附件 7

“区块链”重点专项 2023 年度项目申报指南

（仅国家科技管理信息系统注册用户登录可见）

为落实“十四五”期间国家科技创新有关部署安排，国家重点研发计划启动实施“区块链”重点专项。根据本重点专项实施方案的部署，现提出 2023 年度项目申报指南。

本专项总体目标是：聚焦区块链领域的紧迫技术需求和关键科学问题，建立自主创新的区块链基础理论体系，突破区块链系统构建共性关键技术，加强区块链监管与治理技术研究，构建自主知识产权的区块链基础平台，开展重大应用示范。

2023 年度指南部署坚持需求导向、问题导向，围绕区块链基础理论、区块链系统构建共性关键技术、重点领域示范应用等 3 个方向，启动 9 项指南任务，拟安排国拨经费 0.57 亿元。其中，青年科学家项目拟安排国拨经费 1400 万元，1.2、2.4 指南任务各 300 万元，1.3 指南任务 400 万元，1.4、2.3 指南任务各 200 万元。共性关键技术类项目配套经费与国拨经费比例不低于 1:1，应用示范类项目配套经费与国拨经费比例不低于 2:1。

项目统一按指南二级标题（如 1.1）的研究方向申报。申报项目的研究内容必须涵盖二级标题下指南所列的全部研究内容和考核指标，实施周期不超过 3 年。基础研究类项目下设课题数不超

过4个，项目参与单位总数不超过6家；共性关键技术、应用示范类项目下设课题数不超过5个，项目参与单位总数不超过10家。每个项目设1名项目负责人，项目中每个课题设1名课题负责人，项目负责人可同时担任1个课题负责人。

青年科学家项目不要求对指南内容全覆盖，不再下设课题，项目参与单位总数不超过3家。项目设1名项目负责人，青年科学家项目负责人年龄要求，男性应为1985年1月1日以后出生，女性应为1983年1月1日以后出生。原则上团队其他参与人员年龄要求同上。

除指南中特殊说明外，每个指南任务拟支持项目数为1~2项。“拟支持项目数为1~2项”是指：在同一研究方向下，当出现申报项目评审结果前两位评价相近、技术路线明显不同的情况时，可同时支持2项。2个项目将采取分两个阶段支持的方式，第一阶段完成后将对2个项目执行情况进行评估，根据评估结果确定后续支持方式。

1. 区块链基础理论

1.1 面向物联网的新型区块链体系架构（基础研究类）

研究内容：面向物联网的区块链面临设备组网协同能力弱、强容错计算能力缺失、应用服务自适应功能不足等问题，研究面向物联网的新型区块链体系架构，包括零信任下区块链可信组网理论、轻量化强安全区块链共识协议、基于智能合约的算存一体化机制和可重构编程模型，实现轻量化、高可信、自适

应特性。在网络层研究动态环境下云边端海量区块链节点可信组网与协同，探索零信任数字身份认证与可信组网理论以及动态不稳定环境下物联网设备的共识算法，构建面向无线网与异构网络的轻量化强安全区块链共识协议；在计算层，研究零信任下的去中心化存储与多点协同智能合约，探索区块链云边端高效分层存储机制与异构网络多点协同的智能合约机制，支持按需可信计算环境构建，实现算存一体化；在应用层，研究可重构智能编程模型，支持高可信区块链架构动态重组与云边端资源快速调配，设计多领域应用接口构建方法，利用去中心化机制增强动态网络拓扑下区块链编程模型的智能调优能力与易用性，可形式化证明安全可靠。

考核指标：设计面向物联网的轻量化、高可信、自适应新型区块链体系架构。提出零信任下的区块链可信组网理论以及不少于 3 种可形式化证明安全的、具有自适应性的强容错共识机制；设计不少于 2 种支持物联数据强安全存储证明的去中心化存储方案，支持不少于 100 个分布式节点，实现存储开销降低不少于 50%；提出安全与隐私保护的异构网络多点协同智能合约机制，支持云边端设备部署，支持在资源受限终端设备上实现合约计算；设计不少于 3 套可形式化证明安全可靠、具备分布式智能调优能力的可重构智能编程模型。

