THE FORELAND OF
TRADING TECHNOLOGY

内部资料 免费交流
《准印证》编号沪（K）0671

交易技术前沿

2020年 第四期 总第41期

本期主题
架构探索

No.4

上海证券交易所 SHANGHAI STOCK EXCHANGE
ITRDC 证券信息技术研究发展中心（上海）

内部资料 2020 年第四期（总第 41 期）
准印证号：沪（K）0671

NO.4

主管：上海证券交易所
主办：上交所技术有限责任公司
总编：黄红元
副总编：徐毅林
执行主编：王泊
责任编辑：黄俊杰、徐丹、郭望

上海市浦东南路 528 号
邮编：200120
电话：021-68607128, 021-68607131
传真：021-68813188
投稿邮箱：ftt.editor@sse.com.cn

扫码阅览历期杂志

篇首语

信息系统的基础架构是金融机构业务运行的基石。随着数字化转型的深入，金融科技取代传统模式，业务功能不断丰富，开发运营压力也同步增大。在外部的技术突破，内生的转型需求压力下，信息系统正在向敏捷、灵活、高效、安全的架构转型。本期《交易技术前沿》以“架构探索”为主题，收录来自行业十二篇优秀文章，探讨行业技术前沿。

《新一代分布式核心交易系统解耦之路》分享了传统集中交易到新一代分布式核心交易系统的解耦思想，详述了竞价引擎和综业引擎的独立部署，营运内部化繁为简，可弹性扩容的报盘集群等系统解耦的探索。《基于 Spring Cloud Gateway 的新型业务网关设计与实现》讨论了微服务技术在交易所基础架构中应用遇到的挑战，基于网关解决了相关依赖服务升级方案不统一的问题，并提供了更好的安全防护。《基于分布式调用链框架证券业务系统应用研究》提出了一种分布式调用链框架设计方法，包含调用链信息采集、指标处理、链路展示、指标分析等模块，能够实现端到端的调用信息监控和跟踪，给生产环境问题排查、接口性能分析带来了便利。《安信证券服务化平台，助力业务系统云原生架构转型》描述了安信证券服务化平台实践之路，包括对微服务、容器和云原生等技术的理解、业务系统研发过程中面临的实际问题、服务化平台路线规划、解决方案和实践案例。

以高可用、易扩展、高容量、低成本、快速研发为优势的各类新架构正在进入人们的视野，突破传统方法和思维方式的架构提供了更多思路，以更好地解决海量数据、高效研发迭代、不间断服务等新挑战。可以预见的是，2021 年基础架构和运营方式的变革将产生深远影响。

《交易技术前沿》编辑部

2020 年 12 月 31 日

目录 Contents

架构探索 Exploration

低时延技术 Technology

行业观察 Observation

信息资讯采撷 Information

E 架构探索 Exploration

新一代分布式核心交易系统解耦之路

*王海东 */东方证券股份有限公司*

东方证券长期以来一直秉承解耦思想，不遗余力、积极探索，从 2016 年 12 月开始规划设计，2018 年 5 月完成了兼具稳敏双态特性的证券交易新核心—“东方睿阳”的建设。实现了运维、营运、风控、交易的完全分离；将低延时、高可用、松耦合思想贯彻了整个交易、行情、风控等证券核心交易业务领域。

本文将着重探讨从传统集中交易到新一代分布式核心交易系统的解耦思想及其应用实现后的效果，讲述“东方睿阳”如何实现竞价引擎和综业引擎的独立部署，如何根据权限和费用的业务特点进行营运内部的化繁为简，以及如何实现可弹性扩容的报盘集群等令人振奋的系统解耦探索之路。

一、证券交易系统解耦是证券业务发展的必然趋势

技术系统的专业化发展就是要让专业的工作由专业的系统来完成，证券交易的核心解耦也一直是证券交易技术发展的重要关注点，证券核心交易系统从诞生开始就一直在走着解耦的道路。综合目前所做的各种解耦工作看，一般都是因为某个业务或功能需求的发展推动的，都是由于这些需求的实现多半不再可以简单的与原有核心功

* 现任东方证券股份有限公司系统运行总部总经理。在证券公司核心交 易系统的项目建设、运维管理等一线岗位耕耘 22 年。现致力于以分布式交易系统、“东方云”、业务中台、智能运维为抓手，建设一流的数据中心和一流的财富管理平台，助推公司业务发展。

