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

金融云原生 2.0 发展应用白皮书

北京金融科技产业联盟

2022 年 4 月

版权声明

参编单位与人员

编制人员：

聂丽琴、黄本涛、周豫齐、贾士轩、诸旻、杨梅蕾、翟传璞、白阳、付鑫、李峰风、龙文华、鲁智琼、罗荣敏、毛杰、王骞、张松、周佳煊、周秋硕、郭婷、林丽鑫、张超、刘新华、莫业勤、许广林、林永德、徐旭、沈一帆、夏龙飞、蔡中原、王磊、周海鹏、苏兆聪、王佟、陈大伟、刘会福、杨旭晖、王磊、窦力杰、邓波、张怀强、徐朝俊

支持单位：

北京金融科技产业联盟
华为云计算技术有限公司
中国工商银行股份有限公司
中信银行股份有限公司
广发证券股份有限公司
深圳证券交易所
华夏银行股份有限公司
软通动力信息技术（集团）股份有限公司

目 录

一、数字金融需求推动云原生创新发展

（一）数字金融迎来发展机遇

近年来，我国金融信息化得到了巨大发展、取得了瞩目成就，有力地支撑了金融业的创新发展，为金融服务社会主义市场经济提供了强大动力。当前，新一轮科技革命和产业变革方兴未艾，数字经济蓬勃发展，催生大量新产业、新业态、新模式，金融信息化进入数字化、智能化新时代。

《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》提出打造数字经济新优势，充分发挥海量数据和丰富应用场景优势，促进数字技术与实体经济深度融合，赋能传统产业转型升级，催生新产业新业态新模式，壮大经济发展新引擎。明确深化金融供给侧结构性改革，健全具有高度适应性、竞争力、普惠性的现代金融体系，构建金融有效支持实体经济的体制机制。2021年12月，中国人民银行（以下简称人民银行）发布《金融科技发展规划（2022-2025年）》（以下简称《发展规划》），明确把握数字经济发展新趋势，发挥数据要素倍增作用，将数字元素注入金融服务全流程，将数字思维贯穿于业务运营全链条，强化金融创新的科技武装、数据加持，加快金融数字化转型步伐，全面提升我国金融业综合实力和核心竞争力。

随着5G、移动互联、物联网（IoT）、云计算、区块链、大数据、人工智能（AI）等技术的飞速发展及在金融领域的融合应用，加速推动了金融科技创新不断提升，促进金融机构服务模式、流

程等创新和优化。金融科技加速向银行、保险、证券、资管等金融领域渗透，推动着越来越多的金融机构数字化转型，有效提升金融服务的广度和深度。

（二）云原生赋能金融科技高效发展

传统的高门槛、低效率、同质化的金融产品和服务已不能满足客户的需求，线上化、个性化、场景化的新金融逐渐成为客户的基础诉求。与此同时，技术发展也改变了原有的商业模式，层出不穷的金融创新使得新金融真正成为可能，例如，移动互联网与生物识别技术深度结合，使得金融可以更便捷的触达客户并提供可靠的金融服务；大数据的蓬勃发展解决了数据不对称的问题，有效提升了金融风险的识别能力，使得普惠金融真正成为可能；人工智能也极大地提升了金融机构数据处理效率、业务流程效率、商业决策的效率和准确性。这一切都依赖金融科技具备敏捷的软件产品创新能力，从而为客户提供随时随地持续在线的金融服务。云原生是一种以应用为中心的软件开发方法，为实践者指定了一条低心智负担、能够以可扩展、可复制的方式最大化利用云的能力、发挥云的价值的最佳路径，金融机构也需不断提升自身软件研发能力，构建像互联网公司一样敏捷弹性、快速试错、急速创新的IT交付模式，因此预计云原生架构演进之路将是金融IT演进的必由之路。

云原生1.0被CNCF（Cloud Native Computing Foundation）定义为各组织在公有云、私有云和混合云等新型动态环境中，构

建和运行可弹性扩展的应用，代表着一种新的软件设计理念，应用从一开始就被设计为“长在云上、生在云上”，让云基础设施来接管应用中的非业务性代码和功能，用户可专注于真正有价值的业务代码，充分发挥云的优势，以灵活、低成本的方式构建弹性、可扩展的应用。同时，云原生也代表着一系列的方法论、实践和技术，包括容器、微服务、DevOps）、Serverless、服务网格（Service Mesh）等。云原生技术统一了软件交付和运维的模式，容器技术和容器集群编排技术（Kubernetes）的结合，解决了应用部署自动化、标准化、配置化问题。微服务通过把“巨石应用”拆解为若干单功能的服务，减少了服务间的耦合性，让开发和部署更加便捷和灵活，拆解了业务的复杂性，有效降低开发周期。服务网格让微服务中间件的升级与应用系统的升级完全解耦，在运维和管控方面的灵活性获得提升。Serverless让算力和运维对开发透明，对于应用所需资源进行自动伸缩。

云原生2.0围绕着让应用能够更好地“生于云，长于云”，在已有的技术基础上，补充了分布式云、混合调度、应用驱动基础设施、存算分离、AI数据治理自动化、DevSecOps、异构集成、全方位云安全可信的核心技术和关键能力。

云原生1.0的方法论和技术首先在互联网企业进行应用实践，但随着数字化转型的变革，政企用户大量应用、数据上云并逐步直接使用云服务开发，需要云满足“应用敏捷、业务智能、资源高效、安全可信”的新要求，使云原生进入2.0时代。在金融行

业，云原生2.0不仅需要对已有信息化投资提供“立而不破”的能力，还需要能够帮助金融机构充分利用云上的各种服务能力，以金融应用为中心，构建韧性、弹性、可移植、可扩展的应用，为金融行业提供“全场景极致体验”、“数据全栈智能”、“业务全流程安全”等业务服务能力，提升金融企业软件交付能力，赋予金融企业敏捷迭代、快速试错和创新的竞争力，推动金融行业进行全面的创新升级，打造科技与金融业务协同发展的数字化优势。

（三）云原生成为数字金融重要基石

《发展规划》提出，要着力打造布局科学、安全可靠的数字基础设施，筑牢金融转型与创新发展的“数字底座”，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、动态负载均衡的分布式架构转型，实现敏态与稳态双模并存、分布式与集中式互相融合。

云计算已成为数字金融的重要基石，分布式云计算逐渐替代单纯虚拟化，支撑金融行业的敏态业务需求，将业务需求更快转换为IT交付，向核心业务提供有力支撑，满足业务数字化需求。云原生以容器技术为核心构建的基础设施能提供明显优于基于传统虚拟化技术的第一代云平台的性能，基于分布式架构、微服务架构，提升应用快速开发、部署和迭代升级能力，通过极速弹性伸缩，更好地应对业务高并发，同时彻底屏蔽底层基础设施异构，满足金融企业激增的互联网化业务需求，以微服务实现应用

层由中心化向分布式演进，以DevOps实现高效率的开发运维，为场景金融、生态金融与数字运营提供有力支撑。

云原生技术对重塑金融体系而言，能够在一定程度上改变金融的供给行为特征，而供给曲线的位置既取决于各类金融基础设施的发展程度，又取决于金融服务提供商的管理能力和金融产品创新能力。本白皮书重点研究云原生技术在金融行业的发展与应用，探索金融科技发展与云原生的结合场景，以推动云原生金融应用发展，助力谱写数字金融创新发展的新篇章，为构建新发展格局贡献担当。

二、云原生2.0加速金融业数字化转型

（一）加速金融敏捷创新

云作为金融科技建设发展的重要基础设施，已经逐步由“面向云迁移应用”的阶段演进到“面向云构建应用”的阶段，基于云原生2.0的底层技术，利用智能的调度、高效的管理、软硬资源的协同、安全的隔离，加速金融敏捷创新，主要体现在以下方面。

1.打造全场景极致体验

云原生分布式云架构让金融企业的基础设施，从简单的资源池化，转向为以应用为中心、能感知应用特征、智能高效的云原生基础设施，并通过分布式云的布局，为客户提供业务访问的高性能、低时延极致服务体验。

（1）极致的性能。在应对行情、在线交易类金融业务的流量冲击时，需要 IT 资源能够极速扩容、大规模调度，基于云原生裸金属部署容器、容器直通存储、网络资源等技术缩短 I/O 路径，从而为金融客户提供极致的性能和资源利用率。

（2）极低的时延。金融行业会经常遇到业务跨省、跨运营商访问时延波动大、行情数据大数据量查询时延大等问题，严重影响客户体验，通过使用基于云原生网络、Serverless/Function 毫秒级创建资源、秒级冷启动、容器网口粗度 QoS 等能力，构建单 VPC 内多集群支持百万级容器，提升业务的端到端响应效率、缩短业务时延，优化用户体验。

（3）极简的开发与运维体验。随着新老应用越来越多，进程、服务、资源映射关系复杂，应用关联难度大，导致应用异常时相关告警繁杂，根因告警识别难，复杂的网络拓扑、流量治理无可视化界面，导致故障定位耗时长，同时大量业务跨云、跨区域部署，运维难度也急剧上升，基于云原生定义的行为规则、应用指标度量和智能决策，使用策略驱动的自动化管理，使超大规模云资源全局化高效运维成为可能。

