课题编号： 密级：

国家重点研发计划重点专项

课题实施方案

项目名称： “以链治链”的监管架构与关键技术研究

课题名称： “以链治链”的跨链协同监管体系与方法

课题牵头单位（盖章）： 西安电子科技大学

课题负责人（签字）： 姜晓鸿

所属专项： 云计算和大数据

执行期限： 2020年 11月至 2023年10 月

**课题实施方案编写说明**

课题实施方案是课题实施过程中的重要文档。编制课题实施方案须以课题任务书和课题任务书为基础，要求目标明确，针对性强，系统性表征突出，成果形态明确。各课题在编制实施方案时，可根据自身特点适当进行调整。如下要求供编制实施方案时参考使用。

1、建立完整技术指标体系，明确核心指标。重大共性关键技术、应用示范类课题技术指标要细化到研究基本单元；基础前沿类课题需明确具体的课题科学目标，准确凝练需解决的所有关键技术问题或科学问题。

2、确立明确、清晰的任务（课题）接口关系。围绕总目标，合理进行任务分解，体现课题整体性和一体化组织实施的要求。

3、拟定课题详细的技术路线，制定合理的进度计划，设置关键节点。结合标志性成果，确定阶段考核的主要方式、方法。按照总体进度要求，各课题应对各课题研究进展提出明确要求。

4、明确课题成果形态。提出包括成果形式、技术指标、技术成熟度、成果测试等在内的完整的成果状态表述，建立相应的检查或考核办法，确保课题阶段目标和总体目标的实现。基础研究类课题可参照上述要求执行，实现课题科学目标。

5、结合课题特点，建立有权威、执行力高、操作性强的课题实施组织管理机制。对实施过程中的政策、管理、技术和知识产权等风险进行充分的分析和预判，制定针对性的措施与办法；加强实施过程中的交流和检查，保证经费、人员的合理调度与使用。

目录

[一、 课题概要 5](#_Toc72075197)

[1.1 课题简介 5](#_Toc72075198)

[1.2 课题总体目标和考核指标 5](#_Toc72075199)

[二、 课题任务分解及主要研究工作 6](#_Toc72075200)

[2.1指南考核指标分解 6](#_Toc72075201)

[2.2 课题任务分解及主要研究工作 7](#_Toc72075202)

[三、 课题实施关键节点与具体实施计划 12](#_Toc72075203)

[3.1课题总体实施计划与进度安排 12](#_Toc72075204)

[3.1.1 研究思路和技术路线 12](#_Toc72075205)

[3.1.2 进度安排与主要任务的分工接口概述 13](#_Toc72075206)

[3.1.3 项目任务进度甘特图 15](#_Toc72075207)

[3.2．课题详细技术方案 21](#_Toc72075208)

[3.2.1 技术路线一：动态迁移的跨链节点权限分级机制 21](#_Toc72075212)

[3.2.1.1 研究思路 21](#_Toc72075213)

[3.2.1.2 技术方案 22](#_Toc72075214)

[3.2.1.3 任务各参与单位具体分工 23](#_Toc72075215)

[3.2.1.4 任务研究进度安排 23](#_Toc72075216)

[3.2.2 技术路线二：异构多态的分布式跨链监管技术 24](#_Toc72075221)

[3.2.2.1 研究思路 24](#_Toc72075222)

[3.2.2.2 技术方案 25](#_Toc72075223)

[3.2.2.3 任务各参与单位具体分工 27](#_Toc72075224)

[3.2.2.4 任务研究进度安排 27](#_Toc72075225)

[3.2.3 技术路线三：边云结合的跨链监管协同机制 27](#_Toc72075230)

[3.2.3.1 研究思路 27](#_Toc72075231)

[3.2.3.2 技术方案 28](#_Toc72075232)

[3.2.3.3 任务各参与单位具体分工 30](#_Toc72075233)

[3.2.3.4 任务研究进度安排 30](#_Toc72075234)

[3.2.4 技术路线四：精准高效的密态内容审计方法 30](#_Toc72075239)

[3.2.4.1 研究思路 30](#_Toc72075240)

[3.2.4.2 技术方案 32](#_Toc72075241)

[3.2.4.3 任务各参与单位具体分工 34](#_Toc72075242)

[3.2.4.4 任务研究进度安排 34](#_Toc72075243)

[3.3．课题经费安排及自筹经费落实方案 34](#_Toc72075248)

[四、 课题组织管理机制 37](#_Toc72075249)

[4.1课题内部管理机构和管理制度 37](#_Toc72075250)

[4.1.1 实施课题负责人和课题负责单位法人双责任制 37](#_Toc72075251)

[4.1.2 建立课题任务督查和目标明确、绩效导向的管理制度 37](#_Toc72075252)

[4.1.3 管理人员分工 38](#_Toc72075253)

[4.2课题实施过程中的交流及检查机制 38](#_Toc72075254)

[4.2.1 课题内部数据共享、资源共享机制 38](#_Toc72075255)

[4.2.2 建立课题例会制度 39](#_Toc72075256)

[4.2.3 对课题的执行情况进行第三方评估 39](#_Toc72075257)

[4.3课题实施过程中的风险分析与控制 39](#_Toc72075258)

[五、 课题成果呈现形式及测试方法 40](#_Toc72075259)

[5.1课题成果呈现形式 41](#_Toc72075260)

[5.2定量指标的测试与检验方法 42](#_Toc72075261)

[5.2.1 考核指标总表 42](#_Toc72075262)

[5.2.2 定量指标的测试与检验方法 45](#_Toc72075263)

# 课题实施方案

# 课题概要

## 课题简介

在“以链治链”监管结构和安全模型的基础之上，本课题重点讨论跨链协同机制，从监管者的视角，纵向涉及节点、交易、管理的权限等级设置，横向考虑不同区域的异构跨域协同，继而做到从微观到宏观的分级多域、从物理结构上的端边云结合，以实现全方位、自动化、协同式监管；另外考虑到监管者不一定是绝对可信的，从系统设计的角度，既要考虑对用户隐私行为——密态内容的监督，也要考虑对监督行为的密态内容进行审计。

本课题的主要研究目标是提出“以链治链”架构下跨链分布式监管的协同体系和“以链治链”架构下的新型数据加密审计方法。首先，根据不同密码原语、中继链接、哈希锁定、投票机制、动态优化理论、大数据挖掘和机器学习等理论技术，提出节点分级权限动态迁移机制、跨链监管边云协同技术、安全计算协议自适应生成等关键技术；在此基础上，研发典型应用场景下“以链治链”的跨链协同原型验证程序，并制定适用于该系统的权限分级机制和内容审计方案。

## 课题总体目标和考核指标

**· 课题总体目标**

本课题的总体目标是通过技术研究突破，构建“以链治链”架构下跨链分布式监管的协同体系和“以链治链”架构下的新型数据加密审计方法。利用投票机制、中继机制、哈希锁定、同态加密、动态优化理论、机器学习等理论与方法，解决现有监管方法跨链交互能力弱、协同性差、效率低等问题。提出节点分级权限动态迁移机制、跨链监管边云协同技术、安全计算协议自适应生成等关键技术；在此基础上，研发典型应用场景下“以链治链”的跨链协同原型验证程序，并制定适用于该系统的权限分级机制和内容审计方案。通过项目实施，期望能实现新兴信息通信技术在服务业全要素、全领域、全产业链的深度融合与集成应用，对推动和促进我国物流行业转型及产业升级、提升国际竞争力具有重要意义。

**· 指南考核指标**

通过课题实施，实现除业务链本身的交易延迟，跨链交易性能测试脚本所测的k次跨链过程的平均延迟不超过500ms；k次跨链峰值吞吐量不少于500tps；支持不少于2个协同监管节点；支持不少于2条业务链的跨链交易；形成专利池，完成相关协议、规范和标准（送审稿），建立“以链治链”架构下跨链分布式监管的协同体系。

# 课题任务分解及主要研究工作

## 2.1指南考核指标分解

根据指南要求，结合课题任务书主要研究任务，对指南考核指标中关于本课题的内容按照节点权限分级机制、跨链监管协同技术、密态内容审计方法、原型验证系统及其他指标进行分解和实现，具体如下表1所示：

