

银行业私有云建设发展 调研报告

2022年11月

金融电子化

版权声明

本报告版权属于《金融电子化》杂志社有限责任公司（以下简称：《金融电子化》杂志社），并受法律保护。转载、摘编或利用其他方式使用本调研报告中的文字、图表、观点，应注明“来源：《金融电子化》杂志社”。未经《金融电子化》杂志社的书面许可，任何单位或个人不得断章取义、增删、曲解本报告内容。违反上述声明者，《金融电子化》杂志社将保留追究其法律责任的权利。

本报告所涉及的数据来源于业内数据采样，采用深度访问、抽样调查相结合的统计方法。由于统计方法本身的局限性，报告数据与市场真实情况可能存在统计误差。《金融电子化》杂志社对其独立研究或与其他机构共同合作的所有研究数据、研究技术方法、研究模型、研究结论及衍生服务产品拥有全部知识产权。

本报告及衍生产品最终解释权归《金融电子化》杂志社所有。

前 言

云计算在数字经济和数字金融发展中起到重要的基础性、先导性和战略性作用，已经成为金融业数字化转型的基石和枢纽，国家有关部门高度重视，先后出台多项重要措施，支持和鼓励金融业积极发展和运用云计算。《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》提到：加快推动数字产业化。培育壮大人工智能、大数据、云计算、区块链、网络安全等新兴数字产业。云计算被列为数字经济重点产业中的首位。人民银行《金融科技发展规划（2022—2025 年）》提出：加快云计算技术规范应用，有效释放云端压力，快速响应客户需求，为金融数字化转型提供更为精准、高效的算力支持。

私有云作为云服务的三种模式之一，已越来越成为金融行业的云应用首选。私有云作为金融业重要的基础服务平台之一，通过云服务产品体系和云组织机构的建设和协同融合，能够保障金融行业关键业务应用的连续性、稳定性、高可用性、低网络延迟性和数据安全性。

为更好地了解我国银行业私有云建设的现状，精准把握核心需求，有效发现行业共性问题，宣传成功经验和典型范例，积极推动私有云建设，我们组织了针对银行业私有云建设的调研工作，从银行业云计算应用与未来规划、银行业私有云应用现状与趋势、银行业容器云应用现状与趋势、银行业用户期待与展望等多个维度，采用多种方式，对 100 余家银行业金融机构进行了深入细致的调研，也获得了各方面的大力支持和积极参与，对调研数据进行科学研究与分析，形成了《银行业私有云建设发展调研报告》，期望能为我国银行业私有云建设提供有益的经验和方法。

编制委员会

主任委员	潘润红			
副主任委员	杨文艳			
成员	张学峰	李明富	魏斌	郑艺
排版	韩碧君			

《金融电子化》杂志社有限责任公司
业务策划中心

贡献单位

中国农业发展银行	中国工商银行	中国农业银行
中国银行	中国建设银行	交通银行
中国邮政储蓄银行	中信银行	中国光大银行
华夏银行	中国民生银行	招商银行
兴业银行	广发银行	平安银行
上海浦东发展银行	恒丰银行	渤海银行
浙商银行	北京银行	昆仑银行
天津银行	河北银行	张家口银行
秦皇岛银行	唐山银行	邢台银行
保定银行	邯郸银行	沧州银行
晋商银行	内蒙古银行	阜新银行
抚顺银行	丹东银行	吉林银行
龙江银行	上海银行	南京银行
江苏银行	苏州银行	杭州银行
绍兴银行	嘉兴银行	广西北部湾银行
徽商银行	厦门银行	厦门国际银行
泉州银行	江西银行	九江银行
赣州银行	上饶银行	齐鲁银行
济宁银行	潍坊银行	莱商银行
烟台银行	青岛银行	齐商银行
临商银行	郑州银行	洛阳银行
湖北银行	汉口银行	长沙银行
华融湘江银行	广州银行	珠海华润银行
广东华兴银行	重庆银行	成都银行
贵州银行	贵阳银行	富滇银行
西安银行	长安银行	甘肃银行
兰州银行	石嘴山银行	北京中关村银行

天津金城银行	深圳前海微众银行	山西省农村信用社联合社
江苏省农村信用社联合社	安徽省农村信用社联合社	福建省农村信用社联合社
江西省农村信用社联合社	山东省农村信用社联合社	湖北省农村信用社联合社
广西壮族自治区农村信用社联合社	海南省农村信用社联合社	四川省农村信用社联合社
云南省农村信用社联合社	陕西省农村信用社联合社	甘肃省农村信用社联合社
青海省农村信用社联合社	新疆维吾尔自治区农村信用社联合社	北京农村商业银行
天津滨海农村商业银行	大连农村商业银行	丹东市农村商业银行
上海农村商业银行	江苏江南农村商业银行	江苏张家港农村商业银行
无锡农村商业银行	青岛农村商业银行	武汉农村商业银行
东莞农村商业银行	广东南海农村商业银行	成都农村商业银行
贵阳农村商业银行	宁夏黄河农村商业银行	辽宁新宾农村商业银行
辽宁清原农村商业银行	辽宁宽甸农村商业银行	辽宁沈抚农村商业银行
辽宁东港农村商业银行	辽宁凤城农村商业银行	曲沃县新田村镇银行
朝阳柳城村镇银行	凌源天元村镇银行	无为徽银村镇银行
云霄润发村镇银行	开封新东方村镇银行	上蔡惠民村镇银行
长葛轩辕村镇银行	昆明晋宁融丰村镇银行	阿拉善左旗方大村镇银行

目 录

观点摘要·····	1
第一章 调研背景与方法·····	4
一、调研背景·····	4
二、调研范围·····	4
三、调研对象·····	5
第二章 银行业云计算服务应用现状与关注热点·····	6
一、银行业云计算应用现状·····	6
1. 云计算建设进度不一·····	7
2. 云计算使用程度存在明显的区域差异·····	7
3. 云计算应用呈现多条技术路线并存特征·····	9
二、银行业云计算建设已成为数据中心重点工作·····	9
1. 云计算建设从 IaaS 走向全栈阶段·····	11
2. 信创云建设是当前数据中心工作重点·····	11
3. 容器是 IaaS 延展到 PaaS 过程中的技术热点·····	11
4. 虚拟化正在被云计算替换升级·····	11
三、银行业云计算建设未来规划·····	12
1. 云计算成为推动分布式架构改造的关键技术·····	12
2. 云计算成为金融科技新技术的支撑平台·····	13
3. 信创云成为创新技术关注热点·····	13

第三章 银行业私有云应用现状与趋势	14
一、银行业私有云应用现状	14
1. 私有云成为云平台落地形态的首选	14
2. 私有云逐渐进入核心应用	15
3. 私有云主流建设思路是合作共建	16
二、私有云建设过程中的考虑因素	18
1. 平滑升级能力是私有云建设最受关注的技术价值	18
2. 安全和灾备能力是私有云建设最受关注的管理价值	18
3. 一体化能力是私有云最受关注的使用价值	20
第四章 银行业容器云应用现状与趋势	21
一、银行业容器云应用现状	21
1. 容器云是云原生建设先锋	21
2. 容器云深入敏捷业务应用	22
3. 容器云主流建设思路是合作共建	22
二、容器云建设过程中的考虑因素	24
1. 系统自动发布能力是最受关注的技术价值	24
2. DevOps 能力是容器云最受关注的管理价值	25
3. 一体化能力是容器云最受关注的使用价值	26
第五章 银行业机构的期待与展望	27
一、现状与期待	27
1. 加快完善云计算相关指引或标准	27
2. 逐步建立云管平台，实现多云管理	27
3. 实现非信创云向信创云平滑过渡	28
4. 大力提升云安全管理的多维保障	28
5. 对科技企业的几点期望	28

二、未来建设思路与规划·····	28
1. 加强 IT 基础设施标准化建设·····	28
2. 提升云计算自主可控能力·····	29
3. 有条不紊分步建设云平台·····	29
4. 加大金融科技人才培养力度·····	30
 第六章 银行业云计算实践案例·····	 32
案例 1 邮储银行“金融云平台数字底座”建设·····	32
案例 2 招商银行 ACS 原生云建设·····	36
案例 3 北京银行容器云建设规划·····	40
案例 4 江苏农信夯实金融创新发展的云服务“数字底座”·····	45
案例 5 中国金电“信创金融云”赋能金融机构数字化转型·····	49
 编后语·····	 53
 参考文献·····	 54

观点摘要

中国银行业对云计算认可度高，私有云成为首选

中国银行业对云计算认可度高，参与调研的 129 家银行业金融机构有 89.9% 已使用不同形式的云计算服务，其中私有云使用率最高，达 53.5%，大幅高于其他形式的云服务。

云计算的使用受到业务需求与组织结构的双重影响，呈现出建设进度不一的特征。其中，18 家全国性商业银行均已使用私有云，使用率最高；区域性银行的建设侧重点各不相同，其中京津冀和长三角地区的云服务使用率较高且种类较丰富，其他区域的云建设也各具亮点。

私有云成为银行业云应用首选，中等建设规模占比最高

私有云对底层基础设施和上层应用迭代创新具有重要作用，已成为银行业构建数字化转型基础设施的核心组成部分。截至 2021 年底，银行业私有云建设以 20~500 台服务器的中等规模为最高占比：20 ~ 100 台服务器规模最多，占 27.6%；100 ~ 500 台服务器规模次之，占 25.0%；500 台以上服务器的中大规模私有云占 19.0%，其中 1000 台以上服务器的大型私有云占 12.1%；20 台以下的小规模私有云占 16.4%。

2022 年，综合各受访机构私有云建设规划，我们发现在 20 台以下服务器和 1000 台以上服务器两个规模区间增长明显，这是由于 20 台以下服务器的部分银行业金融机构云化升级从测试验证阶段进入规模化使用阶段，1000 台以上服务器的银行业金融机构进入大规模集中建设阶段。

中国银行业私有云主要应用于开发测试、渠道类和业务类系统

应用开发和测试系统占比最高，达到 53.5%；一般业务类系统陆续上云，渠道类（个人业务和柜台业务）系统占比 42.2%；客户服务类、产品服务类和决策支持类等业务类系统占比 41.4%；核心业务系统办公协同（OA、通讯软件等）占比 33.6%；支付类系统占比 27.6%。

信创云建设是银行业基础设施建设当前及未来关注的焦点之一

信创云可有效支撑并推动新一代应用上线、业务创新和合规建设，银行业在信创试点取得初步成绩之后面临规模化推广。信创云部署成为银行业数据中心的工作重点，占比 42.6%；在云计算建设方面，信创云关注度排名第一，占比 63.6%。在关注的“金融科技新技术发展趋势”中，信创云也排名第一，占比 77.6%。

银行业基础设施建设多条技术路线并存，虚拟化正在被云计算替换升级

目前银行基于自身建设规划，通常会分阶段、按照使用场景，建设多套并存、版本不一、架构不一的云平台。67.4% 的被调研机构使用了虚拟化技术；53.5% 使用了私有云；32.6% 使用了云管平台；容器云和信创云的比例都在 20%～30% 之间。

虚拟化提供计算资源的逻辑抽象，但是云平台需要通过容器、虚拟机、裸金属的联合编排而非单一资源池，支撑复杂程度高的核心应用和新型应用，所以虚拟化技术的替换升级计划增多，成为数据中心的重点工作，整体占比 25.6%，其中有超过 45% 的被调研机构表示将从虚拟化升级到云。

银行业私有云和容器云的主流建设思路是合作共建

云计算技术栈广泛，更新速度快，因此银行私有云建设以外部合作为主的占比超过 70%，其中“选择多家厂商分别建设，赛马制”占比 36.2%，“选择独家厂商建设”占比 35.3%。

容器云自研比例为 34.0%，外部合作为主为 64.0%。超过 40.0% 的银行容器云建设由研发部门牵头。

容器云是银行业云原生建设基础，主要应用于渠道类、开发测试和支付类系统

云原生是构建在以容器技术为核心的基础设施之上的，被调研机构中，66.0% 完成了容器云建设，另外有 4.3% 完成了 DevOps，4.3% 完成了微服务治理。

应用业务中，“渠道类业务（个人业务和柜台业务）”最高，占比 51.1%；“应用开发和测试系统”占比 46.8.%。

平滑升级能力是私有云建设最受关注的高价值技术

私有云建设的技术价值选择中，信创和升级的关注较多，这与私有云的建设阶段有关，一方面，信创从试点走向规模化建设，另一方面，私有云建设多年，亟需兼顾历史和未来的技术方案。

其中，“平滑升级能力，便于大规模部署，保障业务连续性”得分最高。传统私有云一般采用新建和割接两种模式，定制化程度高，产品不够标准化、版本碎片化导致运维复杂化等，造成了银行用户对平滑升级、自动化运维的云平台的高关注和高需求。

“‘一云多芯’能力，支持信创平台建设与应用迁移”得分次之。“一云多芯”相比多云异构，性能和调用颗粒度表现更优，可以基于一体化平台底座提供多样性资源，从而满足屏蔽底层差异，成为快速实现基础软硬件替代和统一业务支撑的关键能力。

一体化能力是银行业容器云最受关注的使用价值

在容器云最受关注的使用价值调查中，“一体化功能，实现容器、DevOps 和微服务治理统一管理”排名第一；“云平台 and 容器云平台的整合，云和容器统一编排调度”排名第二；“容器云运维监控功能，实现自动化运维、统一大屏展示”排名第三。容器云“生于云，长于云”，容器云根植于云，且统一软件交付和运维模式，因此统一管理不仅是向云平台兼容的需求，也与自动化运维、微服务治理相关。

第一章 调研背景与方法

一、调研背景

金融业数字化转型依赖新一代信息技术的应用。以云计算为核心，融合“移、物、大、智、链”等技术，实现新型信息基础设施智能化升级。金融行业加速拥抱金融科技，积极开展信息系统架构转型、软件开发部署方式转型、数据中心云化等工作。面对挑战和新的发展机遇，金融业都在加速业务上云，实现 IT 架构转型与科技应用创新，全面加快云平台建设步伐。

我国金融机构数量众多、发展规模和服务水平各不相同，对金融科技的理解和应用水平不一，在私有云的建设和管理上存在较大差异。大型商业银行基本完成了业务场景全覆盖的金融云服务建设，同时实现了全栈自主创新云服务供给。但多数中小银行由于技术和业务需求的原因，还未进入私有云和信创云的建设阶段。为全面了解现阶段银行业私有云建设的现状，挖掘建设中可借鉴的模式，避免在建设过程中“走老路、走弯路”，尽快弥补云计算建设技术鸿沟，推动数字化转型发展进程，开展此次调研活动，以期在行业内达成共识。

二、调研范围

云计算（cloud computing）是一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式，云服务（cloud service）是通过云计算已定义的接口提供的一种或多种能力。云计算本质上是复杂的信息系统，各模块技术不断迭代，以容器、微服务、服务网格为代表的云原生技术逐渐成为当前技术热点。伴随各行业上云进程深化，及行业云标准的发布实施，云化和数字化转型将进一步加速。

本次调研方向是部署在银行业数据中心内，及部署在主机托管场所的私有云。

三、调研对象

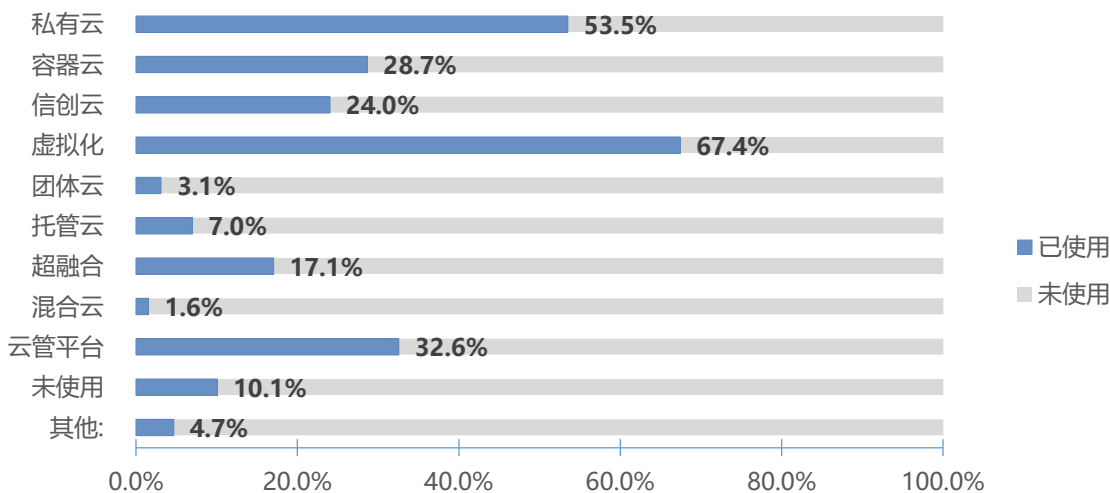
参与调研的银行业金融机构包括：大型商业银行、全国性股份制商业银行、城市商业银行、民营银行、农信社（农商行）、村镇银行。调研采用定量与定性结合的方法。定量方面，通过在线的方式共收集有效问卷 129 份，涵盖了长三角、珠三角、京津冀、中部、西部、东北等六大区域的银行业金融机构。定性方面，与不同类型银行业金融机构代表开展深度访谈。

