区块链网络安全保障：攻击与防御

江沛佩[1,2]，王骞[1,2]，陈艳姣[3]，李琦[4,5]，沈超[6]

（1. 空天信息安全与可信计算教育部重点实验室，湖北 武汉 430072；2. 武汉大学国家网络安全学院，湖北 武汉 430072；
3. 武汉大学计算机学院，湖北 武汉 430072；4. 清华大学网络科学与网络空间研究院，北京 100084；
5. 北京信息科学与技术国家研究中心，北京 100084；6. 西安交通大学网络空间安全学院，陕西 西安 710049）

摘 要：随着区块链技术的迅猛发展，区块链系统的安全问题正逐渐暴露出来，给区块链生态系统带来巨大风险。通过回顾区块链安全方面的相关工作，对区块链潜在的安全问题进行了系统的研究。将区块链框架分为数据层、网络层、共识层和应用层 4 层，分析其中的安全漏洞及攻击原理，并讨论了增强区块链安全的防御方案。最后，在现有研究的基础上展望了区块链安全领域的未来研究方向和发展趋势。

关键词：区块链安全；智能合约；隐私保护

中图分类号：TP309

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021035

Securing guarantee of the blockchain network: attacks and countermeasures

JIANG Peipei[1,2], WANG Qian[1,2], CHEN Yanjiao[3], LI Qi[4,5], SHEN Chao[6]

1. Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Wuhan 430072, China
2. School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China
3. School of Computer Science, Wuhan University, Wuhan 430072, China
4. Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China
5. Beijing National Research Center for Information Science and Technology, Beijing 100084, China
6. School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 710049, China

Abstract: While the security of blockchain has been the central concern of both academia and industry since the very start, new security threats continue to emerge, which poses great risks to the blockchain ecosystem. A systematic study was conducted on the most state-of-the-art research on potential security issues of blockchain. Specifically, a taxonomy was developed by considering the blockchain framework as a four-layer system, and the analysis on the most recent attacks against security loopholes in each layer was provided. Countermeasures that can strengthen the blockchain were also discussed by highlighting their fundamental ideas and comparing different solutions. Finally, the forefront of research and potential directions of blockchain security were put forward to encourage further studies on the security of blockchain.

Keywords: blockchain security, smart contract, privacy protection

收稿日期：2020−08−19；**修回日期**：2020−10−21

通信作者：王骞，qianwang@whu.edu.cn

基金项目：国家重点研发计划基金资助项目（No.2020YFB1005500）；国家自然科学基金资助项目（No.U20B2049, No.61822207, No.61972296, No.61822309, No.61773310）；北京信息科学与技术国家研究中心基金资助项目（No.BNR2020RC0101）

Foundation Items: The National Key Research and Development Program of China (No.2020YFB1005500), The National Natural Science Foundation of China (No.U20B2049, No.61822207, No.61972296, No.61822309, No.61773310), Beijing National Research Center for Information Science and Technology (No.BNR2020RC0101)

1 引言

自 2009 年面世以来，比特币[1-2]作为首个完全去中心化的加密货币在学业界和工业界越来越受到关注。比特币交易的底层数据结构是区块链，大量参与者在区块链上创建交易记录，不需要任何可信第三方参与。区块链作为以比特币为代表的数字加密货币体系的核心支撑技术，逐渐成为一种日益普及、全新的去中心化基础架构与分布式计算范式，并引领了人类信用进化史的新一代革新。从技术层面讲，区块链技术实现了交易的去中心化和一定的匿名性，非实名和交易安全是区块链技术最大的优势。除了虚拟货币以外，区块链还在食品、医疗、汽车、运输业等领域提供数据溯源、公平交易等技术支持[3]，例如，文献[4]利用区块链技术实现了对物流系统中交易的监管，其监管架构和我国管理体系吻合，是报道可见的第一个落地的可监管区块链系统。目前，区块链的广泛运用引起了相关政府部门、金融行业机构、科技企业和资本市场的高度关注。

然而，随着区块链的快速发展与普及，其潜在的安全漏洞也逐渐暴露出来。2020 年 7 月底，西班牙加密货币交易平台 2gether 遭攻击，损失约 140 万美元[5]。最近，在以太经典（ETC, Ethereum classic）平台上爆发的一起 51%攻击导致大约价值 560 万美元的加密货币被双倍消费[6]。由此可见，区块链技术的漏洞可能导致无法挽回的财产损失和隐私泄露。目前，国内研究者针对区块链安全问题进行了系统的综述[7-10]，但这些工作与本文的侧重点和覆盖面有所差别。例如，文献[7]侧重于宏观层面的区块链技术发展；文献[9-10]侧重于介绍区块链威胁和漏洞相关研究，没有详细调研针对区块链威胁的具体防御措施。本文除了调研关于区块链安全漏洞的最新进展外，还详细介绍了目前最先进的防御方法，系统地调研了区块链系统的安全性问题。作为一个集成框架，区块链系统可分为 4 层：数据结构层、网络层、共识层和应用层。本文从区块链系统结构角度出发，深入分析数据结构层、网络层、共识层和应用层的安全漏洞、攻击原理以及对应的防御措施。

在数据结构层，最主要的安全威胁源于区块状态的不一致性和底层密码协议的脆弱性。区块链的底层数据结构由区块组成，区块之间通过哈希指针链接。由于可信中心节点的缺失，区块链节点之间可能会存在状态的不一致性，这为分叉攻击的实施带来了可能性。同时，区块链网络还存在吞吐量有限、效率低的问题，这削弱了现有区块链平台的适用性。因此，研究者致力于研究设计可扩展区块链系统，遗憾的是，可扩展区块链的设计加重了区块链的不一致性。针对这一问题，研究者提出了一系列同时保证区块链一致性和可扩展性的协议[11-14]。另外，区块链的安全性由底层密码协议保证，密码协议的漏洞若被攻击者利用[15-16]，会对区块链中数据的真实性、私密性造成危害，甚至可能造成严重的财产损失。

在网络层，攻击的主要目的是破坏区块传播所需的网络基础设施，其中路由攻击[17]是最常见的攻击之一。它会导致挖矿计算资源浪费，甚至为双重支付攻击提供便利。

在共识层，人们需要着重关注矿池的安全问题。随着区块链全网计算能力的不断增强，采矿难度不断升级，独立矿工的收益越来越难以保障。为了实现稳定的收入流，矿工们联合挖矿，组成矿池。然而，矿池的出现引入了再中心化的威胁，一定程度上破坏了区块链系统的安全支柱，这有利于实施 51%攻击和双重支付攻击[18-19]。同时，矿池技术的发展也引起了激烈的竞争和攻击，如自私挖矿[20]、块克制（BWH, block withholding）攻击[21]、块克制后分叉（FAW, fork after withholding）攻击[22]等，这些攻击将会导致挖矿资源浪费。

在应用层，随着加密货币的不断发展和广泛应用，市场对更透明、更智能、更高效的交易需求逐渐增强，这催生了链下支付通道和智能合约的出现。智能合约被视为区块链 2.0 的标志[23]，然而，智能合约的漏洞可能引发安全问题和隐私泄露问题，如交易跟踪、支付中止和虫洞攻击等[24-26]。随着智能合约的日益普及，其安全性已经引起了广泛关注[27-30]。另一方面，匿名货币系统的出现进一步加强了加密货币的匿名性，但现有的匿名货币系统仍存在隐私泄露问题[31-33]。

