分层跨链结构：一种面向区块链系统监管的可行架构

经普杰[1]，王良民[2]，董学文[3]，张玉书[4]，王骞[5]，Muhammad Sohail[6]

（1. 江苏大学计算机科学与通信工程学院，江苏 镇江 212013；2. 东南大学网络空间安全学院，江苏 南京 211189；
3. 西安电子科技大学计算机科学与技术学院，陕西 西安 710071；4. 南京航空航天大学计算机科学与技术学院，江苏 南京 211106；
5. 武汉大学国家网络安全学院，湖北 武汉 430072；6. 巴基斯坦国立科技大学计算机软件工程系，伊斯兰堡 46000）

摘 要：研究区块链监管存在的问题是至关重要的。鉴于此，提出了一种分层跨链的监管架构（CHA），设计了“监管链–业务链”跨链协作的以链治链的监管模式。该架构以构建去中心化的监管链的方式改善了信息系统监管的集权特性；以策略层和监管层、业务层分离的方式，实现了监管行为和监管技术的分离，从而保证了区块链监管结构的通用性。最后，通过形式化分析方法论证了该架构的分布式可行性，进而证明了方案在跨链监管可靠性方面的技术可行性、适用于不同监管业务的通用可行性及可扩展性。

关键词：区块链；监管；治理；分层监管架构；跨链

中图分类号：TP393

文献标志码：A

DOI: 10.11959/j.issn.1000–436x.2023038

CHA: cross-chain based hierarchical architecture for practicable blockchain regulatory

JING Pujie[1], WANG Liangmin[2], DONG Xuewen[3], ZHANG Yushu[4], WANG Qian[5], Muhammad Sohail[6]

1. School of Computer Science and Communication Enigneering, Jiangsu University, Zhenjiang 212013, China
2. School of Cyper Science and Enigneering, Southeast University, Nanjing 211189, China
3. School of Computer Science and Technology, Xidian University, Xi’an 710071, China
4. School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
5. School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China
6. Department of Computer Software Engineering, MCS, National University of Sciences and Technology (NUST), Islamabad 46000, Pakistan

Abstract: Researching the problems with blockchain regulation is crucial. In view of this, CHA (cross-chain based hierarchical architecture) was proposed to address the problems in blockchain regulatory, and a “chain of custody-business chain” cross-chain collaboration chain-based regulatory model was designed. The decentralized of information system regulatory was improved by building a decentralized governance chain, which realized regulatory by separating the strategy layer from the regulatory layer and the business layer, and achieved separation of regulatory behavior and regulatory technology, thus ensuring the versatility of the blockchain regulatory structure. Finally, the distributed feasibility of the regulatory framework is demonstrated through a formal analysis method, and then the technical feasibility of the scheme in terms of cross-chain regulatory reliability, general feasibility and scalability applicable to different regulatory services are proved.

Keywords: blockchain, supervision, governance, hierarchical regulatory architecture, cross-chain

收稿日期：2022–10–15；**修回日期：**2023–01–11

通信作者：王良民，liangmin@seu.edu.cn

基金项目：国家重点研发计划基金资助项目（No.2020YFB1005500）；江苏省前沿引领技术基础研究专项基金资助项目（No.BK20202001）

Foundation Items: The National Key Research and Development Program of China (No.2020YFB1005500), The Leading-edge Technology Program of Jiangsu Natural Science Foundation (No.BK20202001)

0 引言

作为比特币[1]的底层技术，区块链自提出以来，由于具备去中心化、集体维护等技术特点，在分布式场景下提供可信的执行环境和可靠的数据来源[2]。尤其是随着联盟区块链的出现，区块链技术的实用价值得到了进一步提升，越来越多的传统企业开始结合其业务需求，加快部署区块链网络环境。目前，区块链已经在政务、经济、物联网等实体领域得到了广泛的应用[3-4]，并且在我国“十四五”规划纲要中被列为七大数字经济重点产业之一[5]。区块链的应用规模从简单到复杂，存储内容从少量低频到海量高频，应用场景也从单一独立到丰富协同，这些变化都表明区块链技术正在成为网络可信环境的基础设施[4]。

然而，随着区块链应用规模的扩大，已经出现了一系列恶意区块链应用造成的资金丢失、数据泄露、追责困难等负面问题。尤其是与数字货币相关的应用，一旦出现恶意行为通常会导致大规模的经济损失，例如，以太坊 The DAO 事件和比特币 Bitfinex 被盗事件[6]，均是由于缺乏区块链上交易的监管机制，造成了巨额经济损失，并且很难追责确权。而对于更普遍应用的联盟区块链，一些基于联盟链的方案为了提升交易的性能而弱化了共识机制，造成了恶意节点合谋破坏链上交易的风险，因此如果缺乏有效的监管机制，很容易导致链上数据不可信。区块链缺乏监管的问题已经成为阻碍其在更多业务场景下应用的因素，并被认为是区块链中亟待解决的问题之一[7]。

目前，世界各国都已经注意到了区块链监管的需求，但大多数国家对区块链技术本身的监管保持着审慎的态度[8]，而更加注重对比特币等应用的监管。从 2019 年开始，我国陈纯院士就在相关主题演讲中多次总结了区块链监管的技术思路和相关方案[9]。受此引导，国家和政府更加注重对区块链技术和部署在区块链上的实体业务行为的监管。总体来看，区块链监管存在困难的主要原因有 3 个。首先，现有的中心化监管手段与区块链去中心化、自治性的可信基础存在矛盾。中心化监管方案大多需要利用中心化的监管实体参与区块链中获取业务数据或参与业务决策，实现对区块链中业务数据的获取监管。该类方法虽然实现了对区块链上业务的监管，但它破坏了区块链去中心化、共识决策等信任基础，摧毁了区块链构建可信系统的实际意义。其次，现有多数监管方法和规则通常只针对特定的区块链类型或业务类型，监管技术缺乏通用性。专用的监管方法需要适配待监管区块链的共识机制、网络规模等特点，导致该类方法虽然在具体应用中实现了对特定业务行为的监管，但“一场景一监管”的专有监管开发成本很高，这阻碍了相关技术的推广和应用。最后，具有通用性的区块链监管技术多数为穿透式监管方法[10]，但穿透式监管会导致区块链系统中监管行为与业务行为的高度耦合，极易造成监管行为对业务行为的干扰，影响业务的执行效率和系统交易结果，进而提升监管成本，甚至影响监管行为本身的执行准确性。

针对上述监管需求和现有区块链监管存在的困难，本文提出了一种基于“以链治链”思想的分层跨链监管架构（CHA, cross-chain based hierarchical architecture）。该架构以构建监管链的方式改善了监管行为中心化的集权特性；以构建“策略–监管–业务”分层的方式降低了监管与业务之间高度耦合的关系。分层跨链监管架构实现了监管行为和业务行为的相对独立，监管行为和监管技术的相对分离以及监管策略和监管行为的相对分离无关，从而能够满足区块链监管的通用性需求。该架构所采用的监管与业务分层的结构避免了监管和业务之间的相互影响，能够在保证区块链业务和监管需求的前提下，实现灵活的、准确的、高效的监管。本文的主要研究工作包括以下几个方面。