**表1 指南考核指标及其分解情况表**

|  |  |  |
| --- | --- | --- |
| **类别** | **指南指标** | **分解的二级指标** |
| 节点权限分级机制 | 构建“以链治链”监管架构的节点权限分级机制 | 实现跨链接入环节的多级认证机制、多链数据跨链访问控制机制、以及动态调整的节点权限管理机制 |
| 跨链监管协同技术 | 构建“以链治链”监管架构的跨监管机构协同技术 | 实现边云结合的跨链任务协同机制、以及移动边缘监管节点的放置机制，支持协同跨链峰值吞吐量≥500TPS |
| 密态内容审计方法 | 构建“以链治链”监管架构的密态内容审计方法 | 实现自适应安全的多关键字密文搜查机制、基于安全多方计算的密文审计机制、以及支持噪声动态注入的跨链数据统计分析系统。 |
| 原型验证系统 | 支持不少于2个监管节点协同；支持不少2条业务链的跨链交易；除业务链本身的交易延迟，跨链过程的平均延迟500ms；峰值跨链吞吐量500tps | 支持监管协同节点≥2个，接入业务链不少于2条，跨链平均延迟≤500ms |
| 其他 | 形成专利池，完成相关协议、规范和标准（送审稿） | 专利5项，论文6篇，软件著作权3项  软件构件不少于2项，原型验证系统不少于1项，完成相关协议、规范和标准（送审稿）1项 |

## 2.2 课题任务分解及主要研究工作

为实现课题总体目标和指南考核指标要求，结合上述对指南考核指标的分解情况，课题共设置四个主要研究任务，如图1 所示，包含：动态迁移的跨链节点权限分级机制、异构多态的分布式跨链监管技术、边云结合的跨链监管协同机制、精准高效的密态内容审计方法。最终，研发典型应用场景下“以链治链”的跨链监管协同原型验证系统。



**图1 主要研究内容**

各任务研究内容、关键技术、成果、参与单位及考核指标如下：

**· 任务一：动态迁移的跨节点权限分级机制**

1) 研究内容

- 动态迁移的跨链节点权限分级模型研究

2) 关键技术

- 节点权限按需分级动态迁移技术

3) 成果

- 动态迁移的跨节点权限分级机制

4) 参与单位

- 西安电子科技大学

5) 考核指标

- 发明专利≥1项

**考核指标及评测手段/方法**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **条目名称** | **指标/功能项** | **评测方法** |
| 1 | 发明专利 | 跨链节点权限分级 | 专利：授权书/受理通知书 |

**· 任务二：异构多态的分布式跨链监管技术**

1) 研究内容

- 安全可控的分布式跨链监管方法研究，

2) 关键技术

- 分布式跨链监管技术

3) 成果

- 异构多态的分布式跨链监管技术

4) 参与单位

- 西安电子科技大学

5) 考核指标

- 实现除业务链本身的交易延迟，跨链交易性能测试脚本所测的k次跨链过程的平均延迟≤500ms

- k次跨链峰值吞吐量≥500tps

- 高水平论文≥2篇，发明专利≥2项，软件著作权≥1项，软件系统1个，标准1项

**考核指标及评测手段/方法**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **条目名称** | **指标/功能项** | **评测方法** |
| 1 | 高水平论文 | 区块链跨链安全交互技术 | 论文：录用证明/检索证明 |
| 区块链分布式路由技术 |
| 2 | 发明专利 | 区块链跨链安全交互方法 | 专利：授权书/受理通知书 |
| 区块链分布式路由方法 |
| 3 | 软件著作权 | 跨链安全交互软件/组件 | 软件著作权登记号 |
| 4 | 软件系统 | 跨链安全交互系统：实现除业务链本身的交易延迟，跨链交易性能测试脚本所测的k次跨链过程的平均延迟≤500ms；k次跨链峰值吞吐量≥500tps | 软件：第三方评测机构提供测试报告 |
| 5 | 标准 | 区块链跨链协同监管方面标准 | 国家或行业标准正式立项批复文件 |

**· 任务三：边云结合的跨链监管协同机制**

1) 研究内容

- 边云结合的多模态监管协同模型研究

2) 关键技术

- 边云跨链自动化监管任务调度与协同技术

3) 成果

- 边云结合的跨链监管协同机制

4) 参与单位

- 西安电子科技大学

5) 考核指标

- 协同监管节点≥2个

- 业务链数量≥2条

- 高水平论文≥2篇，发明专利≥1项，软件著作权≥1项，1个软件系统

**考核指标及评测手段/方法**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **条目名称** | **指标/功能项** | **评测方法** |
| 1 | 高水平论文 | 边云结合的任务协同技术 | 论文：录用证明/检索证明 |
| 移动边缘计算场景下的分布式任务协同技术 |
| 2 | 发明专利 | 移动边缘计算场景下的分布式任务协同方法 | 专利：授权书/受理通知书 |
| 3 | 软件著作权 | 边云结合任务协同软件/组件 | 软件著作权登记号 |
| 4 | 软件系统 | 边云结合任务协同系统：边云结合任务协同系统：协同监管节点≥2个；业务链数量≥2条 | 软件：第三方评测机构提供测试报告 |

**· 任务四：精准高效的的密态审计方法**

1) 研究内容

- 精准高效的密态内容审计模型研究

2) 关键技术

- 密态问题近似求解以及安全监管协议自动生成技术

3) 成果

- 精准高效的的密态审计方法

4) 参与单位

- 武汉大学

5) 考核指标

- 高水平论文≥2篇，发明专利≥1项，软件著作权≥1项

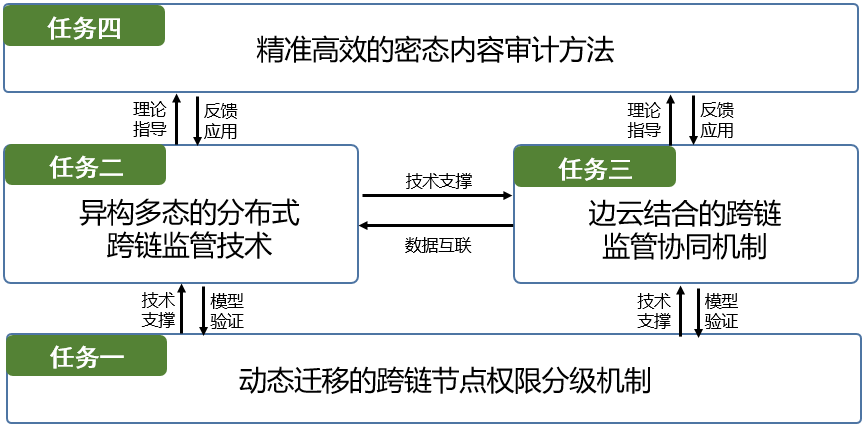
**考核指标及评测手段/方法**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **条目名称** | **指标/功能项** | **评测方法** |
| 1 | 高水平论文 | 具有自适应安全的密文搜索与查询技术 | 论文：录用证明/检索证明 |
| 基于安全多方计算的密文内容审查技术 |
| 2 | 发明专利 | 支持链码的同态加密、差分隐私等数据加密方法 | 专利：授权书/受理通知书 |
| 3 | 软件著作权 | 支持噪声动态注入的链上数据统计分析软件系统 | 软件著作权登记号 |

**参加单位任务分工**

|  |  |
| --- | --- |
| **任务** | **负责单位** |
| 任务一：动态迁移的跨链节点权限分级机制 | 西安电子科技大学 |
| 任务二：异构多态的分布式跨链监管技术 | 西安电子科技大学 |
| 任务三：边云结合的跨链监管协同机制 | 西安电子科技大学 |
| 任务四：精准高效的密态内容审计方法 | 武汉大学 |

各任务的研究内容和考核指标能够全部覆盖指南和任务书的各项要求。其中，各任务间关联关系如图2所示。各任务通过总体方案设计、关键技术攻关、软件系统研制等方式，实现课题的总体目标。



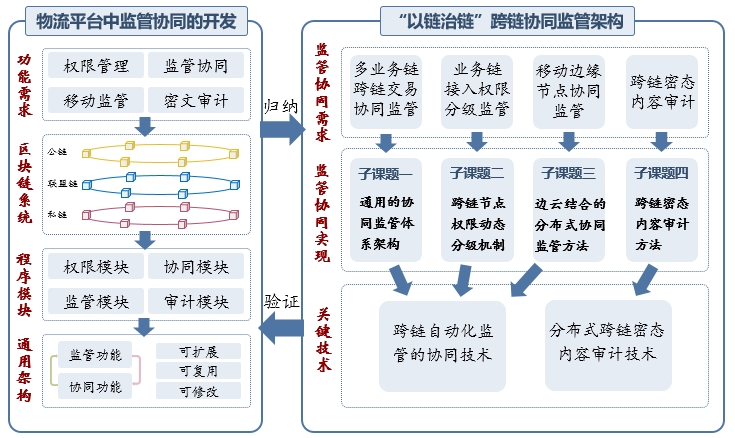
**图2 各任务间关联关系**

# 课题实施关键节点与具体实施计划

## 3.1课题总体实施计划与进度安排

3.1.1 研究思路和技术路线

根据任务书，本课题拟解决的两大关键科学技术问题主要包括：（1）跨链自动化监管的协同机制问题 ；（2）分布式跨链情形下密态内容难于审计的问题。通过项目实施，预期实现跨链监管协同原型验证系统。为此，课题的总体研究思路按照“以链治链”的关键技术突破、系统平台构建和行业应用示范三个层次展开：首先，攻克节点权限分级、监管协同、密态审计三大核心关键技术；基于此，设计新型“以链治链”协同监管架构，并构建权限灵活、权限灵活、协同性强、内容易审计的协同仿真系统；最后，在该平台上进行典型行业的应用示范。