2 区块链系统模型

区块链系统是多种技术和机制的巧妙结合，可分为数据结构层、网络层、共识层和应用层 4 层，如图 1 所示。基于区块链特殊的数据结构、网络

结构和共识协议，区块链具有分散化、不可篡改性、可追溯性和透明性等特性。本节将从区块链层次结构的角度来概述区块链采用的工作机制，从而帮助读者深入理解各个层次的安全威胁和防御。

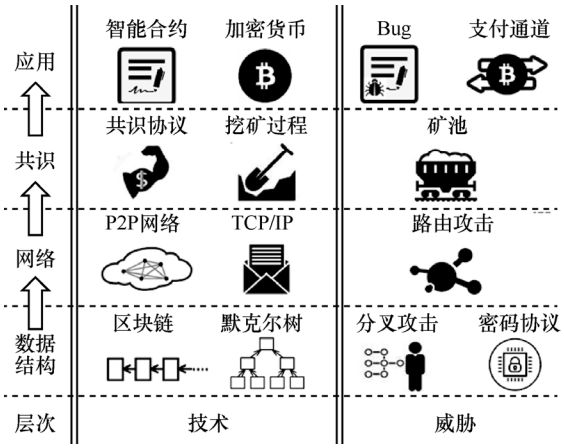

图 1　区块链系统架构

2.1　数据结构层

区块链底层的数据结构是区块，区块之间通过哈希指针链接并形成区块链网络。区块由区块头和区块体构成。区块头中包含关于该区块的主要信息，如上一个块的哈希值、默克尔树根和块时间戳等。根据区块头中的哈希值，可以定位到上一个区块的地址。区块体包含了实际数据，如交易信息等，区块体的内容由区块所有者通过私钥进行签名。由于哈希函数具有单向性和抗碰撞性，并且数字签名具有不可伪造性，区块链的区块内容是不可变且防篡改的。区块链中另一个基础数据结构是默尔克树。默克尔树是一个由哈希值组成的二叉树，它的每一个节点都是由子节点经过哈希函数得到的。在区块链系统中，默尔克树被用来验证交易的完整性，自下而上逐层计算默尔克树的哈希值即可快速验证交易。

2.2　网络层

区块链系统网络层通信的基础结构是基于 TCP 连接的非结构化对等（P2P, peer-to-peer）网络。非结构化网络易于构造，并且对高度动态的网络拓扑（例如，对等者的频繁进出等）具有很强的稳健性。由于区块链网络的目标是尽可能快地分发信息，以达成对区块链的共识，因此在挖矿过程中，新发现的区块会在整个网络中通过泛洪传播。

2.3　共识层

1) 挖矿过程

在共识层中，分布式的参与者对区块链状态达成一致的过程被叫作挖矿。具体来说，为了在区块链网络中达成一致意见，矿工需要运行一个具有容错性质的共识协议，以确保他们都同意附加到区块链条目的顺序。如果要向区块链添加新区块，每个矿工都必须遵循共识协议中指定的一组规则。区块链通过使用工作量证明（PoW, proof of work）机制来实现分布式共识，该机制要求参与者通过破解密码谜题来证明自己的计算能力。成功计算出解决方案的参与者将生成一个区块，并获得铸造该比特币的奖励。

在加密货币平台中，货币的交换以交易链的形式表示。交易链的完整性、真实性和正确性均由分布式矿工验证，他们是去中心化系统的安全支柱。具体来说，挖矿的主要过程如下。

① 矿工将大量待验证的事务捆绑在一个称为块的单元中，并在给定块的情况下执行 PoW 算法。

② 矿工在解开了这个难题后，立即在整个网络上发布关于该区块的广播，以获得采矿奖励。

③ 在成功添加到分布式公共账本（即区块链）之前，该块将被网络中大多数的矿工验证。

④ 当挖掘到的区块成功添加到区块链中时，挖掘该块的矿工将获得一个区块的奖励。

2) 矿池

解开谜题的矿工将获得丰厚的回报，这吸引了大量的矿工参与，显著提高了比特币网络的整体计算能力。密码谜题的难度会随时间变化，系统会根据实际情况将挖掘一个区块的平均时间调整到几乎不变（大约 10 min）。由于生成块的概率与计算能力成正比，单个矿工在有限的计算能力下获得奖励的概率非常低。针对这一局限性，矿工们形成矿池，将群众的力量聚集在一起。在矿池中，矿工们可以解决更简单的密码谜题，并将解决方案（也叫作份额）提交给矿池管理员。然后，矿池管理员将检查该份额是一个部分工作证明（PPoW, partial proof of work）还是一个完整工作证明（FPoW, full proof of work）。注意到，PPoW 对应简单的密码谜题，FPoW 对应原始的密码谜题。接着，管理员分发正比于预估计算能力的奖励给矿工。最终，每个矿工就可以稳定地获得与预期相符的报酬。

2.4 应用层

1) 链下支付通道

目前，比特币网络的最大吞吐量为每秒 7 笔交易（TPS, transaction per second），这意味着用户可能需要等待数十分钟甚至更长的时间才能确认交易。显然，这远远不能满足实际需求。针对这一问题，研究者探究了一系列提高区块链系统可扩展性的方案。提高吞吐量的方法之一是构建链下交易机制[34]，在用户之间建立支付通道，以处理频繁的微交易。链下支付通道的工作流程如图 2 所示。在链下支付通道中，只有在打开和关闭通道时才会访问区块链。提交开启交易后，用户将资金存入相互认可的地址中，并在关闭通道时以最接近的余额返还资金。此外，支付通道网络（PCN, payment channel network）[35]使没有直联通道的用户能通过网络中的一个路径彼此连接。

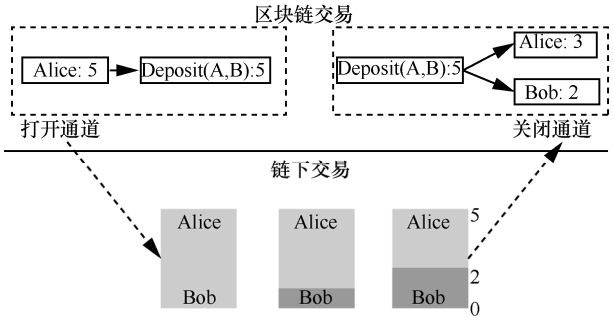

图 2 链下支付通道的基本执行流程

2) 匿名货币

虽然传统加密货币能在一定程度上提供交易匿名性，但实际上比特币网络中的假名地址是伪匿名的。攻击者可以从公开账本中挖掘出许多关于交易的敏感信息，比如交易用户真实身份等。针对这一问题，研究者提出了全新的分布式匿名交易加密货币，如 Dash[36]、Zcash[37]、Monero[38]等。这些匿名货币利用 zk-SNARKs[39]和环签名[40]等密码学工具来保护交易的不可追溯性。