1) 提出一种“策略–监管–业务”分层的区块链监管架构。该架构通过构建监管链调和了中心化监管模式与区块链去中心化特点之间的矛盾，以分层结构和灵活跨链接入的监管技术解决了监管缺乏通用性的不足，避免了监管与业务相互影响造成的监管低效和异常。

2) 针对分层跨链监管架构中监管链与业务链之间异构、灵活、安全的监管需求，设计了一种可靠的异构链间跨链监管方法和一种标准的跨链监管数据结构，实现了监管层与业务层之间监管指令、监管内容和监管结果的安全、高效跨链传输。

3) 从通用性、安全性和可扩展性等技术方面和形式化表征层面对该监管架构进行了可行性分析，证明了该分层跨链监管架构及监管方法对不同的区块链应用具有良好的普适性和可行性。

1　区块链监管技术现状

区块链是一种不依赖于第三方、通过分布式节点进行网络数据存储和处理的技术[11]，具有去中心化、数据透明和防篡改等特点，其相关研究已经取得了较大进展，例如区块链架构方面的综述[12-13]、共识算法[14-15]、智能合约[16]，以及不同场景应用[17-18]的研究。

然而随着应用的增多，人们开始关注区块链的安全问题，也提出了许多针对区块链的安全解决方法[19-22]，包括智能合约安全[23]、数据安全[24]、网络安全[25]等。技术上安全问题的出现，以及区块链恶性事件的频繁发生，让人们开始关注区块链的非法应用问题，思考并研究针对区块链系统的监管机制[4,7]。针对区块链的监管从一开始就受到了高度重视，本节将从区块链监管的发展历程和目前几类具有较大影响力的区块链监管方法入手分析区块链监管技术的现状。

1.1　区块链监管发展现状

目前，研究者已经注意到了区块链监管的需求[26-29]，对于区块链的监管力度总体上日趋增长[27]，但他们对区块链监管保持着审慎的态度，他们通常认为区块链是一种完全分布式的可信网络，不需要对区块链本身进行监管，而针对数字货币存在恶意应用的问题，只需对相关应用进行监管。因此，目前对于区块链的监管态度更多强调对恶意区块链应用的监控和追踪，而不是对技术进行监管。

在我国，针对区块链监管技术的研究更注重通过合法监管手段，保障区块链技术在产业应用中的发展。为此，《贵阳区块链发展和应用》白皮书中提出建立一种可监管、可控制的可信区块链[28]。我国青岛建立了“链湾”研究院，旨在研究区块链监管的具体方案[29]。随后，多地政府和企业对区块链监管技术进行了相关探索。在 2019 CCF 区块链技术大会上，陈纯院士就《联盟区块链关键技术与区块链的监管挑战》[9]进行了主题演讲，总结了目前区块链监管发展的 4 种思路：区块链节点的追踪与可视化；公链发现、探测与异常发现；联盟链穿透式监管技术；以链治链。洪学海等[10]对这 4 种思路及技术方法进行了较深入的分析。由此可见，我国学者更多关注与社会管理结构密切结合的联盟链应用监管技术。

1.2　现有区块链监管方法

目前的研究中可以明确归纳为区块链监管技术的工作大致可以分为数字交易监管、链下监管和接入式监管 3 类。

数字交易监管方案主要从 3 个方面对数字交易进行监管：网络层的节点检测[30]、交易层的数据分析[31]以及应用层的网络流量分析。这些技术可以辅助发现和追踪数字货币交易中的恶意节点、可疑交易和异常用户，提高区块链交易的安全性[32-34]。然而，这些监管技术并未涉及区块链技术本身，而是对区块链运行的节点、业务数据以及交易行为进行的“环境”分析。这可能会破坏应用系统的隐私性，引起用户对区块链系统的担忧。因此，这些通用的监管技术在本领域应用，不能认为是区块链系统的监管技术。

针对其他复杂业务应用，监管方案考虑通过对上链前的业务数据、智能合约和交易结果等内容进行链下审计和检测，达到了对区块链业务监管的目的[35-38]。由于区块链上用户交易是匿名的，因此一旦某个用户通过上链审查获取数据后，就难以对数据和行为进行控制，提前进行用户审查是常规做法，但是这种监管通常利用典型的中心化监管方式。然而，链下监管的方法大多沿用中心化监管思路，对上传前数据和交易结果都以中心化方法实施监管，在一定程度上影响了区块链技术支持交易去中心性、透明性等初衷。

接入式监管是指利用监管实体作为区块链的节点参与区块链网络中获取业务数据或参与业务决策，实现对区块链中业务数据和行为的监管。这类方法虽然可以实现对区块链内业务的监管，但监管方参与到业务区块链的共识和同步中，在很大程度上侵犯了用户交易行为和数据的隐私，违背了系统隐私管理的原则，也破坏了区块链系统构建的初衷。当监管机构作为节点参与业务区块链的存储与同步时，将直接同步获取链内的全部业务数据，因此该方法未必能提升监管效率，但监管机构获取了全部数据，对数据隐私性构成滥用威胁，最终会导致区块链的可信环境遭到破坏，从而影响产业发展。

1.3　跨链监管技术

“以链治链”的监管思想以构建监管链的方式实现监管行为的去中心化，使监管主体不再是一个集权的中心，而是共识的群体，从而有效克服监管对区块链对等可信环境的影响。但是，“以链治链”必然涉及监管链与业务链的跨链合作。

在跨链监管中对跨链方法产生了如下技术困难：跨链性能问题，随着跨链监管规模的扩大，跨链的性能决定着跨链监管的可用性；跨链安全问题，在监管过程中，监管内容均通过跨链传输，跨链安全保证了监管过程的安全可靠；异构链适配问题，监管涉及与多种类型业务链的交互，异构的区块链具有不同的共识和交易类型，异构链的适配决定了监管接入的通用性。

基于区块链的跨链困难问题，学者已经总结了多种方案[39]。根据 Buterin[40]提出的分类方法，这些方案可以分为公证人机制、侧链/中继、哈希时间锁等类型。公证人机制是一种相对容易实现的跨链机制，它可以通过引入可信的第三方来验证和转发跨链消息[41]。但是这种方案由于依赖于第三方存在安全性较弱的问题。侧链方案使用双向锚定技术，实现主链与侧链的交互，但侧链方案通常只适用于具备主从关系的链间的流通，在适用性方面存在不足。中继方案是一种可扩展的跨链技术[42]，它可以自行验证交易数据。中继方案通常使用中继链的方式满足异构跨链交互需求，如 Polkadot[43]和 Cosmos[44]，但这类中继方案往往需要指定共识和网络结构，因此存在实现困难、执行效率低的问题。哈希时间锁是一种不需要信任公证人的安全跨链解决方案，通过哈希锁和时间锁完成链间资产交换[45]，但它并不支持数据的跨链通信。