第二章 银行业云计算服务应用现状与关注热点

一、银行业云计算应用现状

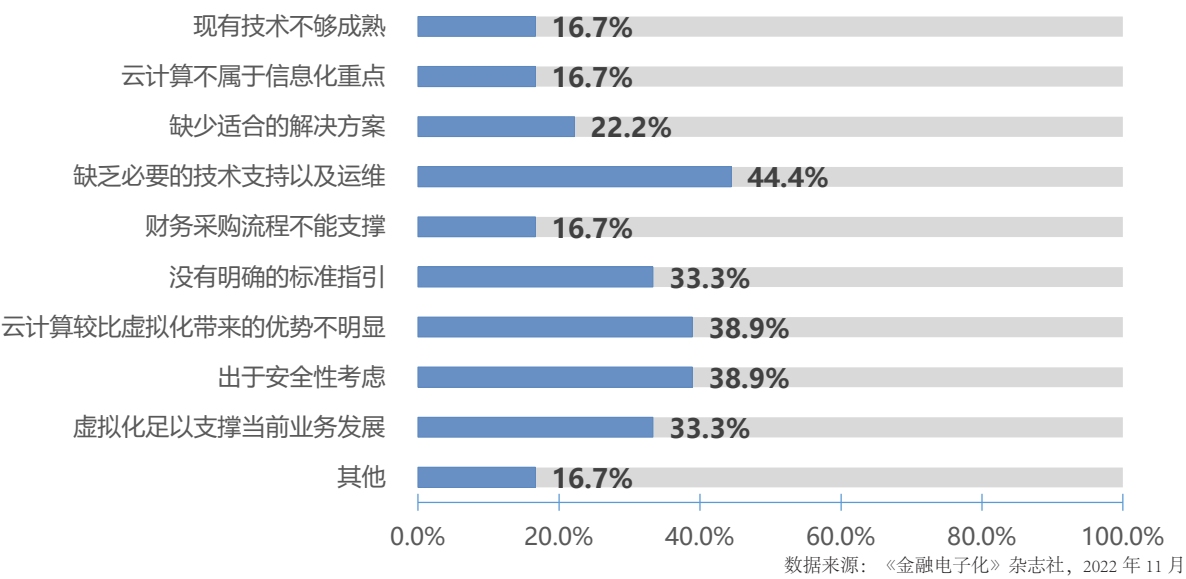
云计算是金融业数字化转型的基石。2017年7月，中国人民银行发布《中国金融业信息技术“十三五”发展规划》，明确要求落实推动新技术应用，促进金融创新发展，稳步推进系统架构和云计算技术应用研究。2019年8月，人民银行印发《金融科技（FinTech）发展规划（2019—2021年）》，提出加快云计算金融应用规范落地实施，充分发挥云计算在资源整合、弹性伸缩等方面的优势，探索利用分布式计算、分布式存储等技术实现根据业务需求自动配置资源、快速部署应用，更好地适应互联网渠道交易瞬时高并发、多频次、大流量的新型金融业务特征，提升金融服务质量。2021年12月，人民银行印发《金融科技发展规划（2022—2025年）》，提出加快云计算技术规范应用，稳妥推进信息系统向多节点并行运行、数据分布存储、动态负载均衡的

图1 银行业云计算服务使用情况调查



数据来源：《金融电子化》杂志社，2022年11月

图2 银行机构未应用云计算的原因调查



分布式架构转型，为金融业务提供跨地域数据中心资源高效管理、弹性供给、云网联动、多地多活部署能力，实现敏态与稳态双模并存、分布式与集中式互相融合。

目前，云计算已经在银行业得到广泛深入应用，成为推动分布式架构改造的关键技术之一，是金融科技新技术的支撑平台。

1. 云计算建设进度不一

云计算在银行业已普遍应用，89.9% 的被调研机构已使用不同形式的云计算服务，其中 53.5% 已使用私有云，24.0% 已使用信创云，28.7% 已使用容器云（见图 1）。

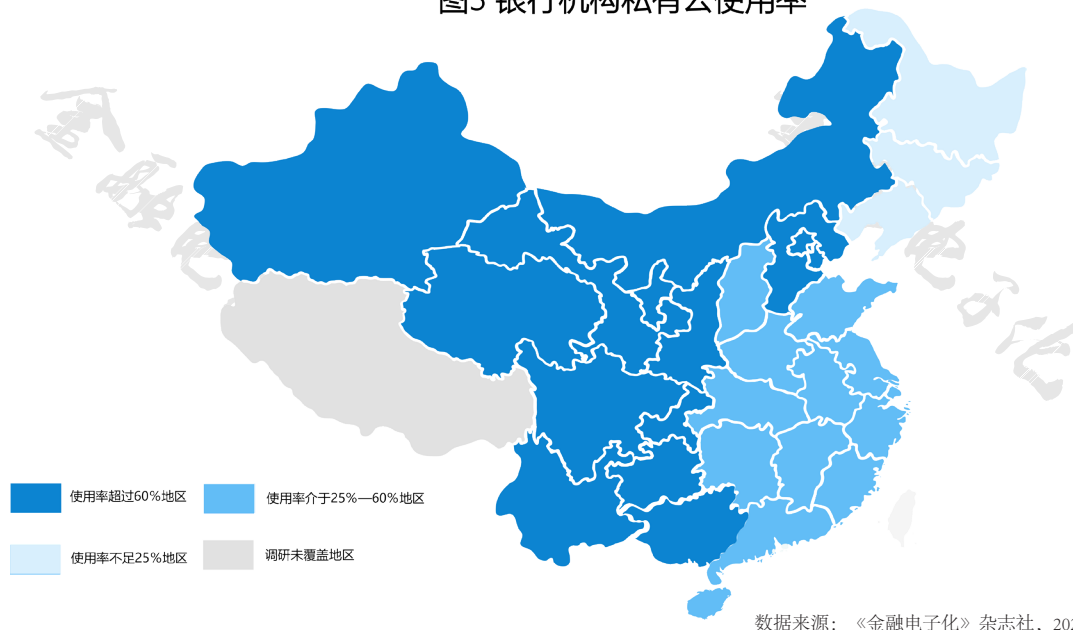
银行业的云化进程并不统一，业务量与组织架构的分散程度影响不同属性银行的云计算服务使用程度。其中，14 家机构的数据中心云化率达 80% 及以上，但多数机构还处于虚拟化到云计算的替换升级阶段。在没有使用云计算的机构中，“缺乏必要的技术支持以及运维”是主要原因（见图 2）。

2. 云计算使用程度存在明显的区域差异

全国性银行的云计算使用程度最高。私有云、容器云、信创云 3 个单项都位列第一，目前 18 家全国性商业银行均已使用私有云，使用容器云和信创云的银行分别高于 70% 和 60%，远超过区域性机构的使用程度。

私有云在不同种类云计算技术中使用率最高。京津冀、西部地区的使用程度最

图3 银行机构私有云使用率



高，比例均超过 60%，长三角地区、中部地区、珠三角地区处于中间位置，比例介于 25% ~ 60% 之间，东北地区上云比例最低，不足 25%。

容器云使用仍处于早期阶段，使用比例最高的京津冀、长三角地区均在 35% 左右，其他地区全部低于 25%。

图4 银行机构容器云使用率

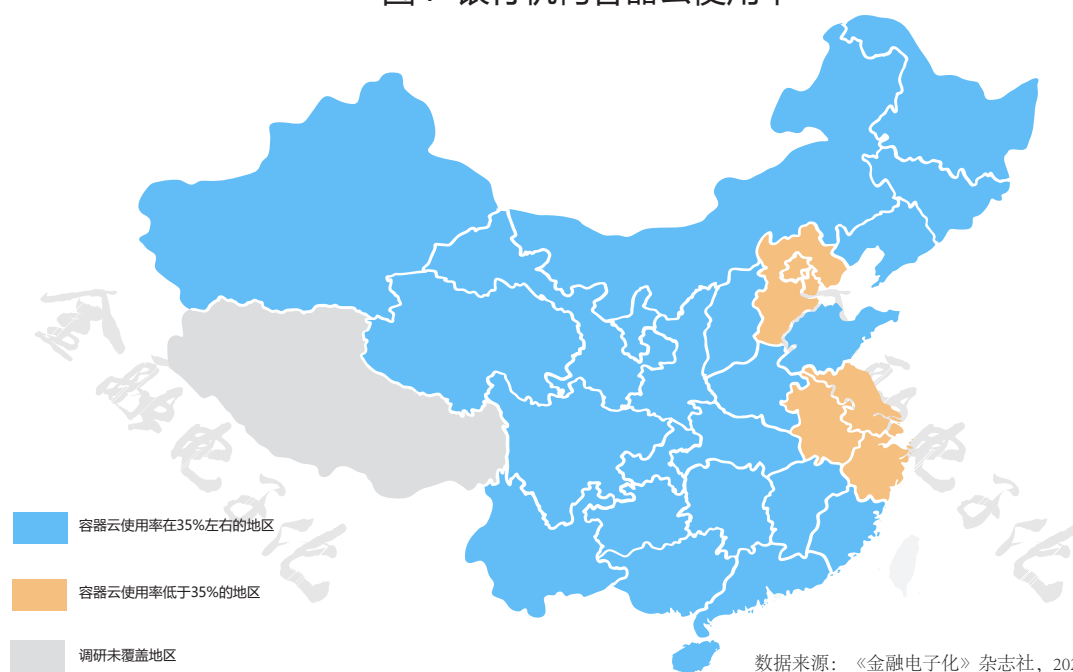
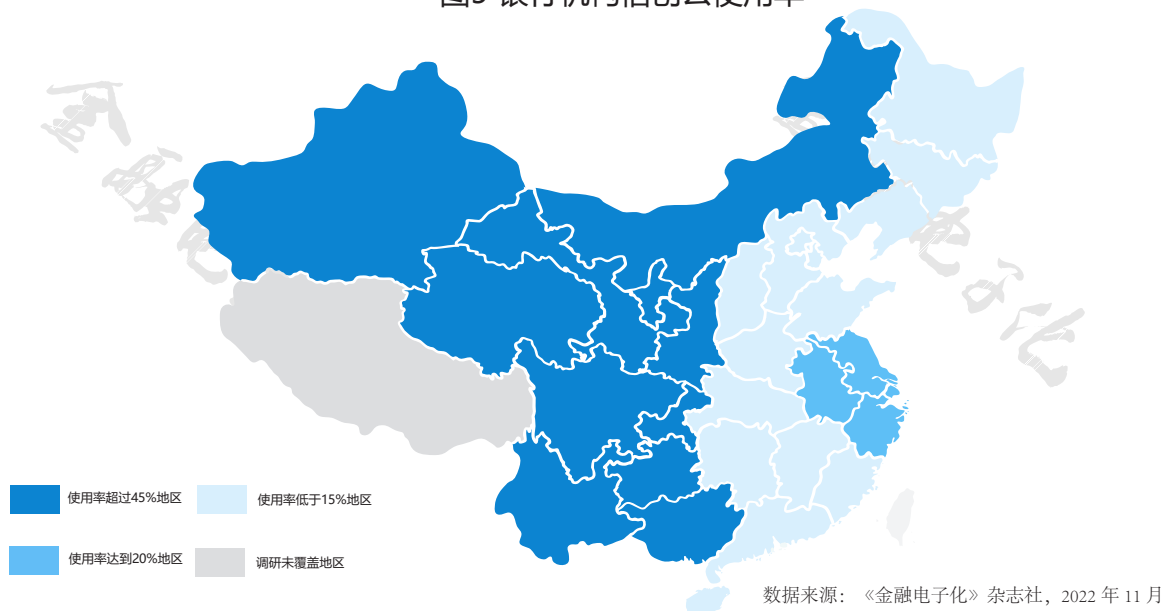


图5 银行机构信创云使用率



大多数机构信创云建设处于选型测试和计划部署阶段，西部地区排名第一，超过45%，长三角地区达到20%，其他区域均低于15%。

3. 云计算应用呈现多条技术路线并存特征

目前银行业金融机构基于自身建设规划，通常会分阶段、按照使用场景，建设多套并存的，版本不一、架构不一的云平台。调查中，虚拟化技术、IaaS、PaaS、开源IaaS、开源PaaS、容器、云原生，以及LOKI（Linux OpenStack Kubernetes Infrastructure）开源基础设施标准的每一代技术都有所应用。

技术使用比例与技术演进时间基本保持一致。67.4%的被调研机构采用了虚拟化的形式；53.5%的被调研机构使用了私有云；32.6%的被调研机构使用云管平台；容器云和信创云的比例都在20%～30%之间（见图1）。

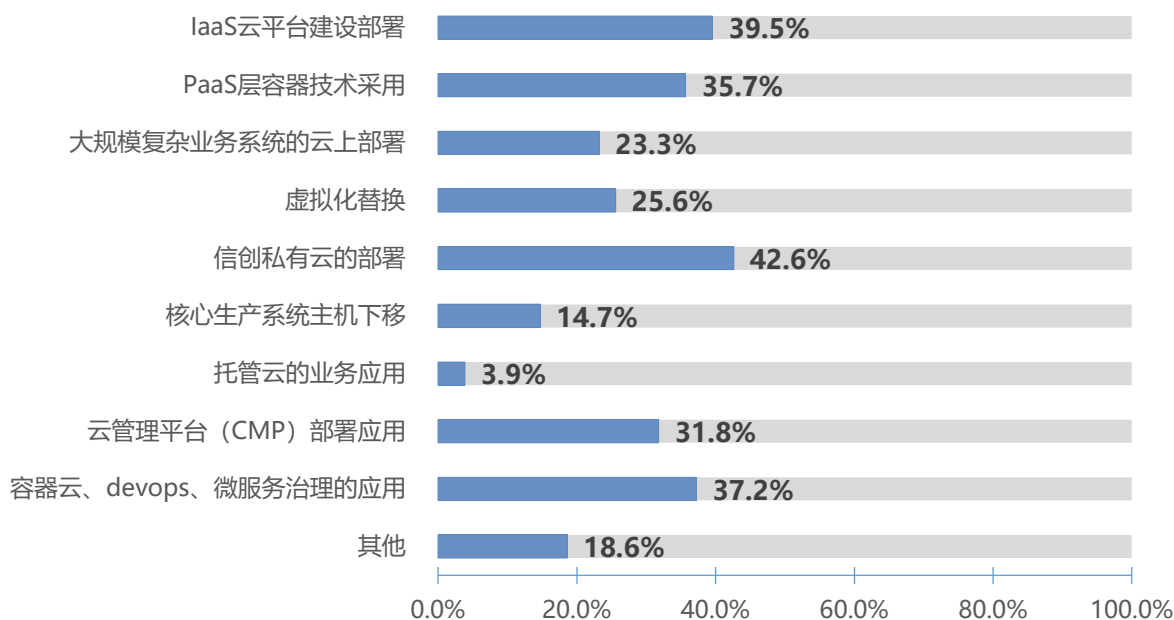
98%的被调研机构认为云计算是信息化建设的重点，云计算作为数字化转型引擎的作用已经得到广泛认可（见图2）。

二、银行业云计算建设已成为数据中心重点工作

云计算是数据中心的重点工作，其中信创云和容器相关技术是关注焦点。信创私有云部署关注最高，占42.6%，IaaS云平台建设部署39.5%，PaaS层容器技术关注度为35.7%，容器云、DevOps、微服务治理的应用等容器相关技术关注度为36.9%。此外，

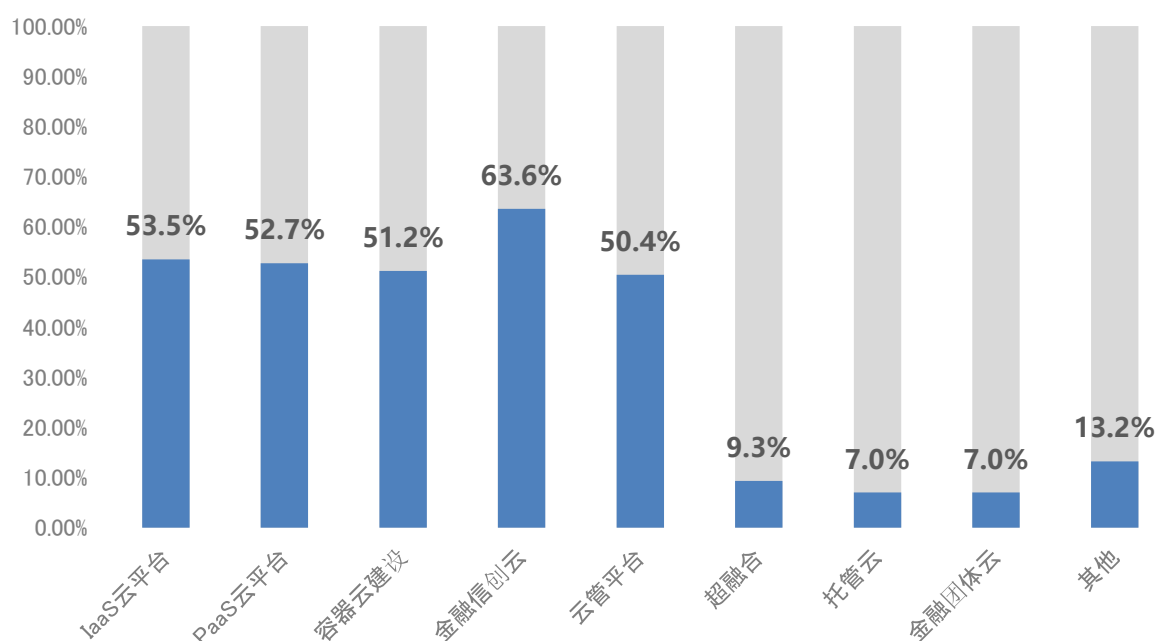
虚拟化替换占比 25.6%，虚拟化正加速向私有云演进。大规模复杂业务系统的云上部署占比 23.3%，边缘业务向核心业务上云进程加速（见图 6）。

图6 银行业数据中心2022年工作重点



数据来源：《金融电子化》杂志社，2022 年 11 月

图7 银行机构2022年云计算建设重点工作



数据来源：《金融电子化》杂志社，2022 年 11 月

1. 云计算建设从 IaaS 走向全栈阶段

云平台已经成为支撑金融业务的基石，云计算的建设重点正在从 IaaS 建设走向全栈建设阶段。私有云、信创云、容器云、PaaS 云、云管理平台建设齐头并进，关注度均超过 50%（见图 7）。

技术路线上，用户选择能够平滑升级的云平台，为未来发展奠定基础。以 IaaS 为基础，放眼全栈，向基础架构云平台、基础架构服务（IaaS）以及平台即服务（PaaS）发展，提高应用深度，扩展应用适用范围，为更多业务系统云化改造和上云之路提供支撑。

2. 信创云建设是当前数据中心工作重点

信创云具有涵盖异构计算资源、异构存储资源、异构网络资源的多样化资源池的能力，并具备符合国家级行业安全标准的能力，可有效支撑并推动新一代应用及业务创新。

信创云建设是当前数据中心重点工作，银行业在信创试点取得初步成绩之后，将进入规模化推广阶段。调研显示，信创云部署成为银行业数据中心的重点工作，占比 42.6%（见图 6）；在云计算建设中，信创云关注排名第一，占比 63.6%（见图 7）。

3. 容器是 IaaS 延展到 PaaS 过程中的技术热点

云原生包括一系列的方法论、实践和技术，涵盖容器云、DevOps、微服务治理等相关技术，容器是其中最核心的部分，解决应用部署自动化、标准化、配置化问题，是 IaaS 和 PaaS 层的技术热点。

容器云、DevOps、微服务治理等相关技术的关注为 37.2%（见图 6）。容器部署可以基于虚拟机和裸金属，银行业用户亟需一套平台实现容器、虚拟机、裸金属的联合编排，从而更好地实现业务支撑。

