问题.

区块链在物联网行业具有可观的应用前景. 区块链与物理世界的安全互联有助于加快去中心化物联网管理系统的实现, 有望解放物理世界中心化负载严重的问题, 颠覆物理世界的组织管理模式. 区块链与物理世界互联既要利用区块链的优势解决物理世界的信息安全、大规模存储和效率等问题, 也要平衡去中心化区块链与中心化物理世界的冲突关系.

大量区块链平台分立于区块链生态体系中, 处于相互独立状态. 众多异构的区块链平台需要有效的跨链技术实现互联. 然而, 区块链跨链技术普遍存在效率低的问题. Interledger、Cosmos 等主流跨链协议也仅能实现跨链的金融支付交易, 协议移植差, 不适用其他应用场景. 虽然 Polkadot 跨链方案支持更多类型的区块链互联, 但是方案设计尚处于研究阶段, 不能广泛应用在区块链平台上. 跨链技术在设计过程中需要更加注意安全性、执行效率和跨链操作的原子性问题.

5.4 系统级安全体系

区块链的发展还需要建立系统级安全体系, 从整体上提升区块链的安全性, 推动区块链安全标准化, 为区块链开发和使用提供设计、管理和使用指南. 区块链系统级安全体系的构建将围绕数据安全、共识安全、隐私保护、智能合约安全和内容安全等安全目标, 关注区块链的物理存储、密钥管理、网络传输、功能应用、机密数据和可控监管等方面的技术规范和保护措施.

6 结束语

区块链解决了分布式网络中的一致性问题, 颠覆了依赖可信第三方实现大规模组织管理控制的传统技术架构, 应用逐渐延伸至金融、物联网、智能制造等众多领域, 成为全球学术界的研究热点. 区块链行业风风火火发展的同时, 技术本身存在的共识安全薄弱、隐私泄露、系统漏洞、监管缺失、扩展性差等问题正阻碍区块链的发展. 区块链安全是系统稳定发展的基石, 包括数据、共识、内容、智能合约和隐私保护等, 自下而上贯穿区块链整个体系架构, 需要依赖密码学组件、一致性共识算法、网络安全技术等多方支撑. 利用平行智能理论和 ACP 方法构建的区块链平行安全理论是指导区块链安全决策的新型理论范式. 区块链安全方面的未来发展也将围绕去中心化高阈值容错的可扩展共识机制设计、隐私保护与可控监管机制之间的平衡、区块链可信互联的实现和完善的安全体系的构建等方向, 促进区块链应用的健康发展.

References

1 Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [Online], available: https://bitcoin.org/bitcoin.pdf, October 5, 2018

2 Dwork C, Naor M. Pricing via processing or combatting junk mail. In: Proceedings of the 12th Annual International Cryptology Conference. California, USA: CRYPTO, 1992. 139−147

3 Yuan Yong, Wang Fei-Yue. Blockchain: the state of the art and future trends. *Acta Automatica Sinica*, 2016, **42**(4): 481−494
(袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, **42**(4): 481−494)

4 Walport M. Distributed ledger technology: beyond blockchain [Online], available: https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain, October 5, 2018

5 Ministry of Industry and Information Technology. Chinese blockchain technology and application development white paper2016 [Online], available: http://www.fullrich.com/Uploads/article/file/2016/1020/580866e374069.pdf, October 5, 2018

6 McWaters R, Bruno G, Galaski R, Chaterjee S. The future of financial infrastructure: an ambitious look at how blockchain can reshape financial services [Online], available: https://www.weforum.org/reports/the-future- of -financial- infrastructure-an-ambitious-look-at -how-blockchain-can-reshape-financial-services, October 5, 2018

7 Takemoto Y, Knight S. Mt. Gox files for bankruptcy, hit with lawsuit [Online]. available: http://www. reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228, October 5, 2018

8 Hon M T W K, Palfreyman J, Tegart M. Distributed ledger technology & Cybersecurity [Online]. available: https://ec.europa.eu/futurium/en/content/distributed-ledger-technology-cybersecurity, October 5, 2018

9 Yaga D, Mell P, Roby N, Scarfone K. Blockchain technology overview [Online]. available: https://csrc.nist.gov/publications/detail/nistir/8202/draft, October 5, 2018

10 De Prisco R, Lampson B, Lynch N. Revisiting the Paxos algorithm. In: Proceedings of the 11th International Workshop on Distributed Algorithms. Saarbrücken, Germany: Springer 1997. 111−125.

