项目编号：2020YFB1005500 密级：公开

**国家重点研发计划项目** 2021 **年度**

**课题技术进展报告**

课题名称： “以链治链”监管结构与安全模型

项目名称： “以链治链”的监管架构与关键技术研究

所属专项： 云计算和大数据

项目管理专业机构： 科学技术部高技术研究发展中心

执行期限：  2020年11月 至 2023年 10月

2021年10月18日

[科技报告编号] 公开范围[延迟期限]

科 技 报 告

报 告 名 称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

支 持 渠 道：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

编 制 单 位：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

编 制 时 间：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

编写说明

一、课题负责人负责组织研究人员编写科技报告，并按相关计划管理的要求审核和提交。

二、科技报告一般包括封面、基本信息表、目录、插图清单、附表清单、正文、附录和参考文献等部分。

三、报告内容应客观真实、准确完整、层次清晰。本领域的专业读者依据这些描述能重复调查研究过程、评议研究结果。

科技报告基本信息表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1.报告名称 | | 中文（不超过40字）：“以链治链”监管结构与安全模型课题年度报告（2021年） | | | | | | |
| 英文：Annual Technology Report on “Govern the chain by chain” Regulatory Structure and Security Model（2021） | | | | | | |
| 2.报告作者及单位 | | 中文：  王良民，东南大学网络空间安全学院  许昱玮，东南大学网络空间安全学院  陈锦富，江苏大学计算机科学与通信工程学院  朱会娟，江苏大学计算机科学与通信工程学院  余春堂，江苏大学计算机科学与通信工程学院 | | | | | | |
| 英文：  Liangmin WANG, School of Cyber Science and Engineering, Southeast University  Yuwei XU, School of Cyber Science and Engineering, Southeast University  Jinfu CHEN, School of Computer Science and Communication Engineering, Jiangsu University  Huijuan ZHU, School of Computer Science and Communication Engineering, Jiangsu University  Chuntang YU, School of Computer Science and Communication Engineering, Jiangsu University | | | | | | |
| 3.使用范围（公开和延期公开，延期公开需明确延期时间）  延期两年公开  原因：内容涉及正在申请的专利和正在评阅中的论文 | | | | | | 4.编制时间（YYYY-MM-DD）  2021-10-18 | | |
| 5.报告编号（单位机构代码+课题编号+/顺序号，XXXXXXXXX -- NNNNUUNNNNNN/NN）  12100000466006770Q--2020YFB1005501/顺序号 | | | | | | | | |
| 6.备注（须注明的特殊事项，如延期公开报告的查询权限、免责声明、报告与其它工作或成果的联系等）  延期两年公开 | | | | | | | | |
| 7. 摘 要 | 中文（600字左右）：  本年度，课题的研究内容主要包括以下四个方面。   1. 基于链上节点代理的跨链监管方案：针对异构环境下“以链治链”的监管需求，我们设计了一种基于链上节点代理的跨链方案。以当前跨链技术中的公证人机制为基础，通过在链上节点设置代理程序构建监管端与业务端之间的分布式网络，通过基于多代理节点的数据巡查与共识机制打破中心化跨链监管的制约，保障跨链监管的安全性。 2. 基于共享节点的跨链监管方案：针对同构链环境下“以链治链”的监管需求，我们提出了一种基于共享节点的跨链数据监管方案。在超级账本网络中为监管链与业务链建立不同的通道与区块链账本，通过两者之间的共享节点实现监管链对业务链的接入，通过链码调用实现监管链对业务链的数据巡查与交易监管。 3. 基于多注意力机制和自适应学习的智能合约漏洞检测方法：我们提出一种基于多注意力机制和自适应学习的智能合约漏洞检测方法，本方法从加速模型训练和降低漏报率两个角度切入，兼具高效率和低漏报率的功能。 4. 区块链平台的安全测评方法：我们提出了一种区块链平台的脆弱性模型构建方法，并提出一种基于脆弱性模型的形式化验证方法，以此构建区块链平台的安全测试框架。基于蜕变测试理论完成测试用例的生成与蜕变关系的构造，并最终生成测试用例集。利用安全测试框架形式化的输出结果对区块链平台的安全级别进行评价。 | | | | | | | |
| 英文（不超过2500个字符）：  In the past year, our research work mainly involved the following four aspects.   1. Cross-chain supervision scheme based on on-chain node agents: We propose a cross-chain supervision scheme based on-chain node agents to meet the supervision demand of "Govern the chain by chain" in heterogeneous environments. Based on the notary mechanism, which is used in the current cross-chain techniques, the distributed network between the supervision side end and the business end is built by setting proxy programs in the on-chain nodes. Furthermore, based on multi-agent nodes data inspection and consensus mechanism, our scheme can break the constraints of centralized cross-chain supervision and safeguard the security of cross-chain supervision. 2. Cross-chain supervision scheme based on shared node: We propose a cross-chain supervision scheme based on shared node to meet the supervision demand of "Govern the chain by chain" in homogeneous environments. We build different channels, i.e. blockchain ledgers, for supervision chain and business chain via Hyperledger Fabric. Moreover, we realize the access of supervision chain to business chain through shared nodes between them and the data inspection and transaction monitoring of supervision chain to business chain through running chaincode. 3. Smart contract vulnerability detection method based on multi-attention mechanism and adaptive learning: We propose a smart contract vulnerability detection method based on multi-attention mechanism and adaptive learning. We design this method from two perspectives of accelerating model training and reducing false negative rate (FNR), and it is a combination of high efficiency and low FNR. 4. Security evaluation framework of blockchain platform: We propose a vulnerability model construction method for blockchain platform as well as a formal verification method based on vulnerability models and use it to build a security evaluation framework for blockchain platforms. We then complete the generation of test cases and the construction of metamorphic relationships based on metamorphic testing methodology and finally generate the test case set. In the end, we can use the formalized output of the security evaluation framework to evaluate a blockchain platform's security level. | | | | | | | |
| 8. 关 键 词 | 中文（3-8个，以分号隔开）：“以链治链”；跨链监管架构；跨链安全通信；智能合约自动化监管；区块链平台安全测评；区块链 | | | | | | | |
| 英文（3-8个，以分号隔开）：“Govern the Chain by Chain”; Cross-chain Supervision Structure; Cross-chain Secure Communication; Smart Contract Automated Supervision; Blockchain Platform Security Evaluation; Blockchain | | | | | | | |
| c9.支持渠道 | 项目名称 | | | “以链治链”的监管架构与关键技术研究 | | | | |
| 主管部门 | | | 科学技术部高技术研究发展中心 | | | 计划名称 | 2020国家重点研发计划 |
| 项目编号 | | | 2020YFB1005500 | | | 应用领域 |  |
| 承担单位 | | | 东南大学 | | | | |
| 合作单位（不超过5家） | | | 江苏大学、西安电子科技大学、武汉大学、北京邮电大学、南京航空航天大学 | | | | |
| 总经费（万元） | | | 917.00 | | | 国拨经费（万元） | 917.00 |
| 项目负责人 | | | 王良民 | | | | |
| 起始日期 | | | 2020年11月 | | | 截止日期 | 2023年10月 |
| 10.联系人 | 姓名 | | 王良民 | 单位 | 东南大学 | | | |
| 电话 | | 18262636788 | E-Mail | wanglm.seu@foxmail.com | | | |

**目 录**

[插图清单 II](#_Toc85302465)

[附表清单 III](#_Toc85302466)

[引言 1](#_Toc85302467)

[1 研究概述 3](#_Toc85302468)

**[1.1](#_Toc85302469)** [研究背景及意义 3](#_Toc85302469)

**[1.2](#_Toc85302470)** [课题一与其它课题的关系 3](#_Toc85302470)

**[1.3](#_Toc85302471)** [课题一研究内容 4](#_Toc85302471)

**[1.4](#_Toc85302472)** [研究技术路线 6](#_Toc85302472)

[2 一种基于链上节点代理的跨链方法及系统 8](#_Toc85302473)

**[2.1](#_Toc85302474)** [现有跨链系统系统存在的问题 8](#_Toc85302474)

**[2.2](#_Toc85302475)** [基于链上节点代理的跨链方法及系统详细技术方案 9](#_Toc85302475)

**[2.3](#_Toc85302476)** [本方法的优点 11](#_Toc85302476)

[3 一种基于共享节点的“以链治链”方法及系统 12](#_Toc85302477)

**[3.1](#_Toc85302478)** [现有区块链系统存在的问题 12](#_Toc85302478)

**[3.2](#_Toc85302479)** [基于共享节点的“以链治链”方法及系统详细技术方案 13](#_Toc85302479)

**[3.3](#_Toc85302480)** [本方法的优点 21](#_Toc85302480)

[4 一种基于多注意力机制和自适应学习的智能合约漏洞检测方法及系统 23](#_Toc85302481)

**[4.1](#_Toc85302482)** [现有智能合约漏洞检测方法存在的问题 23](#_Toc85302482)

**[4.2](#_Toc85302483)** [基于多注意力机制和自适应学习的智能合约漏洞检测方法详细技术方案 24](#_Toc85302483)

**[4.3](#_Toc85302484)** [本方法的优点 27](#_Toc85302484)

[5 一种区块链平台的安全测评方法 28](#_Toc85302485)

**[5.1](#_Toc85302486)** [现有区块链平台安全测评方法存在的问题 28](#_Toc85302486)

**[5.2](#_Toc85302487)** [区块链平台的安全测评方法详细技术方案 29](#_Toc85302487)

**[5.3](#_Toc85302488)** [本方法的优点 31](#_Toc85302488)

[结论 33](#_Toc85302489)

# 插图清单

[图1 课题一与其它课题之间的关系 2](#_Toc86265412)

[图 2 “以链治链”监管结构与安全模型的研究内容 4](#_Toc86265413)

[图 3 “以链治链”监管结构与安全模型的技术路线 6](#_Toc86265414)

[图 4 基于链上节点代理的跨链方案 8](#_Toc86265415)

[图 5 代理程序工作流程示意图 9](#_Toc86265416)

[图 6 代理程序通信示意图 9](#_Toc86265417)

[图 7 安全机制流程示意图 10](#_Toc86265418)

[图 8 基于共享节点的跨链监管方案总体架构图 12](#_Toc86265419)

[图 9 系统3层结构图 14](#_Toc86265420)

[图 10 交易数据流图 15](#_Toc86265421)

