

课题编号：2022YFB2702505

密 级：公开

国家重点研发计划
课题任务书

课题名称：链上数字内容的全链路安全审计与风险处置技术

所属项目：新型链上数字内容的安全智能监管关键技术

所属专项：区块链

项目牵头承担单位：中国科学院信息工程研究所

课题承担单位：北京大学

课题负责人：谢安明

执行期限：2022 年 11 月 至 2025 年 10 月

中华人民共和国科学技术部制

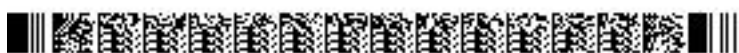
2022 年 12 月 02 日

0003YF 2022YFB2702505 2022-12-02 09:40:13



填写说明

- 一、任务书甲方即项目牵头承担单位，乙方即课题承担单位。
- 二、任务书通过“国家科技计划管理信息系统公共服务平台”，按照系统提示在线填写。
- 三、任务书中的单位名称，请按规范全称填写，并与单位公章一致。
- 四、任务书要求提供乙方与所有参加单位的合作协议，需对原件进行扫描后在线提交。
- 五、任务书中文字须用宋体小四号字填写。
- 六、凡不填写内容的栏目，请用“无”表示。
- 七、乙方完成任务书的在线填写，提交甲方审核确认后，用 A4 纸在线打印、装订、签章。一式八份报项目牵头承担单位签章，其中课题承担单位一份，课题负责人一份，作为项目任务书附件六份。
- 八、如项目下仅设一个课题，课题任务书只需填报课题预算部分。
- 九、涉密课题请在“国家科技计划管理信息系统公共服务平台”下载任务书的电子版模板，按保密要求离线填写、报送。
- 十、《项目申报书》和《项目任务书》是本任务书填报的重要依据，任务书填报不得降低考核指标，不得自行对主要研究内容作大的调整。《项目申报书》、《项目任务书》和本任务书将共同作为课题过程管理、综合绩效评价（验收）和监督评估的重要依据。



课题基本信息表

课题名称		链上数字内容的全链路安全审计与风险处置技术			
课题编号		2022YFB2702505			
所属项目		新型链上数字内容的安全智能监管关键技术			
所属专项		区块链			
密级		■公开 □秘密 □机密		单位总数	2
课题类型		□基础前沿 ■重大共性关键技术 □应用示范研究 □其他			
课题活动类型		□基础前沿 ■应用研究 □试验发展			
课题研究 所属学科		计算机科学技术 计算机软件			
课题成果应用的主要国民经济行业		信息传输、软件和信息技术服务业 软件和信息技术服务业 软件开发			
课题的社会 经济目标		社会发展和社会服务 科技发展			
经费预算		总需求 210.00 万元，其中中央财政专项资金需求 210.00 万元			
课题周期节点		起始时间	2022 年 11 月	结束时间	2025 年 10 月
		实施周期	共 36 个月	预计中期时间点	2024 年 04 月
课题 承担 单位	单位名称	北京大学		单位法定 代表人姓名	郝平
	单位性质	大专院校		组织机构代码	12100000400002259P
	单位主管部门			隶属关系	中央
	单位所属地区	北京市		地市（市、自 治州、盟）	北京市 海淀区
	通信地址	北京市海淀区颐和园路 5 号		邮政编码	100871
	单位开户名称	北京大学			
	开户银行 （全称）	中国工商银行股份有限公司 北京海淀西区支行营业室		汇入地点	北京市 北京 市



	银行账号	0200004509089131151		银行机构代码	102100000458	
课题负责人	姓 名	谢安明	性 别	<input checked="" type="checkbox"/> 男 <input type="checkbox"/> 女	出生日期	1977-01-18
	证件类型	身份证	证件号码	362429197701183816		
	所在单位	北京大学				
	最高学位	<input checked="" type="checkbox"/> 博士 <input type="checkbox"/> 硕士 <input type="checkbox"/> 学士 <input type="checkbox"/> 其他				
	职 称	<input type="checkbox"/> 正高级 <input checked="" type="checkbox"/> 副高级 <input type="checkbox"/> 中级 <input type="checkbox"/> 初级 <input type="checkbox"/> 其他			职 务	无
	电子邮箱	xieanming@pku.edu.cn		移动电话	13366128077	
课题联系人	姓 名	关志	电子邮箱	guan@pku.edu.cn		
	固定电话	62765807	移动电话	13810631266		
	证件类型	身份证	证件号码	210202198004014258		
课题财务负责人	姓 名	王珂	电子邮箱	wangk@pku.edu.cn		
	固定电话	62765807	移动电话	18610690388		
	证件类型	身份证	证件号码	372330199006154651		
其他参与单位	序号	单位名称		单位性质	组织机构代码	
	1	中国科学院计算技术研究所		事业型研究单位	12100000400012342E	
课题参加人数	<u>18</u> 人。其中：		高级职称 <u>1</u> 人，中级职称 <u>1</u> 人，初级职称 <u>0</u> 人，其他 <u>16</u> 人；			
			博士学位 <u>2</u> 人，硕士学位 <u>0</u> 人，学士学位 <u>16</u> 人，其他 <u>0</u> 人。			
课题简介 (限 500 字以内)	<p>随着区块链应用向金融、政务、版权等诸多应用领域大步迈进，链上数字内容呈现多元化、爆发式发展，数字内容形式由单纯的加密货币交易信息扩展到多媒体信息内容，动态演化的内容生成模式提高了链上数字内容的接入与理解难度，也极大地增加了区块链应用的内容安全风险。本课题聚焦于新型链上数字内容的全链路安全审计与风险处置技术，研究多元主体链上链下协同治理模式及关键技术；针对生成数字内容的智能合约及内容本身，开展基于规则模型化的全链路安全审计与功能审计；研究风险处置区块链架构与链外屏蔽技术，最终实现对新型链上数字内容的实时自动化风险追踪与处置能力。本课题研究成果将为国家主管部门开展新型链上数字内容监管提供理论指导和技术支撑，有效提高相关安全事件的预警和处置能力，促进相关行业新型数字内容生态健康、有序发展。</p>					