4. 虚拟化正在被云计算替换升级

云平台正逐步从边缘走向核心，随着更多的新型应用和核心应用具备云原生特性，支撑应用的分布式架构需要从虚拟化走向云平台。云平台需要通过容器、虚拟机、裸金属的联合编排而非单一资源池维度，支撑应用复杂程度高的核心应用和新型应用。所以对虚拟化的替换升级计划增多，成为银行业数据中心的重点工作，整体占比 25.6%，其中有超过 45% 的被调研机构明确表示将从虚拟化升级到云（见图 6）。

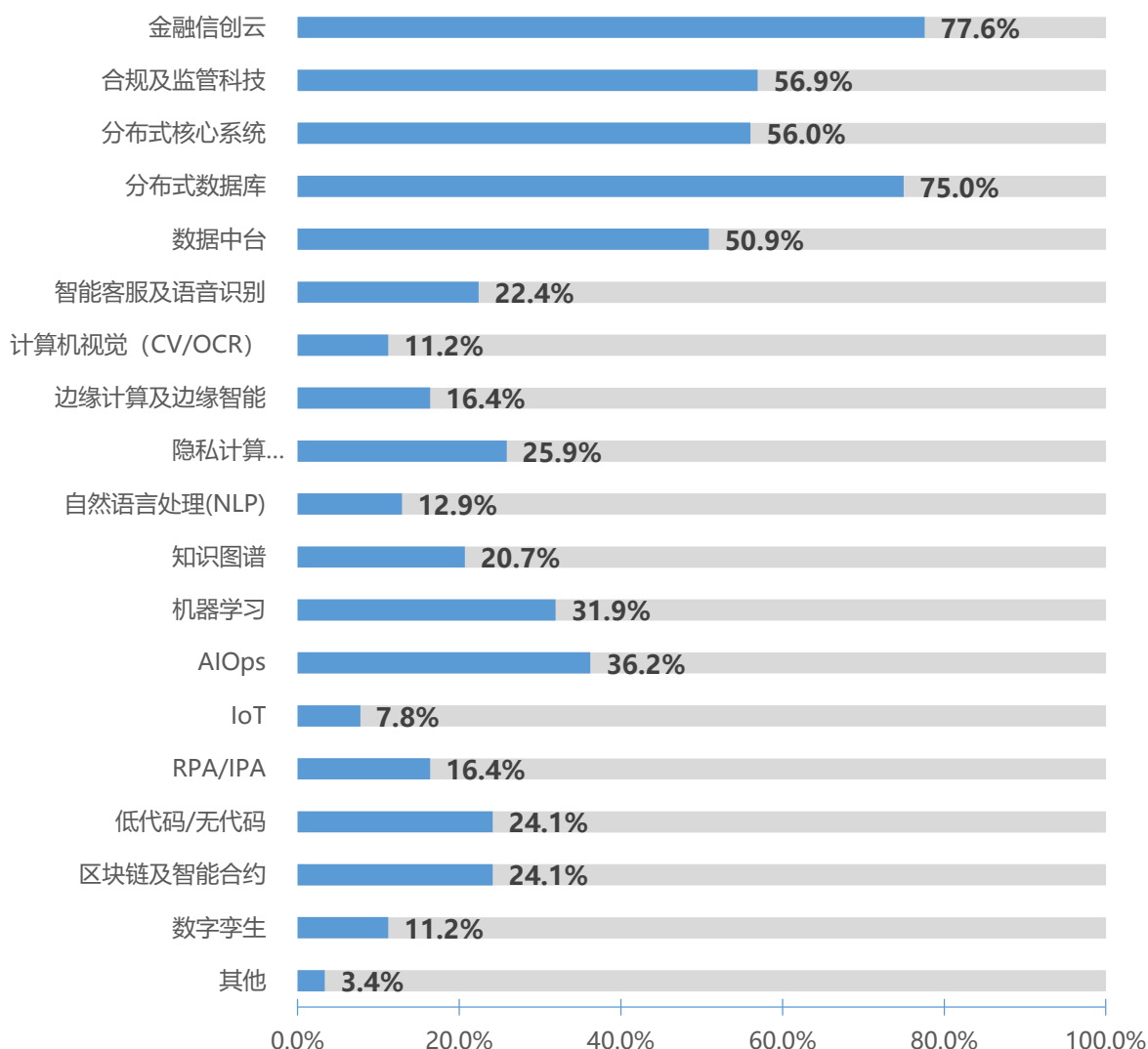
在现状和规划对比中，虚拟化新增下降明显，而信创云、容器云建设将进入加速阶段，私有云建设基本持平。

三、银行业云计算建设未来规划

云计算已经成为银行业推动分布式架构改造的关键技术，成为赋能数字化转型和实现“双碳”目标的方式之一。系统上云，可以通过降低 IT 设备自身能耗，有效降低数据中心的能耗，满足数据中心项目新建、改建、扩建要求。超过 10.1% 的被调研机构选择利用云计算等创新技术实现“双碳”目标。

1. 云计算成为推动分布式架构改造的关键技术

图8 2022年银行机构关注的新技术发展趋势



数据来源：《金融电子化》杂志社，2022 年 11 月

银行系统正在经历从集中式单体架构转型向分布式架构改造，云计算将成为推动这一进程的关键技术。

调研中，在关注的“金融科技新技术发展趋势”中，与分布式架构直接相关的分布式数据库占比达到 75.0%，分布式核心系统占比 56.0%，数据中台占比 50.9%，配套保障分布式架构改造过程中可观察性、业务连续性的 AIOps 工具占比 36.2%。区块链的本质是分布式账本，区块链及智能合约的关注度占比 24.1%（见图 8）。

2. 云计算成为金融科技新技术的支撑平台

创新型金融业务应用需要敏捷高效、弹性可控的 IT 基础设施，这要求 IT 变革需顺应趋势并加快向云端迁移。云平台不仅是分布式核心系统的支撑平台，也是创新技术的支撑平台。

图 8 中，关注度 24.1% 的低代码 / 无代码等创新技术本质上就是一种云的形式。低代码 / 无代码平台虽然有云端和私有化部署两种类型。但是，私有化本地部署本质上是一种基于 PaaS 模式的部署方式。系统布置在本地服务器上，用户可自由操作，可以支持二次开发。

3. 信创云成为创新技术关注热点

在关注的“金融科技新技术发展趋势”中，信创云关注排名第一，占比 77.6%（见图 8）。这与信创云建设面临的技术挑战有关，主要包括以下方面：多样化计算为基础的软硬件尚未成熟而且选择路线较多；核心生产系统下移以及业务广泛应用对基础平台架构提出要求；基于国产化简单替代无法完整应对信息技术应用创新；以及安全合规需求带来的挑战。

“一云多芯”的信创云平台可以基于一体化平台底座提供多样性资源，从而满足屏蔽底层差异，成为快速实现基础软硬件替代和统一业务支撑的关键平台需求。作为资源统一的管理和调度入口，可以同时支持各类不同架构和不同品牌的计算、存储、网络硬件资源，做到生产可用的“一云多芯”。

第三章 银行业私有云应用现状与趋势

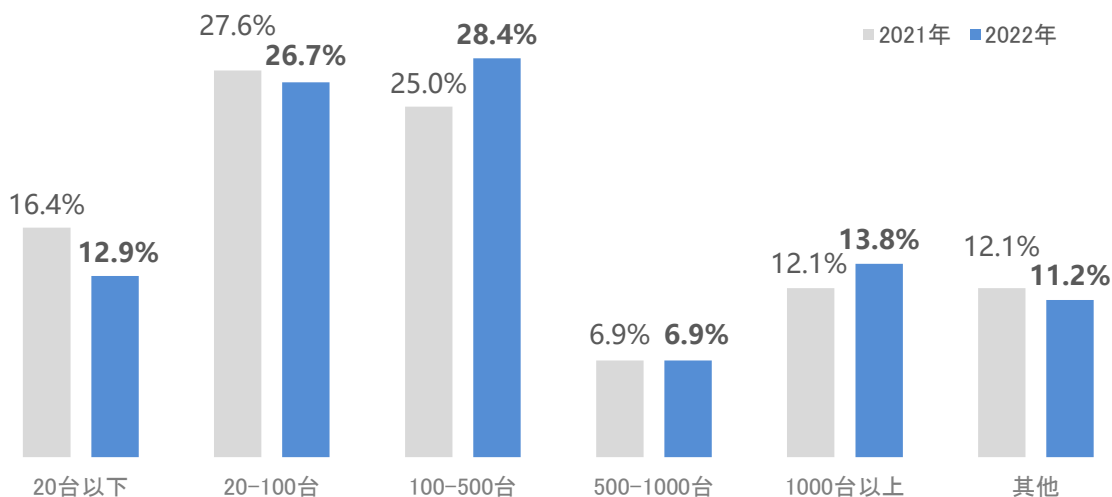
私有云是银行业主要的云计算建设方式，调研中发现，私有云成为云应用首选，大量进入核心应用。在私有云的建设方面，机构多选择与外部厂商合作的方式。在私有云的能力方面，机构选择趋同，平滑升级能力和“一云多芯”能力受到广泛关注，安全相关能力是最受关注的管理价值。

一、银行业私有云应用现状

1. 私有云成为云平台落地形态的首选

私有云能够对底层基础设施云化和上层应用迭代创新具有重要作用，已成为银行构建私有云的核心组成部分。IDC 发布的《中国金融云市场（2021 下半年）跟踪报告》显示，2021 下半年，中国金融云市场规模达到 39.0 亿美元。

图9 截至2021年底银行业私有云建设规模调查



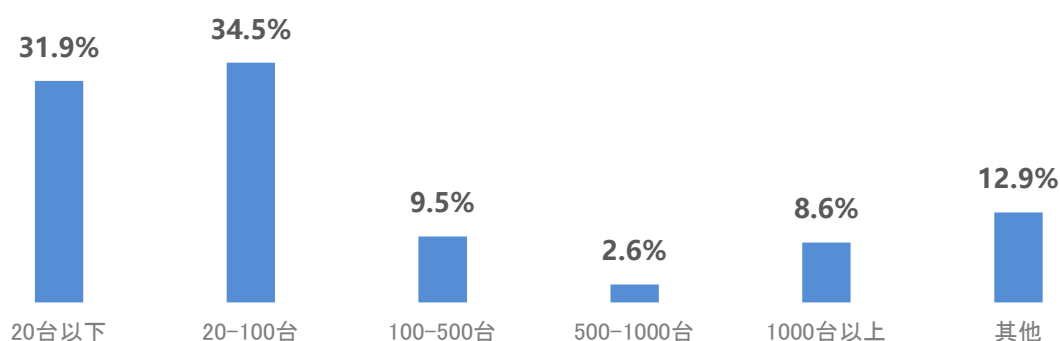
数据来源：《金融电子化》杂志社，2022 年 11 月

截至 2021 年底，银行私有云建设以 20～500 台服务器的中等规模为最高占比：20～100 台服务器规模最多，占 27.6%；100～500 台服务器规模次之，占 25.0%。500 台以上服务器的中大规模私有云占 19.0%，其中 1000 台以上服务器的大型私有云占 12.1%。20 台以下的小规模私有云占 16.4%。另外在本次调研中有 12.1% 的机构选择“其他”，大多是使用金融行业云（见图 9）。

2022 年私有云建设规划中，20～100 台服务器规模最多，占比 26.7%；100～500 台服务器规模次之，占比 28.4%；500 台以上服务器的中大型私有云占比 20.7%，其中 1000 台以上服务器的大型私有云占比 13.8%；20 台以下服务器的小型私有云占比 12.9%。我们发现，2022 年金融机构私有云规模在 100～500 台服务器和 1000 台以上服务器两个区间增长明显，这是由于 2021 年处在 20～100 台以下服务器的部分银行业金融机构私有云使用从测试验证阶段进入规模化使用阶段，1000 台以上服务器的银行业金融机构进入大规模集中建设阶段。

与私有云的规划相比，信创云建设仍集中在试验阶段，100 台服务器以下占比 66.4%，100～1000 台服务器规模占比 12.1%，1000 台以上服务器占比 8.6%，在 2021 年信创云试点成功之后，部分机构开始了信创云的规模化建设（见图 10）。

图10 2022年银行机构计划信创云建设的规模调查



数据来源：《金融电子化》杂志社，2022 年 11 月

2. 私有云逐渐进入核心应用

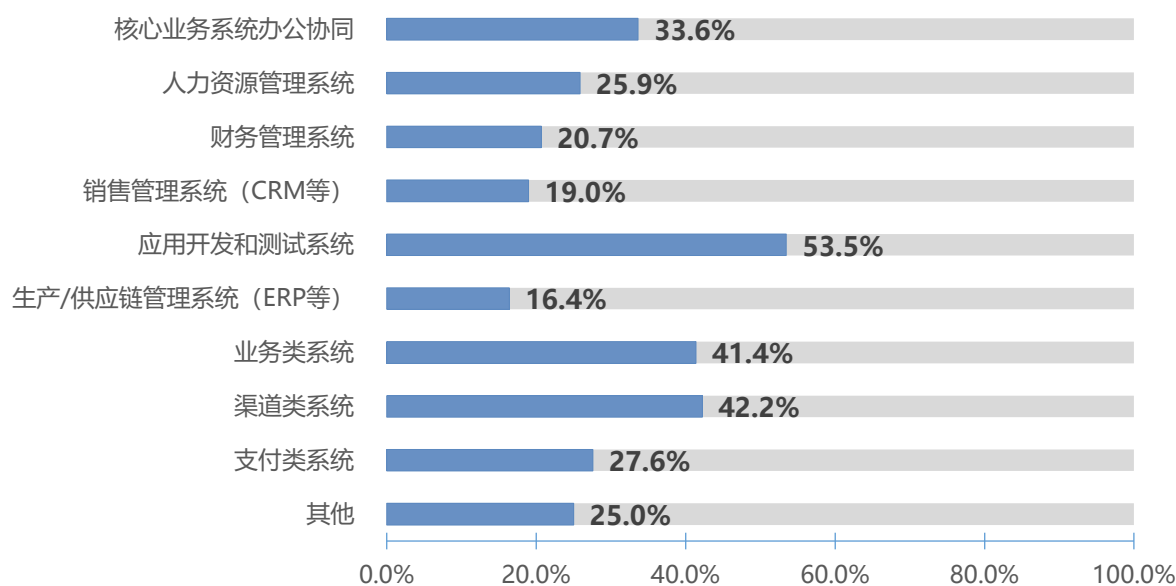
从服务类型来说，银行信息系统一般包括以下 7 种类型：渠道服务类系统：如手机银行、网上银行、柜面前端、第三方外联系统等；客户服务类系统：如客户信息、客户关系管理、押品管理系统等；产品服务类系统：如信贷管理、贸易融资、基金、

债券、理财系统等；核心业务系统：如支付结算、基础账户管理及存取款等银行基础业务系统；决策支持类系统：如经营分析类、监管报送类系统等；基础平台类系统：如总线系统、安全管理平台、运维监控平台等；内部支持类系统：如办公、人力、邮件系统等。

私有云的使用路径，通常先从应用开发和测试系统开始，逐渐覆盖边缘应用直至核心。在迁移上云方面，应用开发和测试系统占比最高，达到 53.5%；一般业务类系统陆续上云，渠道类（个人业务和柜台业务）系统占比 42.2%；客户服务类、产品服务类和决策支持类等业务类系统占比 41.4%；核心业务系统办公协同（OA、通讯软件等）占比 33.6%；支付类系统占比 27.6%（见图 11）。

从边缘应用到核心应用的逐步深化过程中，核心生产系统主机下移成为银行十四五期间私有云建设和运营的重要方向。核心应用的高吞吐、强实时、业务连续性、故障无感知特性对私有云的高性能、低时延、强一致、高可用、高可靠、高安全等能力提出了更高要求。

图11 银行业私有云支撑的业务系统调查

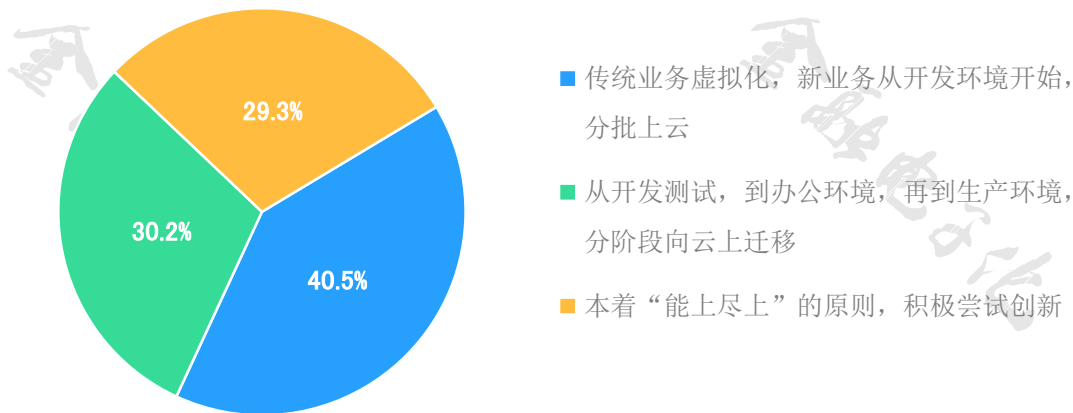


数据来源：《金融电子化》杂志社，2022 年 11 月

3. 私有云主流建设思路是合作共建

银行业私有云建设思路各具特点，40.5% 的被调研机构选择传统业务虚拟化，新业务从开发环境开始，分批上云；30.2% 选择从开发测试，到办公环境，再到生产环

图12 银行私有云建设规划调查



数据来源：《金融电子化》杂志社，2022 年 11 月

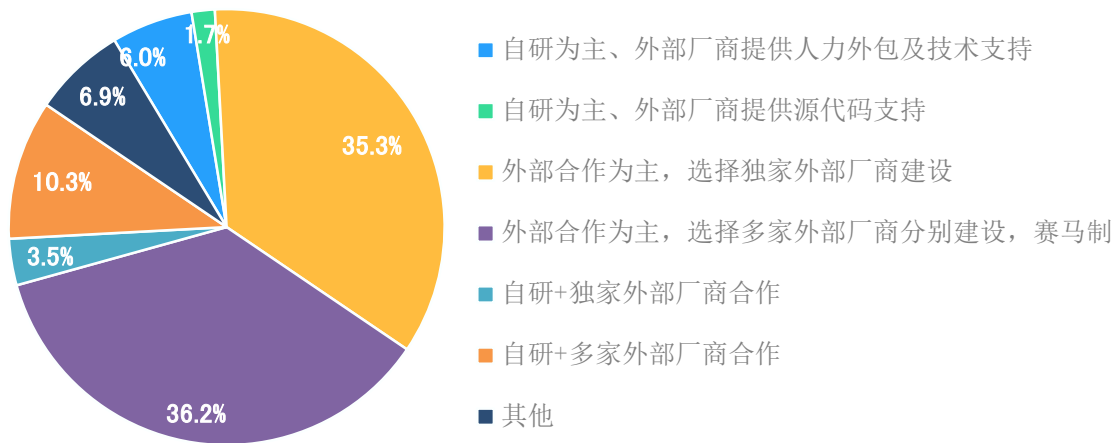
境，分阶段向云上迁移；29.3% 的机构选择本着“能上尽上”的原则，积极尝试创新（见图 12）。