2.构建数据全栈智能

伴随着金融业务进入千行百业，新业务的出现也带来数据的爆发式增长，如何解决传统的金融系统烟囱式架构下业务割裂、数据割裂、系统割裂等一系列问题，打通数据孤岛，发挥数据价值，更有效的将巨大的数据资源转化为高价值数据资产，成为金

融行业数字化转型中的重要课题。

（1）打通数据从资源到资产的通路。通过构建在云原生架构上的金融级分布式数据库、智能数据湖等一系列产品，为金融客户提供从数据产生、接入、治理到服务的全数据生命周期管理，“湖-仓-库”按需加载、有机协同，打造金融行业高可靠、低成本、高效率、打通孤立系统的数据解决方案。

（2）助力 AI 金融场景应用落地。金融是高度数据化的行业，AI 在智能营销、智能运营、智能客户、智能投研等方面大有可为。传统的数据治理还是人力密集型工作，整个过程非常低效，难以满足很多行业的要求。通过引用构建在云原生架构上的 AI 数据治理自动化技术，将数据的获取、清洗以及最终数据知识的提取、主题库的建立、数据目录的发布完全自动化，用户只需指定入湖的数据源和所属业务主题域，系统自动化创建入湖任务，底层资源根据入湖数据量自动扩缩容，智能完成入湖数据的安全等级、分级分类、隐私等级等数据标签的自动识别打标。近年来，AI 逐渐成为提供现代化金融服务的关键技术，且已在金融的诸多场景中有着广泛的落地实践。未来，围绕 AI 在金融行业落地，将发展出 3 个“新”。

AI 开发新模式。预训练大模型是解决 AI 应用开发定制化和碎片化的重要方法。可实现一个 AI 大模型在众多场景通用、泛化和规模化复制，减少对数据标注的依赖。赋能 AI 开发由作坊式转变为工业化开发的新范式。

知识计算新方案。通过应用知识计算解决方案，企业将可以打造自己的知识计算平台，整合分散在不同系统、多种形态的企业数据，形成带有建议性的知识体系，有效用于预测分析和辅助决策，提高企业的经营效率。

AI 行业新高度。通过知识高效、模型高效、数据高效和算力高效，实现对机器和人的高效赋能，推动 AI 在行业的高效落地。

3.保障业务全流程安全

云原生 1.0 阶段，云安全是孤立的安全能力，虚拟化安全、hypervisor 防逃逸、云防火墙等安全服务没有相互联系，云原生 2.0 则提供全方位的立体式运营安全。通过打通离散的云安全服务能力，将云服务及客户应用形式深度融合，构建内置安全能力的云原生应用。云原生 2.0 引入可信智能计算，解决跨行业数据隐私保护与流通碰撞、价值挖掘之间的矛盾。通过使用跨组织、跨行业的多方数据融合分析和多方横向与纵向联邦学习建模，安全多方计算（例如同态加密，差分隐私等）、用户自定义隐私策略、区块链数据计算轨迹的可追溯可审计，解决敏感行业上云安全顾虑，为用户构建体系化的云安全防护。同时，通过遵循金融行业相关安全要求，达到金融应用的安全合规，信息的可信流通。

（1）平台安全合规。安全是金融业务上云最基础的要求。一方面，金融行业受“一行两会”监管，是强监管行业，所以安全合规是金融行业上云最优先满足的要求。另一方面，由于金融

业务的重要性，对业务的连续性有极高的要求，不能出现业务中断，因此，需要为金融行业客户定制打造安全合规的业务平台。

在等保合规方面。需要遵循行业相关技术标准建设，采用独立的模块化设计，物理资源严格隔离。此外，平台还需支持资源专属能力，实现计算、存储物理资源租户级专享，满足数据库、大数据、中间件等高阶服务专属池部署，适配客户多样化的资源隔离诉求。同时，还需通过等保测评、支付卡行业数据安全标准（PCI-DSS）等一系列业内的安全资质认证。

在高可用性方面。平台需要支持同城双活，异地容灾两地三中心高可用部署架构，保障金融业务的不间断稳定运行。

在金融应用方面。平台基于云计算存储资源池构建，满足金融行业客户的应用需求。

（2）数据可信流通。在发掘金融数据价值的同时，对于数据隐私的保护也同样重要。“十三五”规划明确提出“实施国家大数据战略”，加速推进大数据开放共享。“十四五”规划进一步提出要完善数据资源交易流通的安全保障体系，规范数据资源管理。2019 年，网信办颁布《数据安全管理办法》，对企业处理和使用个人数据提出了严格的边界与要求。

可信智能计算服务可在保护数据隐私前提下，实现企业内部和跨企业之间的多方数据安全融合，为金融业数据消费者提供多方数据的安全计算能力，实现数据使用的“可用不可见”，从而打破跨行业“数据孤岛”。参与方敏感数据能够在具有可信执行

环境（TEE）安全支撑的聚合计算节点中进行计算，同时基于区块链技术满足数据在流通、计算过程中端到端的可审计、可追溯的需求，实现数据使用的“可控可计量”，推动数据价值有效释放。

（二）助力金融业务平台构建

随着互联网金融业务的高速发展，用户的金融交易行为逐渐由传统的面对面线下交易演化为线上交易，由于线上业务可不依赖线下网点开展，从而突破了网点辐射范围的限制，使得用户在任何地点、任何时间都能享受到便捷的金融服务和产品，有效地推动了普惠金融的发展。但是，服务线上化也使得业务量难以准确预测，这对金融机构的 IT 架构提出了更高的要求。因此，金融机构为了满足用户突发性网上查询、交易等行为带来的访问量增长，不得不在整体 IT 建设上投入更高的成本，以获取更多和更高性能的服务器资源。与此同时，随着设备规模和业务复杂度的增加，新增需求的交付周期变长，运维难度不断提升。基于此，云原生技术将从以下多个方面构建基础设施，提升业务的稳定性，保障业务的可靠开展，加速企业创新发展。

1.提升应对大规模业务冲击能力

2016 年，中国银行业监督管理委员会印发《中国银行业信息科技“十三五”发展规划监管指导意见》，提出银行业金融机构要稳步推进云计算应用并主动实施架构转型。然而，大部分金融机构仍停留在简单使用云计算资源池为上层业务提供资源共享、

弹性调度的阶段。随着云原生技术的兴起，银行、证券、保险机构逐渐尝试采用容器、微服务等技术进行业务升级，通过细粒度的架构设计与资源管理来提升资源利用率和业务响应效率，虽然以上各类技术升级节省了基础设施建设的成本、提升了利用率，并在一定领域内构建了应用交付标准，但仍未充分发挥出云计算的价值。

云原生技术发展早期，容器服务部署形态主要基于虚拟机，以虚拟机节点作为容器集群的计算节点，并基于此来构建容器的网络、存储和编排能力，虽然这样的堆叠架构可以让整个软件栈分工明确、边界清晰，但也带来了较大的性能损耗和功能冗余。同时，应用与资源之间仍是一种简单的堆叠关系，无法实现有机融合和智能感知。在云原生 2.0 时代，基于应用感知、容器卸载、容器直通网络、容器直通存储等技术，结合裸金属服务器（Bare Metal Server）来构建以容器为核心、以应用为中心的云原生基础设施平台，将成为金融机构充分发挥云计算价值的首选。

直接使用裸金属服务器作为容器运行的环境，减少了虚拟化层带来的资源损耗，再基于容器卸载技术，把容器引擎、容器网络等组件下沉到专属硬件加速卡上，进一步减少由容器平台运行带来的资源占用。一方面，裸金属节点上的计算资源可以 100%被业务负载使用，同时避免了对业务负载的性能干扰，大幅提升整机性能、业务应用性能，尤其是在业务大规模、高密度部署的场景下，性能提升比可达到 100%。另一方面，容器网络、容器存储

组件下沉到卸载卡后可以与传统 IaaS 层的网络、存储组件垂直打通，减少冗余功能。直接以硬件设备直通方式将存储、网络资源分配给容器实例，缩短 I/O 路径，提高网络、存储性能。以上优势再结合 Serverless 架构的容器平台，让企业可以将常稳业务运行在裸金属容器、高弹业务运行于 Serverless 容器，实现资源的最佳配比，在保障业务敏捷的同时，进一步优化资源成本。

2.实现更低的端到端业务时延

面对大规模业务请求，服务器需要快速发放计算、网络、存储等资源，其中要保障业务的高可靠运行，网络能力极为重要，要确保海量计算、存储资源发放后网络能够快速连通、数据传输安全隔离、根据业务的不同特点细粒度配置网络服务质量（QoS）等。面对行情资讯、在线交易等有着亿级用户同时接入的业务平台，需要能提供多线边界网关协议（BGP）、大带宽弹性负载均衡（ELB），目前主流云厂商提供的 BGP 产品都已实现与主流运营商对接，并支持 60+线的 BGP 接入，免除金融机构自建数据中心与各运营对接的复杂性，这样不同运营商手机用户都可以享受同样的高速接入、查询和交易服务，确保良好的业务体验。基于分布式的云原生架构，可以实现业务的就近部署、用户请求就近接入，极大降低了业务端到端的访问时延。

3.优化业务全生命周期管理

传统金融机构由于“烟囱式”组织架构，使得业务系统构建也呈现出烟囱化趋势，如采用不同的技术、架构、开发模式、部

署模式等，造成信息共享不通畅、业务重复建设、数据孤岛等问题，阻碍了“一站式金融服务”目标的达成。以云原生基础设施为底座来支撑业务发展，统一了业务的运行平台，使用容器技术栈来构建在线交易、离线数据分析等不同类型业务的底层运行平台，进一步结合微服务、服务治理等技术，统一业务应用业务的架构设计、开发、部署模式，从而实现跨平台、跨部门间的业务、数据、软件能力共享。