一、目标及考核指标、考核方式/方法

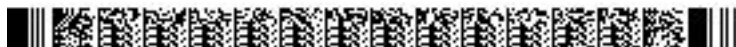
请填写下表。

课题目标、预期成果与考核指标表

课题目标 ¹	预期成果			考核指标 ²				考核方式（方法）及评价手段 ⁴	
	预期成果名称		预期成果类型	指标名称	立项时已有指标值/状态	中期指标值/状态 ³	完成时指标值/状态		
（限 500 字以内。） 本课题面向区块链应用中数字内容多元化、爆发式发展带来的内容安全风险，聚焦新型链上数字内容全链路安全审计与风险处置技术，研究多元主体链上链下协同治理模式及关键技术；针对生成数字内容的智能合约及内容本身，开展基于规则模型化的全链路安全审计与功	主要成果	1	新型数字内容链上链下联合治理架构与方案	<input type="checkbox"/> 新理论 <input type="checkbox"/> 新原理 <input type="checkbox"/> 新产品 <input type="checkbox"/> 新技术 <input checked="" type="checkbox"/> 新方法 <input type="checkbox"/> 关键部件 <input type="checkbox"/> 数据库 <input type="checkbox"/> 软件 <input type="checkbox"/> 应用解决方案 <input type="checkbox"/> 实验装置/系统 <input type="checkbox"/> 临床指南/规范 <input type="checkbox"/> 工程工艺 <input type="checkbox"/> 标准 <input type="checkbox"/> 论文 <input type="checkbox"/> 发明专利 <input type="checkbox"/> 其他_	指标 1.3 多元主体链上链下协同治理模式及关键技术	已完成国内外相关研究的调研报告	提供关于新型数字内容链上链下联合治理模式的架构与方案报告初稿 1 篇	提供关于新型数字内容链上链下联合治理模式的架构与方案报告 1 篇	方案报告通过行业协会/学会组织的同行专家评审
		2	规则模型化的全链路安全审计与功能审计工具	<input type="checkbox"/> 新理论 <input type="checkbox"/> 新原理 <input type="checkbox"/> 新产品 <input checked="" type="checkbox"/> 新技术 <input type="checkbox"/> 新方法 <input type="checkbox"/> 关键部件 <input type="checkbox"/> 数据库 <input checked="" type="checkbox"/> 软件 <input type="checkbox"/> 应用解决方案 <input type="checkbox"/> 实验装置/系统 <input type="checkbox"/> 临床指南/规范 <input type="checkbox"/> 工程工艺 <input type="checkbox"/> 标准 <input checked="" type="checkbox"/> 论文 <input checked="" type="checkbox"/> 发明专利 <input checked="" type="checkbox"/> 其他_软件_著作权_	指标 2.10 数字内容和智能合约安全审计技术 a) 支持涉及不少于 2 个区块链平台的跨函数、跨合约、跨链交易全交易流程的自定义监管规则的安全审计，智能合约平均审计时间不超过 1 分钟，评测结果误报率不超过 10%，漏报率不超过 3% b) 申报发明专利≥1 项 c) 申报软件著作权≥1 项 d) 发表论文≥1 篇	已自主研发智能合约安全分析的符号执行引擎及功能验证模块	研发规则模型化的监管规则语言和执行引擎，能够对链上数字内容及相关智能合约进行合规审计； 申报发明专利≥1 项； 申报软件著作权≥1 项	支持涉及不少于 2 个区块链平台的跨函数、跨合约、跨链交易全交易流程的自定义监管规则的安全审计，智能合约平均审计时间不超过 1 分钟，评测结果误报率不超过 10%，漏报率不超过 3%； 申报发明专利≥1 项； 申报软	编制测试方案，测试方案通过第三方专家评审论证后，由具有检测能力的第三方检测机构进行测试，并提交测试报告； 发明专利申请/授权证明文件； 软件著作权证书； 已发表论文全



能审计；研究风险处置区块链架构与链外屏蔽技术，最终实现对新型链上数字内容的实时自动化风险追踪与处置能力。 本课题研究成果将为国家主管部门开展新型链上数字内容监管提供理论指导和技术支撑，提高相关安全事件的预警和处置能力，促进相关行业新型数字内容生态健康有序发展。	3	风险处置区块链架构与链外屏蔽工具	<input type="checkbox"/> 新理论 <input type="checkbox"/> 新原理 <input type="checkbox"/> 新产品 <input checked="" type="checkbox"/> 新技术 <input type="checkbox"/> 新方法 <input type="checkbox"/> 关键部件 <input type="checkbox"/> 数据库 <input checked="" type="checkbox"/> 软件 <input type="checkbox"/> 应用解决方案 <input type="checkbox"/> 实验装置/系统 <input type="checkbox"/> 临床指南/规范 <input type="checkbox"/> 工程工艺 <input type="checkbox"/> 标准 <input checked="" type="checkbox"/> 论文 <input checked="" type="checkbox"/> 发明专利 <input checked="" type="checkbox"/> 其他_软件著作权	指标 2.11 链上信息处置技术 a) 支持对链上数字内容的可验证删改操作，支持区块链回滚规模不低于 7 天生成的区块数量，在线密码计算延迟不超过 1000 毫秒 b) 支持对于违规数字内容的受控访问以及链外屏蔽 c) 申请发明专利≥2 项 d) 申请软件著作权≥1 项	已 申 报 SM2 数字签名、SM3 密码杂凑算法并行化等与密码理论和密码应用相关的发明专利	支持对链上违规数字内容的可验证删改操作； 申请发明专利≥1 项； 申请软件著作权≥1 项	支持对链上数字内容的可验证删改操作，支持区块链回滚规模不低于 7 天生成的区块数量，在线密码计算延迟不超过 1000 毫秒；支持对于违规数字内容的受控访问以及链外屏蔽，申请发明专利≥2 项；申请软件著作权≥1 项	编制测试方案，测试方案通过第三方专家评审论证后，由具有检测能力的第三方检测机构进行测试，并提交测试报告； 发明专利申请/授权证明文件； 软件著作权证书		
			4	链上新型数字内容全链路安全审计与风险处置子系统	<input type="checkbox"/> 新理论 <input type="checkbox"/> 新原理 <input type="checkbox"/> 新产品 <input type="checkbox"/> 新技术 <input type="checkbox"/> 新方法 <input type="checkbox"/> 关键部件 <input type="checkbox"/> 数据库 <input checked="" type="checkbox"/> 软件 <input type="checkbox"/> 应用解决方案 <input checked="" type="checkbox"/> 实验装置/系统 <input type="checkbox"/> 临床指南/规范 <input type="checkbox"/> 工程工艺 <input type="checkbox"/> 标准 <input type="checkbox"/> 论文 <input type="checkbox"/> 发明专利 <input type="checkbox"/> 其他_	指标 4.5 链上新型数字内容全链路安全审计与风险处置子系统 a) 实现涉及不少于 2 个区块链平台的跨函数、跨合约、跨链交易全交易流程的自定义监管规则的全链路安全审计，实现可验证的区块链删改或回滚操作 b) 实现对违规数字内容受控访问及链外屏蔽功能	已有区块链平台开发环境和分布式系统构建环境，参与区块链与监管系统备案系统建设工作	实现跨函数、跨合约的自定义监管规则的全链路安全审计，实现可验证的区块链删改或回滚操作	实现涉及不少于 2 个区块链平台的跨函数、跨合约、跨链交易全交易流程的自定义监管规则的全链路安全审计，实现可验证的区块链删改或回滚操作，实现对违规数字内容受控访问及链外屏蔽功能	编制测试方案，测试方案通过第三方专家评审论证后，由具有检测能力的第三方检测机构进行测试，并提交测试报告
科技报告考核指标	序号		报告类型 ⁵	数量	提交时间		公开类别及时限 ⁶			
	1		课题年度执行情况报告	3	2023 年 11 月，2024 年 11 月， 2025 年 10 月		非公开			
	2		课题中期执行情况报告	1	2024 年 4 月		非公开			
	3		课题结题报告	1	2025 年 10 月		非公开			
其他目标与考核指标：无										



