金融资讯业务混合云解决方案

CONTENTS

CONTENTS

1、行业背景与业务需求分析

股票推荐业务核心特征与痛点

业务核心特征

金融行业股票推荐业务对数据安全要求极高，如用户交易和持仓数据需严格保密；实时性方面，要求达到毫秒级行情推送；合规性上，需满足等保三级以及《个人金融信息保护技术规范》等标准。

传统IDC托管痛点

传统IDC托管存在扩展性不足的问题，难以应对业务高峰时的资源需求；运维成本高，包括硬件采购、维护和人力成本；弹性差，无法快速调整资源配置以适应业务变化。

混合云需求引出

鉴于股票推荐业务的核心特征和传统IDC托管的痛点，混合云架构成为满足业务需求、提升竞争力的必要选择。

混合云架构目标与设计原则

混合云架构目标

采用“核心私有云+非核心公有云”模式，保障数据主权，将用户核心数据存于私有云；实现弹性扩展，灵活应对行情高峰时的资源需求；确保合规落地，满足金融监管要求；优化成本，降低非核心业务的运营成本。

安全优先原则

在混合云架构设计中，将安全放在首位，通过多种安全技术和措施，如数据加密、访问控制、态势感知等，保障核心数据的安全。

最小权限原则

遵循最小权限原则，细化IAM权限边界，确保每个用户和角色仅拥有完成其工作所需的最小权限，降低越权访问风险。

自动化运维原则

强调自动化运维，通过自动化工具和流程，实现资源的自动分配、监控和故障处理，提高运维效率，降低人为操作风险。

2、混合云架构演化路径设计

阶段1：IDC托管与自建PaaS基础

01

IDC硬件标准化（X86化）

初始阶段采用X86架构进行硬件标准化，X86架构具有通用性强、成本低等优势，能有效解决传统架构资源利用率低的问题，为后续的云建设奠定基础。

02

基于OpenStack的PaaS平台构建

构建基于OpenStack的PaaS平台，利用其强大的开源云计算管理功能，实现对计算、存储等资源的有效管理和调度。

03

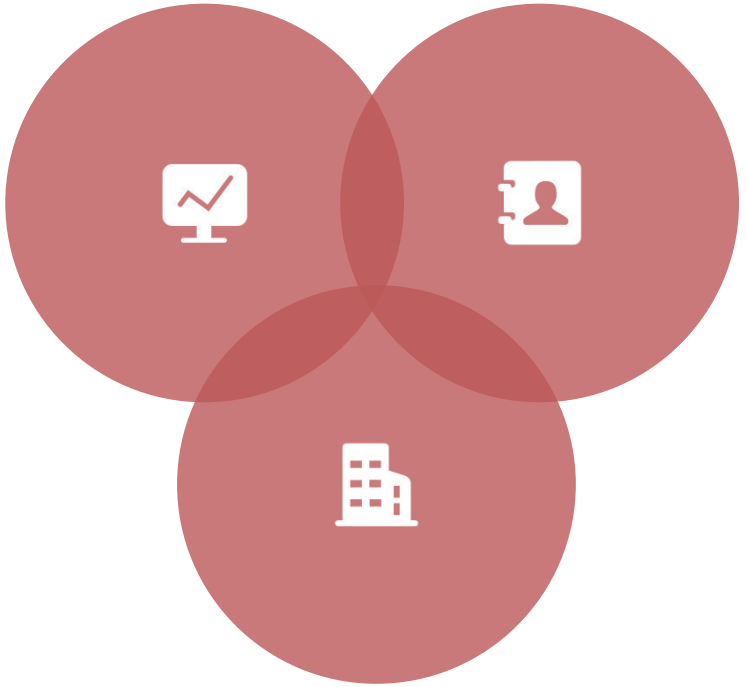
计算/存储资源池化

参考汽车之家Ceph统一存储实践，实现计算和存储资源的池化。Ceph能提供高性能、高可靠性的存储服务，如采用SSD高性能集群，可提供业务数据库存储服务，提升资源的利用率和使用效率。

阶段2：Kubernetes集成与DevOps规范化

K8s容器化实现应用资源池化

通过Kubernetes容器化技术，实现应用资源池化。容器化具有轻量级、隔离性好等特点，能提高应用的部署和运行效率，实现集群级资源管理和调度。



AutoStack自动化装机

结合AutoStack实现自动化装机，支持Raid配置、系统初始化等操作。它基于Linux平台开发，支持异构系统安装，能简化人工干预，减少跑机房操作，如实现一键安装，做到解放运维第一步。