“Kubernetes+Operator”以其良好的可扩展性及较高的社区活跃度，成为各企业的主流选择，主要提供以下几方面的能力。

（1）部署标准。支持通过增加配置文件声明使能弹性伸缩、配置更新、数据迁移等云原生能力。

（2）开发规范。自动生成服务包和配置文件，开发者聚焦业务开发和配置使能。

（3）服务中心。提供服务生态、种类丰富，同时接入服务提供商提供的服务社区版以及企业版供企业自主选购，一键服务实例分发，秒级部署，开箱即用。

（4）服务生命周期管理。结合多集群管理和边缘云管理，提供跨公有云、混合云、边缘的全场景服务生命周期管理。

通过这些方式，将极大降低云原生服务全生命周期管理的难度，加快企业业务的云原生化升级。与此同时，随着企业云原生应用数量的快速增加，对应用服务的流量治理、运行监控、访问安全以及发布等能力要求也相应提升。在云原生 1.0 阶段，主要

基于以软件开发工具包(SDK)方式进行微服务治理框架的模式，在云原生 2.0 阶段，随着应用数量和种类的爆炸式增加，逐步被非侵入式的微服务治理解决方案取代；Service Mesh 作为现在主流的非侵入式服务治理理念，可为用户提供包括负载均衡、熔断、限流等多种治理能力，让业务的灰度发布、流量治理更加简单，Istio（由 Google、IBM 等开源的微服务管理、保护和监控框架）则是 Service Mesh 的代表性开源项目之一，可以帮助企业快速构建服务化的应用架构。

（三）高效推动各项业务发展

1.赋能营销业务开展

伴随人口结构和社会财富分配的不断演变，人们的消费需求、生活方式等发生了翻天覆地的变化，金融行业业务规模的逐步扩大以及客户群体的变化，其积累的以老带新、网点营销、电话营销、组合营销等传统营销模式的不足日益显现，因此基于用户画像的智能营销模式在金融行业加速普及，尤其在金融科技的快速推动下，传统金融机构正在积极将云计算、大数据、人工智能等新技术，深入应用到营销领域，加速金融智能化营销建设。

（1）支持全面的客户洞察，统一客户 ID、标签、画像体系构建。通过对异构数据源的处理，整合多渠道客户、营销活动数据，自动化跨渠道打通“ONE ID”，实现数字化数据管理。基于客户统一的“ONE ID”，将客户的身份属性、消费属性、活动属性和兴趣爱好等进行梳理聚合，形成典型标签模型，再根据不同

的客户标签做精准营销或个性化推荐。基于客户海量数据，对客户社会属性、活动属性、消费属性和兴趣爱好等信息通过文本挖掘、自然语言处理、机器学习、预测算法、聚类算法等进行模型构建，从不同维度、颗粒度对客户进行描述，搭建客户画像体系。

（2）支持全渠道、智能化营销投放。通过对营销活动场景化封装，构建可视化、场景化营销模板，支持精准营销一键发布。实时营销平台可提供营销规则策略配置、营销决策、营销事件侦测等能力，保障营销过程中实时获取每位客户的渠道行为，触发个性化营销策略，提升用户体验和企业效益。

（3）支持营销数据迭代与优化。根据营销过程中产生的用户触达、交易数据、营销数据和运营数据分析，形成反馈信息和可自动执行任务。成为用户标签、下一次营销活动设计的输入，再次启动闭环并持续迭代，提升营销流程的价值，打通首尾形成闭环。流批一体的营销活动数据整合，形成统一客户视图，提供营销活动过程中全面、多元的数据报表，确保营销效果。

数字化营销时代，金融行业的客群管理智能化、数字化已成为必然趋势。而在智能化、数字化进程中，大数据是不可忽视的力量，通过大数据打破数据孤岛，打通内外部各大营销渠道，实时追踪客户数据，构建精细化客户标签以及精准的客户画像，找出优质和潜力客群，最后针对将这些客户进行有针对性的营销活动。实现真正意义上的客群管理作用于实时营销，精准客户营销策略。

2.提升风控智能化水平

（1）金融风险是金融行业长期面临的挑战，新冠肺炎后疫情经济时代形势愈加严峻。Kroll 行业调查显示，全球有超过 84%的企业遭受过欺诈问题的困扰，而在金融行业，这一数字是 91%，在所有遭到欺诈的行业中排名榜首。未来，全球进入新冠肺炎后疫情经济时代，大量交易转向线上、非接触性交易，呈现出传统的线下渠道快速向移动互联网渠道和境外迁移的态势，遏制在线欺诈将面临更大的挑战。根据 Juniper Research 的新研究，到 2025 年，全球在线企业将因在线支付欺诈而损失超过 2060 亿美元，这一数字几乎是亚马逊 2020 年净收入的 10 倍。

（2）随着黑灰色产业链产业化、精准化、移动化和技术化，金融欺诈风险呈现欺诈模隐蔽化、场景化、社工化。庞大的黑灰色产业链，当前已经形成了较完整的产业链，团伙作战且欺诈工具制造、欺诈实施、洗钱销赃等分工明确。当前金融风险场景呈现多样性，其中互联网欺诈、伪卡盗刷、电信诈骗、交易跨境赌博等成了国内银行业损失较大的风险场景。而且很多风险欺诈呈现社工化，也就是社会工程学，黑产通过对社会人的心里弱点、习惯弱点进行分析，例如电信诈骗等场景。社会工程学由此延伸出社工库，黑客们将获取到的用户数据进行整理归档(也称洗库)，以便集中查询的数据库，社工库里除了典型的账户密码，甚至还包括关联的其他社交信息、银行信息等敏感用户信息。

（3）黑产与金融从业者间的攻防大战，其场景不断演变、战场不断扩大、技术不断升级，整个攻防是“情报+技术+机制”的综合大战。其中，情报数据是金融风控的基础，智能化的风控技术是风控的保障，完善的金融监管制度是风控的法规保障。未来，风控对抗技术大致呈现如下趋势。

风险控制对情报数据的维度要求越来越高。传统风控判断主要是从持卡人账户维度进行风险判断，无法应对互联网金融线上支付、秒贷、电信诈骗等场景。未来风控所需要的数据维度，不仅仅涉及持卡人、卡片、MAC、IP、WIFI、设备指纹、商户等，还对于风控技术的可扩展性和灵活性提出了更高的要求。

风险控制更加强调实时化。传统风控一般为事后分析，缺乏事中监控处理。主要是原因是事中对复杂、高并发场景的实时计算能力要求高，既要实现每笔风控检测，又要保障用户体验，难度较大。往往一笔风险事中拦截要求在 50ms 内完成，才能更好的满足业务的风险控制诉求，这其中涉及几百个规则、上千个变量的应用和计算。

风控策略更加智能化且精度更高。未来线上交易、贷款等金融业务呈现交易短平快的趋势，传统的专家经验能够考虑的维度有限，而且机器学习模型，可以通过反复训练、让成千上万维数据参与风险评估，模型能做成来专家很难总结出来的经验，行业经验来看模型相比专家经验能提升超过 10%的分析精度，可带来上亿元的风险止损。

3.强化经营分析能力

（1）金融行业数字化转型的逐步深入。越来越多的金融企业借助数据技术和数据平台提升管理效率和决策的科学性，企业用户对经营分析数据平台提出了新的要求。一方面，经营全面反映运营情况，分析对象包括财务系统和各个信息系统的数据，以前已存在但被低估价值的数据正在不断被挖掘出新的价值，跨系统数据聚合和海量数据分析能力成为经营分析数据平台的基础。另一方面，业务场景和形态趋于多元化，新业务形态催生新的数据，新的算法模型不断产生，经营分析的边界持续延展，经营分析总结历史规律并预测未来走势，承载业务决策的权重日益增长。数据平台逐渐成为金融企业的核心业务系统，应提供更加稳定的高可用平台。

（2）金融行业经营分析技术稳步发展。为支持集群规模高扩展，容量性能匹配经营分析数据，分布式云数仓应对金融行业的需求，可提供完整的高扩展、高性能、多源分析的解决方案。基于分布式云化底座，增加集群节点数量不仅需要在容量方面实现线性扩展，还需在数据加载、处理性能方面做到线性扩展。通过攻克节点间通信的技术问题，解决大规模通信、大规模集群管理的关键技术，实现数据仓库的高扩展性，匹配金融行业经营分析海量数据聚合的容量和计算能力的要求。

经营分析技术强调对比，通过实时数据与历史数据关联分析，可以感知金融业务运行状况，并预测可能会出现的风险与问

题，及早发现并及时干预。经营分析数据平台功能包含以下几方面，**一是数据实时入库，**通过高并发小批量模式，线性扩展流数据入库性能，根据业务数据量规格，可达到每秒上千万条数据的入库性能，改变传统数仓 T+1 大批量加载模式。二是**数据实时分析，**支持基于流式数据的持续计算查询，通过 SQL 完成流式计算，实现亿级数据秒级聚合。**三是实时数据与历史数据关联分析，支持**增量数据与全量数据关联查询，实时呈现业务变化趋势，同时支持从结构化数据到多元数据分析。