综上，跨链技术主要负责维护跨链监管过程的安全、适配和高效，是跨链监管可行、可信的核心技术。

2　分层跨链监管架构

为了研究通用的、自动化的、不影响区块链业务交易，且能保障区块链产业健康发展的监管架构和方法，需要降低监管行为和业务行为的耦合度，尽可能减少监管行为对业务执行的干扰。为此，本文提出了一种基于“以链治链”思想的 CHA，以及适用于 CHA 的跨链监管流程和标准的跨链监管数据格式。

2.1　分层跨链监管架构

本文提出的分层跨链监管架构将业务、监管、和许可等功能模块相互分离，如图 1 所示。在 CHA 中，业务层主要负责集成现有的实体业务，执行区块链网络的业务行为；监管层主要负责通过在业务链中设置共享监管节点或跨链接入的方式实施监管行为，实现监管的需求；许可层则依据监管政策，为合法监管措施予以许可，这样实现了监管和法律法规一致，使监管链对业务链的监管有了判断依据，同时，也实现监管内容（监管什么内容）和监管实施技术（用什么区块链技术来实现监管）的无关性。

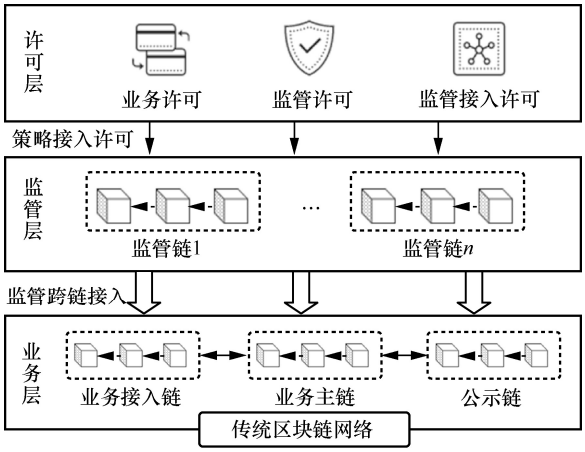


图 1　分层跨链监管架构

由此可见，不同于余春堂等[46]提出的针对物流应用的专有监管方案，CHA 具有监管意义上的通用性和灵活性，不再局限于具体的业务场景和行为；此外，CHA 也与杨东等[47]提出的关于“以链治链”的“依法治链”取证思想不同，CHA 是一个用于指导监管技术实施的区块链技术架构，该架构不仅支持和实现了“依法治链”取证的思想，更重要的是调和了集权监管和区块链去中心化技术特性的矛盾，实现了监管行为和业务行为的松散耦合，从技术上降低了监管对业务行为实施的影响，提高了监管技术的通用性和灵活性。

分层隔离的设计具有如下优点：业务层内的业务行为和监管层内的监管行为能够按照自身的既有逻辑和规范运行，而监管链和业务链间的交互即监管接入可以通过跨链技术实现；独立许可层的设置为分层跨链监管架构的监管通用性和灵活性提供了保证，一方面可以令监管许可这种制度策略和链上监管执行这种技术方案分离，另一方面确保了监管对业务的接入不是业务链对监管链跨链行为的“完全服从”，而是业务链与监管链依据许可层制定的接入策略实施的合法监管行为，并且以共识协商和去中心化作为监管执行的可信基础；监管层和许可层分开，也使监管内容和监管技术独立，区块链监管技术的创新和相关监管政策的修改之间不会产生相互影响。

为此，CHA 的三层分离结构达成了 3 个方面的目标：实现了监管链与业务链的松散耦合；实现了监管技术与监管内容的相对独立；实现了监管内容和监管技术的无关性。

2.2　基于 CHA 的交易监管实施流程

CHA 可以实现对多种类型业务区块链的接入监管，因此该架构既能够适应监管行为和业务内容的多样性，也具有对业务链和监管链规模的扩展性。本节对 CHA 进行了实例化的一般性过程分析——将跨链监管抽象为一个监管部门对一个业务部门交易的监管实施过程，在实施过程中设计了 4 个阶段共同完成监管层对业务行为的接入监管，如图 2 所示。

1) 注册与接入阶段。该阶段监管链和业务链主要进行两方面的注册与接入。首先，监管方和业务方会根据许可层的接入策略和实际监管、业务需求，将监管链或业务链接入监管架构中，使其能够执行监管或业务行为。此外，为了实施监管链对业务链的跨链接入监管，接入监管架构的监管链和业务链还需要在中继链上完成注册和认证。

2) 监管授权阶段。当监管链发起监管请求后，需要经过许可层授权许可才能通过中继链接入可监管的业务层区块链中，未获得策略许可的监管链无法接入并执行监管行为。

3) 监管动作执行阶段。该阶段是监管实施的关键阶段。首先，监管链将根据监管需求向业务主链发起监管请求，业务链则根据监管指令执行监管合约获取监管行为所需的业务数据，并将数据跨链返回监管链。接下来，监管链将对业务数据执行监管动作，如果存在异常业务行为，则监管链需要进一步请求对业务接入链内容的监管，更细粒度地追踪异常行为。

4) 监管结果发布阶段。监管动作执行完成后，如果未出现异常业务，则可直接将监管结果跨链同步至信息公示链中。否则，需要将具体异常信息同步至信息公示链中公示。

2.3　基于 CHA 的跨链数据格式

在使用该分层监管架构实施交易监管流程时涉及多种异构链间的通信交互，为了保证监管架构有效使用，本文设计了一种通用的跨链监管机制。此外，为了应对异构区块链之间缺乏统一数据格式的问题，本文设计了一种标准的跨链通信数据结构，可自适应地转换为不同类型区块链内的数据格式。当监管链发起监管请求时，可以将监管指令按照标准的数据结构跨链发送至业务区块链，业务链收到监管请求后，可以将该数据结构自适应地转换为业务链数据格式，从而获取监管指令，进一步根

