“区块链”重点专项
2022 年度项目申报指南建议
（征求意见稿）

1. 区块链基础理论

1.1 面向区块链分布式场景的密码技术（基础前沿类）

研究内容：针对分布式场景下区块链安全性、可扩展性和性能等需求，研究区块链中应用的分布式密码算法，设计针对分布式密码算法的密钥管理机制，设计具有可证明安全性的分布式数字签名算法；针对区块链的隐私保护和监管需求，研究环签名、代理重加密等密码技术的设计理论，结合其在区块链中的应用，设计安全高效的环签名算法以及代理重加密协议；针对区块链在节点规模、系统性能等方面的需求，研究分布式协商协议的设计理论，设计安全高效的分布式协商协议。

考核指标：设计针对分布式密码算法的密钥管理机制，可支持密钥的分布式生成和安全更新，支持国家密码管理部门认可的密码算法；提出具有可证明安全性的分布式数字签名算法，支持至少 100 个以上的交互参与方，满足抵抗恶意中止健壮性等特性；提出具有可证明安全性的分布式协商协议，通信复杂度达到线性量级；提出具有可证明安全性的环

签名算法，满足可追踪、可撤销等特性；提出具有可证明安全性的代理重加密协议，满足密文不可链接性和抗合谋安全性等特性；发表高质量论文，申请发明专利 10 项以上。

1.2 面向区块链的抗量子计算公钥密码技术（基础前沿类）

研究内容：针对量子计算对区块链密码的安全威胁和对区块链系统带来的长期安全挑战，研究具有抗量子计算能力的区块链密码算法设计理论，设计可抵抗量子攻击的数据加密、数字签名等区块链密码算法；设计可抵抗量子攻击的身份认证、安全通信、安全共识等区块链密码协议；研究抗量子安全的区块链系统设计理论，提出抗量子安全的区块链原型系统设计方法；研究区块链中现用密码技术向抗量子计算密码技术迁移的解决方案。

考核指标：提出在抗量子安全模型下具有可证明安全性的区块链密码算法，算法应至少具有 128 比特的量子安全强度，可支持数据加密、数字签名等功能，算法单次加密解密或签名验签时间合计小于 1 毫秒，算法加密密文尺寸小于明文尺寸 50 倍，算法签名尺寸不超过 5,000 字节；提出在抗量子安全模型下具有可证明安全性的区块链密码协议，可支持身份认证、安全通信、安全共识等功能；提出具有抗量子计算能力的区块链原型系统设计方案，系统应支持不少于 50 个的共识节点，并分析系统性能与抗量子密码算法参数之间

的关系，给出满足不同应用场景需求的优化算法参数选取方案并在原型系统中进行验证；提出区块链中现用密码技术向抗量子计算密码技术迁移的解决方案；发表高质量论文，申请发明专利 10 项以上。

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（基础前沿类）

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；构建复杂网络环境下共识协议的合理安全模型；研究在网络异步/半同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；设计安全共识机制中的密码学及关键技术组件（门限签名、聚合签名、可靠广播等）的优化算法，研究基于以上方案的新型可证明安全的高效分片共识方案。

考核指标：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 50ms；给出精准的共识评估模型刻画共识协议的安全性；提出具有可证明安全性的共识算法，在网络带宽不低于 100Mbps 时，延迟低于 200ms，吞吐量达到 60,000TPS（每秒处理事务）；对安全共识系统中需要的密码学、分布式系统关键组件进行优化和改进，并提出高效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%；发表高质量论文；申请发明专利10项以上。

1.4 智能合约与法律的创新理论及方法（青年科学家项目）

研究内容：针对法律条文因自然语言歧义性、模糊性带来的法律风险，研究基于区块链智能合约表达法律条文的法学原理；研究基于智能合约的法律条文表征模型，降低法律诉讼的经济和时间成本；分析对法律条文进行形式化表达的可行性与正当性，研究法律条文与对应形式化表达模型之间的一致性判定方法，比较法律条文的形式化表达和文字表达之间的优劣；研究面向法律条文的智能合约语言，研发转换至可编程语言引擎，形成可执行的智能合约；研究法律条文智能合约的高效生成和验证方法，保障一致性、准确性和安全性；研究智能合约应用的法律规制，设计智能合约监管合规化技术方案和相应的评测方法；设计以智能合约对法律条文进行诠释的原型应用系统。