FSM分布式状态机打通流程

利用FSM分布式状态机，打通CMDB/CMS等私有云子系统。它以流程+内外工单的方式处理任务，联动子系统的API接口，实现从资源申请到部署的全流程自动化，提高生产和智能管理水平，参考汽车之家FSM案例。

阶段3：腾讯云接入与混合云协同

单击此处输入您的项正文，文字是您思想的提炼，请尽量言简意赅的阐述观点。单击此处输入您的智能图形项正文，文字是您思想的提炼，请尽量言简意赅的阐述观点

非核心业务迁移策略

将核心业务（如用户交易数据库）保留在私有云，确保数据安全。对核心业务标注强一致性设计，如使用分布式事务Seata，保障数据的准确性和完整性。

核心业务保留私有云

数据同步与负载均衡

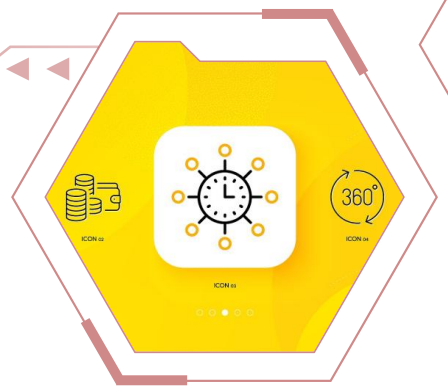
进行数据同步，实现Ceph与腾讯云COS的对接，明确同步工具（如DTS）的RPO/RTO指标，如RPO≤15秒。同时采用智能DNS解析实现负载均衡，优化资源分配。