能合并实现，从而不得不进行解耦，分离出新的系统或子系统。

解耦的方式主要有横向和纵向两种：其中横向解耦是指将单个业务指令分解成多个环节，例如从简单的 C/S 架构变成多层架构就是将业务实现和通讯层进行了拆分，可以说是证券交易系统的第一次解耦；网上交易等复杂终端的出现是第二次横向解耦的产物，其目的是让终端承载更多的业务指令预处理和业务结果的综合整理为投资者提供更快、更好的服务。而纵向解耦则是指将业务进行分类，按照一定的原则将某一类或某几类相关的业务组成一个集合与原有业务进行分离形成新的系统或子系统。例如 CRM 等系统的出现就是纵向业务解耦的一种场景；账户业务的分离则是集中交易后的又一次旗帜鲜明的业务纵向解耦。随着业务的发展横向解耦产生了系统的小核心大外延，而纵向解耦推动核心业务实现的高内聚和松耦合。

从上述业务解耦的发展过程我们一般认为系统解耦的推动力是业务的发展，其最终实现则依赖合适的技术引领。

二、证券交易系统解耦需要从证券业务领域驱动系统设计

经过十多年的发展，集中交易已经当之无愧的成为证券交易的核心系统，其业务规模和处理能力也都发展到了极致，然而业务发展不会止步，对系统的要求也不会停止，系统解耦还在路上。尤其是机构业务的蓬勃发展使得当前核心交易系统面临性能、容量、监管、营运、运维等诸多更高的要求，其根本原因是核心交易系统所服务的各个业务领域都有了较大的成长，需要重新定义和规划，解耦方式也不仅仅局限于横向和纵向，往往会是一个综合的方案。

以性能为例，投资者对交易性能的要求一直是证券交易不懈的追求，现阶段整个链路时延已经进入微秒级的争夺，传统集中交易的 TCP 通讯和传统数据库技术基础决定了其性能难以达到这个量级，再加上集中交易所综合的业务品类和控制要求也使得业务指令需要穿过层层逻辑判断才能达成业务目标。我们知道一般情况下只有竞价业务才会有性能的要求，非竞价业务的性能要求则相对要弱一些，但传统集中交易的各种交易功能实现是紧耦合的，因此如果要使用新技术提升性能就可能会同时提升了多种业务的性能，显然不够经济，而且会因为链路上的功能繁多导致性能提升的空间有限。所以我们要将传统的交易领域划分成竞价交易领域和非竞价交易领域，然后针对竞价交易领域进行专业的性能优化。同时，鉴于机构客户的资产和交易特点，其单一账号往往资产规模较大，竞价交易频率较高，多个同类产品叠加后的交易峰值有可能会达到每秒几十万笔的情况，传统集中交易面对这样的脉冲就会产生阻塞，甚至会因为紧耦合设计而蔓延到其他业务处理功能上，竞价交易领域与非竞价交易领域充分解耦后不但可以有效隔断阻塞的蔓延，还会因为性能好和弹性扩容等能力从根本上减少阻塞的发生。

营运和风控管理领域也是如此，随着业务品类的增加，营运和风控的需求与日俱增，必须通过对业务的价值链和操作管理进行多层次的解耦和标准化才能做好与之匹配的业务设计。例如竞价业务与综合业务在营运管理上就有着较大的差距，表现在权限和费用等实现上也有着非常大的区别，因此这部分营运管理可以再解耦成竞价的营运管理和综业的营运管理，这也是使用高内聚的方法来进行解耦的思想体现。以费用为例，竞价业务的费用主要是佣金、印花税、过户费，种类少，算法也很稳定。而基金的认购、申赎和分拆、要约收购、大宗交易、回购等综合业务的费率就品类繁多，算法也不尽一致，会因为业务发展有较大变化，甚至不同市场的要求还有很大区别。传统集中交易将所有品类计费模型合并在一

个计费模块中实现的设计显然已经不太能适应现有业务的发展，因此营运管理的业务领域也会在计费方面分成竞价计费和综业计费两类、甚至更多类的业务模型，否则频繁的修改会导致系统的不稳定，复杂的设置也会给营运管理带来很多不必要的麻烦。解耦后，竞价业务的费用实现无需考虑综合业务的各种特点和场景，数据结构规整，业务实现稳定；而综合业务的权限和费用则可以非常灵活的满足各类需求，无需顾忌对竞价业务影响。同样，业务权限、适当性、统计分析、等营运和事前、事中、事后的风控管理等都应该遵循业务的发展而进行适当的解耦，以实现各个专业领域的专业化服务。

