资本市场金融科技创新试点（上海）
项目公示表

填报时间：2024 年 1 月 26 日

■ **试点公示** （对于通过试点申请的项目，《公示表》将在项目公示阶段对社会公开）

□ **辅导公示** （对于通过辅导申请的项目，《公示表》将在项目公示阶段对社会公开，标*项目可酌情填写，或填“暂无”、“不适用”）

一、项目基本信息	1.1 申报单位（以重要性为序逐行列明单位营业执照上的全称）	1.1.1 牵头申报单位： 国泰君安证券股份有限公司
		1.1.2 联合申报单位 ： 中国银联股份有限公司 上海银行股份有限公司
	1.2 项目名称	基于隐私计算和区块链的财富管理数字化精准服务项目
	1.3 项目类型（可多选）	□金融服务□科技产品■业务辅助□合规科技□监管科技 □行业平台□行业基础设施 □其他（需补充说明）：_____
	1.4 应用场景	（试点项目应用业务领域、主要功能、提供的服务、解决的问题等。） 国泰君安、中国银联、上海银行三方秉持“开放共赢”的合作理念，发挥各自领域的数据优势，打破数据壁垒，在安全合规的基础上帮助机构利用外部数据来丰富自身客户画像，通过数据互联互通不断识别和加深对投资者财富管理需求、风险承受能力、产品偏好的了解，从而提供更精准的日常响应维护、更有效的投资者教育、更符合适当性要求的财富管理服务，携手助力普惠金融，推进共同富裕。 项目融合利用隐私计算和区块链技术，共同打造一个安全合规数据共享案例。通过使用隐私计算技术，基于密文对数据进行处理和安全计算，保护数据作为金融机构的核心资产而不泄露，解决数据共享过程中数据的“隐私性”问题；设计合理的授权流程，满足《个人信息保护法》、《数据安全法》等新规要求，充分履行用户授权和个人信息使用告知义务，解决数据共享过程中数

		据的“合法合规"性问题；结合区块链存证等机制，所有操作上链存证、可追溯，构建安全可信的共享环境。
	*1.5 数据应用	（试点项目使用的数据来源，应区分内/外部数据，区分公开/私有数据，明确数据主体、采集方式、数据规模、数据分类、安全级别、数据共享和融合应用安排等。） 本试点项目均由国泰君安、中国银联和上海银行提供合法的数据源，由各机构内部采集、使用、处理及存储，与外部网络充分隔离，合作方基于各自的内部数据进行建模并最终形成多元化的客户标签名单，在客户授权前提下通过隐私计算技术进行名单的安全交集运算，识别共有交集客户群体。
	*1.6 实施计划	（项目研发、测试、上线等各主要阶段时间节点及进度安排。试点申报项目应已完成研发、测试等主要工作，已经在生产环境实际运行或具备在被允许试点之日起一年内上线运行条件。针对分期建设开发的项目，应注明各期或版本的主要内容和日程安排，远期目标可作为单独项目后续另行申报。） 实施计划如下： 1、项目前期准备：1个月，完成前期材料准备，多方业务和技术沟通。 2、系统开发：2个月，完成合作协议、需求确认、区块链模块开发、隐私计算模块开发。 3、项目测试：1个月，完成内部系统改造，功能测试、性能测试、联调测试。 4、试运行：完成财富管理客户标签体系建设和共享场景试运行，进行灰度发布，并基于灰度发布结果调整系统模型，进行系统优化升级。 5、正式运行、成果汇报：正式上线运行，并进行成果汇报。
	1.7 面临的困难及解决思路	（试点项目研发过程中可能或已经面临的各类困难，包括但不限于技术、业务、人力、资金、合规、风控等方面，以及后续解决的方向和思路。） 1、用户授权带来用户体验问题。按照《个人信息保护法》要求，个人信息处理者在处理个人信息前需要获得用户授权同意。信息处理前需要签署授权文件，增加了客户操作的复杂度。在本次试点中，将以友好的交互模式提示客户签署授权文件，且只对于签署了授权文件的客户进行信息查询共享。 2、 隐私计算带来的性能问题。当前隐私计算技术发展仍处于初级阶段，其面临的主要问题是在算法性能方面。当前隐私计算的算法性能相比传统的建模算法性能仍有差距较大，算法运行

