《研究课题说明》（供参考）

序号	研究领域	研究方向	研究课题	研究内容	所需专业
1	人工智能-技术研究	AI基础底座	模型引擎及算子优化	一是开展模型推理优化方法研究，覆盖计算图优化、算子融合、内存管理、量化压缩与并行调度等关键技术，建立从基线构建到精度回归的标准化流程； 二是面向金融高并发、低延迟、安全可信等业务需求，研究推理性能与业务可信性协同优化机制，形成可复用、可验证的方法论与工程范式。	计算机科学与技术、软件工程、人工智能、电子信息、数学等相关专业
2		大模型优化	国产异构算力上的大模型推理优化	一是研究国产异构芯片上统一推理运行时、编译与算子优化及自动调优，提升模型与算子的跨平台适配能力和性能可移植性； 二是研究互连与带宽受限条件下的分布式推理，探索拓扑感知的并行切分、缓存复用与计算通信协同调度，提升资源利用率和服务稳定性； 三是研究低比特量化、高效解码与请求感知调度的协同优化，在满足精度和服务时延的前提下提升吞吐，降低单位Token推理成本。	计算机系统结构、计算机科学与技术、高性能计算、软件工程、电子工程等相关专业
3		多模态融合	面向深度伪造攻击的多模态防伪识别技术研究	一是开展多模态防伪检测融合机制研究，探索交易信息、系统环境信息与多类生物特征信号的有效融合与特征关联； 二是开展面向生成式AI的深度伪造攻击识别技术研究，剖析产业化换脸伪造攻击特征，设计面向深度伪造的攻击样本识别算法； 三是开展适配金融支付场景的下一代人脸防伪检测体系架构研究，形成涵盖多模态协同、动态决策与可信认证的总体技术方案。	计算机、人工智能、应用数学、金融工程、统计学、数据科学等相关专业
4	人工智能-应用场景	AI+风控	人工智能风控大模型应用研究	一是面向反欺诈、反电诈、反洗钱场景，研究大模型在超大规模实时交易中的信息理解、风险研判与异常识别方法； 二是针对支付链路跨机构、跨场景风险传导特征，研究多源风险信息融合与关联风险识别方法； 三是围绕AI智能体参与交易支付的新形态，研究智能体交互、授权、决策与执行的风险特征，探索相适应的风险识别机制与风控体系架构。	计算机、人工智能、应用数学、金融工程、统计学、数据科学等相关专业
5		AI+运营	面向业务运营领域的文档治理与知识体系构建研究	一是针对银联多模态业务知识治理难点，结合支付清算业务特性，搭建适配业务场景的智能化知识治理总体框架； 二是运用知识提取技术对文档、语音、图表等多类业务资源进行结构化解析与深度挖掘，抽取核心业务知识，完成知识加工与资产化； 三是对多源异构知识统一梳理归集，构建层次清晰、支持动态迭代的业务知识体系，实现知识高效检索与长效复用，赋能银联数字化智能运营。	计算机科学与技术、人工智能、软件工程、数据科学与大数据技术、信息安全、金融科技等相关专业
6	人工智能-智能体	智能体构建	智能体（Agent）运行态与基础设施研究	一是研究长程任务状态管理、断点恢复与工具调用副作用控制，提升中断和失败后的执行一致性； 二是研究有限上下文预算下的记忆写入、检索与压缩，兼顾信息保真与跨会话一致性； 三是研究执行隔离、运行观测与资源调度机制，建立覆盖任务成功率、恢复能力和成本的评测方法，开展原型验证。	计算机科学与技术、人工智能、机器学习、软件工程、计算机系统结构等相关专业
7			大模型后训练、强化学习与智能体对齐	一是研究领域数据合成与任务轨迹构造方法，结合人工反馈和自动反馈，提高训练数据质量与利用效率； 二是研究面向长程任务的奖励建模、过程监督与强化学习方法，重点解决延迟反馈下的信用分配和低成本探索问题，提升复杂推理与工具调用能力； 三是研究业务规则约束下的偏好对齐、幻觉抑制与结果验证方法，在知识问答、数据分析等任务中评估能力泛化、执行可靠性和约束遵循情况。	计算机科学与技术、软件工程、人工智能、电子信息、自动化、数学、统计学、信息安全、金融科技等相关专业
8			长周期服务中的智能体架构自适应进化技术研究	一是开展金融合规约束下的智能体进化安全对齐机制研究，将规则编码为进化过程的硬约束，防止“进化退化”与策略越界； 二是开展跨会话长周期经验蒸馏与隐私保护继承机制研究，设计面向数天至数周交互周期的关键决策锚点识别与隐私脱敏技术； 三是开展进化过程的可解释评估与专家可控机制研究，确保进化过程的透明度与人工可干预性。	计算机、人工智能、机器学习、软件工程、计算机系统结构等相关专业
