附件1

2020年度区块链领域课题方向和研究内容

**方向1. 区块链技术支撑服务平台关键技术研发与应用**

**研究目标**：构建区块链技术支撑服务平台，降低区块链使用门槛，支撑各类区块链应用建设快速落地。

**研究内容**：（1）研究快速组网建链的技术。（2）研究支持多底层区块链架构和多云服务的区块链资源和数据管控和协同技术。（3）研究跨链技术，实现数据互联互通。（4）研究区块链监管技术，实现平台对区块链网络、节点、数据和智能合约的有效监管。

**方向2. 面向业务灵活适配的区块链共识算法研究**

**研究目标**：推进区块链共识算法领域研究，满足不同业务场景对不同共识算法的需求，提升共识算法效率和区块链性能。

**研究内容**：（1）研究面向多样化业务需求的松耦合、灵活适配的共识机制框架体系。（2）研究面向大规模高频次交易的区块链共识算法及其安全性证明方法，形成自主可控的共识算法。

**方向3. 智能合约关键技术研究与应用**

**研究目标**：针对当前区块链智能合约面临性能和安全挑战，研究智能合约关键技术，提升智能合约性能和安全水平。

**研究内容**：（1）研究智能合约性能提升技术。（1）研究智能合约引擎性能与安全检测技术。（3）研究智能合约形式化验证等安全分析技术。（4）研究基于智能合约的激励机制与应用。

**方向4. 区块链安全与隐私保护关键技术与工具研发**

**研究目标**：面向区块链数据隐私保护需求，突破区块链安全与隐私保护关键技术，提升区块链平台数据隐私水平。

**研究内容**：（1）研究基于对称与非对称相结合的同态加密算法及在区块链中的应用。（2）研究群签名、环签名和零知识证明算法及在区块链系统中的应用。（3）研发区块链数据隐私保护工具，包含链上数据安全加解密、签名、证明等功能模块。

**方向5. 区块链软硬件结合关键技术研究**

**研究目标**：围绕区块链和实体经济融合对区块链基础设施智能化与可信性的需求，研究区块链软硬件结合关键技术，提升源头上链数据的安全性和真实性。

**研究内容**：（1）研究数据可信上链的芯片和硬件技术，提升上链数据的真实性。（2）研究基于芯片和硬件的区块链安全技术。（3）研究区块链硬件唯一性保障技术。（4）研究区块链硬件加速等性能提升技术。

**方向6. 区块链开源模式及标准化研究**

**研究目标**：推动区块链开源生态影响力与区块链技术标准化建设水平，引导区块链技术高质量有序发展。

**研究内容**：（1）研究区块链在政务服务、金融服务、信用体系、智慧城市、卫生健康、公共安全、电子商务等不同领域实施标准，推动北京市区块链应用场景有序建设。（2）研究国内外主流区块链开源社区的运作模式和商业模式，研究研究新型区块链开源生态建设与治理方法，打造拥有国际影响力的区块链开源生态。