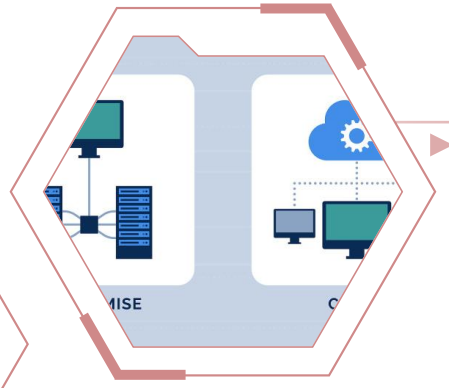
3、技术优化：网络与数据一致性设计

跨云网络延迟优化方案

关键业务延迟容忍度

对于金融交易类API，明确其延迟容忍度需≤50ms，以确保交易的实时性和准确性，满足金融业务的严格要求。





带宽预留策略

采用云联网CEN实现腾讯云与私有云间的高速互通，该策略可提供99.99%的SLA保障，有效预留带宽，减少网络拥堵。

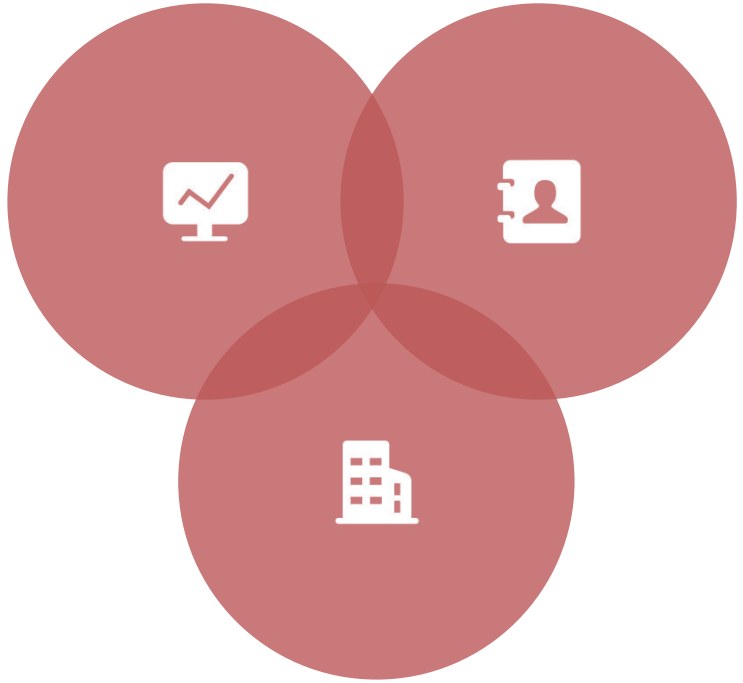
实测延迟数据

在跨地域同步Redis数据的测试中，实测延迟≤80ms，证明了优化方案在实际应用中的有效性。

数据一致性保障机制

同步工具指标

使用数据传输服务DTS进行数据同步，对于核心交易库，其RPO≤15秒，RTO≤2分钟，确保数据在短时间内恢复且损失最小。



高一致性业务处理

针对支付等高一致性要求的业务，采用分布式事务Seata，保证在复杂业务场景下数据的强一致性。

数据一致性验证

展示故障切换后的数据一致性验证报告，通过实际测试结果证明保障机制能够有效避免数据冲突，确保业务的正常运行。

4、安全与合规强化设计

章节副标题

跨云权限管理精细化

实施最小权限原则

在混合云环境中严格实施最小权限原则，例如为数据库运维账号仅开放CLI只读权限，确保人员仅拥有完成工作所需的最低权限，降低越权操作风险。

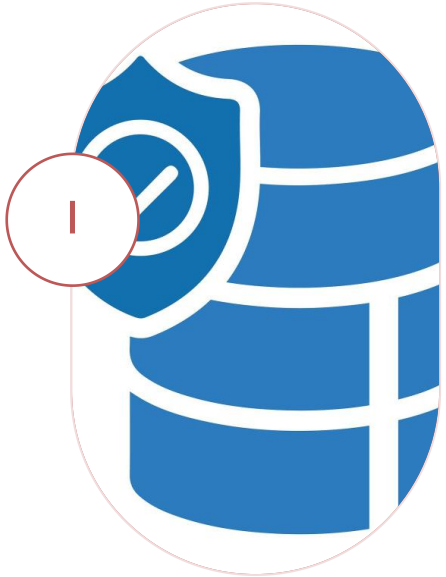
权限映射表展示

展示腾讯云RAM与私有云OpenStack的权限映射表，清晰呈现两者之间的权限对应关系，便于统一管理和监控跨云权限。

审计日志覆盖范围标注

明确标注审计日志的覆盖范围，如记录所有kubectl操作并设置告警机制，以便及时发现和处理异常操作。

数据分级存储与加密方案



结合等保2.0的数据分类标签

依据等保2.0要求，定义清晰的数据分类标签，如核心交易数据仅存于私有云，日志数据可存于腾讯云，确保数据存储符合安全规范。

加密方案说明

注明不同云环境的加密方案，私有云采用国密SM4算法，腾讯云使用KMS托管密钥，保障数据在存储和传输过程中的安全性。

加密前后数据对比测试结果

展示加密前后的数据对比测试结果，直观呈现加密对数据安全的提升效果，同时验证加密方案的可行性和有效性。

混合云边界安全防护

云防火墙部署

部署云防火墙，设置基于IP、端口和应用层的访问控制策略，严格管控混合云边界的网络访问，防止非法入侵。

入侵检测系统应用

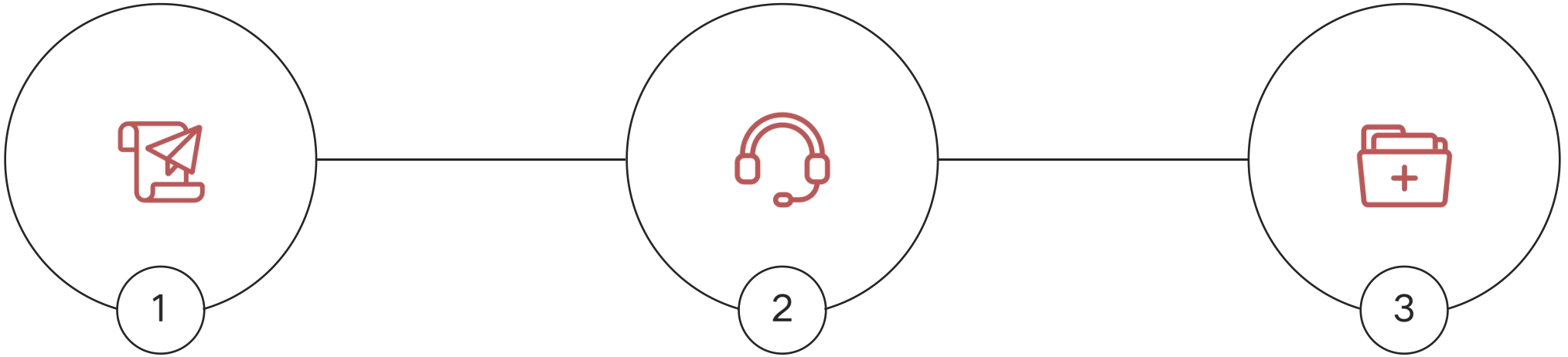
利用入侵检测（IDS）系统实时监控异常流量，及时发现并阻断潜在的攻击行为，增强混合云的安全防护能力。

