·专题一:区块链技术及应用·

区块链安全监管技术研究综述

洪学海[1,2*] 汪 洋[2] 廖方宇[2]

(1. 中国科学院 计算技术研究所,北京 100080;
2. 中国科学院 计算机网络信息中心,北京 100190)

[摘 要] 区块链的安全监管技术已经成为区块链技术及应用研究的重要发展方向之一。本文从区块链的技术特点及其产生安全与监管问题的本源、区块链安全事件频发带来的监管技术发展以及区块链安全监管技术未来的主要研究方向三个方面进行了综述,重点阐述了区块链节点的追踪与可视化、公链的主动发现与探测、联盟链的穿透式监管和以链治链四个方向的技术研究进展情况。

[关键词] 区块链;安全;监管;以链治链

区块链是一项集成计算机科学、数学、经济学等多领域研究成果的组合式创新技术,有潜力为金融、政务、产权、供应链等诸多行业提供变革机会,已成为社会关注的热点名词和市场追捧的热门对象[1,2]。目前,各国对区块链技术本身大多持鼓励和支持的态度,经过概念创新和技术迭代,区块链的应用场景已经扩展到了供应链、身份认证、公益慈善等众多新领域。但由于区块链的监管难题,导致区块链的安全事件频发,形势急剧恶化[3]。如互联网安全公司白帽汇安全研究院发布的《区块链产业安全分析报告》显示,2011 年到 2018 年 4 月,全球范围内因区块链安全事件造成的经济损失高达 28.64 亿美元(约合人民币 196.06 亿元)。因此,为了区块链的健康发展,加强对区块链技术及其应用安全监管研究已经成为业界共识[4]。

1 区块链技术特点及其安全监管问题的技术本源

1.1 区块链的技术特点

区块链是比特币的底层实现技术,原理是将一段时间内系统中产生的交易数据保存入区块,每一个区块通过记录上一区块散列值以及本区块的哈希值等方式彼此相连,形成了一种块链式的数据结构,是一种以密码学算法为基础的点对点分布式账本技术,是分布式存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块的生成过程是链上节点对系统中交易数据顺序性和当前状态一致性达成共识的过程,同时节点根据权限能够参与链上数据的计算、同步与存储,进而能够拥有整个系统的数据备份,能够在没有中心机构节点的场景下,通过分布式共识的方式,构建一个多节点平等参与的数据共享网络。区块链有如下的主要技术特点[5]:

(1) 去中心化的分布式账本系统。区块链本质上是一个去中心化的分布式账本系统,它将密码和时间标签等数据,存储在分布式的数据节点上。这样,互联网上还有多个原始凭证备份,单独的篡改某

洪学海 博士,中国科学院计算技术研究所研究员,中国科学院计算机网络信息中心研究员、博士生导师。主要研究领域为高性能计算、大数据与云计算和区块链等。先后承担国家重点研发计划、国家自然科学基金、国家重大专项等各类课题 20 余项。发表期刊和学术会议各类论文 70 余篇,独立和合作专著 5 部。

收稿日期:2020-01-14;修回日期:2020-02-21

* 通信作者,Email:hxh@ict.ac.cn

本文受到国家自然科学基金项目(91646127)、中国工程院重大咨询项目(2018-ZD-03-02)和中国科学院战略研究专项项目(GHJ-ZLZX-2019-04-2)的资助。

个节点数据就毫无意义。重要的是它不同于传统的中心化网络,对一个中心节点进行攻击就有可能破坏整个系统,而去中心化的网络采用分布式记录、分布式存储和点对点通信,任意节点的权利和义务都是均等的,系统中的数据块由所有节点共同维护。这样就避免了被某个人或机构操纵,无论任一节点遭受攻击或停止工作,都不会影响整个系统的运行。因此,它具备匿名、无需信任、开放性、信息难以篡改、可追溯、集体维护和高度透明等特点。

(2) 不可篡改和加密安全性。区块链技术的哈希算法能将任意原始数据(无论是图片还是音乐)对应到特定的字符串,成为哈希值。只要有节点被恶意篡改,哈希值就会发生变化,很容易被识别。所以一旦数据经过验证并添加至区块链被储存起来,除非能够同时控制住系统中超过 51%的节点,否则单个节点上对数据库的修改是无效的,如果有节点想要颠覆一个被确认的结果,其付出的代价将远高于收益,因此区块链的数据稳定性和可靠性极高。