3) 智能合约

在应用层，最具影响力的技术之一是智能合约[23]，它是在以太坊区块链中一段特定地址上的程序。以太坊区块链是目前最受欢迎的支持智能合约的去中心化平台。智能合约由合约中可执行单元的函数和智能合约状态数据组成。在智能合约中，程序代码记录多方之间的逻辑合约条款，并预定义触发条件和响应动作。智能合约中函数是由时间或事件（例如添加到区块链中的事务）触发的，并由达成共识的矿工存储和执行，执行的正确性由区块链的共识协议保证。此外，智能合约还可以接收、存储和发送自己的值。理想情况下，可以认为智能合约是由一个可信的全局机器执行的，它将诚实地执行每条指令。在智能合约的辅助下，金融交易规则可以在没有可靠第三方的情况下执行。

3 区块链安全威胁及攻击

去中心化是区块链系统最吸引人的特性之一，但这一特性也带来了潜在威胁。在区块链自由市场中，恶意参与者可能会利用区块链系统的潜在威胁来获取非法利益。本节将从数据结构层、网络层、共识层、应用层讨论针对区块链的安全威胁，并在表 1 中进行了总结。

3.1 数据结构层安全威胁

区块链的基本组成部分为区块。在交易过程中，不断有新的区块链接到区块链中，而链接过程存在区块链状态不一致和分叉的威胁。另外，区块链底层高度依赖密码算法，攻击者可以利用密码系统的漏洞造成用户私钥泄露，从而引发财产损失等安全问题。

1) 区块链状态不一致性

由于区块链系统中缺乏可信中心节点，交易信息由多个节点共同维护，而这种自由的交易增加了区块链状态的不确定性。具体来说，区块链的安全性建立在绝大多数矿工或计算能力是可信的并且工作在最长的链上这一假设。但实际上，区块链系统的一致性是具有不确定性和概率性的，它需要通过长时间的时延来确认交易，以避免攻击者篡改和利用。不一致的一个主要后果是分叉。如果某个恶意的矿工能成功分叉出一条合法的链，其他所有矿工将切换到这条新的最长链上[21]。这样一来，所有只发生在旧链上的交易都将被取消，从而导致重复消费（即双花攻击[41-42]）和交易反转等一系列问题，造成财产损失。

2) 用户私钥泄露

在比特币交易系统中，交易过程是将资产的所有权从发送方地址转移到接收方的公共地址，该交易内容由签名者使用私钥签名。通常，用户通过比特币钱包存储私钥，比特币钱包是一种树状层次化确定性结构，其私钥和地址由一个主种子生成。在比特币钱包标准 BIP32 架构中[43]，给定主公钥和子

表 1　　区块链安全威胁和防御方法

安全问题	威胁和攻击	描述	负面影响	防御方法	层次
区块链状态不一致性	蓄意分叉	有意地分叉合法链，并在其上进行交易	双重支付，交易反转	集体签名 Rapid ChainChain-Space	数据结构层
密码系统漏洞	用户私钥泄露	分析密码系统漏洞，推测用户私钥	财产损失	加强密码系统安全性	
网络基础设施漏洞	路由攻击	隔离部分网络或时延块传播	采矿资源浪费，双重支付	增加节点连接的多样性，加密通信	网络层
再中心化	51%攻击、双花攻击、网络分区	攻击者控制网络中大量算力	财产损失，交易审查，区块链系统损坏	SmartPoolProof-of-Personhood	共识层
矿池竞争	自私挖矿	选择性地传播被挖掘的块来使其他诚实矿工的块失效	采矿资源浪费	更新 Beacon 值，联合费用	共识层
	BWH	发送 PPoW，而不发送 FPoW	采矿资源浪费		
	FAW	自私挖矿和 BWH 的结合	恶意分叉		
支付通道的安全漏洞	交易跟踪	通过相同通道的关联跟踪交易	信息泄露	BOLT	应用层
	支付中止	通道容量不足导致的交易中止	信息泄露	Fulgor、Rayo	
	虫洞攻击	窃取合法矿工的报酬	财产损失	AMHL	
匿名货币交易隐私泄露	交易指纹识别	分析比特币交易中数额、节点输入输出数量，追踪交易	信息泄露	减少交易信息泄露	应用层
	侧信道攻击	通过时间信息推断交易发出者和接受者的身份	信息泄露	使用无时间差别加密算法	
智能合约漏洞	重入攻击	在智能合约能终止前重新进入函数	财产损失，不公平挖矿	正式认证 符号化执行 运行时间监测	应用层

私钥，攻击者可以非常容易地恢复出主私钥。Courtois 等[15]通过分析比特币钱包密钥管理方案中的随机数和随机事件里的关联性，提出了一种私钥恢复组合攻击。这种攻击能够破坏存储在系统中的密钥安全性，更严重的是，父节点私钥泄露将直接导致子节点私钥泄露，这也被叫作特权升级攻击。另一方面，区块链底层所使用的椭圆曲线数字签名算法（ECDSA, elliptic curve digital signature algorithm）中随机数的重用也可能被攻击者分析、利用，从而使用户私钥暴露[16,44-45]。如果攻击者获取了受害用户的私钥，他/她就能伪造该用户的签名并完成任意交易，比如将受害用户的资产转移到非法账户上。

3.2　网络层安全威胁

在网络层，区块链网络的基础网络基础设施漏洞和自身 P2P 网络结构是引发安全问题的主要原因。

路由攻击[17]是一种被广泛研究的网络攻击，在路由攻击中，自主系统通过劫持边界网关协议（BGP, border gateway protocol）[46]来拦截和操纵比特币流量。Apostolaki 等[17]指出，网络基础设施具有 2 个有利于路由攻击的特点：第一，少数几个自主系统承载大部分比特币节点；第二，路由可以拦截到大量比特币节点的连接。基于这 2 个特点，可以进行分割攻击和时延攻击。在分割攻击中，AS 层攻击者通过劫持边界网关协议，从区块链网络中隔离一组节点 P，这些节点 P 在总挖掘能力中占有相当大的比例。通过利用集中的比特币矿池，攻击者只需劫持 39 个前缀就可以隔离占总挖掘能力近 50%的节点。分割攻击要求攻击者完全控制受害者的流量，而时延攻击则只需时延区块向单个节点的传播，甚至可能只拦截一个连接。由于区块链流量是未加密的，且节点在向一个节点请求阻塞后 20 min 内不会再向另一个节点请求阻塞，攻击者可以通过拦截区块链流量来延迟或阻塞在某些连接上的传播。

通过路由攻击，攻击者可以隔离网络的一部分节点或时延区块传播，这会造成巨大的挖矿能力浪费和收入损失，并使网络暴露于各种各样的漏洞中，如双花攻击[41-42]等。

3.3　共识层安全威胁

区块链的实现很大程度上得益于共识层的设

计。在这一层中，区块链在一个分布式去中心化的账本上运行，链中的所有节点通过共识机制保持统一运行状态。目前，共识层中的大多数安全威胁都是随着矿池的出现而产生的。

1) 再集中

随着开采难度的增加，为了保证个体矿工的稳定收入，越来越多的大型比特币矿池随之形成。然而，这违反了区块链去中心化的原则。如果网络中超过一半的计算能力由单一的矿池运营商控制，区块链将会面临 51%攻击的威胁。51%攻击指的是攻击者控制着比特币网络中超过 51%的采矿能力。显然，将算力集中到一个矿池中有利于实现 51%攻击。矿池运营者可以利用池中大量参与者的强大计算能力发起大规模攻击，如双花攻击[41-42]、网络分割[17]和拒绝服务（DoS, denial-of-service）攻击[47-48]等。此外，由于矿池运营商肩负着分配资源和评估矿池参与者工作量的工作，恶意的矿池运营商可能会有不当行为，例如非法审查区块中的交易等。除了恶意运营商外，矿池中也可能存在恶意矿工，他们可能伪造多个节点，从而发起女巫攻击[49]，女巫攻击同样有利于 51%攻击和分叉攻击的实现。