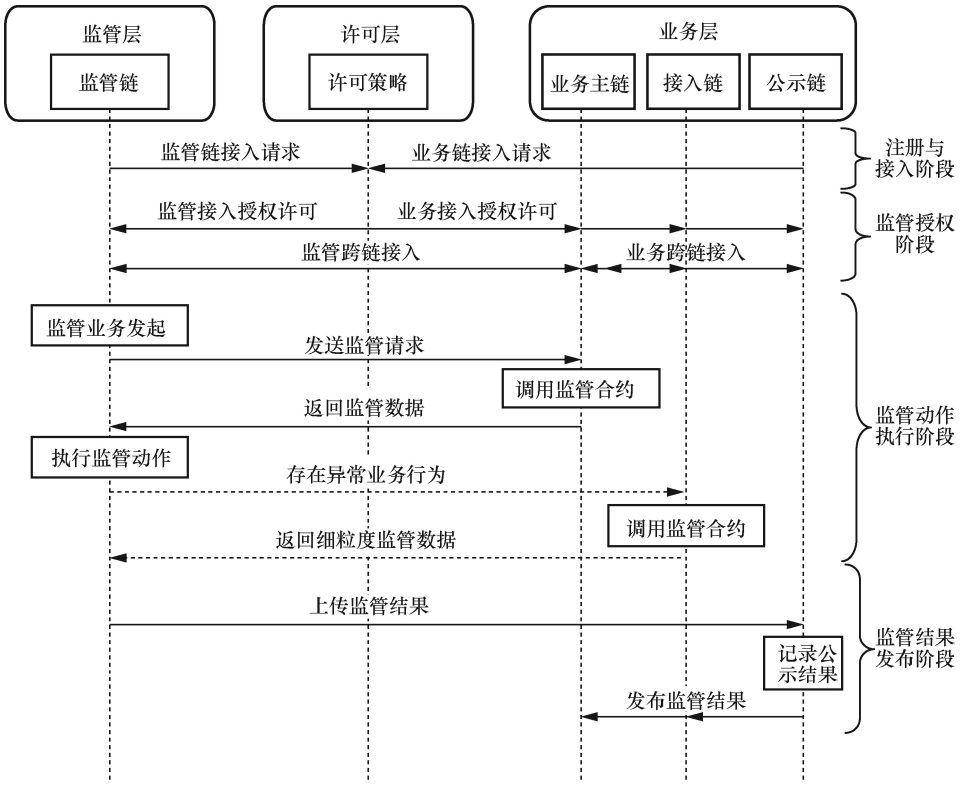


图 2　监管架构中监管执行流程

据监管指令执行功能合约，收集监管数据。标准的跨链通信数据结构如表 1 所示。

表 1 标准的跨链通信数据结构

符号标识	参数描述
BC_{Reg}	监管链
BC_{Busi}	业务链
Type	跨链交易类型
T_{id}	跨链监管交易标识符
Timestamp	时间戳
Confirm	接收的确认标识符
$T_{content}$	交易具体内容
m	监管请求命令

根据表 1 中所示的数据格式，可以定义一条跨链监管请求。该监管请求由 BC_{Reg} 发起，请求监管 BC_{Busi} 中的业务行为，跨链交易类型 Type 可定义为监管发起，T_{id} 表示跨链监管交易标识符，该标识符可以根据监管链和业务链之间的跨链频次定义；Timestamp 表示跨链监管的时间标识；Confirm 表示目的链接收跨链交易的确认标识符（通常为布尔类型），$T_{content}$ 封装了跨链交易的具体内容。在跨链监管请求中，该内容通常为跨链指令，为了确保跨链内容的隐私，该内容通常使用密码学方法加密后以密文形式传输，保证传输过程的数据安全。

2.4 基于 CHA 的跨链监管机制

基于 CHA 实施跨链监管时，监管链将链内发起的监管交易按照该数据结构转换为跨链监管请求，可以通过中继跨链的方式将该请求同步至业务链中[48]，业务链接收到该监管请求可自适应地将交易数据结构转化为业务链的交易格式，并从中获取监管指令，再利用业务链内的功能合约根据监管指令获取业务数据。根据 CHA 跨链监管的流程，利用该监管架构执行一次完整的跨链监管通常包含 4 个阶段，如图 3 所示。

1) 跨链注册阶段。当监管链或业务链得到许可层授权加入监管架构后，为了实施监管链对业务链的跨链接入监管，它们需要在中继链上完成注册和认证。

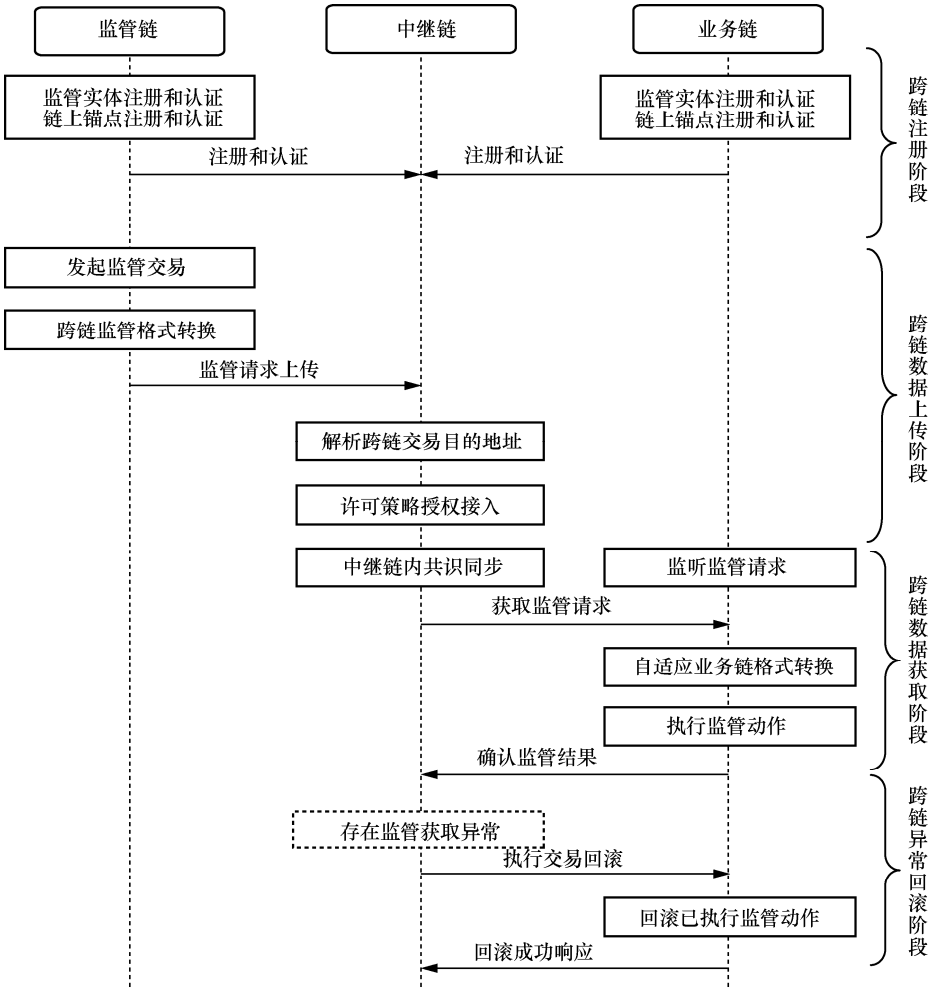


图 3 跨链监管执行流程

2) 跨链数据上传阶段。监管链将链内发起的监管交易按照标准数据结构转换为跨链监管请求，并将请求通过监管链的代理节点上传至中继链，中继链可以记录该上传过程，并根据请求中的 BC_{Busi} 字段确认监管请求的目标业务链。

