金融机构小程序运营的现状、问题及对策

◎于涛　余孟严

摘要：金融小程序已快速发展成各类金融机构的自营网络阵地。金融小程序通过金融机构与用户的相互链接，积极发现和满足金融服务需求，不仅推动了金融机构尤其是中小金融机构的数字化转型，也提升了金融服务水平。然而，金融小程序的业务开展和完成均是在互联网平台上进行的，在业务服务时对消费者以及监管部门来说并不可见，独立性存疑，数据安全性未得到广泛认可，存在隐私保护、安全隐患等问题，影响消费者权益和金融安全。事实上，金融小程序通过一系列的技术设置和合同约束，在独立性和安全性上能够实现必要的保障。因此，认可金融小程序为金融机构自营场所，并通过合规约束加强风险管控，既是平台金融常态化监管的具体举措，也是从功能监管到行为监管的具体体现。

关键词：小程序；独立性；数据安全；行为监管

中图分类号：F832　　**文献标识码：**A

金融机构小程序（以下简称“金融小程序”）是金融机构数字化转型的具体体现，虽然有效提升了金融服务水平，但在独立性和安全性等方面存在一些问题和认知分歧。正确认识金融小程序的业务实质并进行有效的合规管控，有助于促进金融小程序稳健发展，更好提高金融服务效率。

一、金融小程序运营的现状和特点

小程序是指不需要下载安装即可使用的应用程序，用户可借此进入应用并获得相应服务。从技术上看，小程序是平台内的云端应用（无须安装），不是原生移动互联网应用程序（Application，APP），通过 Websocket 双向通信（保证无需刷新即时通信）、本地缓存（图片与 UI 本地缓存降低与服务器交互延时）以及互联网平台底层技术优化实现了接近原生 APP 的体验。

小程序自 2017 年出现后，凭借“无须下载、无须安装、触手可及、用完即走、无须卸载、不占内存、开发成本低”等优势，相关技术和生态迅速

作者简介：于涛，国务院发展研究中心金融所副研究员；余孟严，首都经济贸易大学国际经济管理学院。

发展，已经成为各类商家、金融机构[①]触达和服务客户的重要线上渠道。当前，主要平台小程序数量已经超过 800 万个，日活跃用户超过 8 亿人，年度成交总额达数万亿元。金融小程序更是成为金融机构智能化和数字化转型的重要载体。

（一）金融小程序的基本功能

金融小程序优化、拓宽了金融机构的服务功能。当前，金融小程序已经发展成为各类金融机构重要的展业工具，在 APP 前端发挥补充和导流作用，主要提供以下四类功能：一是信用卡业务，部分银行通过小程序提供信用卡申请、账单查询、额度查询、积分查询等基本功能；二是网点服务，多数银行实现了基于位置信息的网点查询、排队查询、排队预约等功能，为用户提供便民服务；三是资讯类功能，如可通过小程序提供实时外汇、贵金属、结售汇等信息；四是理财业务，部分银行通过小程序应用展示和销售理财及理财子产品。当前，支付宝平台入驻金融类小程序超过 2400 个，涵盖了信贷、保险、基金等不同业态的主体。

（二）金融小程序的特点优势

相较于监管部门已经认可的 APP 和 HTML5[②]（以下简称“H5”），金融小程序具有鲜明优势，提供了线上引流的新渠道，能够流畅便捷、低成本、高效的提供金融服务，是数字金融发展的最新形态，既提升了金融服务的效率，也提高了金融服务的质量，推动金融机构数字化转型加快发展。

金融机构小程序迎合个人线上化趋势，在触达客户引流方面具有鲜明优势，明显提高了金融机构的营销效率。一是金融小程序成为金融机构提供线上服务的新渠道。数字经济及移动互联网的发展，推动了个人金融服务模式的升级。随着年轻客群和中老年客户普遍的线上化转移，线上金融服务需求已经成为基本的业务诉求。小程序模式凭借其操作的便利性与灵活性，积极回应金融服务需求，促进线上与线下场景融合，有效助力金融机构实现增量市场的渠道创新与拓展。二是金融小程序无须下载安装即可使用，基本具备 APP 功能，体验顺畅、推广便捷。APP 的下载需要耗费较多的时间和流量、占用更多的手机存储空间，这都降低了用户的下载意愿，使得客户非必要不安装。相较而言，小程序具有较高的营销效率，被推荐用户一经访问即可完成关注，几乎不占用客户额外时间，服务请求延时较少，也没有流量和内存的顾虑。