关键词：物联网，区块链，体系架构，高可信，轻量化，自适应，资源受限。

1.2 基于区块链的隐私计算关键技术（青年科学家项目）

研究内容：针对现有隐私计算在半诚实模型以及恶意模型下的可用性与安全性问题，建立基于区块链的新型隐私计算框架，研究基于区块链的隐私计算身份认证协议、信任模型与激励机制。在隐私计算身份认证方面，研究基于区块链的隐私计算分布式可信身份认证体系，支持大规模轻量级身份认证场景；面向半诚实模型，基于联邦学习、多方安全计算、可信执行环境、同态加密等隐私计算技术，提出数据、计算过程及结果安全可信的隐私计算模型；面向恶意模型，建立多方在竞争、对抗及合作模式下的动态博弈隐私计算激励机制，研究基于区块链智能合约的博弈收益体系及其可信执行技术，形成恶意攻击下隐私计算的安全性防护能力。

考核指标：建立基于区块链的新型隐私计算框架，满足隐私计算半诚实模型以及恶意模型场景的需求；支持不少于 2 种轻量级身份认证体系；在半诚实模型中，提出数据、计算过程及结果安全可信的隐私计算模型，链上处理耗时≤3 秒；在恶意模型中，提出不少于 2 种动态博弈下的激励机制，不少于 2 种恶意攻击的安全防护方法。

关键词：隐私计算，博弈，恶意模型，半诚实模型，激励，轻量化身份认证，安全。

1.3 基于区块链的 Web 3.0 新型技术体系架构（青年科学家项目，拟支持 2 项）

研究内容：针对 Web 3.0 技术体系不明确、技术组件不成熟

等问题，以结构化、可互通、可扩展、可监管为目的，在基础设施、基础组件、服务组件等层面研究基于区块链的新型高兼容、高吞吐量的 Web 3.0 技术体系架构。研究支持异构互通的 Web 3.0 网络架构和协议栈层次框架，满足 Web 3.0 中的分布式存储、计算和点对点通信需求；研究满足线性一致性的高性能区块链基础组件划分及协作机制，满足 Web 3.0 在数据、身份、资产、权益等层面的需求；研究可支撑丰富 Web 3.0 应用的服务组件框架，支持低代码开发、快速部署、模块化和可扩展等技术特点，具备监管友好的 Web 3.0 应用管理机制及用户接入规范。

考核指标：提出基于区块链的 Web 3.0 技术体系架构；提出技术互通的 Web 3.0 网络架构和协议栈层次框架，实现基于轻量级虚拟化技术的 Web 3.0 网络协议栈原型验证系统；设计不少于 5 种 Web 3.0 基础组件和交互协作协议；提出具备 Web 3.0 应用管理和用户接入规范的 Web 3.0 服务组件框架。

有关说明：拟支持 2 项。

关键词：Web 3.0，区块链体系架构，协议栈，接入规范与价值激励。

1.4 基于网络动力学的区块链多层结构分析理论与方法（青年科学家项目）

研究内容：针对区块链系统在线运行时安全与性能的动态分析需求，以网络动力学为基础理论体系和研究视角，将网络层、共识层、合约层抽象为多个复杂网络结构，以网络结构中的共识节点

和用户节点行为为分析对象，提出在不完备测量数据条件下区块链在线运行时的安全与性能动态分析方法及优化策略；针对网络层网络结构与数据流动耦合的安全性问题，研究多种攻击策略下的网络鲁棒性分析、关键链路识别等方法，提出网络层结构动态优化策略；针对共识层共识节点多轮通信的收敛一致性问题，研究共识层网络的智能重构方法，提出共识层低通信复杂度的动态快速收敛策略；针对合约层多用户参与、多应用交织场景，研究合约中用户行为特征与合约驱动关系，提出合约层复杂网络动态演化行为分析方法和突变涌现机理，建立合约层复杂安全事件的预测框架。

考核指标：建立网络层、共识层、合约层多层网络动态分析与测量方法，提出一套理论模型及原型验证系统，在以太坊、波卡等不少于 2 种主流公有链平台上进行验证，评估该模型对区块链鲁棒性、安全性、效率等方面的提升效应；提出不少于 3 种网络层攻击分析模型，包含网络鲁棒性分析、关键链路识别等方法；提出不少于 3 种可复用、可重构的共识机制，并实现智能选择；提出不少于 3 种合约层复杂安全事件的预测框架，预测准确率 ⩾80%。