2) 矿池间的恶性竞争

矿池之间竞争激烈，矿工可能会为了在竞争中获得优势而采取各种攻击手段。一个典型的单人挖矿攻击是自私挖矿[20]。自私的矿工通过选择性地传播被挖掘的块来使其他诚实矿工的块失效，从而蓄意生成分叉。矿池中另一个常见的攻击是 BWH 攻击[21]。在 BWH 中，来自攻击矿池的矿工潜入受害矿池中，在挖矿过程中，攻击者只发送部分工作证明，不发送完整工作证明，最终攻击者可以通过分摊其他矿工发现的完整工作证明从受害池中获取不该属于他/她的报酬。显然，这种攻击方法“损人不利己”，获得的效益很少，甚至可能低于攻击者本该得到的报酬。Kwon 等[22]将 BWH 与自私挖矿相结合，提出了一种新型攻击，名为 FAW 攻击，进一步提高了攻击的效益。与 BWH 中立即丢弃完整工作证明不同的是，在 FAW 攻击中，攻击者将保留完整工作证明块。如果一个矿工在攻击矿池和受害矿池之外生成了有效块，攻击者将把这个块提交给受害矿池的矿池运营商，当矿池运营商传播这个块时，会导致蓄意分叉。如果大多数矿工选择了攻击者区块的分支，那么受害矿池和攻击者均将获得奖励。由于 FAW 攻击的收益对计算能力和网络容量要求不高，因此它比自私挖矿更实用。当 2 个矿池均采用 FAW 时，规模更大的矿池总是受益，小池总是损失，这也打破了 BWH 中双输的矿工困境。不过，FAW 和 BWH 在考虑到算力调整策略的情况下无法达到最优收益，Gao 等[50]提出了算力调整克制（PAW, power adjusting withholding）攻击，能达到更高的收益。

3.4 应用层安全威胁

在应用层，近期研究主要集中在提高性能和拓宽区块链系统的应用潜力上[34,51]，下面，讨论与之密切相关的安全问题。

1) 支付通道的隐私和安全问题

链下支付通道为比特币的交易带来了便捷性，然而，链下支付过程存在着各种潜在的隐私泄露风险。首先，同一通道中的交易是可链接的，这使交易跟踪成为可能。其次，在 PCN 中，当 2 个没有直联通道的用户利用中介用户帮助完成交易时，很难对中介用户保密 2 个用户的身份和交易金额，因为支付路径的唯一标识符隐含了用户和交易信息。更严重的是，当多个事务共享一个容量有限的通道时，所有的支付都将被终止，并导致 PCN 的死锁[25]。同时，虫洞攻击[26]使攻击者能通过隔离中间用户并与恶意矿工合谋来窃取合法矿工的交易费用。因此，为了确保链下支付通道的安全使用，支付通道的隐私和安全问题是值得关注和研究的。

2) 匿名货币交易隐私泄露

匿名货币在一定程度上保护了交易的私密性，然而，最近的一些研究发现目前的解决方案并不完善，仍存在隐私泄露问题。Kappos 等[31]系统地分析了 Zcash 中交易的匿名性，通过研究 Zcash 的透明交易和隐蔽矿池交互，Kappos 等发现利用简单的试探法就可以将隐蔽池中 69%的值和交易联系起来。Biryukov 等[32]则提出了几种“指纹”识别用户交易的攻击。由于比特币交易中的数额可以细分到非常高的精度，交易数额可以被攻击者用作该交易的指纹，从而追溯交易的内在联系。同时，通过观察隐蔽交易输入和输出的数量（该信息在 Zcash Sapling 版本中是公开的，目前版本已经修复），攻击者可以向目标地址发送大量的小额比特币，并跟踪涉及该地址的后续交易。最近，一种远程侧信道攻击[33]分析了匿名交易的证明周期，最终利用零知识证明所需时间的不同、ping 的回应时间等侧信道信息来推断交易发出者和接受者的身份。以上列举的几种

攻击方法说明现有匿名加密货币系统无法达到完全的匿名性，因此，完善匿名货币架构、提高设计的安全性是至关重要的。

3) 智能合约漏洞

在应用层，智能合约也成为安全漏洞的滋生地，经过研究者的大量研究，智能合约的安全漏洞已充分暴露[52]。造成巨大损失的安全漏洞之一是时间限制。时间限制确定了当前状态下允许的操作，一般来说，时间限制是由所有矿工一致同意的块的时间戳决定。在区块中使用相同的时间戳能确保智能合约在矿工中执行结果的一致性。然而，由于时间戳的选择存在一定的不确定性，拥有合约中一定份额的攻击者可以通过选择有利于自己利润的时间戳在挖矿中取得优势。

另一个更严重的安全漏洞是重入问题[53]。理论上，当调用智能合约的非递归部分时，不应该在终止之前重新进入它，从而保证事务的原子性和顺序性。然而，某些指令下的回退机制（例如 CALL 和 CALLCODE 指令）允许攻击者重新进入调用函数。这会导致意外的行为和调用循环。此外，诸如 DELEGATECALL、SELFDESTRUCT、CALL 和 SSTORE 等指令，如果在智能合约中被滥用，可能会造成财产损失。然而，在智能合约的预期行为和实际行为之间很难发现指令的滥用和不匹配。更严重的是，区块链的不变性意味着在部署后智能合约的缺陷得到修复的可能性微乎其微。

4　区块链安全对策

本节将探讨针对区块链系统潜在安全问题的对策，以防御第 3 节中所阐述的攻击。

4.1　数据结构层安全对策

1) 高效保持一致性

如 3.1 节所述，区块的不一致性会引起区块链结构分叉等问题，而保证一致性会影响到区块链系统的运行效率，从而削弱可伸缩性。然而，为提高性能而设计的新方案可能会面临更严重的不一致性问题。

为了提高交易的一致性同时保证高吞吐量，Syta 等[54]提出了一种可扩展的集体签名协议 Cosi 来提高交易的确认效率。在 Cosi 中，首先由领导者要求验证某个区块，然后一群证人利用沟通树和施诺尔多重签名[55]共同签署该区块。生成一个单聚合集体签名后，所有共同签署人就可以通过树外的验证者来验证它，从而减少了每次交易的成本和时延。在 Cosi 的基础上，Kogias 等[11]设计了 ByzCoin——一个具有较强一致性的可扩展区块链架构。如图 3 所示，为了减少确认时延，ByzCoin 中的块被分为微小块和关键块。同时，ByzCoin 利用生成树拓扑来提高吞吐量。有了这些安全措施，当攻击者掌握的计算能力不超过 1/4 时，该系统就可以抵御多重攻击，例如双重支付和蓄意分叉等。然而，底层的 CoSi 协议会使 ByzCoin 变得不可靠，同时会暴露较高的出错概率。因此，文献[12]对 CoSi 协议进行了改进，构建了稳健生成树拓扑，并使用 BLS 多重签名[56]替代了之前的 Schnorr 多重签名，使 ByzCoin 更加可靠。BLS 多重签名可以通过生成树在单轮内完成签名，这样减少了消息的传输，从而降低了失败概率。