11 Lamport L. The part-time parliament. *ACM Transactions on Computer Systems*, 1998, **16**(2): 133−169

12 Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. New Orleans, USA: OSDI, 1999. 173−86

13 Ongaro D, Ousterhout J K. In search of an understandable consensus algorithm. In: Proceedings of the USENIX Annual Technical Conference. Philadelphia, PA, USA: USENIX ATC, 2014. 305−119

14 Oki B M, Liskov B H. Viewstamped replication: a new primary copy method to support highly-available distributed systems In: Proceedings of the 7th Annual ACM Symposium on Principles of Distributed Computing. Toronto, Ontario, Canada: ACM, 1988. 8−17

15 King S, Nadal S. Ppcoin: peer-to-peer crypto-currency with proof-of-stake [Online], available: https:// bitcoin.org/bitcoin.pdf, October 5, 2018

16 Buterin V. A next-generation smart contract and decentralized application platform [Online], available: https://github.com/ethereum/wiki/wiki/White-Paper, October 5, 2018

17 Yuan Yong, Wang Fei-Yue. Blockchain and cryptocurrencies: model, techniques, and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2018, **48**(9): 1421−1428

18 Peters G W, Panayi E. Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money. *Banking Beyond Banks and Money*. Berilin: Springer, 2016. 239−278

19 VukolićM. Rethinking permissioned blockchains. In: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. Abu Dhabi, United Arab Emirates: ACM, 2017. 3−7

20 Danezis G, Meiklejohn S. Centrally banked cryptocurrencies [Online]. available: https://arxiv.org/abs/1505.06895, October 5, 2018

21 Halpin H, Piekarska M. Introduction to security and privacy on the blockchain. In: Proceedings of the 2017 Security and Privacy Workshops (EuroS&PW). Paris, France: IEEE, 2017. 1−3

22 Heilman E, Kendler A, Zohar A, Goldberg S. Eclipse attacks on bitcoin′s peer-to-peer network. In: Proceedings of 24th USENIX Security Symposium. Washington, D.C, USA: USENIX, 2015: 129−144

23 Delmolino K, Arnett M, Kosba A, Miller A, Shi E. Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. In: Proceedings of the International Conference on Financial Cryptography and Data Security. Christ Church, Barbados: Springer, 2016. 79−94

24 Bernstein D J. *Introduction to Post-quantum Cryptography*. Berlin: Springer-Verlag, 2009. 1−14

25 Qin Bo, Chen Li Chang-Hao, Wu Qian-Hong, Zhang Yi-Feng, Zhong Lin, Zheng Hai-Bin. Bitcoin and digital fiat currency. *Journal of Cryptologic Research*, 2017, **4**(2): 176−186 (秦波, 陈李昌豪, 伍前红, 张一锋, 钟林, 郑海彬. 比特币与法定数字货币. 密码学报, 2017, **4**(2): 176−186)

26 Garay J, Kiayias A, Leonardos N. The bitcoin backbone protocol: analysis and applications. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Sofia, Bulgaria: EUROCRYPT, 2015. 281−310

27 Chen L, Jordan S, Liu Y K, Moody D, Peralta R C, Perlner R A. Report on post-quantum cryptography [Online], available: https://www.nist.gov/publications/report-post-quantum-cryptography, October 5, 2018

28 Torres W A A, Steinfeld R, Sakzad A, Liu J K, Kuchta V, Bhattacharjee N, et al. Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice ringCT v1. 0). In: Proceedings of the 23rd Australasian Conference on Information Security and Privacy. Wollongong, NSW, Australia: ACISP, 2018. 558−576

29 Jarecki S, Kiayias A, Krawczyk H, Xu J. Highly-efficient and composable password-protected secret sharing (or: how to protect your bitcoin wallet online). In: Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P). Saarbrucken, Germany: IEEE, 2016. 276−291

