北京金融科技产业联盟
BEIJING FINTECH INDUSTRY ALLIANCE

银行业开源生态发展报告

The Report of open source ecological development of banking institutions

北京金融科技产业联盟

2023 年 2 月

前 言

本报告由北京金融科技产业联盟开源专业委员会组织编写并拥有相关版权。凡转载、引用、摘录或以其他方式利用本报告观点、内容、图表的，都应注明“引用来源：北京金融科技产业联盟”。

编制委员会

主任：

潘润红

编委会成员：

聂丽琴　潘　妍　张海燕

编写组成员：

胡达川　李　寻　李　卫　许一骏　石砾磊　狄晓晓
陈　榕　李　振　李博文　冯晓文　郭　贞　李　鑫
李佩芳　袁　巍　孙　超　孙　曼　彭潇盟　谢　娜
张广斌　张永亮　刘子成　陈玟慧　赵叶红　周文泽
吴冕冠　赵　峰　梁大功　王媛媛　魏弋钧　边思康
陆碧波　付　辉　耿　航　杨　扬

参编单位：

北京金融科技产业联盟、国家工业信息安全发展研究中心、北京国家金融科技认证中心有限公司、中国建设银行股份有限公司、建信金融科技有限责任公司、中国银行股份有限公司、中国工商银行股份有限公司、中国农业银行股份有限公司、交通银行股份有限公司、兴业银行股份有限公司、上海浦东发展银行股份有限公司、浙江网商银行股份有限公司、苏州棱镜七彩信息科技有限公司、蚂蚁科技集团股份有限公司、腾讯云计算（北京）有限责任公司

感谢以上机构及人员对本报告编写的大力支持！

目 录

一、背景及意义

在全球数字经济的浪潮下，开源技术已成为新一代信息技术发展的基础和动力，尤其在推动信息技术应用创新和数字化转型方面效果显著，已成为银行业重构技术栈和重组供应链过程中最重要的力量和源泉，为金融科技发展创新注入了巨大活力。

2021 年 10 月，人民银行办公厅、中央网信办秘书局、工业和信息化部办公厅、银保监会办公厅、证监会办公厅联合发布《关于规范金融业开源技术应用与发展的意见》(以下简称《意见》)。《意见》明确“要规范金融机构合理应用开源技术，提高金融机构应用水平和自主可控能力，促进开源技术健康可持续发展”。

为落实《意见》相关要求，引导金融机构切实提升开源技术应用安全合规水平，推动金融业开源生态健康可持续发展，北京金融科技产业联盟（以下简称联盟）开源专委会组织开展课题研究，由国家工业信息安全发展研究中心牵头，联合专委会 9 家成员单位编制本报告，报告以银行业金融机构为主要研究对象，从生态现状、开源风险与痛点问题、未来发展趋势、建议对策四个维度对银行业开源生态发展情况进行详细解读，并给出银行业开源生态建设优秀实践案例供借鉴参考。

本报告将有助于深化理解行业开源生态建设情况，准确把握行业机构落实《意见》相关要求中存在的困难和问题，为后续形成相对可落地工作方案提供重要参考。

二、银行业开源生态现状

（一）政策环境

开源战略地位进一步凸显，已上升为国家中长期发展规划。《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》首次将开源列入国家五年规划，明确提出“支持数字技术开源社区等创新联合体发展，完善开源知识产权和法律体系，鼓励企业开放软件源代码、硬件设计和应用服务”；国务院印发的《“十四五”数字经济发展规划》提出“支持具有自主核心技术的开源社区、开源平台、开源项目发展，推动创新资源共建共享，促进创新模式开放化演进”“鼓励开源社区、开发者平台等新型协作平台发展，培育大中小企业和社会开发者开放协作的数字产业创新生态，带动创新型企业快速壮大”；工业和信息化部发布《“十四五”软件和信息技术服务业发展规划》，系统布局“十四五”开源生态发展，将“繁荣国内开源生态”作为主要任务之一，从开源基金会、开源文化、开源基础设施、开源项目、开源人才等多个方面提出了发展要求。随着系列国家政策的出台，开源已经成为重构软件产业生态的国家战略，社会各行各业紧跟规划，加快开源工作部署。

金融行业积极布局，陆续出台多项政策，为金融业稳妥推进开源生态建设与开源治理提供了基本遵循。《意见》为金融行业安全合规使用开源技术，以及开源生态的健康、可持续发展提出了指导意见，“鼓励金融机构积极参与开源生态建设，依法合规分享开源技术应用经验，共享开源技术研究成果。通过主动开源、贡献代码解决行业共性问题，提升开源技术整体应用水平。鼓励金融机构之间开展开源项目合作，实现优势互补、互利共赢、共同发展”。同年，中国人民银行发布了《金融科技发展规划（2022-2025年）》，提出金融行业发展的八项重点任务，其中在开源生态方面，提出“依法合规参与数字技术开源社区等创新联合体”。

行业相关政策的出台，将有效推动开源技术在金融行业的安全合规应用，促进行业开源生态的培育和发展，促进金融机构数字化转型，对金融业产品服务、经营模式、业务流程将产生深远影响。

（二）基础设施

基础设施是行业开源生态培育和开源治理的重要数字底座，是工作开展的重要抓手和主要阵地。从行业开源软件应用与发展的维度出发，代码托管平台和漏洞库是基础设施最核心的组成部分。

1. 代码托管平台

代码托管平台集聚各类开源资源，是开源代码的“存储池”、开源软件孵化推广的“温床”、程序员的精神“家园”，是开源生态的重要组成要素。近年来，我国集中涌现出一批开源代码托管平台，包括以 Gitee、GitCode 为代表的面向公众开放的支持公开库托管与协作的代码托管平台，以 CODING、云效、CodeHub、效率云为代表的带有代码托管功能的面向企业提供项目管理服务的平台或服务，以及金融行业内源性金融开源平台（OFTP），整体呈现差异化发展格局。

在支持公开库托管与协作的代码托管平台中，Gitee 由 OSCHINA 推出，用户数达到 800 万。GitCode 由专业开发者社区 CSDN 推出，拥有 CSDN 3500 万的开发者用户基础，具有海量的开源文档资源库，是国内开源开发者用户量、互动量极高的社区。GitLink 是中国计算机学会(CCF)官方指定的开源创新服务平台，已有 5 万开发者、千余家组织入驻，仓库数量累计 140 万；为我国创新型软件产业发展提供了关键技术支撑和实践指南，支持了我国航空、航天、国防等多个关键领域的可信软件生产。上述平台都支持社区内的开发者与国际开源社区联动，定期组织开源技术沙龙、主题会议、产业报告编制等，普及开源技术，弘扬开源文化。

在面向企业提供项目管理服务的平台或服务中，CODING、云效、CodeHub、效率云，依次分别由腾讯云、阿里云、华为云、百度云提供技术支持与服务，以项目管理为目标，提供代码协作开发服务。

在行业内源平台中，金融机构逐步凝聚开源发展共识，共建行业开源平台社区生态，加大培育、支持开源项目孵化与推广运用的力度。由联盟组织、中国银联承担建设金融开源平台（OFTP），赋能金融领域开源项目孵化，为用户提供高质量的软件源码管理服务。作为以服务金融机构为主的代码托管性质的服务平台，现阶段已接入金融机构 70 余家，160 余人，主要承接的开源项目包括金融业生僻字处理项目（RUCC）、金融业开源项目生态监测平台等。

2. 软件漏洞库

漏洞库因其掌握大量漏洞具体利用细节和过程，并能及时更新新曝光漏洞，而备受软件开发商、软件用户关注和青睐，可分为国家漏洞库和行业漏洞库。目前，国内的两类漏洞库尚未实现对开源软件漏洞的区分和分类，尚未实现对开源项目的全覆盖。

在国家层面，为有效及时的管控信息安全漏洞，切实履行漏洞分析和风险评估的职能，由中国信息安全评测中心承建运维的中国国家信息安全漏洞库（CNNVD）于 2009 年投入使用，向国家、行业和公众提供多种灵活的信息安全数据服务。为我国重要行业和关键基础设施安全保障工作提供了重要的技术支撑和数据支持，对提升全行业信息安全分析预警能力，提高我国网络和信息安全保障工作发挥了重要作用。截止 2021 年底，已积累漏洞数据近 4 万条，补丁与修复措施 7 万多条，网络受害与安全事件信息 1000 多万条。

在行业层面，联盟发起金融业开源技术信息服务平台 FOST 风险信息共享计划（以下简称 FOST 风险信息共享计划）。依托平台风险通报服务模块，通过聚焦开源漏洞及风险，为金融机构

共享已知的风险和漏洞信息，实现风险通报一站式服务。FOST 风险信息共享计划主要面向金融机构、安全厂商、科技公司、科研院校等机构，在开源技术风险、漏洞信息等方面开展合作，整合资源，建立风险漏洞和安全事件的发现和共享机制，提高金融业开源技术风险防范和处置能力。数据来源包括但不限于金融机构、安全公司等上报的风险信息；从动态感知平台公开、国家漏洞库网站等获取的风险信息。通报范围为金融业主要使用的开源技术、产品。

（三）现状概述

联盟于 2022 年针对十余家具有代表性的全国性股份制商业银行，开展关于落实《意见》情况的线下研讨交流。从反馈信息结合 2020 年末联盟开展的“金融机构开源软件应用情况调查”结果来看，各机构均已建立了内部开源技术应用管理协调机制与规章制度，大多数机构已将开源技术发展纳入到了自身的信息技术发展规划。并且，不少金融机构已经从单向的获取逐渐转变为主动、双向的对外贡献，中信银行、微众银行等不同规模、不同性质的银行已主动或计划对外开源项目，大多数金融机构能够积极参加开源社区以及相关的社会组织活动。