**图3 课题技术路线图**

3.1.2 进度安排与主要任务的分工接口概述

课题实施共分为三个阶段，各阶段目标均按照“以链治链”的关键技术，系统平台和应用示范进行设定，其中关键技术包括面向复杂结构区块链的跨链分布式路由和安全交互技术、面向大量不同类型节点的多级权限管理和积极性评估模型、面向支持链码密态内容审计的同态加密和多方计算密文审查技术等等。

边云结合的任务协同与放置、同态加密、自适应安全的密文搜查、安全多方计算的密文审查；系统平台包括作为理论指导的面向工业互联网的“以链治链”架构下协同监管体系；应用示范包括物流平台的开发等。阶段目标具体如下：

第一阶段（2020年11月至2021年10月）：本阶段项目和课题启动，明确各自目标，全面开展相关研究，主要完成动态迁移的跨链节点权限分级技术研究，设计高效的多级权限管理及监督方案，与此同时开展研究区块链跨链安全交互技术，以及开展构建“以链治链”跨链监管架构，以及加密数据搜索与查询技术相关研究。

第二阶段（2021年11月至2022年10月）：本阶段项目和课题全面展开，相关研究和系统研制。主要完成跨链特征分析技术研究，设计高效的区块链跨链安全交互技术，与此同时研究区块链分布式路由技术和面向移动边缘计算的分布式任务放置协同方法。完成加密数据分析研究，设计支持链码的同态加密、差分隐私等数据加密方案，抽取数据审计的共性计算操作，构建合规属性集，与此同时研究在加密数据上完成复杂计算任务近似求解方法，完成具有自适应安全等级或多关键字的密文搜索与查询等技术研究，并开展加密数据统计分析研究。

第三阶段，（2022年11月至2023年10月）：本阶段项目和课题全面展开，相关研究和系统研制。主要完成跨链安全交互技术研究，实现跨链安全交互系统。完成边云结合任务协同研究，设计最优的边云结合任务协同方案，并且能够实现边云结合任务协同系统。完成移动场景下的分布式任务放置协同技术研究，并能够实现跨链协同原型验证系统。完成差分隐私的数据保护方案研究，设计链上数据的前期去隐私化处理机制，实现支持噪声动态注入的链上数据统计分析，与此同时完成基于混淆电路的隐私保护方案研究，实现基于安全多方计算的密文内容审查方案。

根据上述课题的三个阶段目标，你定了项目关键节点详细的实施计划，包括每个阶段的成果及交付物、考核指标、考核方式以及计划完成时间等，具体如下表2所示。

另外，根据课题的总体技术方案及任务分工，初步制定了本课题的总体实施计划方案，同时对各主要任务单元的分工接口进行了规划和设计，如图4所示。

3.1.3 项目任务进度甘特图

对应上述计划安排，课题进度安排中重要时间管理结点交付物情况说明如下。

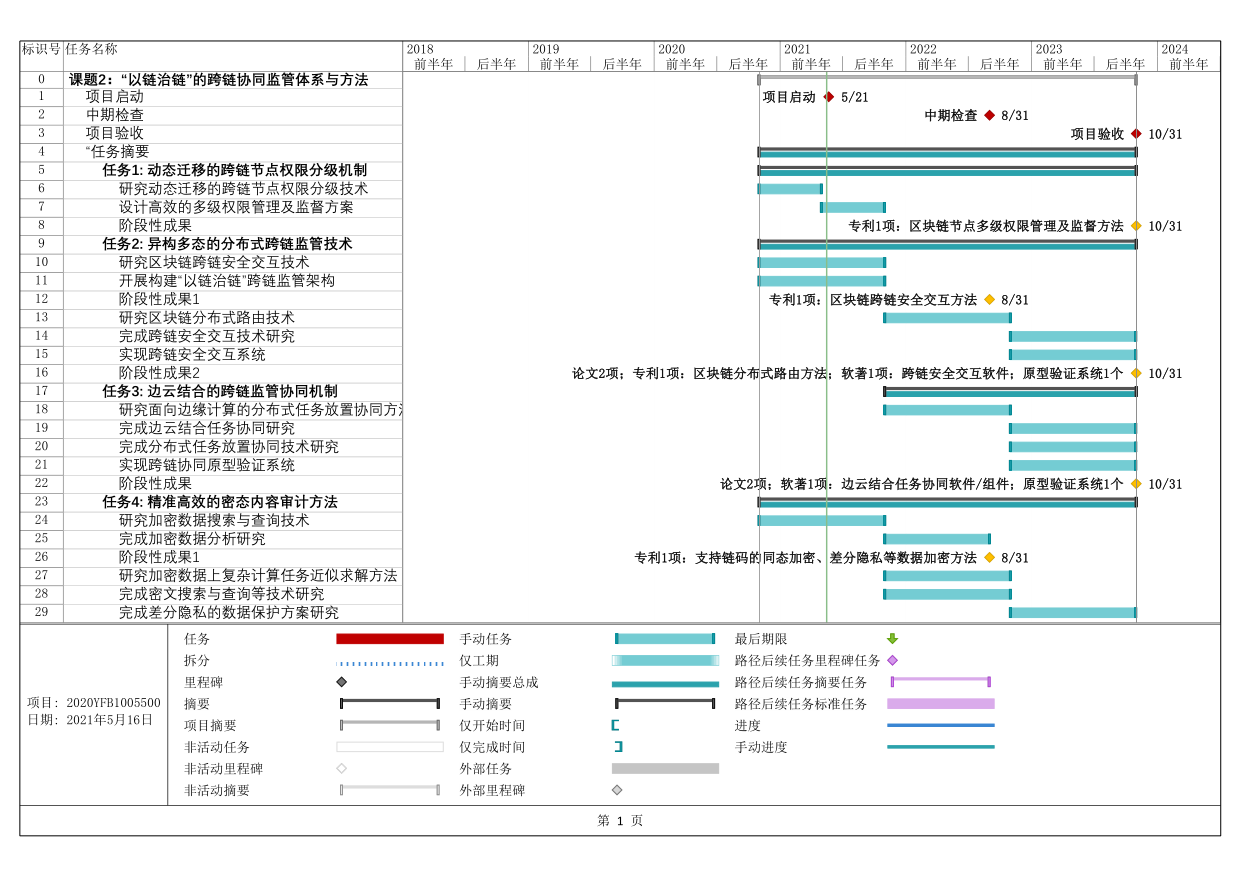
1. **课题重要管理时间节点：**

* 2021年11月：课题第一年度技术进展报告；
* 2022年07月：课题中期技术进展报告；
* 2022年11月：课题第二年度技术进展报告；
* 2023年10月：课题最终科技报告。

1. **课题任务重要里程碑或交付物：**

* 2021年4月：课题内部技术报告1篇；
* 2021年10月：课题年度技术进展报告1篇，专利1项；
* 2022年4月：课题中期技术进展报告1篇，专利1项；
* 2022年10月：课题年度技术进展报告1篇，论文2篇，专利1项；
* 2023年4月：专利1项；
* 2023年10月：课题最终科技报告1篇，论文4篇，专利1项，软件著作权3项，课题子系统软件2项，课题原型系统1项。