[图 15 区块链平台的安全测评总体框架 23](#_Toc86265422)

[图 16 基于脆弱性模型的区块链平台安全测试 24](#_Toc86265423)

[图 17 基于蜕变测试的区块链平台安全测试 25](#_Toc86265424)

[图 18 区块链平台安全等级评价 25](#_Toc86265425)

# 附表清单

[表 1 主流跨链技术对比](#_Toc1288575689)

# 引言

课题一总的研究目标是提出区块链“以链治链”中用户对等交互的跨链安全模型和“以链治链”区块链系统的安全测评模型。具体包括：采用区块链技术构建监管链，研究监管链的分布式监管体系；提出跨链监管的安全需求分析和安全机制；提出自动化分布式智能合约及其异常行为监管框架和原型验证系统；研究出一套适用于区块链平台的脆弱性模型，形成适用于区块链平台中对未知的漏洞利用蜕变测试进行安全性测试的新方法及面向区块链平台的安全等级评价体系。

本年度，课题的研究内容主要包括以下四个方面。

1. 基于链上节点代理的跨链监管方案：针对异构环境下“以链治链”的监管需求，我们设计了一种基于链上节点代理的跨链方案。以当前跨链技术中的公证人机制为基础，通过在链上节点设置代理程序构建监管端与业务端之间的分布式网络，通过基于多代理节点的数据巡查与共识机制打破中心化跨链监管的制约，保障跨链监管的安全性。
2. 基于共享节点的跨链监管方案：针对同构链环境下“以链治链”的监管需求，我们提出了一种基于共享节点的跨链数据监管方案。在超级账本网络中为监管链与业务链建立不同的通道与区块链账本，通过两者之间的共享节点实现监管链对业务链的接入，通过链码调用实现监管链对业务链的数据巡查与交易监管。
3. 基于多注意力机制和自适应学习的智能合约漏洞检测方法：我们提出一种基于多注意力机制和自适应学习的智能合约漏洞检测方法，本方法从加速模型训练和降低漏报率两个角度切入，兼具高效率和低漏报率的功能。
4. 区块链平台的安全测评方法：我们提出了一种区块链平台的脆弱性模型构建方法，并提出一种基于脆弱性模型的形式化验证方法，以此构建区块链平台的安全测试框架。基于蜕变测试理论完成测试用例的生成与蜕变关系的构造，并最终生成测试用例集。利用安全测试框架形式化的输出结果对区块链平台的安全级别进行评价。

# 研究概述

## 研究背景及意义

习近平总书记强调要把区块链作为核心技术自主创新的重要突破口，加快推动区块链技术和产业创新发展，从国家战略上推动了区块链应用和研究的迅速发展，同时也带动了解决区块链监管问题成为行业发展的迫切需要。但由于区块链监管研究缺乏统一的项目组织，亟需具有系统性和通用性的自动化“以链治链”技术，以满足区块链监管中的多样化、动态性需求，为区块链蓬勃发展提供保障。

## 课题一与其它课题的关系

针对指南的研究内容，围绕本项目所提出的研究内容，设置4个课题，课题研究内容及其关系如图1所示。各课题之间既紧密耦合，又有创新特色，能够在保持各课题独立性的同时，共同推进项目的进展。

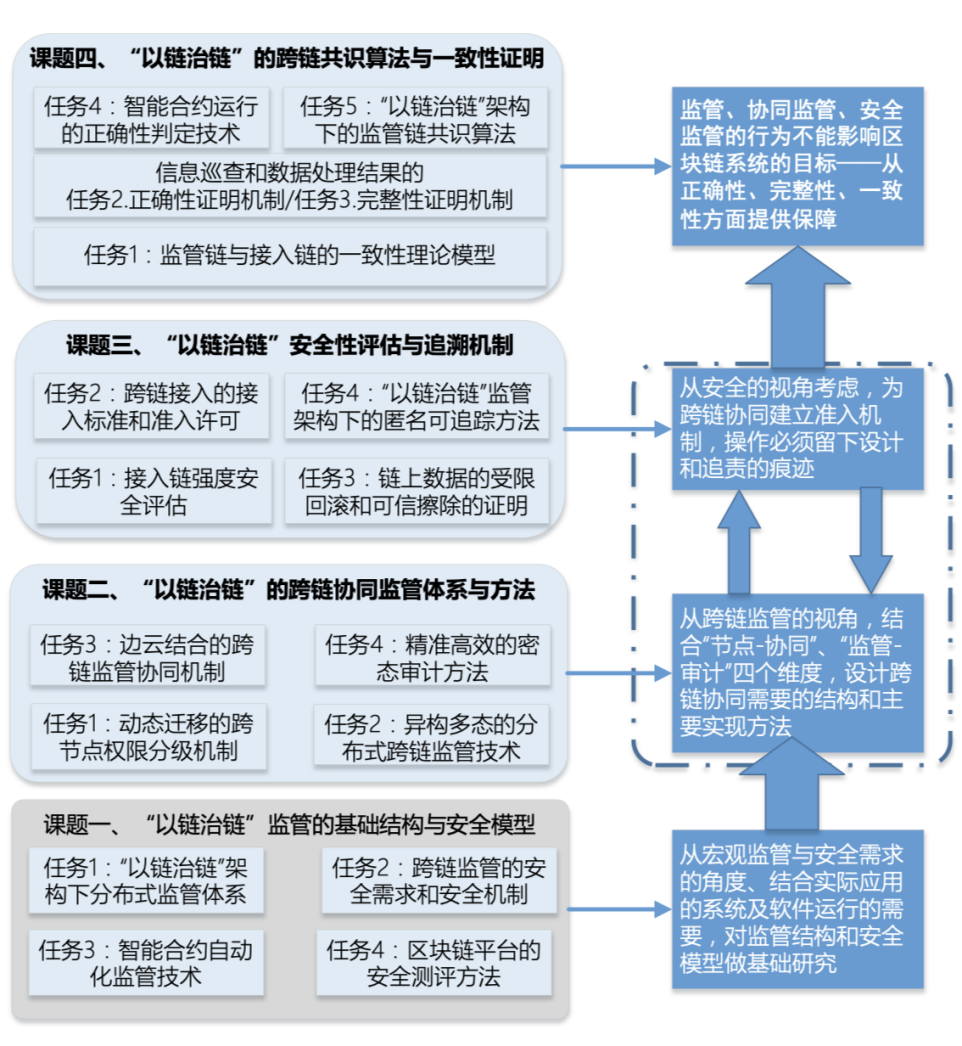


图1 课题一与其它课题之间的关系

课题一从全局的宏观视角，考虑以链治链的区块链监管架构、模型、软件与系统的监管及安全测评；课题二和课题三在课题一提出的基础架构和模型之上，考虑跨链的交互机制与跨链交互的安全，具体说是课题二在课题一结构下考虑如何实现监管链和接入链的交互，考虑监管功能的实现；而课题三考虑该架构和交互模式下，如何维护系统的安全，如何做到责任可追溯的证据提供，考虑监管行为自身的安全性；课题四在课题一、二、三所定义的宏观结构、执行机制和安全要求之下，如何实现跨链的区块链业务不受影响，即如何达成共识，如何保证数据业务执行的一致性、完整性和正确性。

## 课题一研究内容

### 拟解决的关键科学与技术问题

1. 监管需求与区块链用户的对等性需求之间的矛盾问题

区块链系统能够赋予所有用户节点以公平对等的方式参与系统行为中。这是区块链获得用户认可、吸引用户加入的关键特点。但是区块链系统若鲁莽地引入监管角色，将会引起用户节点对区块链系统的抵制。本课题为调和监管需求与区块链用户的对等性需求之间的矛盾，提出区块链“以链治链”中用户对等交互的跨链安全模型，为自动化监管构建可信运行机制提供基础理论与基本机理。

1. 区块链系统物理结构上的分布式特性与软件功能上内聚特性之间的矛盾问题

接入链的分布式部署与软件功能的内聚性之间的矛盾使得现有的安全测评模型不适用，如何设计一种支持“以链治链监管模式”的安全模型，是本课题要解决的关键技术之一。为此，本课题从当前安全测评领域“分布式-功能松耦合”和“集中式-功能内聚”两类固有模式中，拓展出新的研究领域与研究方法，提出“以链治链”区块链系统的安全测评模型。

### 拟开展的主要研究内容

本课题计划开展以下4方面的研究，主要内容如图2所示。

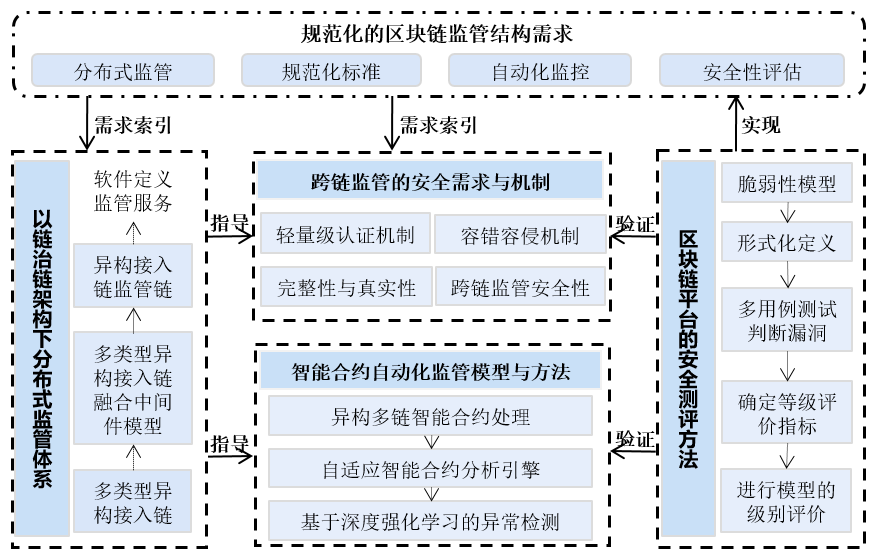


图 2 “以链治链”监管结构与安全模型的研究内容

1. “以链治链”架构下分布式监管体系

分布式监管体系需求包括异构链的接入技术、监管链与接入链之间的跨链通信机制、面向异构接入链的中间件融合技术、跨链监管的性能分析与优化技术。针对上述安全需求，采用区块链技术构建“以链治链”的新型监管架构，并在此架构下提出一种新型的监管链共识算法，基于新型监管架构设计并实现分布式监管体系和框架，同时对跨链监管进行形式化建模和仿真建模以实现对跨链监管的性能优化。