备注：

1. **“课题目标”**，应从以下方面明确描述：（1）研发主要针对什么问题和需求；（2）将要解决哪些科学问题、突破哪些核心/共性/关键技术；（3）预期成果；（4）成果将以何种方式应用在哪些领域/行业/重大工程等，并拟在科技、经济、社会、环境或国防安全等方面发挥何种的作用和影响。（5）所列主要成果原则上不超过5项，如有其他重要成果放在“其他”成果中表述。
2. **“考核指标”**，指相应成果的数量指标、技术指标、质量指标、应用指标和产业化指标等，其中，数量指标可以为专利、产品等的数量，论文代表作应注重质量，不以数量作为评价标准；技术指标可以为关键技术、产品的性能参数等；质量指标可以为产品的耐震动、高低温、无故障运行时间等；应用指标可以为成果应用的对象、范围和效果等；产业化指标可以为成果产业化的数量、经济效益等。同时，对各项考核指标需填写立项时已有的指标值/状态以及课题完成时要到达的指标值/状态。同时，考核指标也应包括支撑和服务其他重大科研、经济、社会发展、生态环境、科学普及需求等方面的直接和间接效益。如对国家重大工程、社会民生发展等提供了关键技术支撑，成果转让并带动了环境改善、实现了销售收入等。若某项成果属于开创性的成果，立项时已有指标值/状态可填写“无”，若某项成果在立项时已有指标值/状态难以界定，则可填写“/”。
3. **“中期指标”**，各专项根据管理特点，确定是否填写，鼓励阶段目标明确的项目课题填写中期指标。
4. **“考核方式方法”**，应提出符合相关研究成果与指标的具体考核技术方法、测算方法等。
5. **“科技报告类型”**，包括项目综合绩效评价（验收）前撰写的全面描述研究过程和技术内容的最终科技报告、项目年度或中期检查时撰写的描述本年度研究过程和进展的年度技术进展报告以及在项目实施过程中撰写的包含科研活动细节及基础数据的专题科技报告（如实验报告、试验报告、调研报告、技术考察报告、设计报告、测试报告等）。其中，每个项目在综合绩效评价（验收）前应撰写一份最终科技报告；研究期限超过2年（含2年）的项目，应根据管理要求，每年撰写一份年度技术进展报告；每个项目可根据研究内容、期限和经费强度，撰写数量不等的专题科技报告。科技报告应按国家标准规定的格式撰写。
6. **“公开类别及时限”**，公开项目科技报告分为公开或延期公开，内容需要发表论文、申请专利、出版专著或涉及技术诀窍的，可标注为“延期公开”。需要发表论文的，延期公开时限原则上在2年（含2年）以内；需要申请专利、出版专著的，延期公开时限原则上在3年（含3年）以内；涉及技术诀窍的，延期公开时限原则上在5年（含5年）以内。涉密项目科技报告按照有关规定管理。



二、课题研究内容、研究方法及技术路线

（一）课题的主要研究内容

拟解决的关键科学问题、关键技术问题，针对这些问题拟开展的主要研究内容，限1000字以内。

本课题拟解决科学问题“通过规则模型化的监管语言、区块链链式结构上的创新，以及基于可验证计算、属性加密等多种密码理论和技术上的创新，从机制上可以支持在保证链上数字内容安全可用和用户身份隐私的同时，满足监管所需的数据审计要求和追踪、追溯、追责、整改等后续要求”。具体问题如下：

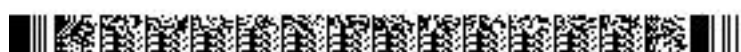
1）解决复杂数字内容交易交互中功能属性形式化和安全属性覆盖范围问题。基于区块链的数字内容，如 NFT、数字藏品等，是由一个或多个部署在区块链平台上的智能合约组成。本课题将对编程语言描述的数字内容进行建模，将其功能和条款转换为规则模块化中间代码，结合调用完整性、原子性、可变账户独立性和交易环境独立性等特征，对相关智能合约进行形式化建模，并通过一致性测试保证合约内容和合约代码的一致性。通过为典型的数字内容智能合约如：ERC721，设置约束模版，将形式化方法用于已有的跨链数字内容交易的安全分析，通过反馈进一步提高属性的覆盖范围。

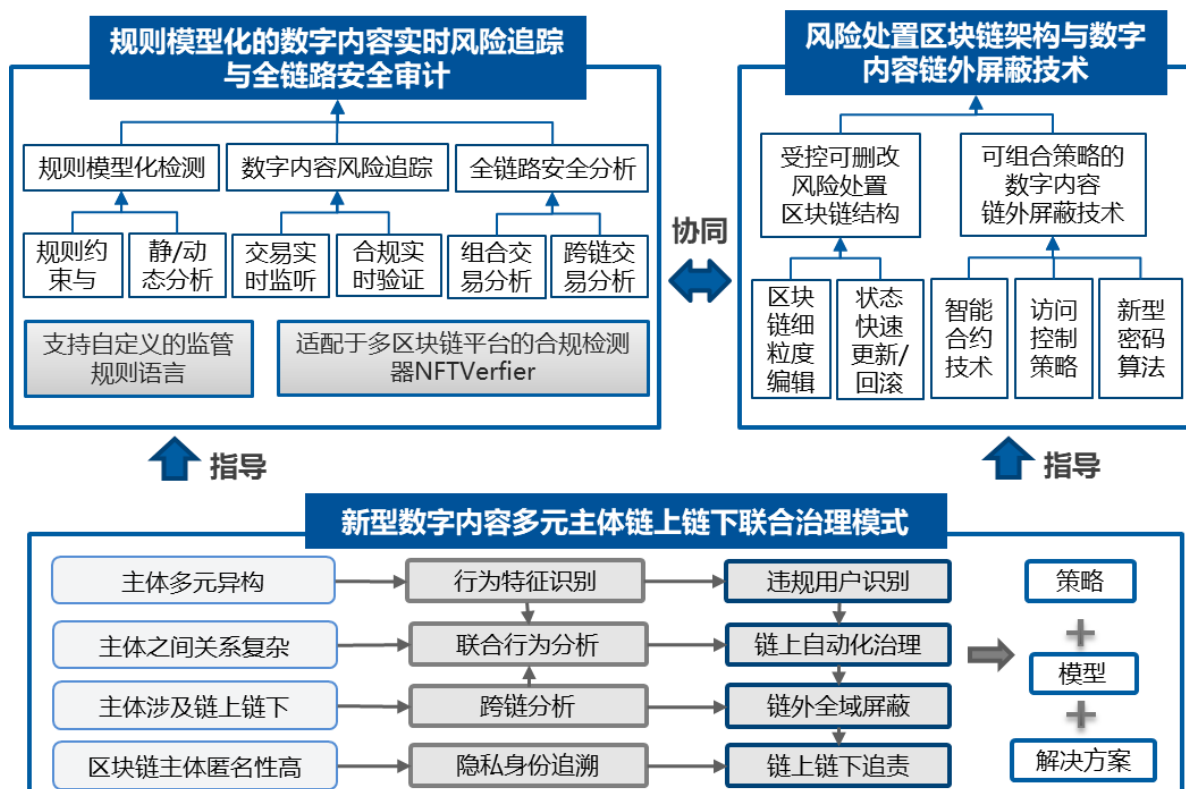
2）解决链上数字内容风险处置与区块链不可更改、公开透明特性之间存在矛盾的问题。本课题将研究不影响区块链网络可用性或不依赖硬分叉的情况下实现对区块链级、交易级、数据项级等不同层次内容的回滚或受控删改问题。另一方面，对于去中心化区块链平台的违规数字内容，本课题将研究数字内容的统一接入安全共享机制，对链上违规数据、敏感数据进行精准屏蔽，实现开放环境下细粒度访问控制。

（二）课题采取的研究方法

针对课题研究拟解决的问题，拟采用的方法、原理、机理、算法、模型等限1000字以内。

本课题围绕“研究新型链上数字内容的全链路安全审计与风险处置技术，实现对新型链上数字内容的实时自动化风险追踪与处置能力”等要求展开以下三方面研究：





（1）新型数字内容多元主体链上链下联合治理模式

(2) 规则模型化的数字内容实时风险追踪与全链路安全审计



违法交易或者无效交易。

（3）风险处置区块链架构与数字内容链外屏蔽技术

研究监管友好的区块链数据层和合约层架构及接口标准。对于链上实体的行为违规，支持在合约层面对违规数字内容及相关链上实体进行锁仓、出入账冻结等监管操作。对于链上数字内容违规，设计支持区块链回滚和细粒度状态修改的新型区块结构和链式结构，研究区块链受控修改的密码杂凑算法，构建可验证的链上数字内容删改安全模型，在监管链与目标链达成共识后，能够以较低的时间和计算资源，完成对已发布的不同层级的链上内容的删改，且不影响区块链网络的可用性。针对面向去中化的公开数字内容存储系统，研究多源数字内容安全接入、安全共享、协同一致的机制和模式，研究基于门限密码和属性密码的数字内容访问控制机制，以及基于国产区块链浏览器和区块链钱包的违规数字内容屏蔽机制。