1. **本课题任务研究进度甘特图如下：**



**表2 项目关键节点管理实施计划表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **成果及交付物** | **考核指标** | **考核方式** | **计划完成时间（月）** | **责任单位** | **责任人** |
| 1 | 专利：区块链节点多级权限管理及监督方法  专利：区块链跨链安全交互方法 | 专利2项 | 专利：授权书/受理通知书 | 2021年10月 | 西安电子科技大学 | 姜晓鸿 |
| 2 | 论文：具有自适应安全的的密文搜索与查询技术  专利：区块链分布式路由方法  专利：移动边缘计算场景下的分布式任务协同方法  专利：支持链码的同态加密、差分隐私等数据加密方法 | 专利3项  论文1篇 | 专利：授权书/受理通知书  论文：录用证明/检索证明 | 2022年10月 | 西安电子科技大学  武汉大学 | 姜晓鸿  王骞 |
| 3 | 论文：区块链跨链安全交互技术  论文：区块链分布式路由技术  论文：边云结合的任务协同技术  论文：移动边缘计算场景下的分布式任务协同技术  论文：基于安全多方计算的密文内容审查技术  软著：跨链安全交互软件/组件  软著：边云结合任务协同软件/组件  软著：支持噪声动态注入的链上数据统计分析软件系统  标准：区块链跨链监管方面标准  软件：跨链安全交互系统  软件：边云结合任务协同系统  原型系统：跨链协同原型验证系统 | 论文5篇  软著3项  标准1项  软件2项  原型系统1项 | 论文：录用证明/检索证明  软件著作权登记号  国家或行业标准正式立项批复文件  软件：第三方评测机构提供测试报告 | 2023年10月 | 西安电子科技大学  武汉大学 | 姜晓鸿  王骞 |

**图4 课题的总体实施计划方案和各主要任务单元的分工接口**

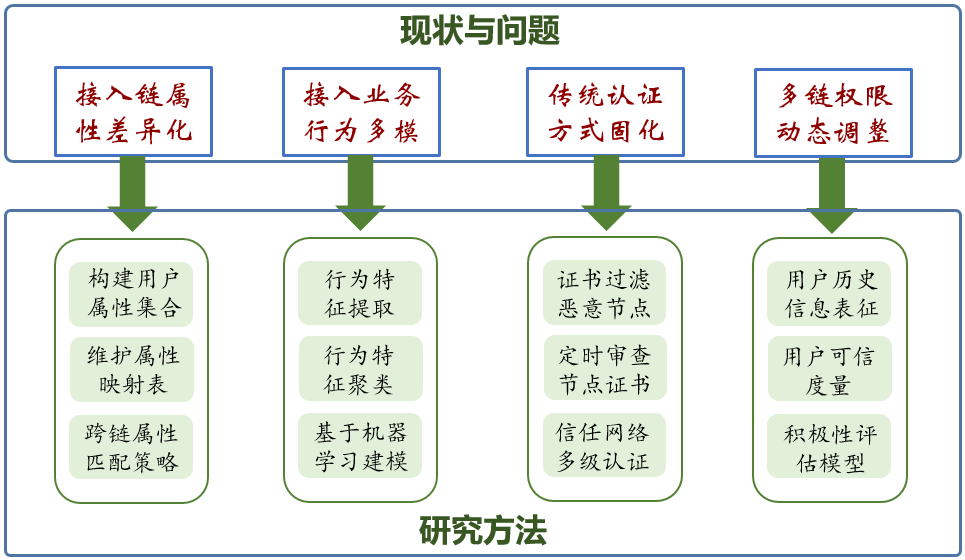
## 3.2．课题详细技术方案

根据课题的总体技术方案，下面按照跨链监管协同的关键技术、系统平台和应用示范，分别给出各自具体的技术路线。

3.2.1 技术路线一：动态迁移的跨链节点权限分级机制

**3.2.1.1 研究思路**

当前物流行业的区块链系统中已经部署了大量的节点，而拥有大量复杂信息的物流环境下，节点分级机制是未来发展的方向，节点分级机制主要包括动态迁移的跨链节点权限分级技术、高效的多级权限管理及监督方案。目前国际上各大政府组织和学术研究团队已经对基于区块链的节点权限方面取得了不俗的成就。然而，在多属性、多模式、多认证、多权限的复杂物流环境下，实现精确的身份认证、权限升降等方面仍然面临着挑战。  
 为此，面向不同的区块链业务场景下的动态迁移的跨链节点权限分级机制（对应任务1），针对不同领域下区块链业务场景复杂、角色繁多、可信度存疑等特点，开展区块链用户节点权限动态分级机制研究。基于信誉计算和多人投票机制研究节点权限动态调整技术，探索链间权限迁移对安全强度的影响，研究同构/异构链不同模态下权限可控迁移机制。为基于区块链的物流行业提供安全、多样的节点权限分级机制，同时为分布式跨链监管机制（任务2）和边云结合的跨链监管协同机制（任务3）提供相应的技术支持。



**图5 任务一研究思路**

**3.2.1.2 技术方案**

研究包括两项内容，分别是“动态迁移的跨链节点权限分级技术”和“高效的多级权限管理及监督方案”。第一项内容拟通过构建用户属性集合和行为特征提取，进而实现跨链属性匹配策略和机器学习建模，实现动态迁移的跨链节点权限分级。第二项内容拟通过证书过滤恶意节点和用户历史信息表征，进而实现信任网络多级认证和积极性评估模型，实现高效的多级权限管理及监督方案。



**图6 任务一技术路线**

下面依次展开说明两项研究内容的技术方案。

**· 内容一：研究动态迁移的跨链节点权限分级技术**

1）构建基于区块链动态迁移跨链节点的跨链属性匹配策略

该技术研究的关键在于节点的属性，以形成维护属性映射表，实现动态迁移跨链节点的跨链属性匹配策略。

2）基于机器学习区块链动态迁移跨链节点行为建模

该技术研究的关键在于节点的行为特征提取，基于行为特征聚类，实现基于机器学习区块链动态迁移跨链节点行为建模。

**· 内容二：设计高效的多级权限管理及监督方案**

1）构建基于联盟链动态迁移跨链节点的信任网络多级认证

该技术研究的关键在于证书过滤恶意节点，基于定时审查节点证书方案。实现基于区块链动态迁移跨链节点的信任网络多级认证。

2）构建基于联盟链动态迁移跨链节点的积极性评估模型

该技术研究的关键在于审查用户历史信息表征，构建用户可信度量模型。实现基于联盟链动态迁移跨链节点的积极性评估模型。

**3.2.1.3 任务各参与单位具体分工**

本任务的主要研究工作包括（1）区块链节点多级权限管理及监督方法；（2）研究动态迁移的跨链节点权限分级技术。

本任务由西安电子科技大学承担完成。承担指标完成1项专利和1项新技术。

**3.2.1.4 任务研究进度安排**

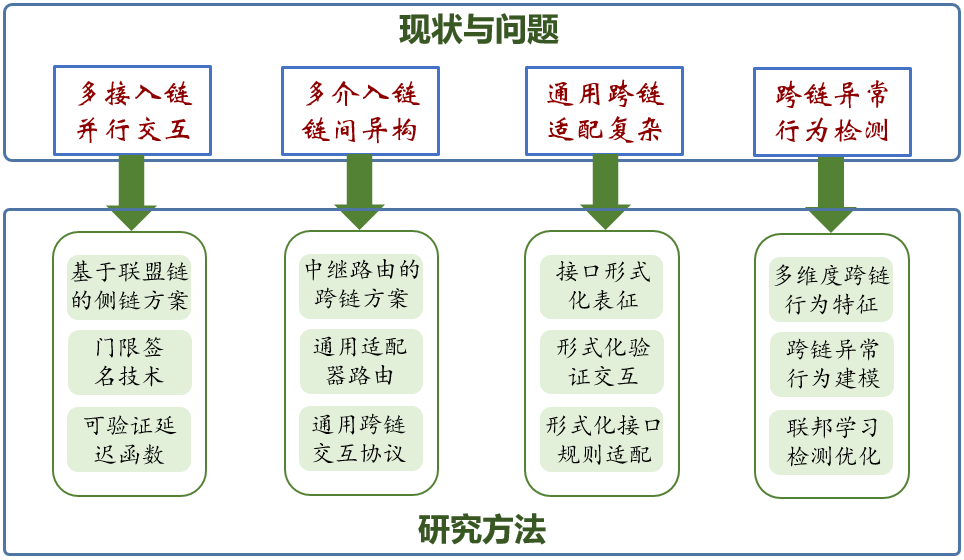
根据项目任务书的计划，任务研究的年度进度安排如下表所示

|  |  |  |  |
| --- | --- | --- | --- |
| **年度** | **任务** | **考核指标** | **成果形式** |
| 2020年11月-2021年6月 | 区块链节点多级权限管理及监督方法 | 实现跨链接入环节的多级认证机制 | 完成1项专利和1项新技术 |
| 2020年11月-2023年10月 | 研究动态迁移的跨链节点权限分级技术 | 实现动态调整的节点权限管理机制 |

