# 隐私计算开源创新 数据市场有望提速

**本报记者 李晖 北京报道**

随着数据要素市场培育提速，隐私计算作为数据安全流通的关键技术，如何加快其技术开发以及商业化的速度成为市场关切。

市场共识在于，在隐私计算“商业化大网”中，算法迭代、开源生态和场景普及缺一不可。去年10月，央行等部门联合印发《关于规范金融业开源技术应用与发展的意见》，强调“鼓励开源技术提供商，加快提升技术创新能力，切实掌握开源技术核心代码，形成自主知识产权，夯实产业支撑能力”。

《中国经营报》记者从多位业内人士处了解到，当前国内开源方日渐增多，但依据的相关标准自成体系，目前金标委、银行业协会、信通院等机构均在加快相关工作，与业界共同推动开源技术标准建设与信息化规划的衔接配套。记者近期获悉，蚂蚁集团已正式开源其隐私计算框架。

## 市场培育亟须技术降门槛

**不同技术路线的隐私计算产品在互联互通上存在先天壁垒，也加重了数据孤岛问题。**

国家工信安全中心测算数据显示，“十四五”期间，我国数据要素市场规模将突破1749亿元，整体上进入高速发展阶段。作为解决数据安全流动的关键技术，隐私计算行业的发展备受关注。

IDC数据显示，2021年中国隐私计算市场规模已突破8.6亿元，未来有望实现110%以上的市场增速。艾瑞咨询预计，到2025年，中国隐私计算市场规模将达到145.1亿元。

市场规模爆发与市场需求和技术普及速度高度相关。在蚂蚁集团隐私智能计算技术部总经理王磊看来，数据交易要素市场化存在四个关键因素，分别是高价值数据源、产业化应用、数据交易市场和隐私计算技术，但四个要素目前均面临亟须解决的问题。

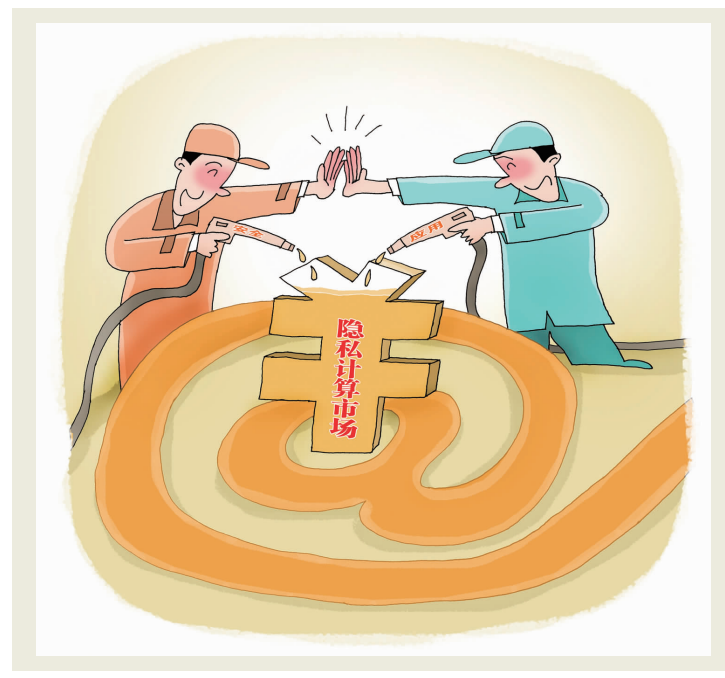
“数据交易市场目前的确权和定价机制是不太完善的，市场上也缺乏高价值数据，目前隐私计算的产业化应用更多是在金融领域的风控环节和少量营销场景，场景不够丰富，这也是蚂蚁集团决定开源其隐私计算框架的重要原因。”王磊表示。

中国信通院调研统计显示，55%的国内隐私计算产品基于或参考了开源项目。一位隐私计算创业公司人士向记者透露，从技术开发的供给侧看，如果每遇到一个新场景都从头开发，不但导致技术资源浪费，而且数据安全和隐私合规很难保证。从银行等金融机构需求侧看，不同技术路线的隐私计算产品在互联互通上存在先天壁垒，也加重了数据孤岛问题。

此外，隐私计算自诞生起就存在“数据黑盒”问题。在算法监管日益严格的当下，开源通过算法协议和实现方案的公开可验证有利于使用者了解其技术逻辑，促进技术透明化，并及时发现问题。