如图（图一）是很多券商同行在积极探索的业务解耦思路之一，其设计驱动力显然都来自证券业务领域模型的细分和发展。

实现后营运、运维、风控等管理业务领域不再与核心交易领域紧耦合，而是变成一个可以适当打开的外壳来支撑核心交易，这个变化是业务的横向解耦，可以将不需要的业务处理从链路中剥离掉。同时管理业务领域和核心交易领域内部也进行了解耦，这个变化就是按照业务类型进行了纵向解耦。两者结合就可以达到如下的效果：

1、对性能要求高的投资终端可以直达引擎，交易链路更简洁；

2、核心交易领域从传统交易中剥离出来后，交易业务的实现不再与营运、风控、运维等管理业务绑定，核心交易执行时所占用资源也将减少；

3、竞价和综业引擎独立，综业发展的时候可以保持竞价稳定，竞价发展的时候修改内容少，投入少，风险可控；

4、各类管理业务适当解耦后通过明确的接口进行交互，可独立部署，也便于弹性扩容；

至此，证券交易业务领域分解成了身轻如燕、固若金汤的竞价业务领域和多个身手敏捷、百花齐放的其他业务领域。当前的一段时间内，该模型将会驱动证券核心交易系统的进一步解耦。

三、证券交易系统解耦的分布式技术应用

业务领域解耦后，自然就要驱动技术进行实现，虽然事件驱动、观察者、责任链等设计模式和面向接口的编程方式仍然是系统解耦的开发技术基础，但原有基于传统数据库的集中交易，其各方面的能力受制于数据库、小机、TCP 通讯等技术的限制，已经很难有效满足当下先进业务功能的迫切要求。而新一代分布式架构采用的无锁队列、零拷贝、流水线、RDMA、可靠组播等底层技术将业务处理和通讯时延都降低到了微秒级，成功突破了传统业务处理毫秒级的性能瓶颈。于是新一代分布式证券交易核心系统应运而生，承接了当下的技术发展使命，开始引领证券交易系统的解耦之路。

图一：业务解耦思路

图二：报盘集群化

过往的经验告诉我们，没有低延时，解耦后的系统应用将会更加冗长和缓慢，随之而来的就是性能瓶颈和阻塞蔓延；没有高可用，解耦后的系统就会单薄而脆弱，随之而来的就是不稳定和难运维。这两个技术特点是分布式技术引领系统解耦的关键技术基础，在对业务逻辑分析透彻的前提下，这两项技术的灵活运用可以使得系统解耦游刃有余。经过多年的实践和探索，东方证券选择了以低延时为核心基础的分布式高速消息总线为技术架构，其优秀的高可用特性在现有可选的消息总线中也无出其右者。

以报盘集群为例，东方证券在长期的系统运行管理工作中，深入剖析报盘运维痛点，借鉴沪深证券交易所的成熟经验，运用分布式技术的解耦特性，先将报盘部署成竞价和综业两类平台，再将竞价类的报盘按交易量进行分组，每组 2-3 个报盘通道形成集群，然后将综业类的报盘合并成另一组集群，终于完成了多年的愿望，极大的降低了报盘运维的复杂度，并收获了一定的业务效益：

1、如图（图二）所示报盘集群化后报盘通道数从 8 个减少到 6 个，而且原有证券席位数量越大，可以节约的席位和通道数量越多；

2、报盘有效连接数从 16 条减少到 6 条，降低了应用程序监控和网络管理的复杂度；

3、实现了报盘的热备高可用，主报盘应用服务异常后可以零丢失、无感知的自动切换到备用服务上，无需人工判断和操作；

4、实现了通道的负载均衡，同一集群的报盘通道所承载的报盘压力是均衡的，无需根据业务量波动而人工调配；

5、每组集群的通道数量可以根据实际需要简单的增减，运维方便快捷。

上述方案在提升报盘运维能力的同时，还实现了单个股东账号报盘容量上线的突破，客户席位与报盘通道的解耦也使得内部账号迁移时无需顾忌报盘席位的修改。并且，由于完成了竞价和综业的报盘解耦，两大类业务之间的报盘再无影响，业务功能有效内聚，真正实现了竞价的稳态和综业的敏态。

因此，我们认为报盘集群应用是一次非常成功的解耦实践，是高内聚、低耦合设计思想的典型应用案例。实现集群后，竞价业务报盘集群侧重多分组均摊交易通道保障安全稳定、支持弹性扩容；综合业务报盘集群则只需要共享一组交易通道可以节约资源，并与竞价隔离支持业务的敏捷开发。

四、总结

以证券交易业务领域解耦模型驱动的集中交

易分布式演化之路已经全面启程。其本质是数据流消息化后给业务解耦带来的核心价值，业务逻辑实现不再是需要数据时由应用去获取，而是数据化身为消息在各个组件之间高速流动，驱动业务的完成（图三）。