考核指标：建立一套用智能合约表达法律的法理理论和基于智能合约的法律条文表征模型；设计一种面向法律条文的智能合约语言,具备表达不少于3种法律条文类型的能力；研发可编程语言引擎，支持转换至不少于2种编程语言的可执行智能合约；构建一个针对合约化的法律条文评测体系，支持生成智能合约与法律条文的一致性不低于90%，法律条

文要素规则关联的准确性不低于85%；形成一套智能合约应用的配套监管规范，提出智能合约的法律规制建议；设计一套支持不少于三类应用场景的智能合约表示法律条文的原型系统；发表高质量论文，申请发明专利5项以上。

1.5 面向区块链的新型密码研究（青年科学家项目）

研究内容：针对区块链在安全性与隐私保护等方面的需求，开展适合区块链的新型密码理论和技术研究。1）研究同态密码等新型密码的设计以及在区块链中的具体应用；或2）研究适用于区块链的新型杂凑函数的设计；或3）研究零知识证明、隐私计算、匿名签名等实现区块链隐私保护的新型密码。

考核指标：1）提出适用于区块链的同态密码算法新型设计理论和实用化关键技术，提出或实现与SEAL、Helib、HEAAN等开源库具有可比较性能或针对区块链应用具有明显优势的全同态密码方案；或2）设计适用于区块链的具有256比特安全强度的新型杂凑函数，能抵抗已知攻击并具备充足的安全冗余，且实现性能与SHA3-512相当；或3）设计支持轻量级终端的可证明安全的非交互式零知识证明方案，设计布尔电路单次AND门计算效率达到微秒级以下的隐私计算协议，设计常数签名长度的可证明安全的匿名签名方案。

2. 区块链系统构建共性关键技术

2.1 区块链存储与数据管理关键技术与方法（共性技术类）

研究内容：针对区块链数据管理实现低时延高吞吐面临的技术瓶颈，研究区块链多模态数据多种类节点链上链下轻量化高效存储方法；研究支持多模态数据溯源与复杂查询的高效可信执行与检索技术；研究支持多种类节点间高吞吐、高并发事务处理机制，支持多源数据共享与协同执行；研究分片下的自适应可验证索引高效构建方法与动态可扩展共识策略；研制高吞吐低时延的区块链数据管理系统，并在医疗、金融、交通、能源、食品等至少 3 个领域的联盟机构进行应用验证。

考核指标：针对区块链多模态数据管理共享协同需求，研究区块链数据管理关键技术与方法，实现区块链环境下的高效数据管理系统；研究在全节点与轻量化节点混合架构下，支持数值、文本、序列、视频等 4 种模态以上的数据共享、轻量化存储方法，并支持 PB 级数据规模应用；提供支持复杂查询以及溯源查询的可信查询算法，响应时间达到百万条/秒级；多模态数据共享负载下区块链数据管理系统吞吐率达到 60,000TPS 以上；支持 3 种以上可验证索引自适应构建方法；在医疗、金融、交通、能源、食品等至少 3 个领域进行高性能区块链数据存储与管理应用验证；申请发明专利 15

项以上。

2.2 区块链智能合约语言关键技术（共性技术类）

研究内容：针对我国在智能合约编程语言方面缺失的现状，研究简洁、安全的智能合约编程语言，支持复杂业务逻辑的抽象和表达；研究针对该编程语言的编译器，实现词法分析、语法分析、代码生成、代码优化等功能；研究针对该智能合约语言的执行引擎，使智能合约的部署和执行具有性能高、资源开销小等优势；研究针对该智能合约语言的验证工具，可基于模型检验或定理证明方法对智能合约的正确性、安全性进行验证；研究针对该智能合约语言的智能化开发环境，构建支撑智能合约开发、管理的软件平台。

