计算机研究与发展
Journal of Computer Research and Development

DOI: 10.7544/issn1000-1239.202330297
x(x): xx-xx, xxxx

一种多链协同治理的“以链治链”监管框架

陈晓丰[1,3] 宋兆雄[2] 郑佩玉[3] 张 珺[4] 于 智[5] 孙 毅[2,6]

[1](区块链与数据安全全国重点实验室(浙江大学) 杭州 310027)

[2](中国科学院计算技术研究所 北京 100190)

[3](杭州趣链科技有限公司 杭州 310051)

[4](内蒙古大学计算机学院 呼和浩特 010021)

[5](浙江大学软件学院 浙江宁波 315048)

[6](中国科学院大学计算机科学与技术学院 北京 100049)

(chenxf.alfred@zju.edu.cn)

A Multichain-Collaborating Chain-Supervising-Chain Supervision Framework

Chen Xiaofeng[1,3], Song Zhaoxiong[2], Zheng Peiyu[3], Zhang Jun[4], Yu Zhi[5], and Sun Yi[2,6]

[1](*State Key Laboratory of Blockchain and Data Security* (*Zhejiang University*), *Hangzhou* 310027)

[2](*Institute of Computing Technology*, *Chinese Academy of Sciences*, *Beijing* 100190)

[3](*Hangzhou Qulian Technology Co.*, *Ltd.*, *Hangzhou* 310051)

[4](*College of Computer Science*, *Inner Mongolia University*, *Hohhot* 010021)

[5](*School of Software Technology*, *Zhejiang University*, *Ningbo*, *Zhejiang* 315048)

[6](*School of Computer Science and Technology*, *University of Chinese Academy of Sciences*, *Beijing* 100049)

Abstract Nowadays, the blockchain ecosystem has been prospering and public blockchain applications and services have been booming. With the concept of Web3.0 getting heated, this trend would be more and more compelling. This fact, while granting more momentum to digital economy development, also brings about a greater challenge to the blockchain supervision practice. The technical traits of blockchain infrastructure and blockchain applications and the need of automatic, multiparty, hierarchical, and multi-dimensional supervision has been calling for innovation of and compliance with the supervision schemes designed and implemented for Web2.0. To meet this requirement and face the challenge, this paper proposes a multichain-collaborating, chain-supervising-chain supervision framework. This framework puts forward an architecture consisting of layered and hierarchical supervision chains and heterogeneous supervised chains and designs the basic procedure of blockchain supervision under this architecture. Then the paper abstracts the supervision technologies under this architecture into substrate layer, decision layer, cross-chain layer, access layer, execution layer and data layer. With this abstraction, the paper proposes a series of backbone supervision schemes that are most vital to supervision system construction. Under this framework, the paper implements a supervision system targeted at blockchain applications and shows the effectiveness and feasibility of the system by experiment and exemplary applications.

Key words blockchain; supervision; chain interoperability; multichain collaboration; governance

摘 要 当前区块链生态飞速发展,面向公众的区块链应用服务不断增多,随着 Web3.0 概念的升温,这一

收稿日期: 2023-04-03; **修回日期**: 2023-10-30

基金项目: 国家重点研发计划项目(2020YFB1005400); 国家自然科学基金项目(61972382); 内蒙古自然科学基金项目(2020MS06017)

This work was supported by the National Key Research and Development Program of China (2020YFB1005400), the National Natural Science Foundation of China (61972382), and the Natural Science Foundation of Inner Mongolia (2020MS06017).

通信作者: 孙毅(sunyi@ict.ac.cn)

趋势将愈发明显.这在给数字经济注入新活力的同时,也给区块链应用监管带来更大挑战.区块链及其应用的技术特性以及自动化、多中心、多级多维的监管需求客观要求对Web2.0监管技术进行兼容与创新.针对这些需求与挑战,工作提出了一套多链协同的“以链治链”监管框架,设计了一个由分层多级监管链和异构接入链构成的监管架构,并明确了该架构下区块链监管的基本流程;将该框架下的监管技术体系抽象成基础层、决策层、跨链层、接入层、执行层和数据层,并提出一系列对监管系统构建最为关键的监管骨干机制.在监管框架和骨干机制的指导下开发了一套区块链应用监管系统,并通过实验和应用试点验证了系统的有效性和可行性.

关键词 区块链;监管;跨链互操作;多链协同;治理

中图法分类号 TP393

随着区块链技术的不断发展,各种区块链基础设施以及依托于这些基础设施的互联网应用(后简称区块链应用)层出不穷.这些应用随着区块链概念的不断升温和相关技术的日臻成熟积累了一定的用户群体,并逐渐在数字经济领域崭露头角,产生了不可忽视的社会影响.与此同时,区块链衍生的新应用、新业态也逐渐暴露出诸多安全隐患,容易被一些不法分子利用传播违法有害信息,实施网络违法犯罪活动,损害公民、法人和其他组织合法权益,带来信息安全风险,为政府的监管工作带来巨大技术挑战.解决区块链应用监管问题,实现区块链应用的可管可控,把依法治网落实到区块链管理中,已经成为推动区块链技术、生态安全有序发展的关键.

在我国区块链应用发展的初期,其基础设施以私有链[1]或联盟链[2]为主,业务形态以面向企业与面向政府为主.这些应用的受众范围有限,往往局限于机构或企业内部,其数据、接口并不向公众开放.同时,用户需要受到严格的注册和权限认证机制的管理才能对区块链进行读写[3-4].在这种情况下,区块链应用监管的问题还不够凸显.随着我国区块链应用及业态的发展和丰富,数字藏品、非同质化代币(non-fungible token , NFT)等面向公众的区块链应用和服务开始不断产生.当前仅在相关管理部门进行备案的面向公众的区块链信息服务数量已经突破3 000项.这些应用赋予了用户相对开放的读写权限.它们在创造了数字化经济发展新形态的同时,也使区块链应用监管面临巨大需求与挑战.同时,随着Web3.0概念的不断升温[5],基于区块链技术的下一代互联网应用已经成为国际各方布局的重要赛道.可以预见,基于区块链的开放互联网应用很有可能在未来的某个节点井喷.为了应对这一趋势,我国产业界和学术界也已经开始不断探索适合我国国情的区块链新形态,比如开放许可链等概念已经被提出[6].对开放区块链甚至类公有链技术的潜在需求客观上也对区块链应用监管提出了更高的技术要求.

虽然区块链应用监管的重要性和迫切性已日趋凸显,但从技术层面分析,其仍面临非常大的挑战.

首先,区块链具有的内在特性为链上数据安全和应用监管带来了新的问题和挑战.区块链具有分布式,去中心化的特征,公有链系统更具备开放性和匿名性.区块链系统与传统分布式系统都能实现数据的分布式冗余备份.但由于区块链去中心化的特性,其数据更新和备份无法由中心化的机制进行统一、集中的管理.这导致区块链的监管相较于传统中心化系统更为困难,亦更不可控.早期比特币、以太坊等公有链上经常随机出现各种敏感言论[7].这些言论往往通过交易字段的形式共识上链;任何用户均可以通过开放网络上传此类数据,数据上传者真实身份更是难以追溯;数据一旦上链,全网可以通过区块链浏览器等设施进行浏览.同时,区块链难以篡改的特性带来的数据隐私和内容安全的问题更为突出.无论是公有链还是联盟链,问题数据一旦上链,数据状态完整记录于所有全节点的账本中,基本无法清除与屏蔽.

其次,区块链应用模式较传统互联网应用也具备一些新的特点,传统互联网应用的监管思路和技术很难适用.随着区块链技术的发展,链上内容和服务已由单一的静态内容模式转变为由程序自动化生成的动态模式.当前公有链或开放许可链均可支持用户部署智能合约.智能合约语言大部分是图灵完备的编程语言,具备非常强大的应用刻画和构建能力.随着Web3.0概念的升温和人工智能等技术的成熟,用户生成内容(user-generated content, UGC)[8]甚至AI生成内容(AI-generated content, AIGC)[9]将可能成为主流.这对互联网监管平面是一个巨大的扩充,也对监管机制、方法和监管系统的通用性、灵活性、

可拓展性等提出了更高的要求. 同时, 区块链技术催生的 NFT 等区块链应用新形态的不断出现, 也让区块链应用合规性监管面临新的技术难题.

最后, 区块链应用监管在监管模式上也亟待创新. 区块链应用监管的方法和机制既要考虑技术上的可行、有效, 又要综合考量一系列社会学层面的问题, 适应国情, 做到既能向前兼容传统监管思路, 又能向后兼容解决新的问题和挑战. 传统互联网的中心化监管模式在 Web2.0 时代取得了良好的效果. 但应该注意到, Web3.0 时代区块链应用的核心精神在于规则透明, 多方共识, 其监管机制也应适应性地向“规则透明, 多方共治”的方向发展. 同时又应考虑到区块链应用去中心化的特征对多地域、多部门、多主体的多级监管、多维监管带来了更大的挑战. 如何让多权限层级, 多社会维度的监管方有效的协同监管成为一个重要问题.

针对以上区块链应用监管的重要问题和挑战, 本文设计了一套多链协同治理的“以链治链”监管框架, 并在该框架的指导下进行了监管系统的实现.

本文的主要贡献有 2 点:

1)创新性地提出“以链治链”的监管思想和一套多链协同治理的“以链治链”区块链应用监管框架, 该框架以区块链技术本身作为区块链监管的核心支撑, 从基础层、决策层、跨链层、接入层、执行层和数据层进行了相关监管骨干机制的设计, 不仅能够满足区块链内在特性、区块链应用模式新特点等带来的监管新需求, 同时为 Web3.0 时代的多中心、自动化、多级多维监管提供了新思路.

2)结合框架的设计, 实现了一套区块链应用监管系统. 本文在实验环境下对系统的性能进行了测试, 验证了系统的有效性和可行性. 同时, 该系统已经在地方多个相关部门进行应用试点, 取得了良好的示范效果, 从实践上论证了“以链治链”应用监管框架的可行性和先进性.

1 相关工作

当前学术界对区块链应用监管方面的研究整体还处于探索阶段, 尚不具备一些通用的技术思路、框架和论证成熟的实践. 由于区块链监管实践与社会生态紧密相关, 不同国家在区块链监管领域的研究侧重与整体思路也呈现出一些差异.