1. 生态合作

互联网银行方面，以微众银行、网商银行为代表的互联网银行主动拥抱开源技术，并且积极参与到开放原子开源基金会、开源中国 Gitee、开源社、GitHub、Linux 开源基金会、Apache 软件基金会、CCF 开源发展委员会等开源团体。与此同时，互联网银行积极也参与开源社区，并在业务系统中使用开源软件，不仅降低了业务开发成本，还丰富了开源社区的业务应用场景。此外，互联网银行也反哺社区，通过将内部孵化的产品进行开源，捐赠给开源社区，为开源社区提供了可以应用于金融场景的优秀开源产品。

在传统银行方面，从金融业参与较多的开源社区情况来看，传统商业银行对深化“数据”价值的需求集中，加入相关技术社区的积极性更高。例如，微众银行牵头的开源隐私计算 FATE 社区得到了中国银联、中国银行、建设银行、工商银行、农业银行、光大银行等机构的大力支持。金融机构与科技企业、科研院所、高等院校、科研院所等机构开展合作，将加强金融机构开源技术人才培养，促进开源技术迭代升级和成果转化。其中，工商银行、中国银行、招商银行、浦发银行、浙商银行等参与区块链跨链陆羽开源项目；工商银行等与科技企业合作开展 MySQL 数据库金融分支版本项目；光大银行与趣链科技合作开展区块链 BaaS 平台跨链子平台项目。

机构间围绕业务共性问题的解决、关键技术痛点的攻关，组成了金融业开源技术生态共建的雏形。在落实《意见》过程中，金融机构普遍增强了开源软件的应用治理意识及主动向开源生态贡献的积极性。

2. 对外开源

金融机构作为开源技术产品的主要使用方，在基础平台、业务系统、前端渠道中应用了大量的开源技术，通过近年的开源技术应用实践，逐渐从单一的开源技术应用开始开源贡献输出。2021 年 4 月，华为云、工商银行、浦发银行等机构联合发起的项目 Karmada 正式开源，为金融业机构建设跨云、跨数据中心的应用资源池提供详实有效的落地指导与帮助。浦发银行也陆续将其数据存储 Piraeus 项目和海量作业调度系统 Harrier 项目对外开源，支持各类异构计算平台海量计算作业的配置、管理和监控。中信银行在人民银行统筹推动和联盟的组织下，开源金融业生僻字处理项目（RUCC），并将代码托管至金融开源平台（OFTP），供我国金融行业范围内白名单机构使用。除此之外，微众银行也对开源持积极态度，2019 年初，微众银行对外开源自研项目 FATE（Federated AI Technology Enabler），为行业内提供工业级

联邦学习框架；此外，微众银行逐步开源 WeDataSphere 大数据平台套件，包括计算中间件 Linkis 等核心组件，形成了领先的大数据开源生态。

虽然与 2020 年相比，已对外开源并计划对外开源的金融机构总数倍增，金融科技拥抱开源的积极性显著提升，但目前金融机构整体上对外开源还大多处于观望状态，尚需一定的时间学习沉淀。

（四）开源治理体系建设

1. 对内治理

随着开源软件在我国银行业的广泛应用，金融机构逐渐强化开源治理工作，内部开展的工作主要包括制度建设、运维保障、文化建设三方面。

在制度建设方面，多家大型商业银行已制定企业级开源治理流程与管理文件，具备明确的开源软件治理人员责任划分。中国建设银行发布了开源软件产品管理规程及实施细则，以保障开源软件产品在信息系统中的安全可控与稳定运行；中国农业银行结合商业银行特点和自身实际情况设计了一套融合传统和开源理念的软件管理体系和框架 TOSIM（Traditional & Open-source Software Integrated Management），规范企业内部的开源管理；与此同时，交通银行也根据自身企业技术架构发展，制定了开源软件管理办法、开源依赖库管理细则等，形成了自身开源软件管理模型。

在运维保障方面，浦发银行成立了开源治理的配套组织架构，明确开源治理职责分工，同时建设开源治理平台，实现开源软件全流程、一体化、自动化管理；中国银行加强专家培育和队伍建设，打造了包括开源技术架构师、开源安全专家、开源软件开发专家在内的三支专家队伍，明确各方职责，确保高效协同；中信银行成立了专业的开源治理团队，启动开源治理平台建设，实现

开源资产管理线上化。

在文化建设方面，中国工商银行、中国建设银行、中国农业银行、浦发银行等多家头部银行机构均加入了联盟开源专业委员会、金融行业开源技术应用社区（FINOC），学习先进开源治理经验，并将开源技术治理推广至每个流程中，引导企业内部科学化、规范化、制度化的使用开源技术。

2. 标准建设

金融机构基于开源技术应用取得了科技创新、业务赋能等积极成效，在内部开源管理过程中，还总结经验主动对外开展标准、制度建设，护航金融业参与开源生态行稳致远。

在行业标准方面，多家头部商业银行、互联网银行结合自身管理经验、互联网和金融的双重属性，为金融机构应用开源软件建言献策，在联盟组织下与产业机构共同编制了金融行业标准《金融业开源软件应用管理指南》《金融信息系统开源软件应用评估规范》《金融业开源技术 术语》等标准，为进一步规范金融机构开源软件的资产管理提供了宝贵的经验。

在团体标准方面，2021 年，中国互联网金融协会正式发布《金融行业开源软件评测规范》《金融行业开源软件服务商评测规范》，为银行机构评估和选择合适的开源软件及服务商提供参考依据，保障银行业开源软件的应用安全，促使开源软件服务商提升企业竞争力。2022 年，联盟正式发布《金融技术产品开源项目管理指南》，该标准由中国工商银行软件开发中心主笔编制，填补了金融技术产品对外开源标准的空白，切实保障金融技术产品开源管理流程的规范性和可行性，促进金融机构合法合规、拥抱开源。

三、银行业开源风险与痛点分析

金融机构早期普遍在对外开源方面缺乏顶层战略规划及外部开源社区同步发展互促的机制；随着越来越多的开源技术引入，金融机构在开源技术治理与发展上面临着以下问题与挑战。

（一）痛点问题

1. 概念认知不足

随着近年来信息化快速发展，开源这一概念已经不再局限为开源软件，《意见》首次提出的“开源技术”是指“金融机构从代码托管平台、技术社区、开源机构官方网站等渠道获取的，或通过合作研发、商业采购等方式引入的开源代码、开源组件，开源软件和基于开源技术的云服务等”。联盟在开源软件的应用数量的交流中发现，同量级商业银行之间反馈的开源软件及组件的应用量级差异约三百余倍，说明不少机构仅仅将主动引入开源社区公开或发布的版本视为开源软件，有配套付费服务、或基于开源软件开发的商业版、间接采购引入和依赖包引入的开源软件/代码均未被视为开源软件。由于机构之间对于开源软件的界定、统计方式和治理范围存在巨大差异，也就导致了遗漏在“开源技术”范围之外的开源软件可能处于管理盲区，如果发生安全合规风险，会导致更高的处理难度及成本。

2. 内涵理解不深

在联盟 2020 年《金融机构开源软件应用情况调查报告》中发现，不少机构在顶层科技战略的设计上尚未认识到参与开源生态对助力自身的开发效率、技术实力、模式创新的积极作用，也就造成了内部管理不配套、开源文化缺失、人员及精力不足的状况。在《意见》发布前，鲜见以机构为责任主体承担社区成员角色，对开源社区的贡献往往属于开发者的个人行为，并非持续性的机构行为；代码质量的提升、安全漏洞的修复往往要依靠上游社区新陈代谢。仅少数机构认为自身要提高回报社区的能力，绝大部分机构依然侧重于关注软件的技术研发维护能力，缺乏主动参与开源工作和贡献开源生态的意识和动力，导致金融机构面对开源软件缺陷与问题时大多处于被动的局面，未能形成良好的产用双方技术共建能力。

近两年来，随着《意见》发布和开源文化在金融业的推广，不少商业银行也逐渐加入了开源操作系统、隐私计算框架等大型开源社区，但除了少数头部商业银行科技实力雄厚，能够投入较大开发资源，更多的金融机构主要以需求意见提出者的角色进行贡献，因此金融机构整体上在开源产业生态链中贡献度较低。

3. 主动开源不畅

由于商业银行普遍未建立自上而下的对外开源战略，对外开源意愿多来自于开源产业或同业相关动作的启发，内部又缺乏针对性的激励及多部门密切配合的对外开源工作机制，导致参与社区或对外开源大多由科技团队“单打独斗”、自下而上推动。而开源能否形成收益或商誉提升，可能是商业银行评价项目成功与否的首要标准，由科技团队主导完成一套效果量化、投入产出比分析、内部立项、采购等“非技术性”工作的难度较大。同时，商业银行对外开源的态度更加审慎，对代码质量、运营规则等准备阶段工作质量要求更高，给科技团队提出了更高的开源门槛。因此，与科技公司对外开源的效率相比，传统商业银行科技团队面的挑战更多，对外开源的内部流程更复杂、孵化时间更长。

4. 法规宣导不足

主动对外开源方面，与 2020 年相比，金融机构对外开源意愿与能力得到增强，但存在忽视许可证兼容性、强互惠型许可证理解偏颇的情况。在联盟组织编写金融行业开源技术系列标准工作过程中也发现，起草人以技术序列专家为主，机构间对法律合规有关的术语释义、许可证审查事项等条款更难达成一致共识。根据交流调研，将法律合规风险纳入开源软件引入评估障碍的商业银行数量倍增，但其中仅 1 家机构安排了开源合规主题研讨活动，其他开源主题培训基本为技术能力、应用能力、管理能力提升类培训及活动。

从制度执行方式与频率来看，与技术安全审查相比，金融机构在法律合规审查规范、完善程度与执行力度上相对较弱；且该

部分机构也均表示过自身亟待补足法律合规风险应对能力，反应出了金融机构目前对开源软件存在的法律合规风险认知得到大幅提升，但对于提升法律合规风险应对能力的需求还未得到有效满足。