记者注意到，近年来监管、消费者权益保护及自身风控等对算法和模型的安全性及可解释性的要求越来越高，也推动了行业技术透明化趋势。比如，《个人信息保护法》明确要求，自动化决策结果对个人权益有重大影响时要能说明清楚原因；2021年3月，央行发布并实施的《人工智能算法金融应用评价规范》也要求，应用AI算法需满足安全性和可解释性；2022年年初，银保监会颁布《银行业、保险业数字化转型指导意见》，其中特别提到防范模型和算法风险，要求确保模型的可解释性和可审计性。

这种“可解释性”其实面向了金融业务中的多个相关方。华夏基金董事总经理、首席数据官兼首席技术官陈一昕向记者表示，“可信”即包含了“可解释性”的含义。对开发者来说，可以保证后续调优改进过程的有效进行；对于应用用户，比如保险保费定价系统的客户而言，可以为模型给出的不同定价结果做出详细说明；对于金融监管者，可以保证其从全流程上对AI模型进行约束并防范金融风险。



“十四五”期间，我国数据要素市场规模将突破1749亿元。 视觉中国/图

据记者了解，蚂蚁集团的隐私框架“隐语”主要定位于解决技术先进性和技术长期发展问题。相对于国内侧重某一类技术的开源平台，其通用框架目前支持包括多方安全计算（MPC）、联邦学习（FL）、可信执行环境（TEE）等在内的多种主流隐私计算技术，也支持多种技术进行灵活组合。同时，“隐语”已向社区开放了多方安全计算和联邦学习的核心代码。

上述多技术灵活组合的趋势也是降低行业使用门槛的一种方式。中国信通院云大所大数据与区块链部副主任闫树向记者表示，去年以来，隐私计算行业出现几个明显趋势：第一是如何加速性能；第二是如何提升产品稳定性；第三是真正从操作、算法二次开发、方便部署、说明文档等方面降低使用者门槛。整体看，适配不同场景，不同规模的数据，在安全和性能之间再平衡的产品越来越多。

## 标准化建立需求迫切

**隐私计算跨平台互联互通不只需要在技术层面进行攻关，更需要在商业层面继续突破，同步推广运营实施标准。**

事实上，伴随去年隐私计算进入“商业化试点”后，技术路线赛马的现象日益明显。

记者不完全统计，近年来，国内外很多大厂和创业团队都在积极开源，在隐私计算技术范畴，至少包括百度的PaddleFL、Mesa-TEE，阿里达摩院的Federated-Scope等。其中，较为知名的是由工商银行、中国银联、微众银行、VMware、星云Clustar等多机构共同治理的FATE开源项目/社区。此外，由产学研用近50家单位联合发起的国内首个国际化自主可控隐私计算开源社区——开放群岛（Open Islands）开源社区也在今年5月成立。

各技术流派的公司各自为战，采用不同的技术架构，开源软件的标准并不一致，这也导致不同技术范式之间很难连通，不仅给金融机构的决策带来难题，还可能形成数据“大孤岛”。因此，加快推进开源隐私计算技术应用的标准化已成为业界共识。

记者了解到，目前多个相关部门已推动隐私计算相关技术标准建立。闫树向记者表示，从标准体系层面规范隐私计算跨平台互联互通势在必行，中国信通院云大所牵头的隐私计算联盟、大数据技术标准推进委员会（TC601）也正在推进相关技术标准的研讨和编写。

中国银行业协会首席信息官高峰指出，开源软件需要遵循相应的工作标准，包括流程标准、技术标准、运营标准、推广标准、知识产权与法律标准等。中银协倡导各会员机构，加强开源技术及应用标准化建设，瞄准一些急需的、重点的领域，加快标准制定与实施。加强开源技术标准建设与信息化规划的衔接配套，依法合规使用开源技术。

“虽然《个人信息保护法》和《数据安全法》已经出台，但实践中尚无法律判例，技术在一些场景使用时会逐步迭代，法律界和技术界会根据实践逐步取得一些共识，互相推动前进。”王磊表示。

此外，面对目前市场上的众多开源方，开发方和使用机构更关注哪些指标？王磊指出，银行在招标和共建时主要关注技术的易用性和合规性，如果一个框架使用门槛高就很难用起来。另外，比较关注技术合规标准问题，但这方面行业仍在摸索阶段。

一位股份制银行技术部门人士向记者透露，目前在各种隐私计算的开源框架中，联邦学习开源框架相对比较成熟并逐渐形成主流，大型商业银行通常考虑在成熟框架上自研，从联合开发起步。

王磊同时指出，目前很多隐私计算产品的标准化程度比较低，定制压力大。相关技术和产品的标准化，将有利于推动隐私计算行业的商业化。

闫树认为，隐私计算跨平台互联互通不只需要在技术层面进行攻关，更需要在商业层面继续突破。需要充分结合具体业务的落地需求，可以在研讨编写技术标准的同时，同步推广运营实施标准。