云计算技术栈广泛，更新速度快，因此私有云建设以外部合作为主的占比超过 70%，其中“选择多家外部厂商分别建设，赛马制”占比 36.2%，选择独家厂商建设占比 35.3%（见图 13）。

此外，也有部分机构选择自研为主，外部厂商为辅的建设策略。“自研 + 多家外部厂商合作”占比 10.3%；“自研为主、外部厂商提供人力外包及技术支持”占比 6.9%；“自研 + 独家外部厂商合作”占比 3.5%；“自研为主、外部厂商提供源代码支持”占比 1.7%（见图 13）。

另一方面，因厂商的单项技术研发力量较强，选择独家外部厂商合作的占

图13 银行业2022年私有云建设思路调查



数据来源：《金融电子化》杂志社，2022 年 11 月

38.8%；46.5% 的机构选择了与多家外部厂商合作，在多家外部厂商共同提供支撑的情况下，兼容性问题出现，选择开源生态切实可行（见图 13）。

不同机构的 IT 架构和业务差异较大，私有云的外部支持厂商类型多元。参与本次调研的银行中，私有云外部支持厂商占比较高的 5 家中，既有布局私有云的公有云厂商阿里云、腾讯云、青云（QingCloud），也有综合 IT 服务提供商华为云，还有独立的私有云服务提供商易捷行云（EasyStack）。

信创云建设时间较短，且是一个包含技术、管理、政策等多维度视角的系统工程，与私有云市场的外部支持厂商略有不同。参与本次调研的机构中，信创云外部支持厂商占比较高的 5 家中，有综合 IT 服务提供商华为云、浪潮云，有布局私有云的公有云厂商阿里云、腾讯云，还有独立的私有云服务提供商易捷行云（EasyStack）。

二、私有云建设过程中的考虑因素

1. 平滑升级能力是私有云建设最受关注的技术价值

私有云建设的技术价值选择中，信创和升级的关注较多，这与私有云的建设阶段有关，一方面，信创从试点走向规模化建设，另一方面，私有云建设多年，亟需兼顾历史和未来的技术方案。

其中，“平滑升级能力，便于大规模部署，保障业务连续性”得分 4.63。传统私有云一般采用新建和割接两种模式，定制化程度高，产品不够标准化、版本碎片化使运维复杂等，造成了银行用户对平滑升级、自动化运维的云平台的高关注和高需求。

“‘一云多芯’能力，支持信创平台建设与应用迁移”得分 4.58；“一云多芯”相比多云异构，在性能和调用颗粒度方面表现更优，可以基于一体化平台底座提供多样性资源，从而满足屏蔽底层差异，成为快速实现基础软硬件替代和统一业务支撑的关键平台需求。

此外，“容器存储功能，云平台提供 CSI 接口”得分 2.6，“裸金属功能，云平台具备裸金属数据库纳管能力”得分 2.16，“平台轻量化能力，3 台服务器即可实现控制、计算、存储、网络的最小化云部署”得分 2.13（见图 14）。

2. 安全和灾备能力是私有云建设最受关注的管理价值

云平台容灾系统建设是一项复杂的系统工程，依托于数据复制技术和网络切换恢

图 14 银行业私有云建设技术价值调查

银行业私有云建设技术价值调查	得分
平滑升级能力，便于大规模部署，保障业务连续性	4.63
一云多芯能力，支持信创平台建设与应用迁移	4.58
容器存储功能，云平台提供 CSI 接口	2.6
裸金属功能，云平台具备裸金属数据库纳管能力	2.16
平台轻量化能力，3 台服务器即可实现控制、计算、存储、网络的最小化云部署	2.13
其他	0.34

数据来源：《金融电子化》杂志社，2022 年 11 月

复策略，把银行的重要信息系统在灾备中心重新规划设计。银行业业务连续性要求高，因此对容灾备份能力要求高，原中国银行业监督管理委员会办公厅印发《商业银行数据中心监管指引》的通知要求金融机构设立异地模式的灾备中心，其中重要系统的灾难恢复能力要达到《信息安全技术 信息系统灾难恢复规范》中定义的灾难恢复等级第 5 级（含）以上。

此外，在安全方面，网络等级保护 2.0、网络安全审查办法，以及行业相关政策对云建设安全体系、标准的规划建设提出要求，覆盖物理设备层、云平台层、云服务层、云应用层及数据层在内的全栈关键安全能力。银行业务高度依赖安全可靠和稳定运行的数字化技术的支撑。

私有云建设的管理价值在完成监管和业务增值方面都有体现。“云安全能力，保证云的安全性”得分 4.63；“容灾备份能力，支持两地三中心或三地五中心的同城双活和异地灾备”得分 4.12；“全栈云能力，体现业务的价值”得分 3.59；“兼容性能力，保障管理有序”得分 3.03；“利旧能力，保护投资”得分 1.98；另外，其他得分 0.23。其中，云安全能力和容灾备份能力既是监管需要也是业务需要，得分较高，全栈云和

图 15 银行业私有云建设的管理价值调查

银行业私有云建设的管理价值调查	分数
云安全能力，保证云的安全性	4.63
容灾备份能力，支持两地三中心或三地五中心的同城双活和异地灾备	4.12
全栈云能力，体现业务的价值	3.59
兼容性能力，保障管理有序	3.03
利旧能力，保护投资	1.98
其他	0.23

数据来源：《金融电子化》杂志社，2022 年 11 月

兼容性能力因为能够更好地支撑业务发展也受到关注（见图 15）。

信创云将构筑由芯到云数据中心安全的基础软硬件设施，进一步提高安全水平。

3. 一体化能力是私有云最受关注的使用价值

多种云平台建设容易造成整体建设碎片化和运维困难。云平台的一体化运维和运营是其价值体现的一个关键指标，碎片化问题将影响银行云应用的深入推进。

因此，运维是私有云使用过程中最为关注的价值，与之相关的“一体化功能，实现 IaaS，PaaS，监控运维，ITSM 的统一管理”得分 6.31；“云运维监控功能，实现自动化运维、统一大屏展示”得分 6.12；此外，“多云管理功能，体现混合多云管理”得分 4.74，这三项都与云化程度加深有关（见图 16）。

图 16 银行业私有云建设的使用价值调查

银行业私有云建设的使用价值调查	得分
一体化功能，实现 IaaS，PaaS，监控运维，ITSM 的统一管理	6.31
云运维监控功能，实现自动化运维、统一大屏展示	6.12
多云管理功能，体现混合多云管理	4.74
自服务功能	3.4
用户权限管理功能	3.32
审计类功能	2.66
云计费功能，体现云的价值	2.21
其他	0.35

数据来源：《金融电子化》杂志社，2022 年 11 月

第四章 银行业容器云应用现状与趋势

容器云是数据中心重点建设方向，从调研结果看，容器云建设呈现冰火两重天的状态，虽然被调研对象中只有 1/3 在进行容器云建设，但是在这些开始建设容器云的银行中，66.0% 完成了建设，并且半数银行已经覆盖渠道类和业务类等系统。容器云的技术价值和管理价值受到了广泛关注，特别是平滑升级能力，以及能够实现开发测试到生产运维的 DevOps 能力。此外，业务弹性扩展的支撑能力受到广泛认可。

一、银行业容器云应用现状

云原生应用被定义为“生于云，长于云”，代表着一种新的软件设计理念，同时包括了一系列的方法论、实践和技术，容器相关技术是其中最核心的部分，解决了应用部署自动化、标准化、配置化问题。

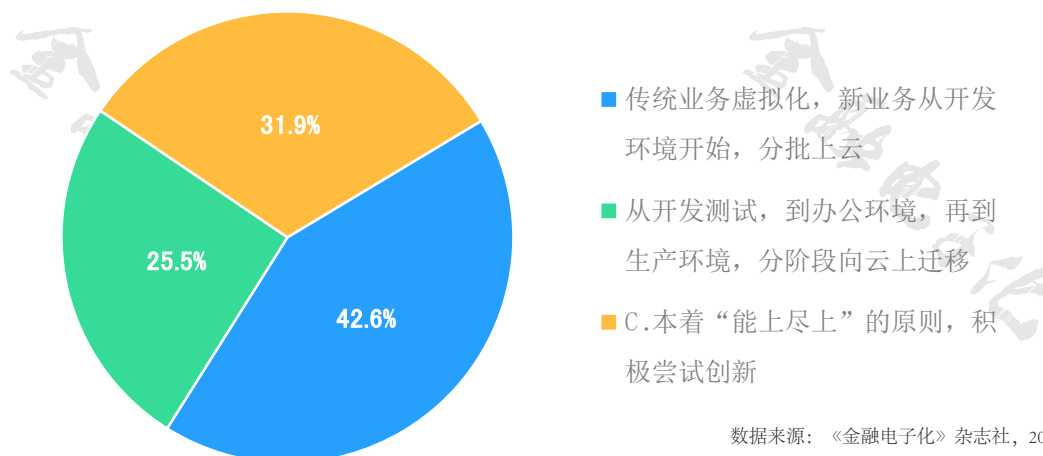
1. 容器云是云原生建设先锋

容器云有利于统一软件交付和运维的模式，从而更好地支撑以互联网业务为代表的敏态业务创新需求。因此，容器云建设比私有云更为积极，32.0% 的被调研机构选择了本着“能上尽上”的原则，积极尝试创新，一方面私有云建设基础良好，对于容器云的接受程度更高，另一方面容器云对于业务的促进加速了这一进程。

此外，“传统业务虚拟化，新业务从开发环境开始，分批上云”占比 42.6%；“从开发测试，到办公环境，再到生产环境，分阶段向云上迁移”占比 25.5%（见图 17）。

云原生的相关技术中，微服务治理实现应用层由中心化向分布式演进，DevOps 实现高效率的开发运维，而云原生是构建在以容器技术为核心的基础设施之上的，所以，容器云的建设进度相对其他建设较快。被调研机构中，66.0% 完成了容器云建设，另外有 4.3% 完成了 DevOps，4.3% 完成了微服务治理（见图 18）。

图17 银行业容器云建设规划调查



2. 容器云深入敏捷业务应用

容器云是云原生的基础，在满足敏态业务创新的领域优势突出。容器云让云基础设施来接管应用中的非业务性代码和功能，用户可以灵活、低成本的方式构建弹性、可扩展的应用，赋予银行敏捷迭代、快速试错和创新的能力，在敏态业务的优势明显。

应用业务中，渠道类业务（个人业务和柜台业务）最高，占比 51.1%；“应用开发和测试系统”占比 46.8.%（见图 19）。

3. 容器云主流建设思路是合作共建

容器云有利于统一软件交付和运维的模式，实践路径上，出现不同部门牵头的情况。

图18 银行业容器云建设进度调查

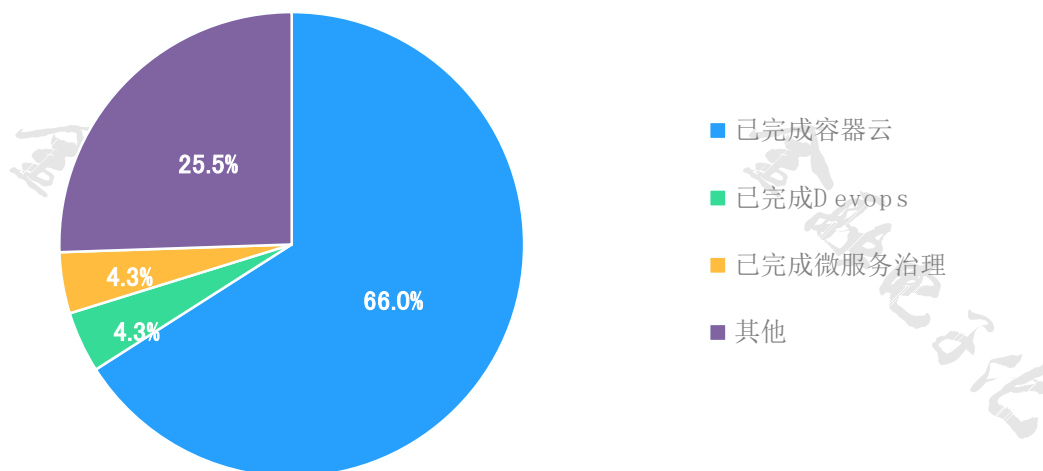
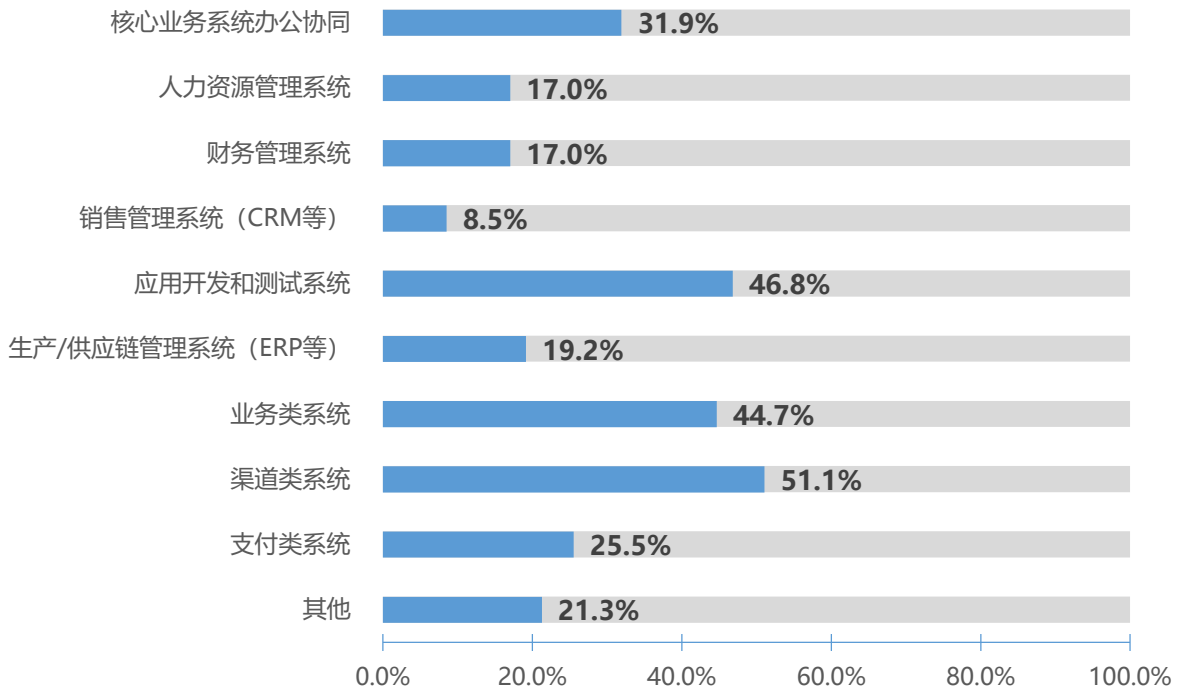


图19 银行业容器云支撑的业务调查



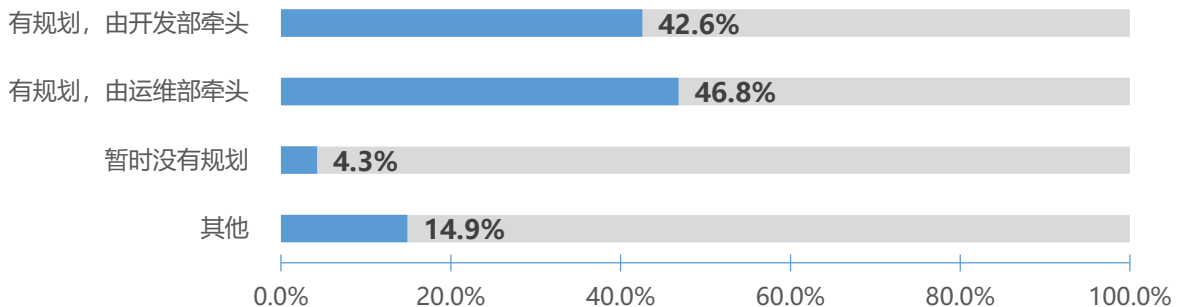
数据来源：《金融电子化》杂志社，2022 年 11 月

46.8% 的机构由运维部门牵头，解决运维的问题；42.6% 的机构由开发部门牵头，主要用来解决新业务研发问题。整体而言，接近 90% 的被调研机构都有容器云规划（见图 20）。