30 Fleder M, Kester M S, Pillai S. Bitcoin transaction graph analysis [Online]. available: https://arxiv.org/abs/1502.01657, October 5, 2018

31 Saberhagen N. CryptoNote v 2.0 [Online]. available: https://static.coinpaprika.com/storage/cdn/whitepapers/1611.pdf, October 5, 2018

32 Noether S. Ring signature confidential transactions for Monero [Online]. available: https://eprint.iacr.org/2015/ 1098, October 5, 2018

33 Miers I, Garman C, Green M, Rubin A D. Zerocoin: anonymous distributed e-cash from bitcoin. In: Proceedings of the 2013 IEEE Symposium on Security and Privacy. Berkeley, CA, USA: IEEE, 2013. 397−411

34 Bitansky N, Chiesa A, Ishai Y, Paneth O, Ostrovsky R. Succinct non-interactive arguments via linear interactive proofs. In: Proceedings of the 2013 Theory of Cryptography. Tokyo, Japan: Springer, 2013. 315−333

35 Sasson E B, Chiesa A, Garman C, Green M, Miers I, Tromer E, et al. Zerocash: decentralized anonymous payments from bitcoin. In: Proceedings of the 2014 IEEE Symposium on Security and Privacy. CA, USA: IEEE, 2014. 459−474

36 Decker C, Wattenhofer R. Bitcoin transaction malleability and MtGox. In: Proceedings of the 2014 European Symposium on Research in Computer Security. Wroclaw, Poland: ESORICS, 2014. 313−326

37 Karame G O, Androulaki E, Roeschlin M, Gervais A, Ĉapkun S. Misbehavior in bitcoin: a study of double-spending and accountability. *ACM Transactions on Information and System Security (TISSEC)*, 2015, **18**(1): No.2

38 Rajput U, Abbas F, Heekuck O. A solution towards eliminating transaction malleability in bitcoin. *Journal of Information Processing Systems*, 2018, **14**(4): 837−850

39 Lewenberg Y, Bachrach Y, Sompolinsky Y, Zohar A, Rosenschein J S. Bitcoin mining pools: a cooperative game theoretic analysis. In: Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems. Istanbul, Turkey: AAMAS, 2015. 919−927

40 Nayak K, Kumar S, Miller A, Shi E. Stubborn mining: generalizing selfish mining and combining with an eclipse attack. In: Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P). Saarbrucken, Germany: IEEE, 2016. 305−320

41 Reed M G, Syverson P F, Goldschlag D M. Anonymous connections and onion routing. *IEEE Journal on Selected areas in Communications*, 1998, **16**(4): 482−494

42 Bonneau J, Narayanan A, Miller A, Clark J, Kroll J A, Felten E W. Mixcoin: anonymity for bitcoin with accountable mixes. In: Proceedings of the 2014 International Conference on Financial Cryptography and Data Security. Christ Church, Barbados: Springer, 2014. 486−504

43 Valenta L, Rowan B. Blindcoin: blinded, accountable mixes for bitcoin. In: Proceedings of the 2015 International Conference on Financial Cryptography and Data Security. San Juan, Puerto Rico: Springer, 2015. 112−126

44 Maxwell G. CoinJoin: bitcoin privacy for the real world [Online]. available: https://bitcointalk. org/index. php, October 5, 2018

45 Ruffing T, Moreno-Sanchez P, Kate A. CoinShuffle: practical decentralized coin mixing for bitcoin. In: Proceedings of the 2014 European Symposium on Research in Computer Security. Wroclaw, Poland: ESORICS, 2014. 345−364

46 Ziegeldorf J H, Grossmann F, Henze M, Inden N, Wehrle K. Coinparty: secure multi-party mixing of bitcoins. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. New York, USA: ACM, 2015. 75−86

47 Yuan Yong, Ni Xiao-Chun, Zeng Shuai, Wang Fei-Yue. Blockchain consensus algorithms: the state of the art and future trends. *Acta Automatica Sinica*, 2018, **44**(11): 2011−2022
(袁勇, 倪晓春, 曾帅, 王飞跃. 区块链共识算法的发展现状与展望. 自动化学报, 2018, **44**(11): 2011−2022)