关键词：网络动力学，复杂网络，动态优化，鲁棒性，行为特征，安全预测。

2. 区块链系统构建共性关键技术

2.1 基于区块链的大规模分布式可信智能计算关键技术及应用（共性关键技术类）

研究内容：针对大规模分布式智能计算面临的海量多源异构

数据和模型可信、分布式智能算力协同等问题，研究基于区块链融合人工智能、大数据等技术的大规模分布式可信智能计算技术架构；研究基于区块链的大规模分布式数据可信治理技术，实现数据真实性完整性验证、数据合规和数据确权；研究基于区块链的面向数据全生命周期的元数据体系和分布式过程数据库构建方法；融合区块链、机器学习、多方安全计算、形式化验证等技术，研究大规模分布式可信人工智能建模技术和区块链链上链下协同智能模型执行技术，实现建模、推理及结果的全过程可信验证和模型确权保护；研究数据、模型、算力等可信智能计算要素在区块链上的标准表示方法及其链下接口规范，研究基于智能合约等技术的智能计算需求与分布式算力交易撮合的链上匹配和链下可信验证技术；构建基于区块链的自主可控大规模分布式可信智能计算网络技术平台并进行应用验证。

考核指标：提出大规模分布式可信智能计算技术架构，支持分布式数据节点数≥3000 个、分布式智能算力节点数≥100 个；实现数据真实性完整性验证和确权、元数据体系和分布式过程数据库等数据可信治理技术，支持 PB 级链下数据和 TB 级链上数据，支持至少 5 种模态 TB 级数据的全生命周期合规处理；实现链上链下协同的分布式智能模型训练、保护和执行技术，实现分钟级分布式推理过程可验证，支持代码级形式化验证的安全协议；实现数据、模型、算力的链上表示和匹配、链下验证和追溯技术，算力撮合交易吞吐量≥50000TPS，单个交易可支持不少于 200 个

参与节点（包括数据节点和算力节点），参与节点支持 PB 级数据和亿级可通讯机器学习参数模型，实现分布式模型的训练、保护、集成和执行全过程上链和可信验证；实现基于区块链的自主可控大规模分布式可信智能计算网络技术平台，在金融、医疗、交通、安防等至少 1 个场景进行应用验证，应用场景机构数量≥20 个；提交国际/国家/行业标准提案不少于 2 项。

关键词：区块链，智能合约，人工智能，大数据。

2.2 基于区块链的 Web 3.0 前沿技术（共性关键技术类）

研究内容：面向 Web 3.0 技术对于网络开放自治、用户数据自主管理需求，构建以区块链技术为基础的 Web 3.0 前沿技术群；面向 Web 3.0 用户自主身份管理需求，研究基于区块链技术的可信分布式数字身份管理机制，实现自主数字身份创建与端到端的用户身份管理；面向 Web 3.0 价值流通需求，研究跨应用的数字资产流通机制，构建依托区块链的经济运行模型，设计数字资产的数据确权与供需匹配方法；面向 Web 3.0 用户分布式自治需求，研究用户共建共治的生态治理机制，设计去中心化的用户声誉评价方法和用户权益激励方法；面向 Web 3.0 数据安全与隐私保护需求，研究监管友好的数字资产全生命周期安全防护方法；开发 Web 3.0 原型系统，在社交、数字娱乐等领域开展应用验证。

考核指标：提出以区块链技术为核心的 Web 3.0 前沿技术群；实现去中心化数字身份的自主创建与管理，支持亿级用户规模，身份验证时间≤500ms；提出 Web 3.0 的经济运行模型，支持对文

字、图片、视频等不少于3种模态的数据确权，支持用户数字资产交易的供需匹配功能；支持从用户的社区行为、用户贡献度等方面对用户声誉进行评价；支持工作量、存储空间等不少于5种用户权益激励形式；支持多方安全计算、零知识证明等不少于3种对用户数字资产的隐私保护技术；开发Web 3.0原型系统，在社交、数字娱乐等至少1个领域开展应用验证，用户规模达到十万级。

关键词：Web 3.0，分布式数字身份，经济运行机制，治理机制。

2.3 基于区块链的新型信任体系（青年科学家项目）

研究内容：针对区块链单一技术无法为互联网中数字经济活动提供全流程信任支撑的问题，研究基于区块链的新型信任体系，包括数据可信上链、链上信任增强、链上信任管理以及与传统信任体系的互通互信技术方案。研究数据可信上链技术，基于区块链技术锚定外部数据产生链上信任，保障数据上链的真实性与时效性；研究链上信任增强技术，推动区块链与新一代数字技术的融合创新，满足链上信任传递的低时延与高安全，打造链上链下可信协同架构；研究链上信任管理机制与方法，提出链上信任管理通用模型，构造链上信用体系；研究链上信任与传统信任体系的互通互信方案，实现链上链下信任闭环。