建设过程中，容器云的自研比例为 34.0%，外部合作为主为 64.0%，超过 40% 的银行容器云建设由研发部门牵头（见图 20、21）。

因为容器云技术比较复杂，需要强大的研发力量作为支撑，与外部厂商合作，可

图20 2022年银行业容器云建设部门调查

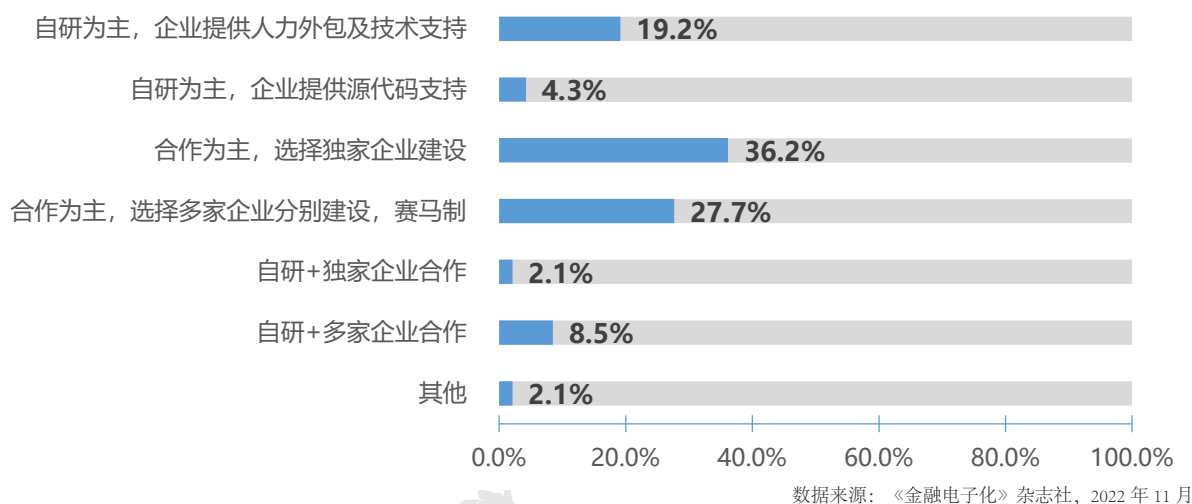


数据来源：《金融电子化》杂志社，2022 年 11 月

以很好地弥补内部研发能力的不足，所以超过半数的机构选择了外部合作为主。

容器云应用时间较短，服务提供商呈现多种类型。在参与本次调研的机构中，容器云外部支持厂商占比较高的 5 家中，既有布局私有云的公有云厂商阿里云、腾讯云，

图21 2022年银行业容器建设思路调查



也有综合 IT 服务提供商华为云，还有独立的容器云服务提供商博云、灵雀云。此外，还有一部分私有云服务提供商提供容器云服务，并占据一部分市场份额。

二、容器云建设过程中的考虑因素

1. 系统自动发布能力是最受关注的技术价值

与私有云相比，容器云建设时间较短，成熟度较低，又叠加信创需求，以及业务需求的深度绑定，需要解决的问题较多，因此技术价值关注程度普遍较高。

一方面，需要支撑敏态业务创新，因此“系统自动发布能力，支持灰度、蓝绿和金丝雀发布”达到 93.6%；“部署灵活性，支持云上、裸金属新部署以及纳管存量容器云”达到 76.6%；另一方面，需要与建成的云平台统一管理，保障业务连续性，所以，其中“平滑升级能力，便于大规模部署，保障业务连续性”占比最高，达到 91.5%。

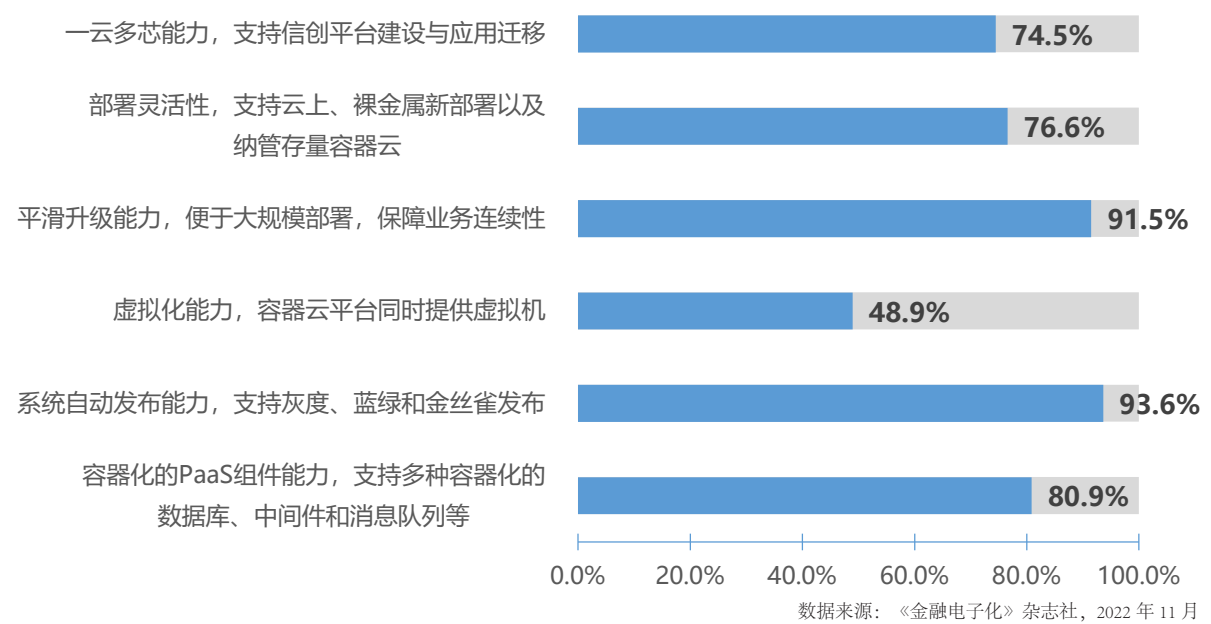
“容器化的 PaaS 组件能力，支持多种容器化的数据库、中间件和消息队列等”为 80.9%；此外，为满足信创要求而必须考虑的“‘一云多芯’能力，支持信创平台建设与应用迁移”能力关注度为 74.5%。关注度最低的“虚拟化能力，容器云平台同时提供虚拟机”项目是 48.9%，部分机构选择了稳态业务使用虚拟化或传统 IT，敏态

业务使用容器云，一定程度上规避了这个问题（见图 22）。

2. DevOps 能力是容器云最受关注的管理价值

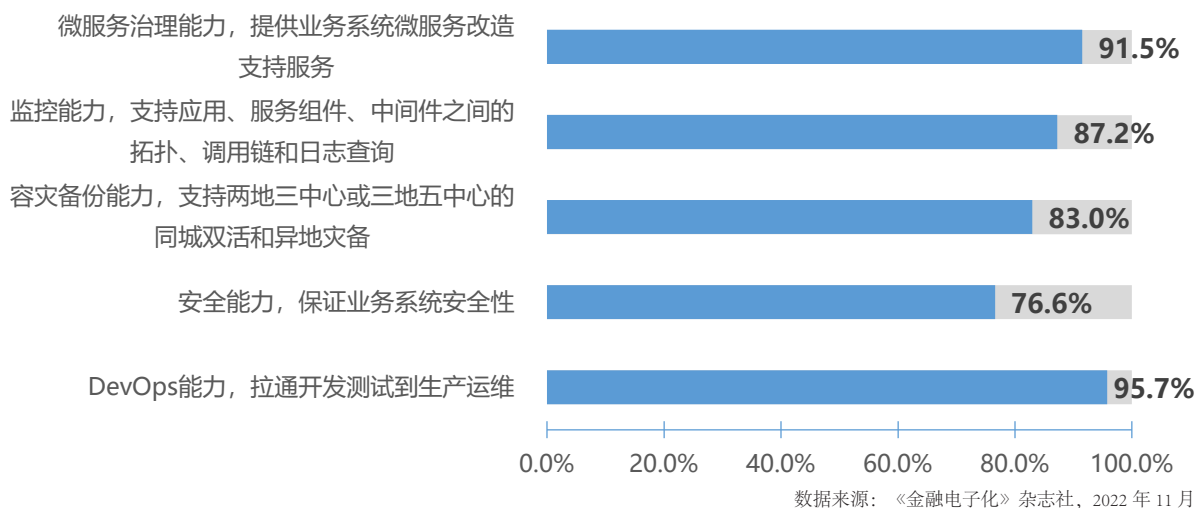
与技术价值类似，容器云建设的管理价值也受到了全面关注。“DevOps 能力，拉通开发测试到生产运维”最高，达到 95.7%，研发或者运维部门高度关注；微服务实现应用层由中心化向分布式演进，“微服务治理能力，提供业务系统微服务改造支持服务”为 91.5%；“监控能力，支持应用、服务组件、中间件之间的拓扑、调用链和日

图22 银行业容器云建设的技术价值调查



志查询”达 87.2%；“容灾备份能力，支持两地三中心或三地五中心的同城双活和异地灾备”达 83.0%；“安全能力，保证业务系统安全性”达到 76.6%。安全稳定始终是银行 IT 中需要考虑的重点问题，在容器云建设中，容灾备份和业务安全关注度与其他项目相比较低，是因为目前容器云在核心业务上使用较少。随着更多核心业务构建在容器云上，对于安全的关注将会提升（见图 23）。

图23 银行业容器云建设的管理价值调查



3. 一体化能力是容器云最受关注的使用价值

被调研机构在容器云使用过程中，关心的价值集中在统一性方面，“一体化功能，实现容器、DevOps 和微服务治理统一管理”得分 5.02；“云平台 and 容器云平台的整合，云和容器统一编排调度”得分 4.68；“容器云运维监控功能，实现自动化运维、统一大屏展示”得分 4.4；“容器安全性，支持基于容器的安全沙箱”得分 3.6（见图 24）。容器云根植于云，且统一软件交付和运维模式，因此统一管理不仅是向云平台兼容的需求，也与自动化运维、微服务治理相关。从建设进程来看，虽然容器云建设完成但彼此割裂，因此需要统一的控制层面进行统一编排、统一租户管理和授权，统一的软件定义网络，统一的监控及运维体系。

图 24 银行业容器云建设的应用价值调查

银行业容器云建设的应用价值调查	平均综合得分
一体化功能，实现容器、DevOps 和微服务治理统一管理	5.02
云平台 and 容器云平台的整合，云和容器统一编排调度	4.68
容器云运维监控功能，实现自动化运维、统一大屏展示	4.4
容器安全性，支持基于容器的安全沙箱	3.6
CI/CD 的灵活性，可灵活定义基于多种开发语言的应用打包和发布	3.45
基础设施的云原生，提供面向微服务应用的云原生产品	2.96
SDN 能力：平台提供软 SDN 能力，可以为 Run-C 容器、安全容器、云原生虚拟化提供统一组网	1.66

数据来源：《金融电子化》杂志社，2022 年 11 月

第五章 银行业机构的期待与展望

随着云计算技术的逐渐成熟，国家有关部门高度重视并积极引导，云计算成为金融科技新技术的支撑平台，得到广泛应用。在未来的一段时间内，银行业将继续推进云计算建设，特别是信创云将迎来黄金发展阶段。参与调研的 129 家银行业金融机构对 2022 年的云建设持乐观心态并充满期待，同时围绕金融行业云计算标准等提出了未来建设思路和规划。

一、现状与期待

1. 加快完善云计算相关指引或标准

各机构结合应用实践，对制定相关标准提出了一些希望，其中包括：明确公有云在生态场景业务中的使用标准；研究发布关于混合云的标准和政策；形成接入多云纳管平台的统一标准，能兼容主流厂商各种主流配置的资源（包括存储、服务器、网络设备）；建立云服务管理成熟度评价模型以及信创云服务性能评价模型相关标准。

信创云建设方面，中小银行机构希望监管部门能够提供信创云的建设标准和指导意见，完善云计算平台的安全、监控、运维、容灾体系。

大型银行希望参与云原生技术如容器、分布式服务、数据库、智能化运维等相关指引或标准的编写。

2. 逐步建立云管平台，实现多云管理

随着各机构混合多云的建设和发展，多云管理成为关注焦点。建立完善的云管平台，实现多云统管，实现交付运维自动化是私有云建设的重要工作。

此外，在传统业务上建设云管理平台，实现传统业务上云；基于不同芯片 X86、ARM 所构建云的完全统一化管理也被多次提及。

希望进一步规范私有云产品硬件兼容性和多云协同管理，避免被云计算软件服务商过度绑定硬件产品。

3. 实现非信创云向信创云平滑过渡

多云架构下非信创云与信创云如何平滑过渡也是本次调研的热词。做好信创云与非信创云的适配对接，实现应用的平滑迁移是大家关注的焦点。

4. 大力提升云安全管理的多维保障

在私有云建设过程中，安全是基础，建设高可靠、高可用和高安全的私有云平台是银行机构努力的目标。云计算因其多租户、泛在网络访问、快速弹性伸缩等特点，对边界安全、应用安全、数据安全等金融安全层次提出了更高的要求。被调研机构普遍认为，应从平台、主机、资源、应用、代码、容器、中间件以及租户的数据等层面进行安全管理；建议通过云安全解决方案，建立网络信息安全保护体系；同时，加强优化访问控制机制、用户权限管理以及安全审计能力。

当前，金融云安全是各银行机构关注的重点。云上的业务数据和网络安全均须满足监管的要求。

信创云方面，以安全可靠国产软硬件为基础，构建关键信息基础设施，提升关键信息基础设施自主可控能力，是目前的工作重点；完善“一云多芯”架构是各机构关心的热点。

5. 对科技企业的几点期望

在与科技企业的合作上，被调研机构提出了几点期望：

- (1) 云厂商能够提供兼容性更好的信创方案；
- (2) 云厂商能够更多地提供云内底层技术，提高系统上云的可靠性和稳定性；
- (3) 云服务商能协助使用者加强云计算方面的技术培训；
- (4) 云平台技术更加成熟稳定、易用性强、生态建设更加完善，便于自主可控；
- (5) 推动云产业与信创工作融合，提升主流云平台“一云多芯”的支持范围。

二、未来建设思路与规划

1. 加强 IT 基础设施标准化建设

近年来，标准在深化金融改革中的基础性、引领性作用日益增强。调研中，多数

机构把提高标准化建设水平作为云计算建设的未来工作重点。

总体上看，这些标准化工作建设和规划思路集中在以下四个方面：一是践行云原生基础资源扩缩容必备的“不可变基础设施”理念，采用 IaC（基础设施即代码）技术与各类镜像形成一体化管理，为应用所需的基础资源提供快速精准的生产能力，提高云平台的资源供给质量与效率；二是提升基础资源体层的融合，提升云平台组件兼容性，逐步建立规范化云计算运维服务体系，加强资源管理水平，逐步完善云计算安全技术管控手段和规范，提升运维效率；三是依靠云技术提升规范化、标准化能力，从而提高自动化能力，逐步达成对外提供 IT 服务的目标；四是加快云计算技术规范应用，稳妥推进信息系统向多节点并行运行、数据分布存储、动态链路负载的分布式架构转型。

在当前数字化转型的大趋势下，随着金融科技快速发展，金融数字化转型向更深层次推进，场景化、个性化、智能化的高效金融服务不断涌现。与此同时，数字化时代所具有的开放性和互动性，使得金融领域更容易产生业务、技术、数据、网络等多重风险的叠加，加强 IT 基础设施的标准化建设变得尤为紧迫和重要。

2. 提升云计算自主可控能力

云计算作为数字化转型的基础底座，需要自主可控。

部分机构计划并希望，未来建设“一云多芯”的云计算平台，提供自主可控的算力能力；逐步加大自研力量，消化吸收业界成熟的云底座，打造符合自身需求的云平台；在完善自身云计算能力的同时，将信创工作与云的建设有机结合起来，形成具有自身特色的云计算技术路线，逐步形成对分布式架构的自主开发设计和独立升级能力。

部分机构建议，云计算应坚持关键技术自主可控原则，对业务经营发展有重大影响的关键平台、关键组件以及关键信息基础设施，要避免单一来源、降低外部依赖。大力发展和建设信创云，从平台、主机、资源、应用、代码等各个层面进行安全策略管理，切实保障自主可控基础体系建设的供应链安全。

3. 有条不紊分步建设云平台

在云计算平台实施和建设上，被调研机构普遍都是按照统一规划、分步实施、持续改进的原则，业务上先简后繁，技术上先易后难，持续推进分布式架构转型。

大中型银行的做法，先是持续建设总行云和分行云，再是规划建设场景生态云；或者先推动基础设施池化、云化，再推动应用上云，提升应用敏捷性，最后是推动信

创的使用。

具体来说：第一步，全面提高云服务质量和体验，提升主动服务意识，分场景做好基础设施支撑能力；第二步，加强架构规划和执行，制定云技术平台演进路线，构建统一云技术服务目录，试点多云管理架构；第三步，持续优化流程、制度、安全、组织配套体系，推动云技术架构实施，保障云服务高效、稳定运行。

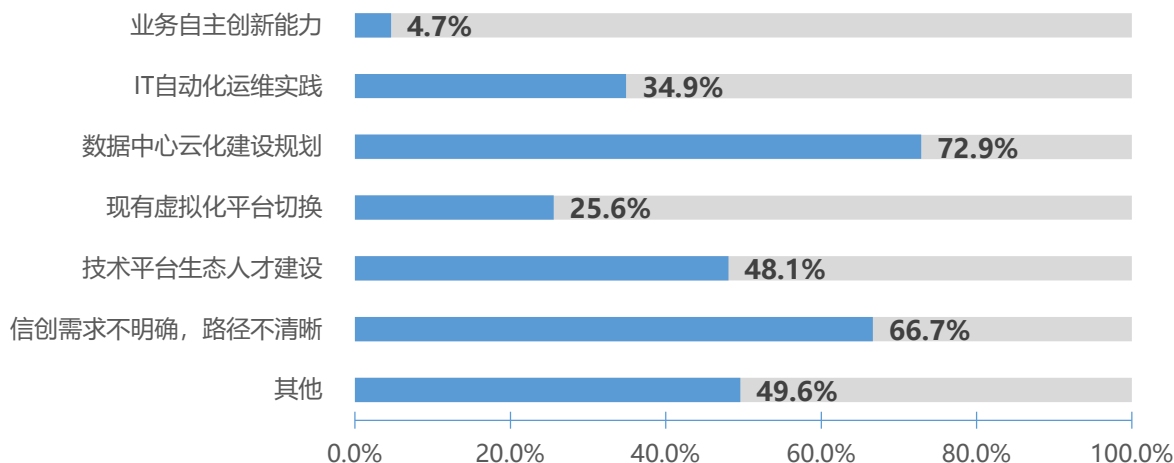
对于区域银行机构而言，总体思路是，搭建信创云、同城灾备云、异地灾备云，推动新老应用上云。具体做法是，第一步，推动数据中心全面云化，建立云化的两地三中心架构，建设云的运维支撑体系，包含自服务、自动化、智能运维等；第二步，推动应用上云，包含推动应用云原生建设及上云，推动云就绪应用迁移上云，助力服务能力提升；第三步，推动分布式技术与云的结合，如分布式数据库等；第四步，推动数据中心网络架构适配改造，推广 SDN、SD-WAN 等技术应用，与云平台形成技术联动；第五步，围绕云平台建设配套开发平台，包含 aPaaS、iPaaS 平台。

4. 加大金融科技人才培养力度

人才是企业发展的最重要的战略资源，做好金融科技人才培养，建设高水平金融科技人才高地，提升金融科技从业人员的能力和水平，已成为行业共识。

调研中我们发现，IT 技术面临的主要挑战由人才培养、技术能力两方面组成，其

图25 银行业当前面临的IT技术挑战调查



数据来源：《金融电子化》杂志社，2022年11月

中人才建设挑战最多，“技术平台生态人才建设”占比 72.9%，“数据中心云化规划建设”占比 48.1%，技术能力相关项目的“IT 自动化运维实践”占比 66.7%，“业务自主创新能力”占比 49.6%。此外，由于“信创需求不明确，实施路径不清晰”带来的挑战占 34.9%（见图 25）。人才挑战与云技术更迭快相关，特别是行业应用人才结构相对薄弱，需要既懂行业业务流程，也要对云计算有相当的认识，能够帮助银行实现“业务上云”的咨询引导。在技术上，云化程度加深，对运维管理的要求进一步提升，这也是容器相关技术得到快速应用的重要推动因素。