1. 跨链监管的安全需求和安全机制

当前区块链服务与应用存在数据传输安全、跨链协同安全、隐私信息保护、容错容侵等一系列问题，而传统的密码学安全机制无法完美解决，故将密码学机制和非密码学机制相结合，研究跨链监管的安全体系架构。在接入环节，实现对接入链的认证和节点身份追踪；在跨链交互环节，保证数据的机密性、完整性和真实性，并克服恶意节点的干扰；在数据使用环节，实现各种数据的私密性、容错容侵等监管技术。

1. 智能合约自动化监管技术

针对不同区块链平台上的智能合约设计机制、实现方式、源码公开率等参差不齐导致传统手工和半自动化智能合约监管机制难以监管跨平台异构智能合约的问题，同时考虑智能合约数量的爆发式增长带来的数据存储和计算压力的挑战，拟综合自然语言处理、数据挖掘与分析、深度学习、强化学习等技术，构建独立于区块链平台的通用智能合约分析引擎，构造完备、规范、通用的形式化表征方法，以完善深度强化学习检测模型的输入。

1. 区块链平台的安全测评方法

针对“以链治链”监管安全模型，研究一种基于脆弱性模型的区块链平台安全测评方法。首先研究一种有效的面向区块链平台的脆弱性模型构建方法；然后，生成区块链平台安全测试框架；在上述测试框架的基础上，进一步研究基于蜕变测试的区块链平台安全测试方法，并对得到的蜕变关系进行理论验证，以解决测试预期结果不确定问题（oracle 问题）；最后，建立新型面向区块链平台的安全等级评价体系并实现测评。

## 研究技术路线

本课题拟在“以链治链”的监管架构下解决监管需求与区块链用户对等性需求之间存在矛盾的问题，以及区块链系统在物理结构上的分布式特性与软件功能上的内聚性特性之间存在矛盾的问题。技术路线如图3所示，拟在设计与实现“以链治链”的分布式监管体系的基础上实现2方面的技术突破。具体采用的方法、原理、机理、算法以及模型介绍如下：

1. 针对监管需求与区块链用户的对等性需求之间存在矛盾的问题，本课题拟采用分层分治策略，将中间件理论模型与实现技术融入到异构链接入监管链的过程中，实现两者共存的“以链治链”分布式监管体系；拟在“以链治链”的监管体系中提出保留用户对等交互的跨链安全模型，结合密码学与非密码学技术设计覆盖跨链监管全周期的安全模型与机制，实现对接入、跨链交互、数据使用环节的安全保障；拟整合自适应智能合约分析引擎与智能合约异常检测模型，设计自动化分布式智能合约的监管框架与方法，实现一个可迭代优化和自生长的监管模型，从而构建一个全方位的监管体系。
2. 针对区块链系统在物理结构上的分布式特性与软件功能上的内聚性特性之间的矛盾问题，本课题拟提出基于软件脆弱性模型的区块链平台安全测评方法，实现覆盖网络协议、智能合约、分布式账本、共识机制等功能模块的全面安全性测试，从软件的角度完成对整个区块链平台的功能内聚性测试；拟采用形式化单子符号系统实现对安全测试框架的形式化建模，进而基于蜕变测试的理论与技术研究基于形式化安全测试框架的测试用例生成方法与蜕变关系构造方法，找到具有较高使用效率的测试用例集和正确的蜕变关系，检测区块链平台的安全漏洞，从理论角度实现区块链节点分布性测试。

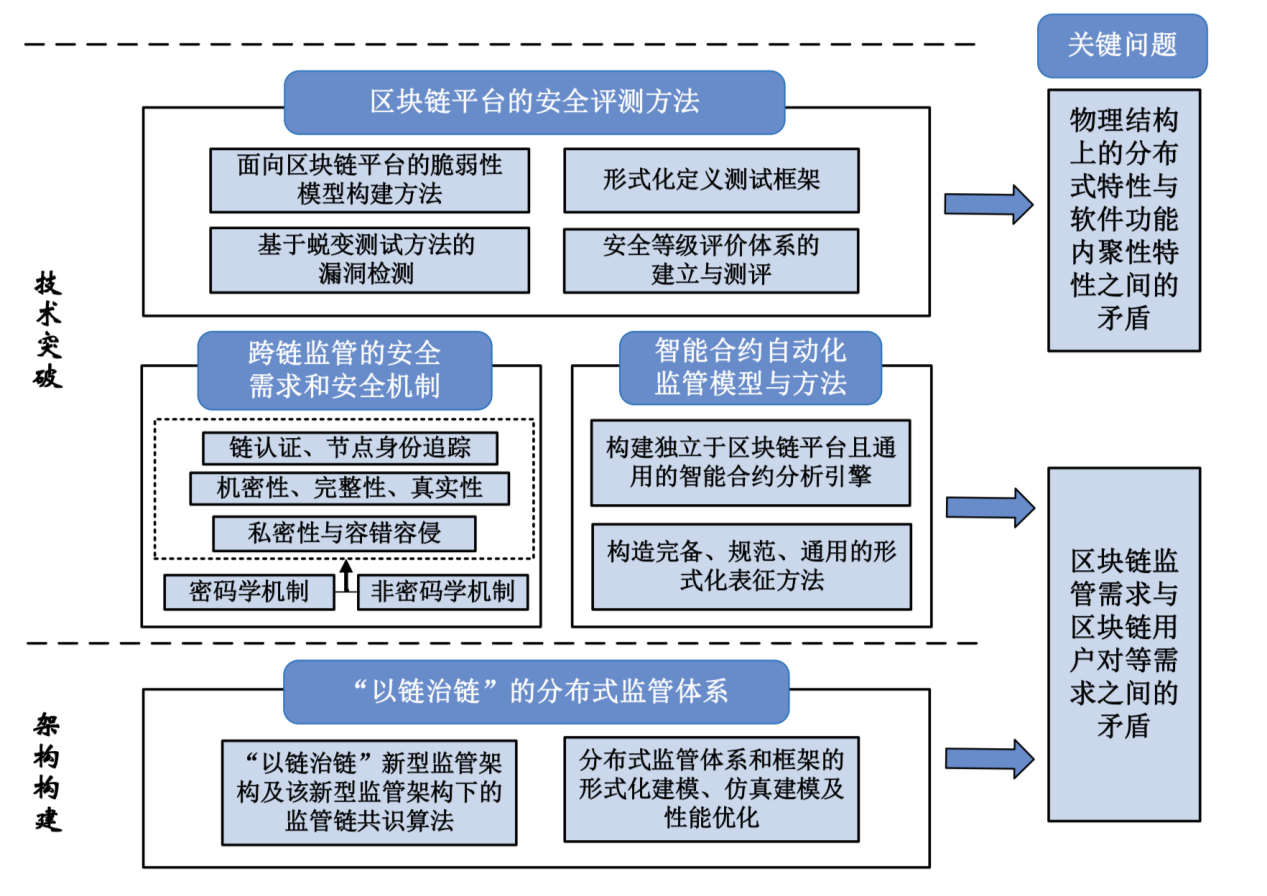


图 3 “以链治链”监管结构与安全模型的技术路线

# 一种基于链上节点代理的跨链方法及系统

## 现有跨链系统系统存在的问题

区块链因其具有去中心化、不可篡改、全程留痕、可追溯、 集体维护、公开透明等优点，自诞生以后便被认为是解决互联网信任与价值可靠转移难题的有效手段，在数字货币、交易结算、数字政务、存证防伪数据服务等领域具有广阔前景。近年来，国家已经把区块链作为核心技术自主创新的重要突破口，从国家战略上推动了区块链应用和研究的迅速发展，同时也促使解决区块链监管问题成为了行业发展的迫切需要。

目前在区块链监管方面使用的是传统的中心化监管模式。由于区块链自身的特性，中心化监管模式存在三个问题，“管不了”、“管不住”和“管不得”。“管不了”，即由于区块链的匿名性的特点，使得监管机构很难实现有效监管。“管不住”即目前大量不同类型的区块链项目大量共存，中心化的监管模式很难实现对异构区块链的大规模监管。“管不得”，由于监管的集中式管理需求与区块链应用中用户和业务的分布式需求存在矛盾，企业组织或个人用户可能会技术性对抗集中监管。

由于中心化监管模式的局限性，“以链治链”分布式区块链监管模式成为了区块链监管的主要发展方向。分布式监管模式避免了监管机制过度中心化的问题，可以在保护用户隐私的前提下，实现有效监管，很好的解决了监管需求与区块链用户的对等性需求之间存在矛盾的问题。在“以链治链”区块链监管模式下，各种异构链可借助跨链技术接入监管链，从而实现对异构区块链的大规模监管。

目前主流跨链技术主要有公证人机制、哈希锁定机制、中继/侧链机制和分布式密钥控制机制。每种跨链技术都有不同的实现原理和各自的优缺点。

表 1 主流跨链技术对比

|  |  |  |
| --- | --- | --- |
| 跨链机制 | 优点 | 缺点 |
| 公证人机制 | 简单易实施 | 中心化 |
| 哈希锁定机制 | 去中心化、原子性 | 仅支持资产交换 |
| 中继/侧链机制 | 去中心化 | 实现难度大 |
| 分布式密钥控制机制 | 去中心化 | 实现难度大 |

当前基于四种跨链技术已衍生出了多种不同的跨链方案及项目，其中最有名的即为Cosmos和Polkadot。Cosmos和Polkadot均采用中继链实现跨链，但二者均主要服务于资产的跨链交换和转移。对于数据跨链传输，二者的设计过于臃肿，且不能不能满足该场景对数据跨链的原子性、安全性、高效性和通用性的需求。同样其他大部分方案也都不能直接应用于“以链治链”区块链监管场景。就安全性为例，在“以链治链”区块链监管场景，跨链方案必须保证跨链数据获取时的真实性、跨链数据传输时的隐私性和跨链数据提交时的准确性，而目前很少有跨链方案可以做到同时保证三个阶段的跨链安全性。

## 基于链上节点代理的跨链方法及系统详细技术方案

本方案旨在，在“以链治链”区块链监管场景下，实现区块链之间的数据跨链传输。在该方案中每个区块链节点都会运行一个代理程序，所有代理程序组成一个P2P网络，代理程序具有操作区块链以及与其他代理程序通信的功能。