(3) 共识机制和契约保障的系统安全可信。区块链世界中的工作量证明、权益证明机制、授权权益证明、实用拜占庭容错算法(PBFT, Practical Byzantine Fault Tolerance)等提供了构建机器信任的基础,把价值作为奖励,保证了区块链网络的自治与系统的稳定。

(4) 最低成本的信任方式和安全可靠的价值传递。区块链则用加密技术和分布式共识机制等代码构建了机器信任,这是一个最低成本的信任方式。区块链节点之间无需任何信任也可以进行交易,而且所有节点都必须遵守同一交易规则来运作。这个规则是基于共识算法而不是信任,因此在系统指定的规则范围和时间范围内,节点之间不能够并且也无法欺骗其他节点,自然无需任何第三方介入。因此,由于区块链使用了加密算法对数据块加密、防止篡改以及使用合约机制等,使得人类可以方便地、低成本和安全地传递价值,能更好地解决价值传递的真实性、唯一性和完整性。

1.2　区块链安全监管问题的技术本源

导致全球区块链安全事件的原因包括两个方面:一方面是其共识机制、私钥管理、智能合约等存在的技术局限性所面临的安全问题;另一方面,区块链去中心、自治化的特点给现有网络和数据安全监管手段带来了新的挑战。各类安全事件的频繁发生给区块链在新模式下的应用管理敲响了警钟,区块链安全问题也引发了政产学研等各界的广泛重视。

2018 年 9 月,中国信息通信研究院与中国通信标准化协会近日联合发布的《区块链安全白皮书》中,从技术架构设计的角度将区块链技术典型应用架构划分为四层(图 1),自下而上依次包含存储层、协议层、扩展层和应用层,报告对每层应用分别进行了详细的风险描述[6]。

首先,在存储层,主要来源于环境的安全威胁。存储层可能存在的安全风险有基础设施安全风险、网络攻击威胁、数据丢失和泄露等,威胁区块链数据文件的可靠性、完整性及存储数据的安全性。其次,

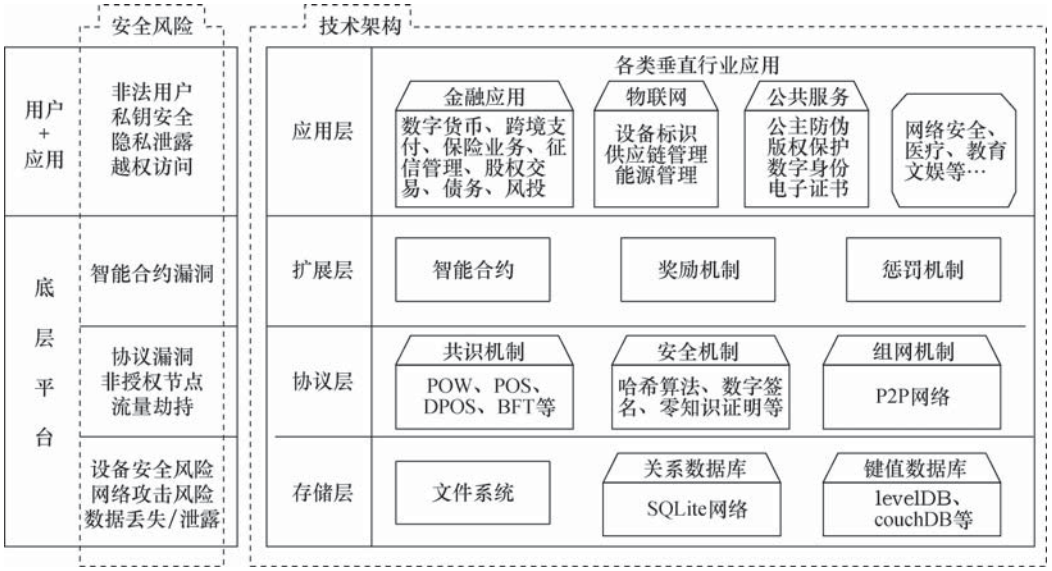

图 1　区块链技术典型应用架构

(来源:中国信息通信研究院《区块链安全白皮书》2018)