3.2.2 技术路线二：异构多态的分布式跨链监管技术

**3.2.2.1 研究思路**

当前物流行业的区块链系统中需要政府部门的监管，而拥有复杂场景和信息的物流环境下，部门跨链监管是未来发展的方向，异构多态的分布式跨链监管技术主要包括多链安全交互技术、以链治链的跨链监管架构。目前国际上各大政府组织和学术研究团队已经对区块链跨链交易技术方面取得了不俗的成就。然而，在多链交互、链间异构、跨链适配、跨链监管的复杂物流环境下，实现安全的“以链治链”的跨链监管架构等方面仍然面临着挑战。  
 为此，面向不同的区块链业务场景下的异构多态的分布式跨链监管技术（对应任务2），通过多模态区块链交易场景下，分析用户敏感数据的类型以及敏感程度，结合同态加密或者保序加密等安全防护机制，研究可定制的授权安全交互和链间安全隔离方案；通过机器学习技术，构建跨链异常行为模型，同时对比部分已知恶意节点信息，并考虑采用联邦学习机制或改进机器学习解释流程，对学习后的异常行为模型在安全性方面和效率方面进行优化，提高跨链异常行为识别的准确率和隐私性。为基于区块链的物流行业提供安全的跨链监管交互机制，同时为边云结合的分布式监管协同机制（任务3）提供相应的技术支持。



**图7 任务二研究思路**

**3.2.2.2 技术方案**

研究包括两项内容，分别是“区块链跨链安全交互技术”、“以链治链”跨链异常监管架构。第一项内容拟通过基于联盟链的侧链方案和中继路由的跨链方案，进而通过门限签名技术和通用适配器路由技术，实现可验证延迟函数和通用跨链交互协议。第二项内容拟通过接口形式化表征和多维度跨链行为特征，进而实现形式化验证交互和跨链异常行为建模，实现形式化接口规则适配和联邦学习检测优化。

****

**图8 任务二技术路线**

下面依次展开说明两项研究内容的技术方案。

**· 内容一：区块链跨链安全交互技术**

1）构建可验证延迟函数

该技术研究的关键在于基于联盟链的侧链方案，通过门限签名技术，实现可验证延迟函数。

2）设计通用的跨链交互协议

该技术研究的关键在于中继路由的跨链方案设计，基于通用适配器路由，实现通用跨链交互协议。

**· 内容二：“以链治链”跨链异常监管架构**

1）构建形式化接口规则适配

该技术研究的关键设计接口形式化表征，基于形式化验证交互方案。实现形式化接口规则适配方案。

2）构建联邦学习检测优化

该技术研究的关键在于多维度跨链行为特征监管，针对跨链异常行为建模。实现联邦学习检测优化方案。

**3.2.2.3 任务各参与单位具体分工**

本任务的主要研究工作内容包括（1）区块链跨链安全交互技术；（2）“以链治链”跨链监管协同架构

本任务由西安电子科技大学承担完成。承担指标完成2篇论文，2项专利，1项软著，1个原型验证系统。

**3.2.2.4 任务研究进度安排**

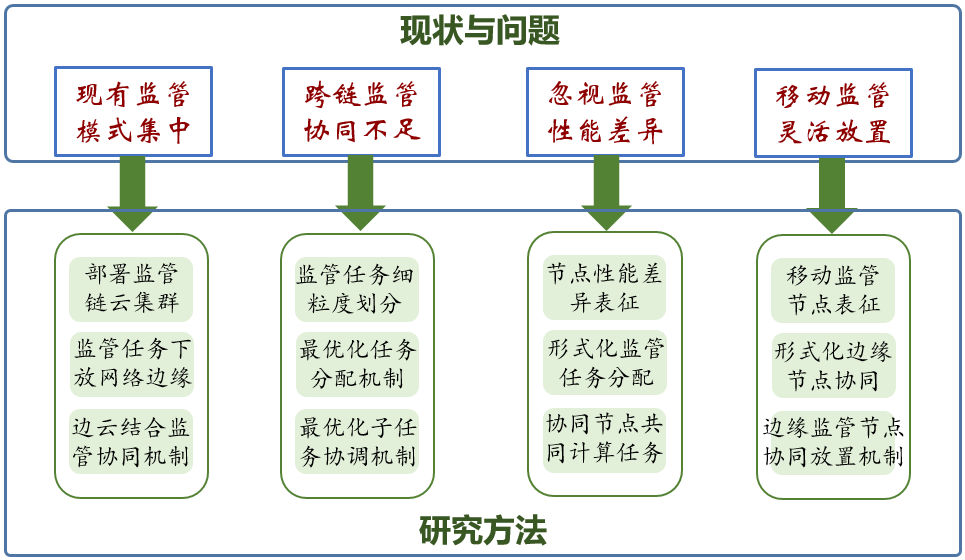
根据项目任务书的计划，任务研究的年度进度安排如下表所示

|  |  |  |  |
| --- | --- | --- | --- |
| **年度** | **任务** | **考核指标** | **成果形式** |
| 2020年11月-2021年10月 | 区块链跨链安全交互技术 | 支持协同跨链峰值吞吐量≥500TPS | 完成2篇论文，2项专利，1项软著，1个原型验证系统。 |
| 2020年11月-2021年10月 | ”以链治链“跨链监管协同架构 | 支持监管协同跨链平均延迟≤500ms |

3.2.3 技术路线三：边云结合的跨链监管协同机制

**3.2.3.1 研究思路**

当前物流行业的区块链系统中需要多个部门的联合监管，而拥有复杂场景和海量数据的物流环境下，多部门联合跨链监管是未来发展的方向，边云结合的跨链监管协同机制主要包括面向边缘计算的边云结合任务协同研究，移动监管节点放置协同技术研究。目前国际上各大政府组织和学术研究团队已经对云计算中心监管方面取得了不俗的成就。然而，在分布式监管、监管协同、节点放置策略、节点灵活性的多部门监管的物流环境下，实现边云结合的跨链监管协同仍然面临着挑战。  
 为此，面向不同的区块链业务场景下的边云结合的跨链监管协同机制（对应任务3），对面向不同业务跨链需求以及同构/异构链的监管差异，采用中继和哈希锁定等技术，实现多模态的跨链交互授权；在不同业务场景下，分析交易对象、交易模式、交易数据之间内在关联和差异，使用同态加密和匿名支付等技术，研究面向不可信场景的链间安全隔离技术，实现跨链交互的安全性和隐私性保护；针对分布式区块链场景复杂、节点众多的特点，面向不同粒度的监管需求，使用最优化技术研究边云结合监管节点放置和协同机制，实现监管任务执行的低延迟和高吞吐量。为基于区块链的物流行业提供通用可扩展的跨链监管协同机制，同时为分布式跨链监管机制（任务2）提供相应的技术支持。



**图9 任务三研究思路**

**3.2.3.2 技术方案**

研究包括两项内容，分别是“边云结合的任务协同研究”、“移动监管节点放置协同技术研究”。第一项内容拟通过监管任务细粒度划分和节点性能差异表征，进而实现最优化任务分配机制和形式化监管任务分配，实现最优化子任务协调机制和协同节点共同计算任务。第二项内容拟通过构部署监管链云集群，进而实现监管任务下放网络边缘，实现边云结合监管协同机制。