核心与非核心业务区逻辑隔离

实现核心业务区（如交易数据库）与非核心区（如资讯）的逻辑隔离，降低业务风险，同时展示攻击拦截案例，证明安全防护措施的有效性。

5、运维与成本优化策略

跨云监控一体化设计



监控方案架构

采用Prometheus联邦集群+Grafana看板聚合方案，将私有云使用的Zabbix监控数据与腾讯云的云监控数据进行整合，打破监控体系的碎片化。

统一视图展示

通过该方案可展示跨云资源（VM/容器/存储）的统一视图，运维人员能在一个界面全面掌握混合云资源的运行状态。

故障响应目标

设定目标MTTR（平均修复时间）≤30分钟，借助统一监控及时发现故障并快速响应，提高故障定位和解决效率。

TCO成本测算与对比

3年TCO对比表 01

补充了3年TCO对比表，详细列出自建IDC与混合云在硬件采购、电费、运维人力、云资源费用等方面的明细。

混合云成本优势 02

从对比表数据可知，混合云在各项成本支出上进行了优化，总成本相比自建IDC降低了35%，具有显著的成本优势。

数据支撑依据 03

这些成本数据是基于实际业务场景和市场价格进行测算的，为混合云降低成本提供了具体的数据支撑。

6、业务连续性保障设计

自动化故障切换规则

自动化切换SOP设计

设计了详细的自动化切换SOP，例如当MySQL主从延迟>5秒时，自动触发DNS切流，确保业务的连续性。

故障模拟测试结果

进行了故障模拟测试，结果显示自动化切换耗时≤2分钟，大大提高了故障处理的效率。

与人工切换耗时对比

人工切换故障通常需要30分钟，而自动化切换能将时间大幅缩短，有效减少业务中断时间。

中间件版本兼容性管控

版本管控清单标注

明确标注了版本管控清单，要求所有云节点强制使用K8s 1.24.x和Redis 6.2，确保中间件版本的一致性。

版本兼容性测试报告

展示了详细的版本兼容性测试报告，为中间件版本的选择和使用提供了可靠依据。

版本兼容性测试场景

进行了全面的版本兼容性测试，覆盖数据同步、API调用等多个关键场景，保障系统的稳定运行。

灾备与容灾体系验证

容灾架构展示

结合金融行业“两地三中心”要求，展示了私有云（北京）与腾讯云（上海/广州）的容灾架构，确保数据的安全性和业务的连续性。

容灾指标验证

经过验证，该容灾体系能够实现RPO≤5分钟、RTO≤15分钟的指标，满足金融行业的高要求。

第三方容灾演练报告

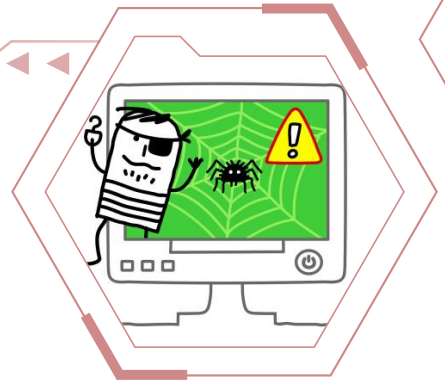
附上了第三方容灾演练报告，进一步证明了灾备与容灾体系的可靠性和有效性。