另一个提高区块链吞吐量的解决方案是分片[50,57]机制，它将处理交易的开销分割为多个较小的节点

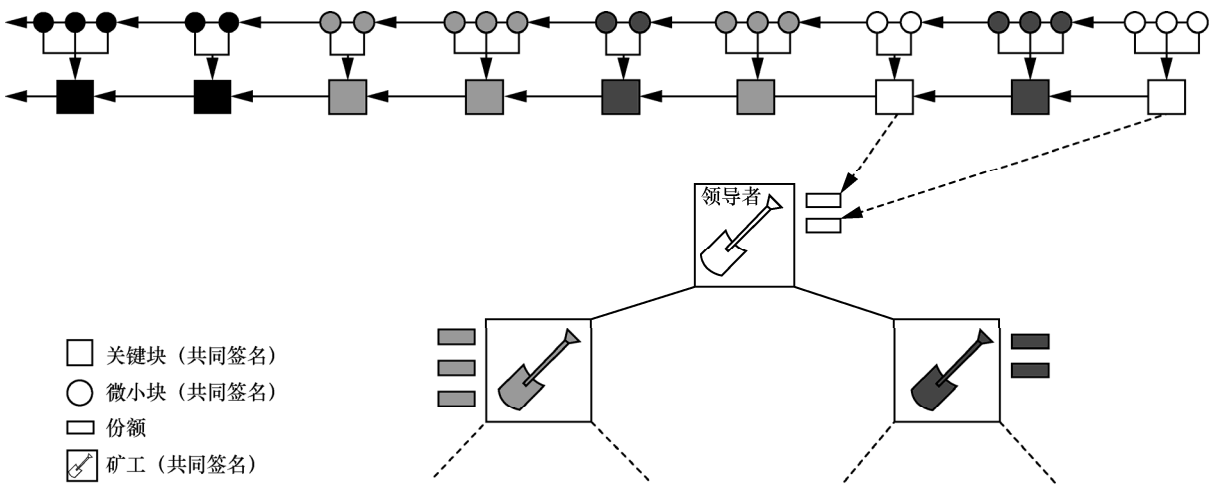

图 3　Byzcoin 的基础框架

组[13-14]。对于基于分片的区块链系统，分片之间的不一致性称为拜占庭故障（BF, Byzantine fault）[58]。为了克服拜占庭故障，RapidChain[13]在协议层对拜占庭故障进行处理。RapidChain 在分片中建立了一个参考委员会，它们需要接收到足够多相同的关于同一区块的消息来验证领导者节点，并在较小的委员会中实现 1/3 的总弹性。RapidChain 能高弹性地对抗拜占庭故障，可以容忍少于 1/3 的破坏节点，优于之前的方案[50,59]（这些方案可以容忍不超过 1/4 的破坏节点）。随后，ChainSpace 实现了一个基于分片的智能合约平台，并使用提出的 S-BAC 协议来保持节点之间的一致性[15]。在 ChainSpace 中，审计者可以发现试图将无效交易或对象引入诚实分片中的恶意分片。文献[60]对实用拜占庭容错协议进行了改进，降低了节点间通信成本，同时结合信誉模型，在一定程度上防御了女巫攻击。然而，之前的分片方案要么不能支持完整的分片，要么降低了分片后的攻击难度。考虑到这一问题，Wang 等[61]提出了 Monoxide 系统，该系统通过引入异步一致性区域的概念，能在不影响去中心化和安全性的情况下对区块链系统进行线性扩展。在每个分片中，Monoxide 采用 Chu-ko-nu 挖矿技术来确保每个区域的有效挖掘能力相当，使攻击者对任意区域的攻击与对整个网络的攻击一样困难。

2) 加强密钥管理和密码系统安全性

针对 3.1 节所述的安全漏洞，BIP32 架构[43]加强了密钥生成函数，其中，子密钥的生成不再直接依赖于父节点的公钥，而是结合父节点的扩展私钥和索引来生成子密钥，该操作能有效防止父节点密钥的泄露。不过这种方案使子节点和父节点的公钥失去了链接性，即无法从父节点公钥生成子节点。Gutoski 等[62]借鉴了冗余的思想，存储多个主私钥，从而增强了比特币钱包对主私钥泄露的容忍性。但这种防御手段仍无法抵抗特权升级攻击。Fan 等[63]设计了一种新型的 HD 钱包方案，该方案使用单向陷门函数处理私钥，进而对所有子节点隐藏私钥，能有效抵抗特权升级攻击。

4.2 网络层安全对策

为了防止路由攻击，从部署的角度划分，可以实行短期和长期对策[17]。短期对策更容易部署，不需要对协议进行任何更改。在区块链网络中，如果来往于一个节点的流量经过多个不同的路径，攻击者必须知道相关的 IP 地址，否则就会摧毁所有的路由。因此，如果节点所有者能增加节点连接的多样性，攻击将变得极其困难。此外，节点还可以监控相关的统计数据，以检测往返时间的突然变化、连接的分布情况等。检测到不寻常事件的节点可以建立额外的随机连接来保护自己不受攻击。

从长远来看，对比特币通信进行加密可以防止信息泄露，例如采用消息认证码（MAC, message authentication code）可以防止消息被篡改；使用 P2P 流量加密协议[64]，可以防止攻击者获取关键信息。这 2 种对策都增加了时延攻击的难度。此外，比特币用户可以要求多个对等方提供某个区块，以免被阻断或错过区块。文献[65]提出了一种通用的检测方法，该工作对挖矿全过程进行了状态模拟，并通过分析区块链当前的状态检测，判断当前区块链系统所面临的攻击力度。

4.3 共识层安全对策

1) 确保区块链的分散化

为了解决共识协议（例如工作量证明或权益证明）的再集中化问题，Borge 等[19]提出了全新的个人身份证明机制（PoP, proof-of-personhood）并设计了一种名为 PoPCoin 的加密货币。个人身份证明协议利用集体签名和环签名将在线身份和离线实体结合起来，使加密货币重新分散化。在 PoPCoin 中，系统为每个用户分配了一个加密的身份令牌，同时不泄露关于个人的敏感信息。这样一来，既保证了问责性，又保证了匿名性。PoPCoin 将加密货币的铸造与用户实体结合，并使每个矿工以相同的速度铸造新币，这使虚拟用户与现实世界紧密联系，从而有利于抵御女巫攻击[49]。

PoPCoin 提供了一种与真人绑定的去中心化货币铸造机制，而 SmartPool[18]则探索了去中心化矿池的可行性，它的核心思想是利用智能合约替代之前的矿池运营商。为了保证采矿奖励分配的公平性，SmartPool 使用概率验证技术来确保恶意矿工不会获得额外利益。这样一来，区块链安全将依赖于整个网络和以太坊的共识机制，而不是单一实体，同时，所需费用也会比普通矿池低。