随着业务分析精细化，经营分析关注财务信息、业务信息、市场信息、管理信息等多方面的信息，信息格式更加多元化。经营分析数据平台应根据业务分析需要，扩展数据分析边界，增加图分析、机器学习、统计分析等先进的算法模型，对各个业务系统中的信息进行格式化呈现。

经营分析数据平台应具备跨 AZ（可用区）/Region（云区域）的部署能力，保障业务稳定持续可用，并提供数据强一致性，保障经营分析的结果可信。应用同城跨机房的双活集群部署方式，以抵御机房级故障，确保单 AZ 故障不影响数据平台的正常运行。金融行业的企业经营分析，并非是数据的罗列和泛泛的总结，而是通过数据分析总结历史规律，预测未来走势，数据平台需要协助及时提供有效的经营决策信息，从而实现支持业务决策，规避经营暗礁，构建竞争壁垒。

（四）构建安全的金融业务体系

金融机构内部包括其职能部门、分支机构和合资公司，有着很强的数据融合需求，而金融机构与外部组织包括同行业、政府、互联网、运营商之间的数据融合也日趋活跃。通过数据的流通和汇聚，得到个人和企业用户画像，并应用于营销、风控、个性化定价等业务场景，可显著降低运营风险，同时提升资源配置效率。但数据在金融业的大规模流通仍面临关键挑战。首先，企业内外部对数据融合共享有着强烈的需求，但由于业务竞争、数据泄露风险等因素影响，多方主体间数据的融合共享仍存在诸多障碍。其次，由于数据的可复制性，一旦把数据提供给需求者，就有失控被不断复制和传播的风险，数据拥有者也就对数据流通产生顾虑。最后，结合多个参与方的数据建模具有很高的价值，但涉及到多方合作，往往沟通成本大，且缺乏高效的机制来实现多方高效合作，如图 1 所示。

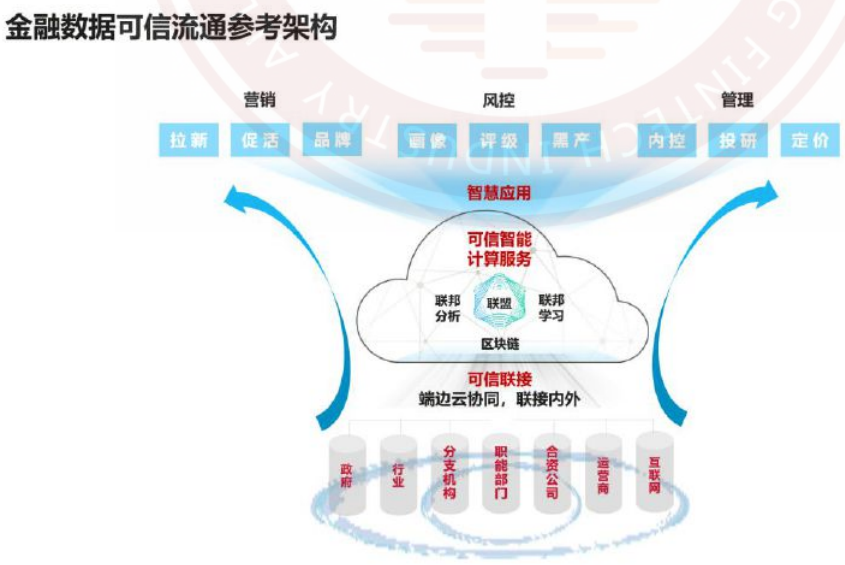

图 1 金融数据可信流通参考架构

通过技术手段保障在不暴露明文数据的前提下，建立多方数据流通的机制，实现多方数据建模，对于产业链和组织内部效率提升意义重大。隐私计算技术是解决上述问题的关键技术手段。例如，利用多方安全计算、联邦学习等技术，对不同来源数据在数据接入、传输、处理、使用等过程中进行全链路安全保护。不同参与方分别扮演监管者、数据处理者、数据拥有者、数据使用者的角色。数据使用方提出数据使用申请，获得监管者审批后，基于数据拥有者的加密数据进行查询和模型训练，最终数据使用方只能获得被审批的数据处理结果，无法获得数据拥有方的原始或加密数据。隐私计算技术也可以和区块链技术进行有机结合，进行数据确权和存证。基于这种技术和机制，打消了组织关于数据泄露的顾虑，也形成固定的可追责、可追踪的机制，使得数据共享和流通变得更加容易和可靠。

在金融专区云原生架构基础之上，通过部署可信计算服务，构建满足《多方安全计算金融应用技术规范》（JR/T 0196—2020 ）的可信计算节点，能够为金融机构、组织、用户等提供安全的联合数据分析、脱敏传输等数据安全交换能力，并在金融风控、营销、管理、安全层面有广泛的应用需求。

1.在风控层面。首先可以基于多方数据，对个体和企业建立更全面准确的画像。单一来源的数据难免存在数据样本和数据维度有限、有偏差等问题，基于隐私计算技术对多方数据进行分析，

可以在合规的前提下，对个体和企业画像进行补全或校正。例如，针对债券类金融产品进行评级，结合多源数据实现更加准确的动态评级。行业各方还可形成行业联盟，结合各方单点数据对黑产进行联合打击。

2. 在营销层面。对金融机构而言，圈定其服务和产品的潜在客户至关重要，一般可通过现有活跃用户具有相似性特征的人群发掘其他潜在用户，从而针对这些潜在客户进行精准的拉新、促活和品牌宣传，这将有效提升营销效率。可信计算服务能够在合规前提下，对种子用户的画像信息和广告商的数据进行联合建模，通过训练模型来预测更广泛受众对品牌或产品的倾向性，帮助圈定目标受众。

3. 在管理层面。内外部数据的可信流通都具有重要意义。首先，通过对企业内部数据的整合，可提升内控、审计和管理效率。其次，获取充足的与市场竞争、技术创新、业务发展等有关的外部数据，可有效支撑管理层进行战略规划和重大投融资决策。最后，客户消费、社交等行为数据可帮助企业进行新产品的研发和推广，从而显著提高企业经营效率。

4. 在标准层面。2020 年 10 月，人民银行印发《云计算技术金融应用规范 技术架构》（JR/T 0166—2020）《云计算技术金融应用规范 安全技术要求》（JR/T 0167—2020）《云计算技术金融应用规范 容灾》（JR/T 0168—2020）标准，明确云计算技术金融应用管理要求和安全技术要求，在防范化解云计算技术应

用风险、保障金融业务连续性、提升金融用户体验、保护消费者合法权益等方面发挥了重要作用，产生了积极效果。

三、金融云原生2.0转型建议

以容器、Kubernetes、微服务等技术为代表的云原生技术，经过近几年的蓬勃发展，在弹性扩展、降低使用成本、技术成熟度等方面均取得了长足发展，成为赋能业务创新的重要推动力，其应用场景在金融行业，已经逐步深入到核心业务，给金融数字化转型带来了极大的价值，随着云原生 2.0 的阶段到来，我们提出如下建议。

（一）制定转型路径

应聚焦“统一云原生基础设施、软件云原生架构、以应用为中心”的目标，结合金融机构当前信息化建设现状及数字化转型关键需求制定目标可达的云原生路径，逐步实现敏捷交付、快速弹性、平滑迁移、无损容灾等技术能力，并从基础资源为中心转移到以应用自动化为中心的工作开展模式。

（二）注重试点示范

应从金融业务场景出发，明确哪些业务适合采用容器作为基础设施、哪些业务的数据可快速适配迁移到云原生环境、哪些业务可以进行云原生改造、哪些场景适合在云原生基础上进行开发，对业务系统进行场景评估分析，挑选出具备代表性的业务场景进行试点示范，总结经验后形成可复制的典型做法、解决方案，逐步提升金融云原生的深度与广度。

（三）加强组织统筹

金融云原生转型应坚持遵循《金融科技发展规划（2022—2025 年）》相关要求，强化组织协调、凝聚行业共识、结合实际科学谋划，形成金融管理部门、金融机构、科技企业、社会团体等紧密配合、协同高效的工作格局，着力使用云原生技术加快金融机构数字化转型。

（四）强化安全保障

应做好对金融云原生涉及的基础设施、数据、应用的安全评估，对云原生的开发、管理、运维进行全流程的安全管控，对整体实施过程出现的难点问题及时提出针对性的对策和措施。同时应着力强化云原生规划实施与要素供给的协调联动，积极争取政策和资金支持，切实保障云原生规划落地实施过程中所需要的资源，全面激活使用云原生支撑金融数字化转型发展的内生动力。

四、未来发展趋势

金融业是我国信息化建设程度最高的行业之一，金融机构普遍具有较强的研发能力。例如，银行业普遍利用分布式技术重构核心系统；保险业客服、销售、理赔等环节广泛应用大数据、人工智能、物联网等新技术；证券业运用科技手段在客户服务、产品设计、资产定价、资产配置、交易系统、运营管理等多个方面强化资产管理能力。

金融机构已普遍应用云计算相关技术，但当前的云平台主要以“资源为中心”，更多关注资源节约、动态资源分配等方面，

重点解决运维、部署、扩容的难题，但传统应用单体架构过于厚重、烟囱式架构带来的一系列问题并未得到有效解决。如何在保证业务连续性的前提下实现架构的平稳升级，以及如何实现云原生新生能力与既有能力有机协同，是金融机构普遍面临的现实问题。