3) 跨链数据获取阶段。业务链的代理节点从中继链中监听到监管请求后，将自适应地转换该跨链监管请求为业务链的交易格式，从中获取跨链监管的具体指令，并根据指令执行监管动作。

4) 跨链异常回滚阶段。当业务链成功获取跨链监管请求，业务链将修改跨链监管请求中的 Confirm 字段为 1，表示该跨链监管过程完成；否则标记为 0，表示该过程存在异常，业务链未能实施监管动作。如果业务链未能正常获取或执行监管指令，跨链监管出现异常，中继链可以对未确认的异常交易进行回滚操作，避免监管数据泄露。

2.5 基于 CHA 的物流区块链系统监管示例

为了更清晰地说明该监管架构对区块链系统的监管实施方法和过程，本节给出了一个面向区块链物流系统的监管实施案例，从而证明 CHA 功能实施的可行性，并有助于对 CHA 普遍适用性和相关性能的理解。

1) 基于区块链技术的众包物流系统

随着物流需求的扩展，传统物流公司中心化的业务模式需要各个物流企业拥有完整的仓储、运输全流程资源，极易分散物流服务能力，造成部分公司无法满足物流需求或部分公司物流资源闲置的情况，导致物流服务效率降低等问题。为了解决这一问题，物流行业需要整合现有的资源，因此研究者提出了众包物流模式。然而相比于中心化物流系统，众包物流模式由于涉及信息的外包处理，因此在隐私安全和可信等方面存在问题。为了解决此问题，可以通过构建物流区块链网络实现，如图 4 所示。各个物流公司可基于联盟链构建业务主链，即业务应用平台，在该平台中，寄件人/收件人作为需方，可以通过节点接入等方式接入业务平台中，在业务主链内发布物流需求等；各个物流资源提供方（如仓储公司、货运公司）可以维持自身的业务链，并以接入链的形式接入业务主链中获取或上传业务功能需要或产生的具体业务数据，配合主链完成物流业务。此外，为了保护物流信息的真实可信，在业务功能层中，还设置了一个公示链用于平台信息的公示，业务主链可定时将交易数据公布到公示链中，利用公示链完全去中心化的特性，确保业务信息的可信，为监管机构对该平台内的物流交易信息进行监管审计提供可信可靠的数据。

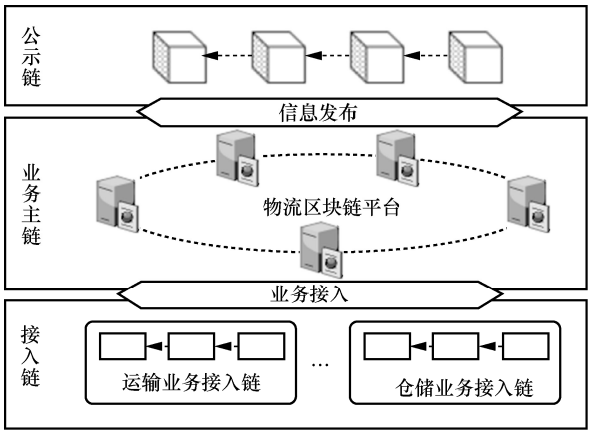


图 4　物流区块链网络

2) 面向区块链物流系统的接入监管

为了实现对分布式的众包物流区块链网络的全面监管，在监管层中可以设置多个部门的监管链对该业务层的物流系统进行接入监管。以邮政部门监管为例，如图 5 所示，邮政监管链首先在授权许可下接入各个物流公司的业务主链中，监管链可以根据监管需求收集监管数据或调用业务链内监管合约，跨链执行对业务主链内物流数据的获取和物流业务行为的监管。当检测到物流数据或业务行为存在异常时，可以进一步追溯到异常原因及所属的业务环节（如运输环节等）；当物流过程中某一业务环节出现异常时，监管部门可通过接入该业务环节的业务子链对具体业务进行监管检测，进一步追溯到具体异常问题；当监管链完成监管数据获取、监管动作执行得到监管结果后，为了发挥结果对后续物流过程对资源提供方的选择指导，需要将监管结果跨链同步至业务层的公示链中记录并在业务层公示，保证监管结果的真实可信。

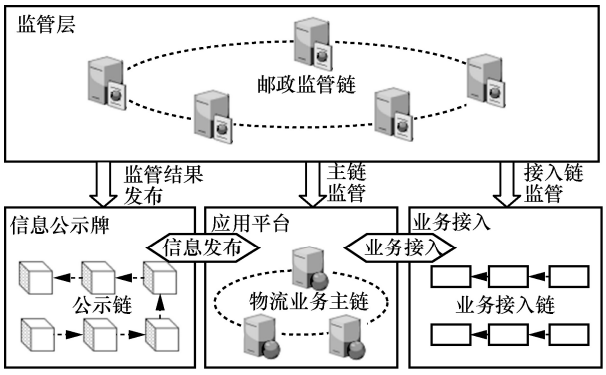


图 5　监管动作实施

3) 监管策略设置

为了调和监管的集中式权威需求和区块链业务的去中心化需求，CHA 中设置了独立的许可层，实现了监管策略和监管实施的无关性，监管机构可以根据自身的监管需求实时地调整和更新监管策略，保证监管的灵活和通用。许可层在该架构中主要承担三方面的许可授权，即业务层中接入链的接入许可、监管层中各监管部门监管链的接入许可和跨链监管准入许可。3 类许可功能共同维护监管架构中的业务行为和监管行为的安全可信。此外，监管策略的设定确保了只要符合许可策略和跨链需求，监管和业务部门就不需要重新针对性地设计专有区块链，这一特点为监管链和接入链的复用提供了帮助。

3 分层跨链监管架构性能分析

使用分层跨链监管架构对区块链应用实施监管，要求该架构能够广泛适用、灵活扩展和安全可靠，为此本节主要从通用性、可靠性、可扩展性和安全性等方面分别对分层跨链监管架构的可行性进行分析，并对架构整体采用形式化表征方法，证明了该监管架构对区块链的监管是可行的。

3.1 监管架构的通用性分析

该监管架构的核心思想是将业务、监管和策略分层，构建一种监管与业务松散耦合的通用监管方法，因此通用性是衡量该监管架构可行性的重要指标。本节针对异构链间跨链监管通用适配的问题设计了一种跨链监管机制。通过中继跨链和一种标准的跨链通信数据结构，异构的监管链和业务链上不同类型的数据可以进行标准格式转换和跨链通信，因此该架构不对监管链和业务链类型做出限制，监管方和业务方可根据监管需求和业务行为选择链类型，只要通过策略许可接入监管即可利用通用的跨链监管机制实施跨链监管。

