附件 8

“区块链”重点专项 2021 年度
项目申报指南建议

（征求意见稿）

国家重点研发计划启动实施“区块链”重点专项。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与共性关键技术，加强区块链监管与治理技术研究，推动建立区块链与其它前沿信息技术相融合的新一代信息基础设施与服务，开展在重点领域的应用示范，打造具有国际竞争力的区块链技术与产业生态。

根据本重点专项工作部署，现提出 2021 年度项目申报指南建议。2021 年度指南部署坚持问题导向、分步实施、重点突出的原则，拟围绕区块链基础理论、系统构建与共性关键技术、安全监管与治理等 3 个技术方向先期启动 7 个指南任务。

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

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，研究支持多链（片）并行的高性能区块链体系架构，提升区块链系统的可扩展性和可伸缩性；研究支持海量业务并发的区块链体系架构，提

升区块链的交易并发处理性能；研究基于国家密码算法的区块链内生安全架构，实现区块链节点行为的全维多粒度安全防护；研究区块链的节点身份认证、分级访问控制、数据加密及隐私保护等核心功能在区块链体系结构的支持机制。

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；交易并发处理的吞吐量达到60,000 TPS；基于国密算法实现区块链海量节点行为的持续安全防护，威胁阻断准确率不低于90%；实现面向新型区块链体系结构的身份认证机制、新型分级访问控制、隐私保护机制、国产加密及数据密态运算。

1.2 面向区块链的高容错密码体系关键技术研究

研究内容：针对区块链高容错密码的安全性、可扩展性和高性能等问题，研究满足一致性、活性等安全属性的密码学新原理；提出满足该属性的密码设计机理，设计大规模、高性能的拜占庭容错算法、设计理论性能最优的异步算法；研究主动安全的容错密码理论，设计分布式密钥重分享协议。

考核指标：提出的拜占庭容错算法在半同步网络不少于600个节点参与时吞吐量达到60,000 TPS，确认延迟不大于一分钟；异步网络环境下在消息复杂度、时间复杂度、通信复杂度等指标上达到理论最优；密钥重分享协议支持国密算法，在不少于600个节点参与时同步网络环境下延迟不大于100秒。

1.3 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

研究内容：针对拜占庭共识机制，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，研究安全高效、可支持动态节点、高延展性的共识机制设计理论和拜占庭共识系统架构；研究可证明安全高效的分片共识方案；构建复杂网络环境下的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，延迟低于 200ms，吞吐量达到 60,000 TPS；给出支持节点动态加入和离开的可证明安全共识算法，延迟增幅低于 50ms；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%。

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

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，具体包括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；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机制；研究链上扩容与链下扩容协同优化方法；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，部署于不少于 3 种主流区块链系统，交易确认延时不超过 1 秒、吞吐量不低于 60,000 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。

2.2 区块链可证明安全隐私保护技术研究

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，设计区块链匿名交易体系，设计通用安全可重组的隐私保护协议；研究区块链账号混淆机制，隐藏区块链交易发送方与接收方之间的交易关联关系；研究监管友好的区块链交易隐私保护机制，保护交易双方的地址、金额等敏感的交易信息，同时支持针对特定异常交易的追踪溯源；研究基于国产自主知识产权区块链平台的匿名交易平台，在金融等典型领域开展示范应用。

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，提供严格的安全性证明；提出不少于 3 种区块链账号混淆方法，隐藏区块链交易发送方与接收方之间的交易关联；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追踪溯源；区块链匿名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；在 32 个共识节点的规模下，交易吞吐量不低于 60,000 TPS，交易平均延时小于 1 秒；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。

2.3 区块链评测技术体系与系统研究

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的检测评估方法；研究区块链内容安全评测技术；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；以区块链在能源、金融、物联网等典型应用为评测场景，研制差异化评测模板，实现穿透式评测，并对区块链系统的国产自主可控程度进行评测。

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、内容安全及内容安全防护的评测技术；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；构建评测工具库，建设评测系统，需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；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。

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

研究内容：面向区块链生态中存在的安全风险，研究适用于公有链、联盟链的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安全风险知识图谱构建技术，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，实现区块链不同层级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穿透以及跨账户、跨平台的穿透式监管等能力；形成金融、能源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：结合典型公有链及联盟链特征，形成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、区块链生态安全风险知识图谱构建、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，识别效率提升1倍以上；支持图谱构建、融合、推理等，形成百万级规模的实体关系图谱；数字身份关联推理分析准确度达到90%以上；形成国内金融、能源等区块链场景监管方案，应用规模不少于2类典型场景，每类场景下区块链应用不少于3个。