		往往需要数秒甚至数十秒，对于金融行业大部分毫秒级的实时性业务具有一定应用局限性。因此在本项目中，在离线情况完成求交算法运行，并在线提供财富管理服务。
	1.8 专利、认证或奖项	（项目所获得的专利、认证或奖项的名称、时间及颁发单位等主要信息。） 1、一种联邦学习的多方安全计算方法及装置 CN202011112386.7，2021 年 1 月 5 日，国家知识产权局。 2、一种联邦学习中的样本对齐方法、装置、设备及存储介质 CN202111140469.1，2021 年 12 月 24 日，国家知识产权局。 3、基于区块链和 IPFS 的高效信任解决方法 CN109639406A，2019 年 4 月 16 日，国家知识产权局。
二、依法合规原则评估	*2.1 涉及的业务场景是否由持牌机构提供	2.1.1 申报机构已取得的证券期货相关法定业务资格名称（本表所称证券期货相关业务指受到中国证监会及其派出机构或相关自律组织认可并进行监管的业务，业务资格取得方式不限于行政审批、备案、登记等）： 证券经纪；证券自营；证券承销与保荐；证券投资咨询；与证券交易、证券投资活动有关的财务顾问；融资融券业务；证券投资基金代销；代销金融产品业务；基金投顾业务；为期货公司提供中间介绍业务；股票期权做市业务；中国证监会批准的其他业务。
		2.1.2 本次申报项目业务场景涉及的业务资格： 代销金融产品业务；基金投顾业务试点资格
	2.2 现行法律法规和监管规定符合情况 (对与项目应用场景相关的业务法规和技术规范符合情况进行梳理分析，是否存在违反禁止性规定的情形)	2.2.1 证券监管部门的相关法规及符合情况（不存在违反禁止性规定的情况，包括但不限于账户实名、资金安全、公平交易、个人信息保护、可控数据跨境流动、反洗钱、网络安全等）： 不存在违反相关法律法规情况。严格按照《个人信息保护法》要求，在信息共享前需要客户签署《个人信息处理告知同意书》，取得客户授权同意后才可以进行相关信息共享和查询。
		2.2.2 行业协会、交易所等自律组织的相关规范及符合情况（要求同上）： 不存在违反相关法律法规情况，同 2.2.1。
		2.2.3 国家或其他管理部门的相关法规及符合情况（要求同上）： 不存在违反相关法律法规情况，同 2.2.1。
	*2.3 出具合规评估意见的机构、评	2.3.1 评估机构名称（公司合规部门或第三方专业机构）： 国泰君安法律合规部

	估时间及评估结论	2.3.2 出具时间（如包含有效期的请注明）： 2024 年 1 月 12 日
		2.3.3 评估结论（最终结论）： 根据现有方案描述，本方案总体风险可控。使用了隐私计算技术以实现信息交互安全可控，依据共享范围最小化的原则进行信息传递，对关键流程和重要节点数据上链存证留痕，并在保障客户知情权和决定权方面进行了机制安排。 **1.信息交互环节采取了多项安全措施，以降低客户信息泄露的风险** 本项目使用了隐私计算中的隐私保护集合交集技术，即基于两家金融机构的名单数据算出交集数据，但是双方都无法获知交集以外的对方集合数据的任何信息。隐私计算技术可以实现数据的“可用不可见”，保障各方数据安全，实现跨行业的数据联合求交、联合建模等场景应用。 交互内容为密文，确保不会造成客户信息泄露。本项目涉及的采集、统计、存储客户信息均在各自内部系统完成，由各自机构完成自主管理和私有化系统部署，三方内部系统充分隔离。三方交互的数据仅为名单 ID 数据，且经过了严格加密处理，极大降低了数据泄露风险。 **2.共享范围最小化** 通过技术手段，严格控制共享的客户范围。本项目使用集合求交算法获得交集客户，确保了共享客户的范围为合作方共有客户（通过手机号、身份证号识别客户），同时确保共享信息的客户均已签署授权文件。 **3.关键流程和重要节点数据上链存证留痕** 利用区块链技术实现多方数据融合应用过程中的交互信息可追溯、不可篡改，确保信息共享有效留痕。一是将信息交互过程留痕，通过把隐私计算技术中涉及的交互流程信息上链存证，二是把客户签署查询授权文件的哈希进行上链存证。有利于防止发生客户未授权的敏感信息交互，及后续内部自查及监管检查追溯。
三、有序创新原则评估	3.1 技术创新情况	（试点项目所使用的新兴技术及为业务赋能的基本原理，与传统技术方案相比的价值体现。涉及多项技术应用的，可逐条列明，同时注明多项技术的融合应用原理与价值。） 1、利用隐私计算技术实现在客户授权情况下数据安全共享，探索实现数据共享合法合规路径。 隐私计算技术是指在无可信第三方的情况下，多个参与方共同计算一个目标函数，并且保证每一方仅获取自己的计算结果，无