3.2 监管架构的可靠性分析

在该监管架构中，监管动作和业务自身的可靠性可依赖于区块链的可信执行环境，因此跨链监管过程的安全可信是监管架构可靠的重要因素。为了保护监管层与业务层松散耦合，通过跨链接入实施监管的情况下，监管动作的可信执行、监管数据的安全获取，以及监管异常的高效追溯，本节在跨链监管过程中设计了多种安全方法保护架构的安全可信。

1) 在跨链监管通信机制中，为了保护跨链内容的隐私性，本文方案设计对跨链交易中包含的具体内容，如监管指令、监管内容、监管结果等使用密码学方法在传输过程中加密保护，只有授权业务链可以解密，获取监管相关内容。

2) 在跨链监管执行时，为了确保跨链监管过程的原子性和数据内容的一致性，本文在跨链监管数据结构中加入了接收确认字段 Confirm，并在跨链监管机制中加入了回滚机制，可以实现异常监管回滚，避免监管相关内容的泄露。

3) 在跨链监管机制中，本节利用了基于中继链的跨链通信方法，不仅有助于异构链间的通用适配，在中继链中完整地记录跨链监管行为，当监管存在异常时，还可通过在中继链上执行追溯过程确定异常监管的具体位置。

3.3 监管架构的可扩展性分析

“以链治链”监管架构的可扩展性主要包括 2 个方面，一方面是该监管架构可扩展的规模，即架构可接入的监管链与业务链的数量；另一方面则是架构中跨链监管的性能指标，即跨链监管的吞吐率和时延。通常情况下，监管架构的规模与跨链监管的时延呈正相关趋势，即监管架构中接入链数量越多，跨链监管过程的时延越长，而监管架构的吞吐率将受限于中继链的性能。为了对架构的可扩展性进行定量分析，本文实例化了 3 条联盟区块链，分别模拟监管链、业务链和中继链进行性能测试。具体实验环境部署如表 2 所示。

表 2 实验环境部署

联盟区块链	硬件环境	操作系统	链类型	共识节点数量/个	共识算法
监管链	i5-1137G7 4 GB	Ubuntu	Fabric2.0	3	Raft
中继链	i7-10750H 8 GB	Ubuntu	Fabric2.2	3	Raft
业务链	i5-9400F 4 GB	Ubuntu	Fabric1.4	3	Raft

由于请求上传和请求获取属于不同的操作类型，使用相同的发送速率可能会导致中继链的硬件限制，因此本节分别对监管请求上传和访问进行了两组仿真实验。如图 6 所示，对于上传操作，当上传速率低于 65 tps 时，中继链吞吐率与上传速率相同，平均时延约为 0.1~0.3 s，说明监管请求上传操作被立即执行；当上传速率超过 65 tps 时，吞吐率保持在 65 tps，并且上传操作的时延增加，说明上传请求不能立即执行；当上传速率超过 100 tps 时，平均时延超过 80 s，之后时延会逐渐减少，说明出现了异常，有些监管请求上传失败。由于业务链从中继中获取监管请求是

一个查询中继链的过程，不需要经过中继链共识，因此跨链访问过程的吞吐率更高。本节将获取速率设置为 350 tps，当获取速率达到 350 tps 时，访问请求操作的吞吐率与获取速率仍相同，平均时延始终在 0.01 s 左右。这说明当获取速率超过 350 tps 时，仍然没有达到访问请求操作的性能阈值。尽管这两项跨链监管的性能指标与硬件环境有关，但从该仿真实验分析可以看出，架构中监管与业务松耦合，通过跨链监管接入的方式不会影响监管的效率，该架构在性能方面具有可行性。

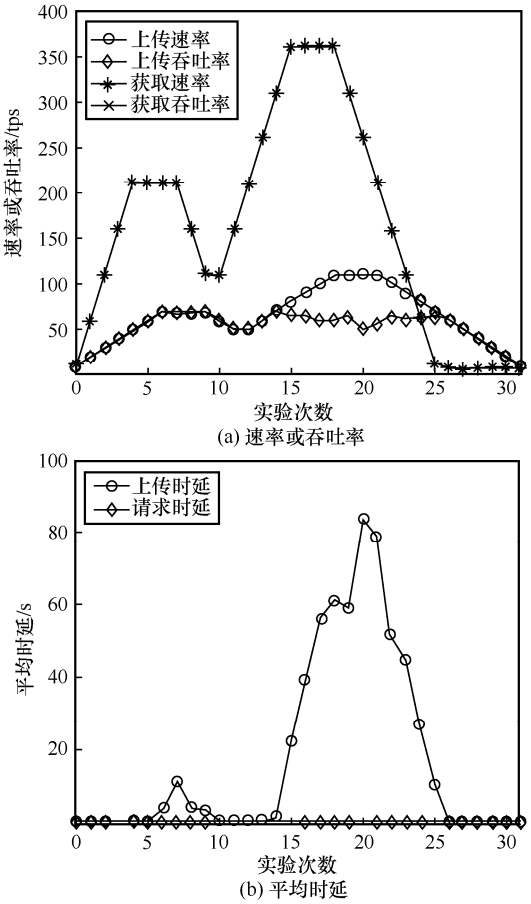


图 6　跨链监管通信开销

可以预见的是，随着监管业务越来越复杂，监管架构的规模随之扩大，跨链监管业务的时延将会不断增加。因为随着监管架构中接入链的不断增加，中继链的网络结构更加复杂，共识和同步需要消耗更长的时间，因此为了维持监管架构的可扩展性，需要不断优化区块链的网络结构、共识算法和硬件条件。

3.4　监管架构的安全性分析

区块链分布式、不可篡改的特点保证了链上业务和数据的安全性，而安全与可信也是区块链应用的基本属性，分层跨链监管架构也应在保证业务和数据安全的前提下实施监管行为。为此本节针对可能存在的常见攻击方式对监管架构的安全性展开分析，证明监管架构的安全可行。

1) 防 DoS 攻击。在监管过程中，可能存在恶意的业务区块链大规模上传非法或恶意数据，造成业务主链平台的堵塞，影响正常业务和监管行为。在该架构中，针对监管和业务接入问题设计了专门的许可层和接入许可策略，只有符合接入权限的业务和监管链才可以完成跨链接入，实施业务和监管行为，因此该方法可以避免攻击者恶意传输造成的系统故障。

2) 防窃听攻击。应用该监管架构实施跨链监管数据交互的业务和监管数据可利用属性基加密等密码方法实施隐私保护和访问控制。即使数据已经被窃听，如果攻击者不满足访问控制策略，其也无法通过哈希碰撞或合谋等方式对数据进行解密，获得监管和业务数据明文。