5. 安全风险挑战

对银行业而言，数据安全、隐私保护、系统稳定是重中之重；使用开源软件虽然在一定程度上会给企业带来成本上的节约，但是伴随而来的是安全屏障更加脆弱、数据隐私泄露风险不断加剧。在目前引入开源软件的企业中，大多数都遭受过开源代码投毒或者恶意攻击事件，而开源软件往往不会经历太多实际的业务性测试，遇到问题时可能无法得到及时的修复，解决风险需花费大量的时间。对于银行业来说，特别是对于很多中小银行来说，内部开源技术治理还不够成熟，缺乏配套的专业人员和工具，即便遇到恶意攻击事件的概率很低，如果发生也将为银行带来不可逆的损失。

（二）风险及应对

1. 安全风险

除开源软件已曝光的安全漏洞以外，开源软件的安全风险还可能来自于因为代码缺陷而引起的尚未曝光的安全漏洞以及木马、后门等恶意攻击，甚至可能因为研发人员安全意识薄弱，在向开源社区回馈代码或者对外开源过程中，导致数据或隐私泄露。

为应对开源软件安全风险，行业机构应建立组织完善、职责清晰、流程明确、标准合理、管理有效的开源软件安全管理体系，实现对风险的知悉、预防和修复。开源软件安全管理措施包括以下 6 项：

一是安全准入。在引入开源软件时做好安全测评、漏洞检查等工作，确保引入开源软件满足一定安全标准；建立本地软件存储库；**二是安全使用**。开发人员需按照统一要求，安全合规使用

已入库的开源软件，严禁私自使用未引入开源软件；**三是安全退出**。对于因安全原因不宜再使用的开源软件，需在关联性分析基础上，制定妥善的退出方案，并列入不推荐使用清单；**四是漏洞监测**。采取多种技术手段，持续监测、监视已入库开源软件的漏洞情况，及时准确的通报所发现漏洞；**五是漏洞处置**。开源软件使用方需安全漏洞处置要求，及时进行漏洞处置，不能及时处置的需采取妥善的风险缓释措施；**六是漏洞复测**。开源软件安全管理部门需对漏洞修复情况进行复测，确保漏洞修复工作的有效性、时效性。

除此之外，参考即将发布的国家级、行业级相关标准，做好内部制度保障；在流程与工具保障方面，可引入第三方管理工具，确保引入及对外的开源组件和代码安全合规以及与 DevOps 深度集成，建立 DevSecOps 体系。

2. 法律风险

全球范围内，开源许可协议已达上百种，其中存在大量未通过 OSI 或 FSF 组织认证的非标准许可证。不同开源许可协议之间可能存在不兼容[1]情况，近年来许可证的变更[2]也为判断评估兼容性、适用性增加了难度。违反许可证的条款造成违约行为，可能面临知识产权侵权等风险，例如被权利所有人提起专利诉讼并收取费用。若开源软件未应用许可证或使用了非认证的许可证，其开发者也面临知识产权失权的风险。

为应对许可证合规风险，需要增强风险防范意识，关注建立

[1] 不兼容：不同开源许可证的许可证条款会存在对同一描述对象的描述不一致的情况，若描述双方对描述对象的描述互相矛盾且均为强约束，则此两种许可证不兼容，产生条款效力上的歧义。如 AGPL-3.0 与 GPL-2.0，无论在何种条件下，均不可同时存在于同一项目中。

间接兼容：若描述双方对描述对象的描述不一致但在部分条件下实际上一致，则此两种许可证间接兼容。如 GPL-3.0 与 AGPL-3.0 则是间接兼容，使用者不能根据 GPL-3.0 的条款对 AGPL-3.0 下的代码进行传递或修改，但可以将在这两个许可证下发布的单独模块或源文件组合到一个项目中。

直接兼容：若描述双方对描述对象的描述相一致，或描述互相矛盾但至少一方为弱约束或无约束，则此两种许可证直接兼容，如 MIT 与 GPL。

[2] 部分权利所有人可能会变更其开源软件的许可证，下游使用者如果不及时察觉和做出风险评估，可能会面临合规风险。如 2021 年，Elastic 公司将旗下的知名开源项目 Elasticsearch 和 Kibana 的开源许可证由 Apache2.0 变更为 SSPL 和 Elastic License 的双许可。

风险防控全流程管理，加强风险防范工作协同。首先在引入时落实风险检查与评估工作，从源头减少相关知识产权风险。在开发过程中，合规左移，将开源合规风险检查能力建设到企业开发流程中，贯穿软件开发整个生命周期，统一管理、持续跟踪；软件发布前，可以通过合规性分析工具等进行产品发布前验证审核，同时相关人员做好产品合规审核。审核具体内容包括：具体的软件成分一致性、软件版本一致性、开源许可合规风险等。

同时，完善知识产权体系建设，正确面对开源知识产权风险，增强开源许可证相关研究。精准解读开源许可证条款规则，做好风险评估保障。跟踪开源知识产权相关司法案例，法务人员需要对已经发生的开源纠纷案例进行跟踪分析，通过对案件争议焦点、判决结果的分析，一方面了解法官对开源软件知识产权问题的判决依据，为以后开源法律纠纷应对打好基础，另一方面掌握开源软件的诉讼动向，便于企业提前做好诉讼防控准备。

3. 供应链风险

开源的广泛应用，使得软件供应链的开源化趋势越来越明显，软件供应链也越发复杂化和多样化。由于软件供应链的特殊性，使得其攻击具有门槛低、隐蔽性强、影响范围广等特点，随之而来的供应链风险也层出不穷，主要包括断供风险及攻击风险。

1）供应链断供已出现过“经典案例”[3]，不得不让用户开始重视断供风险，出口管制[4]和司法管辖权[5]也放大了断供风险的可

[3] 在 2019 年美国政府将华为公司列入出口管制“实体清单”后，谷歌即宣布停止向华为提供基于 Android 系统的更新服务及应用。

[4] 从现有开源基金会和托管平台的情况来看，开源基金会的管理办法差异较大，例如，Linux 基金会自身的管理办法不受美国出口管制，但其旗下的虚拟化项目 Xen 明确要求其使用并出口者遵循美国出口管制;Apache 基金会的管理办法明确说明遵循美国出口管制，旗下绝大多数项目如 Hadoop、Spark 等，在备案(5D002)后即不受出口管制。而 GitHub、SourceForge 和 Google Code 3 个代码托管平台均明确声明遵守美国出口管制条例，并且司法管辖权均在加州。这意味着如果一个开源项目或开源组织声明遵从美国的出口管制条例，此时一旦美国修改条例，将一些核心基础软件加入到管制中，那么我国大量核心开源项目将受到出口管制。2019 年 7 月，GitHub 托管平台就曾因美国贸易管制政策，限制了克里米亚开发者的账户，导致其托管的开源代码无法访问。因此，一旦美国针对中国公司的贸易管制政策蔓延到开源项目，中国公司托管在海外的开源代码资产将面临冻结风险。尤其是当一个开源项目或开源组织指定了司法管辖权归属于美国某法院，则所有围绕使用条款展开的纠纷，都将以该美国法院的判决为准，他国企业胜诉的几率将十分渺茫。

[5] 按照美国出口管制条例的规定(734.7b 和 742.15b)，所有“公开可获得”的源代码(不含加密软件以

能。对此，银行业一方面需要加强自身开源技术掌控力，积极发展和应用不易受管制的开源项目。另一方面，制定完善的风险评估体系和管理计划，打造供应链韧性，加强对多级供应商的风险管理，提高供应链风险预警。

2）攻击风险已经成为一种新型威胁。近年来，互联网关键技术产品在开发、交付、使用等不同环节遭受了多起实际攻击，利用企业外部合作伙伴的安全疏忽与缺陷造成的关键基础设施破坏、敏感数据泄露、信息系统入侵等网络安全事件层出不穷。对此，许多机构曾提出多个解决方案，如谷歌的 SLSA，CNCF in-toto 框架、Microsoft SCITT 框架等。可借鉴此类安全框架，结合机构内部自身状况，制定适合机构的供应链攻击风险解决架构体系。

综上，开源软件供应链安全首先要树立正确的安全意识，将供应安全标准规范，供应链安全规章制度与供应链安全管理体系相融合，制定软件供应链安全治理顶层设计，管理范围覆盖开发、交付到使用全生命周期及资产链条的上游研发至下游用户侧全方位覆盖，打造可信任、可评估、组成成分透明的可信实体。将安全检测结合安全可信白名单机制、风险预警、与情报收集机制保证内部环境安全。通过建立软件成分清单（如 SBOM），源代码管理、漏洞库管理等安全风险管控机制，保证软件供应链数据的安全可信。同时，配合安全检测技术、如代码审计、软件成分分析、动态安全检测等技术支持可评估能力建设。加快建立软件成分清单生成与使用规范，建立管理手段与工具方法库，标准化软件成分和软件成分可视化流程，保证组件透明理念的落实。

及带加密功能的其他开源软件)，都是不被出口管制的，而“公开可获得”的带加密功能的源代码，虽不会被限制出口，但需登记备案(5D002)。司法管辖权是指法院或司法机构对诉讼进行裁决和判决的权力。使用网站或注册会员时，如果其使用条款或会员条款中指定了司法管辖权的归属，则代表合同双方同意只承认指定的司法机关做出的判决为赔偿的依据。