		法通过计算过程中的交互数据推测出其他任意一方的输入数据。本项目使用了隐私计算中的隐私保护集合交集技术，即基于两家金融机构的名单数据找出交集数据，但是双方都无法获知交集以外的对方集合数据的任何信息。 2、利用区块链建立可信、平等、可追溯环境，鼓励高质量数据共享。 区块链技术具有防篡改、可追溯、数据存证、智能合约、开放共享等诸多特性，它能摆脱传统模式中对于中心化机构的服务依赖，有利于建立一个平等、互信的执行环境。无论机构大小都能以平等身份加入系统，易于形成平台效应。在本项目中，将客户的授权文件以电子存证的形式进行特征值链上保存。同时和隐私计算技术相结合，将将双方安全求交过程中的信息流上链，有利于后续监管审计追溯。 与传统技术对比: 传统方案，数据交换往往通过第三方中心化机构，数据主权难以保护，还可能由于黑客盗取、系统漏洞等原因造成数据大规模泄露。本方案是基于区块链点对点网状数据共享模式，实现按需共享、点对点共享，基于用户授权后共享，隔离风险、防范风险扩大，区块链构建对等网络，有利于形成平台效应。 基于 PKI 等传统密码学的方案解决了数据传输过程中的保密和安全问题，但是在数据使用环节仍然是明文，这既有损数据源方对于数据保密性的利益，也易发生数据泄露风险。隐私计算则是完全基于密文运算，运算过程中涉及的数据均经过了加密处理，从中反推回原始数据的可能性目前仅存在理论中，同时相对于同属于隐私计算的匿踪查询技术，不经意传输算法的结果仅数据查询方知道，数据源方并不知晓，而隐私集合交集技术的结果对于数据查询方和数据源方都是对等的，更好的帮助数据源方确认用户授权和告知等个人信息保护义务。
	3.2 技术领先优势	（项目技术应用、业务模式、工作流程等属于首创还是对同业做法有显著改进；所用技术先进性衡量指标及相对其他同业做法的主要优势，如：算法、技术路线、设备平台等方面。） 本项目基于国泰君安及相关方已有研究成果进一步优化升级。国泰君安早在 2019 年就承担了中国证券协会重点课题《区块链在行业数据生态建设的应用研究》，提出使用区块链和隐私计算技术助力数据生态建设。该课题获得了年度优秀课题，相关研究成果已被行业广泛认可并应用在黑名单共享领域，本项目基于已有成熟研究成果进一步优化升级，扩展到了财富管理领域，属于行业首创，本先进技术主要优势：

