附件 4

“区块链”重点专项 2021 年度项目申报指南

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，现发布 2021 年度项目申报指南。

本重点专项总体目标是：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。

2021 年度指南部署坚持问题导向、分步实施、重点突出的原则，围绕区块链基础理论、区块链系统构建共性关键技术、区块链安全监管与治理技术 3 个领域方向，拟启动 8 项任务，拟安排国拨经费 1.16 亿元。其中，围绕区块链基础理论与方法、威胁感知与取证两个方向，拟部署 4 个青年科学家项目，拟安排国拨经费 1200 万元，每个项目 300 万元。除区块链基础理论方向、区块链安全监管与治理技术方向、青年科学家项目外，其他项目配套经费与国拨经费比例不低于 1:1。

项目统一按指南二级标题（如 1.1）的研究方向组织申报。除特殊说明外，每个项目拟支持数为 1~2 项，项目实施周期不超过 3 年。项目应整体申报，须覆盖该二级标题下指南所列的全部内

容。区块链基础理论类项目下设课题数不超过3个，项目参与单位总数不超过4家；共性技术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。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1983年1月1日后出生，女性应为1981年1月1日后出生。原则上团队其他参与人员年龄要求同上。

指南中“拟支持数为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，可同时支持这2个项目。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 新型区块链体系架构设计理论与方法（基础理论类，拟支持2项）

研究内容：针对当前区块链体系架构在性能、可扩展性、安全性、隐私保护等方面的困难与挑战，研究新型的多链（片）并行区块链体系架构，提升区块链系统的可扩展性和可伸缩性；研究海量业务并发支撑技术，提升区块链的交易并发处理性能；研究链上链下智能化协同优化技术，将复杂业务逻辑迁移至链下执

行；研究适应复杂多变运行环境的区块链高效同步方法；研究区块链的节点身份认证、分级访问控制、跨域可信及隐私保护等核心功能在区块链体系结构的内生支持机制。

考核指标：提出高性能多链（片）并行区块链体系架构，支持的并行分片数不低于1000，跨链（片）关联交易对系统性能不造成显著影响；提出支持海量业务并发及链上链下交互等新型交易处理机制，支持区块链系统整体通量线性可扩展；提出高效区块链同步方法，适应多样化、高动态运行环境，随着节点规模增大，性能保持稳定；实现面向新型区块链体系结构的身份认证、新型分级访问控制、跨域可信及可信服务等机制；发表高质量论文；申请发明专利10项以上。

1.2 高延展性可证明安全共识算法及系统设计理论与方法研究（基础理论类，拟支持2项）

研究内容：针对拜占庭共识机制的动态节点增删安全性缺乏理论保障、异步网络环境安全性难以保障、系统可延展性弱等问题，研究可证明安全高效、可支持动态节点、高延展性、高吞吐量的共识机制设计理论；研究在网络异步的环境中同时保障安全性及活性的高性能共识算法和负载低、延展性强的容错系统架构；研究可证明安全的高效分片共识方案；构建复杂网络环境下共识协议的合理安全模型。

考核指标：提出具有可证明安全性的异步共识算法，在网络带宽不低于100 Mbps时，延迟低于200 ms，吞吐量达到60000

TPS；给出支持节点动态加入和离开的可证明安全的拜占庭共识算法，延迟增幅低于 50 ms；提出分片共识及存储方案，可延展至 500 个节点以上，分片后吞吐量提高 200%；给出精准的共识评估模型刻画共识协议的安全性；发表高质量论文；申请发明专利 10 项以上。

1.3 高并发可扩展区块链存储的基础理论和方法研究（青年科学家项目，拟支持 2 项）

研究内容：针对传统链式区块链难以支撑高频次高并发应用场景的需求，研究区块链系统的高效可扩展存储理论、缓解存储压力的轻量级弹性区块链数据模型、支持数据查询检索的高效完整性及一致性验证技术。

考核指标：核心区块链弹性可扩展存储模型具备创新性；支持基于图式区块链的轻量级可扩展数据分级存储功能；实现至少对 10TB 区块链数据的高效一致存储，将存储开销降低 5 倍以上；支持高效可信存储的数据索引机制，并能对查询结果进行有效验证；发表高质量论文；申请发明专利 5 项以上。

2. 区块链系统构建共性关键技术

2.1 区块链性能模型及多层级协同优化关键技术研究（共性技术类）

研究内容：针对传统区块链低性能与高频交易需求间的矛盾，研究区块链性能模型及多层级协同优化技术。研究多指标约束下的区块链性能模型；研究低时延低冗余区块链网络传输协议

及数据传播架构，支持大规模节点应用的高效数据分发和数据同步；研究适用于大规模网络部署的低开销且兼顾公平与效率的区块链共识机制；研究数据存储模型及高效存储与访问机制；研究智能合约并行执行冲突消解技术，提高合约并行执行效率。

考核指标：提出多指标约束下的区块链性能模型，基于该模型设计至少 3 种主流区块链系统的性能优化方法；建立 1 套区块链性能多层级协同优化技术体系，部署不少于 3 种主流区块链系统，交易确认延时不超过 1 秒；在多核 CPU、千兆局域网、SSD 硬盘、16 个共识节点的规模下，测试转账类业务的吞吐量不低于 55000 TPS；研发区块链智能合约执行平台，支持不少于 10 种应用场景的智能合约；申请发明专利 15 项以上，提交国际/国家/行业标准草案 2 项以上。