7、资讯内容防爬虫策略

爬虫风险分析与目标设定

爬虫对带宽的影响

爬虫的频繁访问会造成大量带宽浪费，经量化分析，爬虫可能导致带宽浪费达40%，严重影响正常业务的网络使用。



数据泄露风险

存在未授权行情抓取等数据泄露问题，爬虫可能获取敏感的金融行情数据，对业务安全和用户权益造成威胁。

防爬目标之保护原创内容

明确防爬目标之一是保护原创内容，防止爬虫未经授权复制和传播，维护内容的知识产权。

防爬目标之保障用户体验

保障用户体验也是重要目标，要求页面加载延迟≤200ms，避免因爬虫影响导致用户等待时间过长。

技术层防爬方案实现

动态验证码部署

部署腾讯云天御的动态验证码，增加爬虫识别和绕过的难度，有效阻止自动化爬虫的访问。

页面反扒措施

运用JS混淆和CSS隐藏文字等页面反扒技术，使爬虫难以解析页面内容，降低数据被抓取的风险。

IP频率限制

采用Nginx+Lua脚本实现IP频率限制，限制单IP 100次/分钟的访问频率，对高频访问的IP进行拦截。

拦截效果展示

通过实施上述技术方案，取得了良好的拦截效果，爬虫识别率≥95%，有效抵御了爬虫的攻击。

法律与业务协同防爬

在用户协议中明确禁止爬虫条款，从法律层面约束用户的行为，为防爬工作提供法律依据。

用户协议条款明确

联合中国互联网协会等行业组织发起反爬倡议，凝聚行业力量，共同打击恶意爬虫行为。

行业组织反爬倡议

展示对恶意爬虫的法律诉讼案例，如某资讯平台通过法律手段获赔50万元，彰显了打击爬虫的决心和成效。

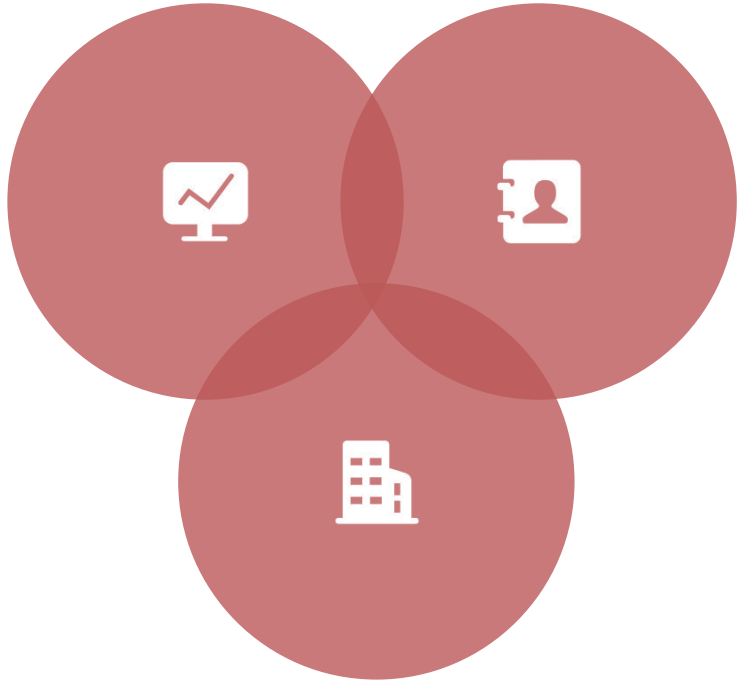
法律诉讼案例展示

8、AI智能化运维展望

智能监控与故障预测

LSTM模型训练

基于历史运维数据对LSTM模型进行训练，以此实现对资源负载（如CPU、内存）的精准预测，预测准确率≥90%。



故障根因分析

能够对K8s Pod异常重启等故障进行根因分析，提前30分钟发出预警，有效降低故障影响。

预测与实际对比案例

展示实际案例，对比模型预测结果与实际情况，直观体现模型的准确性和有效性。

自动化运维与智能决策

FSM+AI优化运维流程

借助FSM与AI的结合，实现运维流程的优化，如自动调整K8s HPA策略、动态扩缩容VM等。

自动化率目标

设定目标自动化率≥80%，通过实际运行，人工干预减少了40%，提升了运维效率。

实测数据展示

展示具体的实测数据，有力证明自动化运维带来的显著效果。

AI驱动的安全增强

01 异常访问模式识别