图 4 基于链上节点代理的跨链方案

基于链上节点代理的跨链方案的整体架构如图4所示，本方案将由3个模块和3个机制构成。3个模块分别为监管模块、业务模块和跨链服务器模块。3个机制为权限控制机制、跨链通信机制和跨链安全机制。

监管模块与业务模块主要由监管链、业务链及每个节点对应的代理程序组成。代理程序需要实现两个功能，第一个功能是通信功能，第二个功能是区块链操作功能。在实际运行中时，为了分别实现两个功能，代理程序将同时运行两个线程，分别是通信线程和业务线程。在业务线程中，代理程序将借助各个区块链项目的SDK，实现区块链的读写操作的功能。为了实现对区块链的操作，一般还需在区块链上部署与跨链业务相关的智能合约，该智能合约将充当区块链对外数据交互的接口，其至少具备区块链数据读取和存储两个基本功能。在通信线程中，因为区块链本身不具备与外界通信的功能，所以区块链将借助代理程序来实现通信功能。



图 5 代理程序工作流程示意图

跨链通信机制其主要目的是实现监管链与业务链之间的跨链数据传输功能，是监管模块与业务模块之间实现跨链通信的技术支持。为了实现数据的跨链传输，在本方案中跨链通信机制将构建一个跨链P2P网络，位于不同区块链的节点将借助代理程序通过跨链P2P网络实现数据跨链传输。



图 6 代理程序通信示意图

跨链安全机制的目的是保证跨链数据的正确性、隐私性和完整性，它是跨链通信与区块链的安全保证。整个跨链过程可以分为三个阶段跨链数据获取阶段、跨链数据传输阶段和跨链数据提交阶段。跨链安全机制将利用共识机制和密码学技术，保证跨链数据的真实性、准确性和隐私性，从而抵御跨链三个阶段中可能面临的安全风险与挑战。



图 7 安全机制流程示意图

权限控制机制的目的是借助数字证书技术实现跨链系统的访问与接入控制，它主要在跨链服务器模块中通过密码学技术进行实现。

## 本方法的优点

基于链上节点代理的跨链方案是一种基于公证人机制的改进方案，本方案所设计的跨链通信机制、跨链安全机制和权限控制机制。在跨链通信机制中，不同节点借助其对应的代理程序实现数据的跨链传输，用分布式的代理程序取代了中心化的数据转发的公证人，解决传统公证人机制带来的中心化问题。在跨链安全机制中，本方案分别就跨链的三个阶段可能面临的安全风险与挑战给出了解决方案，很好的保证了跨链书的真实性、准确性和隐私性。在权限控制机制中，本方案借助数字证书技术，实现跨链系统的访问与接入控制，满足了相应的业务需求，保证了系统的安全性。

# 一种基于共享节点的“以链治链”方法及系统

## 现有区块链系统存在的问题

目前，区块链凭借着“去中心化”、“不可篡改”、“可供追溯”等特性已经应用到了数字货币、供应链、政府审计等各个领域。而如何解决区块链技术的引入所产生的一系列安全威胁和安全问题就成为一个亟待解决的课题，其中最有效的解决方案是对区块链系统进行监管以及巡查等，这样能最大程度的保证区块链系统数据免遭安全攻击。但是，在经典的监管场景中，监管者一直都是以中心化的权威角色出现，通过其角色特权对整个业务进行监管治理，然而这样的监管方式并不适用于区块链场景，这种中心化监管会严重破化区块链自身去中心化、自治化的特性。面对严峻的区块链安全监管形势，我们既需要保护好区块链自身的特性，与此同时还需要对区块链进行可控的监管，也就是说，我们需要解决好监管需求与区块链用户的对等性需求之间的矛盾问题。

就区块链的监管问题，Lu QingHua等[3]曾提出了一种系统OriginChina，它可以生成代表法律协议的智能合约。该系统使用智能合约进行区块链交易的监督检查，只限于单链上的节点交易，对于多链业务以及大规模的业务，该方法不具有普适性。文献[2]提出的一种基于区块链双链结构的可监管数字货币模型就采用了类似的机制，但该方法只适用于数字货币的朔源，但并不涉及其他应用场景下的监管治理操作，这还需要进一步设计相应的基于区块链的监管机制。

根据现有的研究可知，我们也可以通区块链的机制来监管区块链本身的行为，即实现“以链治链”机制。“以链治链”机制需要设计一套合理的数据组织结构、数据溯源流程和监管操作规则等以用来进行区块链的数据监管。

## 基于共享节点的“以链治链”方法及系统详细技术方案

### 系统总体架构与设计思路

本节将介绍基于共享节点跨链监管方案的总体架构和设计思路，并将整个系统分为了事务层、数据传输层以及网络层三层进行简要阐述。

我们实现了一个基于Hyperledger Fabric（超级账本）的“以链治链”区块链监管系统，设计了一个基于共享节点的跨链监管方案，该方案的总体架构如图8所示。

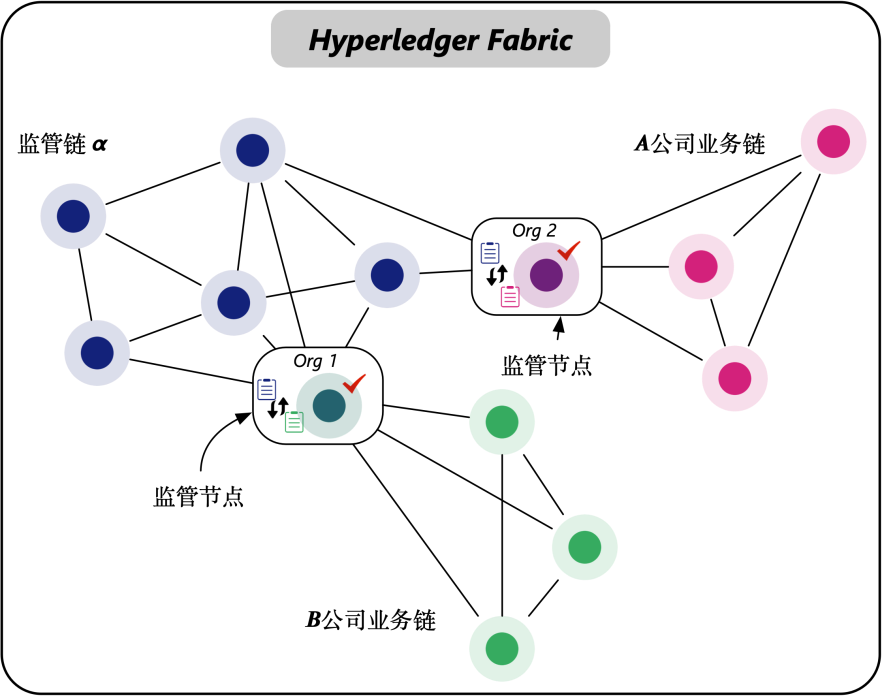


图 8 基于共享节点的跨链监管方案总体架构图

该系统基于Hyperledger Fabric搭建，上层区块链包括了监管链和业务链两种类别，业务链属于普通区块链，只限于完成参与组织所发起的交易提案，实现通过区块链的方式完成各方交易信任度的提升，业务链参与组织可以是多方的，比如某公司内的开发、运营、人事、财务等各部门参与公司的日常经营，为了防止各部门存在欺骗、作恶行为，将各部门数据记录到区块链中，董事会也可以随时通过查询链上的数据了解公司运营情况。但是这样一条公司内部的区块链仍缺乏监管，比如监管公司业务的一些政府部门如何参与到业务链中完成监管。  
 为了解决监管的问题，本系统设计了监管链，监管链由相关监管机构控制，区块链中记录被监管者交易数据的统计信息，这些统计信息可能是监管者感兴趣的重要信息，比如税务监管机构如果作为监管者接入到监管链，那么它可能会提交一个用户链码，收集整理底层业务链中被监管机构的税务状况，根据收集的数据分析判断该公司是否有逃税、漏税等违法行为。由于被监管公司的数据是由底层业务链中直接调用回监管链中的，并且数据的底层传输使用的是gRPC协议，该协议可以保证数据在传输过程中不会受到其他人的篡改，因此数据从底层业务链到上层监管链不会发生任何改变，监管数据的真实性和完整性得到了保障。

该系统架构在业务链与监管链的接口处采用共享节点的方法进行跨链（通道）通信，采取这种方式有以下两个主要原因：

1. 在Hyperledger Fabric网络中，不同通道相当于不同的链，通道之间不能直接进行通信。那么如果两个通道之间存在一个共享节点，那么其通信的复杂度就会大大降低，通信的效率也会增加。
2. 采用这样的设计能保证位于公司业务链的节点能够参与到上层监管链当中来，这对解决中心化监管与去中心化区块链之间的矛盾问题具有非常重要的意义。举例而言，当一个公司选用区块链平台而非传统的中心数据库平台来实现业务数据记录的时候，它最想利用的是区块链的去中心化、不可篡改、匿名性等特点维护整个公司的业务，那么此时如果有一个监管者以中心化的方式对其进行监管，无疑对其使用区块链的初衷是一种损害。因此，这里我们使用共享节点就是为了让受监管者本身参与到监管中来，避免了监管者与被监管者激烈的对立矛盾。这样的共享节点是由业务公司自己部署的既参与底层通道，又参与上层监管通道，他对于上层监管链中的数据有一定享有权，并且也能关注到监管机构对各公司的监管行为，避免出现不公现象。总的来说，共享节点的设计能够完美解决区块链监管矛盾问题。

该系统还考虑了认证服务和排序服务两个模块，排序服务是由Hyperledger Fabric中的Orderer节点提供的，认证服务是由网络中的CA和MSP提供的。那么该系统中的排序节点应当由监管机构统一部署，排序节点是完全可以信任的，不会发生作恶事件，因此排序服务由排序节点提供不会造成安全风险。该系统中各组织包含的角色有：节点、客户、管理员三类，认证服务从Hyperledger Fabric网络本身出发也没有问题，认证服务由监管机构负责提供，这样也可以完全避免认证出现安全问题。