在协议层，主要来源于区块链的核心机制的安全缺陷。该层安全风险主要由区块链技术核心机制中存在的潜在安全缺陷引发，包括来自协议漏洞、流量攻击以及恶意节点的威胁等。第三在扩展层，主要来源于成熟度不高的代码实现漏洞。在区块链扩展层较典型的实现是智能合约或称可编程合约，由于智能合约的应用起步较晚，大量开发人员尚缺乏对智能合约的安全编码能力，其风险主要来源于代码实现中的安全漏洞。第四，在应用层，主要来源于各类传统安全隐患集中显现。应用层安全风险涉及私钥管理安全、账户窃取、应用软件漏洞、DDoS 攻击、环境漏洞等。

2 区块链安全事件频发带来的监管技术发展

区块链技术特点使得区块链的安全监管问题非常突出。同时经过这么多年的发展，区块链也被分为几种不同的类型。一般情况下，根据网络中心化程度的不同，区块链被分为三种类型，分别为公有链，私有链和联盟链。三者除了在性能、隐私、安全和准入性上有着各自不同的特点和优劣之处，在不同的应用场景发挥着不同的作用（表 1）。而这些新发展出来的各种区块链技术和应用带来更多的安全监管问题。

表 1 公有链、私有链和联盟链的特点

	公有链	联盟链	私有链
参与者	任何人自由进出	联盟成员参与	个人或公司内部
记账人	所有人	联盟成员协商确定	自定义
共识机制	PoW/PoS/DPoS	分布式一致性算法	分布式一致性算法
激励机制	需要	可选	不需要
中心化程度	去中心化	多中心化	中心化
隐私数据保护	存在没隐私和全隐私两个极端	隐私保护弱	保护隐私
安全性	易受攻击	存在特有的攻击	抗恶意攻击能力强
典型场景	虚拟货币	支付、结算	审计、发行
突出特点	信用的自建立	效率与成本优化	透明和可追溯性

中国工程院陈纯院士在 2019 CCF 区块链技术大会上发表了《联盟区块链关键技术与区块链的监管挑战》主题演讲，提出了区块链监管的挑战和技术发展趋势。总结起来，目前区块链监管技术发展方向主要有：(1) 区块链节点的追踪与可视化；(2) 公链发现、探测与异常发现；(3) 联盟链穿透式监管技术；(4) 以链治链。下面介绍这些方向研究的主要进展情况。

2.1 区块链节点的追踪与可视化研究进展

本文认为区块链节点追踪与可视化就是构建一个区块链中全部节点的“图谱”。区块链节点是负责维护区块链运行的网络节点，可以是小型设备、普通计算机或大型功能强大的服务器。节点分为“全节点”和“轻节点”，全节点就是拥有全链所有的交易数据的节点，轻节点就是只拥有和自己相关的交易数据的节点。区块链节点的追踪和可视化就是要查清一个区块链中的各类节点的网络地址、账户地址和交易等情况，并用动态的可视化方法展现各类节点的网络地址、账户地址和交易信息的情况，方便管理者对一个区块链的参与者进行有效的管理。以比特币区块链为例，比特币节点具有路由、数据库、挖矿和钱包这四个功能，任何一个比特币节点都实现了这四个功能中的其中几个，实现了四个功能的节点被称为全节点。路由就是 P2P 网络中的路由，按照比特币网络协议实现彼此连接。数据库就是比特币的区块链记录，里面记录了从创世块至今的所有区块。拥有完整区块链的节点仅依靠自己就能验证收到的交易的有效性。挖矿负责将最近收到的交易记录打包到区块，经过计算后加入到区块链中。钱包在交易时对交易进行签名，提供比特币账户地址。

比特币节点建立一个或多个连接后，节点将一条包含自身 IP 地址的消息发送给其相邻节点。相邻节点再将此消息依次转发给它们各自的相邻节点，从而保证节点信息被多个节点所接收，并保证连接更稳定。新接入的节点可以向它的相邻节点发送获取地址（getaddr）消息，要求它们返回其已知对等节点的 IP 地址列表。这样各个节点维持一个地址列表，通过这个地址列表可以追踪到区块链中的各个对等节点，通过对这个 IP 地址列表信息的可视化就可以展示整个区块链节点中的网络拓扑结构。