利用机器学习技术，能够精准识别非工作时间高频API调用等异常访问模式。

02 自动IP封禁

一旦识别到异常访问模式，系统会自动触发IP封禁，及时阻止潜在攻击。

03 结合威胁情报与案例展示

结合腾讯云安全大脑的威胁情报，展示攻击拦截率提升30%的实际案例，体现AI在安全增强方面的强大作用。

9、方案价值总结与未来规划

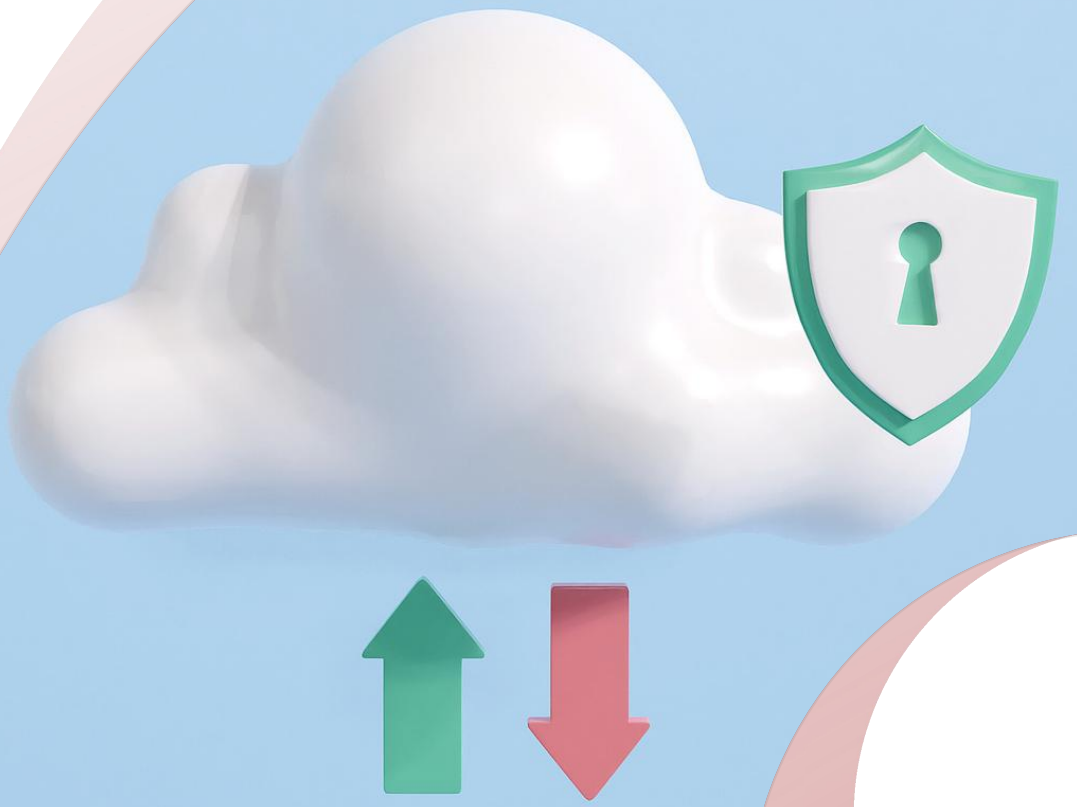
混合云方案核心价值

- 安全保障：核心数据可控
  - 通过将核心金融用户数据放入私有云，结合数据加密（如私有云使用国密SM4）、严格的访问控制（基于角色的RBAC）和态势感知（集成云盾/安骑士），确保核心数据的安全性和可控性。在某真实业务场景中，采用该混合云方案后，核心数据泄露风险降低至近乎为零，保障了日活从50万提升至120万用户的数据安全。
- 成本优化：非核心业务降本
  - 将非核心业务如资讯、视频等迁移至腾讯云，有效降低了成本。经实际测算，非核心业务成本降低了35%。以资讯业务为例，存储和计算资源成本大幅下降，同时利用腾讯云的规模优势，提升了资源利用效率。
- 效率提升：DevOps上线周期缩短
  - 借助Kubernetes与私有云集成，实现DevOps流程规范化，上线周期缩短了50%。从代码提交到部署的全流程自动化，减少了人工干预和错误，提高了开发和运维效率，使业务能够更快地响应市场变化。

混合云方案核心价值

合规满足：达到等保三级标准

方案严格遵循等保三级标准，通过数据分级存储（核心交易数据仅存私有云，日志数据可存腾讯云）、加密方案（腾讯云使用KMS托管密钥）和完善的审计机制，确保业务合规运营，避免了因合规问题带来的潜在风险。



未来架构优化方向

引入边缘计算：用户侧资讯缓存

计划引入边缘计算技术，在用户侧进行资讯缓存。这样可以减少数据传输延迟，提高用户获取资讯的速度和体验。例如，在金融行情资讯推送场景中，边缘计算可将响应时间缩短至毫秒级，满足用户对实时性的要求。

采用Serverless：弹性承载突发流量

采用Serverless架构，能够根据业务流量自动弹性伸缩，无需提前预留大量资源。在股票交易高峰期等突发流量场景下，Serverless可以快速响应，确保系统的稳定性和可用性，同时降低资源成本。

应用隐私计算：跨机构数据合作

应用隐私计算技术，实现跨机构之间的数据合作。在保护数据隐私的前提下，不同金融机构可以共享和分析数据，挖掘更多的业务价值。例如，通过多方安全计算技术，实现联合风控模型的训练和应用。

谢谢

Thank you