金融科技的发展将推动云原生 2.0 从技术和单一的业务场景，向着产业金融、普惠金融和国家级金融基础设施的方向发展。未来，云原生 2.0 技术将持续加速金融机构在供应链金融、农业金融和工业互联网金融等领域的探索和实践。

（一）物的信用，增强供应链金融服务能力

2021 年 4 月 19 日，中国银行发布《关于创新供应链金融服务模式全力支持产业链供应链现代化水平提升的十五条措施》。积极推动供应链金融数字化、场景化、智能化发展，提升产业链供应链现代化水平、助力实体经济发展贡献金融力量。通过利用云原生技术和 AI 大模型开发动产算法，结合射频识别（RFID），智能摄像头等智能终端的能力，进一步解决产业链上游中小企业“先货后款”模式下的资金占用问题，有力的支持供应链产业链稳定循环和优化升级。

利用云原生的 AI 大模型泛化能力（例如一个模型同时做行为异常，轨迹异常检测），批量训练人员异常行为，出入库异常检测等 9 个算法，实现异常样本种类多、少样本，AI 流水线模型

开发，降低了金融科技的门槛。这些模型预置于仓库智能摄像头，实现实时掌控货物的动态出入情况。

通过在仓库侧部署 RFID 和带算法的智能摄像头，同时将 RFID 和智能摄像头的数据融合到经销商的仓储管理系统，并将此系统和银行的风控系统进行对接，可有效赋能金融机构线上实时贷款业务流程，加快中小经销商的资金流转。在与浦发银行的实践中，实现了线上贷款全流程，将贷款流程从过去的 5 天到账变为实时到账，并将资产的风控提升为 7*24 小时的实时监控和预警。同时，通过同业信息共享，支持为多个小微企业实现放款。

（二）生产信用，促进农业金融服务下沉

2021 年 4 月，人民银行联合 6 部委发布《关于组织开展金融科技赋能乡村振兴示范工程的通知》，提出探索运用大数据、人工智能、物联网、区块链、5G 等新一代信息技术，在安全合规的前提下，推金农村金融机制和模式的创新，优化农村金融产品与服务的供给。通过利用云原生 2.0 技术，结合卫星图像或数据采集技术，进行图像学 AI 处理，使得农村金融服务得以下沉。

场景一：针对大田作物融合金融科技的卫星信用贷。具体地，利用卫星数据的处理，对农作物的地块、对气象、农作物长势等做画像，掌握贷款申请人所属地块的位置，并对地块是否适宜种植某些农作物做出评估，同时对历史灾害天气做分析预测农作物的长势，从而实现对大田作物的贷前和贷后的低成本精准管理。经过在河北、云南、陕西等地试点，大幅提升贷款额度在 30 万

以下种植户的贷款可得性，该数据还可为政府精准补贴农户提供生产过程的监测功能。

场景二：在“一村一品”“一镇一特”“一县一业”的金融服务方面，可利用卫星图像 AI 处理能力，支持保险机构针对性的农产品气象指数险的开发。例如茶叶的倒春寒气温指数险、海参的温度指数险、生蚝的风灾指数险等。气象指数险无需保险机构人员现场勘察定损，即可获得推送式理赔服务，因此种植户或者养殖户能够获得精准的保障。基于此，对于有融资需求的农户，可鼓励农户配置农产品气象指数险，然后针对性提供贷款等金融服务。

场景三：基于云原生区块链的 TICS 可信智能计算服务开发的农业金融平台，通过联接生产、加工、物流环节在统一的账户实现融资闭环。平台采用了 OCR 自动识别订单的功能，为农事生产提供场景化精准滴灌的金融服务，同时也为政府精准补贴提供依据。同时该平台可通过微信扫一扫，为消费者提供从溯源地到物流的全流程服务，不仅提升了农产品的融资价值，同时还为农产品的溯源地提供了乡村文旅二次变现机会。

以农业产业园为抓手，通过对产业园的梳理，落地农业金融平台，实现一个账户贯通产供销的全流程和融资闭环运行，对农事全过程进行实时风控，推动金融服务的精准滴灌和下沉。

（三）智改数转，推动工业互联网金融发展

2020 年 3 月，工业和信息化部办公厅发布关于推动工业互联网加快发展的通知，鼓励智能化改造生产流程和设备，快速推动企业数字化转型。基于此，金融机构纷纷响应，推出智改数转的贴息低息贷款，利用云原生 2.0 快速支撑工业企业的转型。目前金融机构已在技术和金融服务等方面支撑了上百家工业企业的智改数转。

探索工业互联网金融的建设路径，以 100 国级、1000 区级的工业互联网基地为抓手，梳理细分子行业的全生命周期的智改数转和金融需求，针对性的设计和匹配金融产品，并对接政府补贴，提供全生命周期的一站式精准滴灌实时的金融服务。

五、金融云原生2.0实践案例

（一）商业银行云原生实践

1.中国工商银行云原生实践

近几年互联网的崛起，对金融行业的金融模式及服务模式都产生了巨大的冲击，迎着全新的机遇与挑战，金融业也做出了巨大的革新，金融业务系统入云已是大势所趋。

当前，中国工商银行（下文简称“工行”）已形成了以基础设施云、应用平台云、金融生态云以及具有工行特色的分行云四大组成部分的工行整体云平台架构。工行云平台技术栈采用了业界比较领先的云产品和主流开源技术，在此基础上结合一些典型的金融业务场景，进行了深度化定制。

基础设施云。基于云产品结合运营运维需求进行客户化定制，构建新一代基础设施云。

应用平台云。通过引入开源容器技术（Docker）、容器集群调度技术（Kubernetes）等，自主研发建设应用平台云。

上层应用方案。基于 HaProxy、Dubbo、ElasticSearch 等建立负载均衡、微服务、全息监控、日志中心等周边配套云生态。

在容器云方面，基于工行自主研发的云平台建设成效显著。首先体现在规模上，目前应用平台云容器规模已超 30 万，拥有业务容器约 70,000 个，同业规模领先，同时保证新增应用全面上云，核心业务也已 100%上云；其次是业务场景全覆盖，核心的银行业务系统，包括个人金融体系的账户、快捷支付、线上渠道、纪念币预约等，均已实现容器化部署；最后，新技术应用也积极接轨云化部署，如核心技术支撑类应用——MySQL 等数据库应用、Redis 等中间件、微服务框架，以及新技术领域，如物联网、人工智能、大数据等应用也均已入云。以下举四个典型案例分别阐述工行的云原生实践。

（1）多集群管理及容灾实践

随着核心业务应用入云规模持续扩张，工行面临最大的挑战是应用的容灾以及高可用，在这方面工行也做了许多积极探索。

云平台支持多层次故障保护机制，确保同一业务的不同实例会均衡分发到两地三中心的不同资源域，确保单个存储、单个集群甚至单个数据中心发生故障时，不会影响业务的整体可用性。

在故障情况下，云平台通过容器重启及自动漂移，实现故障的自动恢复。

但随着业务规模的扩大及大量异构集群的出现，工行目前的容器云集群规模已增长到一百余个，多集群场景下的管理和容灾的问题也逐渐凸显，通过容器云的多云管理平台已无法解决全部问题。**一是可用性受限，**PaaS 集群本身为故障域，缺少跨集群故障自动恢复机制。**二是资源调度受限，**应用容器自动调度及弹性伸缩局限于单集群内部。**三是集群不透明，**应用团队需要单独选择具体 PaaS 集群进行容器部署。

在此背景下，工行基于自身研发积累，积极参与社区共建多云管理项目，即采用云原生多云容器编排项目 Karmada（Kubernetes Armada 是一个 Kubernetes 的扩展管理系统），该项目为多集群管理将带来如下价值。

资源调度。基于自定义跨集群调度策略，对上层应用透明，支持两种资源绑定调度，实现两种关联对象协同调度。

容灾备份。支持动态绑定（Dynamic Binding）调整，对故障恢复和恢复后的流量负载有较大帮助，同时，支持按照集群标签或故障域自动分发资源对象。

集群管理。支持集群注册、全生命周期管理，并开放统一的、符合社区标准的应用程序编程接口（API）。

资源管理。支持 kubernetes 原生对象，当上层应用迁移到多云平台上时，无需修改代码，同时支持子集群资源部署状态获取，资源对象分发也支持“pull” “push”方式。

（2）MySQL 容器化实践

在传统环境下，MySQL 一般按照单实例单物理机的模式进行部署，随着数据库实例数量大幅攀升、服务器规模不断扩大，传统运维手段存在维护成本高，交付能力差等问题，难以应付大规模的环境交付。传统 MySQL 部署运维方式主要存在以下问题。

资源密度较低。与 ORACLE 相比，MySQL 数据库实例单体性能容量较小，一般在 500G 以下，数据量过大就需要进行分库处理，但是单物理机单实例的部署方式依然保持不变，大批数据量小的数据库系统单独部署，最终导致 MySQL 的服务器资源利用率偏低。

运维效率偏低。随着业务的发展，传统数据库扩容手段的时效性是个棘手的问题，目前，MySQL 一体化运维平台主要关注的 MySQL 层面的自动化运维，在服务器、存储、网络等基础设施环节的运维和交付仍然需要较多手工操作。

服务输出能力不足。MySQL 用户需要提交的环境设备申请单较为复杂，环境搭建完成后仍然需要通过邮件等方式通知用户环境信息。服务输出能力严重不足，对于 MySQL 最终用户来说，服务供给周期较长。