小程序和自有 APP 在开发维护成本方面存在较大差异。从开发成本看，自有 APP 由于存在技术开发和维护工作量大、需要单独的服务器资源部署等原因，成本以千万元甚至亿元为单位，而小程序的开发维护成本较低，甚至通过云端共享可实现基于频次使用的廉价收费。并且，移动端开发一般需要兼顾 IOS 和 Android 两个平台，必然提高开发成本。

综合来看，小程序是金融机构尤其是中小金融机构数字化转型的关键支撑。自有 APP 是大型金融机构数字化转型的重要工具，但由于开发成本高、新用户引流拓展主要依靠自身资源等原因，很难成为数千家中小金融机构的优选。总之，金融机构通过互联网开放平台提供的小程序等服务，不仅为大型银行业金融机构、股份制银行、中大型城商行提供了用户服务补充入口，也为缺少自有 APP 的中小型农商行等提供了触达和服务互联网场景用户的主要入口，成为推动中小金融机构数字化转型的可靠工具。小程序实质上成为中小金融机构借助金融科技提升自身服务水平和竞争力的关键选择。

二、金融机构小程序运营存在的问题

在快速发展中，金融小程序运营存在独立性质疑、隐私保护、安全隐患等问题，进而涉及消费者权益保护、金融风险等。金融业务的敏感性、风险性、

① 银行业金融机构通过移动互联网自营渠道触达用户的方式通常有三大类，包括自有 APP、官方网站和基于应用软件开放平台接口开发的自营渠道，如微信 / 支付宝小程序、微信公众号、支付宝生活号等。

② HTML5 是 Hyper Text Markup Language 5 的简写，是构建 Web 内容的一种语言描述方式。HTML5 利用 Web Worker 将 Web 应用程序从原来的单线程业界中解放出来，通过创建一个 Web Worker 对象就可以实现多线程操作。

创新性、复杂性，加之小程序本身的安全性、稳定性等，都凸显出金融小程序安全运营的复杂性和重要性。

（一）金融小程序的独立性问题

作为金融机构应用金融科技的新形态，金融小程序尚未被周知，未彻底解决独立性质疑。有质疑认为，由于金融小程序依赖于互联网平台，开放平台有能力直接决定小程序获取信息的方式和范围，因而金融小程序并不具有独立性。事实上，金融科技不断介入传统金融机构业务是大势所趋，对金融机构的解构和重构仍在过程中，对传统金融业务的重塑也在各个环节、流程和模式上梯次实现，小程序就是新近形态。在小程序下，金融机构的业务开展和完成均是在互联网平台上进行的，在业务服务时对消费者以及监管部门来说并不能直观显示和外部可见，不如传统金融机构在物理网点或 APP 中展业明显，相关的金融监管也是在探索中逐步实现，这都容易令人对金融小程序的独立性产生疑问。

（二）隐私保护和数据安全问题

小程序在个人信息流转全生命周期的主要环节（收集、使用、对外提供 / 传输、删除）中均可能存在一定的违反个人信息利用规定的问题。这容易给不法分子利用小程序进行作弊欺诈、恶意植入木马或病毒、篡改业务数据、盗取用户隐私信息等行为留下漏洞，存在一定的安全隐患问题。若未经有效防护，在客户与小程序交互过程中，金融小程序容易发生隐私数据泄露等安全事件①。例如，银行小程序的核心代码若泄露，就容易产生较大的安全隐患。

此外，由于小程序在本质上是 Web 应用，在应用开发方式、功能交互、应用交付流程等方面与普通应用程序并没有根本差异，因此并不能避免传统的应用安全问题。如果应用开发商没有将安全防护能力覆盖到小程序，有可能使其成为黑客入侵的突破口。

总之，针对上述问题以及可能的诸多风险，有种观点认为，金融小程序需要页面跳转到金融机构自有 APP 之后完成相关业务（所谓“跳端”），以更好规避风险、维护金融消费者合法权益。