三、主要创新点

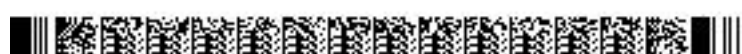
围绕基础前沿、共性关键技术或应用示范等层面，简述课题的主要创新点。具体内容应包括该项创新的基本形态及其前沿性、时效性等，并说明是否具备方法、理论和知识产权特征。每项创新点的描述限 500 字以内。

创新点 1：提出面向新型数字内容复杂交易场景的监管规则语言和合规检测器

现有智能合约安全审计工具仅支持对单个智能合约的检测，难以支撑交易场景更为复杂的新型数字内容的审计。本课题面向链上数字内容的安全需求、功能需求，以及监管需求设计了监管规则语言用于相关智能合约的开发，其包含安全属性定义、功能属性定义和监管合规定义三大模块。监管人员可以自定义数字内容相关合约的安全约束，功能约束和监管规则约束。为支持全链路的实时审计，本项目提出适配于多个区块链平台的交易合规检测器 NFTVerifier，实时监听并捕获来自多个区块链平台的数字内容交易，通过将执行过程中的逻辑不变量与属性约束进行等价性判定，将交易划分为合规交易、违法交易或者无效交易。该方案解决了复杂交易场景下跨函数、跨合约甚至跨链数字内容交易的审计难题，突破了现有技术瓶颈，提高了现有智能合约审计的适用性和覆盖度。

创新点 2：创新提出监管友好的链上数字内容处置机制

本课题提出监管友好的风险处置区块链数据层和合约层架构及接口标准，支持在合约层面对违规数字内容及相关链上实体进行及时处置。提出支持交易回滚和细粒度状态修改的新型区块结构和链式结构，以及支持区块链受控修改的密码杂凑算法，可通过授权节点对链上违规数字内容进行可验证删改。提出基于门限密码和属性密码的链上数字内容访问控制机制，支持去中心化链上数字内容的链外屏蔽及受控访问。上述方案解决数字内容风险处置与区块链不可更改、公开透明特性之间存在矛盾的问题，从机制上可以在保证链上数据安全可用的同时，满足监管所需的数据审计和追踪、追责、整改等后续要求，极大提升了对于链上数字内容的监管和处置能力。



四、预期经济社会效益

课题的科学、技术、产业预期指标及科学价值、社会、经济、生态效益。限 500 字以内。

科学价值分析：在新型链上数字内容的安全审计与风险处置方面，建立了面向新型数字内容复杂交易场景的监管规则语言和合规检测器，以及监管友好的链上数字内容处置机制，将对今后应对新型链上数字内容发展引发的安全风险隐患，各级主管监管部门全面开展新型链上数字内容监管工作提供技术指导。

社会效益分析：本课题的研究成果是新型数字内容区块链平台服务体系的重要组成部分，对规范服务内容、提升境内数字藏品等新型数字内容区块链平台的建设和产业化服务技术水平具有重要意义。这也将有助于确保行业的规范性、安全性，为行业领域和国家相关部门开展监管工作提供良好的基础。

经济效益分析：本课题研究建立的安全审计与风险处置技术与相关工具，能够帮助监管部门及早采取预防补救措施，降低可能发生的经济损失。由于当前以数字藏品为首的新型区块链数字内容平台发展迅速，市场需求大，在本课题研究成果的基础上，可以进一步承接新型数字内容区块链平台安全检测和风险研判等工程化研究开发任务，有效进行技术交流和成果转让，实现“科研-开发-产品-市场”的良性循环。



五、课题年度计划

按每 6 个月制定形成课题的计划进度，应将课题的考核指标分解落实到年度计划中。

1、年度：2022 年 11 月—2023 年 4 月

任务：开展新型链上数字内容监管技术调研，对链上数字内容多元主体监管体系和链上链下联合治理模式进行详细设计。

考核指标：形成多元主体链上链下联合治理模式的技术报告初稿 1 篇。

成果形式：技术报告初稿。

2、年度：2023 年 5 月—2023 年 10 月

任务：对监管规则语言的安全属性、功能属性、合规属性进行详细设计；对风险处置区块链的数据层和合约层架构及标准进行详细设计。

考核指标：形成规则模型化的数字内容监管语言相关软件著作权 1 项；形成课题年度执行报告 1 份。

成果形式：软件著作权；课题年度执行报告。

3、年度：2023 年 11 月—2024 年 4 月

任务：针对监管规则语言开发并测试链上数字内容合约合规检测工具；开发可修改区块链密码算法模块以及链上数字内容访问控制模块；完成中期验收工作。

考核指标：形成链上数字内容全链路安全审计原型工具 1 项；形成可修改区块及访问控制原型系统 1 项；形成链上数字内容全链路安全审计相关发明专利 1 项；形成可修改区块链算法相关软件著作权 1 项；形成课题中期执行情况报告 1 份。

成果形式：软件；原型系统；发明专利；软件著作权；课题中期执行情况报告。

4、年度：2024 年 5 月—2024 年 10 月

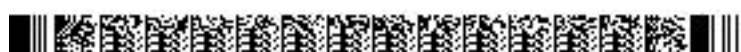
任务：面向复杂交易场景完善链上数字内容合规检测工具；扩展风险处置区块链平台以支持链上违规数字内容处置及链上违规交易回滚。

考核指标：形成链上数字内容全链路安全审计工具 1 项；形成风险处置区块链系统 1 项；形成风险处置区块链相关发明专利 1 项；形成基于规则模型化的数字内容监管规则语言相关论文 1 份；形成课题年度执行报告 1 份。

成果形式：软件；原型系统；发明专利；论文；课题年度执行报告。

5、年度：2024 年 11 月—2025 年 4 月

任务：完善链上数字内容全链路风险追踪与安全审计工具；完善风险处置区块链平台；



在课题一监管系统内集成关键技术成果。

考核指标：链上新型数字内容全链路安全审计与风险处置子系统 1 项。

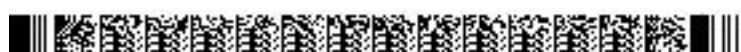
成果形式：原型系统。

6、年度：2025 年 5 月—2025 年 10 月

任务：对链上数字内容全链路风险追踪与安全审计工具进行第三方测试；对风险处置区块链平台进行第三方测试；完成结题验收工作。

考核指标：链上数字内容全链路风险追踪与安全审计工具第三方测试报告 1 份；风险处置区块链平台第三方测试报告 1 份；形成课题年度执行报告 1 份；形成课题最终科技报告 1 份。

成果形式：第三方测试报告；课题年度执行报告；课题最终科技报告。



六、课题组织实施机制及保障措施

1、课题的内部组织管理方式、协调机制等，限 500 字以内。

（1）分级管理、责任到人

课题负责人对课题的具体实施全面负责，提供课题实施的配套条件、人员组织，做好任务分解、进度安排；定期开展课题协调交流会，做好课题内各个参与单位之间的研究任务协调与工作配合，并定期与项目牵头单位就课题的进展情况进行交流汇报，及时报告课题执行中出现的重大问题。

课题骨干负责根据项目总体目标、技术路线需要，带领技术人员严格按照课题具体要求开展课题研究工作；负责推进课题成果的申报及应用转化。落实课题实施方案，完成经费预算和决算报告、年度报告、中期学术进展报告、结题总结报告及项目牵头单位要求的其他材料。