当前研究中，对区块链中的节点进行追踪的任务已经转变到对区块链节点的交易数据特征研究，以便发现区块链交易的更多行为特征。Zheng Liwen 等[8]提出了基于 Kademlia 算法的区块链节点自动发现机制。Kademlia 是一种分布式哈希表（DHT）技术，但是与 Chord，CAN，Pastry 等其他 DHT 实现技术相比，Kademlia 已经基于 XOR 建立了新的 DHT 拓扑，该算法极大地提高了路由查询

的速度,从而可以快速地发现相邻节点,为区块链节点的快速追踪和可视化奠定基础。罗强等[9]提出了一种基于云的区块链节点主动发现的系统和方法,具体方法包含:新节点向 BaaS 平台发送查询可信区块链节点的请求;服务搜索代理搜索本地服务库,获取可信节点列表;通过服务代理向 BaaS 平台查找节点认证服务;服务分析代理对新节点的服务请求进行服务需求分析,根据 XML 格式进行服务组装;可信节点向新节点发送节点认证请求。依次进行密钥交换、验签等节点认证处理;新节点通过服务代理向 BaaS 平台发送添加节点服务 Add_Peer 搜索请求;服务代理向新节点的节点代理模块返回添加节点认证服务 API;新节点通过服务代理向可信节点发送添加节点服务请求,实现可信节点添加新节点网络信息等处理;节点添加成功后,启动进行数据同步。

2.2　公链的发现、探测与异常发现研究进展

公链的主动发现、探测就是如何在网络中发现一个在运行的公有链。根据青岛天德信链科技、赛迪(青岛)区块链研究院等单位 2018 年联合发布的《全球公链项目技术评估与分析蓝皮书》,全球约有几万条公链,但实际开发者只有几百个[10]。报告指出全球总共发布了 2 万多个数字代币,这意味着大约有 2 万多条公链出现。但事实上,目前大约有 2000 条公链还“活”着。也就是说,基本 90%以上的公链都是“僵尸”链。而在此其中,大约只有 200 条左右公链是有价值的。网络世界中,区块链行业野蛮生长,并且有些区块链核心技术团队转战各处灰色地带逃避监管,制造风险隐患。因此,对这类区块链进行监管就成为重要的任务。需要注意的是,本文认为对公链主动发现和探测的主要任务是针对拥有服务功能的公链,一般有服务功能的公链是由开发组织或是社区在互联网上运行和维护的。

对于公链的主动发现和探测,本文作者查阅了大量的文献,没有查阅到有专门针对这个问题研究的文章。针对公链的研究目前主要集中在针对某种应用建立起一条公链以及对一种公链的性能改善和防攻击的安全方面[11]。本文认为,这种情况的出现是因为公币性质的公链需要信用,已经被纳入到监管部门的“沙箱”进行监管了,不需要再主动发现和探测。还有一种情况就是没有信用的公链,成为“僵尸”。本文认为,针对存在并运行、维护的公链的主动发现和探测,对其可以借用互联网舆情的技术套路来爬取它们的网络信息,并用公链数据特征的挖掘方法,发现公链的运行状况,从而及时发现并探测到公链的存在。

目前,已有一些专家学者针对公有链系统中用户、交易、智能合约提出了一些主动发现和异常检测方案。Michele Spagnuolo 等[12]提出 BitIodine 方案,用于自动解析区块链、集群地址,对地址和用户进行分类,对来自比特币网络的详细信息进行图形化、导出和可视化,达到追踪用户身份和资金流动情况的目的。方案主要是设计并实现一个分类器,通过使用几个网络爬虫来自动或半自动标记集群,逐步更新属于已知身份的地址列表。同时,创建了一个面向特征的数据库,允许快速查询任何特定地址,以查询汇总检索余额、交易数量、接收金额、发送金额以及与特征活动(如赌博,采矿,交换,捐赠,恶意软件)相关的概率等数据,用于后续聚簇。另外,可以查询最近有效的地址,并使用交叉过滤器以有效的方式过滤结果,该方法已被实际应用。Thai Pham 等[13]使用从斯坦福网络分析项目获得的比特币交易数据集,包括比特币系统从启动到 2013 年 4 月的 6 336 769 条用户数据和 37 450 461 条交易数据。通过数据集构建用户网络图(用户为点,用户间交易为边)和交易网络图(交易为点,交易金额为边),从两个图提取不同的关系特征,使用幂度和密度定律、K-means 聚类算法计算局部离群因子(LOF)来对用户或交易的异常情况进行分类。Chen Weili 等[14]通过数据挖掘和机器学习方法,从以太坊智能合约的账户和操作代码中提取特征,构建一个分类器来检测智能合约中潜在的庞氏(Ponzi)骗局恶意行为。该方法具有较高的实际应用精度,探测到截至 2018 年有超过 400 个庞氏骗局正在以太坊中运行。此外,该方法能够在庞氏骗局创立之初即可被检测到异常行为,能够起到安全风险预防的作用。