考核指标：设计一种新型智能合约编程语言，支持常规数据结构，支持常规数据结构的序列化与反序列化，支持循环、递归等操作，支持常用密码算法（含国家密码管理部门认可的密码算法），支持安全的智能合约版本升级，支持并行执行，支持异步函数调用，支持周期性自动事务，支持原生交易索引语义，支持异常捕获与处理机制，支持定义合约事件，支持跨合约调用；研发针对该智能合约语言的编译器，支持智能合约代码按级别优化，支持智能合约 ABI 生成，支持生成智能合约代码调试符号；研发针对该智能合约语言的执行引擎，支持用户输入参数调用执行智能合约中的方法，记录合约执行的结果、事件、异常和执行所消耗的资源，支

持限定合约执行的资源消耗上限，引擎执行性能达到单线程每秒 1 亿次整数操作，执行内存消耗不超过状态及输入参数总量的 2 倍，支持自动垃圾回收；研发针对该智能合约语言的验证工具，支持基于智能合约功能规范和智能合约代码实现的正确性验证，支持基于通用漏洞和用户自定义漏洞的安全性验证；研发针对该智能合约语言的智能化开发环境，支持智能合约在线编译、调试、测试、管理，支持多人协作开发模式；在不少于 3 个区块链平台上集成执行引擎，在金融、政务、民生等领域落地不少于 5 个示范应用；申请发明专利 15 项以上。

2.3 区块链链上链下数据可信交互关键技术（共性技术类）

研究内容：针对区块链系统无法保证链下数据来源真实性、传输可靠性、隐私安全性、上链及时性等问题，研究区块链与物联网、边缘计算、大数据、隐私计算等技术的融合创新，保障链上链下数据的可信交互；研究低时延高安全自适应的链上链下网络通信方案，支持在多类型终端大数据容量和复杂网络环境下数据的高效安全传输，以及区块链系统与其他系统之间的数据交换；研究支持国家密码管理部门认可的密码算法的隐私保护算法及标准化工程实现，提高数据的隐私保护能力，支持可验可查但敏感数据不上链、隐私数据不泄露场景；研究跨行业通用的链上链下互操作方案，支

持多层级跨系统大规模的链上链下数据交互并进行应用验证。

考核指标：研究 1 套通用的区块链链上链下数据可信交互技术框架，实现数据来源真实、网络传输可靠、执行过程可信及敏感信息安全；提出不少于 3 种保障数据来源真实可信的技术方法，并验证存在虚假来源、传输干扰等不可靠环境中的有效性；提出不少于 3 种支持国家密码管理部门认可的密码算法的链上链下数据隐私保护方法，实现敏感数据链下存储链上映射，有效保障使用过程中敏感数据的正确性、隐私性和安全性；提出不少于 1 种低时延高安全自适应的链上链下网络通信方案，实现千万级数据量下数据上链时延不超过 1 秒，数据传输过程安全可靠，具备网络异常情况下的主动容错能力；在农业、交通、工业互联网、智慧城市、能源等不少于 3 类区块链典型应用场景中验证万级数据终端 TB 级数据量下的平台技术成果；申请发明专利 15 项以上；提交国际/国家/行业标准草案 1 项以上。

2.4 安全弹性的区块链网络关键技术（共性技术类）

研究内容：针对底层网络的可靠和健壮对于区块链应用和系统的安全可信与执行效率的重要性，研究提升区块链承载网络传输性能的关键技术以及对常见网络攻击的安全防护机制；设计区块链网络的安全架构，具有较强的故障容忍性；研究新型的网络拓扑结构，区块链网络数据的通信和转

