附件 6

“区块链”重点专项
2023 年度项目申报指南

（征求意见稿）

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。专项实施周期为 5 年（2021~2025 年）。

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。

1. 区块链基础理论

1.1 基于区块链的新型智能物联体系架构（基础研究类）

研究内容: 针对资源受限的智能物联网面临的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，研究基于区块链的新型智能物联体系架构，包括智能物联系统组织架构、通信模式、算存一体化机制和编程模型，实现轻量化、

高可信、自适应等特性。在网络层研究动态环境下云边端海量异构设备可信组网与协同，提出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共识机制，构建面向无线网与混合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，提出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，实现智能物联系统算存一体化；在应用层，研究可重构智能编程模型，支持高可信架构动态重组与云边端资源快速调配，提出多元应用接口构建方法，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：设计基于区块链的轻量化、高可信、自适应智能物联体系架构。提出零信任下的可信组网理论以及不少于 2 种可证明安全的异步网络共识机制；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；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；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：智能物联；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体系、信任体系与激励体系。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，研究基于区块链的可信隐私计算模型，实现数据、计算过程以及计算结果的安全可信；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技术体系，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；在恶意模型中，提出不少于 2 种博弈收益模型，不少于 2 种恶意攻击的安全防护方法；发表高质量论文并申请发明专利。

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 Web3.0 新型技术体系架构（青年科学家项目）

研究内容：针对 Web3.0 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 Web3.0 技术体系。研究支持同构或异构互通、与 Web2.0 兼容的 Web3.0 网络架构和协议栈层次框架，满足 Web3.0

中的分布式存储、计算和点对点通信需求；研究高性能区块链基础组件划分及关键组件协作机制，满足 Web3.0 在数据、身份、资产、权益等层面的需求；研究可支撑丰富 Web3.0 应用的服务组件框架，实现低代码开发、快速部署、模块化和可扩展等特点，具备监管友好的 Web3.0 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 Web3.0 技术体系；提出支持平台或技术互通的 Web3.0 网络架构和协议栈层次框架；设计不少于 5 种 Web3.0 基础组件和交互协作协议；提出具备 Web3.0 应用管理和用户接入规范的 Web3.0 服务组件框架；发表高质量论文并申请发明专利。

关键词：Web3.0；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，以网络结构中的节点与用户行为为分析对象，提出在不完备测量数据条件下区块链的多个复杂网络结构动态分析与测量方法；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、关键链路识别方法，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，在长安链、Fabric 等不少于 2 种主流区块链平台上进行验证；提出不少于 3 种网络层攻击分析模型；提出不少于 3 种共识机制的智能重构方法；提出不少于 3 种合约层复杂安全事件的预测框架；发表高质量论文并申请发明专利。

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；研究融合区块链、机器学习、多方安全计算、形式化验证等技术的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≥3,000 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 级链上数据库，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，支持 PB 级数据和亿级参数模型，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≥20,000TPS，单个交易可支持不少于 100 个参与节点；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，在医疗、安防等至少 1 个场景进行应用验证，应用场景机构数量不少于 20 个；提交国际/国家/行业标准草案不少于 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核心的 Web 3.0 技术体系模型；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。

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，从“信息、信任和信用”角度出发，研究构建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机制等方面功能，构建信任基础设施和体系。研究数据可信上链技术，保障数据上链的真实性和时效性；研究区块链与隐私计算、分布式数字身份等技术的融合创新，保障信任传递能力，强化底层信任，满足链上信任传递的低时延和高安全，打造链上链下高效协同架构，构建以区块链为支撑的算法信任理论体系；研究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；研究链上原生信任与链下传统信任体系的互通互信，实现链上原生和链下并行情况下，“信息、信任和信用”的闭环管理。

考核指标: 构建基于区块链的新型信任体系，提出基于区块链的通用信任体系；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，构建不少于 3 种区块链融合其他前沿信息技术的算法信任方案，实现链上性能峰值吞吐量⩾10,000TPS；提出链上原生信任关系模型，构造链上信用体系，支持 C2C、B2C、B2B 和 G2B 等不少于 4 类链上社会关系场景；提出链上原生信任与链下传统信任体系的互通模型，实现千万级数据量下链下存储与链上映射的正确性、隐私性和安全性，满足数据传递的高通量与低时延。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；信任互通。

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，研究多形态、多属性的数字资产版权保护、安全和隐私保护、分布式身份认证技术；根据数字资产流通主体类别多样性特点，研究支持数字资产流通的算法可验证、逻辑可审计和监管可穿透的分布式共识方法。

考核指标：建立覆盖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、隐私安全的数字资产流通通用技术框架；提出不少于 5 类数字资产价值评估模型和 5 类的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，支持分布式身份认证、实时审计、隐私保护、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，覆盖数字资产链上生成、登记、交易、托管、监管等过程。

关键词：数字资产；价值评估；分级分类；数字资产流通；状态通道。

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，数据要素核验准确性≥95%，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，月交易额≥10亿元；开发软件工具不少于30项，提交国际

/国家/行业标准草案不少于 5 项。

关键词：区块链；数据要素；流通与交易；激励机制；监管。