上述方案的共同点是从大量历史数据中选取公有链系统中节点行为的特征,基于数学模型对异常行为进行预测和分类。但实际上传统的异常探测技术还有众多工程实现方法,因此公有链异常探测技术在未来还有更多的角度去探索。

Tao Qi 等[15]在研究食品安全监管的问题过程中对区块链中的恶意节点的评估等提出的一种方法。该方法提出了层次化的多域区块链网络结构和二次检查机制,通过区域节点共同治理、监管节点辅助监管、上级区域仲裁等方式,可以及时纠正和更换恶意监管节点。为了优化监控节点的选择,提出了可信度模糊综合评价模型,该模型可以考虑节点性能指标的各种影响因素,客观公正地评价该区域内各节点的综合信誉。此外,还设计了数据块结构模型,该模型能够支持监控节点的替换。She Wei 等[16]针对无线传感器网络中现有的恶意节点检测方法不能通过检测过程的公平性和可追踪性来保证

的问题，提出了一种用于无线传感器网络恶意节点检测的块链信任模型（BTM），给出了信任模型的整体框架，并构建用于检测恶意节点的区块链数据结构。最后，利用区块链智能合约和无线传感器网络的四边形测量定位方法，实现了对三维空间恶意节点的检测，并将投票一致性结果记录在区块链中。

2.3 联盟链的穿透式监管技术研究进展

联盟链是指其共识过程受到预选节点控制的区块链，是弱中心化的私有链。联盟链兼顾了公有链的去中心化和私有链的高效。本文认为联盟链“穿透式监管”是借用金融领域“穿透式监管”的概念，对联盟链中参与各方的各种行为的本质进行监管，以应对监管对数据的真实性、准确性和甄别业务性质等方面的要求。因此，联盟链穿透式监管的表现形式是一种功能监管、行为监管。

陈纯院士认为联盟链和监管将是未来区块链行业的研究热点。联盟区块链对监管的友好主要表现在四个方面：有准入体系；智能合约加入到监管的规则中，能全面提升监管的自动化水平；联盟区块链支持穿透式监管；容易标准化监管的接口，实现集中式监管[7]。

以 R3、Hyperledger、金链盟为代表的联盟链，强调同业或跨行业间的机构或组织间的价值与协同的强关联性以及联盟内部的弱中心化，以强身份许可、安全隐私、高性能、海量数据等为主要技术特点。一般而言，联盟链的共识节点均是可验证身份的，并拥有高度治理结构的协议或商业规则。如果出现异常状况，可以启用监管机制和治理措施做出跟踪惩罚或进一步的治理措施，以减少损失。联盟链的某些应用在单链上无法完整实现，需要在多链架构下的可扩展性、隔离性、高性能、互操作等特性的帮助下实现。联盟链相对公有链可以选择更强一致性的共识算法以提高跨链安全性，同时联盟链也拥有更高的可监管度，进一步增强了跨链安全性。联盟链网络由成员机构共同维护，网络接入一般通过成员机构的网关节点接入。联盟链平台应提供成员管理、认证、授权、监控、审计等安全管理功能。一般当网络上有超过 2/3 的节点确认一个区块，该区块记录的交易将得到全网确认。此外，多链的联盟链一般将网关作为记账节点，因此，本文认为联盟链的穿透，一般是穿透网关节点，依赖于网络 TCP 协议和 P2P 协议，联盟链的穿透可以通过 TCP“打洞”和 P2P“穿透”来实现。