9			金融智能体可信互联研究	一是开展互联协议与网络架构研究，融合包括A2A在内通用协议与UCP金融专用协议，探索智能体名称服务、语义感知路由与网络拓扑等关键机制； 二是开展通信安全与信任机制研究，构建端到端加密、抗重放、密码学签名等安全机制，建立基于零信任的跨机构身份验证与动态授权体系。	人工智能、计算机科学与技术、计算机网络、网络安全、通信工程、软件工程等相关专业
10			面向未来机器经济的智能体支付网络关键技术研究	一是开展多智能体并发支付性能建模与评测基准研究，建立涵盖延迟、吞吐量等核心指标的性能评测体系； 二是开展跨机构智能体支付清算冲突协调机制研究，设计冲突消解算法，保障最终结算确定性与安全性； 三是开展面向机器经济的支付网络可扩展性架构研究，探索分层结算网络协议设计、资源调度策略等关键问题，支撑超大规模智能体支付网络稳定运行。	计算机、人工智能、应用数学、金融工程、统计学、数据科学等相关专业
11		智能体安全	智能体治理与安全研究	一是开展智能体评估与准入研究，面向金融业务场景构建智能体评估指标体系与方法，探索基于能力与风险的分级准入管理； 二是开展智能体全链路行为审计研究，建立覆盖任务规划、工具调用与业务操作的全链路关联机制，研究多智能体级联调用的授权传递与权限约束，形成监测、告警、阻断、降级、人工介入与责任追溯相衔接的治理闭环。	人工智能、计算机科学与技术、网络空间安全、信息安全、通信网络等相关专业

序号	研究领域	研究方向	研究课题	研究内容	所需专业
12	数据应用与治理	隐私计算	隐私计算与隐私保护大模型技术与应用研究	一是开展隐私计算互联互通关键技术研究，面向异构平台互通难题，研究安全算子与原语、安全传输协议等核心模块，构建标准化、可扩展的互联互通技术体系； 二是开展数据要素流通标准与技术方向研究，调研数据要素政策标准与演进趋势，研究隐私计算与国家数据基础设施有机融合，助力数据要素安全合规跨域流通； 三是开展隐私保护大模型研究，覆盖训练、微调、推理、RAG及智能体应用等全阶段，研究跨域数据隐私保护方案，确保各阶段隐私安全。	计算机、信息安全、网络空间安全、密码学等相关专业
13		可信数据流通	面向金融支付场景的可信数据流通技术体系研究	一是开展数据可信流通机制研究，探索多主体协同下的权责关系、授权边界与可信交付机制，构建适用于金融支付场景的数据可信流通框架； 二是开展数据受控使用关键技术研究，探索可信执行环境、数据沙箱等技术的适配机制、使用控制与安全边界，以及服务协同与受控计算方法； 三是开展可信治理与审计评价研究，探索数据使用规则的表达与执行、全过程可信审计及效果评价方法。	计算机、数学、人工智能、信息安全等相关专业
14		高质量数据集建设	金融行业高质量数据集建设与数据智能分析研究	一是开展大模型训练高质量数据集研究，探索种子数据扩增、领域知识注入、多模型混合蒸馏等数据合成技术，构建多维度质量评估体系，实现指令、思维链与推理轨迹数据的规模化生成； 二是开展企业知识库技术研究，探索多路径混合检索增强机制与自适应检索策略，建立知识库全生命周期治理体系； 三是开展本体论数据资产语义体系研究，构建智能体可理解、可检索、可执行的语义底座。	人工智能、计算机科学与技术、计算机网络、网络安全、通信工程、软件工程等相关专业
15		数据分析	基于支付大数据的消费经济量化分析方法研究	一是构建基于支付数据的宏观消费监测框架，验证支付数据在宏观经济分析中的有效性，形成覆盖多维消费指标的系统化监测框架； 二是开展政策效应评估与因果推断研究，依托微观支付数据刻画消费行为变迁，构建政策制定与效果评估的量化评估方法论； 三是探索隐私计算、大模型等前沿技术在宏观消费分析与预测中的应用，提升分析框架的智能化水平与预测精度。	经济、金融、计算机、信息安全、统计、数学等相关专业
16		商户经营	基于多粒度空间信息的可信商户数字底座研究	一是开展多模态融合的商户实体对齐算法研究，融合空间、交易与业态多源特征，实现千万级商户高效精准归一； 二是开展空间拓扑驱动的商户置信度评分模型研究，结合图神经网络量化商户物理存在与经营稳定性； 三是开展分级自适应落地技术体系建设，配套标准化校验规则，支撑全量商户场景规模化应用。	计算机科学与技术、人工智能、应用数学、统计学、金融科技等相关专业