2) 阻止 FAW 攻击

要检测一个矿池是否被攻击，可以比较矿工提交的 PPoW 和 FPoW。然而，简单的检测攻击是不够的，因为攻击者还可以使用女巫节点获得额外的奖励。一个可行的解决方案是定期更新 beacon 值[22]，如果一个区块包含未更新的 beacon 值，那么它就是

不合法的。另一种方法是引入参与费用来减少女巫节点的数量，但这可能会降低矿池对矿工的吸引力。另外，更有利于 FPoW 的奖励分配方式也有助于激励矿工们诚实挖矿。

4.4 应用层安全对策

1) 链下支付通道的保密性和匿名性

近年来，大量工作致力于分析和提升链下支付通道的安全性。为了构建具有良好保密性的支付通道，Green 等[24]提出了盲链轻量交易（BOLT, blind off-chain light-weight transaction），断开了统一支付通道中交易的联系。作者设计了 3 种支付通道：单向支付通道、双向支付通道和间接支付渠道，并讨论了每种类型的安全风险。BOLT 能在商家不知道付费者身份的情况下创建匿名支付通道。不过在更一般的情况下，交易路径中会存在多个中介，为了保护多跳支付网络的隐私，Malavolta 等[25]设计了多跳哈希时间锁定合约（HTLC, multi-hop hashed time lock contract）。作者在通用可组合性框架的基础上提出了 Fulgor 和 Rayo 这 2 个协议。Fulgor 是 PCN 上首个保护隐私的支付协议，但它是一个阻塞式协议，容易造成死锁；Rayo 是一个非阻塞式协议，解决了死锁问题。基于这 2 个协议，HTLC 能保证支付通道途径的其他用户无法获取交易隐私信息。然而，目前保证支付渠道安全的解决方案，要么是不兼容的[24]，要么是低效的[25]。鉴于上述缺点，Malavolta 等[26]进一步提出一种名为匿名多跳锁（AMHL, anonymous multi-hop lock）的新机制，构建了一种具有高互操作性的实用隐私保护 PCN，该方案通过牺牲额外的一轮通信避免虫洞攻击。表 2 对以上 3 种方案进行了比较。

2) 匿名货币增强

针对指纹分析攻击，Kappos 等[31]提出，如果用户与矿池的交互行为没有规律，该攻击的效率会大大降低。因此可以采取均等支付的方式来抵抗该攻击，即用户均在相同的时间间隔内交易相同数额的资金。这种防御方法能有效抵抗指纹分析攻击[31-32]对用户特有行为的分析。与侧信道攻击的防御思路类似，文献[33]提出可以在底层使用无差别加密算法进行基本操作，这样一来，攻击者无法通过加解密的时间差异侧面推测出敏感信息。但以上的增强方案会使匿名货币系统效率大大降低，因此，如何在保证效率的情况下设计出匿名性好的加密货币系统是目前学术界和工业界的一大挑战。

3) 智能合约加强

为了解决智能合约的安全漏洞，研究者试图从各个方面加强智能合约中的安全短板。Kalra 等[27]设计了 ZEUS，实现了智能合约的自动形式化验证。它制定了规范的 Solidity[66]（一种用于区块链的高级编程语言）语义和策略来确定合约是否可以接受，并提供了从 Solidity 到 LLVM 的位码转换程序。ZEUS 在给定策略规范的情况下能自动插入验证条件。相较于支持 LLVM 级别检测的 ZEUS，TEETHER[28]则致力于字节码级别的验证，可以自动检测第三方漏洞。与开发阶段的调试工具 ZEUS 不同，TEETHER 可以使用符号执行，在不访问合约源代码的情况下，在以太机上检测现有合约的漏洞。通过形成程序的控制流图（GFC, control flow graph），TEETHER 对程序的输出进行分析，以发现其潜在的缺陷路径。TEETHER 和 ZEUS 有不同的设计目标，TEETHER 只关注恶意转账行为，而 ZEUS 更关注智能合约的正确性和公平性。

然而，当恶意行为正在进行时，TEETHER 和 ZEUS 的检测将失去作用。为了解决这个问题，Rodler 等[29]设计了 Sereum 来实时检测重入攻击，该攻击能导致存储变量的改变和进程中合约状态的恶意更新。基于 EVM 字节码指令级别的运行时监视器，Sereum 采用污点跟踪的方法监控变量更新，可以有效地检测可疑行为，防止了基本的和高级的重入攻击。同时，Sereum 对 EVM 进行了扩展，引入了用于监视和防御的污染引擎和攻击检测器。Sereum 能动态地检测重入攻击，但对其他类型的攻击无能为力。Zhang 等[30]设计了 TxSpector，它通过记录字节级的交易进程并构造执行流图（EFG, execution flow graph）来提取数据之间的逻辑关系，最后用户

表 2　3 种链下支付通道方案的比较

方案	交易路径	实现基础	关注问题	是否支持无脚本	应用
BOLT	单跳	压缩 E-cash	隐私	否	Zcash、Bitcoin
HTLC	多跳	多跳 HTLC、ZK-Boo	隐私、并发性	否	Bitcoin、PCN
AMHL	多跳	匿名多跳锁	隐私、互操作性	是	大部分加密货币、原子交换、互操作 PCN

能根据自己制定的规则来进行实时检测，该通用框架可以检测重入攻击、DoS 等多种攻击。

5 区块链安全技术的研究展望

针对前文所总结的区块链系统的安全问题，本节将讨论关于加强区块链安全与防护工作的 4 个研究方向。

5.1 防御网络层攻击

利用边界网关协议劫持等网络攻击，攻击者可以在控制网络运营商的情况下延迟网络中消息的发送，并在以太坊平台上发起平衡攻击。网络是区块链交易的底层基础，在区块链上进行交易时必须考虑网络布局的影响。因此，研究调查更多针对网络的攻击效果并进一步研究 BGP 劫持带来的解决安全问题仍是必要的。

5.2 改进共识层协议

为了实现区块链系统的稳健性和可扩展性，需要在共识机制的安全性和有效性之间进行权衡。集体签名可以提高基于生成树拓扑的可伸缩性，但树结构可能会受到恶意领导节点和中心化的影响[11]。因此，有必要对防范恶意领导和集体签名去中心化进行深入分析。此外，尽管最近的研究在减少女巫节点攻击上取得了一些进展[26]，但目前的研究仍然缺乏能足以防御各种攻击的系统且实用的共识协议。

5.3 加强应用层智能合约

1) 提高链下支付通道的隐私性和匿名性

PCN 目前已经被广泛用来减轻区块链网络的负担，并有许多研究致力于建立具有隐私保护的 PCN 以确保匿名性。然而，PCN 中还存在许多仍未被攻击者利用的弱点，如路由的庞大规模、网络的形成和流动性等。这些弱点一旦加以利用，很有可能对区块链网络形成巨大的安全威胁。另一个问题是 PCN 内部和外部的隐私泄露。HTLC 作为链下支付通道安全措施的核心，其通道路径具有独特性和固定性，但这一操作会公开交易中涉及的用户身份。当 PCN 含有多个中介点时，保持来自中间节点的交易量是一个未解决的问题。此外，根据文献[25]，必须以匿名为代价来维护同步。因此，如何找到一种同时保证同步和匿名性的方法是一个有待解决的问题。