2.2 区块链可证明安全隐私保护技术研究（共性技术类，拟支持 2 项）

研究内容：针对区块链数据公开透明、无中心节点管控、隐私保护困难的问题，研究区块链系统的隐私安全风险，研究区块链匿名交易技术，研究通用的安全可重组的隐私保护技术；研究监管友好的区块链交易隐私保护机制，涵盖零知识证明、账号匿名、同态加密、安全多方计算等技术与方法，保护交易身份和交易内容等敏感的交易信息；研究交易追踪溯源技术，支持针对特定异常交易的识别和追踪溯源；研究基于国家认可的商用密码算法的隐私交易平台，在工业、农业、政务、商务、民生、金融等

领域开展示范应用。

考核指标：区块链协议具备在并发混合使用场景下的安全性，提供严格的形式化等证明，实现区块链交易隐私保护机制的功能正确性和规范一致性证明，满足可追溯性和可验证性；提出不少于3种区块链交易隐私保护方法，保护交易双方身份和内容等敏感信息；实现监管友好的区块链隐私保护系统，支持权威监管机构对异常交易信息的识别和追踪溯源；区块链隐私交易平台支持用户账户数量不低于10亿；支持日交易量不低于10亿笔；链上存储量可弹性扩展；平台技术成果应用于不少于3类场景；申请发明专利15项以上,提交国际/国家/行业标准草案2项以上。

2.3 区块链评测技术体系与系统研究（共性技术类）

研究内容：针对区块链快速发展与评测体系、技术手段尚不完备之间的矛盾问题，研究建立区块链评测技术体系，涵盖性能、功能、真伪性、安全性、可靠性和合规性等方面；研究新型区块链技术的组件化评测方法；研究区块链系统的脆弱性发现、对抗策略与问题关系验证机制；研究区块链密码算法及协议、密码模块和密码应用安全性的检测评估方法；研究区块链信息内容安全评测技术；研究多样性测试数据集构造方法，保障异构区块链性能测试公平性；构建评测工具库，设计实现区块链评测系统，支持评测策略的自适应调整；以区块链在法定数字货币、数据生产要素流通、智慧城市、金融科技、工业互联网、政务民生、能源、社会治理等应用为评测场景，研制差异化评测模板，实现穿透式

评测，并对区块链系统的创新程度进行评测。

考核指标：建立区块链评测技术体系，形成 1 套区块链评测规范；提出不少于 3 种区块链系统脆弱性、内容安全防护、共识有效性的评测技术；研制区块链脆弱性评测工具，支持多种网络协议、共识算法等的对抗推演和评测；研制区块链密码评测工具，并实际完成不少于 2 款区块链密码产品评测；提出不少于 3 种测试数据集构造方法；提出面向智能合约的功能正确性和安全性评测方法，构建自动化评测工具，支持 3 个以上主流区块链平台，自动化检测 20 种以上常规智能合约安全漏洞；构建评测工具库，支持对区块链设备接入、数据存证和流通、智能合约、跨链、安全防护等方面进行评测；建设评测平台，支持大规模网络节点，性能测试上限达到 12 万 TPS，兼容不少于 5 种底层链，具备区块链隐藏安全风险评测能力、高风险漏洞检测定位能力，支持评测策略自适应调整和执行；在法定数字货币、数据生产要素流通、智慧城市、金融科技、工业互联网、政务民生、能源、社会治理等应用中设计并实现不少于 3 种典型区块链应用场景的评测模板，支持区块链应用生态的自动化安全风险测试评估；申请发明专利 15 项以上，提交国际/国家/行业标准草案 3 项以上。

2.4 区块链安全威胁感知与取证研究（青年科学家项目，拟支持 2 项）

研究内容：针对区块链层出不穷的安全威胁，设计具有高兼容性、高扩展性且具有快速响应能力的区块链安全威胁感知平台；

研究各类区块链安全威胁的内部机理；提出应对已知和未知类型安全威胁的通用解决方案；设计区块链海量数据快速获取和存储方法；设计在海量区块链数据中快速关联安全威胁的算法；研究可扩展的区块链安全威胁取证系统，支持自定义的取证模式，以支持多种取证场景。

考核指标: 区块链安全威胁感知平台的性能开销不超过10%; 区块链安全威胁感知平台能发现不少于10种类型的安全威胁; 区块链安全威胁感知平台能应用于三种以上主流区块链基础平台；支持在10亿级交易数量的区块链上开展安全威胁取证；从10亿级区块链数据中关联安全威胁的时间开销不超过5分钟；支持不少于5种安全威胁取证模式；申请发明专利5项以上。

3. 区块链安全监管与治理技术

3.1 区块链生态安全监管关键技术研究（共性技术类，拟支持2项）

研究内容: 面向区块链生态中存在的安全风险，研究区块链安全生态监管技术框架，实现对区块链生态体系的监管。研究精细化深度分析与识别技术，研究账号、交易、链群三维一体的区块链生态实体关联关系构建技术,研究区块链数字身份关联技术; 研制区块链生态安全监管系统，实现区块链生态共性安全风险识别与定位、安全风险事件的精准刻画和风险及时发现预警、网络空间与物理空间的实体关联以及跨账户、跨平台的关联式监管等能力；形成法定数字货币、数据生产要素流通等区块链场景下的

生态安全风险分析技术和安全监管方案，开展监管示范应用。

考核指标：构建区块链安全生态监管技术框架，提出共性安全风险规范，明确区块链不同层级安全风险；提出不少于3种具有精细化深度分析与识别、区块链生态实体关联关系构建、区块链数字身份关联等能力的技术；支持不少于10类安全风险点的分析与识别；支持实体关系的构建、融合、推理等，形成千万级规模的实体关系库；对智能合约异常交互行为的检测准确率超过90%；面向法定数字货币、数据生产要素流通、智慧城市、金融科技、工业互联网、政务民生、能源、社会治理中的至少2类区块链应用场景形成针对性监管方案并进行应用示范，每类场景下部署区块链应用不少于3个；申请发明专利15项以上，提交国际/国家/行业标准草案3项以上。