### 系统3层结构设计

该系统从功能实现上又可以将其分为三层：事务层、数据传输层和网络层，每一层都负责不同的功能实现，如图9所示。

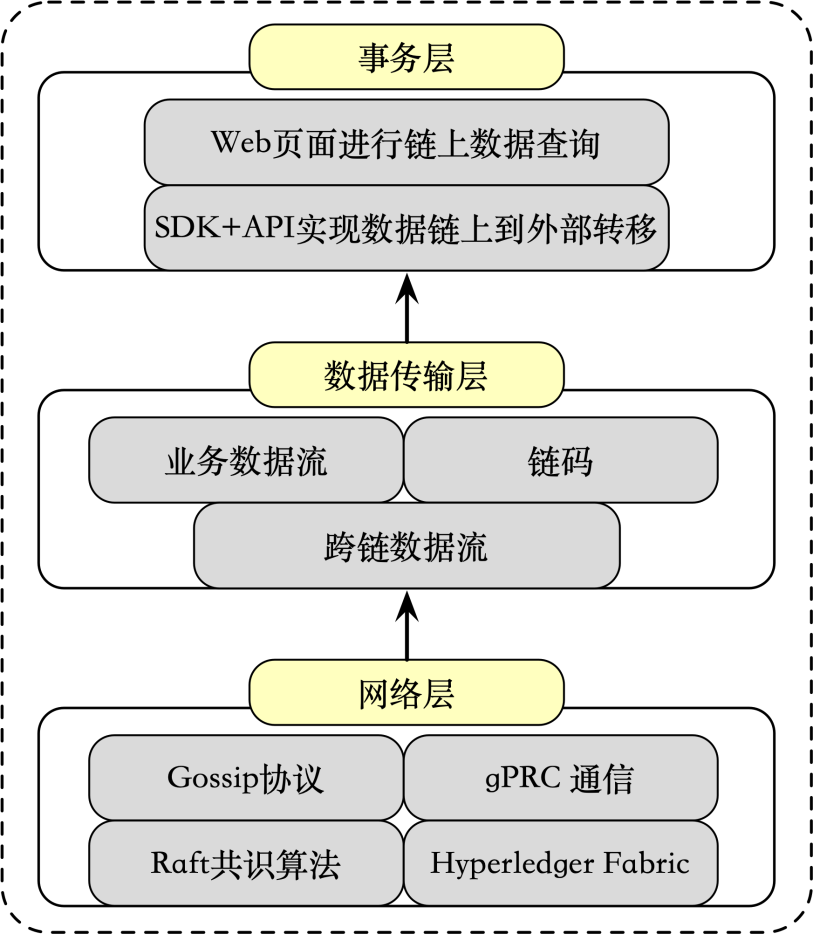


图 9 系统3层结构图

该系统底层为系统网络层，网络层是基于Hyperledger Fabric超级账本网络组建而成的，在其中运用了Gossip协议、gRPC通信协议，以及排序节点内部的Raft共识算法等；系统中间为数据传输层，这一层是实现区块链中的业务数据流以及跨链数据流如何进行转移以及交易功能的；最上层是事务层，事务层通过SDK连接区块链内外的数据，并搭建Web网页在链外进行区块链中数据的查询展示等。

系统的网络层主要负责底层网络基础设施的搭建，主要是基于Hyperledger Fabric原本的网络框架，沿用底层的Gossip协议和gRPC通信协议，在排序节点中使用Raft共识算法保证节点间的共识一致性，并且根据系统架构搭建所需的各组织、节点，配置相应的排序服务和认证服务，加入不同的通道。超级账本网络在组织内部的通信使用Gossip协议。它是一种分布式通信协议，它使用的场景是针对对等节点，当其中一个种子节点有状态需要更新给网络中的其他成员时。而gRPC协议被使用在组织间，以及客户端与节点之间的通信。它是一种高效、开源的RPC框架，RPC即一种远程过程调用协议，它提供了一套可以让应用程序之间可以进行通信的机制，这种机制遵循C-S模型。使用gRPC协议可以让服务接口具有更严格的约束和限制，同时相较于普通的程序调用也具有更好的性能。在超级账本中不同组织间，尤其是排序节点、对等节点和客户端节点通信时，更加符合C/S的通信模型，因此选用gRPC协议更加合理高效。目前超级账本网络中排序节点所支持的共识算法有Solo、Kafka和Raft等。排序节点主要负责网络中交易排序的工作，排序节点可能有多个，那么这些排序节点会接收来自各组织不同节点的交易提案，如何在多个排序节点中达成排序结果的一致就需要排序节点之间的共识算法。

系统的数据传输层主要实现业务链上的数据传递、监管链跨链数据传递以及链码功能。监管链跨链的数据流只需要在业务链的基础上增加共享节点的跨链操作流，链码需要根据链上数据流进行功能设计。图10展示了在本系统业务链中交易数据在系统各节点角色中的流动情况。

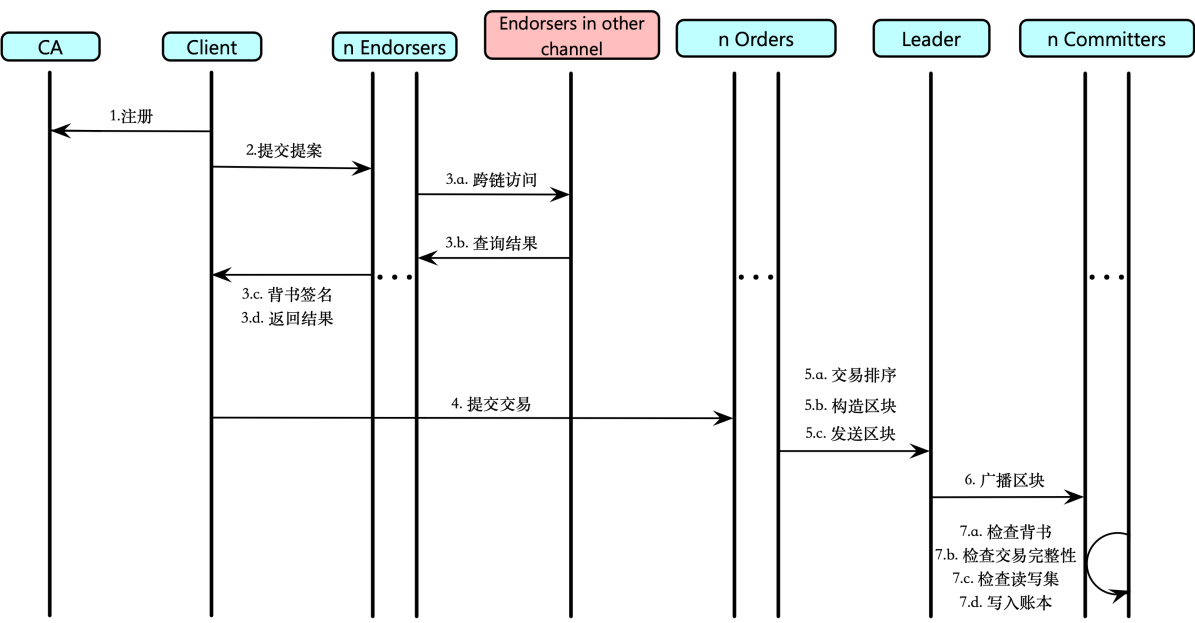


图 10 交易数据流图

系统事务层的主要功能是通过SDK进行区块链内与链外的数据传递，另外通过一个Web页面进行链上数据的查询与展示，并且提供接口让用户可以与区块链进行数据交互。

## 本方法的优点

本系统实现了基于共享节点的跨链数据巡查方式，相较于其他区块链互操作技术，在系统设计上更为简单，没有引入新的通信开销，只是在共享节点中进行了跨通道的通信，因此该系统在跨通道查询时的性能不会受到很大的影响，同样这样的性能完全满足监管机构进行监管的需求。

对于本系统的安全性，我们从保密性、完整性和可用性三个方面（CIA特性）分析，首先超级账本区块链技术本身就使用了密码学的技术对数据进行加密保护，链上的数据都是保密的，对于没有进入通道的节点或者实体，都没有权限进入通道进行数据访问，因此该系统具有很强的保密性；然后，对于系统中数据的完整性同样能够被保护，超级账本对每一笔交易、每一个区块都具有追溯的功能，并且在每一个区块头中都具有区块内容和上一个区块的哈希值，另外在区块链中具有共识机制，因此在部分节点出现故障、数据丢失甚至作恶的情况下，整个系统依然可以正常运行，因此该系统具备完整性；最后对于系统的可用性，系统除共享节点外的部分节点崩溃都不会使整个系统不可用，但是对于系统共享节点的攻击会导致系统监管行为的不可用。总的来说，本系统基本具备保密性、完整性和可用性，整个系统的安全性能够保障。

# 一种基于多注意力机制和自适应学习的智能合约漏洞检测方法及系统

## 现有智能合约漏洞检测现状

智能合约，是一种以信息化的方式传播、验证或者执行合同的计算机协议。在智能合约中，所有规则公开透明，合约内的规则以及数据对外部可见，所有交易公开可见，不会存在任何虚假或者隐藏的交易，也就是说智能合约具有公开透明、不可篡改等特点。智能合约虽然极大的扩展了区块链的应用场景与现实意义，但是其本身就是一段程序，近年来针对智能合约的攻击导致的安全事件时有发生。如果这些异常交易行为能及时发现并做出响应，将能有效避免或降低经济损失。

目前智能合约的检测主要有两种手段，分别是人工审计和自动化审计。随着智能合约数目的日益增长，人工审计费力耗时效率低下，显然不匹配当前背景下的智能合约漏洞检测；自动化审计包括基于特征的代码匹配、基于形式化验证以及基于符号执行和符号抽象，基于特征的代码匹配能快速响应新漏洞，而基于形式化验证以及基于符号执行和符号抽象的自动化审计可以有效的降低智能合约漏洞检测的误报率和漏报率。

## 当前方法存在问题

尽管上述的自动化审计方法有智能合约异常检测中取得了一定的效果，但是在以下几个方面仍有待进一步完善：（1）智能合约中的函数和特征变化性比较多，特征不稳定，这造成特征码的定位难度加大，特征码的有效性降低；（2）基于形式化验证的审计方法自动化程度低，需要技术人员二次校验；（3）分析方法复杂繁琐需要比较长的分析时间；（4）误报率较高。

随着深度学习技术的逐渐成熟，基于深度学习实现的目标检测等方法日益成熟。将深度学习用于检测智能合约异常任务，可以有效提取高层次有效的特征，并且接口封装程度高，只需将智能合约的字节码文件作为神经网络的输入，经网络计算获得网络预测结果，实验发现用深度学习去检测智能合约漏洞，具有更低的误报率。