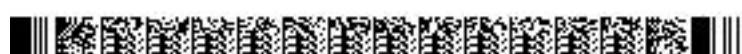
（2）统筹安排、有效监督

课题成立“应用示范小组”和“技术协调小组”。技术协调小组针对所在课题研究任务，由所有课题参与单位的技术骨干构成，负责课题关键技术的攻关；应用示范小组负责课题成果的应用转化，以应用单位的人员为主，部分技术开发人员参与，确保应用开发和成果转化效率。

2、课题实施的相关政策，已有的组织、技术基础，支撑保障条件，限 500 字以内。

政策保障是本课题顺利开展的重要支撑。本课题的研究符合《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》、《关于加快推动区块链技术应用和产业发展的指导意见》、“区块链”重点专项等战略规划，是增强国家核心科技竞争力的关键方向。项目方协调了科研院所、相关企业和管理部门等单位协同推进技术创新、产品研发、检测技术提升、规范体系建设、应用解决方案、示范应用评价研究等，形成本课题实施的外部政策保障。

课题承担单位北京大学在区块链基础理论与技术、智能合约编程语言、区块链安全与隐私保护、区块链创新应用等方面均取得了大量高水平研究成果，研发了自主可控的联盟链平台 RegChain、智能合约编程语言 RegLang、密码算法库 GmSSL 等代表性技术成果，有效支撑区块链全链路审计和处置技术研究工作，并能够为课题提供必要的研究场地、设备、人力、软件资源、网络等全方面的资源支撑。在项目管理方面，建有完整和高效的科研项目管理机构和管理机制，对科研项目的整体管理、进度管

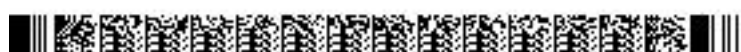


理、人力资源管理、采购管理、资金管理、风险管理等制订有完善的管理方法，充分保障课题实施。

3、对实现项目总目标的支撑作用，及与项目内其他课题的协同机制，限 500 字以内。

课题五所负责的全链路安全审计与风险处置关键技术，对应数字内容监管的最后一个环节——审计与处置阶段，为课题一研制的监管系统提供关键集成模块，与课题二至课题四互为补充和支撑，共同实现新型链上数字内容安全监管系列知识库和风险识别分析模型与工具。

既有共同项目目标，又有具体细致分工。北京大学作为课题承担单位将与其他课题参与方紧密合作，完成预设的研究任务；在年度检查、中期检查及重点节点检查等环节及时发现并解决课程成果集成与对接过程中存在的问题，并以检查结果为依据，实施滚动支持、动态调整、大局优先的课题管理机制。



七、知识产权对策、成果管理及合作权益分配

限 500 字以内。

本课题的知识产权归属、成果管理及合作权益分配按国家有关规定执行，各方经协商，形成如下原则：

（1）依托单位与合作单位在申请本课题之前各自所获得的知识产权及相应权益均归各自所有，不因共同申请本课题而改变。

（2）因课题需要，各自向对方提供的未公开的、或在提供之前已告知不能向第三方提供的与本课题相关的技术资料、数据等所有信息，包括但不限于各自所有或合法拥有的任何计算机程序、代码、算法、公式、过程、观念、图表、照片、制图、设计、产品、样品、发明创造、技术秘密、版权、商标、产品研发计划、预测、策略、规范、实际或潜在商业活动的信息等。未经提供方同意，不得提供给第三方。

（3）严格执行《科技成果登记办法》，实行国家科技计划重大成果报告制度，课题实施过程中取得重大成果时，及时向科技部的计划管理机构报告。

（4）根据科技成果特点，根据相关法律法规的规定适时以专利申请、著作权登记等方式对研究成果的原创性和首创性予以保护。在不影响课题的专利申请或其它知识产权保护的前提下，课题产生的学术报告、论文和专著在进行对外发表时，均要求标注课题所属重大专项经费资助字样和课题编号。



八、需要约定的其他内容

限 500 字以内。

无。

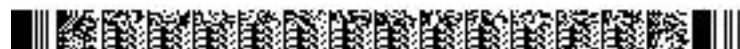


九、课题参加人员基本情况表

填表说明： 1. 专业技术职称：A、正高级 B、副高级 C、中级 D、初级 E、其他； 2. 投入本课题的全时工作时间（人月）是指在课题实施期间该人总共为课题工作的满月度工作量；累计是指课题组所有人员投入人月之和； 3. 课题固定研究人员需填写人员明细； 4. 是否有工资性收入：Y、是 N、否； 5. 人员分类代码：B、课题负责人 C、项目/课题骨干 D、其他研究人员； 6. 工作单位：填写单位全称，其中高校要具体填写到所在院系。														
序号	姓名	性别	出生日期	证件类型	证件号码	专业技术职称	职务	最高学位	专业	投入本课题的全时工作时间（人月）	人员分类代码	在课题中分担的任务	是否有工资性收入	工作单位
1	谢安明	男	1977-01-18	身份证	362429197701183816	副高级	无	博士	计算机软件与理论	18	课题负责人	负责课题统筹、全链路审计和处置技术研究工作	是	北京大学计算机学院
2	王珂	男	1990-06-15	身份证	372330199006154651	其他	无	学士	计算机软件与理论	30	课题骨干	理论研究	否	北京大学计算机学院
3	李悦	女	1997-02-26	身份证	142326199702260821	其他	无	学士	计算机软件与理论	30	课题骨干	理论研究	否	北京大学计算机学院
4	陈子明	男	1999-04-15	身份证	411302199904150018	其他	无	学士	计算机软件与理论	30	课题骨干	理论研究	否	北京大学计算机学院
5	曹逸轩	男	1993-07-10	身份证	371325199307100516	中级	无	博士	计算机软件与理论	18	课题骨干	研究新型链上数字内容的标识技术	是	中国科学院计算技术研究所
6	孙磊	男	1992-05-19	身份证	61043019920519051X	其他	无	学士	计算机软件与理论	30	其他研究人员	关键技术研究	否	北京大学计算机学院



7	崔冬琪	女	1998-12-05	身份证	610323199812050923	其他	无	学士	计算机软件与理论	30	其他研究人员	关键技术研究	否	北京大学计算机学院
8	付旭宇	男	2001-03-08	身份证	421222200103080010	其他	无	学士	计算机软件与理论	18	其他研究人员	关键技术研究	否	中国科学院计算技术研究所
9	李保霖	男	1999-11-04	身份证	210106199911044033	其他	无	学士	计算机软件与理论	30	其他研究人员	验证测试	否	北京大学计算机学院
10	宋煦	男	1997-09-18	身份证	51010519970918001X	其他	无	学士	计算机软件与理论	30	其他研究人员	验证测试	否	北京大学计算机学院
11	吴江	男	1998-09-30	身份证	321023199809306815	其他	无	学士	电子信息	30	其他研究人员	技术方案实现	否	北京大学软件与微电子学院
12	刘鑫	男	1995-10-25	身份证	370481199510250013	其他	无	学士	电子信息	30	其他研究人员	技术方案实现	否	北京大学软件与微电子学院
13	陆阳	男	1998-05-06	身份证	452227199805060279	其他	无	学士	电子信息	30	其他研究人员	技术方案实现	否	北京大学软件与微电子学院
14	赵萌	男	1997-04-04	身份证	130528199704041235	其他	无	学士	电子信息	30	其他研究人员	技术方案实现	否	北京大学软件与微电子学院
15	杨璧鸿	男	1999-07-01	身份证	610103199907012819	其他	无	学士	计算机软件与理论	30	其他研究人员	关键技术研究	否	北京大学软件与微电子学院
16	周进爵	男	2000-05-31	身份证	140602200005319014	其他	无	学士	电子信息	30	其他研究人员	关键技术研究	否	北京大学软件与微电子学院
17	谭诗意	女	1999-09-22	身份证	510322199909225507	其他	无	学士	电子信息	30	其他研究人员	技术方案实现	否	北京大学软件与微电子学院
18	秦紫笛	女	1999-02-01	身份证	43080219990201002X	其他	无	学士	计算机软件与理论	18	其他研究人员	研究新型链上数字内容的标识体系构建方法	否	中国科学院计算技术研究所
固定研究人员合计										492	/	/	/	/