以上问题的解决思路是：研发相应的存储和网络插件，实现容器数据持久化，以及实现扁平化的容器网络，并基于 MySQL 运维支撑体系建设 MySQL 自服务平台，完善从基础设施到上层数据库全面的 MySQL 运维体系。通过 MySQL 容器化主要带来如下价值。

资源密度提升。容器化部署后，MySQL 数据库实例资源密度最大可提升 3 倍，节省数千台物理机资源，除此之外，还有网络交换机、光纤交换机等其他设备资源。

运维效率提升。基于 PaaS 平台实现设备、网络、存储，数据库多个专业方向的自动化串联，大大减少环节之间衔接的沟通工作，最终通过 MySQL 自服务平台实现 MySQL 数据库实例的一键式创建，监控、高可用、故障应急等 MySQL 专业运维工作都统一在运维平台下进行操作和自动化的实施。

服务输出能力提升。MySQL 的最终用户可以通过自服务平台自助化的创建立等可用的 MySQL 实例，同时可以在 MySQL 运行过程中可查看 MySQL 容器运行状态，并进行自助分析。

（3）基于 Operator 的实践

随着云平台技术的发展，越来越多的应用基于 Kubernetes 平台入 PaaS 云，实现容器化部署。容器化部署可以让应用享受一键搭建、一键伸缩、一键升级等红利，无状态应用的特性支持其在任意时刻进行部署、迁移、升级等操作，可以享受入 PaaS 云带来的快速上线、弹性扩容的红利。与无状态应用对应的有状态

的中间件应用，比如 Redis、ElasticSearch、Zookeeper 等，在容器化部署方面主要存在以下问题。

缺少通用入云框架支持。中间件应用入云在复杂编排部署、网络持久化和持久化存储方面存在诸多难点，需要通过框架层面解决。在编排部署方面较为复杂，不同类型节点启动和变更顺序有要求，且配置上存在依赖关系，如 Kafka 集群的 broker 节点需在 zookeeper 集群后启动，且需单独配置 zookeeper 集群的地址列表。此外，此类应用对存储具有持久化需求，需要在 Pod 内实现持久化存储，Pod 迁移或重启等情况下存储内容不能丢失。

缺少配套交付运维体系。缺少有状态服务入云框架，匹配个性化开发模式，配套交付、日志、监控等的标准化体系。

自服务能力不足。缺少应用自主配置、自助申请的企业级能力。

通过搭建基于 Operator 的中间件云平台即可解决上述问题，Operator 就是通过控制器和定制资源的机制，使 Kubernetes 不仅可以运维无状态应用，还可以执行由用户定义的运维能力，实现更复杂的自动化运维应用进行自动化部署和交互。基于 Operator 机制能够实现缓存、消息、数据库等容器化部署，实现有状态应用的快速供应，并利用云原生能力实现高可用的迁移和自愈。中间件云平台为工行的中间件部署带来如下价值。

打造 GPaaS 服务通用入云框架。一是自定义编排框架，基于 Operator 实现有状态应用各类节点依赖关系的编排，实现全生

命周期的运维管理。二是网络持久化，结合 Headless Service 和 StatefuleSet 的特性，实现节点访问地址不变。三是持久化存储，通过 StatefulSet 实现存储绑定关系持久化，容器宕机后存储可准确复原。

建立交付运维标准化体系。实现 GPaaS 服务编排引擎合作开发共建，对接行内 DevOps 标准交付体系及日志监控体系。

完善自服务能力。建设 GPaaS 门户实现上下游链路整合，支持服务自助配置和申请。

（4）Service Mesh 实践

微服务架构是当今互联网和金融机构渐趋主流的系统架构模式，其核心是集成服务通信、服务治理功能的服务框架，微服务框架在持续演进同时，服务网格作为一种新型的微服务架构，因架构灵活、普适性强，被认为具有较好发展前景。工行主动探索服务网格领域，从 2019 年开始服务网格技术预研工作，通过对服务网格技术深入研究和实践后，于 2021 年建设了服务网格平台。服务网格与现有微服务架构融合发展，助力工行应用架构向分布式、服务化转型，承载未来开放平台核心银行系统。

工行从 2015 年开启了 IT 架构转型工程，截止目前分布式体系已覆盖 240 余个关键应用，生产已有约 50 万个分布式服务节点，日均服务调用量超 110 亿，交易峰值逾 10 万吞吐量（TPS），逐步实现了超越主机性能容量的集群处理能力。工行分布式服务平台在稳定支撑已有业务系统的平稳运行同时，也存在一些业界

共性的挑战。一方面，存在非 Java 的异语言系统需分别实现对应的基础框架，同时维护多套框架成本较大。另一方面，多产品线下，各应用使用了不同版本的基础框架，推动各应用升级框架周期较长，生产并行运行多版本的基础框架，兼容压力较大。

为解决当前痛点，工行积极引入服务网格技术，探索解耦业务系统与基础设施，完善服务治理能力。工行服务网格平台集成了原有分布式体系的注册中心、服务监控等基础设施，将原服务框架客户端中最基础的通讯协议编解码能力以轻量级客户端的形式保留在业务系统中，其余服务框架客户端的能力均下沉至流量代理（Sidecar）中，可与服务框架兼容发展，平滑过渡。目前工行已完成服务网格平台的建设，在与分布式服务平台融合发展过程中，打通了异构语言系统的服务治理与监控体系，解耦了业务与中间件系统，丰富了流量治理能力，主要价值如下。

定制流量代理。分别针对异构系统与高频联机服务定制个性化 Sidecar，已满足异构系统的完全透明无侵入的接入能力，与保证性能的高频服务交易场景。

监控运维能力。服务网格平台内置了完善的监控与报警能力，支持向第三方监控系统上报服务监控、链路监控等监控指标；并具备根据单位时间内的业务请求异常率阈值的报警，且能在触发限流、熔断、降级、故障自愈等服务治理功能时，同步触发对应的报警事件。

服务治理能力。服务网格平台已具备细粒度的流量精准匹配能力，从流量身份标识角度识别特定标识的流量合集，并对这部分流量进行精准管控。平台现已支持（标签级/方法级/服务级/应用级）限流、熔断、降级、路由、流量镜像、链路加密、鉴权、故障演练、故障隔离等企业级的流量管控能力。

安全管控能力。服务网格平台已支持安全认证能力，支持国密及多种主流算法构建加密通道，实现更加安全的数据传输，以零信任网络的安全态度，实现全链路可信、加密；并能识别调用方身份标识，根据身份标识设置访问控制策略（黑/白名单）。在有多接入方的业务场景中，可预防个别客户系统故障或者恶意攻击，对异常客户实施黑名单管控，拒绝非法访问，保护本系统的可用性。

（5）基于 Serverless 函数计算实践

Serverless 作为云原生架构的重要组成部分，是最有潜力的云计算技术发展方向。通过 Serverless 技术，开发者只需关注业务逻辑而无需关注底层服务器等基础设置资源，从而提高开发者的研发效率和创新能力。

当前，工行已建立较为完备的云计算、分布式架构体系及容器云平台，分布式服务体系建设成效显著，已积累大量可复用的业务服务资产。同时也面临着诸如银行业务处理线上化和自助化的绝对数量和占比持续提升，大量业务系统需要进行改造；商业

银行竞争加剧及互联网企业的跨界渗透，要求银行信息系统必须满足快速创新需要等挑战。

为解决当前痛点，基于 Serverless 高效弹性伸缩、免运维管理、快速上线等技术优势，工行于 2018 年完成自研可提供无服务容器（Serverless container）能力的 Serverless1.0 平台，并于 2020 年建设完成 Serverless 2.0 函数计算平台，结合工行各分布式服务，适配工行金融技术架构和业务场景，提供函数管理、应用管理、事件管理、工作流管理、发布管理和日志监控等能力，覆盖函数的开发测试、运维监控全链路环节。目前 Serverless 函数计算平台已完成包括分布式批量任务、应用后端服务、AI 模型发布等多个业务场景落地试点，通过业务实践，总结函数计算主要价值如下。

弹性伸缩。当业务有较明显的高峰和低谷，或者业务有临时的容量需求时，通过 Serverless 函数计算可高速且稳定地实现自动弹性扩容以应对峰值压力。

降低成本。仅当请求发生时，应用程序实例才会被加载执行，空闲时应用程序实例会被停止和卸载，不会持续在线占用资源，从而实现按需使用。同时平台提供监控、日志、负载均衡等统一运维能力，可降低应用运维成本。

快速上线。开发者只需专注业务逻辑开发，可显著提高开发者生产力；应用的功能被拆解为若干个细粒度无状态函数，可提升开发效率，同时迭代周期变短可加快应用交付速度。

推进创新。对于实验性的工作，如 AI 模型部署，无需提前准备底层基础设施，部署成本低，同时可快速验证开发应用程序的有效性，有利于创新发展。

2.华夏银行全栈云原生实践

2015 年，华夏银行与华为成立联合创新实验室，先后在云计算、大数据、5G 等八大领域开展创新合作，并取得业界多项成果，包括首个云网协同金融云、业界首个全栈鲲鹏容器云等。华夏银行自 2017 年与华为共同打造华夏金融私有云，逐步构建了多生态的“全链条可信云”，支撑了移动营销经理 APP、微信银行等业务的发展。2020 年，为进一步加速业务和科技融合，支撑数字化转型业务创新，华夏银行将可信云升级为混合云模式，为未来产业云的进一步建设提供了架构以及技术储备。华夏银行多生态全链条可信云原生架构平台技术特点主要体现在如下四个方面。