		1、采用金融科技前沿技术，创新性提出基于区块链与隐私计算的综合技术解决方案。 该项目采用隐私计算与区块链结合的技术手段构建跨行业的数据融合应用新典范。隐私计算技术可以实现数据的“可用不可见”，最大限度的保证各方数据安全，实现跨行业的数据联合求交、联合建模等场景应用。利用区块链技术实现多方数据融合应用过程中的交互信息可追溯、不可篡改。同时，结合区块链技术，实现多方数据价值评估策略，还将与监管链打通，助力智能监管。 本项目将对隐私计算平台及区块链平台进行融合应用，隐私计算借助区块链获得了可信执行环境。区块链经过隐私计算获得数据保密能力，两者相互赋能，形成跨行业数据融合应用的创新平台型基础设施。 2、研发基于主流开源隐私计算平台，实现平台自主可控。 该项目拟基于主流开源隐私计算平台研发，确保平台自主可控。平台将实现安全求交、联合建模、联合推理等建模能力，并实现信息存证、平台管理、服务审计等平台管理功能。平台利用业界领先的安全匹配算法、安全机器学习算法进行联合求交、联合建模等工作。
	3.3 服务对象与渠道	（试点项目上线后的预期服务对象，区分内/外部，区分机构/个人；涉及个人投资者的，应详细描述获客渠道、服务方式、适当性要求等；试点单位应按照风险可控原则合理确定服务投资者范围、规模和适当性要求等。） 本试点项目预期服务对象为国泰君安、中国银联、上海银行三方的财富管理个人客户，通过联合服务实现精准交叉获客。在合法合规基础上，通过联合活动、服务短信、MOT 推送、大数据电销等方式开展与客户适当性相匹配的数字化精准服务。
四、风险可控原则评估	4.1 业务风险防控	4.1.1 业务风险点（应结合试点项目特点，描述试点项目上线后可能面临的业务风险，包括但不限于市场风险、信用风险、流动性风险、操作风险、合规风险、舆情风险等）： 1、外部数据源数据质量不高可能导致匹配上的目标人群量级很小，实际服务效果不达预期的风险。 2、模型构建的数据基础不够扎实，有外部环境变化使客户群特征改变导致模型失效，对人群结果形成误判，未能达成精准服务目的。
		4.1.2 风险监测机制（应描述如何采取措施及时发现和准确评估上述业务风险，针对各类风险分别列举）： 1、监测人群匹配情况，确保人群生产过程规范和可控，并确保人群量级，防止因匹配人群量级太小导致服务效果不佳。

		2、跟踪精准服务效果，与未服务人群进行对比分析。根据服务效果不断优化匹配模型。
		4.1.3 风险控制措施(应描述如何采取措施防控上述业务风险,针对各类风险分别列举)： 1、双方业务系统采取了逻辑隔离的方式，仅提供特定人群一对一加密匹配，最大化保护客户隐私及数据安全。 2、模型匹配成果在大规模应用于精准服务前，将进行 MVP 的服务测试，由相关同事对模型匹配的人群质量进行检验，通过后开展全量精准服务。同时对效果进行追踪和归因分析，并对模型进行优化。
		4.1.4 应急预案(应描述如若上述业务风险发生将如何采取有效措施尽可能降低或消除负面影响)： 若效果未达预期需与各合作方检查模型因子，调整模型参数，生成新的匹配人群，再次进行精准服务，总结服务经验，提升服务效果，异常情况暂停业务。
	4.2 技术风险防控	4.3.1 技术风险点(应结合试点项目特点，描述试点项目可能存在的技术风险，包括但不限于网络安全风险、数据安全风险等)： 1、数据安全、平台安全风险：本项目将在国泰君安、银联、上海银行三方搭建区块链节点和隐私计算节点，短期内节点直接通过互联网信道加密通信，存在被黑客攻击、病毒攻击等造成数据泄露的风险。 2、技术安全、算法可信风险：隐私计算技术主要依靠 OT（不经意传输）、PSI（隐私集合求交）等算法实现，这些算法虽然经过了学术界论证，但是正在应用在产业界案例还较少，部分算法由底层代码逻辑封装，对外围相当于“黑盒”，故也可能存在性能较差、潜在未知漏洞等风险。
		4.3.2 风险监测机制(应描述如何采取措施及时发现和准确评估上述技术风险,针对各类风险分别列举)： 1、针对数据安全风险，遵循“早发现、早报告、早处置”原则，加强对网络安全风险、数据安全风险相关信息的收集、分析、判断和监测，建立日常生产运行监控机制，7×24 小时实时监控系统运行状况，对网络流量进行检测，尽早发现其中恶意攻击请求和主机攻击行为，并及时采取相应的措施。 2、针对算法性能和可信风险：进行开源治理、白盒源代码扫描、灰盒应用安全检测，再结合外部威胁情报与漏洞预警平台实时对平台自身安全漏洞做持续性检测。对于性能问题，对核心链路、接口、功能模块、硬件资源等异常情况进行告警，设计超时