48 Kiayias A, Panagiotakos G. Speed-security tradeoffs in blockchain protocols [Online]. available: https://eprint.iacr.org/2015/1019.pdf, October 5, 2018

49 Sompolinsky Y, Zohar A. Secure high-rate transaction processing in bitcoin. In: Proceedings of the 2015 International Conference on Financial Cryptography and Data Security. San Juan, Puerto Rico: Springer, 2015. 507−527

50 Pass R, Seeman L, Shelat A. Analysis of the blockchain protocol in asynchronous networks. In: Proceedings of the 2017 Annual International Conference on the Theory and Applications of Cryptographic Techniques. Paris, France: EUROCRYPT, 2017. 643−673

51 Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: a provably secure proof-of-stake blockchain protocol. In: Proceedings of the 2017 Annual International Cryptology Conference. Santa Barbara, USA: CRYPTO, 2017. 357−388

52 Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of activity: extending bitcoin′s proof of work via proof of stake [extended abstract]. *ACM SIGMETRICS Performance Evaluation Review*, 2014, **42**(3): 34−37

53 Duong T, Fan L, Zhou H S. 2-hop blockchain: combining proof-of-work and proof-of-stake securely [Online]. available: https://eprint.iacr.org/2016/716.pdf, October 5, 2018

54 Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N. Algorand: scaling byzantine agreements for cryptocurrencies. In: Proceedings of the 26th Symposium on Operating Systems Principles. Shanghai, China: ACM, 2017. 51−68

55 Chen L, Xu L, Shah N, Gao Z, Lu Y, Shi W. On security analysis of proof-of-elapsed-time (poet). In: Proceedings of the 2017 International Symposium on Stabilization, Safety, and Security of Distributed Systems. MA, USA: Springer, Cham, 2017. 282−297

56 Milutinovic M, He W, Wu H, Kanwal M. Proof of luck: an efficient blockchain consensus protocol[Online], available: https://eprint.iacr.org/2017/249.pdf, October 5, 2018

57 Zeng Shuai, Yuan Yong, Ni Xiao-Chun, Wang Fei-Yue. Scaling blockchain towards bitcoin: key technologies, constraints and related issues. *Acta Automatica Sinica*, DOI: 10.16383/j.aas.c180100
(曾帅, 袁勇, 倪晓春, 王飞跃. 面向比特币的区块链扩容: 关键技术, 制约因素与衍生问题. 自动化学报, DOI: 10.16383/j.aas.c180100)

58 Luu L, Narayanan V, Zheng C, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM, 2016. 17−30

59 Kokoris-Kogias E, Jovanovic P, Gasser L, Gailly N, Ford B. Omniledger: a secure, scale-out, decentralized ledger via sharding. In: Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP). CA, USA: IEEE, 2018. 583−598

60 Eyal I, Sirer E G. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 2018, **61**(7): 95−102

61 Bag S, Ruj S, Sakurai K. Bitcoin block withholding attack: analysis and mitigation. *IEEE Transactions on Information Forensics and Security*, 2017, **12**(8): 1967−1978

62 Kiayias A, Koutsoupias E, Kyropoulou M, Tselekounis Y. Blockchain mining games. In: Proceedings of the 2016 ACM Conference on Economics and Computation. Maastricht, The Netherlands: ACM, 2016. 365−382

63 Carlsten M, Kalodner H, Weinberg S M, Narayanan A. On the instability of bitcoin without the block reward. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria: ACM, 2016. 154−167

64 Luu L, Chu D H, Olickel H, Saxena P, Hobor A. Making smart contracts smarter. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria: ACM, 2016: 254−269

65 Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (sok). In: Proceedings of the 2017 International Conference on Principles of Security and Trust. Uppsala, Sweden: Springer, 2017. 164−186

66 Zhang F, Cecchetti E, Croman K, Juels A, Shi E. Town crier: an authenticated data feed for smart contracts. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. Vienna, Austria: ACM, 2016. 270−282

67 Peterson J, Krug J, Zoltu M, Williams A K, Alexander S. Augur: a decentralized oracle and prediction market platform [Online]. available: http://media.abnnewswire. net/media/en/whitepaper/rpt/93144-Augur_Whitepaper.pdf, October 5, 2018