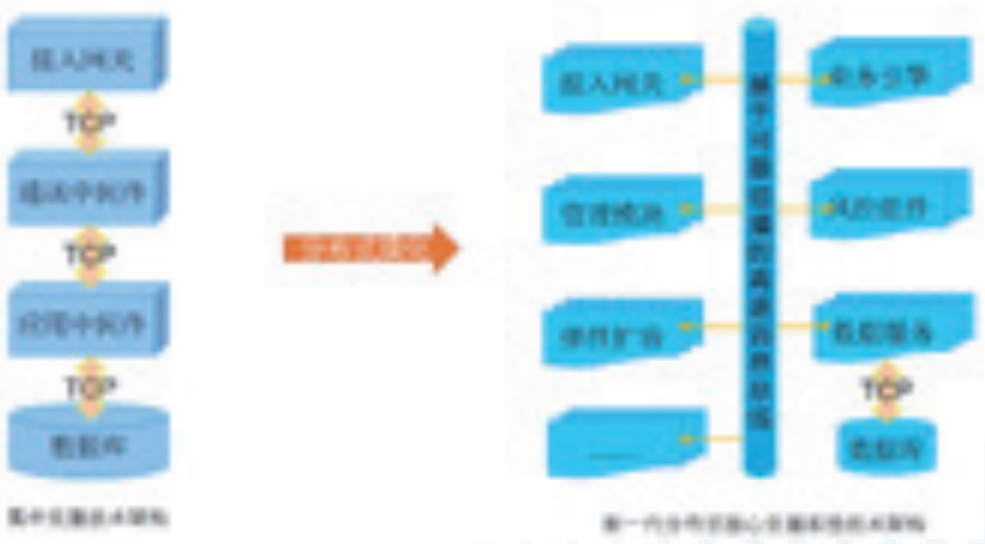
1、数据库不再是业务运行的核心基础，避免了系统因数据库产生单点故障和性能瓶颈；

2、应用系统间的接口清晰，可以合理分拆独立部署，也便于合并组合适配业务模式的变更发展；

3、应用组件可根据业务需求各自进行快速的弹性扩容；

4、系统模块在设计之初就自带主备和负载均衡等高可用特性。

展望未来，随着业务领域模型的发展和系统设计开发的成熟度提升，证券核心交易系统将在分布式技术架构基础上践行解耦之路，不断创新演化，并拓展到证券行业的其他应用领域，打破同质化竞争，助力券商行业的数字化进程。



图三：分布式演化

基于Spring Cloud Gateway 的新型业务网关设计与实现

陈波、陈明辉 / 上交所技术有限责任公司

随着微服务技术在交易所基础技术架构中的不断发展，越来越多的通用功能不断独立成微服务部署。对于大部分内部应用，都有接入部分通用功能的需求，如登录、鉴权验证、负载均衡、限流监控、缓存等。若每个服务独立编写相关代码，显然会增加工作量且并不稳定。当相关依赖服务升级时，所有服务必须同步升级，而各服务的接入方式存在一定差异，且升级方案互不统一，导致升级成本相对较高。网关的出现恰好解决了这些问题，通用功能可在网关实现，减少各个服务的冗余代码，同时可对部署在网关背后的服务提供更好的安全保障。不同于客户端的网关服务对并发的要求，业务内网关将需要接入更多公司内部的统一需求，设计重点更偏向于基础功能的接入。

在经历了网络安全攻防演习行动后，我们发现很多服务接入的方式不统一，甚至部分老旧的系统没有接入新的基础服务，导致缺少登录控制、权限控制等相关的安全防护，因此在网关的设计上，我们增加了更多的安全控制功能，确保接入应用的访问安全。

一、术语导读

本文涉及专业术语及简称如表 1-1 所示，后续使用到相关术语时会使用简称，特此说明。

表 1–1 ：本文所涉及相关术语

术语	简称	说明
Spring cloud gateway	Gateway	Spring cloud 官方团队出品的网关组件
Zuul	Zuul	Netflix 公司出品的网关组件
WebFlux	WebFlux	Spring 官方团队出品的响应式 web 框架
Spring Reactor	Reactor	Spring 官方团队出品的响应式编程框架，WebFlux 基于此框架
WRK	WRK	HTTP 压测工具
Filter	Filter	特指网关中的过滤器
Airport	Airport	大数据团队自研网关系统服务端。
Airport-Client	Airport-Client	大数据团队自研网关系统客户端。
UUMS	UUMS	用户登录认证系统
Permission	Permission	大数据团队自研权限管理系统
Galaxy	Galaxy	大数据团队自研基础数据服务
Luna	Luna	大数据团队自研的报表开发平台
ELK	ELK	华为自研分布式数据库，注意与 Es+Logstash+kibana 区分。
Actuator	Actuator	Springboot 提供的监控插件