		处理机制。建立定期巡检机制，安排专人按照系统巡检手册对系统全链路进行检查，编制巡检报告和结论，对发现的问题及时处理。
		4.3.3 风险控制措施(应描述如何采取措施来防控上述技术风险,针对各类风险分别列举)： 针对上述技术风险，采取如下风控措施： 1、针对数据安全、平台安全风险。在系统上线前进行全链渗透性测试、安全扫描、压力测试，对相关操作人员进行应急处置培训;建立系统IP白名单机制,只允许授权的IP白名单接入系统;建立系统信息隔离机制，做好系统隔离和数据隔离，严控访问权限，降低数据泄露风险。建立数据备份、应用备份、网络备份机制，在发生突发情况下尽快恢复业务系统; 2、针对隐私计算技术风险。对系统进行充分的功能和性能测试、聘请第三方安全检测机构对算法安全性进行认证，保证核心代码自主可控。
		4.3.4 应急预案(应描述如若上述技术风险发生将如何采取有效措施尽可能降低或消除负面影响)： 联合银联、上海银行等合作方一起制定《基于隐私计算和区块链的财富管理数字化精准服务项目应急措施》，并且按照该措施进行定期演练，主要的 应急流程包括： 1、发生异常情况时，三方相关管理人员及技术人员到故障现场进行异常情况分析和处理。 2、现场值守人员及系统管理员进行紧急处理，紧急处理措施包括检查系统日志、重启数据库及相关中间件、重启操作系统等，紧急处理失败情况下切换备份系统，如果切换备份系统失败，需要中止节点运行并通知业务人员，暂停提供服务，待系统恢复后再开展业务。 3、故障处理完成后，需要编写故障报告，并进行留痕备查，对故障过程中发现应急措施不合理的，需要对应急措施进行修正。
	*4.3 投资者保护机制	4.3.1 客户投诉渠道(接受客户投诉的渠道信息，包括但不限于营业网点地址、通讯地址、电话、传真、电子邮箱、官方网站等)： 国泰君安证券官网地址：https://www.gtja.com 国泰君安证券通讯地址：上海市南京西路768号国泰君安大厦 国泰君安证券全国统一服务热线：95521 国泰君安证券反馈邮箱：95521@gtjas.com

		国泰君安证券传真：021-38670666
		4.3.2 投诉处理机制（客户投诉受理与处理机制相关内容，包括但不限于受理部门、受理时间、处理流程、处理时限等信息）： 1、国泰君安在收到客户投诉信息后，将基于投诉基础事实，在保护投资者合法权益的基础上与客户积极沟通，充分协商，促进投诉事项的妥善解决。 2、国泰君安评估后认为本单位无法独立处理重大投诉事项，或重大投诉事项涉及多单位业务、需协作处理的，将牵头成立跨单位投诉处理专项小组，召集相关单位协调处理，妥善处置投诉事项。相关单位在本单位职责范围内配合投诉处理工作。 3、国泰君安通过公司客户投诉管理系统持续跟进并录入投诉事项办理进度、调解情况（如有）、诉讼或仲裁情况（如有）等信息，并上传相关留痕材料，直至所涉投诉事项全部处理完毕。 4、如经投诉事项发现本试点项目在机制、流程、运行、系统等方面存在待整改完善之处，国泰君安将牵头及时、妥善地开展投诉后续整改完善工作，与联合申报单位一起制定项目整改方案，并对重要材料予以留痕。
		4.3.3 风险补偿机制（应描述申报单位就本试点项目建立的风险补偿和赔付机制，确保试点项目出现意外风险时能够及时对投资者损失进行合理补偿，降低试点项目的负面影响。对于多个单位联合申报的试点项目，应明确风险补偿责任主体）： 国泰君安与联合申报单位一起制定风险补偿机制，基于区块链不可篡改记录，对进行相关历史记录进行追溯，明确风险责任主体、制定风险赔付机制，切实保障金融消费者合法权益。对于非客户自身责任导致的资金损失，提供合理补偿，降低试点项目负面影响，充分保障消费者合法权益。
		4.3.4 项目退出机制（应描述试点项目因发生特殊情况需终止或下线时的工作安排。项目退出应平稳有序，确保投资者资金和数据安全，最大程度减少对市场的负面影响。退出机制包括但不限于退出触发条件、业务退出安排、技术退出安排等内容）： 国泰君安与联合申报单位一起制定项目退出预案，在保障用户信息安全的前提下进行系统平稳退出。 （1）技术退出。数据处理方面：按照《网络安全法》、《个人