68 Grishchenko I, Maffei M, Schneidewind C. A semantic framework for the security analysis of ethereum smart contracts. In: Proceedings of the 2018 International Conference on Principles of Security and Trust. Thessaloniki, Greece: Springer, 2018. 243−269

69 Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP). CA, USA: IEEE, 2016. 839−858

70 Yuan Yong, Zhou Tao, Zhou Ao-Ying, Duan Yong-Chao, Wang Fei-Yue. Blockchain technology: from data intelligence to knowledge automation. *Acta Automatica Sinica*, 2017, **43**(9): 1485−1490
(袁勇, 周涛, 周傲英, 段永朝, 王飞跃. 区块链技术: 从数据智能到知识自动化. 自动化学报, 2017, **43**(9): 1485−1490)

71 Yuan Yong, Wang Fei-Yue. Parallel blockchain: concept, methods and issues. *Acta Automatica Sinica*, 2017, **43**(10): 1703−1712
(袁勇, 王飞跃. 平行区块链: 概念, 方法与内涵解析. 自动化学报, 2017, **43**(10): 1703−1712)

72 Thomas S, Schwartz E. A protocol for interledger payments [Online]. available: https://interledger.org/interledger. pdf, October 5, 2018

73 Collberg C, Davidson J, Giacobazzi R, Gu Y X. Toward digital asset protection. *IEEE Intelligent Systems*, 2011, **26**(6): 8−13

74 Wang Fei-Yue. Computational experiments for behavior analysis and decision evaluation of complex systems. *Journal of System Simulation*, 2004, **16**(5): 893−897
(王飞跃. 计算实验方法与复杂系统行为分析和决策评估. 系统仿真学报, 2004, **16**(5): 893−897)

75 Wang Fei-Yue. Artificial societies, computational experiments, and parallel systems: a discussion on computational theory of complex social-economic systems. *Complex Systems and Complexity Science*, 2004, **1**(4): 25−35
(王飞跃. 人工社会、计算实验、平行系统: 关于复杂社会经济系统计算研究的讨论. 复杂系统与复杂性科学, 2004, **1**(4): 25−35)

韩 璇 中国科学院自动化研究所复杂系统管理与控制国家重点实验室助理工程师. 2018 年获得中国科学院大学软件工程硕士学位. 主要研究方向为理论密码与区块链技术.
E-mail: xuan.han@ia.ac.cn
(**HAN Xuan** Assistant engineer at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. She received her master degree in software engineering from University of Chinese Academy of Sciences in 2018. Her research interest covers theory of cryptography and blockchain technology.)

袁 勇 中国科学院自动化研究所复杂系统管理与控制国家重点实验室副研究员. 青岛智能产业技术研究院副院长. 2008 年获得山东科技大学计算机软件与理论专业博士学位. 主要研究方向为社会计算, 计算广告学, 区块链技术. 本文通信作者.
E-mail: yong.yuan@ia.ac.cn
(**YUAN Yong** Associate professor at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. He is also the vice president of Qingdao Academy of Intelligent Industries. He received his Ph. D. degree of computer software and theory from Shandong University of Science and Technology in 2008. His research interest covers social computing, computational advertising, and blockchain. Corresponding author of this paper.)

王飞跃 中国科学院自动化研究所复杂系统管理与控制国家重点实验室主任, 国防科技大学军事计算实验与平行系统技术研究中心主任, 中国科学院大学中国经济与社会安全研究中心主任, 青岛智能产业技术研究院院长. 主要研究方向为平行系统的方法与应用, 社会计算, 平行智能以及知识自动化.
E-mail: feiyue.wang@ia.ac.cn
(**WANG Fei-Yue** State specially appointed expert and director of the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. Professor of the Research Center for Computational Experiments and Parallel Systems Technology, National University of Defense Technology. Director of China Economic and Social Security Research Center in University of Chinese Academy of Sciences. Dean of Qingdao Academy of Intelligent Industries. His research interest covers methods and applications for parallel systems, social computing, parallel intelligence, and knowledge automation.)