**图10 任务三技术路线**

下面依次展开说明两项研究内容的技术方案。

**· 内容一：面向边缘计算的分布式任务放置协同方法**

1）构建最优化子任务协调机制

该技术研究的关键在于监管任务细粒度划分，设计最优化任务分配机制。实现最优化子任务协调机制。

2）构建协同节点共同计算任务

该技术研究的关键在于审查节点性能差异表征，通过形式化监管任务分配。实现协同节点共同计算任务。

**· 内容二：移动监管节点放置协同技术研究**

1）构建边云结合的监管任务协同机制

该技术研究的关键在于部署监管链云集群，通过监管任务下放网络边缘，实现边云结合监管协同机制。

2）边缘监管节点协调放置机制

该技术研究的关键在于审查移动监管节点表征，通过形式化边缘节点协同。实现边缘监管节点协同放置机制。

**3.2.3.3 任务各参与单位具体分工**

本任务的主要研究工作内容包括（1）面向边缘计算的分布式任务放置协同方法（2）边云结合任务协同研究；（3）分布式任务放置协同技术研究

本任务由西安电子科技大学承担完成。承担指标完成2篇论文，1项专利，1项软著，1个原型验证系统。

**3.2.3.4 任务研究进度安排**

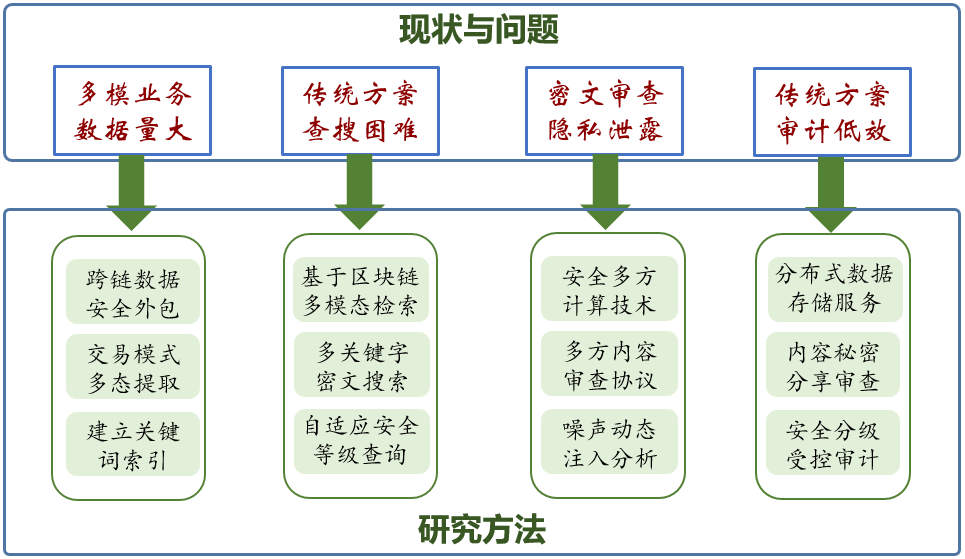
根据项目任务书的计划，任务研究的年度进度安排如下表所示

|  |  |  |  |
| --- | --- | --- | --- |
| **年度** | **任务** | **考核指标** | **成果形式** |
| 2021年11月-2022年10月 | 面向边缘计算的分布式任务放置协同方法 | 支持监管协同节点≥2个 | 完成2篇论文，1项专利，1项软著，1个原型验证系统。 |
| 2022年11月-2023年10月 | 移动监管节点放置协同技术研究 | 支持接入业务链不少于2条 |

3.2.4 技术路线四：精准高效的密态内容审计方法

**3.2.4.1 研究思路**

当前物流行业的联盟链系统中需要保护个人隐私和数据审计，而拥有复杂场景和海量数据的物流环境下，密态内容审计是未来发展的方向，精准高效的密态内容审计方法主要包括研究加密数据搜索和查询技术和完成加密数据分析研究。目前国际上各大政府组织和学术研究团队已经对密态审计方面取得了不俗的成就。然而，在海量数据、安全搜查、隐私保护、高效审计的复杂物流环境下，实现精准高效的密态内容审计等方面仍然面临着挑战。  
 为此，面向不同的区块链业务场景下的精准高效的密态内容审计（对应任务4），针对分布式跨链情形下密态内容难于审计的问题，拟研究链上加密数据的搜索与查询技术，实现丰富的语义搜索、自适应安全等级的加密搜索、支持数据动态更新、前向和后向安全，为快速准确的海量敏感数据密文搜索创造理论基础；拟研究链上加密数据的统计与分析技术，实现复杂计算问题的求解和支持噪声动态注入的链上数据统计分析。进一步研究多种隐私保护机制下安全性、效率和分析结果精确性之间的内联关系，以满足监管方对不同审计任务的需求。为基于区块链的物流行业提供精准高效的密态内容审计机制，同时为分布式跨链监管机制（任务2）和边云结合的跨链监管协同机制（任务3）提供相应的技术支持。



**图11 任务四研究思路**

**3.2.4.2 技术方案**

研究包括两项内容，分别是“跨链密文搜索和查询技术”、“跨链密文审计”。第一项内容拟通过构建跨链数据安全外包和设计基于区块链多模态检索，进而实现交易模式多态提取和多关键字密文搜索，实现建立关键词索引和自适应安全等级查询。第二项内容拟通过安全多方计算技术和分布式数据存储服务，进而设计多方内容审查协议和内容秘密分享审查协议，实现噪声动态注入分析方案和安全分级受控审计方案。



**图12 任务四技术路线**

下面依次展开说明两项研究内容的技术方案。

**· 内容一：跨链密文搜索和查询技术**

1）构建关键词索引技术

该技术研究的关键在于跨链数据安全外包，通过交易模式多态提取技术，实现关键词索引策略。

2）构建自适应安全等级查询

该技术研究的关键在于设计区块链多模态检索，通过多关键字密文搜索技术，实现自适应安全等级查询。

**· 内容二：跨链密文审计**

1）构建噪声动态注入分析

该技术研究的关键在于安全多方计算技术，基于多方内容审查协议方案。实现噪声动态注入分析。

2）构建安全分级受控审计

该技术研究的关键在于分布式数据存储服务，设计内容秘密分享审查方案。实现安全分级受控审计。

**3.2.4.3 任务各参与单位具体分工**

本任务的主要研究工作内容包括（1）研究跨链密文搜索和查询技术；（2）完成跨链密文审计研究；

本任务由武汉大学承担完成。承担指标完成2篇论文，1项专利，1项软著。

**3.2.4.4 任务研究进度安排**

根据项目任务书的计划，任务研究的年度进度安排如下表所示

|  |  |  |  |
| --- | --- | --- | --- |
| **年度** | **任务** | **考核指标** | **成果形式** |
| 2020年11月-2021年10月 | 跨链密文搜索和查询技术 | 实现自适应安全的多关键字密文搜查机制 | 完成2篇论文，1项专利，1项软著。 |
| 2021年11月-2022年10月 | 跨链密文审计 | 实现基于安全多方计算的密文审计机制、以及支持噪声动态注入的跨链数据统计分析系统 |

## 3.3．课题经费安排及自筹经费落实方案

**（1）课题经费预算总表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 预算科目名称 | 合计 | 中央财政专项资金 | 其他来源资金 |
| （1） | （2） | （3） | （4） |
| 1 | 一、经费支出 | 222 | 222 |  |
| 2 | （一）直接费用 | 189 | 189 |  |
| 3 | 1、设备费 | 22.5 | 22.5 |  |
| 4 | （1）购置设备费 | 22.5 | 22.5 |  |
| 5 | （2）试制设备费 |  |  |  |
| 6 | （3）设备改造费 |  |  |  |
| 7 | （4）设备租赁费 |  |  |  |
| 8 | 2、劳务费、专家咨询费、会议/差旅/国际合作交流费、其他支出 | 135.4 | 135.4 |  |
| 9 | （1）劳务费 | 56.2 | 56.2 |  |
| 10 | （2）专家咨询费 | 16.6 | 16.6 |  |
| 11 | （3）会议/差旅/国际合作交流费 | 62.6 | 62.6 |  |
| 12 | （4）其他支出 |  |  |  |
| 13 | 3、材料费、测试化验加工费、燃料动力费、出版/文献/信息传播/知识产权事务费 | 31.1 | 31.1 |  |
| 14 | （1）材料费 | 3.3 | 3.3 |  |
| 15 | （2）测试化验加工费 |  |  |  |
| 16 | （3）燃料动力费 |  |  |  |
| 17 | （4）出版/文献/信息传播/知识产权事务费 | 27.8 | 27.8 |  |
| 18 | （二）间接费用 | 33 | 33 |  |
| 19 | 二、经费来源 | 222 | 222 |  |
| 20 | （一）中央财政资金 | 222 | 222 | / |
| 21 | （二）其他来源资金 |  | / |  |
| 22 | 1、地方财政拨款 |  | / |  |
| 23 | 2、单位自筹资金 |  | / |  |
| 24 | 3、其他渠道获得资金 |  | / |  |

**（2）第一阶段经费预算表：2020.11-2021.10**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 预算科目名称 | 合计 | 中央财政资金 | 其他来源资金 |
| （1） | （2） | （3） | （4） |
| 1 | 一、经费支出 |  |  |  |
| 2 | （一）直接费用 | 73.8 | 73.8 |  |
| 3 | 1、设备费 | 7.5 | 7.5 |  |
| 4 | （1）购置设备费 | 7.5 | 7.5 |  |
| 5 | （2）试制设备费 | 0 | 0 |  |
| 6 | （3）设备改造费 | 0 | 0 |  |
| 7 | （4）设备租赁费 | 0 | 0 |  |
| 8 | 2、材料费 | 1.1 | 1.1 |  |
| 9 | 3、测试化验加工费 | 0 | 0 |  |
| 10 | 4、燃料动力费 | 0 | 0 |  |
| 11 | 5、差旅/会议/国际合作与交流费 | 20.8 | 20.8 |  |
| 12 | 6、出版/文献/信息传播/知识产权事务费 | 9.2 | 9.2 |  |
| 13 | 7、劳务费 | 18.7 | 18.7 |  |
| 14 | 8、专家咨询费 | 5.5 | 5.5 |  |
| 15 | 9、其他支出 | 0 | 0 |  |
| 16 | （二）间接费用 | 11 | 11 |  |