然而，智能合约的特征过于庞大，导致训练的成本高，耗时久，此外，智能合约构建的数据集往往是良性样本远远多于恶意样本，也就是说无漏洞的样本数多于有漏洞的样本数，而普通的深度学习方法采用的是交叉熵损失函数来训练，导致训练出的模型漏报率较高。

## 基于多注意力机制和自适应学习的智能合约漏洞检测方法详细技术方案

针对现有技术中存在的不足，本课题提供一种基于多注意力机制和自适应学习的智能合约漏洞检测方法，本方法从加速模型训练和降低漏报率两个角度切入，兼具轻量级和低漏报率的功能。主要技术方案如下：

1. **样本集构建：**爬取与智能合约交易相关记录并构建样本集，该样本集为正负样本不均衡数据集，提取数据样本集中的原始特征并构建特征矩阵如下：



其中，是指统计出来的特征数目，即数据集的原始特征维度，表示样本的数量；，；记（特征矩阵第个列向量）为第个特征向量，为第个特征；若智能合约特征向量存在特征所表征的现象，则对应的值为1，否则值为0；以80%，20%的比例划分特征矩阵，得到训练集特征矩阵与测试集特征矩阵，以下简称训练集与测试集；

1. **构建深度神经网络AdaNet：**构建DSE模块，将样本集构建过程中获得的高维度智能合约特征有序放入多个通道中，用于加速深度学习网络的训练和提取多样化特征；构建MA模块，MA模块具有三条不同感受野的通道，同时配备不同的注意力机制模块，用于提取不同维度的特征；构建AdaLoss损失函数，自适应平衡正负样本的损失，并结合反向传播算法训练网络；
2. **测试：**将测试集输入到训练完成的智能合约异常检测模型，并给出预测结果。其中，DSE模块的具体过程如下：
3. 降维：使用一个全连接层，将特征数为的原始特征降维至大小为的新特征，且新特征中的每一个单元，都含有所有原始特征的信息；
4. 计算特征重要性：将新特征输入到双层的全连接层，第一层全连接层采用的激活函数是Rectified Linear Unit(ReLU)，目的是增加网络的非线性和使网络具有稀疏性，第二层全连接层采用的激活函数是sigmoid，由于其输出范围是，可以用于表征每一个特征的重要性，此处将其输出值设为；
5. 重标定：特征和输出值相乘，得到新特征向量，然后将通道数为1的特征向量重塑成多通道的特征向量，其中的形状为，而的形状为 ， 均为人为可选择的超参数，选择时需满足；重塑过程为：将的维度变换为的维度。重塑过程只涉及张量维度变换，不涉及其它任何算术运算；然后将新特征向量作为深度学习网络的输入。

构建MA模块的具体过程如下：

1. 构建MA模块第一通道（整体感知通道）：假设输入的特征为经过空洞卷积计算后的特征为，最后经过注意力公式计算得到特征为，和MA模块其他两层的输出一起作为下一层神经网络的输入特征；
2. 构建MA模块的第二通道（局部感知通道）：采用多个小卷积核连续卷积的方式进行特征的提取；假设卷积核的大小为，堆叠个这样的卷积核，最终的感受野大小为：



根据第一通道中的感受野大小来堆叠若干个小卷积核从而达到和第一通道一样的感受野；设卷积运算为，输入特征为，卷积后的结果为，则有如下公式：



此处引入通道注意力机制，即通过反向传播来学习每一个通道特征的重要性；此处注意力计算需依次进行挤压和激励；最后将激励后的结果与卷积后的结果进行乘法运算得到输出，与MA模块的其他通路输出一起作为下一层网络结构的输入特征。

1. 构建MA模块的第三通道（降维通道）：通过进行卷积核为的卷积计算并进行ReLU激活，即。
2. 融合：将MA模块前三条通道的输出结果 相加并进行一次ReLU激活，即，是ReLU激活函数，将作为下一个MA模块的输入特征，如此堆叠多个MA模块。

AdaLoss损失函数的详细过程如下：

1. 计算整个样本中正负样本的权重：假设正样本的数量为，负样本的数量为，那正样本的权重为，负样本的权重为，其中；
2. 计算加权交叉熵：公式如下：



其中 是神经网络的输出值，而是样本的标签，即真实值；

1. 优化AUC：在不平衡问题中，AUC是评定模型好坏的重要指标，然而AUC是不可微的，因此无法直接参与反向传播，也就是说直接优化AUC通常是一个NP难问题，但是可以根据Wilcoxon-Mann-Whitney系数来对AUC做极大似然估计。通过最小化WMW系数的损失值达到优化AUC的目的，具体的优化公式如下：



其中是神经网络中正类的输出值，是负类的输出值，和则是网络的超参数， ；

1. 合并损失函数：将加权交叉熵和WMW损失值加和，另外在WMW前面加一个权重更佳，即合并后的损失函数如下：



将新的损失函数（AdaLoss损失函数）代替原始的二分类交叉熵损失函数进行模型训练，而新的损失函数具有更低的假阴性，更高的AUC，适用于不平衡任务优化的场景，通过反向传播训练好的AdaNet输出的概率值经过转换即为最后的输出结果。

## 本方法的优点

本方法是一种基于多注意力机制和自适应学习的智能合约漏洞检测方法，首先通过抽取智能合约交易行为的多维度原始特征构建数据集，其次提出一种深度学习多注意机制自适应权重模型AdaNet用以学习原始特征的重要性并挖掘不同特征间的关联关系；基于所提AdaNet模型，针对智能合约漏洞领域样本正负样本不均衡问题通过最小化类AUC损失以获得比传统分类模型更强的泛化性能。

# 一种区块链平台的安全测评方法

## 现有区块链平台安全测评方法存在的问题

区块链系统和传统的软件有很大区别，它的底层是一个去中心化的分布式网络，可能跨越多个子网、多个数据中心、多个运营商，这使得它具有边界模糊、故障复杂、类型多样的特征。与传统软件测试相比，区块链本身包含公有链、私有链、联盟链等多种类型，且不同类型在用户权限、最大节点数等平台自身特征方面均有不同，因此区块链测试需要同时考虑所有的安全问题，从而保证区块链系统的可靠运行，这也导致测试方案更加复杂。

区块链架构可以分为基础层和合约层，基础层包括算法模块、加密算法模块、数据管理模块等作为底层支撑构建的部分，合约层指智能合约，针对区块链平台的安全检测可以从这两个方向分别进行。针对基础层的安全检测目前还未出现强人工干预的自动化检测方法，主要依赖于白盒和渗透测试，白盒测试需要对庞大的区块链代码进行详细审计，并人为设计大量测试用例，检测周期长，且需要大量的人工工作，效率低下。渗透测试同样需要较大的人工参与度，且依赖安全人员的检测经验，极易由于人为疏忽或者经验不足而未能发现潜藏漏洞。由于利用智能合约安全漏洞发起的攻击占区块链安全事件的极大多数，因此针对智能合约的安全检测研究较多，主要方法包括：模糊测试、符号执行。模糊测试通过构造模糊测试输入和随机的函数调用序列检测智能合约是否存在安全漏洞，然而智能合约所承载的业务逻辑较为复杂多变，无法设定一个准确的判断条件用于确定模糊测试的数据结果是否满足漏洞特征，同时它们的检测策略比较单一，即使是同一种漏洞在不同的代码场景出现，也无法保证准确检测。符号执行通过符号执行收集的上下文条件分析字节码特征从而判断是否有漏洞，然而符号执行过程中所覆盖的代码路径随着条件判断/循环的增多呈指数级增长，覆盖全路径的计算时间不可接受，而若限制执行路径深度，则极大可能导致未能检测到包含漏洞的代码块。

此外，在区块链系统测试过程中还会遇到软件测试理论的两个基本难题：

（1）可靠测试用例集难题。由于在软件测试过程中无法进行全覆盖测试，因此需要对测试输入空间进行约简，同时又需要保证测试用例集合的充分性，满足这种条件的测试用例集合被称为可靠性测试用例集。（2）测试判定难题。即使能够找到满足条件的测试用例T，在执行每个测试用例时怎样判定测试结果是否正确也面临严峻的挑战。然而，在实际的软件工程中，由于软件开发受人为因素、成本因素等多种因素的制约，需求规格通常并不完善，不可能针对每个随机的输入都给出确定性的预期输出。

## 区块链平台的安全测评方法详细技术方案

研究区块链平台安全测评方法总体工作路线是：首先构造覆盖网络协议、智能合约、分布式账本、共识机制等功能模块的区块链平台的脆弱性模型并用形式化单子符号系统表征脆弱性模型，进而构造区块链平台安全测试框架；然后，基于蜕变测试的理论与技术研究基于形式化安全测试框架的测试用例生成方法与蜕变关系构造方法，找到具有较高使用效率的测试用例集和正确的蜕变关系；最后，通过建立包括可用级、实用级、自主验证级、权威评估级和理论证明级五个等级的面向区块链平台的安全等级评价指标，利用安全测试框架中形式化后的测试结果输出模块对被测试区块链平台的安全级别进行评价。

图片包含 日历

描述已自动生成

图 15 区块链平台的安全测评总体框架

具体的实施细节可以划分为以下步骤：

1. 针对构建面向区块链平台的分布式布置特征和模块间高内聚性的特点，在传统分布式系统平台脆弱性模型的基础上进一步构建考虑区块链平台中网络协议、智能合约、分布式账本、共识机制等模块的脆弱性模型，从而形成一套完备的区块链平台脆弱性模型。利用单子符号系统对脆弱性模型中的元素类型、接口函数和结合关系进行形式化定义，生成一个包含测试方法、测试规则、测试算法和测试结果等模块组成的区块链平台安全测试框架；使用单子符号系统Model Action Language表征区块链功能模块，使用分支时序逻辑语言表征系统需要达到的安全属性合集，输入到形式化验证工具NuSMV模型检测器中运行，并根据输出结果生成区块链平台的脆弱性状态图，根据每个安全属性的输出结果赋予每个脆弱性状态一定的权重，最后引入可靠性理论为区块链平台计算出一个攻击期望值。

图示

描述已自动生成

图 16 基于脆弱性模型的区块链平台安全测试

1. 针对被测区块链系统构造蜕变关系，即当程序输入满足一定的关系时，其相应的输出也就必须满足某种关系。根据蜕变关系涉及的参数和原始测试用例，生成后续测试用例。接着，分别运行这两种测试用例并判定对应的输出是否满足蜕变关系，如果测试输出不满足蜕变关系则相应的测试用例中一定存在失效，即程序一定存在故障；而如果测试输出满足蜕变关系，则证明相应的测试用例执行正确。