考核指标：提出通用性数据可信上链技术，实现MB级数据可信上链过程≤500ms；提出链上信任增强技术，围绕可信计算、可信身份与可信数据协作等方面，实现不少于3种区块链融合其

他新一代数字技术的链上链下可信协同方案；提出链上信任管理通用模型，支持 C2C、B2C、B2B 和 G2B 等不少于 4 类链上社会关系场景；提出链上信任与传统信任体系的互通互信方案，满足千万级字节数据量前提下的链下存储与结合传统信任体系的链上动态存储映射，满足正确性、隐私性和安全性要求，实现链下存储及链上动态存储映射过程的高通量与低时延；在数据流通、数字贸易、数字金融等数字经济领域选取至少 1 种典型场景开展信任体系理论验证。

关键词：可信上链，信任增强，信任管理。

2.4 基于区块链的数字资产流通关键技术（青年科学家项目）

研究内容：围绕碳证、版权等资产或权益数字化形成的数字资产，研究基于区块链技术的具有实用性权益的数字资产流通理论和技术体系，建立多类型数字资产跨链/平台流通理论与动态可扩展技术架构；研究基于区块链技术的可编程数字资产的表征和权益的关联方法、价值评估模型、分类分级机制和可信交易方法，并具有高效率、可扩容性、公平性、安全性等特性；根据数字资产流通生命周期过程需求，研究基于智能合约的数字资产链上发行、版权登记、智能交易、记账和对账、托管的流通技术；根据数字资产流通过程的差异化保护需求，研究基于区块链的数字资产存证、交易和验证技术，支持多形态、多属性的数字资产版权保护、安全和隐私保护；根据数字资产流通主体类别多样性特点，研究支持高效异步共识的数字资产流通的算法可验证、逻辑可审

计和监管可穿透的方法。

考核指标：建立基于区块链的多类型数字资产流通技术体系，提出分层、跨平台、动态扩容的通用技术框架；提出不少于5类数字资产价值评估模型和5类数字资产分级分类管理模型，开发发行、交易等流通类智能合约，覆盖能源、版权等至少10个应用领域；提出数字资产可信流通机制，研发分布式数字资产交易关键技术组件1套，支持多方实时审计、隐私保护、交易穿透监管等；设计基于区块链技术的多类型数字资产流通原型验证系统，支持高效异步共识机制，模拟环境下50个节点规模的交易吞吐量≥10000TPS；覆盖数字资产链上生成、登记、交易、托管、监管等过程，模拟环境下订单处理量单日≥50000笔。

关键词：数字资产，价值评估，分级分类，数字资产流通。

3. 重点领域示范应用

3.1 基于区块链的数据要素市场关键技术与示范应用（应用示范类）

研究内容：围绕我国“十四五”规划和2035年远景目标纲要中建立健全数据要素市场规则的目标，基于区块链理论与技术成果研究构建数据要素市场的技术体系，支撑数据要素资源化、资产化、资本化。针对数据要素在采集、存储、流通、交易和治理中的问题，研发新的增强数据确权、标记、存储、交易、利用和治理过程的技术；针对数据要素合规性和产权保护问题，研究基于区块链的数据交易核验工具，跟踪数据使用情况，实现交易

数据的全流程溯源；针对数据的价值和利益分配问题，提出多元主体参与的激励机制，建立数据要素的新型市场分配机制；研发基于区块链技术的分布式数据交易平台，在相关领域开展数据生产要素流通应用示范，形成可复制、可推广、可借鉴范式。

考核指标：建立基于区块链的数据生产要素流通和交易模型，制定不少于3种数据要素交易规则，支持不少于3种类型的数据交易服务；提出增强数据确权、标记、存储、交易和利用的综合解决方案；研发数据要素市场监管治理工具，实现数据要素准确核验，百万条上链数据核验效率达秒级；建立不少于2种多元主体参与的激励机制，制定不少于3种数据要素的新型市场分配方案；研发基于区块链技术的分布式数据交易平台，在不少于3个行业领域完成数据交易示范应用，平台参与交易账户数≥10万，产生显著经济效益；形成较完善的软件工具集不少于30个，提交国际/国家/行业标准提案不少于5项；采用区块链重点专项支持的区块链基础平台作为底层平台。

关键词：区块链，数据要素，流通与交易，激励机制，监管。