三、满足合规约束的金融小程序可视作金融机构自营网络平台

小程序作为一种云端应用程序，是金融机构 APP 嵌入互联网场景平台的精简版。

（一）金融小程序在合规后具有独立性

金融小程序通过一系列的技术设置和合同约束（用户协议）维护了金融机构独立管控和技术独立性，保障了其完整的数据权限，并实现了法律独立性。

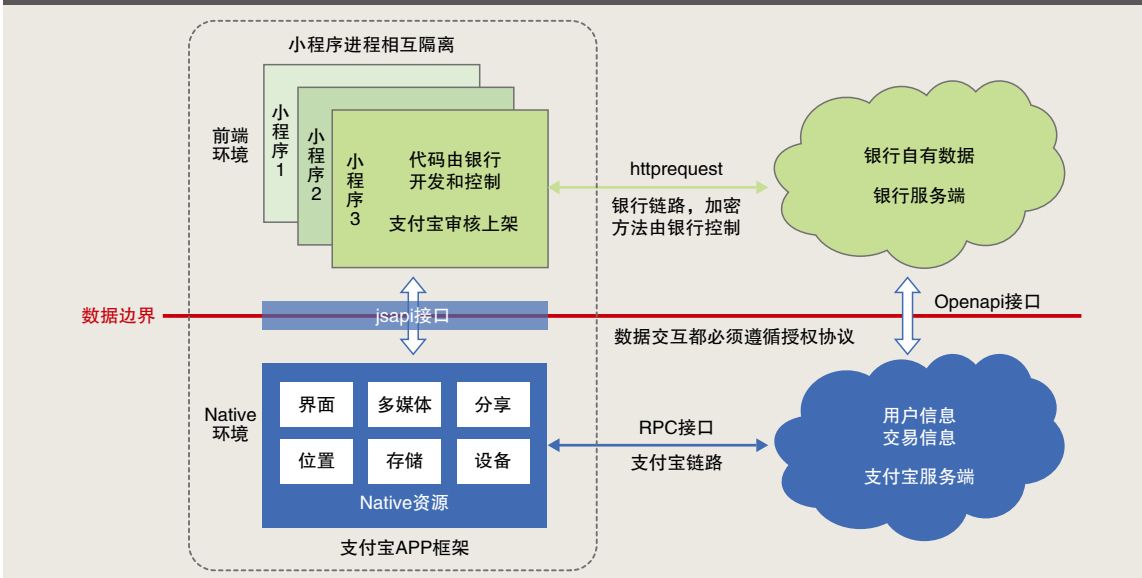
一是金融小程序在技术上有独立性，为金融机构独立管控。互联网平台受金融机构委托为其提供小程序技术框架和开发工具，并不介入服务流程。小程序的客户端代码和服务端代码，权属方均为金融机构，相关小程序的代码也由金融机构完全控制。小程序与金融机构之间传输数据的加密方法由金融机构控制，密钥可以在端上加密存储或存储在小程序云端。

二是金融小程序运行独立。每个小程序启动时，以独立进程运行，与互联网平台进程及其他小程序均隔离。在信息交互干预方面，开放平台不参与信息的处理，仅仅起到传输信息的技术支持作用，无法获取、存储金融机构在运营过程中通过小程序向用户传输的信息（见图 1）。账户管理、资金管理等服务仍由金融机构提供，平台只提供页面搭建装修等技术服务。

三是金融小程序具有完整的数据权限。小程序上金融机构的自有数据，存储在金融机构自身服务端，相关数据和信息无法被平台或其他小程序获取，互联网平台仅为传输信息提供技术支持。在数据处

① 2021 年 3 月，网信办等发布的《常见类型移动互联网应用程序必要个人信息范围规定》，明确将小程序纳入管控范围。

图1 支付宝小程序基本架构



资料来源：支付宝官网

理能力方面，小程序开放平台无法定点处理小程序内每个具体信息，若一定要屏蔽某个信息，只能对该小程序断开服务，和浏览器断开链接、屏蔽展示类似。相关金融服务在银行自有机房完成，用户和交易数据均记录在银行自有机房，银行与平台的通讯通过专线对接，同时有对应安全通讯措施保障通讯的信息安全，银行享有完整数据权限。

四是金融小程序独立性获得法律认可。法院判例认为[①]，从技术原理来看，小程序是开发者独立运营的一组框架网页架构，只通过指定域名与开发者服务器通信，开发者服务器数据不保存于互联网平台，开发者通过小程序直接向用户提供数据和服务。互联网平台无法进入开发者服务器查看或处理相关内容。互联网平台对小程序开发者提供的是架构与接入的基础性网络服务，系根据不特定类型服务对象指令自动提供技术服务。互联网平台的服务本身不主动参与信息的处理，信息接入 / 传输由服务对象发起，由基础性网络服务的固有技术设置接收处理，服务对象可以进行任何互联网增值服务或应用，其系被动处理传输信息。此外，从处理能力看，基础性网络服务无法对服务对象提供的信息内容进行具体处理，其处理的客体是作为整体的信息载体数据或信息传输通道，而非细分到每一个具体信息项目的内容。