图片包含 图示

描述已自动生成

图 17 基于蜕变测试的区块链平台安全测试

1. 结合软件可信分级指标中给出的评价体系以及评价指标，考虑到区块链平台的检测效率、检测性能、误报率、准确性、时间开销、资源开销、应用领域、易用性、优缺点等因素，将区块链平台评价为：可用级、实用级、自主验证级、权威评估级和理论证明级五个等级。根据待评估的区块链平台，设计评估矩阵以结合每一个因素进行模糊评判，然后将模糊综合评价模型应用到区块链平台评估中。通过使用模糊综合评价对每项指标进行多次评价并统计评价的分布比例，最后输出包括区块链平台安全等级及各个指标参数的评估报告。

图片包含 多边形

描述已自动生成

图 18 区块链平台安全等级评价

## 本方法的优点

采用的基于脆弱性模型的形式化验证方法用具有形式语义的记号和工具明确地表述所要设计的计算机系统的设计要求，给出系统规范，并根据系统规范利用上述记号和工具对系统具有的性质和最终实现的正确性进行严格的证明，能覆盖完整的设计状态空间。对于白盒测试、渗透测试、模糊测试等方法，它们只是检验了在使用某些测试向量时系统不会出现漏洞，但无法保证当使用其他测试向量时漏洞不会出现，而形式化验证对指定描述的所有可能的情况进行验证，有效地克服了随机性较大的不足。形式化验证的完备性取决于属性的完备性，而后者可以基于设计要求建立清晰明确的模型。此外，采用蜕变测试不但可以用于不同类型的软件测试中，而且也有助于故障定位和程序证明。无论是应用于不同的被测程序，还是与其它测试方法相互结合，蜕变测试的主要目的就是为其它测试技术生成的测试用例提供测试判定。当其它测试技术面临测试判定难题时，进行蜕变测试可以有效地解决它们面临的问题。

# 一种基于多维评价指标的权威节点选举机制

## 现有区块链平台权威节点选举机制存在的问题

在“以链治链”架构下，如何调和监管需求与共识算法效率、安全性之间的矛盾，是本任务要解决的关键问题。

在区块链系统中，一般情况下各个节点分散且平行。整个系统要顺序运行且公平公正，实现所有节点的行为状态结果一直，所有节点共同管理和维护系统。共识机制就是为实现上述目的而提出管理机制。

在公链中，因不存在准入机制，所以采用计算密集的PoW算法，共识操作会消耗大量计算资源；同时，为了保证共识协议的安全性，区块的共识速率被人为地限制，导致网络吞吐量较差；目前区块链系统中算力多集中在少数的矿池，使得51%攻击变为会切实发生的威胁，影响区块链系统的安全性。

在联盟链/私链这类存在准入机制的区块链中，共识协议普遍采用Crash Fault Tolerance方案，这在提高性能的同时牺牲掉了安全性，同时还存在着过强的安全假设，即要求加入节点是完全可信的，没有考虑到节点作恶的情况。

什么是共识机制，共识机制在区块链的作用，现有的共识机制有哪些，选举在共识机制中的作用。

常见的共识机制的选举方案存在的问题，

共识机制需要改进的点。

## **基于多维评价指标的权威节点选举机制详细技**术方案

本方案扩展了区块链基本块结构，提出了监管区块结构的设计。设计思路如图16所示，本研究扩展了区块的事务消息内容，包括基本的操作信息Base Info、节点的状态信息Sys.Node Info和控制信息Control Info。节点信息用于维护信用节点评价指标体系，实现监督链节点相关数值的量化监控和评价，通过评价算法筛选合适节点构建节点候选集，实现节点的非交互、无感知、平滑地动态更新。控制信息包括授权信息和审计信息，用于监管链的扩容，提高系统吞吐量。

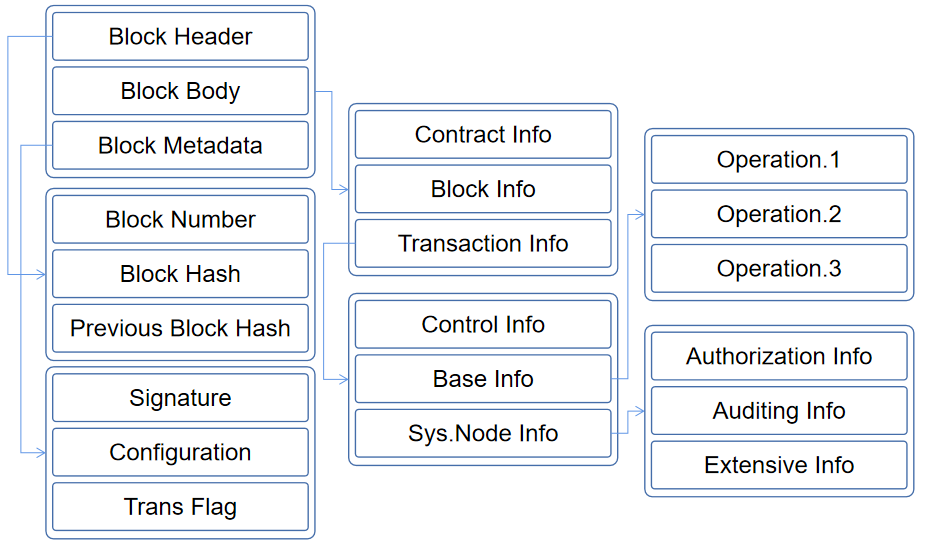


图 16 监管链区块结构基本设计思路

以联盟链为基础的监管链摒弃了公共链通过PoW缓解拜占庭错误的方案，强化了权威节点的作用和能力。联盟链的权威节点通过了合法验证，降低作恶风险。本研究提出了信用节点评价指标，包括节点稳定度、节点联通度、数据合法性和哈希率。这四个指标综合反映了一个节点在审计链中的安全性、可靠性、稳定性和可用性。

审计链的节点逻辑上分为三类：客户节点、中间节点和权威节点。通过强化权威节点保证审计链的工作效率，但权威节点并非一成不变。通过信用节点评价指标体系，对三类节点进行度量和评价。

如图17所示信用节点分类与状态迁移，新加入的节点被认为是恶意节点，只有被评价指标体系认可的节点才能称为合法的节点，而且三种节点的身份可以相互转化。三种节点在功能上有重叠，权威节点拥有客户节点和中间节点所有的能力，中间节点具备客户节点的所有能力。

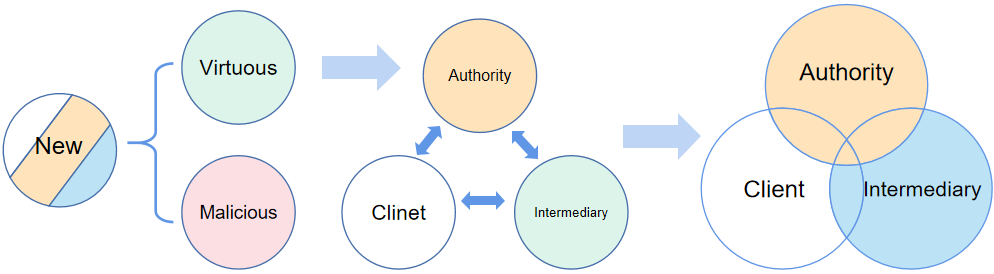
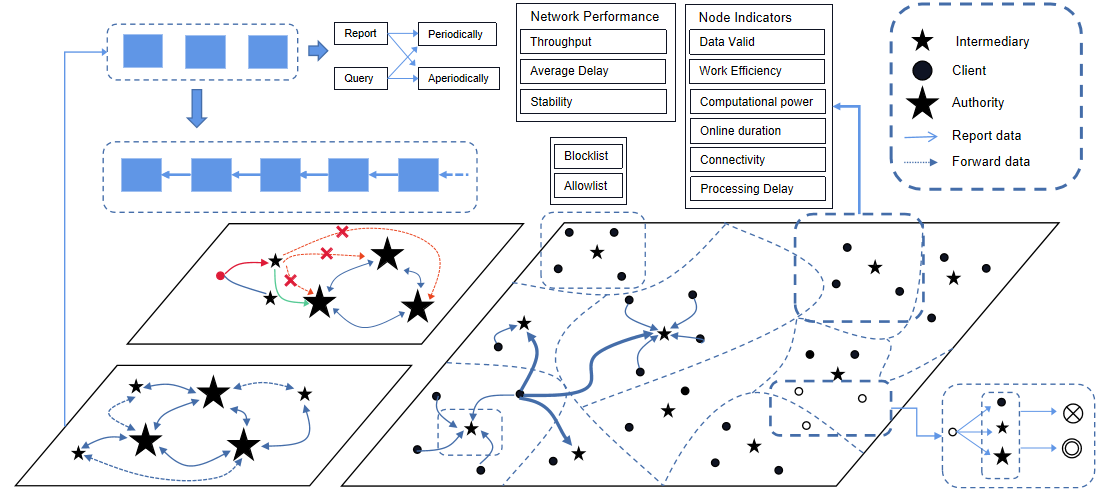


图 17 信用节点分类与状态迁移

监管链通过非交互式选举方式实现权威节点的动态更新。通过2.2.2信用节点评价体系，构造权威节点候选集，并持续动态更新该集合。根据监管链的需要，权威节点通过候选集实时更新。被淘汰的节点失去权威节点身份，由候选集补充。权威节点之间通过内部协议达成快速共识。每次补充的权威节点在本次共识结束后加入网络。权威节点的选择通过2.3成果展示的信用节点评价指标体系通过全网选举产生，选举活动和节点更新动作是异步的，不会造成阻塞，因此更新将非交互、无感知、平滑的完成。

监管链的三种节点组成立体扁平P2P网络结构。根据节点类型设计整体分层网络，局部扁平P2P网络，分层结构实现网络低成本扩容与演进。如图18所示，低层级节点向高层级节点汇聚，节点之间组成P2P的扁平拓扑结构。不同层级的组网自下而上，组成立体网络，并保持去中心化结构。