（1）全栈业务承载及云原生架构演进。既支持传统业务的云化转型，又支持基于云原生应用的业务创新；硬件上支持小型机、Intel x86、ARM 架构泰山服务器等多类型设备的管理，资源层支持 KVM（Kernel-Based Virtual Machine）、VMware、容器等多类型资源池的管理，以及多样操作系统、中间件、分布式数据库、数仓、大数据服务等能力，还可提供全栈云原生基础设施服务能力支持新业务的探索。

（2）标准、开放、完整的“云原生应用生态”。通过搭建云原生应用市场，联合行内各部门、ISV 及金融行业，统一发布和运维兼容业界应用标准 Operator/Helm 的中间件，可支持各类应用根据业务创新需要混合搭配。

（3）全行“一朵云”视角，容器跨云统一管理。按照用户逻辑构建“一横三纵二平台”，包括总分行、集团、产业三大用户群，以及业务使能和数据使能两大应用平台。支持跨云、跨区域的容器集群管理，实现全局统一应用管理，轻松解决业务异地容灾、高峰跨云弹性等容器调度问题；支持应用服务网格，应用无侵入、多语言服务治理。

（4）以应用为中心的“云原生基础设施”。依托华为云全栈金融云平台，基于业界稳定成熟、性能先进的 Docker、Kubernetes 等技术，以及 Istio 服务网格框架，结合华夏银行自研的云原生应用开发平台以及 DevOps 流水线，实现从“以资源为中心”向“以应用为中心”管理方式的转变。

华夏银行在线类业务，在面对访问量峰值、秒杀场景时，基于采用的云原生架构，可快速完成资源弹性扩容。新架构上线后，开发运维效率大大提高，迭代频率缩短为 1 周 1 次，产品上线时间从原来的 2 小时降低 5 分钟，同时故障数减少 90%，资源利用率提升超过 20%。华夏全栈云作为国内银行业较早支持“全栈自主可控+云原生架构”的云平台，在业内颇具示范意义。基于云

原生的技术，通过全面云化、全栈智能，实现无处不在、多元化、全场景的金融服务。

3. 中信银行全栈云原生实践

2021 年，中信银行全面启动技术自主可控的金融全栈云建设，将公有云的关键技术栈全面私有化部署，实现全面的云原生技术革新。该项目是中信银行十四五期间重点项目，居中信集团十大科技创新项目之首。为保证全栈云原生工程的成功，打造全生态的云原生架构，中信银行在以下几个方面进行重点攻关。

（1）落地和适配公有云体系架构

在全栈云规划阶段，中信银行规划了开发测试云、生产云、子公司云和生态云。目标是所有业务系统能够运行在全栈云上，从而支撑银行数字化转型和业务高速发展，同时具备支撑银行所有子公司、中信集团所有子公司和海量外部生态客户的能力。但是，全栈云技术架构和云原生体系在金融行业落地的普遍面临难题。一方面是其来源于采用先进的公有云的全栈云技术框架，拥有丰富的云服务，但在私有云环境落地时，其基于海量小租户设计的出发点和银行单一租户的特点出现冲突。另一方面是其 IP 不固定以及通过软件控制的设计思路，往往与银行强调规划、强调严格管理的理念出现矛盾。

中信银行在充分理解全栈云技术体系的基础上，与华为联合攻关，进行多层次的高可用设计和高扩展性设计，将云原生技术的灵活性和金融行业的运维特点相结合，全面落地了全栈云方案，并完成了金融特性适配改造。为了实现大规模部署，项目团队设计了多 Region、多地多中心部署、双可用区部署的全方位立体化模式，保证金融级的高可用性；实现了支撑应用双活部署的云内云外协同 DNS、跨中心软件 SDN 互联、NAS 跨 region 共享方案；根据万台服务器规模，设计了高扩展性的多机房网络互联、多 VPC 虚拟网络、多集群扩展的部署模型；针对金融监管要求，设计了多 VDC、多租户、多主机组隔离的资源隔离模型，在符合监管要求下，灵活、弹性的支持总行、分行、子公司的业务上云。

（2）打造高性能、敏捷弹性的云原生架构

由于银行交易本质的要求，需要保证端到端的高性能、低时延、高并发，中信银行在全栈云建设中，100%使用安全可控的软硬件技术，打造了高性能、低时延、敏捷弹性的云原生平台。

高性能算力。全部采用高端的鲲鹏服务器，承载两路高端芯片和高性能网卡，提供超高性能计算能力，作为容器等云原生应用的算力；采用配备高性能 SSD 盘、海量容量的分布式存储，作为云原生应用数据持久化的载体；采用 25G 芯片网络设备，实现

低时延、高带宽的网络架构。充分发挥芯片硬件的性能优势，为云原生提供强大的算力。

敏捷弹性的云原生网络。容器网络和底层 IaaS 网络彻底融合，统一由软件定义网络管理和维护，摈弃了早期的隧道模式，容器网络直接采用 IaaS 网络技术栈，POD 的 IP 地址对外暴露，高效地与外界互通，与 Service Mesh 服务网格无缝对接。融合网络技术栈提升云原生网络性能高达 30%以上，实现云原生环境下真正的云网联动。

全联通的云原生网络。将软件 SDN 技术和硬件云专线技术，软件防火墙和硬件防火墙技术相结合,实现了跨 VPC、跨可用区、跨机房、跨数据中心、跨云的网络互通，同时实现了云原生网络与云外网络的互通，为业务高性能互联互通提供基石。

（3）实现全面、全栈、安全的云原生

中信银行将基础设施领域的云计算技术升级,并与开发领域的技术中台、业务中台、数据中台的技术架构改造相结合，实现将全栈云 IaaS、PaaS 全栈技术一体化部署，建成了符合金融安全标准的云原生平台。

中信银行以华为全栈云容器引擎作为云原生的基础平台，对接制品库和容器安全平台，打造适合金融场景的海量镜像仓库，为业务创新和技术改造提供源源动力；通过 Service Mesh 构建

敏捷的应用服务网格框架，实现跨系统的服务治理，把存量应用和云原生的应用有机整合，实现应用生态的融合；通过华为容器引擎对接自研 DevOps 开发流水线，实现了高效的持续集成；通过容器引擎与 GPU 结合，为人工智能业务提供强大算力；通过将容器引擎和中信自研的乐高等新型开发平台相集成，构建云原生的技术中台。

（4）为云原生的规模使用保驾护航

全栈云是一个体系庞大的产品体系，在金融行业强监管的环境下，运维是一个行业难题，中信银行通过自主研发，实现全栈云与行内系统全方位对接，构建了包含技术规范、制度、流程、运维工具在内的运维管理体系，使用严格的流程管控，符合监管要求，实现了敏捷性和安全性的平衡。

全流程敏捷。通过自主研发的数字化运维 PaaS 中台，实现了自动化变更、自动化运维以及开发、测试、生产环境的敏捷服务。

严格的流程管控。将全栈云的开发、测试、上线、运行、下线等全生命周期纳入流程管控体系，使用了严格的流程管控，符合监管要求，实现了灵活性和安全性的平衡。

全量的用户管控。全栈云用户众多、关系复杂，涉及操作系统、应用、存储、运维、运营等多种用户。通过技术攻关，将用

户统一接入行内堡垒机，对用户统一管控。并自建日常管理用户，实现对全栈云环境全天候的监控和运维。

全量域名管理。域名是应用互联互通的重要途径，如何统一管理全栈云内部域名和业务域名，如何管控云内 DNS 和云外 DNS 是运维的关键难题之一。中信银行的域名 DNS 解析方案，实现了云内、云外联动，统一管理和解析，可与现有生产系统无缝集成。

监控 360 度无死角。自行开发对接程序，将全栈云所有监控统一管控，兼容 SNMP，AOM，kafka 等形式，覆盖 IaaS、PaaS、软件、硬件等，实现无死角监控。

（二）证券公司金融平台建设实践

广发证券一直以来走自研路线，在 2014 年 Docker 等容器技术尚未盛行之时开始投入容器化技术的研究，并于 2015 年开始大规模投入应用，行情、资讯、广发通、消息推送、自选股、统一认证、实时事件处理等核心业务都已生产容器化。随着业务和技术的不断发展，广发证券架构也需要不断升级和创新。一是把 Docker、容器编排管理等技术深度整合到交易系统中，使其获得自伸缩、自监控、自修复的自动化能力。二是实现 Helm 和 Operator 主流的云原生服务管理标准，从而构建云原生服务生态。三是大规模服务实例管理，完成服务流量治理和流量监控。四是加速推进全面安全可控。

目前广发证券借助云原生 2.0，逐步将公司网站、员工服务平台等内部管理系统基于云原生架构进行升级改造。在此基础上创建和管理多样化的容器工作负载，并具备容器故障自愈、监控日志采集、自动弹性扩容等高效运维能力，从而完善应用生命周期管理能力和自动扩缩容机制，提升运维效率；同时通过 CI/CD 流水线，快速在研发/测试/生产环境间分发、部署、上线，提升部署效率。云原生 2.0 技术还提供开箱即用的应用服务网格流量治理能力，客户无需修改代码即可实现灰度发布、流量治理和流量监控能力，进一步简化微服务的管理，提升了应用的可靠性和可监控性。同时广发证券借助云原生的异构能力，构建鲲鹏、海光等多异构底层能力，满足应用从 X86 到 ARM 无缝切换，实现全栈安全可控。