二、概述

随着软件系统架构的演变，微服务架构的使用也越来越广泛，随之带来的是企业对软件系统集成对接与能力开放的需求。网关控制系统针对不同软件系统之间对接过程中带来的多样性、易变性、开发效率等问题，提供轻量级、高性能、易控制的运行环境。网关提供多种系统通用功能，例如接口权限认证、流量控制、登录认证、接口日志、接口缓存、监控告警等。网关本身使用微服务架构，每个微服务本身的轻量化和可扩展性使其能够满足不同业务场景提出的定制化需求，以可插拔式的方式运行业务定制插件。微服务架构同时能够满足不同业务场景的不同组网需求，组网环境下多个微服务的集群部署有利于提高性能。国内外目前对微服务架构的研究主要在将单体应用微服务化，通过逻辑上的分割来体现微服务带来的优势。国内外的网关系统都已有产品应用，国内阿里云率先推出网关产品，提供 API 托管服务，帮助用户开放部署在阿里云上的服务。国外目前比较成熟的微服务网关组件有 Zuul 和 Gateway。

三、技术选型

当前比较流行的 API 网关组件有 OpenRestry、Kong、Nginx、Zuul、Gateway 等，为了更加适应当前的技术架构，对于非 Java 语言开发的网关如 OpenRestry、Kong、Nginx 等将不在考虑之列。在微服务的生态中，Zuul 和 Gateway 应用比较广泛。其中 Zuul 在早期的 1.x 版本有相当多的落地实践，截至到 2020 年 11 月 23 日，Zuul 已经更新到了 v2.2.0 版本。Zuul 2.x 相比 Zuul1.x 基于 Netty Server 实现了异步 IO 接入请求，同时基于 Netty Client 实现了网关到后端业务服务 API 的请求，极大地提高了网关的性能，实现了更低延时、更高性能的网关服务。由于当时 Zuul2 一直未能面世，对于 http2 和 Websocket 的需求进展缓慢。Spring Cloud 官方推出了 gateway，它是基于 WebFlux/Reactor 编写的，支持 http2 和

Websocket，与 Spring Cloud 生态完美兼容。截至本文撰写时 Zuul2 已经发布到 2.2.0。如果对于网关的转发效率，没有太大的需求，建议直接使用 Zuul1.x，它的文档更加完善，实践案例更加丰富。Zuul2.x 和 Gateway 都比较新，相关文档还在不断完善中。目前我们的网关初步规划的接入应用对转发效率上有一定要求，因此 Zuul1.x 不在考虑之列。下面将从几个方面对 Zuul2.x 和 Gateway 进行对比。

1. 兼容性

二者都可无缝对接 Spring Cloud。其中，Gateway 采用了 WebFlux 框架，与传统的 Spring-Web 项目不兼容，若不熟悉，则改造上有一定难度。

2. 功能

功能对比如表 3-1 所示。Zuul 的很多功能都需要基于 Filter 实现，而 Gateway 则提供了许多官方的 Filter，用户只需要去配置即可。在实际的应用中，Gateway 提供的 Filter 也许并不能完全实现需求，需要少量的改造，但是有官方实现作为基础，因此在功能维护上更好。目前许多厂家也逐步从 Zuul1.x 迁移到了 Gateway，网络上能够找到许多开源资料。

3. 性能

针对二者的性能比对，我们做了 WRK 和 AB 测试。WRK 测试采用 10 个线程，200 并发，持续 30 秒，比对结果见表 3-2，其中 Gateway 每秒处理请求个数以及平均时延较 Zuul 有明显优势。AB 测试采用 200 并发，50000 个请求测试，比对结果见 3-3，AB 测试结果同样表明 Gateway 在性能方面较 Zuul 有明显优势。

综上，性能方面，Gateway 比 Zuul 更优，考虑到我们需要在 Gateway 上完成一些自定义的功能，需要查询数据库，这本身会带来一些时延，Gateway 的性能优势可以降低时延，是个不错的选择。考虑二次开发成本和性能，我们尝试在 Gateway 的兼容性上做进一步实践，熟悉了 Webflux 相关内容后，我们选择了 Gateway 作为