本研究扩展了区块链基本块结构，提出了监管区块的设计。将监督链节点划分为客户节点、中间节点、权威节点三种类型。提取三种节点的共性指标，对其量化描述，依据信用节点评价指标体系构建节点演进算法从而构建候选集。依赖候选集通过非交互式地进行节点的动态更新。

在2.2.3中将节点分为三类。权威节点是可信、稳定的，同时应当具备一定算力。本研究提出了多项指标评估一个节点是否具备能力担任权威节点角色，从节点的在线时长、联通度、误码率、算力等方面考量。

Stability Value(SV)：稳定度反映了一个节点在网络中的稳定在线时长。只有SV超过预设特定阈值的节点才有资格成为核心节点。

网络所有节点组成的网络拓扑结构是动态变化的，有的节点稳定在线，有的节点频繁的上线和下线。假设网络核心节点在一个时间片段*t*内数量是固定的，*a*代表网络平均核心节点算力，*n*代表网络核心节点数量。当前网络的总算力*s* = *a·n*。算力*s*刚好满足当前网络处理数据的要求。但是比例*m*的节点在线时间不稳定，为了保证网络的业务处理最低能力，只能保守地把全网算力降为s = *(1-m)·a·n*。对应的，需要降低区块的目标难度。

显然，网络的整体算力变化应该处于一个合理的区间，所以网络中提供算力的节点就需要稳定在线。一个刚加入网络的节点*n*，在时间片段*t*内，在线时长*t1*，离线时长*t2*，离线次数*Toff*，网络要求在线时长*td*。

Degree Value(DV)：节点度是指和该节点相关联的边的条数，又称关联度。网络鼓励节点与更多的节点通信，避免网络出现割边或割点。网络的平均DV提高后，一方面提高网络的稳定性，另一方面减少矿池的出现和私自挖矿等攻击。因此节点的*DV*越高，越可信。低*DV*的节点被认为是孤立的节点。

假设节点*n*在时间片段*t*内与*m*个节点通信，那么节点*n*的*DV*为

假设若干个节点之间相互通信，组成矿池。网络认为这几个节点也是逐渐变为孤立点，其*DV*值逐渐弱化，网络设定衰减系数，新增节点*m*个，表示为：

Validity Value(VV):数据有效性主要衡量两个指标，一方面是衡量节点在规定时间内数据传输精确性。另一方面衡量节点在规定时间内数据的有效性。精确性体现在一个节点如果转发和确认的数据与原数据有差异，可以认为数据被修改。有效性体现在一个节点如果转发和确认的数据已经存在于区块链上，可以认为数据是无效的。*VV*保证了数据的正确性，避免数据被窜改。*VV*也避免了数据重复被确认，造成网络资源的浪费。

假设节点*n*在时间片段*t*内的接受到数据，转发正确数据，打包数据*，*确认有效数据*，*网络的合法性最小值是，*VV*的计算如下：

Computational Power(CP):算力（也称哈希率）是网络处理数据能力的度量单位。即为计算机（CPU）计算哈希函数输出的速度。网络必须为了安全目的而进行密集的数学和加密相关操作。在某一时间段t内，网络处理段数据量是一定的。网络在*t*内处理这些数据需要算力*m hash/s*，全网符合要求的核心节点数量为*n*，则单节点的算力为

网络的数据处理能力需要不断提升，所以核心节点的数量和核心节点的算力也要提升。算力可以作为限制条件排除一些低算力的节点，算力也可以作为竞争指标增强节点的可信度。如果存在一个节点*x*，其算力，网络平均算力为，且有：

节点*x*将在网络中占据主导地位。因此本研究限制节点的算力不可无限膨胀，网络规定底数，以为底的对数作为算力度量值。在鼓励节点增加算力的同时，限制节点进行算力攻击。如下：

本研究提出了多维度指标描述节点的各项性能。这些指标综合体现一个节点的可信度。节点x的可信度表示如下：

,,和表示节点x的稳定度、联通度、数据有效性和算力在可信度中的权重。根据TSN对各个指标需求，各项权重可以调整，且满足

本研究扩展了区块的事务消息内容，包括基本的操作信息Base Info、节点的状态信息Sys.Node Info和控制信息Control Info。节点信息包括2.3.1提出的信用节点评价指标，这些指标用于维护信用节点评价指标体系，实现监督链节点相关数值的量化监控和评价，通过2.3.2多维权威节点选举机制筛选合适节点构建节点候选集，实现节点的非交互、无感知、平滑地动态更新。

如图2-4是区块结构和数据结构设计，区块数据结构的设计目标是实现对被监管链审计的同时，实现网络的可扩展性。审计链在主链存储对被监管链审计的事务，随着网络扩展，主链从传统事务链平滑演进为控制链。区块将从初始区块、过渡区块、控制区块动态演进。控制链存储对扩展子链的控制信息。同时通过叔区块存储网络中的争议和分歧，并通过激励机制鼓励节点同步叔区块，并在主链侄节点存储叔区块相关信息。

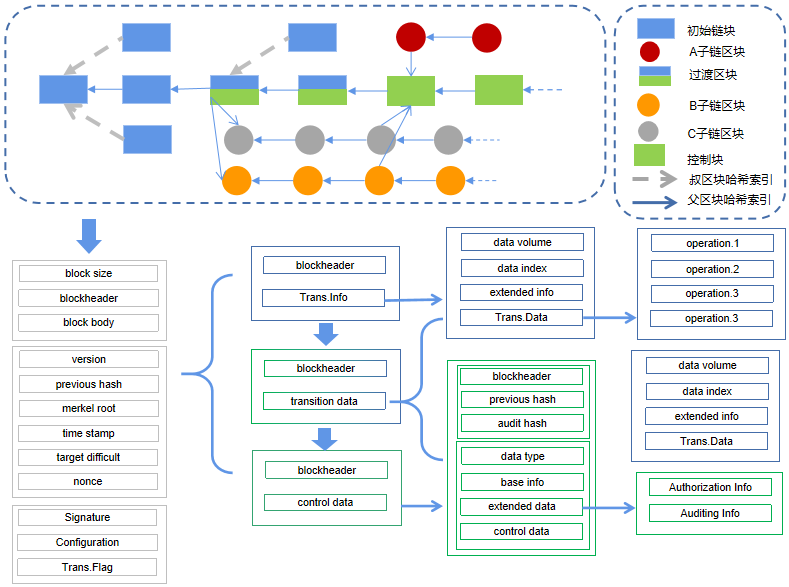


图 2-4 监管链区块与数据结构

## 本方法的优点

采用的基于脆弱性模型的形式化验证方法用具有形式语义的记号和工具明确地表述所要设计的计算机系统的设计要求，给出系统规范，并根据系统规范利用上述记号和工具对系统具有的性质和最终实现的正确性进行严格的证明，能覆盖完整的设计状态空间。对于白盒测试、渗透测试、模糊测试等方法，它们只是检验了在使用某些测试向量时系统不会出现漏洞，但无法保证当使用其他测试向量时漏洞不会出现，而形式化验证对指定描述的所有可能的情况进行验证，有效地克服了随机性较大的不足。形式化验证的完备性取决于属性的完备性，而后者可以基于设计要求建立清晰明确的模型。此外，采用蜕变测试不但可以用于不同类型的软件测试中，而且也有助于故障定位和程序证明。无论是应用于不同的被测程序，还是与其它测试方法相互结合，蜕变测试的主要目的就是为其它测试技术生成的测试用例提供测试判定。当其它测试技术面临测试判定难题时，进行蜕变测试可以有效地解决它们面临的问题。

# 总结

按照课题任务书及实施计划，在本年度，我们主要完成了以下几个方面的工作。

1. 为了实现“以链治链”新型协同监管架构，我们研究了在区块链监管场景下的监管链与多条异构接入链的跨链通信机制，提出了两种不同的跨链监管方案，并在Hyperledger Fabric区块链上搭建了对应的监管架构。第一个方案是基于链上节点代理的跨链方案，在该方案中，多条异构区块链可以借助链上节点构建一个去中心化的跨链监管网络，实现跨链通信。第二个是基于共享节点的跨链监管方案，该方案在区块链框架上建立监管链和业务链两条通道实现业务链的正常交易数据，通过监管链和业务链上的共享节点实现被监管的业务链参与到监管链中的同时，满足上层监管链对底层业务链的交易监管与数据巡查功能。
2. 我们初步研究分析了“以链治链”区块链跨链监管的安全需求。在跨链监管的场景下，我们需要保证跨链数据在跨链的各个阶段的真实性、准确性和隐私性。针对上述需求，我们在所提出的跨链监管方案中均初步设计了安全保证机制。在基于链上节点代理的跨链方案中，我们通过多节点代理程序实现数据巡查并加密传输，保证了监管数据的真实性与隐私性。在监管数据上链的时候，我们利用共识机制，对跨链数据进行验证，保证了监管数据的准确性。在基于共享节点的跨链监管方案中，我们借助Fabric本身的成员管理策略，实现跨链系统的访问与接入控制。
3. 在本年度我们提出了一种基于多注意力机制和自适应学习的智能合约漏洞检测方法。我们爬取了智能合约相关数据以构造样本集，提取样本集中的原始特征并构建了特征矩阵。同时通过多注意机制自适应权重模型AdaNet与反向传播机制来学习各个通道特征的重要性。另一方面，由于所构造的智能合约数据集存在正负样本不均衡的问题，我们根据Wilcoxon-Mann-Whitney系数来对AUC做极大似然估计。通过最小化WMW系数的损失值来优化AUC，从而解决样本不均衡问题。最终与AdaNet模型的输出一道构造并优化新的损失函数最终以达到对模型提出的自适应强泛化等性能要求。
4. 在针对区块链平台的安全测评方法方面，我们提出覆盖区块链平台中的网络协议、智能合约、分布式账本、共识机制等模块的脆弱性模型，并用形式化单子符号系统Model Action Language表征脆弱性模型，从而形成一套较完备的区块链平台脆弱性模型，解决了区块链分布式网络边界模糊的问题。同时我们为区块链系统构造了6条蜕变关系，分别运行原始测试用例以及后续测试用例，判定对应的输出是否满足蜕变关系，如果测试输出不满足蜕变关系则程序一定存在故障，达到了检测分布式区块链系统漏洞的效果。最终，我们参考软件可信分级指标中给出了区块链平台的安全性评价体系以及评价指标，对待评估的区块链平台进行模糊评判，以及对每项指标进行多次评价并统计评价的分布比例，最后输出包括区块链平台安全等级和各个指标参数的评估报告。