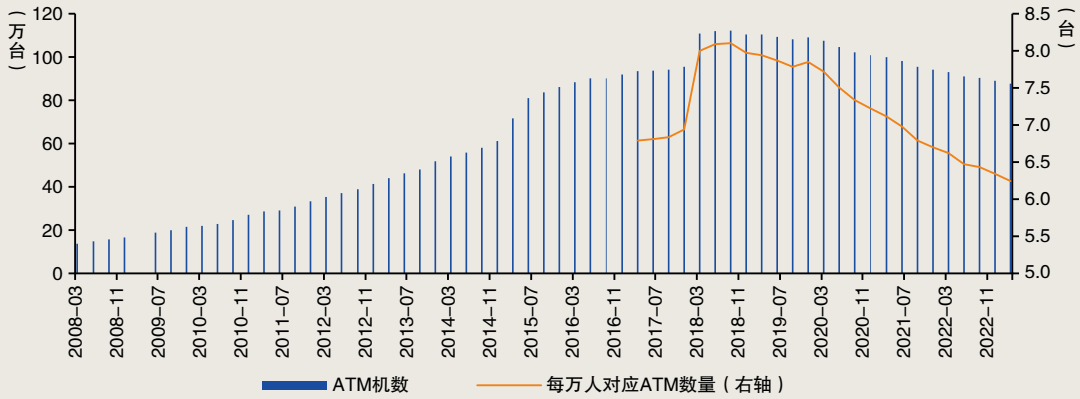
（二）金融小程序在合规后的安全性有保障

小程序的技术框架可以保证开发、运行及运维过程的安全性。当小程序上传到互联网开放平台发布时，开放平台会对小程序进行安全检测，存在安全漏洞时（如密钥硬编码等问题）必须修复后才能上架。同时，互联网确保每个小程序网络安全传输安全，不允许网络明文传输，必须对传输的业务数据进行脱敏或加密，以防用户访问小程序的过程中，被攻击者在网络层窃取数据。基于数据安全保护要求，互联网要求小程序商户不得展示敏感信息，所有数据均需脱敏。以上措施旨在防止小程序发生数据外泄风险。

在数据风险防护方面，目前互联网小程序的技术已经可以保证开发、运行及运维整个过程中均具

① 杭州互联网法院审判的微信小程序侵权案（案号：（2018）浙 0192 民初 7184 号），入选最高人民法院“2019 年 50 件典型知识产权案例”。

图2 我国ATM总数及人均对应数量



资料来源：中国人民银行

备安全性。一是小程序的代码仓储由开发者自行管理和维护。二是小程序前端页面由互联网平台提供相互隔离的容器环境来运行展示，与用户之间产生的数据信息可进行隔离加密存储，小程序间无法互相通信，互联网平台客户端也无法获取相关信息。三是由小程序所属的开发者，自行控制的后台服务器负责交互和处理，为前端页面提供内容展示，使用加密的网络传输协议进行信息传输，外界无法截取或篡改。四是小程序由开发者独立运营及维护，客户是否与开发者之间发生交易以及发生何种交易，是在互联网平台控制和了解范围之外的。

（三）金融小程序是金融机构自营场所的新形态

金融机构自营场所在科技助力下不断轻量化、小型化。在金融科技助力下，以银行为代表的金融机构自营场所一直在进行线上化迁移和动态变化，从传统的物理网点发展到 ATM 到 APP、应用程序编程接口（Application Programming Interface，API）[①]。例如，我国商业银行网点总数已经从 2016 年最高峰的 22.87 万家下降到 2022 年年末的 22.29 万家；ATM 总数量已经从 2018 年 9 月最高的 113 万台下降到 2023 年 3 月的 88 万台，每万人人均拥有量从 8.12 台下降到 6.25 台（见图 2）。与此同时，随着银行业 APP 的快速发展，手机银行月活跃用户规模则在 2023 年 3 月达到 5.33 亿人的规模。全球有 2000 万以上的开发者开发出百亿数量的 API。根据 Markets and Markets[②]的数据，全球 API 管理市场规模在 2023 年为 51 亿美元，比 2018 年增长近 5 倍。

金融小程序（小程序是平台借助 API 开发的）是金融机构在互联网平台上自营场所的新形态，成为金融科技对传统金融业解构和重构过程中产生的新事物。小程序在页面上不直接显示银行业金融机构，虽然并不影响金融机构功能的发挥，但作为新生事物，尚未被监管部门普遍接受和认可。相较而言，支付宝、微信等第三方支付[③]通过底层与银行业等金融机构搭建关系，在页面上也并不呈现出银行业金融机构，但经过长期发展和监管完善，这种支付形式已经为公众和监管部门接受。