（三）证券交易所数字化转型实践

深圳证券交易所（以下简称深交所）目前建成近 300 个系统，覆盖核心交易系统、业务管理系统、市场实时监察和信息服务系统等主要领域。经过多年发展，深交所技术架构也在持续的创新和转型，转型的动力主要来自于三大驱动。一是市场在产品与制度创新、产品快速迭代等方面给技术带来了需求和压力；二是行业监管和系统安全的需求也要求系统技术架构向更稳定、更可靠、可安全方向进行转型；三是以云计算、大数据、人工智能为代表的新技术发展也要求技术架构不断进行更新。

首先，深交所构建了基于容器的高效云原生基础设施，为应用提供可定制的模块化资源，同时以 API 形式开放基础设施的各项能力，通过一个统一的平台来满足不同应用在性能、成本、可靠性等关键指标方面的差异化需求，提升了基础设施的自动化运维程度以及资源使用率。深交所云原生基础资源设施主要基于高性能云容器引擎构建，与原生 kubernetes 相比，资源损耗更小，调度效率更高；在容器网络方面，深交所采用 3 层网络 BGP 路由方案，以满足安全隔离要求，同时集成 SDN 设备，构建保障性更高、性能更好的网络资源平台；在存储方面，容器存储支持块存储、对象存储、文件存储等不同类型，通过基础设施平台统一构建融合存储平台，满足应用的需求。该设计大幅提升了基础设施的性能和利用率、降低了成本，提升了用户的体验。

其次，深交所建立了统一的计算、存储资源池，通过容器引擎统一管理，可进行更细粒度资源配额调配，比如可实现 CPU、内存、GPU 等计算资源的动态调配，资源利用率和分配效率得到显著提高，并实现了算力的灵活调度和弹性扩容。

最后，深交所以应用为中心再升级应用架构，本质是云原生基础设施带来了应用架构的模式转变。传统模式是以基础设施为主体，根据基础设施容量分配额定资源去部署有限应用进行运行，而现在以应用为中心定义基础设施，根据应用需求分配基础设施资源，例如计算资源、网络资源、存储资源等。同时应用架构升级成更为轻量无状态的微服务，这样不仅可保证应用弹性伸缩能

力及快速部署、快速迭代，还可结合微服务的全方位治理能力，实现灰度发布、多版本并行、链路跟踪、限流熔断、自动化测试等能力。

目前，深交所各类应用已陆续基于上述云原生架构进行升级改造。以新 OA 系统为例，最初以烟囱模式开发，各个子系统之间关联性较低，随后进行了服务化改造，将业务逻辑以服务方式提供，形成一定规模的复用。再后升级成为微服务架构，并运行在云原生基础设施上，可以实现 OA 系统的高效部署和弹性伸缩，并具备灰度发布、熔断限流、链路监控等能力，从而提升了 OA 系统的交付效率。

（四）保险公司核心业务系统建设实践

永安保险经过多年的 IT 建设，目前已有超 200 个 IT 系统，这些系统主分为四大类，第一类是核心业务类系统，第二类是渠道业务与服务类系统，第三类是数据分析类系统，第四类是公共基础类系统。近年来新的保险业务生态正在形成，互联网保险与新兴渠道模式是新保险业务生态的重要组成部分，一方面监管要求保险姓保，另一方面业务要求科技创新助力保险业务创新。在此大环境下，永安保险正全力推进基于保险新生态下的 IT 建设，其中基于云原生实施的意健险核心业务系统是其中重要的项目之一，此项目于 2020 年 2 月和 5 月分两批次成功上线，主要有如下特点。

1.在核心业务系统方面。全面覆盖并标准化保险业务与服务场景，使永安保险在与客户和渠道的互融互动，能力对接方面更快捷可控，充分体现保险场景分享，同时结合云原生的一系列能力，帮助永安保险公司提高保险生态数字化转型能力。

2.在业务先性方面。满足意健险销售与服务全流程业务；多组合，实现产品组合出单，具备可扩展其他险类产品能力；支持多渠道的服务方式、满足渠道快速接入(包括 B2B 代理渠道出单、API 快速对接、H5 扫码出单等)；产品配置引擎，支持产品快速上线。

3.在技术先进性方面。基于云原生环境部署并使用云服务组件，如容器、服务网格、分布式缓存与消息队列、微服务框架与监控、前后端分离技术与 H5（跨设备、浏览器）、搜索引擎与读写分离等；基于云原生数据库 GaussDB(for MySQL)实现了主流商业数据库 Oracle 至 GaussDB 的安全切换。

立足云原生全栈能力，意健险核心业务系统可有效应对流量高峰场景下性能和可靠性的问题。在海量数据高并发场景下仍然可以保持数据库超高性能，确保系统数据不丢失，支持跨 AZ 部署，故障恢复时间短（10s），业务连续性程度得到大幅提升，实现 RPO（数据恢复点目标）为 0、RTO（恢复时间目标）秒级，不仅满足了金融监管要求，还降低了数据库运维压力，且整体资源投入节省 25%，大幅提升了业务运转效率，为永安保险数字化转型打下坚实的云上核心分布式架构和数据底座基础。永安保险意

健险核心业务系统主要基于云原生能力构建，支持性能自动扩展，系统运行稳定，用户体验良好，使得传统 IT 架构存在的问题得到解决，技术创新助力业务创新落到了实处。

（五）科技公司系统建设实践

深圳市金证科技股份有限公司（以下简称金证）使用的核心交易系统均采用上一代标准四层集中式系统架构，由于架构中账户、资金、交易、清算等业务功能模块之间存在强耦合关系。一方面，创新业务越来越多，核心业务系统不断增加，这种堆叠式发展构建，使得功能和数据冗余，给业务创新和系统运维带来很多困扰；另一方面，近十多年来，核心系统的技术架构并没有本质化的改变，仍然是单体的多层技术架构，这给系统扩容、定制开发等带来很多限制。基于此，金证开发了基于云原生业务系统，如图 2 所示。

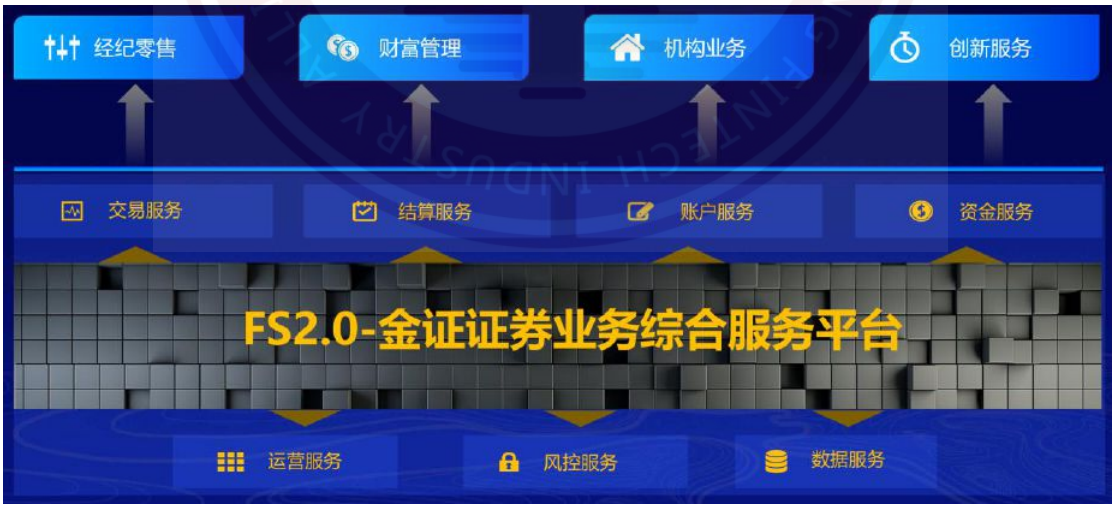

图 2 基于云原生的券商全业务核心底座 FS2.0

FS2.0 根据“领域驱动建模”(DDD)的指导思想，按照功能和场景划分，独立成一组组互不干扰的服务，服务内高度自治，服务之间高度解耦。系统内部，依托 KOCA 平台的服务治理能力，对各个服务进行监控和集中管理；系统外部，通过网关对外呈现标准统一的接口，供外围系统进行互联互通，如图 3 所示。

图 3 “开放、标准、融合”证券交易结算基建系统建设新标杆

金证在研发新一代核心业务系统的过程中，始终秉承分布式的架构思想进行构建和实践，结合当前及未来在业务和技术方面的发展，在业务、技术、运维、开发等方面做了综合考量。以 KOCA 云原生技术平台为技术底座，以 FS2.0-金证综合业务综合服务平台为应用底座，基于交易与清算分离、账户与资金分离、交易服务与通道分离，以及运营整合、接入整合、数据整合、后台服务整合的“三分离、四整合”的设计理念，以“稳态”与“敏态”相分离为设计原则，对交易业务进行纵向解耦，将“稳态”的订单系统和报盘系统和“敏态”的交易服务中台和专业交易终端进

行解耦，构建了具备高可用、高性能、易扩展等特点券商新一代核心业务系统，取得市场的一致认可。