第六章 银行业云计算实践案例

邮储银行“金融云平台数字底座”建设

中国邮政储蓄银行数据中心

长期以来，以云基础设施、大数据、区块链、人工智能、物联网技术为代表的前沿科技，在金融机构战略布局中的比重不断增加。另一方面，复杂多变的国际局势对国家关键基础设施的技术创新化进程提出了新的要求。

在习近平总书记“必须坚持科技是第一生产力、创新是第一动力”的要求下，邮储银行锚定“数字化”和“创新化”，坚持两手抓，两手都要硬，始终把金融科技创新放在全行战略高度，以超大规模金融云底座为重点，加快基础设施能力的优化迭代和技术创新合规建设步伐，支撑邮储银行业务系统广泛落地，持续发力走出一条服务科技自立自强的金融特色发展之路，以金融科技的活水浇筑科技自立自强新高地。

邮储银行金融云数字底座建设挑战

邮储银行金融云建设项目是一个包含技术维度、管理维度、政策维度等多维度视角的复杂且重要的系统工程，在建设过程中，面临以下挑战。

1. 产业侧整体解决方案不充分、集成能力欠缺、建设标准不完善。作为复杂且重要的系统工程，邮储银行金融云平台建设并不适用传统基础软件的产品化建设思路，尤其是在叠加技术创新因素的情况下，大多数的传统集成商也缺乏技术创新金融云的建设经验，同时建设过程中缺乏统一的标准和方法论来提供端到端的建设指导以及建

成后的运维标准。所以需要单独的责任部门专注于在顶层设计、产品选型、系统集成、适配验证、建设落地和运维保障等方面持续优化建设模式、固化相关标准并提供流程保障。

2. 软硬件多路线选型、深度适配和差异屏蔽。金融业对信息技术的功能完备性、处理性能、数据一致性、安全稳定性等要求极高，当前邮储银行硬件层面具备多品牌服务器、网络设备和存储设备，操作系统、中间件、数据库等基础软件也存在各自搭配后的生态兼容以及性能优化的需求。叠加技术创新因素，更是给全面支撑邮储银行数字化转型和深度满足技术创新化合规带来了巨大挑战。

3. 以基础设施服务多样性支撑业务广泛迁移上云的挑战。金融云致力于全面支撑邮储银行业务系统，各类系统对于计算、存储、网络服务的 SLA 要求不尽相同。同时，技术创新建设也面对 OA、一般应用、重要应用在内的多个迁移目标，传统的信息系统迁移到 ARM 技术创新架构难度普遍较大，且行内应用系统种类多数量大，窗口短，追求平滑的要求也给金融云建设带来的挑战。

4. 同业数据中心云平台建设和运维困难。管理碎片化指同业机构多年来分阶段按照使用场景建设多套并存、版本不一、CPU 架构不一的异构云资源池，每个云资源池管理界面、管理手段均不同，带来管理成本上升的问题。同时，由于每类云资源池技术实现不尽相同，带来了运维复杂度提升和运维经验难以统一和沉淀的问题，造成运维困难。

5. 超大规模部署情况下的稳定支撑。对于邮储银行来说，云平台底座作为基础架构集约化建设的重要技术手段，建设目标是面向超大规模落地的场景，要求同样适用于技术创新云平台建设阶段，所以相较于传统架构平台，金融云平台面临规模化后支撑能力持续优化的挑战。

6. 云平台功能无法平滑升级。参考目前金融行业多数机构基础架构云平台建成之后的使用体验，很多同业机构基础架构云建设存在建设即落后的问题，主要表现在大多数金融云提供的功能及能力较固化，平台架构不先进且僵化，不具有持续进化能力等。

7. 技术创新云建设的安全合规。金融行业是安全监管的重点行业，等保合规是业务安全性的重要衡量指标。金融云安全体系建设需要满足最新的网络安全等级保护 2.0 三级要求以及网络安全审查办法的要求，贯彻和落实国家对于金融监管要求成为重中

之重。

邮储银行金融云建设方案

鉴于以上建设挑战和相关需求，邮储银行结合本行实际情况，与易捷行云 EasyStack、华为云等厂商合作，逐步建成了标准化、中立化、多样化、一体化、规模化、可进化的邮储银行金融云。

1. 标准化：实现标准化的金融云建设、运维和安全体系。邮储银行金融云相关工作依据国家及金融业监管相关标准，制定并持续完善符合自身特点与云建设发展方向的标准体系，包含总体标准、技术类标准、服务类标准、安全类标准、管理类标准等 10 个以上的标准规范，指导金融云平台的建设和运维实践。同时，遵循监管机构对金融领域云计算技术应用的安全技术要求，有效防范云平台风险，推进云平台安全资源管理与运维管理工作，并进行云平台安全架构的定期评估与持续改进。

2. 中立化：中立开放与多元适配的兼得之道。考虑金融行业安全可信、监管合规要求，结合多技术路线并存的现状，邮储金融云选择了“兼容并包”“兼而有之”的适配和部署模式，屏蔽底层差异，满足多路线资源兼容，支持在云平台内，以“一云多芯”融合飞腾、鲲鹏等国芯，通过金融云平台在异构资源池之上构建资源统一编排与管理层，对异构资源做抽象设计，实现跨地域、异构资源的统一管理，并实现对于不同类型的解析、编排、调度和自动化部署等功能。

3. 多样化：以多样性服务实现邮储银行大量生产业务系统完整支撑。作为重要的数字化转型基石，云平台须具备云主机、裸金属、容器等融合基础设施资源，同时能够提供块存储、对象存储和文件存储等多种存储服务，兼容集中式存储和分布式存储形态。在实践过程中，针对不同业务系统的资源和性能要求，固化了多样性的模板规格，以稳定支撑为前提兼顾利用率率的提升。

在 PaaS 层面，邮储银行也逐步基于云原生架构提供 Redis、PostgreSQL 等软件基础设施服务，并深度适配上百种开源或商业化软件，深化治理的同时加快业务系统上线速度，固化服务获取流程和相关操作，实现 IaaS+PaaS 融合的全栈金融云的稳固落地。

4. 一体化：统一计算资源、统一 SDN 服务、统一管理的金融云。考虑到应用系

统广泛迁移上云的最终诉求，云平台在中立化的基础上，还需要具备同时提供融合计算实例（云主机、裸金属主机、容器）的能力，以支撑不同业务负载。通过数字原生操作系统管理云主机、容器和裸金属并纳入到一个平台，提供云原生语义的统一管理。同时，采用大规模软件定义网络的方案，实现所有资源的 4 ~ 7 层网络统一自动化部署，提速增效。在资源池之上，采用云管理平台，实现传统云资源池和技术创新云资源池的统一管理，其中技术创新云资源池又兼顾飞腾和鲲鹏多路线的生态要求，拉齐服务能力，降低运维难度。

5. 规模化：超大规模技术创新金融云建设实践。邮储银行金融云平台建设重点解决了大规模部署的难题，在丰台、廊坊、合肥、石家庄多地多中心联合构建大规模金融云平台。从业务规模看，自 2014 年第一个上云的电子渠道业务开始，邮储银行已将信贷平台等核心业务系统、互联网网贷系统、手机银行等数百个关键应用迁移到云平台，应用规模和交易量处于同业领先水平。截至 2022 年 9 月，手机银行、网上银行、移动展业等 201 个系统实现私有云平台部署，云平台日交易量达到 5.89 亿笔，占交易总量的 93%，云技术应用继续保持同业领先水平。从建设规模看，物理节点 1.6 万余台，虚拟机数量大于 8 万台，总 VCPU 算力资源超过 300 万，已经成为国内规模最大的基于技术创新路线的金融生产云之一。

2021 年底完成技术创新云资源池投产工作，并逐步将相关应用迁移到该资源池，支撑邮储银行技术改造业务应用平稳运行。当前技术创新云资源池涵盖异构 ARM 资源池路线，可以支持单集群超过 2000+ 服务器的超大规模，同时也可以根据不同云资源池控制层面部署满足灵活的部署规模需求，覆盖从日常管理类、经营分析类、互联网金融类应用业务，如新一代手机银行、渠道管理平台等数十个的生产业务系统，具备极强的兼容性和可升级能力。

6. 可进化：云平台具备可升级可进化能力。为解决同业广泛存在的建设和管理碎片化、服务能力僵化的问题，邮储银行云平台基于先进的架构设计和工程实践，通过数字原生引擎具备可进化、可升级能力。同时，云平台与云服务分离、全栈全平面全场景编排、全栈云架构支撑行业场景化、云开放平台激活云生态等核心特性为邮储银行提供稳定可靠的 IaaS 云能力，以及可灵活扩展的 PaaS 云能力，成为邮储银行业务创新的沃土。

招商银行 ACS 原生云建设

招商银行信息技术部

一直以来，招商银行始终坚持科技兴行的战略布局，时刻关注科技带来的压力与机会，并主动将其转变为变革的动力。2017 年，招商银行进一步提出“金融科技银行”的战略定位，不断加大运用金融科技手段力度，“以科技敏捷带动业务敏捷”，打造最佳客户体验银行。与此同时，云计算作为 IT 新技术，经历了从概念到标准、从云平台到云原生的进化之旅。在此 IT 变革风起云涌之时，招商银行审时度势，立足未来发展和战略规划，开启了银行的云原生之路。通过云平台和云原生，对传统银行 IT 能力全面重构，构建云计算基础设施，打造符合云原生架构的云服务，支持招商银行在数字化时代快速创新。

2015 年，基于当时公有云发展势头以及招行未来基础设施发展的需要，招商银行对 AWS、微软等云计算先锋公司进行实地考察，了解其在云业务和技术等方面的发展情况。本次考察让招商银行深刻体会到云在新的 IT 变革中的决定性力量，也确定了招商银行发展“云原生”的技术方向。随着 2015 年 6 月第一个 PaaS 平台 PCF(Pivotal Cloud Foundry) 的落地，招商银行正式启动了原生云落地实施的征程。

招商银行原生云建设总体经历了三个阶段。第一个阶段是 PaaS 探索阶段。2015 年 6 月，招商银行基于 PCF(Pivotal Cloud Foundry) 技术，推出行业领先的 PaaS 平台。该平台显著提升了应用的开发、部署和维护的效率，提升了招商银行建设云和管理云的水平，也为招商银行向云原生转型积累了宝贵的经验，为后续的云建设打下了坚实的基础。第二阶段为全栈云阶段。2017 年，招商银行启动 ACS (Advanced Cloud Service) 原生云项目，建设全栈私有云，陆续交付了具备原生云特性的多个可用区，首次在行业内大规模运用新一代存算分离、SDN、NFV 等技术，构建“因云而生”的可靠、

安全、稳定的云计算底座。在此底座的基础上逐步建设基于 K8S+ 容器技术的 PaaS 平台，提供了多种云原生服务。第三阶段是双栈云阶段。2022 年随着原生云信创区正式投产，招商银行进入通用区 + 信创区双栈运行的 ACS 3.0 新模式。该模式向下统一纳管 X86 和信创两个技术栈资源，向上为开发人员提供透明的可混合部署的云计算底座和云原生服务，标志着招商银行已具备在信创基础上持续发展原生云的能力。

招商银行原生云平台建设的成功，离不开前瞻性的规划和科学的管理。建设初期，招商银行是否要建私有云？按照什么方式构建什么样的私有云？目标和愿景是什么？这是我们首先要思考的问题。在深入分析传统虚拟化技术的不足和弊端，并研究参考 AWS、Azure 几家公有云的成功案例后，我们对云计算的发展趋势做出了方向性的研判，对标领先的公有云，建设全球先进的私有云，作为招商银行原生云的建设目标。秉承“以用户为中心”的理念，以云原生场景驱动组织、流程和技术转型，努力寻求云的技术原生化和云底座高可用之间的平衡。建设过程中，我们希望招商银行原生云能够呈现以下五方面的价值。

一是有利于业务安全稳定运行。原生云将 IT 组件服务化，针对每个云服务在基础设施的区域、可用区、服务器集群、可用性集等多领域多层次建立多活、故障隔离和恢复等措施，为云时代银行业务的安全稳定提供了保障。

二是有利于应用敏捷交付。采用分布式技术，原生云平台纳管资源的能力相比传统架构获得飞跃式提升，资源即时交付，且其容量和性能具备弹性伸缩特性，充分满足了互联网时代对应用资源的“大”和“快”的需求。

三是有利于业务快速创新。原生云大力开发和推广用户所需的各类云服务并以可调用 API 交付，业务和开发人员不再关注依赖基础组件的搭建而专注于构建业务本身，并在应用层面反向促进了云服务能力的提升并加速其共享过程，从而显著提升了开发效能，推动了组织层面的创新发展。

四是有利于成本效益提升。原生云对所有资源统一纳管，同时可对资源池进行个性化管理配置，从而实现资源的灵活调配，提升资源池使用率。同时配套建立了云计量计费体系和资源治理体系，通过成本的数字化、可视化，驱动整体 IT 基础设施成本优化，让降本增效进入可持续管理的通道。

五是有利于用户体验提升。贯彻“以用户为中心”的理念，原生云平台建立了配

套的运营、运维组织及流程，并将流程通过云管平台落地，通过提升客户相关指标的数字化运营机制，持续提升用户管云用云体验。

在五个“有利于”的建设理念指导下，经过多年演进，招商银行原生云形成了深圳南山、深圳平湖和上海张江的 3 个区域、共 11 个可用区的云计算基础设施，物理服务器规模已经接近 2 万台，包含自主开发的云服务超过 60 种，服务器 CPU 整体负载 20%，云存储规模超过 80P，是目前最大的私有云之一。招商银行原生云采用分层架构，各层相互解耦，又通过云管平台和云运维平台进行串联，相互协同，支撑招商银行总分行和子公司的大部分业务。



▲ 图 招商银行 ACS 原生云技术架构

在基础设施方面，招商银行原生云采用统一大资源池规划，避免传统虚拟化分割多个小资源池造成的资源割裂，实现资源的高效利用和应用的灵活调配；实现“一云多芯”，信创区与通用区互补，实现原生云双栈架构；实现存储和计算分离架构，具备计算和存储的资源灵活配比能力，既提高了存储和计算的鲁棒性，又增强了维护的便利性；基于 CLOS 网络架构，实现了网络全交换无阻塞能力，为国内银行业内首家部署。在 PaaS 平台方面，基于 Kubernetes 的能力，提供一站式的面向开发人员的容器应用管理统一平台。容器平台对 Kubernetes 的复杂性进行了封装，支持业务应用的快速部署，提供跨可用区的高可用，横向纵向弹性能力，以及微服务治理和应用生命周期管理。在云服务方面，目前以用户自服务的方式提供了超过 60 种常用的云服务，IaaS、数据库、大数据、中间件、安全等 12 大类服务，覆盖了业务系统开发的大部分需求。在云管平

台方面，100% 自主可控，实现云服务模块的产品级解耦，为原生云的持续迭代升级和混合云对接创造了条件。在云运维运营方面，以可靠、高效、易用、成本优化为目标，建立以 SLO 为核心的服务质量等级体系，打造基于 IaC（基础设施即代码）的分钟级交付能力。建立常态的数字化运营机制，通过数字化手段，挖掘改进点，持续提升云管平台用户体验，涵盖云服务、权限管理、规范化使用等多个领域。

云平台背负着为招商银行打造面向未来科技新基建底座的使命，一个先进、坚实的云平台是全面上云的根基所在，根基牢固，才能顺利完成云架构转型，实现对业务创新快速响应的美好愿景。招商银行根据自身技术能力、业务规划和业界技术趋势，制定了 3 年总分行系统全面上云的总体规划、路线图和北极星指标。银行的应用系统上云，面临着业务体量庞大，系统多且复杂，参与人员众多等各种挑战。招商银行在组织上多管齐下，协同推进，成立上云项目组，下设总行、分行、信用卡中心、子公司四个片区，采用片区分层管理、密切协同、扁平支持的工作机制推进整体项目。项目组通过专题培训宣讲、技术开放日等各种手段为上云队伍赋能，提振信心。在上云进入深水区阶段，云网络 SDN 性能、云存储稳定性、资源交付效率、云服务和云底座运行质量等平台基础组件部分都不同程度暴露出问题，上云计划与平台升级扩容计划、流量切换和灰度升级的工期也屡屡出现矛盾和冲突，招商银行上云项目组通过技术攻关、总体协调等措施逐一解决了问题，最终成功支持了应用平稳全面上云。三年内，招商银行总分行及子公司科技同事紧密协同，力出一孔，2022 年底实现了总分行及子公司近 4 万个业务应用上云，承载了约 30 余万个容器实例和 10 万多个虚拟机的稳定运行、每日承载请求量超过 1000 亿次。

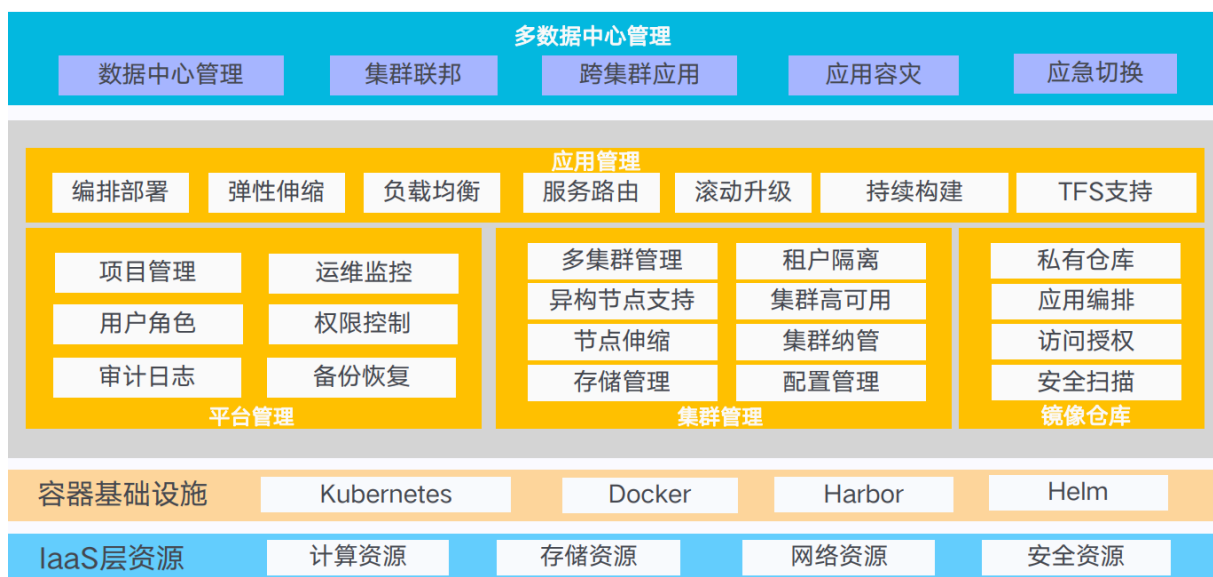
如今，招商银行原生云平台已全面实现 On Cloud，成为招商银行应用开发运行的主力平台，通过提供应用平稳运行、资源海量管理、容量弹性敏捷、服务解耦复用、用户高效运营、资源治理提效等功能，体现了一个真正的云平台在云时代能够发挥的作用。下一步，招商银行信息技术部将继续全面推进设计态、开发态、运行态的云原生架构转型工作，实现用好云、用省云，完成 In Cloud 的目标，为招商银行科技升级和数字化转型注入更强动力。