3) 抗篡改和伪造攻击。为了防止恶意攻击者在跨链监管过程中篡改和伪造数据，该监管架构在数据上传前对数据执行签名算法。当业务主链或监管链接收到数据时，它们可通过验证签名确保数据的真实性和准确性。因此，攻击者无法实现篡改或伪造攻击，避免监管和交易数据在跨链过程中遭到破坏，影响监管结果。

3.5　监管架构可行性形式化验证

上述证明分别从架构的通用性、可靠性、可扩展性和安全性 4 个方面证明了监管架构的技术可行性，但仍缺乏整体性，为此本节对该监管架构进行了形式化建模和表征，进而通过形式化证明和分析方法——有色 Petri 网[49]，证明该监管架构的整体可行性。

图 7 所示的监管架构 Petri 网描述了架构的监管过程。为了描述监管架构实施监管行为的全过程，本节设置了 10 个库所来表示架构中可能出现的 10 种状态类型，8 个变迁来描述不同状态之间的迁移过程，由于在该架构中涉及多种资源的使用，因此设置 3 种类型的令牌：业务 token、监管 token 和许可 token。根据架构分层的特点，可以将该 Petri 网模型分为 3 个子部分。业务层，业务发起者可以发起业务请求，即一个业务 token 触发业务请求（库所 p_1），t_1 表示该业务请求在业务链内的接收和同

步；此时，库所 p_2 表示请求已经记录在链上的状态，该状态可以触发 2 种变迁：t_2（接入链响应业务请求）和 t_3（业务请求记录在公示链中）；接入链响应业务请求后，使业务进入执行状态 p_3，业务执行完成将触发变迁 t_4 完成执行结果的提交，并得到业务结果 p_5；此外，在业务层中请求和业务结果可以分别通过变迁 t_3（请求记录公示）和 t_5（结果记录公示）实现在公示链上的记录。在监管层，库所 p_6 表示监管请求，当 p_6 接收到一个监管 token 时，则可以触发变迁 t_6 实现监管请求上传，该变迁完成后进入库所 p_7（监管链上请求）。此时，库所 p_8 获取许可 token，触发变迁 t_7 允许监管接入，库所 p_9 可获得许可 token。当库所 p_5（业务结果）获得业务 token、库所 p_7（监管请求）获得监管 token、库所 p_9（接入许可）获得许可 token 时，3 个库所可以共同触发变迁 t_8 执行监管动作，获得监管结果。

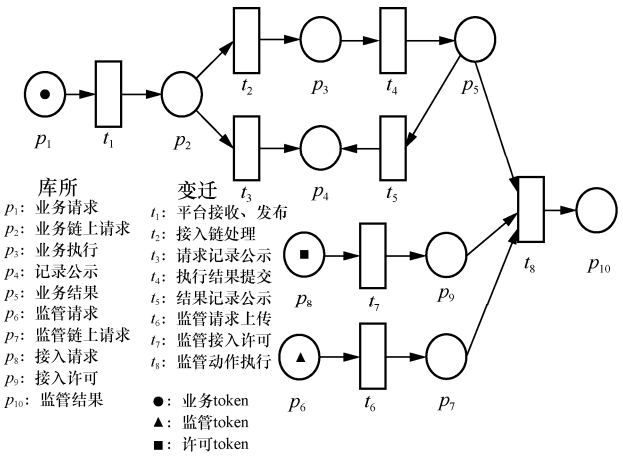


图 7 监管架构 Petri 网

4 结束语

区块链技术自提出以来，已经在多个实体领域得到了广泛应用。但随着区块链产业的发展，由于缺乏监管带来的问题已经越来越严重，如链上恶意数据的删除、区块链系统安全性导致财产损失、链上财产损失链下难以追踪等，已经成为区块链产业发展的主要障碍。为此，本文对现有的区块链安全和监管缺失问题进行了全面综述，针对现有区块链监管中存在的问题和需求，提出了一种基于“以链治链”思想的分层跨链区块链监管架构，设计了监管架构中“监管链–业务链”跨链协作的以链治链监管模式。本文还在 CHA 的基础上根据跨链监管的需求，提出了具有通用性的跨链交互标准数据结构，保证了跨链监管过程的通用、安全和高效。最后，本文就监管架构的技术可行性从通用性、可靠性、可扩展性和安全性等多个方面进行了分析，就监管架构的整体进行了形式化证明，从多个维度充分证明了该监管架构的可行性。

未来的研究工作可从跨链监管的安全性、跨链监管的执行效率、监管链与业务链跨链交易的一致性等方面展开，使监管架构具有更高的可信性和效率，能够在现有区块链实体中得到更广泛的应用。

参考文献：

[1] LU Y. The blockchain: state-of-the-art and research challenges[J]. Journal of Industrial Information Integration, 2019, 15: 80-90.

[2] ZHENG Z B, XIE S A, DAI H N, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//Proceedings of 2017 IEEE International Congress on Big Data (BigData Congress). Piscataway: IEEE Press, 2017: 557-564.

[3] GAD A G, MOSA D T, ABUALIGAH L, et al. Emerging trends in blockchain technology and applications: a review and outlook[J]. Journal of King Saud University - Computer and Information Sciences, 2022, 34(9): 6719-6742.

[4] 孙毅, 范灵俊, 洪学海. 区块链技术发展及应用: 现状与挑战[J]. 中国工程科学, 2018, 20(2): 27-32.
SUN Y, FAN L J, HONG X H. Technology development and application of blockchain: current status and challenges[J]. Strategic Study of CAE, 2018, 20(2): 27-32.

[5] 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.

[6] ZHU L H, ZHENG B K, SHEN M, et al. Research on the security of blockchain data: a survey[J]. arXiv Preprint, arXiv: 1812.02009, 2018.

[7] 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.

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

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

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

[11] HUO R, ZENG S Q, WANG Z H, et al. A comprehensive survey on

blockchain in industrial Internet of things: motivations, research progresses, and future challenges[J]. IEEE Communications Surveys & Tutorials, 2022, 24(1): 88-122.

[12] GAO W C, HATCHER W G, YU W. A survey of blockchain: techniques, applications, and challenges[C]//Proceedings of 2018 27th International Conference on Computer Communication and Networks (ICCCN). Piscataway: IEEE Press, 2018: 1-11.

[13] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.

[14] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11): 2011-2022.
YUAN Y, NI X C, ZENG S, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022.

[15] FU X, WANG H M, SHI P C. A survey of Blockchain consensus algorithms: mechanism, design and applications[J]. Science China Information Sciences, 2021, 64(2): 121101.

[16] MACRINICI D, CARTOFEANU C, GAO S. Smart contract applications within blockchain technology: a systematic mapping study[J]. Telematics and Informatics, 2018, 35(8): 2337-2354.

[17] SHRIMALI B, PATEL H B. Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities[J]. Journal of King Saud University - Computer and Information Sciences, 2022, 34(9): 6793-6807.

[18] SANKA A I, IRFAN M, HUANG I, et al. a survey of breakthrough in blockchain technology: adoptions, applications, challenges and future research[J]. Computer Communications, 2021, 169: 179-201.