四、银行业开源发展趋势

（一）行业产业侧合作更加紧密

银行业在加速推进信息技术应用创新和数字化转型过程中，开源技术凭借其降本增效等突出优点被广泛应用，行业侧开源软件专业服务需求随之被激发，并且越来越旺盛，行业侧与产业侧的合作将更加紧密。**一是开源商业公司，**开源商业公司一般依托某个或多个开源软件，研发商业软硬件产品作为核心业务，此类公司可在开源软件基础上提供定制化产品，满足行业用户特殊的业务需求，简化业务升级路径，节省研发力量，提供商业化服务支持。**二是开源技术服务公司，**此类技术服务或解决方案是指针对某款或某类开源软件（如开源数据库）提供安装部署、迁移、开发、性能调优、故障排查与修复、软件升级、巡检等支持的服务和解决方案，以及其他源码服务等，可缓解行业用户开源软件运维人员数量不足等问题。**三是开源软件安全服务公司，**银行机构引入开源组件的同时也会面临安全、许可证合规等的问题，开源安全厂商填补了行业机构在安全治理层面的技术空白，其开源安全检测工具和解决方案可帮助行业机构建立完善开源治理手段，从开发流程的多个环节入手，有效防范、控制开源组件可能引发的多种风险，筑牢安全防线。**四是开源治理咨询公司，**随着行业开源生态的不断发展，公司内部开源治理工作将从粗放式管理走向精细化治理，如何将开源战略纳入自身信息化发展规划中，如何从组织架构、制度流程、标准规范、工具平台等多方面构建完善公司内部开源治理体系，将成为行业机构开展公司内部开源治理工作的重要课题，开源治理咨询公司可为此提供专业评估、考核服务和专业咨询服务，帮助行业机构建立完善开源治理体系。

（二）生态共建将加快步伐

在《意见》“鼓励金融机构积极参与开源生态建设，依法合

规分享开源技术应用经验，共享开源技术研究成果”的方向上，联盟组织建设了金融业开源技术信息服务平台（FOST），拟提供金融业开源政策与标准、开源技术风险信息通报、开源技术应用、开源项目孵化、开源知识库以及前沿技术跟踪。同时，为落实《意见》提出的金融机构识别开源技术风险等的要求，金融科技产业联盟筹建开展 FOST 风险信息共享计划，建立风险漏洞和安全事件的发现和共享机制，得到了多家机构响应。在金融同业合作方面，由联盟孵化的金融业生僻字处理开源社区汇聚了 60 家金融机构参与，是金融业开源共建的试水项目；还新建了开源软件活跃度监测等孵化项目，形成了主要由金融机构应用需求为主导的开源生态雏形。

（三）更多金融机构进入开源“教程期”

对外开源方面，传统商业银行虽然普遍对开源软件应用治理建立了管理协调机制，但极少有机构建立对外开源管理策略及内部规范流程，主要是因为顶层科技发展战略中往往忽视了掌握对外开源能力的重要性。以“科技创新促进业务发展”为定位的金融机构已意识到，掌握从应用、参与、贡献、内源再到开源这一整套实践发展模式，是保持自身科技实力与创新能力源源不竭的主要路径。但大部分传统商业银行还未充分理解开源的意义，缺乏企业级开源文化推广，不清楚需要遵循的工作原则、机制和流程。因此，为填补此空缺，减低学习成本，联盟组织多家成员单位，根据金融机构技术产品开源流程的特殊性，结合产业机构的开源实践，共同研究制定团体标准《金融技术产品开源项目管理指南》。该标准提出一套以机构为责任主体的开源工作机制、保护知识产权与信息安全为重点的工作方法，为存在对外开源计划的金融机构提供一套较灵活、可借鉴的方法指导，加快金融机构迈向开源的步伐。

（四）技术领域以“数据”为中心辐射

根据金融机构反馈，商业银行开源技术攻关领域广泛，其中大数据、云计算、人工智能（AI）、区块链、数据库等领域占据了“半壁江山”。数据作为重要的基础性资源，对于金融机构的长期发展来说将成为衡量企业价值的重要标尺，也将极大程度上影响未来竞争格局中的地位。随着 2021 年《数据安全法》、《网络数据安全管理条例》、《个人信息保护法》的相继出台，我国数据安全迈入重要发展阶段，如何保障数据安全的同时释放数据要素价值，成为金融业必须面对的挑战，因此金融业未来或将加速打破数据流通的壁垒，实现金融数据融合运用，以挖掘数据更大价值为主要目标深耕相关领域开源技术。

五、银行业开源生态发展建议对策

（一）强化专业人才培养

由于银行机构的科技团队存在不少技术外包，法务团队又侧重于合同法、消费者权益保护等领域，容易出现开源软件“拿来就用”，以及对 GPL 等“强互惠型”许可证“一刀切”的情况，从长期角度来看，可能导致技术创新意识降低、开源软件维护成本增高。为了避免此类问题，企业应该注重培养专业技术人才或引入开源技术、知识产权领域专家；建立分工明确且高度配合的跨领域协同机制，让法务团队参与到企业开源生态建设全流程中，也让技术人才参与对许可证条款解读、常见许可证风险分析等风控管理环节中，通过开源治理的理论与实践，加强人才队伍梯队建设。

（二）推进公共服务体系

一是联合行业侧和产业侧，建立开源漏洞风险通报机制和共享机制，密切跟踪行业安全信息数据，对新曝光开源软件漏洞进行预警，降低安全风险；**二是**完善基础设施建设，搭建开源代码托管平台和信息门户网站，为行业开源项目孵化、社区构建和应用推广提供平台和渠道，壮大行业开源代码储备资源池，实现资

源共享。

（三）探索行业开源项目社区构建

一是鼓励行业机构开源和共建开源项目，用开源赋能信息技术应用创新；**二是**以开源的协作方式培育重点项目，充分调动行业机构力量，面向重点攻关方向，孵化一批基础性、前瞻性开源项目；**三是**借鉴国际开源项目成功经验，发挥优势开源项目引领作用，建立完善生态链各方积极参与的开源社区。

（四）强化标准执行与符合性验证

一是加强针对开源供应商的能力评价体系建设，建立科学统一的开源供应商评价指标，有效衡量开源供应商发展水平，促进开源服务商持续优化改进，降低金融机构与开源服务商的合作风险，护航安全的开源供应链生态。**二是推进金融开源软件应用评估，**全面评价开源软件的法律合规性、产品可用性、技术安全性等内容，为金融业开源软件的选型使用提供数据支撑，保证开源软件在金融系统应用时的适应性、安全性及可靠性。**三是建立开源治理成熟度评估模型，**帮助金融机构落实《意见》相关要求、完善开源治理体系，发现金融机构在开源技术应用管理制度体系、开源产品评估体系及开源知识产权等相关领域中可能存在的问题，形成适合机构发展情况的长效治理机制。

（五）完善内部组织机制建设

一是完善“顶层设计”。行业机构应根据公司自身特点制定开源治理相关方针战略，赢得公司决策层的战略支持。**二是建立“执行机构”。**执行机构负责制定公司内部开源治理相关制度流程、提升公司应用开源和对外开源能力、普及开源知识、培养开源人才、打造公司开源文化等，承担对内管控，对外交流等任务。

附录

银行业开源生态建设优秀实践案例

一、中国农业银行数据湖建设

（一）案例背景

十三五期间，农业银行全面推进数字化转型，业务数据量不断增长，各部门用数需求愈发旺盛。数据种类方面，用户行为日志、客服语音、凭证图像、监控视频等半结构化和非结构化数据，能够为客户营销、风险控制等业务场景提供更多的数据参考，提升数据分析结果的精准度。数据时效方面，各部门对数据加工、数据开发、数据流转、数据治理的响应时间提出了更高的要求。资源成本方面，随着数据量的持续增长，如何提高大数据存储和计算资源利用率，节省资源成本，成为必须面对的现实问题。

金融行业的大数据平台通常按照数据仓库的理念建设，以结构化数据批量处理为主。在新的发展阶段下，大数据平台迫切需要提升以下四方面的能力：一是扩充数据处理范围，支持半结构和非结构化数据的自动化采集、存储、加工、服务；二是提升数据处理时效，加强实时数据采集、存储、计算、服务能力；三是提升数据开发和管理效率，数据需求到达后能够快速完成分析、映射、开发；四是提升大数据资源利用率和交付速度。

数据湖作为大数据新型解决方案，通常具备多源异构数据的采集能力、强大的数据存储和计算能力、完善的数据管理和服务能力，可以满足新形势下灵活多样的数据需求。

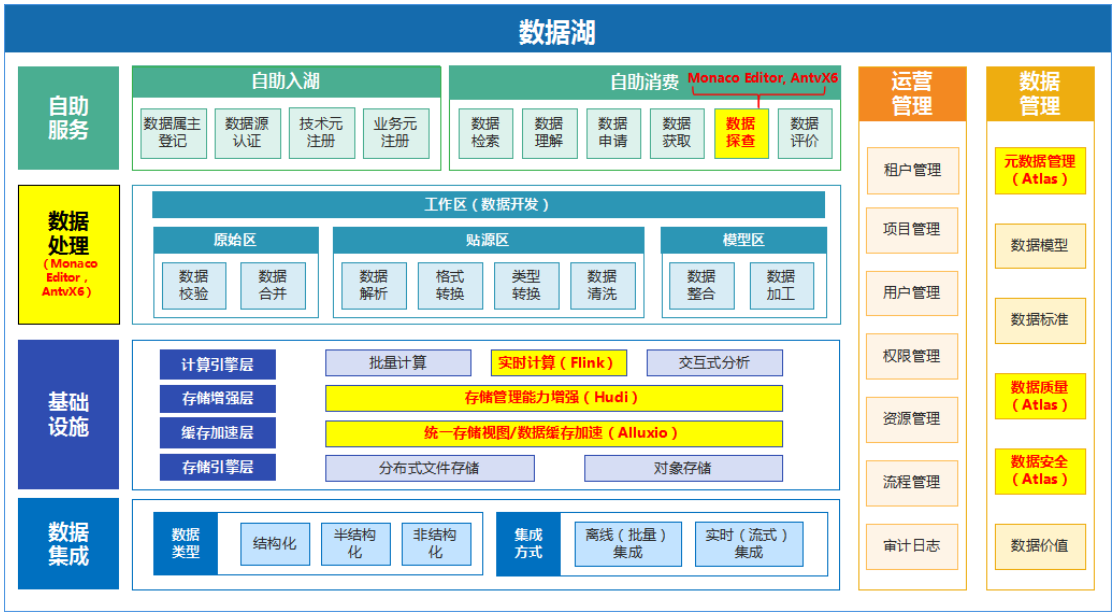
（二）创新成效

1. 技术方案

农业银行数据湖创新融合存算分离、流批一体、湖仓一体多元技术架构，引入六项开源技术，孵化出一套数据湖开源技术栈，构建了存储云+计算云+工具云的大数据新型技术架构。

湖存储层引入数据湖软件 Hudi，实现流批一体存储、事务管理、快速更新等能力；湖加速层引入数据编排软件 Alluxio，一是支持多芯异构存储统一管理，二是利用软件加速技术实现计算加速；湖计算层引入流批一体引擎 Flink 并实现容器化部署，同时支撑实时处理和批量处理场景；湖管理层引入元数据管理软件 Atlas，实现元数据准实时采集和数据血缘智能解析；湖消费层引入 Monaco Editor 代码编辑器和 AntvX6 图编辑引擎，提供大数据可视化低代码开发体验。