北京银行容器云建设规划

北京银行系统运营中心

北京银行自研的容器云平台作为我行整体 IT 规划和数字化转型中的一环，于 2021 年 5 月底投产，已承载 90 余个容器化业务应用系统，其中包括一部分核心和重要的业务系统，支持了关键业务系统的同城双活和异地灾备的等保要求。容器云平台很好地符合我行的 IT 规划路线，在顺应数字化和云原生演进大趋势、配合支撑微服务应用落地、提供云原生基础设施新特性、降本增效等方面带来了显著的变化和新的价值。

后续，北京银行将进一步扩大、深化容器云平台的规模和能力，持续进行云原生、微服务、DevSecOps 等技术方面的演进，提升容器云平台的服务化能力、弹性能力、可观测性、韧性能力和自动化能力。

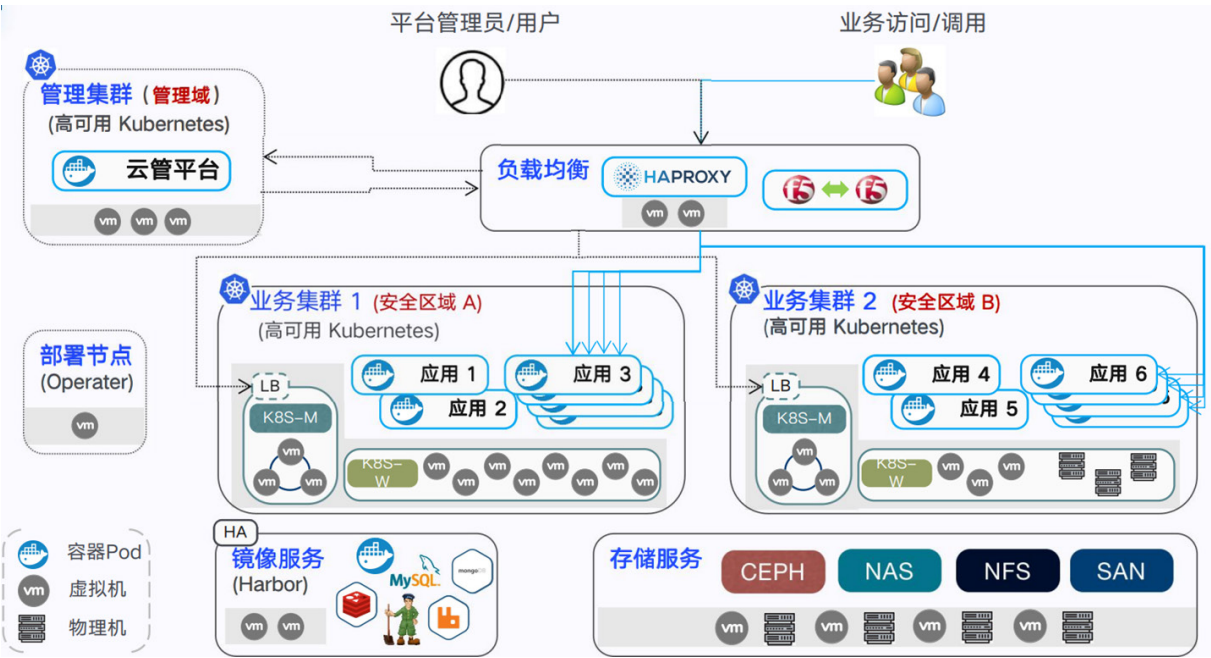


▲ 图 1 容器云功能架构

总体设计

北京银行容器云平台是一个大规模容器集群管理平台，包括：提供容器所需的高可用集群、资源池管理、网络通信方案、存储方案、编排调度引擎、微服务运行框架、镜像管理、事件告警、集群监控和日志收集等。最终设计容器云功能架构如图 1 所示。

北京银行容器云平台具备 PaaS 平台能力，为开发人员提供了构建应用程序的环境，加快应用开发速度，实现平台即服务。在现有 IaaS 平台虚拟化层基础上部署容器云平台，实现底层资源灵活调配的目的，使用 Docker 和 Kubernetes 实现核心的 PaaS 平台容器技术，使用 HAProxy 和 F5 负载均衡设备实现业务访问高可用，使用 Harbor 和制品库作为镜像仓库。其实现架构如图 2 所示。



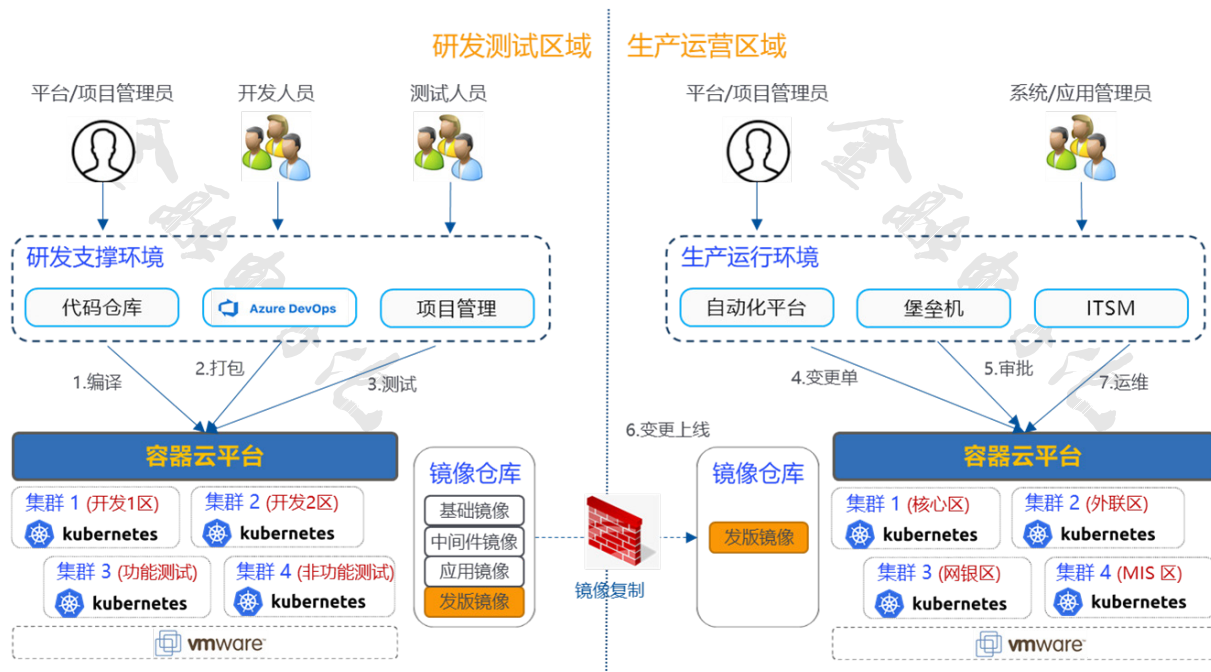
▲ 图 2 容器云平台实现架构

PaaS 平台是通过提高基础设施的敏捷而加快业务的敏捷，与此同时，DevOps 则是在流程交付上加快业务的敏捷，通过 DevOps 可以实现应用的持续集成、持续交付，加快价值流交付，实现业务的快速迭代。具体架构如图 3 所示。

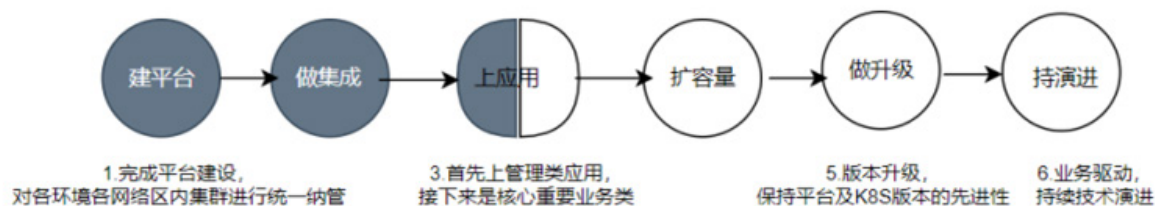
建设路径

北京银行容器云平台整体上采用了分期建设的策略（如图 4 所示）。目前处于三期的中后期，全面应用上容器云的阶段，每期周期约为一年。

一期的主要建设内容是容器云平台自主设计开发，建设技术团队基于我行现状设计



▲ 图3 容器云平台具体架构



▲ 图4 容器云平台建设路径

实现大规模容器集群管理平台。

二期主要工作内容包括运营体系 ITIL，CMDB 等系统对接开发，IPV4/V6 双栈网络基础设施对接开发，NAS 存储对接开发，自动化管理及运维方案研发，多中心、多活方案建设和容器化运营能力建设。

三期主要建设围绕进一步扩大应用上云、深化容器云平台的规模和能力，持续进行云原生、微服务、DevSecOps 等技术方面的演进，提升容器云平台的服务化能力、弹性能力、可观测性、韧性能力、自动化能力。同时为对现有容器云平台进行统一国产化规划、统一设计、逐步改造，产品层面上以国芯国操为基本盘，不断推进国产数据库、国产中间件的使用，完善信创生态环境。

三期建设的具体信息如下：

1. 微服务管理。应用管理员负责运行基于容器镜像的轻量级应用或微服务，提供

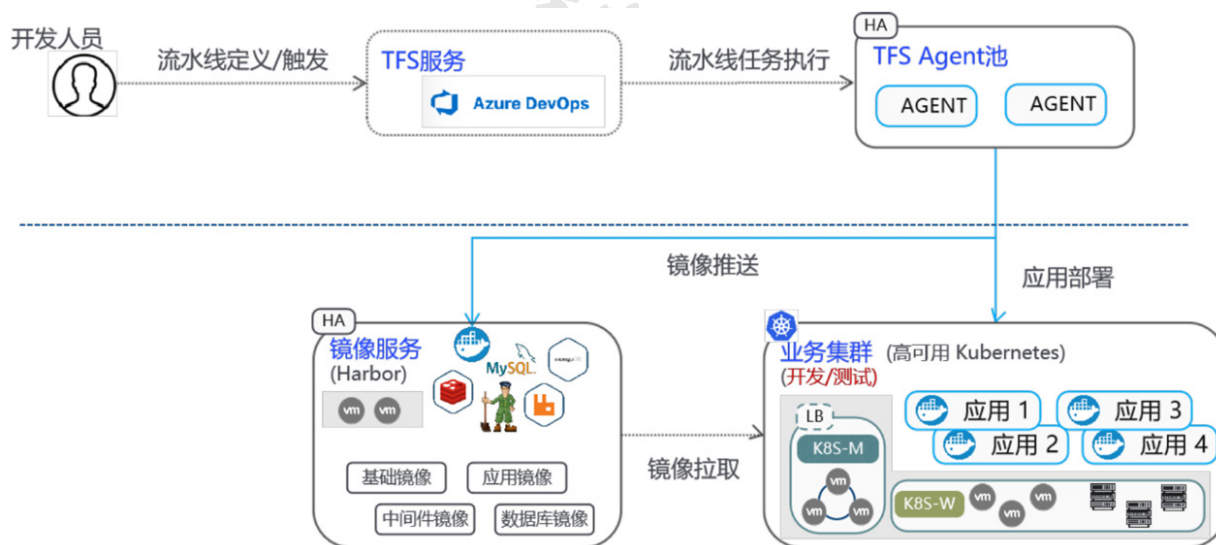
应用的微服务编排能力、应用全生命周期管理。

(1) 应用编排。微服务和容器化给复杂应用部署与管理带来了极大的挑战。而应用编排的目的是为了给容器平台上运行的应用进行建模标准化，描述应用运行的资源需求、部署模式、部署参数、运行时动态规则（弹性伸缩、故障迁移等）。北京银行主要采用 Kubernetes 的 yaml 文件、Helm 等。

(2) 生命周期管理。应用程序的全生命周期管理包括：上架、部署、升级、下架、支持运行时动态管理策略、高可用及故障自愈等；容器云平台提供应用商店功能，多个应用可以通过编写 Chart 文件形式，发布到应用商店中，在应用商店中进行应用程序的一键部署、升级操作。为保障业务连续性，容器云平台通过 Deployment 控制器来管理无状态的应用 Pod，Deployment 为 Pod 和 ReplicaSet，提供了一个声明式定义（declarative）方法，用来替代以前的 Replication Controller 来方便的管理应用。

2.DevOps 建设。持续集成（CI：Continuous Integration）与持续交付（CD：Continuous Delivery）是软件开发和交付中的实践。图 5 为 CI/CD 流程图。

CI/CD 流程：第一步，编码并完成本地调试后提交代码至 Git；第二步，在 TFS 上



▲ 图 5 CI/CD 流程图

触发流水线 CI/CD 过程；第三步，TFS 调用构建代理执行编译、打包等任务；第四步，构建容器镜像并上传到仓库；第五步，将应用部署到指定的容器集群。

3. 安全管理。安全管理的难点在于涉及面广，包括基础设施资源层安全、容器管理调度层安全、容器引擎安全、服务层安全、应用层安全以及镜像层安全。

(1) 基础设施资源层安全。基础设施资源层为容器云平台供给资源，除了裸金属基础设施的安全管理，还通过虚拟化层的隔离；与此同时，K8s 提供了一种网络策略，目前支持 Calico、Weave Net 等，网络策略说明一组 Pod 之间是如何被允许互相通信，以及如何与其他网络 Endpoint 进行通信。

(2) 容器管理调度层安全。容器管理调度层安全主要涉及容器调度、容器生命周期管理等。容器调度可以采用亲和性、反亲和性策略等，确保容器调度到合适的节点上。容器的任何操作可以通过 API 来实现，K8s 支持多种 API 安全访问策略，Node、ARAC、BRAC 等，提供授权、认证、准入机制。

(3) 容器引擎安全。容器引擎通过 Linux 系统安全策略来实现。Docker 支持 Namespace 隔离性，Cgroups 配额资源限制，Capability 权限划分，Selinux/AppArmor 访问控制权限。K8s 通过 API 可以实现 Namespace 隔离性、资源分配和资源限制。

(4) 服务层安全。服务层就是实现微服务，微服务的安全包含数据安全。微服务接口和通信安全也是重点，通常我们需要部署服务网关来实现对服务接口的管理和访问控制，服务接口也需要实现安全的通信机制，比如 SSL/TSL。

(5) 应用层安全。在同一租户下，实现应用等级隔离，运行不同安全等级的应用，因为容器共享系统内核的特点，应用也面临其他等级应用的资源争抢、故障影响等问题。另外，不同等级的应用，往往要求不同级别的运行环境高可用性、安全性，因此在同一租户下，也应该把不同等级的应用隔离开，分别部署到各自专属的资源池内。

(6) 镜像安全。容器服务镜像都基于基础镜像构建，基础镜像安全涉及镜像、系统、容器运行时三部分。系统安全方面面临系统补丁、升级的问题。所以选择合适的镜像仓库，为容器镜像安全保驾护航。北京银行容器云平台采用制品安全扫描 Xray 组件单独部署两台虚拟机，软件自身可实现 HA 高可用，与 Artifactory 结合使用。后端数据库使用 PostgreSQL，采用 Master-Slave 主从模式部署。

江苏农信夯实金融创新发展的云服务“数字底座”

江苏省农村信用社联合社信息科技部

田野“沃土”是金融服务的“热土”，江苏农信作为华东地区重要的省级农村金融机构，成为区域农村金融的主力军、地方金融的排头兵、普惠金融的领跑者。江苏农信积极利用新兴技术来实现省联社的科技金融转型，走一条“服务即管理”的全新路线。自 2017 年开始，江苏农信积极利用新兴技术来实现省联社科技金融转型，深入实施金融科技赋能乡村振兴示范工程，发展农村数字普惠金融，充分运用大数据、云计算、5G 等技术，提高金融机构客户识别和信贷投放能力。根据辖内农商行的需求迫切度、自身技术积累以及新兴技术的应用成熟度，选择云计算作为金融科技切入点。

基于开源路线的自主可控建设原动力

省联社作为扎根区域的本土金融机构，更在脱贫攻坚、践行普惠金融事业中，承担着不可或缺的角色。科技时代，创新为先，以云计算、人工智能、区块链等代表的金融科技知识引领金融业态不断变革，在 IT 基础设施管理层面，我们调研发现以下问题比较突出。

1. 提升资源使用效率，降低计算设备成本。历史过程中积累的大量中低端服务器，虽然采用了虚拟化技术，但缺乏统一的资源调度平台，无法灵活实施调度策略，设备投入、机房空间、电力浪费造成的严峻问题，急需云计算技术提升资源调度效率。

2. 改变存储方式，降低 IOE 设备成本。业务运营以小型机、大型机和集中式存储为主，运维成本较高。同时由于传统厂商的全线技术支持，导致自身技术团队参与 IT 创新机会较少，未能得到充分的培养和锻炼。需要符合信创政策的开源可控技术路线，在满足海量数据爆发态势同时，最大程度降低整体成本。

3. 提高运维效率,降低运维成本。随着全省农商行业务种类和业务规模的快速发展,全省的信息系统硬件数量出现急速增长,运维工作量直线上升,运维人员数量缺口不断加大,需要有效管理手段提升运维工作效率,降低人力成本。