		金融信息保护技术规范》等要求，完成业务数据、交易数据等数据信息备份，归档和清理，保护用户数据信息安全，确保用户其他业务不受影响。资源回收方面：停止本项目相关的系统资源、服务包括服务器、基础组件等，取消三方网络防火墙权限，关闭合作方网络白名单，确保系统安全稳定退出。 （2）业务退出。根据合作方所签署的相关协议中约定的期限，存量业务在规定时间内有序退出，后续不再接受新用户。做好舆情监控，确认业务退出的影响范围，与联合申报方一起确定整改计划。按照整改计划，所有合作方流程关闭后，下线相关业务场景。 （3）客户退出。在客户主动取消授权，或者要求退出试点计划的情况下，允许客户主动退出。在获得授权许可或请求后，对与试点项目相关的数据进行清除，并将客户进行标识，后续不再将客户纳入试点项目运行计划中。

附页：

牵头申报单位承诺	本单位郑重承诺： 1. 本单位在申报资本市场金融科技创新试点（上海）项目过程中，所提供的一切申报材料信息真实、准确和完整。 2. 申报项目符合依法合规、有序创新、风险可控的申报原则。 3. 申报项目不存在违反法律和行政法规情况，不包含国家秘密信息。 4. 本单位将配合监管部门完成后续评审公示、监督检查或风险处置等工作。 5. 本单位已全面开展合规性评估和内控审计，能够有效保障业务连续性和用户信息安全，保证资金安全。 以上承诺如有违反，愿承担相应责任与后果。 单位（公章） 法定代表人（签字）： 2024 年 2 月 19 日

联合申报单位 1 承诺	本单位郑重承诺： 1. 本单位在申报资本市场金融科技创新试点（上海）项目过程中，所提供的一切申报材料信息真实、准确和完整。 2. 申报项目符合依法合规、有序创新、风险可控的申报原则。 3. 申报项目不存在违反法律和行政法规情况，不包含国家秘密信息。 4. 本单位将配合监管部门完成后续评审公示、监督检查或风险处置等工作。 5. 本单位已全面开展合规性评估和内控审计，能够有效保障业务连续性和用户信息安全，保证资金安全。 以上承诺如有违反，愿承担相应责任与后果。  单位（公章） 法定代表人（签字）： 2024 年 2 月 26 日

联合申报单位2承诺	本单位郑重承诺： 1. 本单位在申报资本市场金融科技创新试点（上海）项目过程中，所提供的一切申报材料信息真实、准确和完整。 2. 申报项目符合依法合规、有序创新、风险可控的申报原则。 3. 申报项目不存在违反法律和行政法规情况，不包含国家秘密信息。 4. 本单位将配合监管部门完成后续评审公示、监督检查或风险处置等工作。 5. 本单位已全面开展合规性评估和内控审计，能够有效保障业务连续性和用户信息安全，保证资金安全。 以上承诺如有违反，愿承担相应责任与后果。 单位（公章） 法定代表人（签字）： 2024年 2 月 19 日