2. 说明图示



3. 技术创新

一是实现流批一体存储计算，基于一套环境、一套程序、一份数据，数据处理时效由 T+1 提升至分钟级，并有效降低开发运维成本；二是实现大数据存算分离及上云，支持存储计算资源独立扩缩容，计算资源交付速度由周压降至秒级；三是实现多芯异构存储统一管理，存储规模扩充至 EB 级；四是通过低代码开发和多租户管理实现大数据应用快速构建。

4. 业务创新

一是集中汇聚结构化与非结构化各类数据，可构建以“客户为中心”的全景视图；二是新增实时入湖及 ETL 处理链路，支撑热点交易监测、智能运维等实时分析场景；三是实现元数据智能解析，大幅提升数据管理人力效能，有效加强数据质量和数据安

全管理水平；四是实现数据冷热分区，冷数据存储成本下降约50%。

5. 产业价值

农业银行数据湖建设创新应用多项开源技术，基于鲲鹏ARM 处理器、银河麒麟操作系统等新的基础技术栈进行投产部署，一是落地存算分离技术架构，二是实现湖仓一体技术能力，三是完成流批一体采集、存储、计算、服务能力建设，四是实现计算引擎上云，五是支持大数据多芯异构部署模式，六是构建数据资产、质量、安全智能化管理能力，七是实现大数据可视化低代码开发体验，验证了大数据新型技术栈在金融场景的可行性，有效提升大数据处理能力、大数据精细化管理水平和企业数据治理水平，为其他金融同业机构提供了可借鉴、可推广的示范案例。

二、兴业银行云原生基础平台

（一）案例背景

为进一步打造适应数字化转型的金融科技基础设施建设，兴业银行于 2020 年完成了以容器云为代表的云原生基础平台建设，解决了数字化转型中应用架构快速向分布式、云化转型缺乏统一基础支撑平台的痛点，通过容器云平台带来的标准及快速交付、海量并发、弹性伸缩、局部故障自愈等技术优势，大幅提升应用架构弹性及韧性，有效应对互联网、生态圈应用对海量并发、敏捷迭代、超高性能的要求，已成为全行技术架构升级转型的强力技术底座。

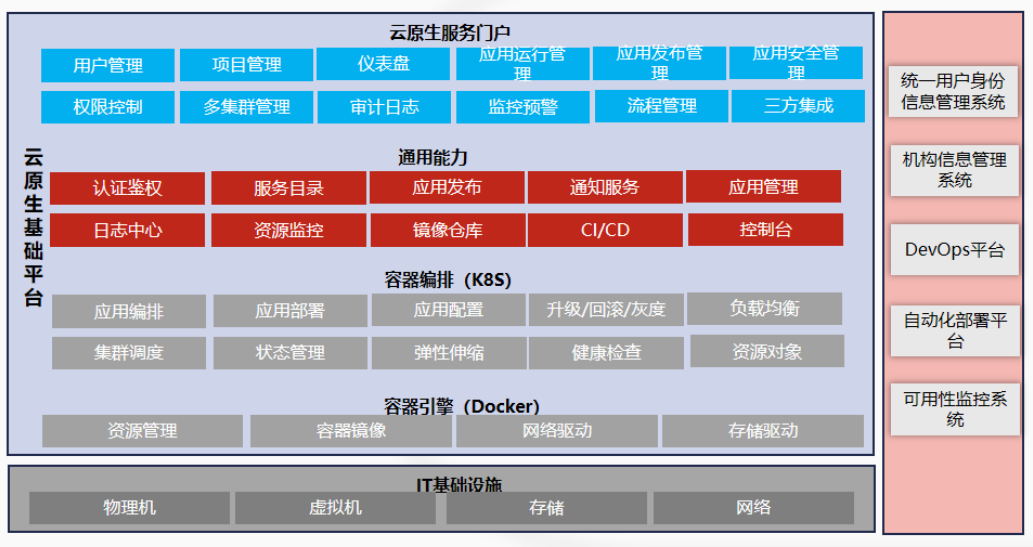
（二）创新成效

1. 技术方案

兴业银行容器云平台包含容器引擎、容器编排、镜像仓库、多集群管理、服务门户等功能。综合考虑到新技术引入及推广历程，在建设初期采用 OpenShift 产品作为容器引擎，自主研发设计统一管理门户，随着应用上云的推进以及技术架构升级的加速，围绕关键基础设施自主可控，逐步完成基于 Kubernetes 开源体系的容器云引擎构建，并完成信创技术体系适配，建成全栈信创容器云平台并已开始推广应用。

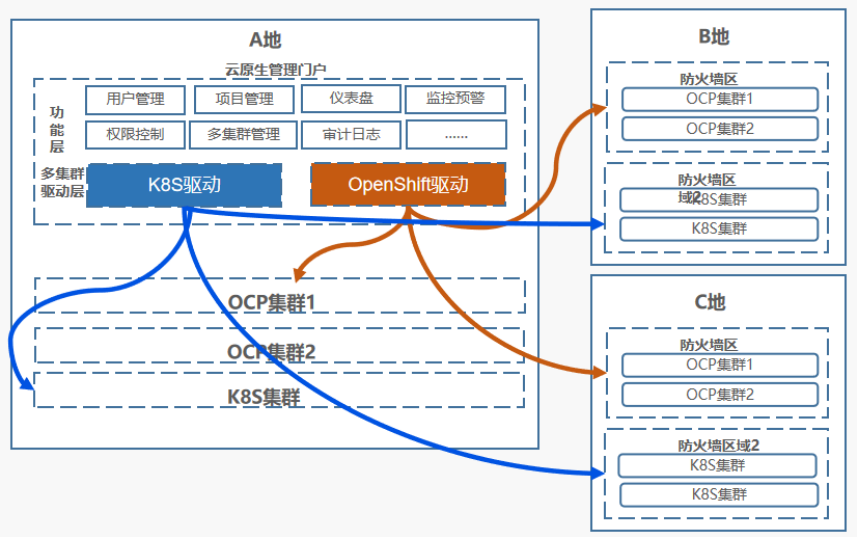
2. 说明图示

兴业银行容器云平台功能设计上包括容器引擎、容器编排、镜像仓库、多集群管理、服务门户等功能，如下图所示。



3. 技术创新

（1）兴业银行云原生基础平台在 Kubernetes 社区标准上实现了多项技术创新，一是自主研发了异构集群管理能力，实现基于 Kubernetes、OpenShift 多类异构容器云引擎管理、屏蔽底层技术差异、对外提供一致用户体验，全面提升对规模化集群的管理能力。



（2）在平台建设中，还基于 VPA 标准自主研发了动态资源控制套件 SmartVPA，通过持续统计应用实际资源使用率，为应用预测出合适的资源值，并动态进行调整和分配，无需人工干预，“用的多，分的多；用的少，分的少”，有效提升服务器资源利用率。该组件基于 Kubernetes VPA 标准自主研发，同时支持

Kubernetes 及 OpenShift 两大引擎，同时基于半衰理论、信心指数设计资源调配算法，精准计算应用资源。在其支撑下可大幅提升基础硬件资源利用率，提升现有资源分配效率，实现精准分配投放，同时也奠定在/离线混部技术基础。

（3）在平台建设中，紧跟国家自主创新战略，通过对信创技术体系的适配打造信创技术底座，通过对芯片、操作系统等的全面适配，建成信创基础技术平台，为应用提供全栈信创资源。同时借助容器云技术优先，支撑信息系统透明化、规模化快速向科创技术体系迁移，已支撑多个领域信息系统基于信创技术体系建设。

4. 业务创新

兴业银行云原生基础平台已作为推动全行技术架构升级转型的重要抓手，在其支撑下，近百个业务系统规模化开展云上迁移，各类环境容器应用规模已突破万级，2021 年新建项目均实现了“应上尽上”，基于其建设的信用卡微信公众号、天网工程、开放银行等重大项目，也均体现出对业务创新发展的助力，在业务响应效率、客户满意度提升等方面成效显著。具有千万级客户的互联网应用好兴动 APP、日均交易金额亿级的全网收单等核心应用，正基于云原生基础平台建设或重构，新技术新工艺赋能业务创新发展逐见成效。

5. 产业价值

目前，兴业银行云原生基础平台已实现规模化推广，技术架构正加速升级，在有力支撑全行经营管理的数字化转型中，也积累一套丰富的云原生架构转型推进经验及保障体系，特别是通过对信创技术体系的适配，在建成了具备自主知识产权的基础平台的同时，也形成了商业银行在信创技术应用推进中的最佳实践，在其建成之后，已有各领域 10 余个应用基于信创技术体系建设，进一步提升了商业银行在关键技术设施的自主掌控能力，随着其的进一步推广应用，其意义和价值将得到更广泛的认可，同时因其在金融行业具有较强的普适性，或可供其他商业银行借鉴或直接使用，具有重要的社会价值。