发算法，网络数据的编码和压缩方法，以降低区块链数据在全网转发的时延，提高通信的有效带宽利用率，同时保证区块链系统的安全性，即对各种网络协议攻击的抵御能力；研究区块链网络的端到端确定性传输技术，保证各区块链节点之间的有限时延抖动；研究流量调度和拥塞控制技术，对不同类型的上层服务提供效率支持，避免底层网络的时延波动及拥塞丢包现象；研究基于内生安全的 DDoS 防御技术，结合真实源地址验证，防止基于伪造地址的多类 DDoS 洪泛攻击，并提出对异常安全行为的事后追溯机制。

考核指标：针对先进的区块链系统体系结构提出并实现高性能高可靠的网络通信系统架构，在受限可控的网络环境下，新型区块链承载网络能够保证 TCP/IP 层端到端的传输时延抖动小于 100 微秒，且该抖动不受地理距离和转发跳数影响；区块链承载网络能避免网络拥塞造成的丢包现象，保障覆盖网络的高质量通信，实现零拥塞丢包目标；在开放公有的网络环境下，在节点数不小于 5000，带宽 40Mbps 以及全球节点部署的条件下，网络通信系统能够支撑至少 10,000TPS 的区块链转账交易吞吐率（可在仿真环境中测试，如在实际区块链系统中部署更佳）；平均 95%的区块或交易数据能够在 15s 内传播至 95%的节点，网络传输的数据冗余度小于 10%；网络具有较强的故障容忍能力，网络系统能够抵御日蚀攻击，DDOS 攻击，交易转发协议及编码中的哈希

碰撞攻击，以及不诚实转发行为等网络攻击；申请发明专利15项以上。

2.5 高性能自适应跨链互通关键技术及试验验证（共性技术类）

研究内容：研究可扩展自适应跨链互通架构，支持大规模同构/异构区块链动态接入，实现多种链间互通模式、多种跨链传输验证机制等的自适应配置，满足不同接入区块链在性能、安全、隐私等方面的差异化需求。研究高性能跨链交互机制，设计实现跨链交互协议栈，实现高效、高并发的跨链传输验证与事务处理，满足链间信息与信任传递的高通量与低时延；研究跨链应用的跨平台实现与部署机制，支持跨链应用在异构接入区块链中的灵活便捷部署与发现，研究跨链资源发现机制，实现跨链资源的快速定位与发现；研究跨链治理与监管技术，实现细粒度的跨链资源访问控制、跨链隐私保护与多层级监管接入机制，解决跨链技术落地与实际应用中的管理难、定责难等问题。

考核指标：提出可扩展自适应异构跨链架构，其中异构是指区块链的共识机制等底层实现不同；设计实现高性能跨链交互协议栈，支持读请求和写请求的确认时延与跨链交互的确认时延保持在同一数量级；提出面向跨链体系的治理与监管机制，包括链的接入准入、跨链资源访问控制、跨链隐私保护、跨链监管技术等；构建1套跨链验证平台，具备支

持不少于5种100条区块链动态接入的能力，并实现任意接入平行链间的跨链互操作，支持5种以上链链互通模式、3种以上跨链验证方法，支持不同接入区块链间的按需自适应配置；设计5种以上跨链应用，每种应用至少在3种以上异构区块链部署实现，并在金融、政务、民生、工业、农业等领域选取具有多链跨链需求的典型应用场景开展应用验证；申请发明专利15项以上，提交国际/国家/行业标准草案1项以上。

2.6 区块链可证明安全隐私保护技术研究（共性技术类）

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，研究通用的安全可重组的隐私安全模型与形式化验证方法；研究监管友好的区块链交易隐私保护机制，研究基于零知识证明和账号匿名的可证明安全身份隐私保护方案，以及基于同态加密和安全多方计算的可证明安全内容隐私保护方案，在保护交易身份和交易内容等敏感的交易信息的同时实现对异常交易的识别和追踪溯源；研究基于国家密码管理部门认可的密码算法的隐私交易平台并开展示范应用。

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

身份和内容等敏感信息并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；基于平台技术成果落地不少于3类应用；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。