区块链应用监管, 被监管的对象是区块链. 一些工作从政策、法律、社会学等宏观层面上思考了区块链被监管的必要性和监管思路. 如赵磊[10] 从法律角度分析了区块链去中心化特性和区块链监管间的关系. 一些工作以综述的形式探讨了区块链监管的技术本源问题和监管技术的潜在发展方向, 如洪学海等人[11] 对区块链安全监管技术进行了综述, 探讨了区块链的技术特点及其产生安全与监管问题的主要原因、频发的区块链安全事件带来的监管技术的发展以及区块链安全监管技术未来的主要研究方向. Wang 等人[7] 根据 4 层结构(网络、传输、共识、应用)对区块链技术和安全问题进行了系统概述, 将区块链安全监管的关键技术分为 3 个方面: 网络层的节点发现技术、交易层的交易记录数据分析技术、应用层的网络流量分析技术, 并讨论了区块链与传统法律之间的关系, 介绍了安全监管的挑战以及该领域未来可能的研究方向.

在区块链应用监管技术方面, 当前的研究大部分聚焦于具体支撑技术的研究, 针对区块链监管的整体性解决方案或框架还很少. Ma 等人[12] 提出了一种具有监管功能的区块链可追溯方案(BTSOF), 监管机构必须获得委员会的同意才能进行追踪. 该工作的核心是进行区块链追溯, 其设计的监管机制本质是多中心化治理机制, 为此其构建了一种非交互式可验证的多密钥共享方案(VMSS 方案), 并利用 VMSS 方案为 Cramer-Shoup 公钥加密方案设计了分布式多密钥生成(DMKG)协议. 另外考虑到区块链监管对区块链应用隐私性的削弱, Shao 等人[13] 提出了一套在许可链上的可追踪的匿名身份框架, 宋靖文等人[14] 提出一套区块链可监管的身份隐私保护方案, 这些工作都是在尝试解决区块链应用监管和用户隐私保护间的矛盾.

同时, 以区块链本身作为监管设施的思路已广泛得到采用, 一些工作从应用的角度思考了如何将区块链技术应用于传统行业的监管工作中. 李贤彬等人[15] 思考了如何将区块链技术应用于传统金融的嵌入式监管中. 梅傲等人[16] 提出了构建以海关为核心的联盟链监管体系方案思路. 方敏等人[17] 则以水产溯源平台为例, 思考了如何通过区块链技术实现跨组织边界的协同监管治理, 尝试解决监管链条中主体间的双重信息不对称和多主体协同治理的困境.

然而, 将区块链技术作为手段(监管链)来进行区块链应用监管的方案和实践(“以链治链”)当前还很少. “以链治链”, 直观理解就是利用区块链技术去进行区块链监管, 这意味着区块链在监管侧需要发挥重要作用, 在被监管侧又是重要的研究对象.

Wen 等人[18] 提出了一种多方环境下的隐私保护区块链监管系统,引入监管链实现区块链上的数据监管,监管数据中的用户信息等敏感信息均采用基于属性加密(attribute-based encryption, ABE)的技术进行加密,从而实现对用户数据的隐私保护和访问控制. 这一方案考虑到将区块链技术应用于区块链监管过程中,但其虽引入了监管链-应用链双层架构并考虑到了单监管链上多方协同的问题,但其未考虑多监管链的情形,更没有考虑到多链监管生态下跨链交互和协同治理的技术问题.

协同治理是"以链治链"路线下的关键技术问题. 当前针对多监管链协同的研究非常少,大多数工作聚焦在单链应用场景下的多方协同治理. 朱婉菁[19] 从多中心协同治理的角度分析区块链应用特性与整套治理生态的契合点和其带来的新问题;解释了多中心协同的概念并指出了存在的问题;从 3 个层面解释了用区块链解决多中心协同的内在逻辑;从数据层、网络层、共识层、激励层、合约层和应用层解释了区块链的技术特性和对于实现协同治理的助推功能;最后从可能性和合法性 2 个角度分析了区块链解决方案的局限性. 宋俊典等人[20] 则提出了一套基于区块链进行数据协同治理的方案,设计了支持审计的数据存储和处理方法,支持溯源问责的数据获取和共享方法和支持验证的分布式数据统计分析和机器学习方法. 国外对区块链治理的研究则更偏向于群体博弈和决策的研究. Pelt 等人[21] 从 3 个层次(链下社区、链下开发、链上协议)、6 个纬度(形成和背景、角色、激励机制、参与方关系、沟通、决策)定义了一个区块链治理框架. Beck 等人[22] 则从经济学角度,讨论区块链经济的治理机制. 此外 DiRose 等人[23] 和 Fritsch 等人[24] 还对分散自制组织(decentralized autonomous organization, DAO) 的治理机制进行了研究和探讨.

综上所述,现有研究还没有针对区块链应用监管采用分层级、多监管链协同的技术路线,缺乏适应国内实际应用需求的,针对区块链应用监管的整体监管框架设计和配套监管机制,更鲜有依托提出的技术框架、机制进行实际监管系统构建的应用实践.

本文研究团队在 2019 年 CCF 中国区块链技术大会的主题报告中首次提出了"以链治链"的思想,多年来针对"以链治链"技术及应用展开研究工作. 本文提出了一种多链协同治理的"以链治链"区块链监管框架,实现了一套境内区块链内容监管系统,并在多个地方的核心部门进行了应用实践.

2 监管框架设计

本文提出"以链治链"的监管思路,并在此基础上提出一种多链协同治理的"以链治链"区块链监管框架. "以链治链"即通过区块链基础设施和相关技术对受监管区块链进行监管的技术路线. "多链协同"指多级多维监管链间以及监管链与接入链间通过监管决策自动化、跨链互操作、异构链接入、分布式边缘自动监管等多层次监管骨干机制相互配合,实现对异构区块链应用的有效监管.

"以链治链"是本框架的核心思想. 以区块链作为监管重要设施,从决策层上实现了多中心化监管,避免了潜在的权责集中问题. 同时,区块链程序自动执行、上链数据多方共识、不可篡改的特性保证了监管过程的透明可审计. 为了实现纵向监管细粒度多级可控、横向多协作部门灵活加入、定制化监管应用按需接入,治链的设施不局限于一条单链,而是分层多级的监管链网络.

监管框架明确了基本监管架构,基本监管流程和监管骨干机制,为实际监管系统的搭建保留合理的设计空间,具备通用、灵活、可拓展的特点. 该框架下区块链监管机制主要解决 6 个层面的技术问题:基础层、决策层、跨链层、接入层、执行层和数据层. 其中基础层解决监管链基础设施层面技术问题;决策层解决监管规则、决策的生成问题;跨链层解决监管数据的链间传输问题;接入层解决监管侧与被监管侧的对接问题;执行层解决具体监管动作的执行机制问题;数据层解决被监管区块链数据隐私以及链上数据、内容的监管机制问题. 各层关系如图 1

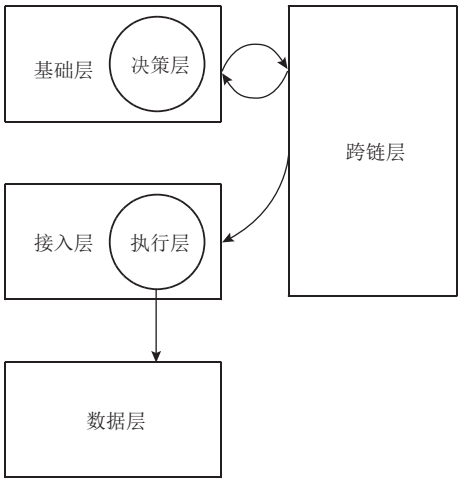

Fig. 1 Abstraction of supervision mechanism

图 1 监管机制抽象

所示.

该框架在明确监管骨干机制的基础上，支持各层机制的模块化配置.

2.1 基本监管架构

本文的基本监管架构如图 2 所示，本节对监管框架中的主要设施、实体和技术需求进行阐述.

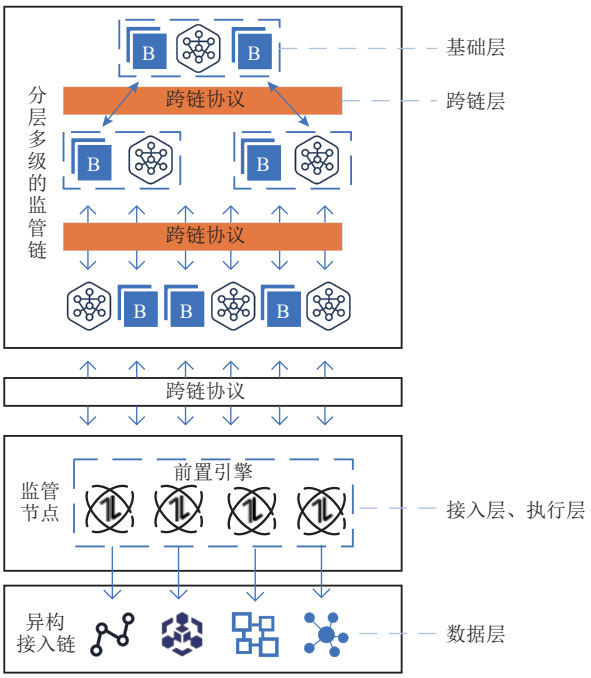

Fig. 2 Basic supervision architecture

图 2 基本监管架构

2.1.1 监管链

监管链是监管框架中核心设施之一，是实现多中心决策、多中心协同、可审计、自动化监管的核心载体，其最小功能集合包含监管规则生成、监管指令下发、监管结果存证、监管规则更新等.

1)链上主体. 链上主体可根据多中心化、效率、安全性、信任根假设等具体情况和需求进行组织. 一般情况下，为了避免权责集中，机制不透明等问题，监管链主体应由多监管角色组成，其物理节点的实际控制权也应由多监管方所有.

2)网络架构. 网络架构层面，监管体系至少包含一条监管链，但框架支持分层多级、多维的监管网络，如图 3 所示. 监管链以链为单位应具备权限分级机制，一般情况下，上层监管链监管权限高于下级监管链.

3)技术特征. 框架支持异构监管链，并不限制链选型，但框架要求监管链具备以下技术特点：①监管链所承担的监管功能较为特殊，其准入模型以联盟链或私链为主. 区块链本身或配套设施具备数字身份管理、访问权限控制等机制. ②由于监管链具备监管结果存证这一基本功能，因而监管链具备混合高效的存储模型，支持多组织类型数据海量存储，支持非结构化大文件存储，并支持海量监管数据的链上存储和高效读取. ③由于监管链应具备监管指令下发等功能，且多监管链间、监管链与接入链间有协同监管机制，因而监管链支持跨链互操作机制. ④如 EVM 等智能合约虚拟机曾是区块链执行层(状态机)的主流技术选型之一，但其有执行效率低，可治理性差，开发不灵活性等一系列缺点[25]，因此监管链为应用特化区块链[26]，监管链应用本身属全链应用[27].