流动人员或临时聘用人员合计	0	/	/	/	/
累计	492	/	/	/	/



课题预算表

表B1 课题编号： 2022YFB2702505 课题名称： 链上数字内容的全链路安全审计与风险处置技术 金额单位： 万元

序号	预算科目名称	金额
	(1)	(2)
1	一、中央财政专项资金	210.00
2	（一）直接费用	167.54
3	1. 设备费	19.95
4	其中：购置设备费	19.95
5	2. 业务费	40.47
6	3. 劳务费	107.12
7	（二）间接费用	42.46
8	二、其他来源资金	
9	三、合计	210.00

注：1. 间接费用无需编制预算说明；2. 绩效支出在间接费用中无比例限制。承担单位在统筹安排间接费用时，要处理好合理分摊间接成本和对科研人员激励的关系，绩效支出安排与科研人员在课题工作中的实际贡献挂钩。



设备费——购置/试制设备预算明细表

表B2 课题编号: 2022YFB2702505

课题名称: 链上数字内容的全链路安全审计与风险处置技术

金额单位：万元

填表说明：

- 1.设备分类：购置、试制；
- 2.购置设备类型：通用、专用；
- 3.试制设备不需填列本表（9）列、（10）列、（11）列、（12）列；
- 4.设备单价的单位为万元/台套，设备数量的单位为台套；
- 5.单价50万元以下的设备不用填写；
- 6.本表只填写中央财政资金购置（试制）的设备。

序号	设备名称	设备分类	功能和技术指标	单价	数量	金额	购置或试制单位	安置单位	购置设备类型	生产厂家及国别	规格型号	拟开放共享范围
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
无记录												
单价50万元以上购置设备合计							/	/	/	/	/	/
单价50万元以上试制设备合计							/	/	/	/	/	/
累计							/	/	/	/	/	/



课题单位经费预算明细表

表B3 课题编号： 2022YFB2702505 课题名称： 链上数字内容的全链路安全审计与风险处置技术 金额单位：万元

填表说明：1.单位类型分课题承担单位、课题参与单位； 2.组织机构代码指企事业单位国家标准代码，单位若已三证合一请填写单位统一社会信用代码，无组织机构代码的单位填写“000000000”。										
序号	单位名称	组织机构代码-统一社会信用代码		单位类型	任务分工	研究任务负责人	合计	中央财政专项资金		其他来源资金
								小计	其中：间接费用	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
1	北京大学	统一社会信用代码	12100000400002259P	课题承担单位	链上数字内容的全链路安全审计与风险处置原理与关键技术研究	谢安明	170.00	170.00	33.26	
2	中国科学院计算技术研究所	统一社会信用代码	12100000400012342E	课题参与单位	规则模型化安全审计任务中的数据分析和模型计算	曹逸轩	40.00	40.00	9.20	
累计							210.00	210.00	42.46	



预算说明

一、中央财政资金

1.设备费

(1) 购置设备费（19.95 万元）

本课题设备购置费预算为 19.95 万元，全部由专项经费支出。测算明细见表 1-1：

表 1-1 购置设备费用预算明细表

序号	设备名称	功能和技术指标	单价 (万元)	数量	金额 (万元)	购置必要性 及用途
北京大学						
1	规则模型化的数字内容全链路安全审计服务器	CPU：Intel Xeon cascadelake V6 4210 *2；内存：16G Dual Rank/Quad Rankx4 DDR4-2400 低功耗内存 *12；硬盘：8T SATA 7200RPM *12；硬盘：960G SATA SSD *2；阵列卡：LSI 3108 或 LSI 3408 及以上芯片，支持 Raid 0、1、5、6、10、50 等，支持 12Gb/S，至少 1G 缓存，带电池；网卡：intel i350 及 i350 以上芯片，四口千兆网卡；网卡：intel 82599 芯片组或 X722 芯片组或 X710 芯片组及以上，万兆网卡（带模块），万兆光口；网卡：intel 82599 芯片组或 X722 芯片组或 X710 芯片组及以上，万兆网卡（带模块），万兆光口；电源：不低于 490W 交直流自适应电源 *2；	4.2	3	12.6	数字内容治理的风险评估和规则模型化研究，支持规则模型化的智能合约编程语言和审计框架，支持实现包含链上、跨链、Web3 服务、链外区块链服务在内的数字内容全链路审计。
2	风险处置区块链架构与链外屏蔽服务器	CPU：2 颗 2nd Generation Intel® Xeon® Scalable Processor, 3*UPI；内存：24 条 2933MHz 内存插槽，支持 DDR4 ECC；网络：双万兆以太网光口，支持虚拟化加速、网络加速、负载均衡等功能；图形卡：GPU 扩展支持 8 片 NVIDIA® Tesla® NVLink & PCIe V100, V100s 支持 8 片 NVIDIA®	2.45	3	7.35	针对链上数字内容风险，研究支持风险内容不同粒度的延迟、阻断、删改、屏蔽的新型区块链架构和关键技术，



		Quadro RTX 6000, RTX 8000 支持 20 片 NVIDIA® Tesla® T4 支持 8 片 Xilinx Alveo U200 FPGA 卡；存储：24 块 2.5/3.5 英寸硬盘（其中 8 个盘位支持 NVMe SSD）+ 2 片 M.2 SSD 硬盘 支持 RAID 0、1、10、5、50、6、60 等，支持 Cache 超级电容保护，提供 RAID 状态迁移、RAID 配置记忆等高级功能；				研究针对无法删改的公链链上违规内容的链外全域屏蔽技术。
合计					19.95	

北京大学设备费购置费 19.95 万元：

1) 拟购置规则模型化的数字内容全链路安全审计服务器 3 台，用于数字内容治理的风险评估和规则模型化研究，支持规则模型化的智能合约编程语言和审计框架，支持实现包含链上、跨链、Web3 服务、链外区块链服务在内的数字内容全链路审计，单价 4.2 万元，小计 12.6 万元；

2) 拟购置风险处置区块链架构与链外屏蔽服务器 3 台，用于针对链上数字内容风险，研究支持风险内容不同粒度的延迟、阻断、删改、屏蔽的新型区块链架构和关键技术，研究针对无法删改的公链链上违规内容的链外全域屏蔽技术，单价 2.45 万元，小计 7.35 万元。

(2) 试制设备费：无。

(3) 租赁设备费：无。

2.业务费

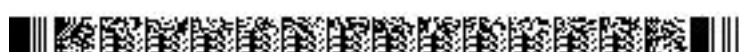
(1) 材料费（5.40 万元）

中国科学院计算技术研究所材料费 5.40 万元：

根据课题需要，拟购买 3 张 GPU 卡，用于规则模型化安全审计任务中的数据分析和模型计算，扩展已有设备的计算能力，单价 1.8 万，小计 5.40 万元。具体测算明细见表 2-1。

表 2-1 材料费用预算明细表

序号	名称	数量	单价（元）	用途	小计（万元）
中国科学院计算技术研究所					



1	GPU卡	3	18000	规则模型化安全审计任务中的数据分析和模型计算	5.40
合计					5.40

（2）测试化验加工费（4.00 万元）

北京大学测试化验加工费 4 万元。

根据课题工作任务及指标需求，需开展“规则模型化的数字内容全链路安全审计平台测试”及“风险处置区块链架构与链外屏蔽平台测试”2 项测试项目。具体测试化验加工费测算明细见表 2-2。