2) 智能合约的安全性

智能合约被认为是最具颠覆性的应用之一，其安全漏洞给大量的投资者和区块链社区投下阴影。Solidity 作为智能合约开发中最常用的语言之一，由于它的特性和安全防范的缺乏，尤其是在公共环境下，Solidity 被认为是不安全的。为了进一步提高智能合约的安全性，一种更安全、对编码人员更有约束的语言是目前的迫切需求。另外，在部署后，由于区块链的不可篡改性，智能合约一旦公开将是不可变的。但是，在智能合约执行期间可能会发现致命的错误。因此，在不修改智能合约的情况下，设计出一种修复漏洞机制是困难但必要的。Krupp 等[28]进一步证明了通过智能合约的字节码暴露漏洞是可行的，因此对字节码层的保护需要进行更多的研究。

5.4 加强匿名货币安全

匿名货币架构目前还存在许多问题，无法达到完全匿名性，例如，攻击者可以通过侧信道、交易指纹等信息跟踪交易。然而，保护侧信道信息的泄露是困难的，而且可能会带来效率的下降，因此可以考虑使用不经意随机存储（ORAM, Oblivious RAM）技术和差分隐私技术来保护交易的敏感信息。另外，如何设计并在区块链系统上应用一种加密时间不固定并且高效的底层加密算法是一种非常有潜力的研究方向。

6 结束语

本文主要关注区块链系统在不同层次上的安全和隐私问题，从区块链的数据结构层、网络层、共识层和应用层 4 个层次分别介绍和分析了区块链系统现有的安全问题及前沿的防御对策。最后，总结了该研究领域的挑战和潜力，并展望了区块链安全未来可能的研究方向。希望本文能为今后区块链安全及相关研究提供指导。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. Manubot, 2019-11-20.

[2] PAXFUL PRESS. Paxful celebrates its 5th year — Reveals hitting $4.6 billion USD in volume and reaching 4.5 million registered wallets [EB/OL]. Paxful Press, 2020-07-14.

[3] IBM. Rewire your industry with IBM Blockchain[EB/OL]. IBM, 2020.

[4] 余春堂, 韩志耕, 李致远, 等. 基于区块链的众包物流分级多层智能服务交易监管架构[J]. 网络与信息安全学报, 2020, 6(3): 50-58.
YU C T, HAN Z G, LI Z Y, et al. Blockchain-based hierarchical and multi-level smart service transaction supervision framework for crowdsourcing logistics[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 50-58.

[5] GOGO J. European Bitcoin exchange hacked for $1.4 million, claims it cannot afford to repay users [EB/OL]. Bitcoin.com, 2020-08-04.

[6] HAIG S. 51% attack bleeds more than $5M from Ethereum classic [EB/OL].

Cointelegraph, 2020-08-06.

[7] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[8] 祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017, 54(10): 2170-2186.
ZHU L H, GAO F, SHEN M, et al. Survey on privacy preserving techniques for blockchain technology[J]. Journal of Computer Research and Development, 2017, 54(10): 2170-2186.

[9] 韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望[J]. 自动化学报, 2019, 45(1): 206-225.
HAN X, YUAN Y, WANG F Y. Security problems on blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2019, 45(1): 206-225.

[10] 斯雪明, 徐蜜雪, 苑超. 区块链安全研究综述[J]. 密码学报, 2018, 5(5): 8-19.
SI X M, XU M X, YUAN C. Survey on security of blockchain[J]. Journal of Cryptologic Research, 2018, 5(5): 8-19.

[11] KOGIAS E K, JOVANOVIC P, GAILLY N, et al. Enhancing Bitcoin security and performance with strong consistency via collective signing[C]//25th USENIX Security Symposium. Berkeley: USENIX Association, 2016: 279-296.

[12] ALANGOT B, SURESH M, RAJ A S, et al. Reliable collective cosigning to scale blockchain with strong consistency[C]// Workshop on Decentralized IoT Security and Standards, co-located with Proceedings of the Network and Distributed System Security Symposium. Reston: Internet Society, 2018.

[13] ZAMANI M, MOVAHEDI M, RAYKOVA M. Rapidchain: scaling blockchain via full sharding[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 931-948.

[14] AL-BASSAM M, SONNINO A, BANO S, et al. Chainspace: a sharded smart contracts platform[C]//25th Annual Network and Distributed System Security Symposium. Reston: Internet Society, 2018: 1-6.

[15] COURTOIS N T, VALSORDA F, EMIRDAG P. Private key recovery combination attacks: on extreme fragility of popular bitcoin key management, wallet and cold storage solutions in presence of poor RNG events[J]. IACR Cryptol. ePrint Arch, 2014(2014): 848.

[16] BRENGEL M, ROSSOW C. Identifying key leakage of bitcoin users[C]//International Symposium on Research in Attacks, Intrusions, and Defenses. Berlin: Springer, 2018: 623-643.

[17] APOSTOLAKI M, ZOHAR A, VANBEVER L. Hijacking bitcoin: routing attacks on cryptocurrencies[C]//2017 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2017: 375-392.

[18] LUU L, VELNER Y, TEUTSCH J, et al. Smartpool: practical decentralized pooled mining[C]//26th USENIX Security Symposium. Berkeley: USENIX Association, 2017: 1409-1426.

[19] BORGE M, KOKORIS-KOGIAS E, JOVANOVIC P, et al. Proof-of-personhood: redemocratizing permissionless cryptocurrencies[C]//2017 IEEE European Symposium on Security and Privacy Workshops. Piscataway: IEEE Press, 2017: 23-26.

[20] EYAL I, SIRER E G. Majority is not enough: Bitcoin mining is vulnerable[C]//International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 436-454.

[21] EYAL I. The miner's dilemma[C]//2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2015: 89-103.

[22] KWON Y, KIM D, SON Y, et al. Be selfish and avoid dilemmas: Fork after withholding (FAW) attacks on bitcoin[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 195-209.

[23] BUTERIN V. A next-generation smart contract and decentralized application platform[R/OL]. White Paper, 2014.

[24] GREEN M, MIERS I. Bolt: anonymous payment channels for decentralized currencies[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 473-489.

[25] MALAVOLTA G, MORENO-SANCHEZ P, KATE A, et al. Concurrency and privacy with payment-channel networks[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 455-471.

[26] MALAVOLTA G, MORENO-SANCHEZ P, SCHNEIDEWIND C, et al. Anonymous multi-hop locks for blockchain scalability and interoperability[C]//26th Annual Network and Distributed System Security Symposium. Reston: Internet Society, 2019: 1-6.

[27] KALRA S, GOEL S, DHAWAN M, et al. ZEUS: analyzing safety of smart contracts[C]//25th Annual Network and Distributed System Security Symposium. Reston: Internet Society, 2018: 1-15.