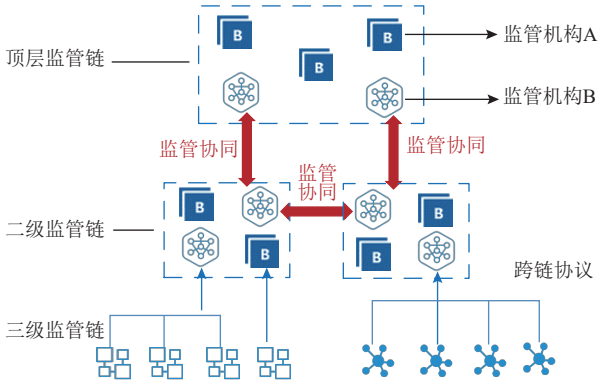

Fig. 3 Supervision chain networking architecture

图 3 监管链网络架构

2.1.2 接入链

接入链是本监管框架引入的特色概念之一，是通过一系列接入层机制，适配并接入了监管链的业务区块链. 换言之，接入链是适配了监管功能的业务链. 区块链监管实践本身面临监管效率、穿透性和业务链被侵入程度的权衡. 本文框架在接入层引入了当前主流的密态审计技术和零知识证明等技术，既实现穿透式监管，又最大程度上保证链上业务的隐私性.

接入链上的核心监管设施是前置引擎，其是分布式边缘自动监管的核心. 前置引擎的最小配置集合包括：哈希索引、隐私安全计算和加密关键词库等. 框架下前置引擎可以根据监管具体需求部署在接入链的监管节点上，也可以在业务方许可的情况下布置于业务节点上. 本框架可以支撑异构接入链的监管.

2.2 基本监管流程

本部分出现符号及其对应含义如表 1 所示.

监管链层级可根据具体监管需求分为 N 个层级，用 SC_{ij} 来表示第 i 层的 j 监管链. A_{ij} 表示 SC_{ij} 的监管权限. 上级监管链权限高于下级监管链，且同级监管链权限相同，即 $A_{ik} > A_{jm}$ ($i < j$, $1 < i,j,k,m < N$), $A_{ik} = A_{im}$

Table 1 Symbols for Basic Supervision Procedure

表 1 基本监管流程符号

符号	含义
N	监管链层级
SC_{ij}	第 i 层的 j 监管链
A_{ij}	SC_{ij} 的监管权限
A_r	读权限
A_w	写权限
M	监管指令
PC_i	接入链
R	监管回执

$(1 < i, k, m < N)$. 监管权限包含读权限 A_r 和写权限 A_w, 高权限监管链可以向低权限或同权限监管链发送监管指令 M. 任意 $SC_{ik}(1 < i, k < N)$ 可以向任意接入链 PC_i (i=1, 2, …)发送监管指令. 任意监管指令接收方在收到指令并完成链上共识后, 需向 M 发出方返回监管回执 R. 监管指令 M 包括横向监管指令和纵向监管指令, 横向监管指令为监管链向同级监管链发出的指令, 纵向监管指令为监管链向下级监管链或接入链发出的指令.

在以上设定下, 基本监管流程如图 4 所示.

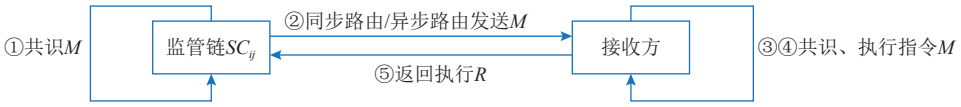

Fig. 4 Basic supervision procedure

图 4 基本监管流程

1)触发阶段. 监管链 SC_{ij} 主体通过链上治理过程对 M 进行链上触发. 链上治理过程可根据实际需求进行定制, 常见手段包含门限签名, 聚合签名, 链上投票等机制. M 在 SC_{ij} 上完成共识.

2)跨链阶段. M 在 SC_{ij} 上完成共识后, 进入跨链阶段. M 从源链到达目的链需依赖监管指令路由. 监管指令路由包含异步路由和同步路由. 同步路由时, M 自身包含有序的监管路径信息, M 必须按照路径信息确定的唯一路径进行逐跳指令传递. 异步路由时, M 自身包含的路径信息是无序的目的监管链集合, 指令发起链可同时向目的监管链发送 M.

3)M 通过同步路由方法或异步路由方法到达接收链后, 接收链对 M 进行验证、共识、执行.

4)当 M 的接收方为监管链时, M 执行以发起链上交易为主. 当 M 的接收方为接入链时, 接入链的前置引擎将根据指令内容和执行层机制对接入链业务进行监管动作. 常见监管动作包括关键词过滤、信息巡查、数据处理等.

5)M 执行后的监管回执 R 将返回指令发起监管链. 回执和监管指令在数据层面的实质相同, 也可以采用同步路由或异步路由的方法进行返回.

3 监管骨干机制设计

如第 2 节所述, 监管框架支持各层具体监管机制的模块化配置. 一些骨干机制的设计对框架下构建的监管系统的有效性和可行性至关重要. 本节明确各层监管机制解决的核心问题, 并对其中一些关键机制进行阐述.

3.1 基础层、决策层机制设计

基础层主要解决监管背景下“以链治链”对监管链、监管节点等链基础设施的特殊技术要求; 决策层主要解决监管链多中心化决策、监管规则、指令自动化、安全执行等技术问题.

针对当前区块链监管背景下, 监管节点共识效率低、稳定性差, 异构区块链监管网络模型缺失, 海量监管存储性能差、成本高等现状, 基础层和决策层解决了大规模异构区块链“以链治链”监管问题中复杂网络共识算法高效与稳定的协同优化、海量异构节点大规模组网高可拓展性与高性能的对立统一、海量高频交易数据场景下的高效存储与分发等技术问题; 构建了混合异构大规模分层组网、锚定监管链数据的混合高效存储等关键模型; 解决了复杂网络下高性能、高鲁棒性监管共识等核心问题.

3.1.1 复杂监管网络的高性能高鲁棒性监管链共识

监管链节点需在复杂监管网络下完成交易快速验证、在弱稳定网络下能保持活性、支持交易信息流水线的动态分发机制, 保证海量交易场景下系统的事务处理能力、稳定性及可用性.

针对监管链, 采取了高效的聚合签名算法降低网络复杂度, 实现了交易的快速验证, 并在网络不稳定, 延迟较高场景下实现了灵活的超时机制来保证系统的稳定性和可用性; 为了提高交易并行处理能力, 采取了交易信息流水线动态分发策略及交易缓

存池机制，在防止交易丢失和快速去重的同时满足了实际场景下交易处理性能.

3.1.2 监管友好的异构大规模分层组网机制

大规模组网的区块链会面临性能低、可拓展性差等问题，为此监管链需支持大规模节点网络动态转发、异构多类型节点的动态组织.

监管链采取了 DNS 广播发现和数据跨域转发机制，实现了节点网络的动态转发. 采用了高效的交易验证模式，实现了监管链网络节点水平拓展，并支持跨域通信，保证海量网络消息的高效传输.

3.1.3 针对锚定监管链数据的混合高效存储模型

监管链配备了区块、状态、大文件数据专用存储引擎，并具备多级缓存机制，从而保证了监管数据的高效存取，保证了在监管链数据量不断增大的情况下读写性能不受影响.

3.2 跨链层机制设计

根据监管框架的设计，多监管链间协同监管、监管链对接入链执行监管等均需要监管指令、监管回执等数据跨独立区块链边界进行传输，进而实现跨链消息的读取以及跨链合约的调用. 本节对监管框架下跨链层骨干机制进行描述.

3.2.1 通用链间传输消息格式

异构区块链的交易格式、加密算法等的不同造成异构区块链在数据层存在隔离. 为了更方便的进行跨链消息的验证和路由，实现跨链网关更一致的跨链消息处理，本文设计了跨链消息的主要数据字段，如表 2 所示.

Table 2 Uniform Cross-Chain Transmission Message Format

表 2 通用链间传输消息格式

参数	说明
From	来源链 ID
To	目的链 ID
Version	协议版本号
Payload	跨链调用内容编码
Timestamp	跨链事件发生的时间戳
Proof	跨链交易证明
Extra	自定义字段

其中 *From* 和 *To* 字段分别代表源链和目的链的 ID，ID 在监管链或接入链向监管系统注册时生成. *Version* 字段标识了具体跨链协议的版本信息.

Payload 字段是跨链调用的内容编码，支持定向加密，可由监管链的业务需求确定. *Timestamp* 字段是跨链交易的一个时间标识.

Proof 字段存储了跨链交易合法性证明，为跨链验证机制提供具体的验证信息. *Proof* 字段内容根据源链的不同而不同，具体的验证方式由异构链的自验证算法等来确定，具体验证规则可通过动态加载的方式注册到跨链验证引擎.

最后，通用链间传输消息格式提供了一个自定义拓展字段，其可根据业务需求进行自定义，比如对现有跨链协议控制信息进行自定义拓展等.

3.2.2 高效跨链路由技术

针对监管框架大规模多层级的监管链-接入链网络，需要通过跨链路由机制进行跨链消息的传递，为此本文设计了一套基于跨链网关与中继链的跨链路由网络，其拓扑如图 5 所示.

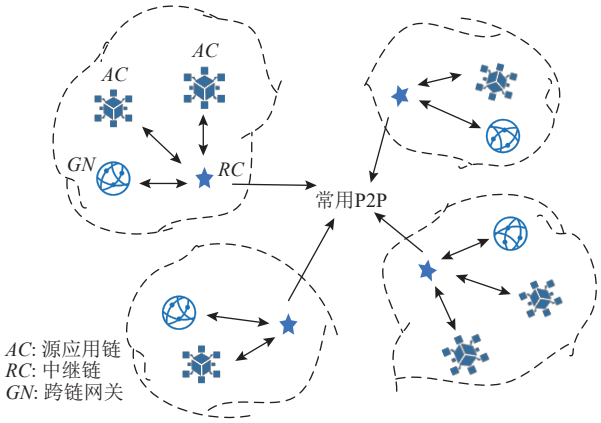

Fig. 5 Cross-chain router network

图 5 跨链路由网络

在跨链数据传输语境下，将监管链与接入链统称为应用链.

1）中继链. 中继链是由多实体控制的节点形成的多中心化的应用特化区块链，从准入机制角度一般为联盟链或私链. 其核心功能是为所连接的应用链的跨链交易进行有效性验证与背书. 在本框架中，我们支持 2 种对跨链交易有效性验证的方法：基于公证人的担保以及基于链自可验证性的算法验证. 对验证结果进行背书则采用公证人集合多签的方案. 1 条中继链至少与 1 个跨链网关进行绑定，该跨链网关为中继链在网络传输层的代理. 中继链上部署跨链验证引擎，该引擎集成了跨链信息验证方法、跨链信息背书方法以及全局中继链的验证元信息等.