表 3–1：Gateway 与 Zuul 功能对比

网关	限流	鉴权	监控	易用性	维护性	成熟度
Gateway	可以通过 IP、用户、集群限流提供了相应的接口进行扩展	普通鉴权、Auth2.0	Gateway Metrics Filter	简单易用	好	社区成熟，但是资料较少
Zuul	可以通过配置 Filter 实现和扩展	Filter 中实现	Filter 中实现	参考资料少	差	开源不久，资料较少

表 3–2：Gateway 与 Zuul 性能对比，WRK 测试结果

指标	直连	Zuul	Gateway
每秒处理请求（个）	22433	6517	9228
平均延时（ms）	13.25	105.06（偶尔超时）	21.83

表 3–3：Gateway 与 Zuul 性能对比，AB 测试结果

指标	直连	Zuul	Gateway
总耗时（秒）	2.748	7.862	6.762
每秒处理请求（个）	18195	6360	7394
平均延时（ms）	11	31	27

基础骨架进行二次开发。

四、Gateway 概念和基础原理

图 4–1：Gateway 原理图

断言：JAVA8 中的条件断言。网关中使用断言，来判断一个请求是否匹配，如判断请求头、请求参数是否符合某个条件。

路由：网关的基础组成部分。由路由 ID、对应的网络资源、一组断言、一组过滤器组成。如果断言全部为真，则匹配该路由。

过滤器：Gateway Filter 的实例。Gateway Filter 是 Gateway 内部定义的一个过滤接口。你可以通过过滤器在网关转发的各个阶段进行介入，实现自己想要的功能。同时 Gateway 也支持相当多种类的过滤器功能配置。

Gateway 的原理如图 4-1 所示。客户端发起请求到 Gateway，首先会经过 Gateway Handler Mapping 进行路由匹配，如果匹配成功则将其发送给 Gateway Web Handler 模块，匹配到路由后，按顺序执行路由中定义的一系列 Filter 的前置代码后到达代理服务模块，再通过定义的转发规则转发到目的服务。当请求返回后则是逆序执行 Filter 中实现的后置代码。

五、架构设计与实现

我们抽取了几个试点项目（Permission、Galaxy、Luna）接入网关试点。用户中心采用公司内部 UUMS 系统，进行登录验证。服务关系如图 4-2 所示。其中所有服务均接入 Eureka 注

图 4–2：服务关系

册中心，其中 Permission、Luna 是前后端分离的 Web 项目，Galaxy 是纯后端服务。我们开发了网关的客户端，Permission、Galaxy、Luna 均接入了该客户端。网关服务端启动后会从 Eureka 初步同步相应的应用服务名并启动相关路由。

接入了网关客户端（Airport-Client）的程序，启动时会向网关的服务端（Airport）发送一些信息，如应用信息、接口信息、监控信息等。用户也可以在网关的配置页面对应用相应的信息、接口信息进行修改。对于非 Eureka 的服务，如 Python 小项目等，暂不支持使用客户端接入，但可以通过服务端的管理页面进行手工添加。一旦服务注册到 Airport 之后，在页面上配置一些转发路由，就可以通过网关对外提供接口服务。

除了基础的路由转发功能，基于 Gateway 做了二次开发的 Airport 网关提供了许多统一的业务功能如请求合法性校验、接口权限验证、登录验证、缓存、审计日志、服务监控、XSS 防护、IP 黑白名单等功能。全局功能流程如图 4-3 所示。

a) 登录认证

登录认证接入了 UUMS 系统提供登录认证服务。为了提供统一的登录认证，我们对原有的接入流程进行了改造。新的接入流程如下：

1. Web 服务的前端页面发起请求经过 Nginx 代理到网关。

2. 网关对请求进行合法性校验，如不通过直接拦截告知非法请求。通过则执行步骤 3。

3. 通过请求获取 session 和 redis 缓存中的 session 缓存存判断用户是否登录。如果未登录则拼接登录跳转地址返回给前端，其结构示例如下：

```
{
    "data": "loginUrl",
    "msg": "请登录",
    "status": 30200
}
```

该链接遵守 UUMS 跳转规范。

4. 前端对返回做拦截，对于 status 为 30200 的返回，跳转到 data 所指定的地址。status 为其他值时表示已通过登录认证，跳转步骤 6。

5. 进入跳转地址后，用户在 UUMS 的登录页面输入账号密码进行登录，验证通过后，UUMS 服务端会请求已经配置到其系统内部的登录接口（该接口由 Airport 服务端统一实现），并附带 token。