三、中国工商银行基于 PaddlePaddle 飞桨的金融遥感影像智能分析能力建设方案

（一）案例背景

卫星产业是我国战略新型产业，国家“十四五”规划提出大力推进天地一体化资讯网络建设和加速卫星商业化应用，人民银行《金融科技发展规划（2022-2025 年）》中提出在农村金融领域，借助卫星遥感在内的新型感知技术，实现融资需求精准授信，推动农业保险承保理赔电子化、智能化，打造数字绿色服务体系。同时为贯彻党中央“实现碳达峰、碳中和目标”以及“全面推进乡村振兴的战略部署”，工商银行发挥大行担当，深入推进“绿色金融、普惠金融”，有效引导全行投融资结构优化调整，发挥大行“头雁引领”作用。

当前工商银行的大型商业信贷项目在信贷管理中存在的“现场调查难、人力成本高、效率待提升，信息不全面”等痛点。（1）项目调查的不便利性。项目选址涉及深山、林地、沙漠、海上等偏远地区，现场定期调查不便，且调研成本较高，调研频率受限。（2）人工全局统计评估困难。由于监控范围较大，人工勘探存在调查信息不全面、审核主观因素较大等痛点。例如铁路公路项目涉及多个道路段，风电项目范围几千公里。（3）国际形势不确定因素带来的影响。存在国际形势等不确定因素无法现场监控，例如受制于疫情影响，境外建设项目无法派遣专业人员前往调查监督。

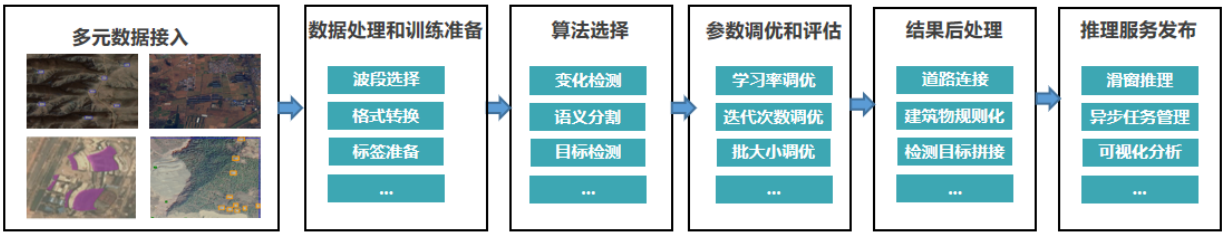
针对以上业务痛点，工商银行将卫星遥感图像智能识别新技术与业务场景的深度融合，基于开源的深度学习框架 PaddlePaddle 飞桨，通过其 PaddleRS 的系列组件，开发地物的分类、识别、变化等深度学习神经网络监控模型，充当遥感数据“解译侠”，自动获取、加工、提取遥感数据信息，形成业务领域价值信息。通过多元化建设风险防控手段，助力风险防控能力自动化、智能化和全面化提升。

（二）创新成效

1. 技术方案

方案上，选择人工智能深度学习方案，与传统遥感分析技术相比，深度学习利用深度神经网络模型模拟人脑的多通路信息传递和处理机制，实现输入数据的分层表达和知识推理。通过数据驱动的自主学习，显著降低对先验知识或人工的依赖；同时网络以卷积为基础，通过分层结构组合低级特征形成更抽象的高级特征，可以提取遥感图像内在的丰富语义特征；深度学习网络的多层结构能够从多尺度提取图像信息，具备表征遥感尺度效应的潜力；深度学习网络数以亿计的参数容量，具有强大的非线性关系学习与处理能力、以及对特征的多维表达能力，更好地契合遥感地表的复杂特征。

在工具选择上，综合考虑自主可控、方案完备先进等要素，选择当前在开源生态相对较为完善的飞桨 PaddlePaddle 框架，Paddle 视觉遥感也具备丰富的算法套件和培训教材文档，可高效实现图像的目标检测、语义分割、变化检测等功能，保障模型具备一定泛化能力。同时选择 GDAL 作为遥感空间数据的处理和格式转换，辅助数据准备工作。



图：模型构建和发布全流程

2. 技术创新

通过应用相关 PaddleRS 和 PaddleCV 套件，针对金融场景适配调优，打造了同业识别范围领先的智能遥感识别能力，首批推出工业建设和农业农村卫星遥感采集和监测体系，赋能信贷业务管理，支撑贷前标的调查、贷中风险控制、贷后预估预警全流程。通过在绿色能源、公路基建、建筑工程、农业授信等 50 余个试点场景综合运用塔吊、桥墩、光伏、风车、建筑物检测、高度测算、面积监控、变化检测等 10 余个智能识别能力，建立适应性

强、准确率高的深度学习模型，能够适应季节、时相、气候、光照等因素造成的卫星影像差异，平均识别准确率可达 90%以上。

3. 业务创新

基于开源深度学习框架和视觉套件技术实现的遥感影像智能分析技术，已在 50 余个场景推广应用，涉及产业园、光伏、风电、矿坑、农业授信等多个绿色信贷场景，以及一带一路沿线公路铁路基建、建筑工程等大型项目。通过定期监测工程建设实时范围、施工面积、公路建设情况、建筑物数量以及建筑用地变化进行实时监控，分析建设进度的变化情况，及时发现风险，为贷后风险预警分析提供依据。共计覆盖超过 1000 亿商业贷款，有效解决了贷后管理环节调查成本高、频率低、监控不全面、疫情期间出行困难等痛点，较大程度提升了大型融资项目贷后风险管理的客观性与准确性，有力加快智慧信贷步伐，展现了信贷管理智能化、精细化、专业化水平，支撑乡村振兴、普惠金融、绿色金融等相关工作。

4. 产业价值

本案例通过应用开源深度学习框架视觉套件，在大数据信用风控领域实现遥感识别能力建设突破，这既是金融数据要素与卫星数据要素融合的突破，也是卫星遥感技术与人工智能技术融合的突破，更是技术和业务融合的突破。充分验证了基于深度学习的遥感影像智能分析技术，在金融行业应用的广泛前景。

工商银行在应用开源技术，融合数据要素，发挥人工智能生产力方面的经验和方案，可供同业进行参考应用。当前遥感数据的企业化运用已具备一定技术和生态基础。同时人工智能技术的进步对海量卫星遥感数据应用带来极大变革，进一步激发了遥感应用创新。金融同业在场景应用上可参考推进加大遥感智能分析识别技术在金融信贷风险防控的应用，在技术上可参考基于 PaddleRS 开源深度学习框架的遥感影像分析技术，打造定制化的遥感分析识别服务。

四、浦发银行区块链应用平台系统建设

（一）案例背景

2019 年 10 月 24 日，习总书记在中央政治局第十八次集体学习时强调，把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展，并进一步指出要实现研究与创新结合、技术与产业和实体相结合、区块链生态和民生相结合。当前区块链技术还处于初期阶段，区块链仍然目前存在诸多问题，在计算性能、扩展性、隐私保护、安全等方面还有待进一步的完善。

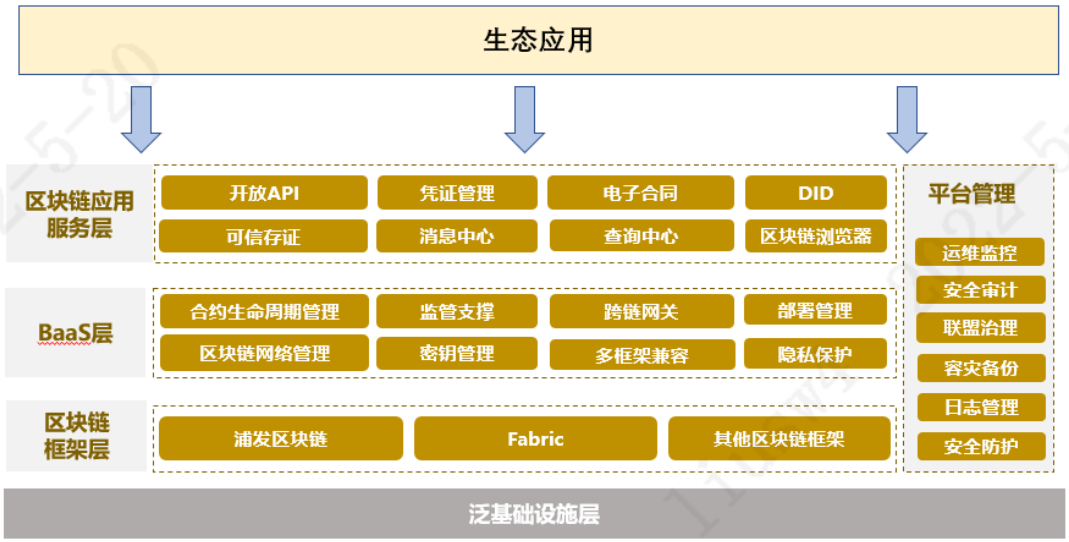
浦发银行于 2018 年启动区块链应用平台建设，围绕降低区块链技术的使用门槛，应用规模化落地需求及解决应用落地“最后一公里”问题，聚焦便捷、统一、高效、安全的平台能力开展探索与实践，充分发挥区块链技术的应用价值。在场景落地上借助区块链与其他技术的融合，使得技术能力叠加后衍生出的创新能力，落实人行安全规范基本要求，提升平台全面运维管理能力，形成基于区块链与创新技术融合，集区块链部署、运维、治理、应用服务及服务开发于一身的金融企业级区块链服务平台。助力浦发银行区块链生态“引进来”及“走出去”协调发展。

（二）创新成效

1. 技术方案

浦发银行通过结合区块链、容器云技术等前沿技术，支持浦发区块链在内的多种区块链框架。其中浦发区块链是基于开源 Hyperledger fabric 1.4.2 版本基础上，进行了全面国密算法、共识协议、安全合规以及安全审计等改造。搭建一个集多链、多租户、多形态的区块链用户管理、运维管理、通用服务于一体的安全、高效、可靠、通用的区块链应用平台。为用户提供全面区块链服务的平台产品，能快速的为企业和开发者在浦发金融云、公有云、私有云中搭建区块链网络。平台聚焦作为企业级区块链 PaaS 建设，支持管理浦发区块链自研框架的区块链网络，同时也支持其他区块链联盟链框架网络技术方案。借助于浦发容器云的技术与产品积累，帮助企业快速、规范的搭建企业级区块链应用业务系