2）跨链网关. 跨链网关是一个链下进程，是跨链数据在网络层传输的核心设施. 1 个跨链网关与 1 条中继链进行绑定作为该中继链在网络传输层的代理. 跨链网关不仅是应用链与中继链间进行数据互通的

基础设施,各跨链网关通过实现常用 P2P 算法,还可以实现彼此在网络传输层的互通.

如图 6 所示,应用链间跨链消息路由的基本流程如下,其中涉及到的符号与其对应含义如表 3 所示.

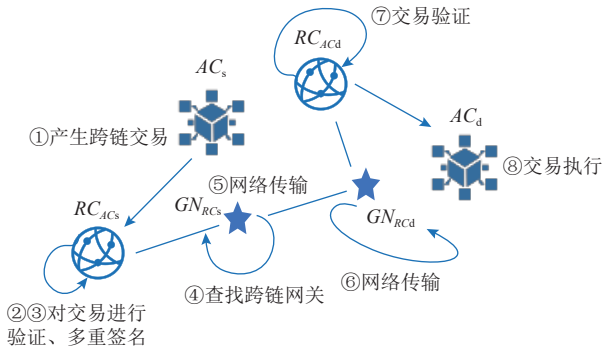

Fig. 6 Cross-chain message routing

图 6 跨链消息路由

Table 3 Symbols for Cross-Chain Transaction Routing

表 3 跨链交易路由符号

符号	含义
AC_s	源应用链
RC_{ACs}	与 AC_s 连接的中继链
GN_{RCs}	与 RC_{ACs} 绑定的跨链网关
AC_d	目的应用链
RC_{ACd}	与 AC_d 连接的中继链
GN_{RCd}	与 RC_{ACd} 绑定的跨链网关

1)跨链初始配置阶段:

① 中继链加入跨链网络之前,需要具有跨链路由功能的跨链网关与中继链绑定,并负责连接中继链和跨链网络中的其他跨链网关.该跨链网关的身份代表中继链在跨链路由网络的标识.

② 新中继链的验证元信息应当同步于监管系统的所有中继链中.根据监管系统具体需求,信息同步可通过各中继链管理员向中继链中注册新加入的中继链验证元信息,也可通过链外可信源向中继链同步新加入中继链的相关信息.

③ 每个跨链网关会维护一个全局的分布式哈希表,记录应用链和中继链的关联关系.跨链网关在加入路由网络时,需要广播所属中继链管理的所有应用链信息,其他跨链网关会根据广播信息进行分布式哈希表的更新.

2)跨链交易路由阶段:

① 当应用链 AC_s 产生跨链交易时,与应用链连接的中继链(RC_{ACs})对应的跨链网关(GN_{RCs})会扫描到该跨链交易;

② RC_{ACs} 中各个节点对跨链交易进行验证,对其有效性进行评判;

③ RC_{ACs} 中各个节点根据交易验证结果对该跨链交易进行多重签名;

④ GN_{RCs} 通过路由算法查找跨链交易的目的中继链 RC_{ACd} 对应的跨链网关;

⑤ 跨链交易通过跨链路由网络进行传输;

⑥ 目的跨链网关 GN_{RCd} 验证 AC_s 的存在性以及跨链交易目的应用链 AC_d 的正确性,即确定 GN_{RCd} 负责 AC_d 的消息转发;

⑦步骤⑥验证通过后,GN_{RCd} 将跨链交易发送给 RC_{ACd};

⑧ RC_{ACd} 通过其跨链验证引擎验证跨链交易有效性;

⑨ 如果 RC_{ACd} 验证有效,GN_{RCd} 将触发 AC_d 上相关区块链交易,执行跨链消息.

3.2.3 链外可信源配置

监管链、中继链等独立区块链在监管框架中的正常运转依赖于可信数据的输入.尽管区块链智能合约以及共识机制等能很大程度为链上计算过程增信,但无法保证上链数据本身的有效性.这就需要我们的监管机制能够提供配置灵活、信息动态更新且安全的可信源.本文提出的监管框架并不限制可信源的形式及可信源的集成方法.可以兼容本监管框架的常见可信源包括链下预言机、可读区块链,以及基于权限的人工信息输入等.这里以基于本监管框架的监管系统对数字身份信息及权限信息的配置为例,简单介绍可信源配置的方法.

1)基于权限的人工信息输入.该可信源是最简单也是最常见的可信源.其一般要求监管系统中心化配置一批具有管理员权限的实体,并提供管理员权限的验证机制.管理员通过调用区块链上交易等手段,在区块链上存储或更新数据.同时,为了避免单一管理员权责集中的问题,利用了聚合签名等技术手段,将区块链读写权限多中心化.如图 7 所示,对于数字身份和权限管理服务,当全局数字身份和权限信息更新时,可通过聚合签名等手段对监管链数字身份及权限管理模块内信息进行更新.

2)可读区块链.传统中心化系统存在单点失效,管理权限集中,机制不透明等一系列问题.而多中心化、规则透明、支持共识算法的区块链系统可以很好的解决这一问题.对于数字身份和权限管理服务,如图 8 所示,通过引入可信的身份管理链等设施,通过跨链互操作机制,实现了身份信息、权限管理信息

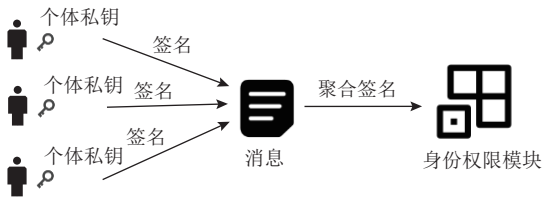

Fig. 7 Manual message input based on authorities

图 7 基于权限的人工信息输入

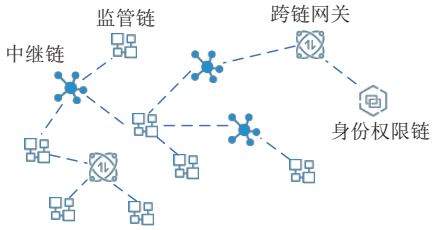

Fig. 8 Readable blockchain

图 8 可读区块链

的可信读取.

3)链下预言机. 链下预言机是专门解决区块链数据来源可信问题的基础设施. 结合执行层可信执行环境(trusted execution environment, TEE)技术, 预言机可以向相关区块链模块填充可信数据. 针对数字身份和权限管理服务, 一种可行的技术思路如图 9 所示:

3.2.4 监管链原生跨链数字身份管理方案

监管链系统一般应为联盟链或私有链, 其必须

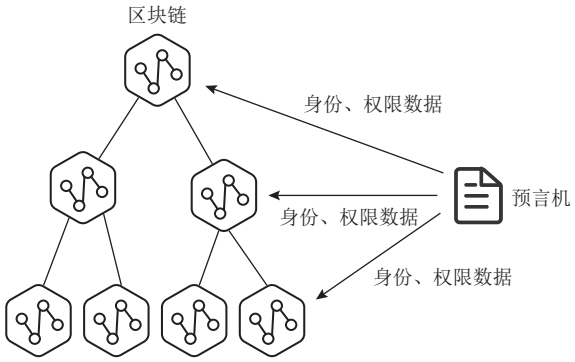

Fig. 9 Off-chain Oracle

图 9 链下预言机

支持数字身份管理等功能才能保证监管功能的正常作用. 而传统中心化系统的数字身份管理技术无法很好的满足异构监管链分布式、多中心化、跨链友好的数字身份管理需求, 为此本文设计了一套监管链原生跨链数字身份管理方案.

该方案整体设计符合 W3C 去中心化身份[28] (decentralized identity, DID)及相关规范, 其支持对链和账户数字身份的管理, 能标识区块链、节点、链上账户甚至合约等实体, 与分层多级监管链的跨链路由消息网络模型紧密配合.

该 DID 的系统基本架构如图 10 所示.

本文中所有的中继链都会实现链数字身份(Chain DID)管理功能及账户数字身份(Account DID)

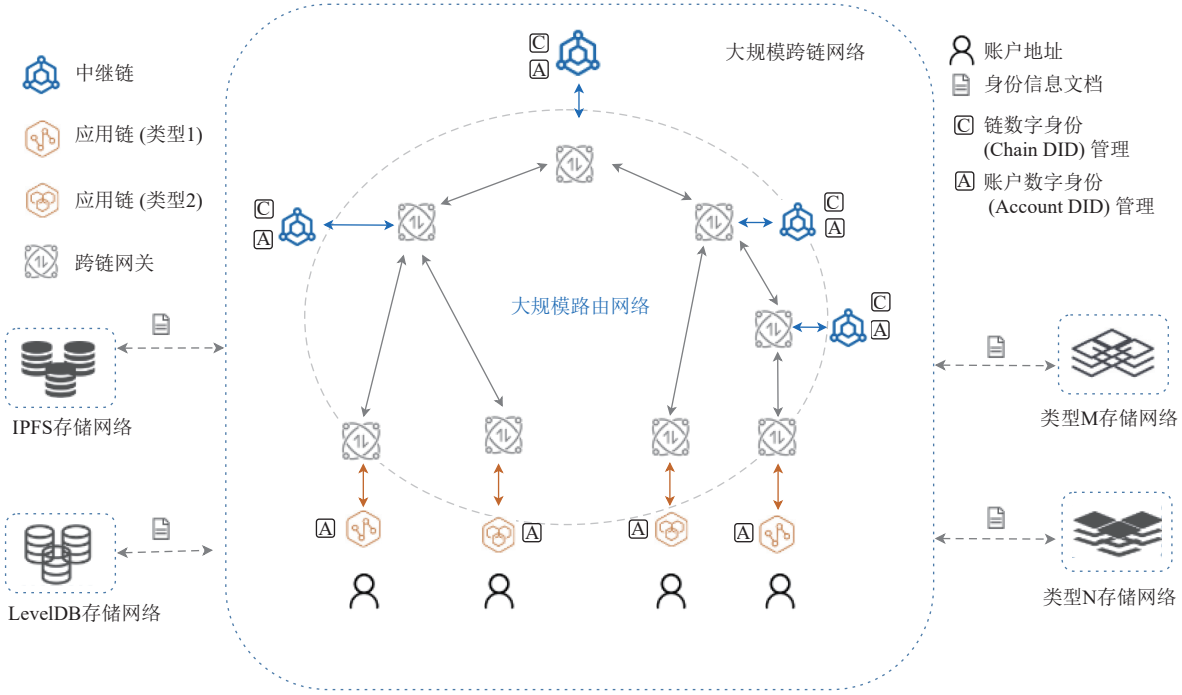

Fig. 10 Network topology of DID system

图 10 DID 系统网络拓扑

管理功能,而应用链(监管链、接入链等)将会实现 Account DID 管理功能. 考虑到整个网络面临账户扩展的需求,方案提供了文档链下存储功能.