17		数据合规使用	人工智能时代的数据应用、共享与隐私保护	一是开展数据安全、隐私保护及人工智能治理相关法律制度比较研究，系统梳理境内外立法监管动态，研判监管发展趋势； 二是开展数据共享开放相关法律问题研究，探索在依法合规前提下跨行业数据合作共享的法律路径； 三是开展生成式人工智能应用数据合规路径研究，涵盖训练数据合法获取与使用、个人信息保护、数据出境与跨境合规等重点问题。	法律、经济、计算机、信息安全、统计、数学等相关专业
18	跨境支付	数字货币	数字人民币2.0支付生态研究	一是研究数币2.0的技术方案和运营机制，包括其智能合约框架； 二是聚焦上海国际运营中心三大平台，分析数币在跨境支付和区块链方面的布局； 三是分析数币发展对银联支付业务的影响，提出应对策略，并对银联支付创新和数币合作提出建议。	经济、计算机、法律、统计、数学等相关专业
19			代币化发展与应用研究	一是研究重点组织和机构在代币化方面的布局； 二是分析传统金融基础设施向代币化转变的必要性，以及代币化发展可能带来的潜在风险； 三是探讨代币化基础设施与传统金融基础设施的融合发展策略。	经济、计算机、法律、统计、数学等相关专业
20	网络安全	密码应用与迁移	密码应用研究	一是跟踪抗量子计算密码国内外标准化进展，开展抗量子计算密码算法研究，并结合银联不同业务场景的性能要求开展算法选型与应用验证； 二是参与国家和行业重点项目及课题任务，结合金融支付相关业务场景，开展抗量子计算密码算法敏捷迁移技术方案设计，并试点开展改造验证。	计算机、密码学、网络空间安全、微电子、数学等相关专业
21		智能攻防	人工智能在网络安全攻防领域的应用研究	一是开展人工智能大模型技术在网络安全攻防中的应用研究，例如智能化漏洞挖掘、智能化攻击渗透等； 二是开展人工智能大模型相关新型攻击手段的防御技术研究，例如AI网络攻击应对等。	计算机、网络空间安全、人工智能等相关专业
22		AI内生安全	人工智能内生安全研究	一是开展大模型内容安全评估研究，构建面向大模型与智能体的安全评测基准，覆盖提示词注入、模型越狱攻击、违规有害内容、个人隐私泄露、幻觉与价值观对齐等维度，建立基于模型反馈的自动化评测方法，形成分类分级的安全评估体系； 二是开展大模型内容安全防护研究，构建输入输出侧检测与拦截机制，研发安全护栏、意图识别、内容审核、越权行为阻断与敏感信息脱敏等技术，实现大模型与智能体交互全链路的实时防护。	计算机、信息安全、网络空间安全、密码学等相关专业

序号	研究领域	研究方向	研究课题	研究内容	所需专业
23	前沿技术储备	量子计算	量子计算与人工智能结合的关键技术研究	一是开展量子人工智能基础理论与算法研究，系统梳理经典AI与量子计算的原理差异与技术互补性，探索金融领域的量子算法创新； 二是开展量子大模型架构设计与高效计算研究，探索量子—经典混合大模型架构，研究量子注意力机制、量子Transformer、量子嵌入层等核心模块，提升量子模型计算效率； 三是开展面向金融场景的量子AI应用研究，围绕金融核心场景优化算法适配性，缓解经典算法在复杂金融建模中的算力瓶颈，形成量子计算支撑金融业务的设计与实现方案。	量子信息科学、量子计算、计算机科学与技术、人工智能、应用数学、应用物理、物理学、金融工程、数量经济学、信息安全、统计学等相关专业
24		区块链	区块链支付基础设施技术研究	一是开展新型支付基础设施理论框架与关键技术体系研究，分析分布式账本、智能合约、原子结算、跨链互操作等技术的适用性与边界，形成支撑支付基础设施演进的理论体系； 二是开展多场景区块链支付原型系统设计与验证，围绕零售支付、批发清结算、跨境B2B等场景，设计基于区块链的原型系统并开展技术验证，为工程化应用提供参考。	计算机、软件工程、密码学、信息安全、电子信息等相关专业
25			面向金融领域应用场景的链网协同基础设施关键技术研究	一是开展链网协同总体架构研究，构建核心支付网络与外部区块链网络隔离可控、协同联动的架构，研究代币服务、网关接入等机制； 二是开展链上链下互操作技术研究，探索交易语义链上表达、账户标记化映射、状态同步及多链互操作机制； 三是开展受监管链上支付安全合规与清算研究，探索链上风险识别、异常交易管控及跨境清算路径等关键方法。	计算机、数学、人工智能、信息安全相关专业