**（3）第二阶段经费预算表：2022.11-2023.10**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 预算科目名称 | 合计 | 中央财政资金 | 其他来源资金 |
| （1） | （2） | （3） | （4） |
| 1 | 一、经费支出 |  |  |  |
| 2 | （一）直接费用 | 73.8 | 73.8 |  |
| 3 | 1、设备费 | 7.5 | 7.5 |  |
| 4 | （1）购置设备费 | 7.5 | 7.5 |  |
| 5 | （2）试制设备费 | 0 | 0 |  |
| 6 | （3）设备改造费 | 0 | 0 |  |
| 7 | （4）设备租赁费 | 0 | 0 |  |
| 8 | 2、材料费 | 1.1 | 1.1 |  |
| 9 | 3、测试化验加工费 | 0 | 0 |  |
| 10 | 4、燃料动力费 | 0 | 0 |  |
| 11 | 5、差旅/会议/国际合作与交流费 | 20.8 | 20.8 |  |
| 12 | 6、出版/文献/信息传播/知识产权事务费 | 9.2 | 9.2 |  |
| 13 | 7、劳务费 | 18.7 | 18.7 |  |
| 14 | 8、专家咨询费 | 5.5 | 5.5 |  |
| 15 | 9、其他支出 | 0 | 0 |  |
| 16 | （二）间接费用 | 11 | 11 |  |

**（4）第三阶段经费预算表：2019.12-2020.11**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 预算科目名称 | 合计 | 中央财政资金 | 其他来源资金 |
| （1） | （2） | （3） | （4） |
| 1 | 一、经费支出 |  |  |  |
| 2 | （一）直接费用 | 74.4 | 74.4 |  |
| 3 | 1、设备费 | 7.5 | 7.5 |  |
| 4 | （1）购置设备费 | 7.5 | 7.5 |  |
| 5 | （2）试制设备费 | 0 | 0 |  |
| 6 | （3）设备改造费 | 0 | 0 |  |
| 7 | （4）设备租赁费 | 0 | 0 |  |
| 8 | 2、材料费 | 1.1 | 1.1 |  |
| 9 | 3、测试化验加工费 | 0 | 0 |  |
| 10 | 4、燃料动力费 | 0 | 0 |  |
| 11 | 5、差旅/会议/国际合作与交流费 | 21 | 21 |  |
| 12 | 6、出版/文献/信息传播/知识产权事务费 | 9.4 | 9.4 |  |
| 13 | 7、劳务费 | 18.8 | 18.8 |  |
| 14 | 8、专家咨询费 | 5.6 | 5.6 |  |
| 15 | 9、其他支出 | 0 | 0 |  |
| 16 | （二）间接费用 | 11 | 11 |  |

# 课题组织管理机制

## 4.1课题内部管理机构和管理制度

4.1.1 实施课题负责人和课题负责单位法人双责任制

本课题承担单位西安电子科技大学对课题进行全面主持、协调和管理，并开展科研工作。落实课题承担单位法人责任，充分发挥课题承担单位在国家科技计划以及国家科技重大专项过程中的组织、协调、服务和监督作用。通过建立一流的工作团队、目标明确和绩效导向的管理制度、规范和经费管理制度，保证课题如期、高质、高效达到预定目标。

课题负责人全面负责并协调整个课题，同时强调课题负责单位和课题参与单位的法人责任。课题负责单位监督课题负责人按照项目的总体要求和签订的任务书管理并执行课题，并与项目负责单位协同，对课题实施有效管理。

4.1.2 建立课题任务督查和目标明确、绩效导向的管理制度

课题实行严格的过程管理，由课题管理小组负责,对课题执行情况进行督查。按照管理办法与课题参与单位签订约束合同，明确课题各参与单位的研究内容、研究进度、考核指标、预算安排、财务审计等责任和义务。课题承担单位严格按照职责开展工作，由课题管理小组负责落实国家及部门相关政策、制度、管理办法、匹配经费和监督检查。

根据既定的研究方案和与科技部签订的任务书,课题对各任务进行动态管理和绩效考评，有计划、有步骤的在关键时间节点对各任务推进的进度、产生的成果、完成的指标等进行考核与评估，根据考核与评估的结果，对各任务的执行情况进行综合绩效考评。将绩效考评结果反馈给各任务，并与各任务负责人(单位)进行充分的讨论与沟通，发现问题并及时整改。

4.1.3 管理人员分工

本课题将成立课题管理小组，组织、管理、监督课题和各任务的执行。课题管理小组，成员包括课题负责人、各任务负责人、课题骨干力量等。课题负责人和各任务负责人承担对课题和各任务的领导和监督职能，任务的具体实施由各任务负责人负责,课题和任务负责人接受课题和任务小组的领导与监督。项目管理小组和任务小组保持日常的沟通和联系，形成有机的工作整体，共同确保课题各任务的顺利执行。

## 4.2课题实施过程中的交流及检查机制

4.2.1 课题内部数据共享、资源共享机制

为了加强课题内部信息流通的流畅，促进数据共享、资源共享，本课题拟采取以下措施：

综合执行课题简报制度、每月及每周会议制度，加强课题内部和各任务之间的沟通、交流和讨论。执行课题简报制度，报告各任务的研究进展以及已获得的研究成果。根据需要，组织必要交流会，除此之外，还将借助学术会议、专业组织例会等机会增加课题组沟通和交流的频次。

课题及各任务建立严格的工作汇报制度，每月召开例会汇报讨论课题各任务进度，进行充分有效的交流与沟通，并及时将研究进程对项目进行汇报。

4.2.2 建立课题例会制度

课题例会制度如下：

(1) 课题中各任务小组计划每周一次进行例会，讨论任务完成情况

(2) 课题组计划每月一次进行例会，汇报讨论课题进度；

(3) 根据课题需要召开课题启动会、方案研讨会、中期研讨会、年度检查会、课题预验收会等会议。

4.2.3 对课题的执行情况进行第三方评估

除了对课题的执行情况进行自查自检外，引入第三方评估制度，对课题的进度、产生的成果、完成的指标、示范工程落实情况等进行独立、科学、公正的第三方评估。评估方可选择具有资质的科研咨询机构或由相关专家组成的独立专家咨询委员会。第三方评估报告是评价课题执行情况的重要依据，课题将根据第三方评估报告对课题执行情况进行及时的查缺补漏，确保课题平稳有序的推进，最终顺利实现研究目标并完成各项考核指标。

## 4.3课题实施过程中的风险分析与控制

课题牵头单位西安电子科技大学，课题参与单位武汉大学均为第一批国家网络安全示范学院，分别在网络体系结构、密码学、信息安全等领域具有深厚的研究基础；课题负责人姜晓鸿教授承担的国家重点研发计划课题，研究了基于区块链技术的“智能服务交易运行机理及性能优化技术”，在面向智能服务交易的应用背景中熟悉了本项目需要的研究体系、研究内容和测试平台；王骞教授是2018 国家优秀青年科学基金获得者，在本课题中牵头密文数据审计和跨链共识算法两个最为困难的研究任务，与他应用密码学和数据安全与隐私领域的研究擅长一致。所以本项目的技术风险、市场风险、政策风险较低。

**表3 课题风险防控预案**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 风险类别 | 风险内容 | 风险 发生 可能 性 | 涉及的研发任务 | 预防风险或减少风险损失的措施 |
| 1 | □技术风险 ☑市场风险 □政策风险 □其他 | 在安全领域或信息领域形成技术集成解决方案1项 | □高 □中  ☑低 | 应用生态 | 借鉴国外先进技术社区的经验，产学研用结合，保持技术的开放性和互通性；提高社区技术服务质量；成立产业联盟和技术联盟，吸引政府、厂商、企业等各类用户；提高社区用户的参与性和活跃性 |
| 2 | ☑技术风险 □市场风险 □政策风险 □其他 | 3年内累计制定国家、行业或核心企业标准3项 | □高 □中  ☑低 | 标准制定 | 由于标准制定到批准时间较长，为保证顺利完成标准的制定，将联合或参与相关标准制定组，完成有关标准制定 |
| 3 | □技术风险 □市场风险 □政策风险 ☑其他 | 合作单位人事变更、优先次序变化，以至于无法完成事先的任务分工 | □高 □中  ☑低 | 演示与验证系统 | 如果现有参与企业合作受到阻碍，多个其他相关企业表示有兴趣，可选择新合作单位。 |