每条区块链的身份标识表(DID Table)用于记录身份标识相关的身份信息,其表项包含身份状态、文档存储地址、文档哈希等字段. 存储链身份信息的身份标识表叫做"链身份标识表"(Chain DID Table),存储账户身份信息的身份标识表叫做"账户身份标识表"(Account DID Table). Chain DID Table 与 Account DID Table 的不同点在于,Chain DID Table 会在网络中所有中继链上进行同步,而 Account DID Table 不会,Account DID Table 只存储自己链上的账户身份信息.

接下来,以链数字身份为例来介绍下数字身份在实际应用场景下的使用流程.

如图 11 所示是 Chain DID 的工作流程,其中:

1)申请 Chain DID. 如图 11 中①,向管理中继链发起请求,发送 Chain DID 名称.

2)审批 Chain DID. 如图 11 中②,管理员对用户的申请请求做出审批,结果为"审批通过"或者"审批驳回".

3)注册 Chain DID. 如图 11 中③④,当审批通过后,可以进行注册. 首先在③中,将链身份的相关信息组织成 Chain Doc 进行存储得到存储地址 docAddr 和内容哈希 docHash. 然后在流程④中,以 docAddr 和内容 docHash 等为参数向最高中继链发起注册请求.

4)解析 Chain DID. 如图 11 中⑤⑥,Chain DID 的信息在所有中继链上同步,所以可以向任意一条中继链发起 Chain DID 解析. 首先在⑤中,客户端对任意中继链发起解析请求,获得该身份的相关信息(包括存储地址和内容哈希). 然后在⑥中,通过存储地址获取实际的 Chain Doc, 进行哈希校验,如果通过则证明 Doc 可信.

当某个 Chain DID 的注册过程在管理中继链上完成后,需要将该新建的 Chain DID Table 同步到网络中其他所有中继链,每次同步的单位是一个表项. 当 Chain DID Table 表项发生新建、更新、删除时,应进行数据同步. Chain DID 数据同步需要借助中继链间跨链操作,这里中继链会向网络中其他所有中继

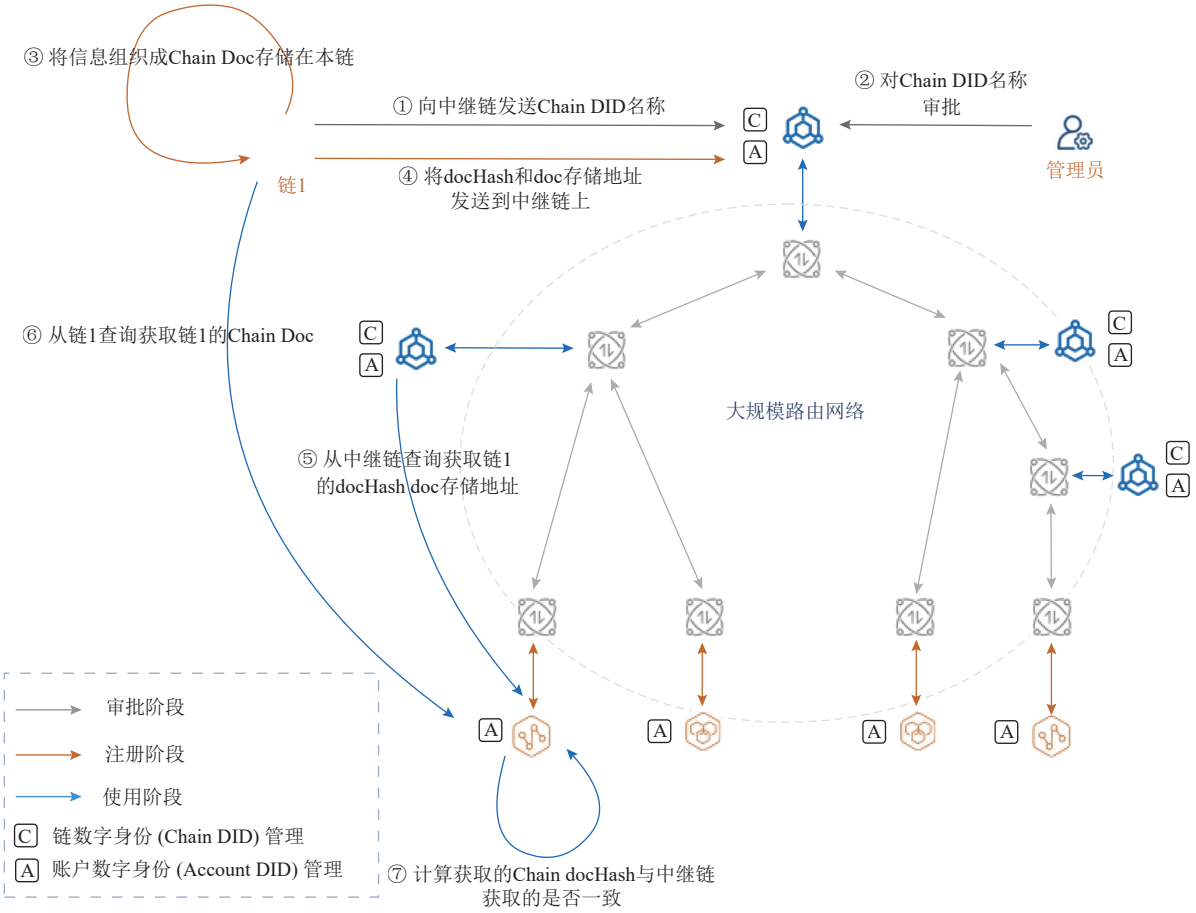

Fig. 11 Workflow of Chain DID

图 11 Chain DID 工作流程

链都发送一次跨中继链的跨链消息以进行数据同步，且整个同步过程是由最高中继链依次往下逐级同步的.

Account DID 的机制与 Chain DID 的机制整体类似，篇幅原因，不再赘述.

3.3 接入层机制设计

接入层机制的设计主要解决 2 个层面的问题. 首先，被监管的异构业务链如何接入监管系统成为接入链，即异构链接入问题. 由于通用的监管方案与系统需考虑向后兼容问题，接入机制应当灵活、可拓展. 其次，接入链如何对架构边缘的业务链数据、内容等执行分布式、自动化的监管动作，即边缘自动监管的问题. 本节对监管框架下的这些机制进行描述.

3.3.1 异构链接入机制

异构接入链接入监管系统的机制应当权衡对业务链的侵入性和监管的效率、穿透性. 本框架提出了一种基于监管节点的异构链接入机制. 为了尽量降低对业务链的入侵性，监管节点不需要是业务链的共识节点或数据全节点. 但其应具备业务区块链某些数据接口的访问权限，如密态链上信息的读取接口权限等. 如图 12 所示，监管节点和业务区块链节点共同构成接入链.

异构业务链的监管节点植入(兼容)过程整体如下：

1)首先异构业务链运营方在注册接入监管系统时构建业务链监管节点，该节点应配置业务链上数据读取与交易调用等权限；所有监管节点同时应为其所属辖域监管链开放接口访问权限，监管链通过 3.2 节明确的跨链互操作机制，可以对监管节点发送监管指令.

2)监管框架明确了监管节点在链下需实现的相关监管动作接口，比如链前检测接口和链上巡检接口，业务链方应对相关链下接口提供接口适配.

3)其中链前检测一般要求业务链交易统一导流到监管节点，监管节点在链下对交易进行监管动作后，再调用业务链接口进行交易上链，该监管动作对业务链入侵性较强，但监管时效性较好.

4)链上巡检则在业务链监管节点接到监管链巡检指令后，通过链下实现的链上巡检逻辑对业务链的历史区块信息进行读取和检测，该监管动作对业务链的入侵性不强，但是监管具有一定滞后性.

以上方案可以灵活的适配各种异构业务链，同时可根据监管效率、穿透性的要求，对独立业务链进行较小的侵入与改造.

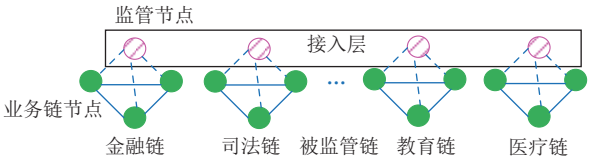

Fig. 12 Mechanism for heterogeneous chain probing

图 12 异构链接入机制

监管节点中最核心的设施是前置引擎，前置引擎可以设置在监管节点上，从而方便进行分布式的边缘自动监管.

3.3.2 分布式边缘自动监管机制

分布式边缘自动监管机制是框架下监管系统对多行业、多地域异构业务链在近端进行自动、下沉监管的核心机制，其载体是前置引擎. 具体机制如图 13 所示.

前置引擎配置在接入链中，由于其位于监管节点上，对业务区块链的业务系统、数据等具有相应的监管权限. 前置引擎配备了隐私计算与密态审计等功能引擎，并支持了计算模型等的动态加载与计算；配备了加密关键词库，加密词库能够动态更新.

分布式边缘自动监管的基本流程如下：

监管规则分发阶段，如图 14 所示.

①分发指令、共识. 监管链触发监管规则分发指令，并在源监管链上进行共识.

②指令下达. 通过 3.2.2 节的跨链信息路由机制，指令下达接入链.

③更新计算模型. 接入链上监管节点接收到指令后控制前置引擎根据指令中的监管规则更新计算模型.

④加载计算模型. 前置引擎加载计算模型.

⑤更新加密词库. 前置引擎根据监管需求更新加密词库.

监管指令执行阶段，如图 15 所示.

①分发指令、共识. 监管链触发监管执行指令，并在源监管链上进行共识.

②指令下达. 通过 3.2.2 节的跨链信息路由机制，指令下达接入链.

③下发监管指令. 接入链上监管节点接收到指令后向前置引擎下发监管指令.

④调用接口载入待监管内容. 前置引擎接收到指令后调用业务链系统相关接口，载入待监管内容.

⑤隐私计算审查. 前置引擎通过自身功能引擎进行隐私计算审查.