3. 区块链安全监管与治理技术

3.1 基于区块链的社会治理与风险防控技术及应用（共性技术类）

研究内容：针对疫情防控、反洗钱、反电信诈骗、网络信息风险防控等社会治理与风险防控中的精准、可信、智能、实时等需求，研究融合区块链、大数据、人工智能、物联网等技术的社会治理与风险防控技术体系；研究基于区块链的分布式数字身份、数据安全可控流转的数字化社会治理可信服务关键技术；研究基于区块链、机器学习和图计算的社会风险防控规则智能化构建技术；研究融合高性能区块链、实时大数据和人工智能的社会风险实时监测、分析、预警和存证技术；研发基于国产自主知识产权技术的区块链社会治理与风险防控技术平台，并在社会风险防控典型应用场景进行应用验证。

考核指标：提出融合区块链、大数据、人工智能、物联网的社会治理与风险防控技术架构；构建面向数字化社会治理可信服务支撑技术体系，包含分布式数字身份管理、隐私

数据可信共享等功能，支持大规模分布式数字身份账户，支持不少于10种隐私数据可信共享算法；提出社会风险防控规则智能化构建技术和自动化部署方案，支持特征规则、神经规则和图规则等3类以上规则的智能化构建技术；构建实时、智能的社会风险监测、分析、预警、存证技术能力，风险关联数据同步存证，社会风险监控流量不低于每秒1,000,000条，每项风险监控指标计算时延小于100毫秒；实现基于区块链的社会治理与风险防控技术平台，在疫情防控、、反洗钱、反电信欺诈、网络信息风险防控等2个以上社会风险防控典型应用场景得到应用验证；申请发明专利15项以上。

4. 区块链基础平台

4.1 非开源联盟链基础平台（基础平台）

研究内容：构建具备自主知识产权的、能满足国家重要核心领域非开源要求的高可控、高安全隐私、高性能可扩展、监管友好联盟链基础平台（简称“非开源自主可控联盟链平台”）；研究支撑海量用户与应用场景的弹性可扩展区块链架构；面向国家密码管理部门认可的密码算法、多维度隐私保护技术、区块链安全态势感知技术、身份安全与密钥管理技术、智能合约安全度量与漏洞检测技术，构建国家商用密码级的安全隐私体系；面向联盟链以链治链分布式监管技术、沙盒式/嵌入式/穿透式监管技术、链上链下协同监管技术，

构建面向异构多层级区块链平台的监管监测体系，提高监管感知、管控与溯源能力。

考核指标：非开源自主可控联盟链平台应支持国家密码管理部门认可的密码算法，并在自主可控联盟链先进的平台架构、安全隐私保护、监管监测等方向具备完全自主知识产权，平台自主代码比例不低于60%，关键核心组件自主代码比例不低于90%；平台每日可处理交易10亿笔以上，支持用户账户数量10亿以上,性能峰值吞吐率100,000TPS以上，交易平均时延小于1秒，链上存储量可弹性扩展；支持区块链身份认证安全保护机制、分级访问控制机制、隐私数据和隐私合约保护机制、国产加密及数据密态运算机制，实现全链路多层级安全隐私保护，支持不少于5种的区块链安全保护机制；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，支持以链治链监管框架，具备3种以上区块链监管能力手段，识别不少于10种异常行为模式，建立非法行为识别信息库，识别准确率不低于95%，形成涵盖金融监管、行业监管和内容监管的区块链协同监管体系；在金融、政务、民生、工业、农业等关键领域选择不少于三个落地示范应用，每个示范应用的注册用户规模不少于10万个；申请发明专利30项以上，软件著作权5项以上，提交国际/国家/行业标准草案3项以上。