王劲松等[17]提出一种基于比特币交易数据特征的增量聚类方法，首先分析区块数据获取钱包地址的可聚类交易，获取聚类地址组；然后通过查找地址索引表，获取以聚类实体间关系；最后基于并查集算法对该区块钱包地址数据进行增量聚类，得到新的比特币实体关系，从而推测实体的类型，对实体进行识别和标注，进而对实体进行交易行为的可视分析。张健毅等[18]等设计了监管的数字货币模型。通过双链结构构成便于监管的数字货币体系。作为核心的联盟链结构中，内部成员负责交易的确认和完整交易数据的加密保存，保存的数据可以在交易追溯中作为凭据；监管机构作为联盟链的参与者加入到系统运行和维护中。

关于联盟链网络威胁，Dey Somdip[19]针对一些机构联合起来创建基于联盟的区块链面临的网络威胁，提出了一种利用智能软件代理来监测区块链网络中利益相关者的活动以检测合谋等异常的方法，并利用有监督的机器学习算法和算法博弈理论来阻止大多数攻击的发生。

2.4 “以链治链”研究进展

“以链治链”就是用区块链的技术治理区块链及其应用。在现实中，以链治链可分为链上治理和链下治理。链上治理与链下治理的区别在于，在链上治理协议中，参与者需要采取行动才能参与治理过程。而链下治理中，大部分人可能并不知道也无法影响治理过程，一个比较著名的链下治理的例子就是比特币区块大小的争论。链上治理可以借助区块链智能合约和共识机制，将治理区块链的法律和合同等条款转化为简单而确定的基于代码的规则，这些规则将由底层区块链网络自动执行。如果区块链上可以部署不受第三方干预的代码，并且监管者鼓励区块链项目方将部分法律转换为代码，推动区块链领域的软件自治，就可以协调不特定主体的正当利益诉求。

比特币 BIP 信号系统是最早的区块链链上治理系统。以太坊矿工投票治理就是以太坊的矿工通过投票选择增加或减少 gaslimit，gaslimit 决定了链上一个区块上可以处理的智能合约数量。Lu QingHuang 等[20]提出了一种系统 OriginChain，它可以生成代表法律协议的智能合约。智能合约将服务和协议中定义的其他条件的组合编纂而成。因此，智能合约可以自动检查并强制执行这些条件，它还可以检查是否提供了法规要求的所有信息，以实现自动化的法规遵从性检查。未来智能合约和人工智能结合，可以令区块链实现自我管理和自我升级，实现去中心化应用的灵活控制，并且不需要任何中断。把智能合约作为外部治理的接口，使区块链本身能够对外部治理做出反应，可以减轻监管机构在现有政治和企业治理系统方面的负担，让其他人可以获得可执行的、可验证的治理系统。

共识机制是区块链链上治理体系的重要组成部分。区块链共识机制中的 PoW 工作量证明、PoS 股

权证明、DPoS 授权股权证明、Paxos、PBFT（实用拜占庭容错算法）、dBFT、DAG（有向无环图）等都是区块链内“博弈”治理的技术手段。刘懿中等[21]从系统模型、共识机制本质、激励设置和安全攻击等角度对现有共识机制进行研究。如果能够将“以链治链”中达成的新的共识机制加入到区块链中，区块链社区可以将表决的过程以及治理规则的起立和变更写入链上，从而可以实现区块链的自动监督。

以链治链的治理机制有待完善。以链治链技术还需要深入发展，包括链上链下的数据协同等。监管者可以通过不同形式制定新规范，影响代码规则，最后通过软件实现区块链的部分内部治理，节约监管资源。同样，以链治链是“博弈”的过程，也是一个复杂的技术实现过程。目前还没有一个标准的“以链治链”的体系结构和技术过程标准化的途径。

3　区块链安全监管技术未来研究方向

区块链安全监管未来的道路还很长。一方面需要从政策、法规和制度的角度出发，制定相关监管制度与法规[22, 23]，另一方面还需要加强对区块链监管技术的研究[24]。本文认为，区块链安全监管技术未来的重要研究方向如下：