而与创业性公司相比，大厂在技术培育的周期上普遍拥有更多耐心。王磊认为，盈利不是这一业务当前的最大诉求，由于隐私计算是助力整个国家数据要素市场化建设的关键技术，未来数据要素市场形成后会有很多新的商业化机会。

# 防风险力度加大 银行严控贵金属交易

**本报记者 王柯瑾 北京报道**

近期，国际金融市场波动加剧，银行个人贵金属交易业务再现收紧。

工商银行公告表示，对代理上海黄金交易所个人交易业务、个人贵金属延期交收合约的开仓交易和个人黄金现货实盘合约的买入交易作出调整。

《中国经营报》记者注意到，除工商银行外，自去年以来，包括中国银行、建设银行、兴业银行等多家银行发布关于个人贵金属业务调整的公告。业内人士分析称，银行根据市场环境变化对相关交易业务进行调整，有利于防范风险。未来，银行贵金属衍生品对个人投资者会进一步趋严，投资者应该在市场波动大时理性选择，增强投资稳健性。

## 业务收紧防范风险

根据工商银行上述公告，自北京时间2022年7月8日收盘清算时起，Au（T+D）、mAu（T+D）、Au（T+N1）、Au（T+N2）、NYAuTN06和NYAuTN12合约标准交易保证金比例将从34%上调至42%，Ag（T+D）合约标准交易保证金比例从38%上调至46%，差异化保证金同步调整。

此外，自北京时间2022年8月15日9:00起，工商银行将暂停代理上海黄金交易所个人贵金属延期交收合约的开仓交易和代理个人黄金现货实盘合约的买入交易，代理个人延期交收合约的平仓交易和代理个人黄金现货实盘合约的卖出交易不受影响。

光大银行金融市场部宏观研究员周茂华表示，“结合以往案例，近期部分银行收紧个人贵金属业务交易主要还是防范潜在风险，保护投资者合法权益。目前，贵金属市场面临复杂环境，波动加大，对于投资者来说行情可预测性下降，潜在风险加大，尤其是部分交易品种带有杠杆。”

一位国有银行研究人士表示，“贵金属投资对个人投资经验和风险承受能力要求较高，尤其是在衍生品交易中，杠杆率较高，投资者面临的风险较大。近期全球大宗商品价格大幅波动，贵金属价格波动也较大，进一步加大了投资者所面临的风险。银行调整贵金属业务，是保护投资者合法权益，推动做好风险管理。”

近日，在美元强势格局下，国际金价创下新低。7月12日，COMEX黄金一度跌至1721.6美元/盎司低点，逼近“千七”关口。

7月6日，上海黄金交易所发布通知称，近期受国际因素影响，全球大宗商品价格出现大幅波动，市场风险明显加剧。各会员单位提高风险防范意识，做细做好风险应急预案，提示投资者做好风险防范工作，合理控制仓位，理性投资。

下转 B2

# 监管规范信用卡催收

**本报记者 杨井鑫 北京报道**

监管规范信用卡业务及债务催收行为再加码。

日前，中国银保监会、中国人民银行发布了《关于进一步促进信用卡业务规范健康发展的通知》，分别对银行信用卡发卡营销行为、授信管理和风险管控、资金流向管理、分期业务管理、合作机构管理、消费者保护等方面进行了规范。值得注意的是，在消费者保护内容中明确规定：必须严格规范催收行为，不得对与债务无关第三人催收。

据《中国经营报》记者了解，当消费者信用卡债务逾期且银行催收无果后，银行往往会将该笔债务委托给第三方机构进行催收，也就是所谓的催收公司。而催收公司在利益驱使下会采取各种不当手段迫使消费者偿还债务，较常见的方式则是“爆通讯录”，即通过给债务无关第三方施压，变相向债务人催收。

市场人士称，银行外部委托催收方式合规性有待加强。鉴于债务的委托人是银行，一旦催收公司在实际业务中出现侵犯隐私、暴力催收等行为，银行也难逃责任。也就是说，在合规性要求下，银行对于外部委托机构合作门槛将进一步提高。

## 投诉居高不下

90天，通常情况下是银行给到客户欠款逾期的极限。一旦超过了90天，银行在内部催收无果的情况下，就会选择委外催收。

实际上，在银行内部催收和外部催收之间存在很大区别。据记者了解，银行员工对信用卡账户逾期90天内的客户主要是以电话方式为主进行催收，也会到客户的经营场所或住所进行提醒。但是，在催收公司接手债务催收工作后，所谓的催收力度就完全不一样，这其中就包括了“爆通讯录”方式。

一家国有银行某支行人士表示，“银行在催收工作中会比较柔性，也不会出现过激的行为，甚至不会让客户在外人面前难堪，这是基于尊重和隐私保护。”