[19] LI X Q, JIANG P, CHEN T, et al. A survey on the security of blockchain systems[J]. Future Generation Computer Systems, 2020, 107: 841-853.

[20] SAAD M, SPAULDING J, NJILLA L, et al. Exploring the attack surface of blockchain: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1977-2008.

[21] KARAME G, CAPKUN S. Blockchain security and privacy[J]. IEEE Security & Privacy, 2018, 16(4): 11-12.

[22] HASANOVA H, BAEK U J, SHIN M G, et al. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures[J]. International Journal of Network Management, 2019, 29(2): e2060.

[23] ATZEI N, BARTOLETTI M, CIMOLI T. A survey of attacks on Ethereum smart contracts (SoK)[C]//International Conference on Principles of Security and Trust. Berlin: Springer, 2017: 164-186.

[24] DEEPA N, PHAM Q V, NGUYEN D C, et al. A survey on blockchain for big data: approaches, opportunities, and future directions[J]. Future Generation Computer Systems, 2022, 131: 209-226.

[25] ZAGHLOUL E, LI T T, MUTKA M W, et al. Bitcoin and blockchain: security and privacy[J]. IEEE Internet of Things Journal, 2020, 7(10): 10288-10313.

[26] 博雅正链. 博雅正链白皮书[R]. 2019.
Boya Regchain. Boya regchain white paper[R]. 2019.

[27] 腾讯安全. CCGP 跨链协同治理平台技术白皮书[R]. 2021.
Tencent Security. CCGP cross-chain collaborative governance platform technical white paper[R]. 2021.

[28] 贵阳市政府. 贵阳区块链发展和应用白皮书[R]. 2016 .
Guiyang Government. Guiyang blockchain development and application white paper[R]. 2016 .

[29] 青岛链湾研究院. 2018 中国区块链技术与产业发展蓝皮书[R]. 2018.
Qingdao Lianwan Research Institute. 2018 China blockchain technology and industry development blue paper[R]. 2018.

[30] LI Z Z, HOU J P, WANG H, et al. Ethereum behavior analysis with NetFlow data[C]//Proceedings of 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS). Piscataway: IEEE Press, 2019: 1-6.

[31] PHAM T, LEE S. Anomaly detection in the bitcoin system - a network perspective[J]. arXiv Preprint, arXiv: 1611.03942, 2016.

[32] CHEN W L, ZHENG Z B, CUI J H, et al. Detecting Ponzi schemes on Ethereum: towards healthier blockchain technology[C]//Proceedings of the 2018 World Wide Web Conference. New York: ACM Press, 2018: 1409-1418.

[33] WU J J, YUAN Q, LIN D, et al. Who are the phishers? phishing scam detection on Ethereum via network embedding[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52(2): 1156-1166.

[34] HUANG T, LIN D, WU J J. Ethereum account classification based on graph convolutional network[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69(5): 2528-2532.

[35] PEREZ D, LIVSHITS B. Smart contract vulnerabilities: vulnerable does not imply exploited[J]. arXiv Preprint, arXiv: 1902.06710, 2019.

[36] SU L, SHEN X, DU X, et al. Evil under the sun: understanding and discovering attacks on Ethereum decentralized applications[C]//30th USENIX Security Symposium (USENIX Security 21). Berkeley: USENIX Association, 2021: 1307-1324.

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

[38] 高峰, 毛洪亮, 吴震, 等. 轻量级比特币交易溯源机制[J]. 计算机学报, 2018, 41(5): 989-1004.
GAO F, MAO H L, WU Z, et al. Lightweight transaction tracing technology for bitcoin[J]. Chinese Journal of Computers, 2018, 41(5): 989-1004.

[39] BELCHIOR R, VASCONCELOS A, GUERREIRO S, et al. A survey on blockchain interoperability: past, present, and future trends[J]. ACM Computing Surveys, 2022, 54(8): 1-41.

[40] BUTERIN V. Chain interoperability[R]. R3 Research Paper, 2016.

[41] 李芳, 李卓然, 赵赫. 区块链跨链技术进展研究[J]. 软件学报, 2019, 30(6): 1649-1660.
LI F, LI Z R, ZHAO H. Research on the progress in cross-chain technology of blockchains[J]. Journal of Software, 2019, 30(6): 1649-1660.

[42] MENDLING J, WEBER I, VAN DER AALST W, et al. Blockchains for business process management - challenges and opportunities[J]. ACM

Transactions on Management Information Systems, 2018, 9(1): 1-16.

[43] WOOD G. Polkadot: vision for a heterogeneous multi-chain framework[R]. White Paper, 2016.

[44] KWON J, BUCHMAN E. Cosmos whitepaper[R]. Distributed Ledgers, 2019.

[45] ZAMYATIN A, HARZ D, LIND J, et al. XCLAIM: trustless, interoperable, cryptocurrency-backed assets[C]//Proceedings of 2019 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2019: 193-210.

[46] 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.

[47] 杨东. “依法治链”与“以链治链”:区块链技术监管的结合之道[R]. 2019.
YANG D. “Governing the chain according to law” and “governing the chain by the chain”: the combination of blockchain technology supervision[R]. 2019.

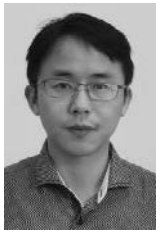
[48] 康博涵, 章宁, 朱建明. 基于区块链的智能服务交易跨链服务框架与通信机制[J]. 网络与信息安全学报, 2021, 7(3): 105-114.
KANG B H, ZHANG N, ZHU J M. Research on inter-blockchain service framework and communication mechanism based on smart service transaction[J]. Chinese Journal of Network and Information Security, 2021, 7(3): 105-114.

[49] JENSEN K. A brief introduction to coloured Petri nets[C]//Tools and Algorithms for the Construction and Analysis of Systems. Berlin: Springer, 1997: 203-208.

[作者简介]

经普杰（1996– ），男，河北廊坊人，江苏大学博士生，主要研究方向为密码学、区块链安全、区块链跨链技术等。

王良民（1977– ），男，安徽潜山人，博士，东南大学教授、博士生导师，主要研究方向为密码学与安全协议、物联网安全、大数据安全及区块链技术等。



董学文（1981– ），男，湖北黄冈人，博士，西安电子科技大学教授、博士生导师，主要研究方向为区块链、认知无线电网络、无线网络安全和隐私等。

张玉书（1987– ），男，甘肃庆阳人，博士，南京航空航天大学教授，主要研究方向为多媒体安全与人工智能、区块链与物联网安全、云计算与大数据安全等。

王骞（1980– ），男，湖北武汉人，博士，武汉大学教授，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。

Muhammad Sohail（1990– ），男，巴基斯坦人，博士，巴基斯坦国立科技大学助理教授，主要研究方向为计算机网络、无线通信等。