⑥前置引擎返回监管结果. 前置引擎向接入链

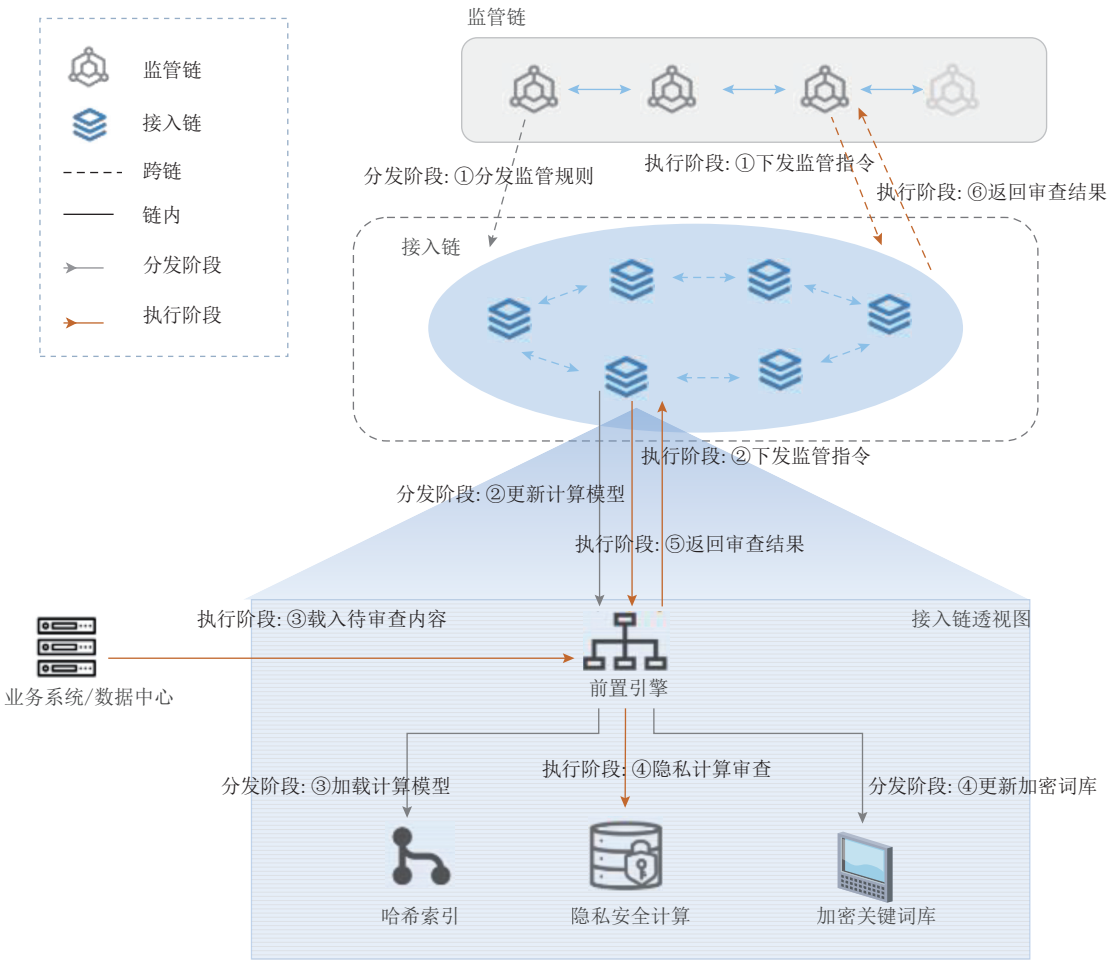

Fig. 13 Distributed autonomous edge supervision mechanism

图 13 分布式边缘自动监管机制

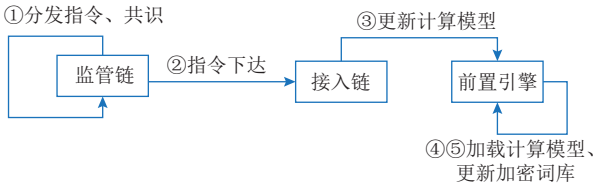

Fig. 14 Supervision rule distribution phase

图 14 监管规则分发阶段

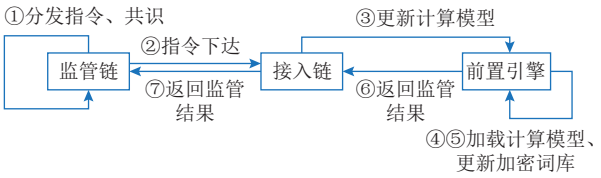

Fig. 15 Supervision command execution phase

图 15 监管指令执行阶段

监管节点返回监管结果.

⑦接入链返回监管结果. 接入链监管节点通过跨链信息路由将监管结果返回监管链.

3.4 数据层机制设计

监管数据层机制针对当前区块链监管背景下密态内容治理的技术挑战, 从接入链数据层、链基础设施层解决区块链数据、内容监管的核心算法和机制. 本文提出以下关键机制.

3.4.1 密态数据审计架构及相关机制

针对链上密态数据的审计, 通过高效可搜索加密技术, 实现了对大规模链上密文数据的过滤和检索; 通过结合函数加密、同态加密等密文计算技术实现了链上数据的密态发布, 并支持密态数据上的多种合规审计; 通过结合密文发布和零知识证明、范围证明等可验证计算实现了对密态数据合规性的简洁、快速合规性证明. 在保证安全隐私的同时提高审计功能性, 提升了密态内容审计的计算和带宽效率, 从而构建了支持大规模、高吞吐量的密态数据审计的架构.

3.4.2 受控隐私保护的身份管理体系

针对接入链上身份隐私和有效监管间的矛盾, 设计了匿名可追踪的群组数字签名方案, 实现了源账户受控身份匿名; 设计了支持可追踪属性加密方

案，实现了目的账户受控身份匿名；通过支持违规行为用户的身份自动发现，细粒度、动态的身份撤销，并融合国产公钥密码标准体系，实现了无需可信第三方的大规模受控隐私保护的身份管理体系.

3.4.3 受控可删改区块链数据层架构

尽管区块链监管应尽量降低对接入链的侵入性，但对接入链数据层监管机制兼容性的研究有利于构建可监管区块链设计标准，并指导后续新型可监管区块链的创新构建实践. 为此在监管框架下研究了支持区块链回滚和细粒度修改的新型区块结构和链式结构，提出了区块链受控修改的密码杂凑函数，构建了可验证数据删除的安全模型，研究了基于密码理论的可验证数据删除技术，监管链和接入链在形成共识后，可以实现对已发布区块链的回滚和不同粒度的修改.

4 监管系统实现及示范应用

本文依据提出的监管框架，利用一系列监管骨干机制，设计、实现了一套适用于注册联盟链的区块链应用监管系统(后简称监管系统). 该工作以监管架构和监管骨干机制为底层技术，以监管链、接入层监管节点为主要设施，设计实现了一套基于“源头预防，过程管控，事后处理”的监管执行层机制，搭建了一套适用于实际监管场景的系统.

区块链总体应用监管系统如图 16 所示. 系统包括总体态势、链前预警、链上违规、管控反馈、巡检管理、数据校验、业务链管理、业务注册和权限管理模块. 以链上违规模块为例，系统展示了被监管的业务链列表. 系统监测到包含违规关键词的交易之后会上报违规信息，用户可以核验该交易，再次确认该交易为有害交易或无害交易.

系统的权限管理体系效果示意图如图 17 所示. 系统支持省级网信办、市级网信办等多层级监管机构接入，同时支持系统管理员、系统用户等多种用户权限，管理员可以向不同级别的用户分配不同的数据访问权限.

同时，本监管系统已经在多个地方有关部门进行了示范应用，取得了良好的应用效果和显著的社会效益.

因为篇幅原因，本节将对区块链应用监管系统的核心部分监管链接入链数据协同系统进行介绍，并对应用监管系统的实验部署和性能表现进行介绍.

4.1 系统整体目标

区块链应用监管系统的监管对象涵盖存证、溯源、版权、BaaS、金融等当前区块链主要应用领域，重点识别、关注、分析具有内容分发、即时通信等传播属性的区块链服务. 同时以“以链治链、全链监管”为主要思路，通过构建监督管理节点服务、监管链服务，提供对以联盟链为主的区块链应用的链上监管服务能力，实现对区块链应用及存储节点上信息内容的发现与监测，从而对具有内容安全风险的区块链应用和节点进行管控.