统，辅助企业建立内外业务的可信协作。平台在区块链落地中积累的创新实践，通过区块链应用服务以及多形态的平台能力，以产品和技术输出赋能金融及产业上下游企业，助力企业加速区块链应用落地，强化金融科技与产业深度融合，提升金融服务实体经济的能力。



2. 技术创新

浦发银行区块链应用平台在设计上创新性的提出基于云链结合、容器化及微服务化的分层架构，平台还基于云原生技术与区块链结合，构建多租户能力，支撑规模化应用运维及部署。在隐私保护方面提供分层分级的隐私保护能力。在监管合规审计方面，提供穿透式区块链的全生命周期管理能力，并申请了多篇专利。以此平台为基础，发布的《Q_SPDB 005-2021 浦发银行金融分布式账本技术应用规范》上榜“2021 年企业标准领跑者榜单”。

3. 业务创新

区块链应用平台提供区块链联盟网络管理、多框架兼容服务化能力。具有快速、高效的联盟链网络管理能力，支持一键部署自主联盟链及快速加入内外部链网模式，构建多形态的区块链即服务能力。助于区块链即服务能力的快速输出。

在监管合规及行业安全方面，平台落实中国人行银行关于《金融分布式账本技术安全规范》（JR/T 0184—2020）要求，支持构建金融分布式账本多级安全保护能力。

平台提供 PaaS 层服务能力，满足不同应用不同企业对区块链能力的要求，提供开放 API，使得区块链+金融服务能够快速触达至中小微企业。在区块链应用落地的创新实践中，沉淀的区块链应用服务及定制化服务支撑能力，通过区块链应用服务能力积木式搭建或定制化改造快速实现落地。

通过区块链应用平台系统，促进浦发银行在区块链应用可信存证、供应链金融等领域的快速落地，探索区块链与可验证计算等创新技术的融合，加速区块链赋能业务创新及应用快速落地。

4. 产业价值

目前基于区块链应用平台已经支撑多个应用场景落地，包括可信存证、供应链金融、浦惠云仓、金融债等。其中在“走出去”方面，依托供应链金融、私募电子合同等场景输出区块链即服务能力。在“引进来”方面，实现基于外部区块链，打通金融同业。

五、交通银行分布式数据库技术规模应用

（一）案例背景

当前银行核心业务系统面临的运行风险、困难和挑战日益增大，为解决“变更风险大、数据库单点瓶颈、高并发交易承载难、总体成本高和关键技术不可控”等痛点，交通银行以“增运行效率、增客户体验、降运营成本”为目标，着力探索和推进银行信息技术关键基础设施自主可控。

在核心业务系统下移过程中，数据库是关键，分布式数据库是当今技术架构转型的必选。交通银行持续关注业界分布式数据库发展动态，并在 2014 年基于开源 OceanBase 技术启动自主知识产权的分布式数据库系统（以下简称 CBase）研发,以应用驱动的迭代模式取得了多项关键技术的突破。

Cbase 数据库是一款以原生分布式数据库技术研发和应用实践为总体建设思路，面向商业银行交易处理特性，具有事务特性的关系型数据库系统。经过开源技术消化吸收和再创新，先后完成 SQL 标准化、高可用架构、弹性伸缩、异地容灾、查询优化、开发运维工具体系等多个迭代版本的研制。该项数据库技术已具备百 TB 级数据处理能力和 30000+TPS 事务处理能力，支持跨地区部署集群，灾难发生时可秒级恢复，数据丢失零容忍。在应用实践方面在交通银行十余套业务系统中推广应用，全链路覆盖网络支付场景，并从容应对 2017-2021 连续五年双十一等“潮汐式”、“爆发式”等高难度业务场景,海量数据存储、横向扩展和 7*24 小时服务能力、复杂 SQL 处理能力和高并发事务处理能力得以充分验证。

（二）创新成效

1. 技术方案

借记卡核心业务和账务系统以“集中+分布”并存的技术路线为基础，基于弹性、融合、敏捷创新的设计思路构建,具备大机和开放上并行运载能力，极大提升核心业务系统的横向扩展能力，解决原大机集中式单一架构的瓶颈问题。开放平台数据库系统选用交通银行自主可控的 CBase 数据库技术支撑上亿级别账户数

据存储、上万 TPS 并发处理的业务场景，大机与开放之间数据服务的对等和同步，按照交易类型、交易频率在大机和开放实现动态分配和调整，系统之间即可以互为备份，也可以独立运行。

2. 技术创新

CBase 分布式数据库采用 share-nothing 系统架构，满足高并发处理需求的同时实现存储和计算资源的线性扩展；设计并实现了集群环境下分布式数据库的自动选主和基于 raft 的数据同步技术，在突破了传统数据库难以兼顾高可用和强一致性的困境的同时，在 X86 服务器基础上搭建集群，摆脱了对高端服务器及高端存储的依赖，大幅减少应用系统成本。实现了分布式二级索引和查询优化器，解决了银行应用对复杂查询的性能要求；保证分布式事务一致性，提出并优化未决事务处理避免无限阻塞造成的死锁问题。

3. 业务创新

2019 年 3 月首家试点行上线，成功在 9 月完成高频借记卡金融交易下移至分布式架构及全行推广。全行借记卡数据从 IBM 大型机 DB2 数据库下移至基于“X86”服务器的自主研发分布式数据库，完成借记卡网上支付等高频交易从主机平稳迁移至开放平台，整个过程系统零停机、客户零影响，借记卡网上支付场景的性能峰值提升到 1 万 TPS。随着借记卡金融交易的逐步下移，2021 年开放平台日常分流已达到借记卡应用交易量的 50%，“双十一”占比达 90%，承载借记卡行内外支付类业务和代发类业务全部交易。

4. 产业价值

交通银行分布式数据库技术规模应用不仅解决了分布式架构下数据库系统选型的痛点，同时也在逐步努力改变“核心技术受制于人”的不利局面，践行国家关键技术自主可控战略，对于企业的数据安全、业务稳定具有重要意义，是金融行业应用先进技术支撑金融服务创新的成功实践。

该应用案例具有鲜明的行业示范性，先后获得人民银行科技风险管理二等奖，银行业科技发展管理课题一类、二类成果和教育部科学进步一等奖等荣誉。在分布式数据库上的建设和实践将

推动银行业摆脱对外部厂商的技术依赖，在数据库方向上形成多源可替代的产品，推动国家安全战略的落地，同时也极大地促进国内数据库产业的蓬勃发展。

六、中国农业银行开源软件一体化管理平台

（一）案例背景

全球开源技术正处于大发展阶段，开源生态已成为孕育关键核心技术的重器和推进数字化进程的新动力，通过开源支撑金融企业核心技术框架，既能确保充分接轨国际主流技术，又能确保以深度参与方式完成金融信息建设，实现从“可用”到“好用”的转变。但金融机构对开源软件的管理还存在许多不足之处。一是开源软件游离在传统管理体系之外；金融行业使用开源软件的时间不长，早期对开源软件管理的重视程度不足，从而导致开源软件游离在传统管理体系之外，无法得到有效管控。二是开源软件往往独立于既有架构之外，具有“集市”化松散开发等特点，导致其与现有系统的标准不统一、接口不一致、互操作性不强，与专有软件融合程度不够。三是开源软件版本迭代快、项目分支多、缺乏商业化支持，测评体系不完善。四是开源软件漏洞引发的安全事件不断发生，给金融行业开源软件安全管理工作带来巨大压力。中国农业银行对标信息技术创新战略要求，鼓励使用开源技术掌握主流核心技术，破解“双不”困境，并为保证整体风险可控，充分利用现有成熟软件管理和工具体系，避免多套体系各自为政、职责交叉混淆和多头分散管理，综合分析研发领域已有管理体系，按照“统筹规划、合理布局、分散实施、优化改进”原则，结合对金融行业开源软件管理方法和实践技术的研究，确定了开源、自研、商业软件一体化融合式管理策略，设计了一套融合传统和开源理念的软件管理体系和框架 TOSIM（Traditional & Opensource Software Integrated Management），形成了完备的开源治理组织和统一的开源管理体系，并依托已有工具和开源技术，建设了统一、协调、补充、兼容的开源管理平台，以更好、更高效地强化开源管理。同时，为坚持履行大行使命担当，尝试通过内部开源和对外开源的方式，沉淀并输出开源技术研究成果。

（二）创新成效

农业银行的“开源软件一体化管理平台”通过整合各方面技术资源，打通开源软件全生命周期管理流程，构建形成开源软件

管理的流程化、线上化和可视化，在农行的软件管理活动中发挥重要的支撑作用。如图 1 所示，农业银行开源软件一体化管理平台实现了对开源软件的全流程、多领域一体化管理，打通开源软件管理流程，为研发协作提供支持，保证开源软件相关管理活动有序开展，提升开源软件管理质量和效率，为 TOSIM 一体化管理体系的落地提供技术平台支撑，实现了从开源软件引入到退出的全生命周期闭环管理。

图 1 农业银行开源软件一体化管理平台

开源软件一体化管理平台具有流程支持、研发支持、配置管理、安全管理和内源社区等功能。农行通过 Spring-boot、Mybatis 等开源组件建设了太行平台，用于支撑各类管理平台快速设计和部署平台框架、便捷访问各类数据库；流程支持平台通过 fastjson 开源组件实现了平台的 json 报文转换功能，支撑开源软件管理全流程的打通，通过贯通运行态和管理态的管理工具，提供了开源软件全行统一使用视图、测评信息、软件及协议目录、漏洞知识库；研发支持平台从开源软件协作开发、问题支持、知识库支持等方面提升开源软件研发建设的质量和效率；配置管理工具实现对开源软件一体化的配置和构建，实现对开源软件资产的全景式管控；安全管理工具包括开源软件漏洞扫描工具和源代码安全检查工具，开源软件漏洞扫描工具能够发现开源软件是否存在已曝光漏洞，源代码安全检查工具能够检查开源软件源代码安全缺