5. 重点领域示范应用

5.1 基于区块链的卫生健康数据可信共享技术及示范应用（应用示范类）

研究内容：针对卫生健康数据的可信共享、深度利用等需求，研究基于区块链技术的信息平台，促进标准化、要素化、安全性、隐私保护下卫生健康数据的有效流通及价值发掘。研究区块链适用的多类型卫生健康数据标准、存储机制和链上链下协同交互机制，支持数据的规范上链、可靠存储与可信共享，提升数据存储与协同共享效率，提高链上数据的可用性；研究高协同卫生健康数据的可信共享与查询审计机制，保证数据使用全流程可稽查、可追溯，促进区块链技术在即时质控、精准评估中的应用；研究基于区块链临床路径全生命周期监管体系，加强治疗过程中的程序化，有效促进事故定责、医疗监管应用；研究多角色主体间多方协作机制，并设计面向卫生健康数据的要素化语义网络，运用区块链技术解决身份认证、访问控制、权限管理、确权鉴权、价值评估、权利分配等问题；研究基于区块链卫生健康隐私保护下的用户对齐、协同分析、同态加密等技术，在防范卫生健康数据泄露、滥用、侵权等风险的前提下，实现跨机构卫生健康数据的深度利用；开展基于区块链的卫生健康数据示范应用，有效支撑卫生健康数据的可靠存储以及在多角色主体间的可信共享。

考核指标：提出基于区块链的卫生健康数据可信存储和链上链下协同交互机制与算法，构建覆盖卫生健康领域15种以上国际标准的医学语言系统,包含500万以上医学概念，提升数据共享效率与可用性；提出面向高协同卫生健康数据的可信共享与查询机制，研发相应软件系统与工具；提出多角色医疗主体间的多方协作机制，形成1套支持卫生健康数据要素定义及规则推理的知识图谱，至少包含3000万概念关系，1000条推理规则，解决身份认证、访问控制、权限管理、确权鉴权、价值评估、权利分配等问题；提出不少于3项卫生健康区块链隐私保护技术，研发不少于8种密文等效机器学习和深度学习方法，防范卫生健康数据泄露、滥用、侵权等风险；建成覆盖至少3个特大城市、不少于5000万上链患者真实世界全流程诊疗记录的示范应用平台，有效支撑PB级卫生健康数据的可靠存储以及在多角色医疗主体间的可信共享，产生显著的经济社会效益；申请发明专利20项以上，提交国际/国家/行业/团体标准草案3项以上。

5.2 基于区块链的可信碳交易与碳中和管理示范应用（应用示范类）

研究内容：贯彻国家碳达峰碳中和的重大战略决策，针对构建高比例清洁能源和多主体低碳资源可信交易与电碳协同运行的应用需求，利用自主可控的区块链底层开放框架平台，建立支持全域碳排放可信监测的高性能区块链体系架

构；研究区域碳排放源在线感知辨识、融汇、溯源技术，构建清洁能源生产、交易、消费关键环节和碳足迹全生命周期可信追踪模型、履约执行及实时监管的机制与方法；研究适应低碳清洁能源市场主体低成本接入认证技术和分级安全防护方法；研究基于区块链技术的企业与个人碳数据记录装置与核算交易机制，实现用户大规模参与的情况下碳交易市场的可靠、高效、稳定运行；构建精准的多维碳排放和碳减排追踪、核查、确权和优化系统，并形成基于区块链的碳交易示范应用。

考核指标：提出 1 套面向清洁低碳能源交易的区块链体系架构方案，部署区块链公共服务平台，节点不少于 30 个，交易并发处理性能达到国内先进水平，可为每一笔低碳清洁能源交易的真实性提供可信标记和追踪溯源；研制一套基于区块链的区域碳排放可信管控平台，支持区域碳排放流的全景、精确、可信监测，以及电碳联合市场协同运行，形成涵盖申报、核查、配额分配、交易、清算等环节的智能合约数不低于 10 类，业务响应验证时间满足实际应用需求；选取 2-3 个省级示范园区规模的典型应用场景，开展碳交易与碳中和管理示范应用，绿电交易量电量不低于 3000 万千瓦时，减少碳排放不少于 3 万吨；申请发明专利 20 项以上，提交国际/国家/行业标准草案 3 项以上。