其核心子系统监管链接入链数据协同系统针对

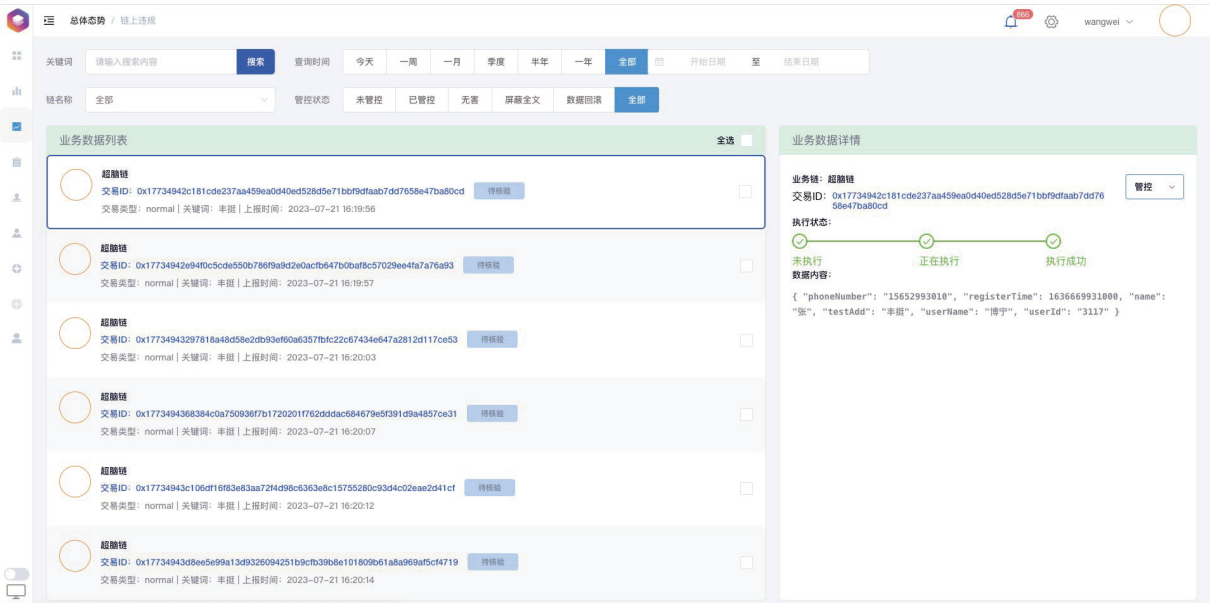

Fig. 16 Illustration of blockchain application supervision system

图 16 区块链应用监管系统示意图

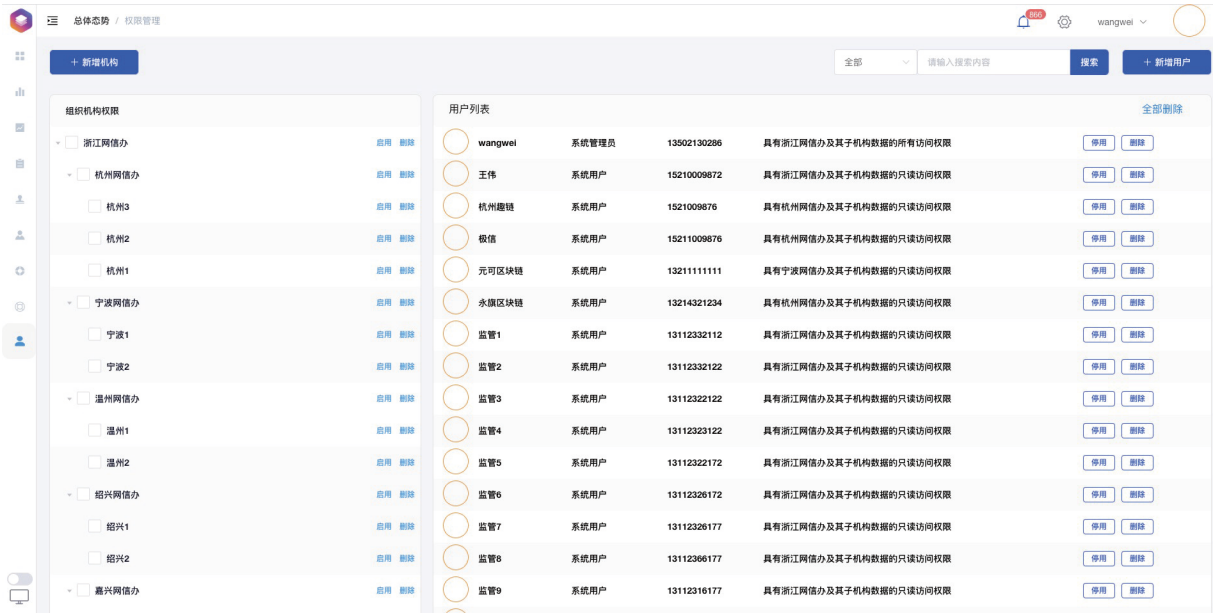

Fig. 17 Illustration of system authority management

图 17 系统权限管理示意图

不同类型区块链难以接入监管系统、海量异构的接入数据难以统一处理问题，设计了接入链数据的统一表达模式和接口规范，接入数据处理结果验证技术和接入链数据巡查技术，实现了数据接入处理、风险识别、结果验证、信息巡查与风险识别等功能.

4.2 系统总体架构

监管链接入链数据协同系统的核心模块包括业管理、协同接入、数据巡查、数据验证、风险识别、数据存储，以及系统安全模块和运维监控等模块. 系统架构如图 18 所示.

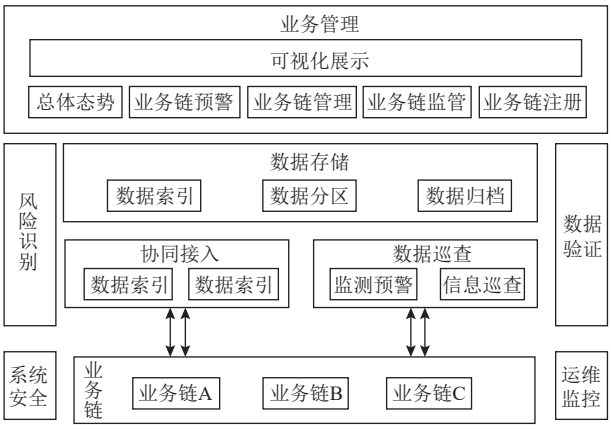

Fig. 18 Overall architecture of system

图 18 系统总体架构

4.3 系统功能模块设计

4.3.1 模块概览及功能设计

下面对几个核心功能模块进行介绍：

1)业务管理模块. 提供可视化展示功能，具体包括总体态势、业务链预警、业务链管理、业务链巡查等功能. 其中，业务链注册模块研发业务链鉴权、密钥管理功能，具备业务链注册功能，可生成 appKey，业务链通过 appKey 与系统进行对接，完成数据接入，并提供接入业务链查询功能.

2)协同接入模块. 根据统一的数据接入规范，实现不同类型的区块链数据的协同接入，保证数据格式的一致性.

3)风险识别模块. 负责对区块链数据进行风险检测，在巡检的过程中，数据巡查模块会调用风险识别模块对已接入数据进行风险检测，并将识别出的风险数据进行上报.

4)数据验证模块. 负责接入数据处理结果的正确性、完整性验证，确保监管链存储数据与接入链数据的一致性.

5)数据存储模块. 提供数据索引、数据分区、数据归档等数据管理服务，实现对接入的多条业务链数据的数据管理功能.

6)数据巡查模块. 负责建立接入链信息巡查和监测预警机制，实现对接入链风险研判，做到安全风险提前预警，预防接入链数据的安全风险隐患. 研发信息巡检模块，实现巡检任务下发、任务管理，通过页面下发巡检任务，接入业务链. 同时，可根据业务链、关键词等条件查询巡检状态与结果.

模块之间关系如图 19 所示.

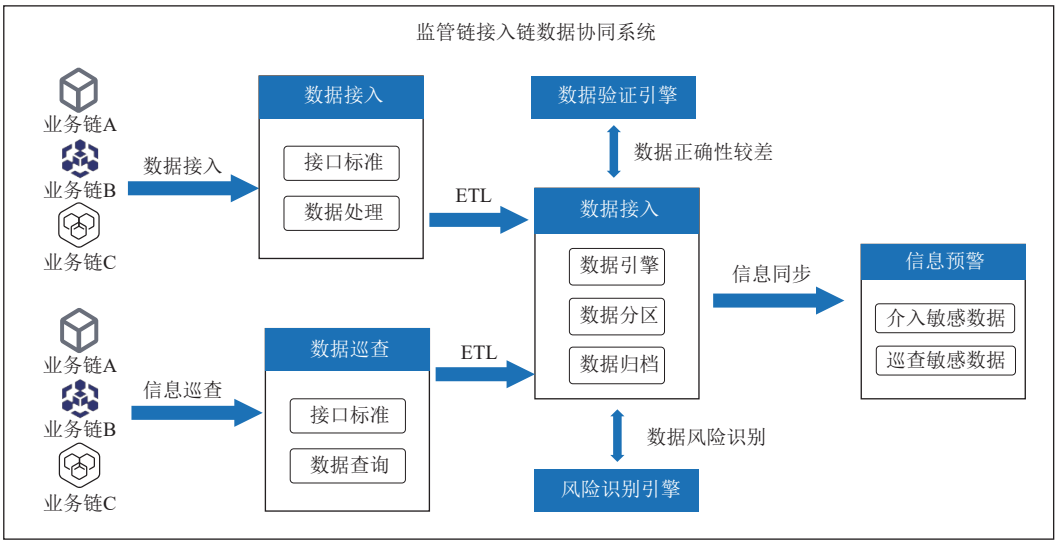

Fig. 19 Relationship diagram of system modules

图 19 系统模块关系图

4.3.2 模块业务流程

各模块的主要业务流程为：

1)预接入的业务链向协同系统提供相关注册信息，实现注册身份，获取系统凭证；

2)预接入的业务链根据数据接入接口规范，调用相关接口实现数据的接入功能；

3)系统对接入数据进行巡查，通过页面下发巡查指令请求，巡检程序调用风险识别模块与数据验证模块，对区块链数据风险与数据正确性进行检测并上报发现的问题，同时响应监管系统的核查.

主要业务流程时序如图 20 所示.

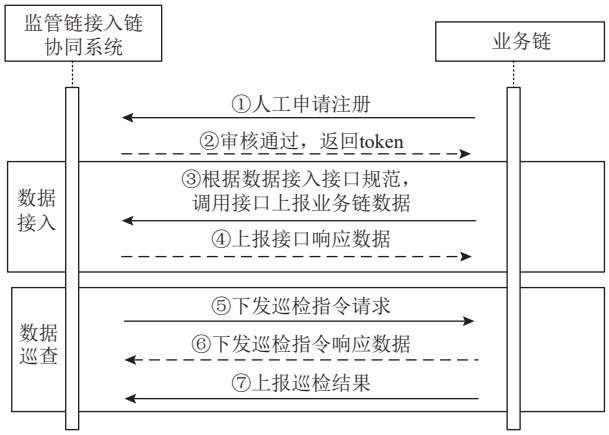

Fig. 20 Main functionality execution sequence

图 20 主要业务流程时序

4.4 整体系统实验性能评价

4.4.1 实验部署物理拓扑

实验的物理拓扑结构如图 21 所示，该物理拓扑已基本可以支撑较大规模的系统实际应用.

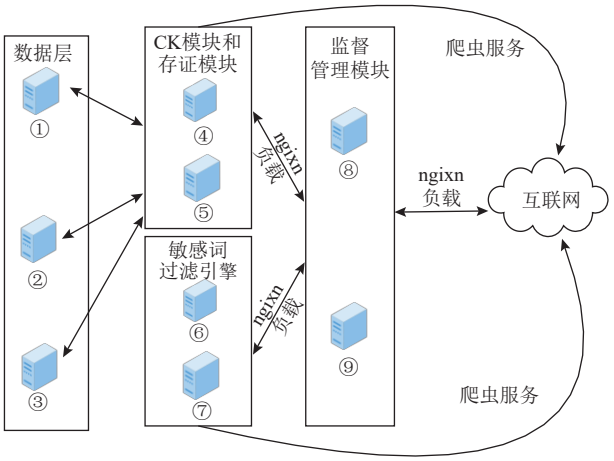

Fig. 21 Deployment of experiment environment

图 21 实验环境部署

4.4.2 系统运行环境配置

系统的实验运行环境如表 4 所示.

4.4.3 性能表现

经实验验证，监管系统的性能表现如表 5 所示.

Table 4 Experimental Runtime Environment

表 4 实验运行环境

序号	设备/软件名称	主要性能指标/软件版本	数量	说明
1	应用服务器	CPU：16 核内存：32 GB 硬盘：：500 GB	9	与实际生产环境 服务器数量配置一致
2	MySQL	8.0	1	主要业务数据库
3	MongoDB	4.4.0	1	次要业务数据库
4	Redis	6.0.6	1	缓存数据库
5	Hyperchain	1.8	1	区块链软件
6	BitXHub	1.6	1	跨链软件
7	JRE	1.8	9	Java 运行环境

Table 5 System Performance

表 5 系统性能表现

功能模块	性能指标
关键词匹配模块	响应时间在毫秒级，吞吐量达到 2 000 TPS 以上架构设计上做到了高可用，可以通过横向拓展提高整体的吞吐能力
监督管理模块	响应时间在毫秒级，跨链监管吞吐量达到 2 000 TPS 以上
业务管控模块	响应时间在 10 s 内，吞吐量达到 500 TPS 以上
监管存证模块	响应时间在毫秒级，吞吐量达到 10 000 TPS 以上，能满足 TB 级别的数据存储规模

可以看到系统的大部分模块的响应时间均在毫秒级，模块的交易吞吐量大部分在 2 000 TPS 以上，已可以满足较高的业务需求. 其中业务管控模块功能不同于存证、转账类简单交易，监管业务通常是复杂的合约交易，因而测量的通量相对较低，但其性能已经足够支撑监管实际业务需求.