4. 集约化建设与运营。在全省云平台规划的调研过程中,已有农商行提出希望将他们的基础 IT 环境迁移至省联社的共享云平台中。农商行普遍科技人员较少,但需要管理全行的 IT 资源,包括机房基础环境和设备、各类外设硬件、自建的应用系统等,工作对象复杂,工作压力较大。农商行期望通过将 IT 基础环境迁移至省联社的共享云平台,降低自身工作的复杂度和压力,而且使用省联社的共享云平台可以规避使用其他云平台的数据安全问题。

云计算自主探索建设关注点

1. 渐进式云平台建设历程与场景延伸。如图 1 所示,江苏农信云平台建设演进经历了 4 个阶段,不同阶段有各自的建设重点,从测试云、生产云、联社云、灾备云到信创云,云平台能力不断强化、一脉相承。最终建成具有江苏农信特色的“应用平台化、数据资产化、基础设施弹性化、信息安全体系化、IT 治理精细化”运营支撑服务体系。



▲ 图 1 江苏农信金融云平台演进历程

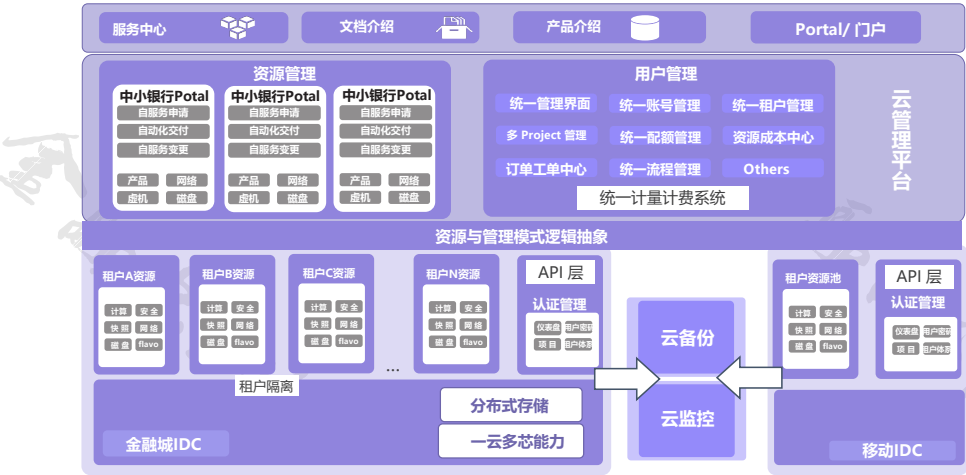
(1) 直击痛点,为辖区农商行做好服务。自 2017 年开始,江苏农信陆续建设测试云、生产云、联社云、灾备云、信创云等 14 朵云资源池,云主机数量近 2 万台,上云之路开展得如火如荼。当前行业云已经运行 50 多家农商行的 3300 余套应用系统,占业务系统的 80% 以上;私有云承载 70% 以上自有业务,包括手机银行、收单系统、微信银行、精准化营销、数字化风控平台等“三农”便捷系统。

(2) 从 IaaS 到 SaaS，云服务生态圈不断延伸。通过集约化建设，农商行享用了更多更便捷的底层资源服务，裸金属、云安全、签名验签等 IaaS 新功能不断增强；依托容器、API 平台、混合编排等技术，提供 PaaS 和 SaaS 的应用商店平台，为省联社、农商行、外部软件提供商的生态圈创造条件。

(3) 中立开放与自主可控的中和之道。由于金融行业安全可信、监管合规要求，江苏农信云计算应用模式选择了“以我为主”的私有云部署模式。云厂商的产品能力、开放能力和服务能力至关重要，如满足业务快速上线要求，极短时间内可视化新建云平台；云厂商先进管理经验的互动交流；故障本地化快速响应；信创建设对于国产化硬件基础设施的开放兼容和大规模生产验证经验。案例的成熟度是银行客户数字化转型的定心丸。

(4) 从虚拟化替代到信创云替代升级。信创业务从边缘走向核心。随着更多新型应用和核心应用具备云原生特性，支撑应用的分布式架构需要从虚拟化走向云平台从而实现替代升级。基于信创服务器裸机部署以及虚拟化提供的计算资源的逻辑抽象无法满足多样化资源与云原生应用，通过软件定义计算、存储、网络的一体化云平台满足金融业务对整体性能的需求，通过容器、虚拟机、裸金属的统一混合编排更好地支撑金融业务的核心应用和新型应用。一体化云平台可深度融合容灾、备份、安全、监控运维等整体云方案，更好地满足金融业务的稳定性需求。

2. 内外兼顾的数字化运营服务体系。与易捷行云 (Easystack) 合作，依托“1+1+N”资源体系服务于省联社内部和各地市农商行两类用户群体。



▲ 图2 江苏农信金融云平台资源逻辑概览

“1”是指基于底层 Kubernetes 架构、一体化设计、平滑无感可进化的新一代数字原生云平台，提供完善的计算虚拟化、存储虚拟化、网络虚拟化、容器、裸金属能力实现了业务场景的全覆盖。云平台各项服务可以实现软件层面的全面自愈，高度自动化运维，深度检测硬件状态及关键服务（数据库、消息队列、计算、存储、网络等）并进行自动化分析。

“1”是指满足业务应用快速部署和基础资源弹性调用的云管理平台，订制化提供工单审批、资源告警、计量计费、成本优化、配额管理、服务目录等能力，形成行业云新服务接入的标准模式及最佳实践。

“N”是指统一监控平台、安全管理平台、日志分析平台、数据备份平台等第三方业务保障模块。面向金融业务连续性目标和业务发展规划，通过各产品联动，规避云环境单点故障、系统故障、资源竞争导致服务能力下降等各类新风险和脆弱性损害。



▲ 图3 江苏农信金融云平台建设选型关注点

3. 自立自强，集聚力量进行原创性科技攻关和生态合作建设。从云基础设施建设前期评测和5年来的应用管理经验看，单纯从产品入手是片面的，应放眼未来、面向发展，综合运用政策指引、人才增强、厂商合作等举措。决策者角度：关注合作厂商的产品成熟度、同区域同行业的案例落地性、产品生命力与公司服务持续性。建设者角度：关注开放架构下规范化、标准化、自动化、智能化发展的运维能力建设；数字化运维支撑工具和运维管理规范；关注合作企业的开放性以及和产品的兼容性；注重储备、培养专业技术团队。使用者角度：关注高安全、高可用、高性能、高稳定的云能力边界；关注产品使用规范便捷、问题响应及时、故障自动化修复、多品牌硬件适配等；可进化一体化云平台的原生云应用的实践、部署、迁移。

中国金电“信创金融云”赋能金融机构数字化转型

金电云（深圳）数字科技有限公司

随着云计算、大数据、容器等金融信息科技应用深度和广度进一步推进，银行在运用私有云开展数字化转型方面均取得了显著成绩。但是不同规模的金融机构在资金预算、技术水平、生态合作等各方面均存在一定差距，同时面临商业模式、数据安全、技术漏洞、监管要求等不同类型的风险，在金融私有云发展的大趋势下面临着巨大的压力。在这种情况下，金融云作为金融机构的另一种解决方案，可以帮助金融机构把握发展新机遇，将金融科技快速融入银行发展战略，提升金融服务的能力和效率，培养差异化核心竞争力。

“金电云”护航金融业信息基础设施

金电云（深圳）数字科技有限公司（以下简称金电云）是经中国人民银行批准设立的国有金融科技企业，以支撑监管、服务金融为己任，按照金融云等级标准，科学布局“多地多中心”，全力构建绿色先进高效的算力体系和“一云多芯”，多云融合、安全自主可控的云技术服务平台，打造金融业重要信息基础设施。

金电云长期承担央行同城灾备中心建设运维工作，并为外汇管理局、农信银、城银清、金融基础数据中心、支付清算协会、互金协会等央行相关单位提供数据中心托管服务。同时，金电云面向金融机构提供涵盖 IaaS、PaaS、SaaS 等全方位专业化云服务及技术咨询、软件开发、托管服务、灾备服务等一体化金融科技解决方案。截至目前，金电云团队研发了四大类 40 多款 SaaS 服务，覆盖核心、信贷、报送等多个关键应用场景。托管服务致力于为用户提供符合监管要求的 IT 基础设施环境，降低 IT 投资成本和运营成本。灾备服务开创与各清算渠道联通的灾备一点接入模式，可实现全

业务应急演练和灾难恢复。现有 100 余家金融机构客户涵盖以唐山银行、海南农信为代表的城市商业银行、省农村信用联社；以珠海横琴银行和梅州客家村镇银行为代表的农村商业银行、村镇银行；以中铁金租、诚通财务和铁建财务为代表的资产管理公司、财务公司、金融租赁公司；以爱建信托为代表的信托公司和保险公司。

“金电云”六大优势助力金融业数字化转型

金电云按金融行业信创要求，基于国内领先云计算技术，广泛适配主流芯片，应用全面云原生，实现敏态与稳态双模并存。基础云环境实现异构 CPU 资源融合，满足不同业务场景需求，强大的异构兼容能力可有效避免单一技术路线局限性和单一产品依赖性。金电云坚持开放共享，与产业行业深度合作，共同推进核心技术持续迭代和技术创新，赋能金融机构数字化转型，提升金融服务深度、广度和温度。

金电云整体解决方案帮助金融机构更加从容应对技术层面、管理层面和监管层面的挑战，能够逐步实现全面满足办公管理类系统应用、金融机具应用、一般业务系统应用和关键业务系统应用等场景的信创改造和应用需求，助力金融行业加速数字化转型。作为信创云平台，金电云具备六大优点：

1. 信创云平台。在分布式云架构的基础上，自主创新构建基于数字原生架构的业界领先云平台。通过可进化架构上的永续生命周期产品，实现云服务与云应用所见即所得，为客户利用云计算技术进入数字化时代提供了更加有力的支撑。

2. 多地多中心。金电云于北京、深圳、重庆、苏州布局建设具备四地多中心架构的云平台，可提供同城双活及高可用异地容灾部署，支持线下及主流云服务商至金融专区的跨云灾备，满足金融行业业务连续性要求，实现业务就近接入。

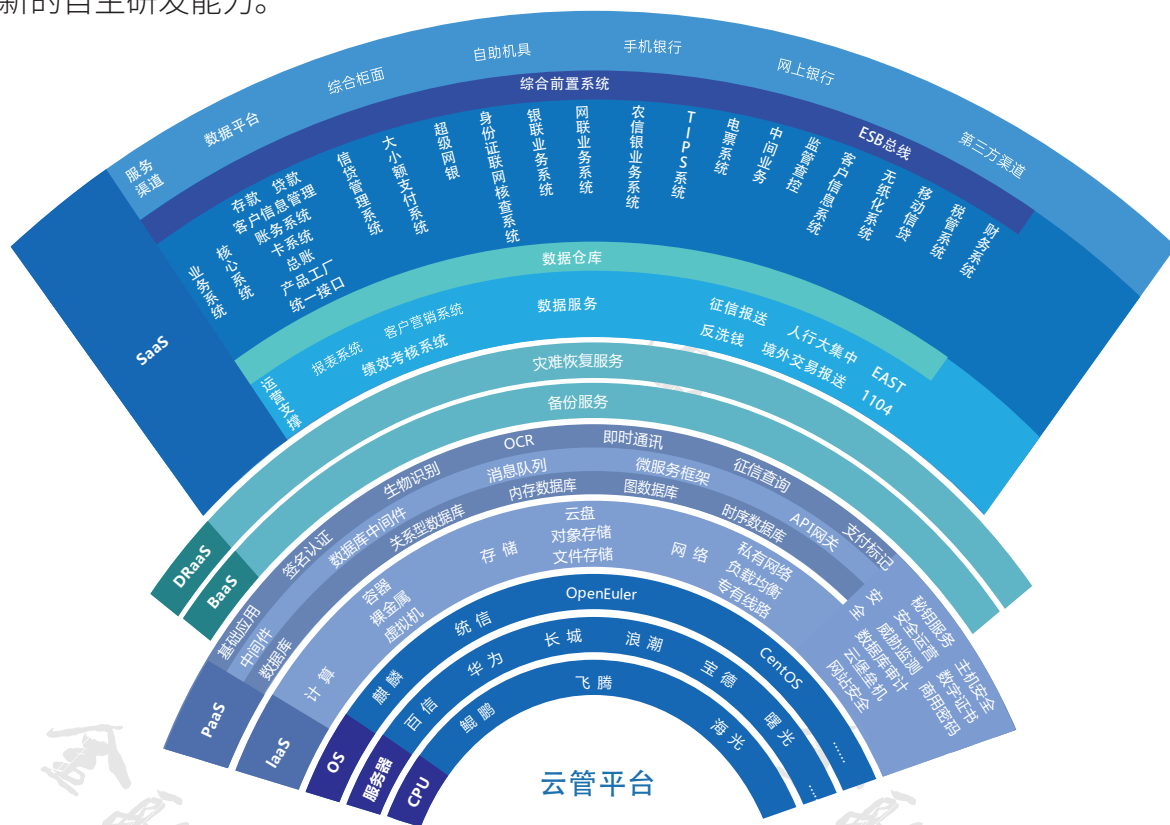
3. 一云多芯。“一云多芯”为用户提供了云化数据中心硬件资源异构的能力，即在同一个云内，并存 2 种及以上不同的芯片的物理服务器。金电云底层物理基础设施由海光、鲲鹏、飞腾多芯混合 CPU 的服务器硬件组成，在此基础上构建软件定义计算、存储、网络资源池，同时兼容主流品牌的网络设备，为客户提供满足不同应用改造、迁移需求的计算、网络、存储等丰富的云产品能力。

4. 多云融合。金电云采用了中国电子云、腾讯及华为等厂商的服务器、存储、网络等数据中心基础设施，此外，金电云正走向生产级适配生态并开源开放，扩展应用

到多云环境，链接基础架构、云服务和金融行业服务全生态厂商，兼容主要中间件和数据库等业务环境，为更多业务系统云化改造和上云之路提供支撑，可为一般应用和核心应用的统一上云提供强有力的支持。统一云管平台实现多云统一管理，确保云平台的开放性、互通性，强大的异构兼容能力可有效避免单一技术路线局限性和单一产品依赖性。

5. 安全高效。安全是目标行业客户的核心要求，金电云不但能够实现有效的用户和资源的隔离，核心业务、开发测试业务、外联业务分区统管，可满足行业监管要求，同时金电云也提供安全服务能力满足业务的安全防护需求并符合安全标准。

6. 自主可控。金电云落实国家信创要求，采用国产技术、使用国产硬件，具备全栈国产化能力；另一方面，掌握核心源代码，有效支撑开发运维一体化体系，具备优化、创新的自主研发能力。



▲ 图3 金电云金融行业整体解决方案

“金电云”面向金融机构提供全方位专业云服务

金电云依托丰富的基础设施建设、金融业务系统开发及金融信创服务等经验，面向金融监管和金融机构提供涵盖 IaaS 层、PaaS 层、SaaS 层的全方位专业云服务。

1.IaaS 层业务服务。包括计算、存储、网络三大类，提供云主机、弹性块存储、虚拟私有网络、容器集群等多种服务。不仅作为云服务资源进行独立发布并提供给云租户使用，同时也是云平台其他服务的基础。IaaS 层可为金融管理部门、金融机构提供生产中心、灾备中心基础设施建设服务，实现算力中心资源充分高效利用。

2.PaaS 层业务服务。基于云平台提供基础平台型服务，包括数据库、中间件、安全三类基础服务，以及签名认证、人脸识别、OCR 识别、即时通讯、支付标记等金融行业常用服务，并逐步衍生出数据分析、人工智能等服务。

3.SaaS 层业务服务。基于云平台的业务系统服务，包括核心业务系统、监管报送、手机银行、网上银行、客户营销、信贷管理系统、渠道中台等，并持续不断丰富服务清单。

在 SaaS 层构建渠道中台，实现为金融机构提供一站式接入服务。渠道中台连通金融机构和网联渠道、银联渠道、二代支付渠道、超级网银渠道、电子银行渠道、农信银渠道等，坚持需求驱动、场景驱动和数据驱动，助力金融机构降低服务门槛，将金融服务融入民生应用场景。通过构建信创监管云平台，实现全栈信创的反洗钱、EAST 报送、1104 报送、征信报送等，满足监管要求，为监管层提供数据分析支撑。

编后语

《银行业私有云建设发展调研报告》终于与读者见面了！

这本凝聚着行业人寄托、朋友们支持、编委尽力的报告，就像是十月怀胎呱呱坠地，我们悬着的心也就落地了。

文章千古事，得失寸心知。

当我们筹划这本报告的时候，有一种忐忑不安的心情，是否有足够的专业知识理解行业发展的现状，是否有足够的影响力获得行业同仁的支持，是否有科学分析的水平为行业的发展提供借鉴，诸如等等，紧张中含有企盼，交流中带有请益，坚定中守着前行。

诚然如此，我们始终坚持“为金融业和金融科技发展服务，为央行履职服务”的宗旨，秉持“理论研究、政策解读、知识普及”的方针，在完成这本报告过程中力求不偏离政策导向、不偏离行业方向、不偏离实际情况，努力求真、求实，最大程度上为行业展示私有云建设的最真实的一面。

有幸的是，在完成本报告的过程中，我们得到了 129 家银行业金融机构专家的倾力支持，他们运用丰富的专业知识和实战经验，毫无保留地提出了许多中肯的意见和建议，对提升报告内容的全面性、准确性和可用性起到了关键和核心作用，同时，他们认真仔细地完成了调研问卷中的每一个问题，也使我们深受感动，体会到了“天下银行是一家”的理念，极大地鼓舞了我们的工作热情。

“积跬步以至千里，积小流以成江海”，这份报告的问世，是我们在开展调研报告和白皮书的领域里迈出了小小的一步，对我们而言也获得了小小的满足和鼓励。我们深知：今后的道路会更长，责任会更重大。前路已过，后途待行，希望各位领导和行业同仁以及科技企业的朋友们一如既往支持我们的工作，我们定不辜负期望，不断努力，为行业贡献更多、更好的作品。

参考文献

- 【1】 《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》
- 【2】 中国人民银行《中国金融业信息技术“十三五”发展规划》
- 【3】 中国人民银行《金融科技（FinTech）发展规划（2019—2021 年）》
- 【4】 中国人民银行《金融科技发展规划（2022—2025 年）》
- 【5】 中国银行业监督管理委员会《商业银行数据中心监管指引》
- 【6】 中国信息安全测评中心《信息安全技术 信息系统灾难恢复规范》（GB/T37046-2018）
- 【7】 IDC《中国金融云市场（2021 下半年）跟踪报告》