（1）区块链运行和交易监管监测技术

区块链系统具有不同于传统信息系统的分布式架构，研究监管监测技术，才能够保证所承载的各种重要业务的正常运行。主要研究内容包括：研究高效的网络流量特征提取和分析技术、远程漏洞扫描技术，实现区块链系统的实时安全测量和态势感知；研究区块链的关联节点发现技术，完成匿名地址关联、匿名节点分析和匿名用户画像；研究典型区块链应用系统的交易数据提取和分析技术，实现异常交易的检测、定位和追溯，实现异常交易的预警和预测；研究区块链系统的去匿名技术和可控隐私保护技术，实现目标用户和目标节点的行为监测和异常预警。

（2）数据内容监管监测和治理体系

针对区块链数据的去中心化特性和数据不可篡改特性，实现数据内容的监管监测和治理。主要研究内容包括：研究区块链系统的特定数据内容快速检测发现和预警技术，研究有害信息的受控回滚技术；研究区块链系统的多中心监管机制和分级治理机制，进行分布式、协作联动的监管中心有效治理；研究区块链行为的关联分析，结合网络流量特征分析，实现区块链匿名节点的身份追踪。

（3）基于区块链的监管监测技术

利用区块链系统的透明化特性，能够在重要行业中实现透明化的行业监管监测。主要研究内容包括：研究区块链交易分析和数据流转分析，实现交易的全流程监测和数据的全生命周期溯源；研究区块链的智能化分析和监控，实现面向特定目标的异常行为检测和预警；研究高效的联盟链监管技术，设计区块链系统的第三方中心监管机制，支持多层次的、联动协作的监管监测，实现对可疑交易和有害数据的快速监测和有效监管；针对重要行业，研究基于区块链的应用服务，以实现透明化的行业监管监测。

（4）区块链技术标准与规范

围绕区块链核心技术，研究制定一套系统完整的区块链技术标准与规范，保障区块链系统建设和应用的安全性和可靠性。主要研究内容包括：区块链基本架构的标准制定，包括建立区块链数据格式规范，参考技术架构规范，区块链基础设施层、核心层、服务层及业务应用管理层之间的接口技术标准；区块链关键技术标准制定，建立区块链相关技术规范，包括区块链共识机制技术标准、区块链隐私保护技术标准、匿名身份管理技术标准、区块链密码协议标准、分布式数据库技术标准等。

4　结　语

总体来看，目前区块链技术及其应用已经非常广泛，其研究方向主要还是集中在“建链”及提高链的性能、算法上，安全问题方面的研究也有很多[25—29]，但针对区块链的安全监管技术研究的还是非常少。而针对区块链应用中问题的监管是大势所趋，因此必须深入区块链的监管技术研究，促进区块链的应用更加健康的发展。

参　考　文　献

[1] Yang Wenli, Garg S, Raza A, et al. Blockchain: trends and future. Pacific Rim Knowledge Acquisition Workshop. Springer, Cham, 2018: 201—210.

[2] 孙毅，范灵俊，洪学海. 区块链技术发展及应用：现状与挑战. 中国工程科学，2018，(2)：27—32.

[3] 区块链的阿基里斯之踝. 2018-09-20，http://www.sohu.com/a/255470325_100217347.

[4] 陈纯. 联盟区块链关键技术与区块链的监管挑战. 电力设备管理，2019，(11)：20—21+28.

[5] 区块链技术发展应用最新态势和风险及政策建议. 中国科学院科学传播局专报（内部），2019-01-25.

[6] 中国信息通信研究院.《区块链安全白皮书》，2018 年 9 月.

[7] 陈纯. 联盟区块链关键技术与区块链的监管挑战，2019 CCF 区块链技术大会（成都）上的报告，2019-10-13，https://www.iyiou.com/p/115275.html.

[8] Zheng LW, Helu XH, Li M, et al. Automatic discovery mechanism of blockchain nodes based on the Kademlia Algorithm. International Conference on Artificial Intelligence and Security, Cham, 2019: 605—616.

[9] 罗强，苏恒，黄肇敏，等. 基于云的区块链节点主动发现系统及方法. 中国，CN110381167A. 2019-10-25.