4.5 应用示范效果

自 2022 年以来，基于多链协同治理的“以链治链”区块链监管框架构建的区块链应用监管系统已经在浙江省区块链综合监管平台建设和重庆市区块链安全发展监管平台建设中进行了应用试点.

经应用试点验证，系统已经实现了以真假链鉴别、链上信息巡检、内容信息审查、业务安全监管、态势分析预警等为核心的体系化区块链监管能力. 试点工作充分验证了“以链治链”监管框架的创新性和先进性，为浙江省和重庆市乃至全国范围内开展高质量的区块链监管提供了有力的技术支撑，为区块链监管全国一盘棋和持续开展高质量区块链监管工作做出了积极有益的探索.

5 结 语

本文设计了一套多链协同治理的“以链治链”的区块链监管框架，满足了自动化、多中心化、多级多维协同的监管需求. 框架在明确了基本监管架构和基本监管流程的基础上，将区块链监管机制抽象分层，并提炼出一系列监管骨干机制，在保证监管系统有效性和可行性的基础上为实际系统构建提供合理的设计空间. 本文还依据提出的监管框架进行了实际监管系统的设计与实现，并通过应用试点以及实验验证论证了其有效性和可行性. 后续我们会对监管框架进一步创新、对具体监管机制进一步丰富，从而更好地支撑国内区块链生态的健康、良序发展.

作者贡献声明：陈晓丰提出总体思路和撰写论文；宋兆雄负责方案设计和论文撰写；郑佩玉负责系统实验；张珺提出指导意见并修改论文；于智参与论文方案可行性讨论与分析；孙毅审阅修订论文.

参 考 文 献

[1] Yang R, Wakefield R, Lyu S, et al. Public and private blockchain in construction business process and information integration[J]. Automation in Construction, 2020, 118(10): 103276

[2] Dib O, Brousmiche K L, Durand A, et al. Consortium blockchains: Overview, applications and challenges[J]. International Journal on Advances Telecommunications, 2018, 11(1): 51−64

[3] Li Zhetao, Kang Jiawen, Yu Rong, et al. Consortium blockchain for secure energy trading in industrial internet of things[J]. IEEE Transactions on Industrial Informatics, 2017, 14(8): 3690−3700

[4] Pahlajani S, Kshirsagar A, Pachghare V. Survey on private blockchain consensus algorithms[C]//Proc of the 1st Int Conf on Innovations in Information and Communication Technology (ICIICT). Piscataway, NJ: IEEE, 2019: 1−6

[5] Liu Zhuotao, Xiang Yangxi, Shi Jian, et al. Make web3. 0 connected[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 19(5): 2965−2981

[6] Wei Kai, Chen Feng, Zhang Yuming, et al. Trusted blockchain: Capability requirements and evaluation guidelines of public permissioned blockchain[EB/OL]. [2023-03-30]. http://117.50.162.194/#/result/result/resultDetail/02d96be84772409fa49d7e4128ae80d5/1

[7] Wang Yu, Gou Gaopeng, Liu Chang, et al. Survey of security supervision on blockchain from the perspective of technology[J]. Journal of Information Security and Applications, 2021, 60: 102859

[8] Daugherty T, Eastin M S, Bright L. Exploring consumer motivations for creating user-generated content[J]. Journal of Interactive Advertising, 2008, 8(2): 16−25

[9] Lin Yijing, Du Hongyang, Niyato D, et al. Blockchain-aided secure semantic communication for AI-generated content in metaverse[J]. IEEE Open Journal of the Computer Society, 2023, 4: 72−83

[10] Zhao Lei. The typification of blockchain and its legal regulation[J]. Studies in Law and Business, 2020, 37(4): 46−58(in Chinese)
(赵磊. 区块链类型化的法理解读与规制思路[J]. 法商研究, 2020, 37(4): 46−58)

[11] Hone Xuehai, Wang Yang, Liao Fangyu. Review on the technology research of blockchain security supervision[J]. Bulletin of National Natural Science Foundation of China, 2020, 34(1): 18−24 (in Chinese)
(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)

[12] Ma Tianjun, Xu Haixia, Li Peili. A blockchain traceable scheme with oversight function[C] //Proc of the 22nd Int Conf on Information and Communications Security (ICICS). Berlin: Springer, 2020: 164−182

[13] Shao Wei, Jia Chunfu, Xu Yunkai, et al. Attrichain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain[J]. Computers & Security, 2020, 99: 102069

[14] Song Jingwen, Zhang Dawei, Han Xu, et al. Supervised identity privacy protection scheme in blockchain[J]. Journal of Software,

2023, 34(7): 3292−3312 (in Chinese)
(宋靖文, 张大伟, 韩旭, 等. 区块链中可监管的身份隐私保护方案[J]. 软件学报, 2023, 34(7): 3292−3312)

[15] Li Xianbin, Xu Yujie, Wu Xiangyi, et al. A preliminary study of embedded supervision thoughts based on blockchain technology[J]. Finance & Economics, 2022, 10: 45−59 (in Chinese)
(李贤彬, 许余洁, 吴相宜, 等. 基于区块链技术的嵌入式监管创新研究[J]. 财经科学, 2022, 10: 45−59)

[16] Mei Ao, Li Haiyan. Dilemma and solution of cross-border e-commerce supervision[J]. Enterprise Economy, 2022, 41(2): 132−139 (in Chinese)
(梅傲, 李海燕. 跨境电商监管的困境及求解——以区块链技术的应用为视角[J]. 企业经济, 2022, 41(2): 132−139)

[17] Fang Min, Zhang Hua. Technology embedding, information dilemma digestion and blockchain supervision: A case oftraceability system of aquatic products in Guangzhou[J]. Journal of Guangzhou University: Social Science Edition, 2022, 21(2): 115−125 (in Chinese)
(方敏, 张华. 技术嵌入、信息困境消解与区块链监管赋能——以广州水产品溯源平台为例[J]. 广州大学学报: 社会科学版, 2022, 21(2): 115−125)

[18] Wen Baodong, Wang Yujue, Ding Ying, et al. A privacy-preserving blockchain supervision framework in the multiparty setting[J]. Wireless Communications and Mobile Computing, 2021, 2021: 1-9

[19] Zhu Wanjing. Collaborative polycentric governance based on blockchain technology: Technology-enabled institutional operation-alization[J]. E-Government, 2021, 2021(5): 58−70 (in Chinese)
(朱婉菁. 基于区块链技术的多中心协同治理: 技术促生的制度可操作化[J]. 电子政务, 2021, 2021(5): 58−70)

[20] Song Jundian, Dai Bingrong, Jiang Liwen, et al. Data governance collaborative method based on blockchain[J]. Journal of Computer Applications, 2018, 38(9): 2500−2506 (in Chinese)
(宋俊典, 戴炳荣, 蒋丽雯, 等. 基于区块链的数据治理协同方法[J]. 计算机应用, 2018, 38(9): 2500−2506)

[21] Pelt R, Jansen S, Baars D, et al. Defining blockchain governance: A framework for analysis and comparison[J]. Information Systems Management, 2021, 38(1): 21−41

[22] Beck R, Müller-Bloch C, King J L. Governance in the blockchain economy: A framework and research agenda[J]. Journal of the Association for Information Systems, 2018, 19(10): 1

[23] DiRose S, Mansouri M. Comparison and analysis of governance mechanisms employed by blockchain-based distributed autonomous organizations[C]//Proc of the 13th Annual Conf on System of Systems Engineering (SoSE). Piscataway, NJ: IEEE, 2018: 195−202

[24] Fritsch R, Müller M, Wattenhofer R. Analyzing voting power in decentralized governance: Who controls DAOs[J]. arXiv preprint, arXiv: 2204.01176, 2022

[25] Kwon J. High-level overview | cosmos SDK[EB/OL]. [2023-03-30]. https://docs.cosmos.network/main/intro/overview

[26] Kwon J. What are application specific blockchain[EB/OL]. [2023-03-20].https://docs.cosmos.network/v0.47/intro/why-app-specific

[27] Zarick R, Pellegrino B, Banister C. Layerzero: Trustless omnichain interoperability protocol[J]. arXiv preprint, arXiv: 2110.13871, 2021

[28] Sporny M, Longley D, Sabadello M, et al. Decentralized identifiers (DIDs) v1.0 core architecture, data model, and representations [EB/OL]. [2023-03-22].https://www.w3.org/TR/did-core/

Chen Xiaofeng, born in 1985. PhD candidate, professor of engineering. Member of CCF. His main research interests include blockchain and DLT, metaverse, Web3.0, and digital technologies and standardization.

陈晓丰, 1985 年生. 博士研究生, 正高级工程师. CCF 会员. 主要研究方向为区块链和分布式账本技术、元宇宙、Web3.0、数字技术与标准化.

Song Zhaoxiong, born in 1993. Master, engineer. Member of CCF. His main research interests include blockchain technology and distributed system.

宋兆雄, 1993 年生. 硕士, 工程师. CCF 会员. 主要研究方向为区块链、分布式系统.

Zheng Peiyu, born in 1995. Master, senior engineer. Member of CCF. Her main research interest includes blockchain and its standardization.

郑佩玉, 1995 年生. 硕士, 高级工程师. CCF 会员. 主要研究方向为区块链技术及其标准化.

Zhang Jun, born in 1975. PhD, associate professor, Senior member of CCF. Her main research interests include blockchain, and future Internet and network security.

张　珺, 1975 年生. 博士, 副教授. CCF 高级会员. 主要研究方向为区块链、下一代互联网与信息安全.

Yu Zhi, born in 1988. Professor, PhD supervisor. His main research interests include AI, blockchain architecture optimization, accessibility.

于　智, 1988 年生. 研究员, 博士生导师. 主要研究方向为人工智能、区块链体系优化和信息无障碍.

Sun Yi, born in 1979. PhD, professor, PhD supervisor. Distinguished member of CCF. His main research interests include blockchain, distributed system, and network architecture.

孙　毅, 1979 年生. 博士, 研究员, 博士生导师, CCF 杰出会员. 主要研究方向为区块链、分布式系统、网络体系结构.