6. Airport 接到 login 接口的请求后，使用该 token 向 UUMS 反查用户信息，并将用户信息存入 session 同时写入 redis session 缓存。

7. 结束。

该流程对于接入网关的应用的后端不需要实现相关登录流程，前端对 response 做相应的拦截修改即可。Airport 转发时会附带 session 信息，接入服务端可在请求的 session 中获取相关用户信息。

b) 接口鉴权：

任何接入到网关的应用，都需要先在网关的管理页面上申请接入密钥。Airport 基于该密钥做权限认证。为了提高安全性，在申请密钥的时候提供了多种加密方法的选择如 md5、sha256、md5hex、sha256hex、sha1hex， 同时在生成签名时密钥拼接默认后缀如（abcdefg）。

表 4–1：接口认证发送方需要发送的相关字段

参数名	说明	示例
AIRPORT-ORG-APP	源应用	Luna
AIRPORT-DES-APP	目的应用	Galaxy
AIRPORT-LOG-ID	时间戳	1606125050
AIRPORT-SIGN	签名	91C7B0D19FFBA6B3ADA065FB20D814DE

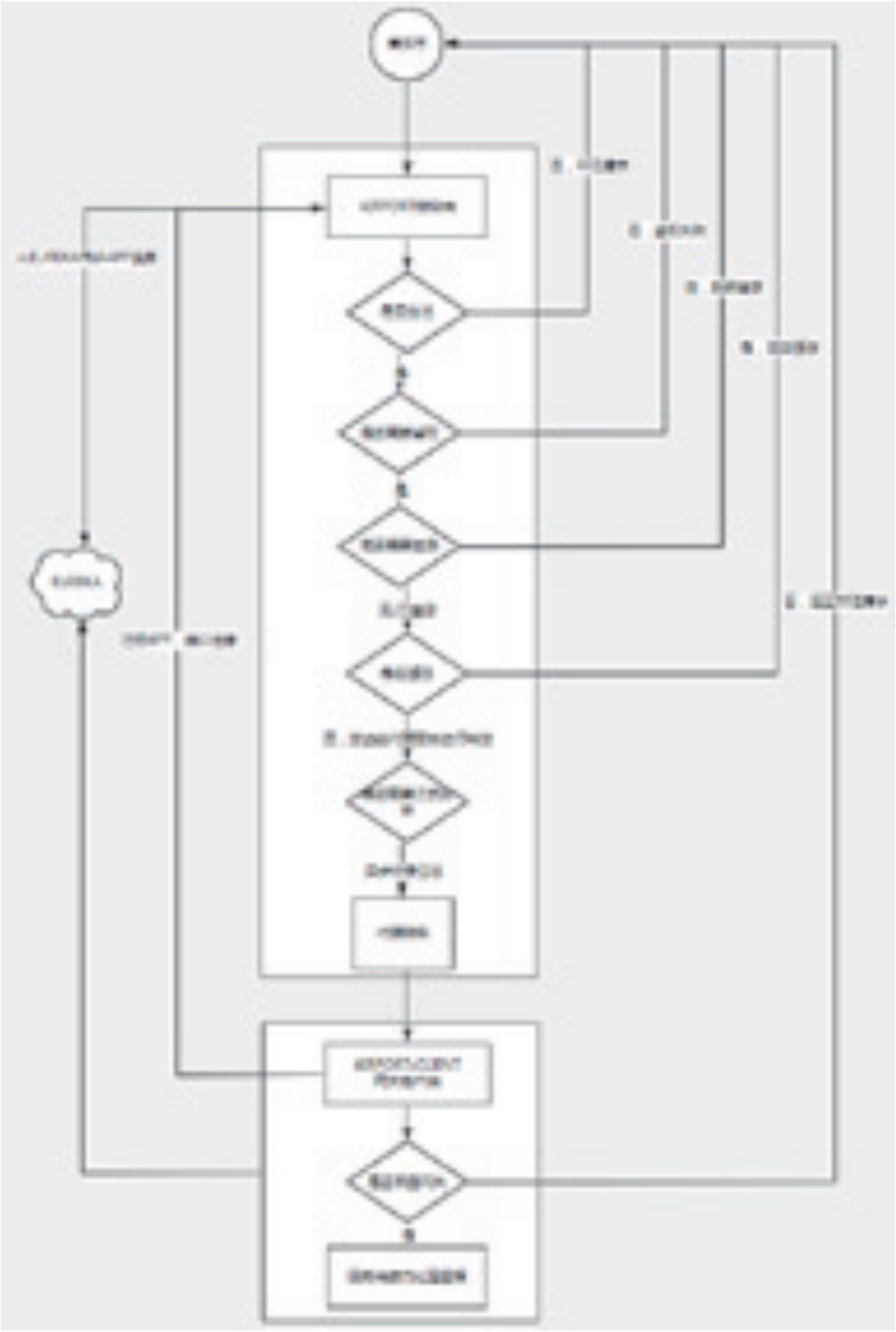


图 4–3：全局功能流程

此外对于任意请求，Airport 都会做 XSS 拦截和 IP 甄别。

请求方需要传递的请求头部参数如表 4-1 所示。注意不论是源应用还是目的应用，都是已经注册在 Airport 之上的应用。签名计算方法（如选择 md5 作为加密方法，申请的密钥为 f35ade77-4a22-40f5-a61d-efd5011e0f46 默认加密后缀 abcdefg）DigsetUtils.md5(luna+galaxy+1606125050+f35ade77-4a22-40f5-a61d-efd5011e0f46+abcedefg)。Airport 收到请求后取出相关头部参数，先判断时间戳是否过期（如限定距当前时间 5 分钟内有效），根据在 Airport 申请密钥时选取的加密方法进行同样的计算再进行签名比对。

c) 缓存：

由于缓存的更新需要接入方根据对应的业务逻辑进行更新，Airport 仅提供了简单场景的缓存配置功能。比如对于数据延时不敏感，但查询压力较大的场景，可以选择在 Airport 中开启缓存。对于复杂的缓存场景，如需要保持缓存一致性，请在接入方实现。

d) 日志：

Gateway 的 response 和 post 请求的 body 都是流式的，不可重复读取，因此定义了一个全局的过滤器，复制请求体和返回内容。需要注意的是，有些服务端开启了压缩选项，需要先解压才能记录可读的返回内容。目前仅支持 gzip 压缩方式。由于集中存储了很多系统的接口日志，后端数据库存储采用了 MySQL+ELK，其中 MySQL 仅保留 7 天日志，ELK 存储全量日志。