四、启示和建议

金融业对信息和效率的依赖度较高，自产生以来就是信息技术最前沿的应用领域。金融小程序

① API 本身是抽象的，API 仅定义了一个接口，而不涉及应用程序在实际实现过程中的具体操作。API 是不同程序之间的传递者或中介，允许不同的应用程序之间交换数据和功能，可以使程序和程序之间通过访问一组例程，而无须访问源代码或理解内部工作机制的细节，在一定程度上解决了数据隔离问题。
② Markets and Markets 是全球领先的市场研究与咨询公司。
③ 支付方式也在经历密码支付、指纹支付、刷脸支付和刷掌支付等形式。

是信息技术在金融领域最新展现形态。接受、认可金融小程序的自营属性是顺应金融科技发展的基本要求。

（一）金融小程序是全新的去中心化应用模式

金融小程序是全新的去中心化应用模式，使金融机构与客户之间的连接更加便利。金融科技将传统的金融空间进一步映射到数字空间，金融的呈现形态和技术实现方式不断变化。在数字经济大发展的背景下，金融科技对传统金融不断解构，将原先的金融实体和要素不断智能化和算法化，与客户、合作伙伴的触达从物理网点转为网页、APP、API、小程序。具体的，以消费者在商场购物的支付行为为例，小程序相当于在商场柜台实现支付（柜台上面的桌布是银行的支付渠道），“跳端”相当于要求银行雇员自带设备（柜台以及相关设备）来为消费者提供支付渠道。

可将认可小程序作为常态化平台金融监管的具体举措。“跳端”将对互联网平台业务产生重大冲击。由于“跳端”需要对客户身份信息进行验证，这就使小程序的便捷优势不复存在，相当于将所有程序都赶回金融机构 APP，进而导致金融机构和平台既有的合作模式难以为继。倘若“跳端”，各大平台既有大部分相关业务将无法开展，50% 没有 APP 的中小银行难以继续开展当前诸多业务。

（二）可将“独立运营”和“完整数据权限”作为界定小程序是否自营的核心要素

金融机构小程序可被认定为其 APP 端口，而不是说非得跳出小程序的 H5 和 APP 才算银行的端口。在移动互联网和金融业务领域[①]，监管部门多对包括小程序在内的 API[②]、APP 或移动金融客户端应用软件基本做相同界定，并已经认定 H5 和 APP 可以作为银行业金融机构的域。

鉴于金融机构自营平台随着科技水平的发展一直在变化，建议监管部门以实质重于形式的原则判断风险、边界，并进行适应性调整。银行等金融机构的核心能力是风险判断和分析能力，具体经营业务的营业场所只是其展业和维护业务、客户的外在场所，而外在场所的形态变化并不会影响其核心竞争力。在金融小程序下，金融机构仍保有对小程序模型及规则的决定权，以及对更为核心的金融风险的分析能力、定价能力。监管在互联网时代的关键是管住相应的接口。在监管规则中，可将“独立运营”和“完整数据权限”作为界定小程序是否自营的核心要素。可通过行业规范条例等进一步明确金融机构和互联网平台合作的权责边界。

（三）宜采用行为监管模式监管金融小程序

基于市场逻辑的互联网金融发展并形成了场景金融等新的金融形式，进而对行为监管提出了迫切要求。金融小程序源于自下而上的金融发展需求。金融小程序是场景金融中的一种行为，建议监管部门对其强化行为监管：一是针对小程序建立相应的技术安全标准，以及配套的三方检测机制，对小程序的数据传输、数据加密、数据泄露进行多维度检测和监控。二是针对特定的金融业务，建议参照互联网保险业务监管的思路[③]，明确技术安全认定标准和落实方式。无论是 APP、小程序，还是小程序运营依托的平台均需获得三级等保认证[④]。

（责任编辑：李楠）

① 2020 年 7 月，中国人民银行发布的《移动金融客户端应用软件安全管理规范》同样适用和规范包括小程序在内的移动金融客户端应用软件。2021 年 3 月，网信办等四部委联合发布《常见类型移动互联网应用程序必要个人信息范围规定》，其中明确 App 的定义为：“App 包括移动智能终端预置、下载安装的应用软件，基于应用软件开放平台接口开发的、用户无需安装即可使用的小程序。”

② 2020 年 2 月，中国人民银行发布《商业银行应用程序接口安全管理规范》行业标准，从技术和管理两方面规范个人金融信息保护措施和金融 API 安全措施。

③《互联网保险业务监管办法》（中国银保监会令〔2020 年第 13 号〕），明确要求对于自营网络平台域名非自有或依托其他网络服务平台提供服务的，所依托的外部平台应至少获得三级等保认证。

④ 三级等保是国家对非银行机构网络信息安全的最高级别认证，由公安机关认可和评定。