[28] KRUPP J, ROSSOW C. TEETHER: Gnawing at Ethereum to automatically exploit smart contracts[C]//27th USENIX Security Symposium. Berkeley: USENIX Association, 2018: 1317-1333.

[29] RODLER M, LI W, KARAME G O, et al. Sereum: protecting existing smart contracts against re-entrancy attacks[C]//27th Annual Network and Distributed System Security Symposium. Reston: Internet Society, 2020: 1-15.

[30] ZHANG M, ZHANG X, ZHANG Y, et al. TXSPECTOR: Uncovering attacks in Ethereum from transactions[C]//29th USENIX Security Symposium. Berkeley: USENIX Association, 2020: 2775-2792.

[31] KAPPOS G, YOUSAF H, MALLER M, et al. An empirical analysis of anonymity in Zcash[C]//27th USENIX Security Symposium. Berkeley: USENIX Association, 2018: 463-477.

[32] BIRYUKOV A, FEHER D, VITTO G. Privacy aspects and subliminal channels in Zcash[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 1813-1830.

[33] TRAMÈR F, BONEH D, PATERSON K G. Remote side-channel attacks on anonymous transactions[C]//29th USENIX Security Symposium. Berkeley: USENIX Association, 2020: 2379-2756.

[34] DECKER C, WATTENHOFER R. A fast and scalable payment network with bitcoin duplex micropayment channels[C]//Symposium on Self-Stabilizing Systems. Berlin: Springer, 2015: 3-18.

[35] POON J, DRYJA T. The Bitcoin lightning network: scalable off-chain instant payments[R/OL]. Bitcoinlightning.com, 2016-01-14.

[36] DUFFIELD E, DIAZ D. Dash: a payments-focused cryptocurrency [R/OL]. White Paper, GitHub, 2015.

[37] HOPWOOD D, BOWE S, HORNBY T, et al. Zcash protocol specification[R/OL]. White Paper, GitHub, 2020-01-15.

[38] MÖSER M, SOSKA K, HEILMAN E, et al. An empirical analysis of traceability in the Monero blockchain[J]. Proceedings on Privacy Enhancing Technologies, 2018, 2018(3): 143-163.

[39] BITANSKY N, CANETTI R, CHIESA A, et al. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again[C]//Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. New York: ACM Press, 2012: 326-349.

[40] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2001: 552-565.

[41] ROSENFELD M. Analysis of hashrate-based double spending[J]. arXiv Preprint, arXiv:1402.2009, 2014.

[42] KARAME G O, ANDROULAKI E, CAPKUN S. Double-spending fast payments in Bitcoin[C]//Proceedings of the 2012 ACM Conference on Computer and Communications Security. New York: ACM Press, 2012: 906-917.

[43] WUILLE P. BIP32: Hierarchical deterministic wallets[R/OL]. Bitcoin Improvement Proposal, 2012-02-11.

[44] BREITNER J, HENINGER N. Biased nonce sense: Lattice attacks against weak ECDSA signatures in cryptocurrencies[C]//International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2019: 3-20.

[45] BREITNER J, HENINGER N. Biased nonce sense: lattice attacks against weak ECDSA signatures in cryptocurrencies[C]//International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2019: 3-20.

[46] REKHTER Y, LI T, HARES S. RFC 1771: a border gateway protocol 4 (BGP-4)[R/OL]. IETF RFC 1771. 1995-03.

[47] VASEK M, THORNTON M, MOORE T. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem[C]//International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 57-71.

[48] JOHNSON B, LASZKA A, GROSSKLAGS J, et al. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools[C]// International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 72-86.

[49] DOUCEUR J R. The sybil attack[C]//International Workshop on Peer-to-Peer Systems. Berkeley: USENIX Association, 2002: 251-260.

[50] GAO S, LI Z, PENG Z, et al. Power adjusting and bribery racing: Novel mining attacks in the bitcoin system[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 833-850.

[51] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 17-30.

[52] LUU L, CHU D H, OLICKEL H, et al. Making smart contracts smarter[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 254-269.

[53] FINLEY K. A $50 million hack just showed that the DAO was all too human[EB/OL]. WIRED, 2016-06-18.

[54] SYTA E, TAMAS I, VISHER D, et al. Keeping authorities “honest or bust” with decentralized witness cosigning[C]//2016 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2016: 526-545.

[55] SCHNORR C P. Efficient identification and signatures for smart cards[C]//Conference on the Theory and Application of Cryptology. Berlin: Springer, 1989: 239-252.

[56] INAMURA M, IWAMURA K, WATANABE R, et al. A new tree-structure-specified multi-signature scheme for a document circulation system[C]//Proceedings of the International Conference on Security and Cryptography. Piscataway: IEEE Press, 2011: 362-369.

[57] CORBETT J C, DEAN J, EPSTEIN M, et al. Spanner: Google’s globally distributed database[J]. ACM Transactions on Computer Systems, 2013, 31(3): 1-22.

[58] GILAD Y, HEMO R, MICALI S, ET AL. ALGORAND: scaling byzantine agreements for cryptocurrencies[C]//Proceedings of the 26th Symposium on Operating Systems Principles. New York: ACM Press, 2017: 51-68.

[59] KOKORIS-KOGIAS E, JOVANOVIC P, GASSER L, et al. Omniledger: a secure, scale-out, decentralized ledger via sharding[C]//2018 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2018: 583-598.

[60] 赖英旭, 薄尊旭, 刘静. 基于改进 PBFT 算法防御区块链中 sybil 攻击的研究[J]. 通信学报, 2020, 41(9): 104-117.
LAI Y X, BO Z X, LIU J. Research on sybil attack in defense blockchain based on improved PBFT algorithm[J]. Journal on Communications, 2020, 41(9): 104-117.

[61] WANG J, WANG H. Monoxide: Scale out blockchains with asynchronous consensus zones[C]//16th USENIX Symposium on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2019: 95-112.

[62] GUTOSKI G, STEBILA D. Hierarchical deterministic bitcoin wallets that tolerate key leakage[C]//International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2015: 497-504.

[63] FAN C I, TSENG Y F, SU H P, et al. Secure hierarchical Bitcoin wallet scheme against privilege escalation attacks[J]. International Journal of Information Security, 2020, 19(3): 245-255.

[64] SCHNELLI J. BIP 151: peer-to-peer communication encryption[R/OL]. Bitcoin Improvement Proposal, 2016-03-23.

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

[66] DANNEN C. Introducing Ethereum and solidity[M]. Berkeley: Apress, 2017.

[作者简介]

江沛佩（1997− ），女，湖北武汉人，武汉大学博士生，主要研究方向为应用密码学、网络安全等。

王骞（1980− ），男，湖北武汉人，博士，武汉大学教授、博士生导师，主要研究方向为人工智能安全、云计算安全、无线系统安全、大数据安全与隐私、应用密码学等。

陈艳姣（1989− ），女，山西代县人，博士，武汉大学研究员，主要研究方向为无线网络资源分配、网络安全、区块链等。

李琦（1979− ），男，浙江临安人，博士，清华大学副教授、博士生导师，主要研究方向为网络安全、移动安全和大数据安全。

沈超（1985− ），男，重庆人，博士，西安交通大学教授、博士生导师，主要研究方向为信息物理系统优化与安全、系统与软件安全、人工智能安全等。