表 2-2 测试费用预算明细表

序号	测试名称	次数	单价（万元）	金额（万元）
北京大学				
1	规则模型化的数字内容全链路安全审计平台测试	1	2.00	2.00
2	风险处置区块链架构与链外屏蔽平台测试	1	2.00	2.00
合 计				4.00

（3）燃料动力费（0.65 万元）

主要用于模型训练、测试，数据处理所需服务器的电费。

中国科学院计算技术研究所燃料动力费 0.65 万元，明细如下：

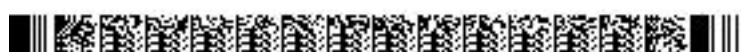
按照平均新购置设备功率为 1.5 千瓦，每千瓦时 1 元，则每年支付 $2*8\text{h}/\text{天} * 180 \text{天} * 0.0001 = 2160$ 元， $0.216 \text{万元}/\text{年} * 3 \text{年} = 0.65$ 万元。

（4）出版/文献/信息传播/知识产权事务费（5.66 万元）

本课题出版/文献/信息传播/知识产权事务费预算为 5.66 万元，全部由专项经费支出。具体测算明细见表 2-3。

表 2-3 出版/文献/信息传播/知识产权事务费预算明细表

序号	项目	单位	单价（元）	数量	金额（万元）
北京大学					
1	文献检索	年	1000	1	0.10
2	论文版面	篇	5000	1	0.50
3	专利申请	项	8000	4	3.20
4	印刷装订	年	2000	3	0.60



5	科技查新	年	2000	3	0.60
中国科学院计算技术研究所					
1	文献检索	/	1000	1	0.10
2	邮寄	年	1200	3	0.36
3	科技查新	/	2000	1	0.20
合 计					5.66

北京大学出版/文献/信息传播/知识产权事务费 5 万元:

- 1) 文献检索费, 1000 元/年, 3 年小计 0.10 万元;
- 2) 预计发表 1 篇论文, 论文版面费 5000 元/篇, 小计 0.50 万元;
- 3) 预计申请 4 项专利, 专利申请费 8000 元/项, 小计 3.20 万元;
- 4) 印刷装订费, 2000 元/年, 3 年小计 0.60 万元;
- 5) 科技查新费, 2000 元/年, 3 年小计 0.60 万元;

中国科学院计算技术研究所出版/文献/信息传播/知识产权事务费 0.66 万元:

- 6) 文献检索费预计 1000 元, 小计 0.10 万元;
- 7) 邮寄费, 1200 元/年, 小计 0.36 万元;
- 8) 科技查新费预计 2000 元, 小计 0.20 万元。

(5) 会议/差旅/国际合作交流费 (24.76 万元)

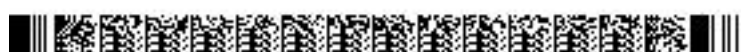
1) 会议费 (8.25 万元)

会议费用于课题开展过程中组织召开课题启动、年度总结、中期检查、课题研讨、结题验收等会议支付的餐费、住宿费和会议室租用等费用, 开支标准按照《关于印发<中央和国家机关会议费管理办法>的通知》(财行[2016]214 号)中 550 元/人天标准(住宿费 340 元/人天 + 伙食费 130 元/人天 + 其他费用 80 元/人天)进行测算, 各单位可根据内部相关财务规定参照执行。

本课题会议费预算为 8.25 万元, 具体测算明细见表 2-4。

表 2-4 会议费预算明细表

序号	会议内容	会期(天)	与会人数	次数	经费(万元)
北京大学					
1	课题启动会	1	5	1	0.275
2	课题中期检查会	1	5	1	0.275



3	课题年度总结会	3	5	3	2.475
4	课题结题验收会	1	5	1	0.275
5	技术沟通交流会	2	5	9	4.95
合计					8.25

北京大学会议费 8.25 万元：

拟召开 1 次课题启动会（会期 1 天）、1 次课题中期验收会（会期 1 天）、3 次课题年度总结会（会期 3 天）、1 次课题结题验收会（会期 1 天）、9 次技术沟通交流会（平均会期 2 天），平均与会人数 5 人，按照 550 元/人/天费用标准，会议费 8.25 万元。

2) 差旅费（16.51 万元）

差旅费用主要用于课题研究过程中前往产业繁荣省份、应用示范省份、会议举办省份（广州、深圳、上海）等开展项目及课题业务研讨、学术交流、现场调研、访谈等产生的外埠差旅费和市内交通等费用。

具体差旅费支出标准按照《中央和国家机关差旅费管理办法》（财行[2013]531 号）、《关于调整中央和国家机关差旅住宿费标准等有关问题的通知》（财行[2015]497 号）、《中央和国家机关工作人员赴地方差旅住宿费标准明细表》（财行[2016]71 号）等国家有关规定，以及各参与单位内部相关规定执行。京外单位国内各城市间往返交通及住宿费用按国内平均价估算。

本课题差旅费预算为 16.51 万元，具体测算明细见表 2-5。

表 2-5 差旅费预算明细表

出差目的	目的地	往返交通费(元)	住宿(元/天)	差旅补助(元/天)	人数	天数	次数	经费(万元)
北京大学								
科学考察/业务调研/学术交流	深圳	3000	400	180	10	3	1	4.74
科学考察/业务调研/学术交流	上海	3000	400	180	10	3	1	4.74
科学考察/业务调研/学术交流	广州	3000	400	180	10	3	1	4.74
中国科学院计算技术研究所								



科学考察/业务调研/ 学术交流	/	3000	450	180	2	2	3	2.29
合计								16.51

北京大学差旅费 14.22 万元：

拟赴深圳、上海、广州三地进行科学考察、业务调研、学术交流各 1 次，每次 10 人、3 天，按照城际交通费 3000 元/人，住宿 400 元/人/天，差旅补助 180 元/人/天，差旅费小计 14.22 万元。

中国科学院计算技术研究所差旅费 2.29 万元：

拟赴外地进行科学考察、业务调研、学术交流 3 次，每次 2 人、2 天，按照城际交通费 3000 元/人，住宿 450 元/人/天，差旅补助 180 元/人/天，差旅费小计 2.29 万元。

3) 国际合作与交流费：无

3.劳务费

(1) 劳务费（102.80 万元）

本课题劳务费预算为 102.80 万元，用于支付课题研究过程中博士生及研究生的劳务支出，全部为专项经费。具体劳务费测算明细见表 3-1。

表 3-1 劳务费预算明细表

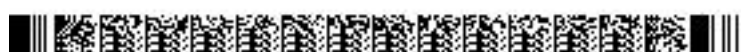
序号	人员类别	人数	标准(元/人月)	人月	金额(万元)
北京大学					
1	博士生	3	2400	30	21.6
2	硕士生	11	1800	30	59.4
中国科学院计算技术研究所					
1	博士后	1	8000	16	12.8
2	硕士生	2	2500	18	9
合 计					102.80

北京大学劳务费 81.00 万元：

拟使用 3 名博士生、11 名硕士生参与课题技术研究，每人投入 30 人月，按照博士生 2400 元/人/月，硕士生 1800 元/人/月计算，劳务费 81.00 万元。

中国科学院计算技术研究所劳务费 21.80 万元：

拟使用 1 名博士后、2 名硕士生参与课题研究，博士后每人投入 16 人月，硕士生每人投入 18 人月，按照博士后 8000 元/人/月，硕士生 2500 元/人/月计算，



劳务费 21.80 万元。

(2) 专家咨询费（4.32 万元）

本课题专家咨询费预算为 4.32 万元。根据课题研究需要，拟聘请本领域有影响的专家进行课题关键技术交流指导与咨询。专家咨询费标准按照《中央财政科研项目专家咨询费管理办法》（财科教[2017]128 号）等国家有关规定，以及各参与单位内部相关规定执行。具体专家咨询费测算明细见表 3-2。