# 课题成果呈现形式及测试方法

## 5.1课题成果呈现形式

课题成果将建立“以链治链”的跨链协同监管体系，并应用在物流行业的转型升级中，形成可复制的经验、专利池、协议、规范与标准，建设完善具有中国特色的物流行业跨链协同监管生态系统。课题成果主要以方法机制、原型系统、协议标准、文章专利及报告的方式呈现。

1. **课题将形成方法机制4套，包括：**

·一套面向物流行业的“以链治链”新型协同监管体系，支持监管协同节点≥2个，接入业务链不少于2条，跨链平均延迟≤500ms

·一套跨链节点权限分级技术

·一套边云结合的跨链监管协同技术，支持协同跨链峰值吞吐量≥500tps

·一套跨链密态内容审计技术

1. **课题将建立原型验证系统1套，包括：**

·跨链协同原型验证系统，包括跨链安全交互子系统和边云结合任务协同子系统

1. **课题将完成相关标准1项，包括：**

·一项跨链监管协同标准

1. **课题将形成专利池、论文以及软件著作权，包括：**

·专利5项、论文6篇、软件著作权5项

1. **项目最终将形成系列研究报告，包括：**

·课题内部技术报告、课题年度技术进展报告、课题中期技术进展报告、课题最终科技报告

## 5.2定量指标的测试与检验方法

5.2.1 考核指标总表

课题成果与对应考核指标细化具体如下表所示。

**课题目标、成果与考核指标表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 课题目标1 | 成果名称 | 成果  类型 | 考核指标3 | | | | 考核方式（方法）及评价手段5 |
| 指标  名称 | 立项时已有指标值/状态 | 中期指标值/状态4 | 完成时指标值/状态 |
| 旨在利用中继机制、哈希锁定、同态机密、匿名传输等理论与方法研究跨链监管协同体系与方法，解决 现有监管方法跨链交互能力弱、协同性差、效率低等问题 | 1：“以链治链”的跨链协同监管关键技术 | ☑ 新技术  ☑ 新方法 | 指标1.1  跨链节点权限分级 | 无 | 综合分析业务场景特征和用户角色特征，分析面向特定场景的用户权限需求 | 对业务需求和用户特征进行综合考量，对用户角色进行分级，结合用户可信度与积极性度量，支持部分用户权限的提升 | 形成技术报告/公开发表论文（录用或检索证明）/申请技术发明专利（受理通知书或授权通知书） |
| 指标1.2  跨链监管技术 | 无 | 初步构建分布式跨链监管方案 | 在“以链治链”框架下，实现多链之间的授权交互和链间隐私保护 |
| 指标1.3  跨链监管协同 | 无 | 调研现有跨链协同方案，分析跨链协同特征 | 在“以链治链”框架下，实现分布式跨链监管协同 |
| 指标1.4  密态内容审计 | 无 | 初步构建密态内容审计框架 | 在“以链治链”框架下，实现密态内容审计 |
| 2：“以链治链”的跨链标准 | ☑ 标准 | 指标2  跨链标准 | 无 | 调研现有跨链方案，分析跨链技术共性特征 | 在“以链治链”框架下，提交  国家或行业标准建议草案1项 | 国家或行业标  准正式立项批  复文件 |
| 3：“以链治链”的跨链协同监管知识产权 | ☑ 论文  ☑ 发明专利  ☑ 其他：软件著作权 | 指标3.1  跨链节点权限分级 | 无 | 跨链场景特征分析和节点权限的需求分析 | 完成专利一项 | 公开发表论文（录用或检索证明）/申请技术发明专利（受理通知书或授权通知书）/申请软件著作权(登记证书) |
| 指标3.2  跨链监管技术 | 无 | 累计专利一项 | 完成专利两项、软著一项、论文两篇 |
| 指标3.3  跨链监管协同 | 无 | 监管协同的场景分析，协同对象、协同目标的特征分析 | 完成专利一项、软著一项、论文两篇 |
| 指标3.4  密态内容审计 | 无 | 累计专利一项 | 完成专利一项、软著一项、论文两篇 |
| 4：“以链治链”的跨链协同原型验证程序 | ☑ 实验系统 | 指标4  跨链协同原型验证系统 | 无 | 初步构建“以链治  链”框架下的跨链协  同原型验证程序，实  现节点权限分级管理  功能，并完成跨链安  全交互的调研和分析 | 完成“以链治链”框架下的跨  链协同原型验证程序，实现节  点权限分级、跨链安全交互以  及分布式协同等功能，系统指  标如下：支持不少于 2个监管  节点协同；支持不少 2条业务  链的跨链交易；除业务链本身  的交易延迟，跨链过程的平均  延迟 500ms；峰值跨链吞吐量  500tps | 第三方检测机构的测评报告 |
| **科技报告考核指标** | **序号** | **报告类型** | **数量** | **提交时间** | | | **公开类别**  **及时限** |
| 1 | 课题年度技术进展报告 | 1 | 2021年11月 | | | 延期公开2年 |
| 2 | 课题中期技术进展报告 | 1 | 2022年7月 | | | 延期公开2年 |
| 3 | 课题年度技术进展报告 | 1 | 2022年11月 | | | 延期公开2年 |
| 4 | 课题最终科技报告 | 1 | 2023年10月 | | | 延期公开2年 |
| 其他目标与考核指标（对于难以采取上述表格细化的项目目标及其考核指标，可在此细化填写。） | | | | | | | |

5.2.2 定量指标的测试与检验方法

课题针对跨链协同监管的关键技术、系统平台和应用示范分别设置不同的考核指标的测试与检验方法。在关键技术方面，针对学术论文，通过录用通知或见刊的方式来考核；针对专利，通过专利受理号和授权号来审核；针对软件著作权，通过软件著作权证书来审核。在系统平台和应用示范方面，针对跨链安全交互系统的交易吞吐量指标，通过现成检验方式进行考核；针对边云结合任务协同系统的协同节点数，接入业务链数，跨链延迟指标，通过现场逐项检验方式进行考核。

除了上述学术论文指标完成情况以论文正式发表或录用通知为准、知识产权指标的完成情况以专利授权证书或受理通知为准、软件著作权的完成情况以软件著作权证书或第三方测试报告为准以外，其它指标中具有一定的方法或技术细节的，其测试与检验方式分别说明如下：

* **关键技术指标方面：**

指标3.2：跨链协同监管可扩展性度量。此项指标着眼于跨链监管领域复杂的多业务链网络环境，研究基于侧链/中继路由的通用跨链监管方法。根据课题任务书的指标表述要求，在项目结题时，在保证完成任务书指标的前提下，支持监管协同节点扩展不少于2个，接入的业务链不少于2条。针对此目标，课题计划尝试整合基于联盟链的侧链跨链模型和跨链中继路由模型，建立支持多种异构链通用跨链监管模型，实现跨链监管系统的通用扩展。指标数值的确认将通过运行跨链协同原型验证系统，通过改变系统协同监管节点数量，检验方法为我们支持至少2个监管节点协同，由第三方检测机构现场确认。以及通过改变加入系统的业务链条数，检验方法为我们支持至少2条业务链的跨链交易，由第三方检测机构现场确认。同时具备学术论文或发明专利等呈现形式。

* **系统平台和应用示范指标方面：**

指标4：跨链监管协同通信平均延迟不超过500ms。该指标旨在保证跨链协同监管过程中监管内容的及时性、可信性。根据课题任务书的指标表述要求，在项目结题时，支持跨链协同监管平均通信延迟不超过500ms。针对此目标，课题计划整合基于云监管节点的边缘节点协同机制和基于云监管集群的移动监管节点放置机制，最优化协同监管通信成本，建立支持低延时的跨链协同监管模型，实现协同监管的实时可靠。指标数值的确认将通过运行跨链协同原型验证系统，通过跨链交易延迟测试脚本，计算出k次跨链过程的平均延迟，检验方法为我们支持跨链协同监管平均通信延迟不超过500ms，由第三方检测机构现场确认。同时具备学术论文或发明专利等呈现形式。

指标4：跨链协同监管峰值跨链吞吐量不少于500tps。该指标旨在保证跨链协同监管过程中大规模并行监管情况下的系统稳定性。根据课题任务书的指标表述要求，在项目结题时，支持峰值跨链吞吐量不少于500tps。针对此目标，课题计划基于通用的跨链通信协议对监管系统性能进行优化，建立支持高并发、高吞吐的跨链协同监管模型，实现监管交易的海量并发。指标数值的确认将通过运行跨链协同原型验证系统，通过跨链交易性能测试脚本，计算出k次跨链的峰值吞吐量，检验方法为我们支持峰值跨链吞吐量不少于500tps，由第三方检测机构确认。同时具备学术论文或发明专利等呈现形式。