[10] 赛迪(青岛)区块链研究院等.《全球公链项目技术评估与分析蓝皮书》,2018. http://www.tdchain.cn/tdchain/report201911.
[11] 朱立,俞欢,詹士潇,等.高性能联盟区块链技术研究.软件学报,2019,30(6):1577—1593.
[12] Spagnuolo M, Maggi F, Zanero S. Bitiodine: extracting intelligence from the bitcoin network. International Conference on Financial Cryptography and Data Security. Springer Berlin, Heidelberg, 2014: 457—468.
[13] Pham T, Lee S. Anomaly detection in the bitcoin system-a network perspective. arXiv preprint arXiv:1611.03942 (2016).
[14] Chen WL, Zheng ZB, Cui JH, et al. Detecting ponzi schemes on ethereum: towards healthier blockchain technology. Proceedings of the 2018 World Wide Web Conference. 2018: 1409—1418. https://doi.org/10.1145/3178876.3186046.
[15] Tao Q, Cui XH, Huang XF, et al. Food safety supervision system based on hierarchical Multi-Domain blockchain network. IEEE ACCESS, 2019, 7: 51817—51826.
[16] She W, Liu Q, Tian Z, et al. Blockchain trust model for Malicious Node Detection in Wireless Sensor Networks. IEEE ACCESS, 2019, 7: 38947—38956.
[17] 王劲松,吕志梅,赵泽宁,等.面向区块链交易可视分析的地址增量聚类方法.计算机工程,2020-02-13,https://doi.org/10.19678/j.issn.1000-3428.0056589.
[18] 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.
[19] Dey Somdip. 2018 10TH COMPUTER SCIENCE AND ELECTRONIC ENGINEERING CONFERENCE (CEEC): Computer Science and Electronic Engineering Conference, 2018: 7—10.
[20] Lu QH, Xu XW, el al. Adaptable blockchain-based systems: a case study for product traceability. IEEE Software, 2017, 34(6): 21—27.
[21] 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.
[22] 邓建鹏.美国区块链监管机制及启示.中国经济报告,2019年,第1期.
[23] 张伟,董伟,张丰麟,等.德国区块链技术在金融科技领域中的应用、监管思路及对我国的启示.国际金融,2019,(9):76—80.
[24] 相生相克,区块链将辅助监管沙盒升级2.0版本,2020-01-06,https://finance.sina.cn/blockchain/2020-01-06/detail-iihnzhha0574853.d.html.
[25] Li WJ, Tug S, Meng WZ, et al. Designing collaborative blockchained signature-based intrusion detection in IoT environments. Future generation computer systems-the international. 2019, 96: 481—489.
[26] Samaniego M, Deters R. Detecting suspicious transactions in IoT blockchains for Smart Living Spaces. International Conference on Machine Learning for Networking. Springer, Cham, 2018: 364—377.
[27] Markus I, Xu L, Subhod I, et al. Decentralized ledger based access control for enterprise applications. 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2019: 345—351.
[28] Tug S, Meng WZ, Wang Y. CBSigIDS: towards collaborative blockchained signature-based intrusion detection. 2018 IEEE Conference on internet of things and IEEE Green computing and communications, and IEEE Cyber, Physical and Social Computing, Smart Data. IEEE, 2018: 1228—1235.
[29] 王姝,晏敏等.基于区块链的科学数据标识技术创新应用模式.数据与计算发展前沿,2019,1(2):62—74. DOI:10.11871/jfdc.issn.2096-742X.2019.02.006. PID:21.86101.2/jfdc.2096-742X.2019.02.006.

Review on the Technology Research of Blockchain Security Supervision

Hong Xuehai[1, 2] Wang Yang[2] Liao Fangyu[2]

(1. *Institute of Computing Technology, Chinese Academy of Sciences, Beijing*, 100080;
2. *Computer Network Information Center, Chinese Academy of Sciences, Beijing*, 100190)

Abstract The safety supervision technology has become one of the most important research direction of blockchain technology and its implications. This paper summarized current related research in four aspects: the technical characteristic of blockchain technology, the origin of the security and regulatory issue, the development of regulatory technology induced by frequent blockchain security event and future research potentials. We highlighted four technology developments: tracking and visualization of blockchain nodes, active discovery and detection of public chain, penetrating supervision of alliance chain and chain governance.

Keywords blockchain; security; supervision; chain governance

(责任编辑 齐昆鹏)