陷情况，实现由过去撒网式漏洞通报处置方式向当前精准定位处置方式的转变，有效降低生产系漏洞风险敞口，保障系统安全平稳运行；内源社区 GTR 基于 Git 开源技术，建立了行内代码交流和开源技术交流平台，作为对外开源试验田，推动行内外技术创新和方案共享。通过农行开源软件一体化管理平台，管理工具可在系统提交测试准入时，从运行态工具实时获取系统组件使用视图，并自动识别协议或安全漏洞风险，生成测评任务推送给用户；在系统进行投产构建时，运行态工具从管理态工具获取组件测评覆盖情况，通过质量门禁控制制品晋级，做到开源软件管理覆盖、软件安全、信息一致、自动更新。

农业银行通过 TOSIM 一体化管理平台建设，加速了行内各业务领域的开源技术应用和产品创新，覆盖了渠道域、客户服务域、产品与服务域、企业数据管理域、业务管理域和基础应用域等 6 大应用域，为 500 余个应用提供有力支撑。

农业银行积极输出开源管理平台体系建设经验，参与行业交流，先后参与了开源管理相关的多部行业标准的修订和编制。2018 年，农行的开源软件管理与应用探索实践课题获得银保监会的银行业信息科技风险管理课题一类成果；2019 年，农业银行成为首批通过信通院可信开源治理能力评估的金融企业；2020 年，农业银行在信通院可信开源治理成熟度评估中被评为最高等级“先进级”；2021 年，农行获信通院颁布的开源治理“OSCAR 尖峰开源企业”，同年开源治理体系与标准化研究工作获得全国金融标准化技术委员会颁布的“年度金融标准化重点研究课题一等奖”。

七、中国工商银行——关注构建自主可控的金融科技开源生态

中国工商银行长期重视和关注开源技术治理，开源软件治理能力处于金融同业领先水平，结合多年应用经验，形成了软件开发中心牵头的开源软件统一协调管理小组，覆盖全行各机构软件管理制度规范，并以软件产品管理系统为核心，集成软件成分分析、安全扫描、项目测试的一体化工具支撑平台，打造一套可信开源治理体系，保障行内开源使用安全、合规、可控。作为金融科技领域头部企业，工商银行也积极参与业界各类开源工作，在开源标准体系制定、开源产业建设、开源项目推广等领域持续投入，有力推动了银行业开源生态的发展。

在开源标准体系建设方面，工商银行积极参与《金融业开源软件应用管理指南》《金融信息系统开源软件应用评估规范》《金融业开源技术 术语》等金融行业标准的编制。同时，汇聚了联盟、浦发银行、微众银行、麒麟软件等机构的一大批金融领域开源人才，助力金融业开源技术标准体系的完善，输出金融技术产品开源管理经验，共同制定了《金融技术产品开源项目管理指南》团体标准。《指南》于 2022 年 8 月正式对外发布，为金融机构提供了一套将自研技术产品对外进行开源的全流程指引，主要从体系建设、流程管理、资源配置、运营等方面，制定了金融机构在进行项目开源时，整体开源组织架构的职责划分以及各阶段项目开源工作的规范要求，适用于银行业机构对技术产品实施自主开源，也可供保险、证券等其他金融机构参考。《指南》加强了金融科技生态与开源生态的进一步融合，同时也填补了金融技术产品对外开源工作机制类标准的空白。

在开源产业建设方面，工商银行也积极参与业界开源产业的建设和推广，于 2021 年顺利完成“可信开源治理评估标准”的 10 大能力指标测评并达到同业最高水平。同时，工商银行深度参与的“云原生多集群管理项目 karmada”获得“OSCAR 尖峰开源项目及开源社区”尖峰案例，工商银行作为参与该项目的头部企业之一，持续参与 karmada 社区的开发和管理工作，在多集群自动调度、伸缩等多个模块做出突出贡献。此外工商银行“工银磐石-分

布式服务”也荣获 “OSCAR 尖峰开源技术创新”尖峰案例，这是业界对工行在云计算及微服务在开源社区技术创新方面所做出贡献的高度肯定。

在开源项目推广方面，工行除了深度参与 Karmada、Loggie 等社区建设之外，也在 Kubernetes、Chaosblade、Dubbo 等各技术领域持续对外输出工行能力，并在部分社区担任 Maintainer、Committer 等角色，负责相关社区的技术演进规划和日常运营等工作。核心开发也积极在各类技术大会和社区沙龙中分享工行在相关技术领域的实践经验，促进开源项目的推广。

未来，中国工商银行将紧跟业界开源发展趋势，与各类开源产业联盟密切联动，大力建设银行业开源共享新生态，全面助力银行开源生态快速发展。

八、浙江网商银行——开源治理实践

浙江网商银行自成立以来，坚持以信息科技为驱动，依托数字技术体系，深入布局移动互联、生物识别、云计算、大数据、人工智能、卫星遥感、区块链、隐私计算等前沿数字技术，自主研发核心业务系统，为小微经营者和“三农”群体提供无微不至的纯线上金融服务。为了提升业务系统中开源技术的应用水平和自主可控能力，网商银行积极响应《关于规范金融业开源技术应用与发展的意见》（银办发〔2021〕146 号），建立健全开源技术应用管理制度体系。结合实际情况，由标准部门牵头，联合架构部、安全部、法务部、合规部等多部门，制定并发布了《开源软件引入规范》和《开源软件全生命周期应用规范》两项企业标准，助力业务系统健康可持续发展。

（一）开源软件引入规范

《开源软件引入规范》重点关注开源软件引入阶段。针对开源软件引入业务系统，该标准制定了详细的评估规则与评估流程，以及在评估流程中的评估清单。

1. 开源软件引入评估

在开源软件正式引入之前，《开源软件引入规范》要求需要开展开源软件引入评估。主要的评估类目和标准要求如下：

（1）执行开源引入决策：由业务技术团队的需求触发，或被动引入隔离时触发，定义了主动引入场景、被动引入场景和基于开源技术的云服务场景下的决策办法；

（2）定义开源合规标准规范：制定一次性更新和定期更新的策略；

（3）执行软件架构评审：架构团队负责评估开源软件引入的架构影响；

（4）定义安全评审机制：安全团队负责定期更新有安全漏洞的开源软件；

（5）定义软件物料清单和风险数据：交付团队负责更新软件物料清单和风险数据；

（6）定义合规评审机制：法务合规提供「开源引入合规判断方法」。

2. 开源软件引入

在引入评估完成后，开展实际引入操作。主要包括：

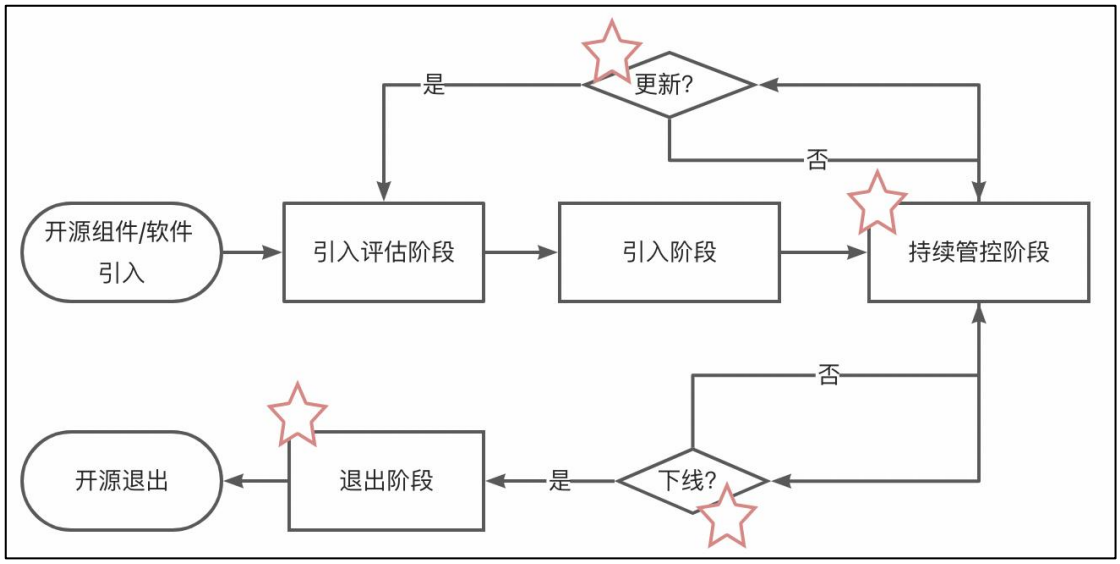
（1）执行安全评审：安全团队触发漏洞扫描，并提供准出标准和决策建议；

（2）执行合规评审：法务合规团队执行开源合规扫描，判断引入的软件是否有合规风险；

（3）开源软件资产管理实时更新：架构团队负责开源软件资产管理平台数据定时更新。

（二）开源软件全生命周期应用规范

《开源软件全生命周期应用规范》重点关注开源软件引入之后的管理，包括持续管控阶段（代码在系统中持续集成、使用、升级）和退出阶段（没有系统使用相应代码后的合理退出）。



1. 持续管控阶段

在持续管控阶段的日常工作主要包括：日常化管控机制、开源组件风险管控、漏洞发现、应急响应及上报机制、安全升级、合规升级、软件版本更新必要性评估、软件版本更新等。

2. 退出阶段

开展退出必要性评估和下线操作完整性评估工作。在开源软件资产管理平台中，开展退出风险评估，保证业务系统稳定运行。