表 3-2 专家咨询费预算明细表

序号	咨询形式	专家人数	天数	次数	费用标准(元/人)	金额(万元)
北京大学						
1	会议	3	2	3	2400	4.32
合 计						4.32

北京大学专家咨询费 4.32 万元：

拟召开 3 次专家咨询会，会期 2 天，邀请 3 名专家，专家费标准为 2400 元/人/天，专家咨询费 4.32 万元。

二、其他来源资金

本课题经费全为中央财政经费，无其他资金来源。



十一、相关附件

1. 乙方与参加单位有关协议（须加盖乙方与参加单位公章、法人签字签章；协议文件须扫描上传。如无参加单位，则不填）；
2. 申报指南规定的其他附件。

国家重点研发计划“区块链”重点专项
“新型链上数字内容的安全智能监管关键技术”项目
“链上数字内容的全链路安全审计与风险处置技术”
课题实施协议

课题名称：链上数字内容的全链路安全审计与风险处置技术

承担单位（甲方）：北京大学

课题负责人：谢安明

协作单位（乙方）：中国科学院计算技术研究所

任务负责人：曹逸轩

签订时间：2022 年 11 月

签订地点：北京市



本协议双方就共同合作参与研究国家重点研发计划“区块链”重点项目“新型链上数字内容的安全智能监管关键技术”项目“链上数字内容的全链路安全审计与风险处置技术”课题（以下简称“课题”）相关事宜，经平等协商，在真实、充分表达各自意愿的基础上，根据有关法律、法规和项目管理部门的相关规定，就本课题研究工作中所涉及的任务分工、研究成果的知识产权、经费分配方式等达成如下协议，并由合作各方共同恪守。

1. 课题分工和考核指标

甲方总体负责课题的组织、协调和实施，负责子任务1新型数字内容多元主体链上链下联合治理模式；负责子任务2规则模型化的数字内容实时风险追踪与全链路安全审计；负责子任务3风险处置区块链架构与数字内容链外屏蔽技术。

具体甲方负责考核指标包括：

（1）完成1篇关于新型数字内容链上链下联合治理模式的架构与方案；

（2）支持跨函数、跨合约自定义监管规则的全链路安全审计。智能合约平均审计时间不超过1分钟，评测结果误报率不超过10%，漏报率不超过3%，申报发明专利不少于1项，申报软件著作权不少于1项，发表高水平论文不少于1篇；

（3）支持对链上数字内容的可验证删改操作，支持区块链回滚规模不低于7天生成的区块数量，在线密码计算延迟不超过1000毫秒；支持对于违规数字内容的受控访问以及链外屏蔽，申报发明专利不少于2项，申报软件著作权不少于1项；

（4）研制链上新型数字内容全链路安全审计与风险处置系统，支持跨函数、跨合约的复杂交易场景下数字内容自定义监管规则的全



链路安全审计，支持链上数字内容的可验证删改或回滚操作，支持对于违规数字内容的受控访问及链外屏蔽功能。

乙方参与子任务1新型数字内容多元主体链上链下联合治理模式研究。

具体乙方负责考核指标包括：

(1) 参与完成1篇关于新型数字内容链上链下联合治理模式的架构与方案。

2. 知识产权

2.1 本协议所称知识产权, 包括依法享有的专利权、著作权、商标权、计算机软件的版权、技术秘密、商业秘密等知识产权。

2.2 课题研究过程中所涉及各方已有的知识产权归原产权持有方所有，合作方有责任对任何其他方保密。

2.3 课题研究过程中新产生的知识产权按各方贡献大小分配，即各方独立完成研究工作所形成的知识产权归各方独立所有；双方共同完成研究工作所形成的知识产权按贡献大小根据相应的比例归各参与方共同所有，任何一方未经合作方同意不得擅自向其他方公开。

3. 经费分配

经费分配方案如下：

本课题中央财政专项共210.00万元，甲方170.00万元，乙方40.00万元。

甲方根据国家科技部及项目牵头单位每年拨付情况和乙方课题进度，按照乙方所占经费比例取整支付。在乙方课题进度符合要求情况下，甲方在收到国家科技部专项经费后45天内支付乙方。

乙方开户名称:中国科学院计算技术研究所

乙方开户银行:工行北京市分行海淀西区支行



乙方银行帐号:0200004509088123135

乙方纳税人识别号:12100000400012342E

4. 数据汇交承诺

双方就课题产生的科学数据做出以下承诺:承诺本课题汇交的数据真实、准确、完整、有效,无学术不端和学术失范行为,并承担因数据不真实等问题带来的一切后果和法律责任;承诺将本课题产生的样本信息、实验数据等科学数据无条件汇交到科技部指定平台。

5. 其他

5.1 本协议未尽事宜,由双方友好协商解决;协议履行过程中,如发生纠纷,由双方协商解决,协商未果时向甲方所在地的人民法院起诉。

5.2 本协议一式8份,双方各执3份,2份用于项目任务书申报,具有同等法律效力。

以下无正文,转签章页。



本页无正文，为单位签章页



甲方（盖章）：

法人（签字盖章）：

樊旗煜

课题负责人（签字盖章）：谢安明

日期：2022.11.22

乙方（盖章）：

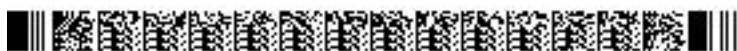


法人（签字盖章）：

李旭东

课题/任务负责人（签字盖章）：曹逸轩

日期：2022.11.22



任务书签署

甲乙双方根据《国务院印发关于深化中央财政科技计划（专项、基金）管理改革方案的通知》（国发〔2014〕64号）、《国务院关于优化科研管理提升科研绩效若干措施的通知》（国发〔2018〕25号）、《国务院办公厅关于改革完善中央财政科研经费管理的若干意见》（国办发〔2021〕32号）、《科技部 财政部关于印发<国家重点研发计划管理暂行办法>的通知》（国科发资〔2017〕152号）、《财政部 科技部关于印发<国家重点研发计划资金管理办法>的通知》（财教〔2021〕178号）、《科学技术活动违规行为处理暂行规定》（科学技术部令第19号）、《科技部财政部关于印发<中央财政科技计划（专项、基金等）监督工作暂行规定>的通知》（国科发政〔2015〕471号）、《科技部 自然科学基金委关于进一步压实国家科技计划（专项、基金等）任务承担单位科研作风学风和科研诚信主体责任的通知》（国科发监〔2020〕203号）等有关文件规定，以及有关法律、政策和管理要求，依据项目立项通知，签署本任务书。

同时，本单位和项目负责人**郑重承诺**：对本项目所有成果产出（包括但不限于新产品、新技术、标准、论文、专利等）的真实性、与项目的关联性等负责，将按要求落实科研作风学风和科研诚信主体责任；项目经费全部用于与本项目研究工作相关的支出，不截留、挪用、侵占，不用于与科学研究无关的支出；严格按照政府采购和保密法律法规规定开展政府采购活动，规范信息公开工作；接受并积极配合相关部门的监督检查。如有违反，本单位和项目负责人以及相关成果产出者愿接受项目管理专业机构和相关部门做出的各项处理决定，包括但不限于终止项目执行、追回项目（课题）经费，取消一定期限国家科技计划项目申报资格，记入科研诚信严重失信行为数据库以及主要负责人接受相应党纪政纪处理等。



项目牵头承担单位（甲方）：

法定代表人签字（签章）：

（公章）

年 月 日

项目负责人签字（签章）：

年 月 日

课题承担单位（乙方）：

法定代表人签字（签章）：

（公章）

年 月 日

课题负责人签字（签章）：

年 月 日