该人士明确表示，第三方催收公司是与银行签订协议的，前者为后者提供催收服务。双方约定在催收到款后会有分成，而催收能否成功与催收公司的收益是挂钩的。

按照他的说法，银行与催收公司的催收流程是一样的，从打电话到上门，但是催收力度不同。据记者了解，为了分成收益，催收公司在催收过程中的手段和套路往往很多，甚至出现过很多暴力催收的情况。

一家国有银行人士认为，催收公司为了与银行达成长期合作，必须要在催收方面“出成绩”，这也会让催收公司的工作人员在压力下采取过激的方式。

然而，催收公司出于业绩考量的某些极端行为，却导致银行相关业务投诉量高企。

从银保监会及地方分支机构公布的银行业消费者投诉中，涉及信用卡的投诉一直居高不下。6月15日，上海银保监局公布了2021年辖内银行业消费投诉情况，在上海银行业消费投诉的事项中，涉及信用卡业务投诉的共有6.46万件，占投诉总量的87.8%。按照投诉的原因划分，催收及征信类的最多，超过2.34万件。

6月2日，广东银保监局公布的2022年一季度银行业消费者投诉情况通报中，辖内机构涉及信用卡业务的投诉量为2504件，环比下降了23.38%。但是，该类投诉在投诉总量中的占比仍然高居58.77%。

一家股份制银行在2021年年报中称，该公司的消费投诉量共计14.3万笔，其中信用卡业务占比达到了86.48%，投诉原因涉及到债务催收方式和手段的投诉占比达到了66.22%。

## 强化约束力度

记者在采访中了解到，消费者在信用卡长时间逾期后，家人、同事、朋友受到催收骚扰情况并不少见，其中恐吓、威胁的情况也时有发生，这也是通常的“爆通讯录”方式。传统的“爆通讯录”是手机上的通讯录被上传，然后被给到催收机构。但是，目前上传手机通讯已经受到了严格限制，仅限于消费者预留的联系人方式。

“对于一些大额的欠债，可能催收公司还是会千方百计地找到消费者身边的亲人、朋友或同事，通过个人的声誉影响对消费者施压。”一位知情人士表示，这种行为实际已经超出了通知的范畴，影响到了债务无关的第三方。

自2019年以来，在国家对“套路贷”“暴力催收”等违法违规行为进行打击的同时，部分催收公司也被处置。

2021年11月，全国金融服务商核心委外机构营业额第二的催收公司团伙——湖南强贲被查，湖南长沙市公安局召开新闻通报会通道了这起特大的公民个人信息案情况，当场抓获犯罪人员177名，扣押冻结资金超过500万元。经调查，该公司主要承接金融机构不良资产管理及信用卡催收业务服务，合作对象覆盖了多家国有银行、股份制银行和中小银行。

据了解，该催收公司从银行获取客户的基本信息用于催收，但同时也将这些信息进行贩卖获利，而这些行为已经超出了其与银行的合作和约束。

“银行在催收方面与第三方催收公司合作是合法的，但是第三方催收公司在催收过程中的行为不容易规范。”上述国有银行人士称，银行只能在合作机构招商过程中做出具体的条款约束，一旦出现违规行为即终止合作。

实际上，第三方违规催收行为并非不能对其合作银行造成影响。

2021年12月17日，北京银保监局发布《关于加强信用卡消费者权益保护的通知》指出，加强信用卡催收业务管理，规范信用卡催收行为和催收用语。严禁对与债务无关的第三人进行催收，银行在可以联系到持卡人的情况下不得联系与债务无关第三人；在联系与债务无关第三人时，仅用于取得持卡人的联系方式或转告持卡人联系银行。当第三人明确愿意为债务人偿还欠款时，可提供还款所需必要信息；当第三人明确要求不得联系时，催收人员不得继续进行联系；严禁冒充司法人员催收，催收人员不得使用“找单位”“找家人”“已经违法”等相关含义以及暗示套现还款的表述；信用卡催收过程应当进行录音，录音资料至少保存2年并能够按照监管机构要求及时提供备查。

2022年6月，北京银保监局的一纸罚单将两家股份制银行推到了“银行催收”的舆论中心。该罚单显示，两家银行的信用卡中心因信用卡催收严重不审慎，被监管责令整改并处以罚款。

如今，监管规范催收行为再加码，对于银行而言，无疑将进一步强化其对于催收委外机构的约束意识和力度。有银行人士称，面对催收委外的逐步规范，催收公司暴力催收、爆通讯录等行为风险越来越高，也不可持续。银行消保部门将加大对第三方合作的规范要求，甚至会终止与一些催收公司合作。