六、安全防护

网络安全、信息安全问题一直备受国家和企业重视。随着 2020 网络安全攻防演习行动的推进，交易所组织了大量的漏洞扫描工作，我们逐步在应用层也增加了许多防护措施。其中一些和应用层服务比较贴近的攻击手法，如 XSS、恶意伪造请求等，比较适合在网关层进行防护。Airport 目前已实现了 XSS 攻击防护与 IP 黑白名单防护。

跨站脚本攻击 (Cross Site Scripting) 是指攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上对其他用户造成影响的 HTML 代码，从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式。为与层叠样式表 (Cascading Style Sheets) 的缩写 CSS 区分开，跨站脚本攻击通常简写为 XSS。

目前比较流行的前端框架，如 Vue、React、Angular 在底层都做了 XSS 防护。不过还是有一些途径可进行 XSS 攻击，如 React 中使用 dangerouslySetInnerHTML，Vue 中使用 v-html 都有攻击风险。一般主流做法是对这些带有攻击性质的字符串进行转义。但有一些场景转义存储，会带来一些新的问题。如本身就是要向后端传递编写的脚本，如果进行转换后端存储将和实际想要存储的数据不一致。目前我们考察了需要接入网关的服务，不存在带有 XSS 攻击性质的参数传递，因此暂时先做了统一拦截，对于带有攻击性质参数的请求，会被拦截。这样做也仅仅是在请求到达后端前做了一层拦截，在后续请求返回后风险依旧存在。总之，关于 XSS 防护，是前端和后端一起配合的工作。在网关层，付出多少代价，取得多大效果还需要结合后续实际应用进行验证和改进。

关于 IP 防护，目前服务基本部署在内网，防护的场景是假设内网被攻入，还有一层拦截能力；或者部分客户端需要临时屏蔽，如某些接入的应用发生故障大量对其他服务发起请求，导致下游服务承载不了，此时可以先屏蔽到异常客户端的所有请求，保障下游服务能正常提供服务。

Airport 可配置黑白名单，其中白名单具有绝对权威，当其中网段与黑名单中有冲突时，优

图 7–1 ：Airport 监控指标示例

先放行。这取决于对待 IP 拦截的原则是优先提供服务，还是优先保障安全牺牲用户。对于内部网关来说，显然前者更符合设计。

七、应用监控

微服务监控有很多解决方案，Airport 基于 Actuator 实现了轻量级的监控。在 Airport-Client 中嵌入 Actuator 插件，定时采样相关监控指标如内存使用量、CPU 使用率、GC 耗时、线程数量、JVM 相关指标、请求数量等上报到 Airport 服务端，由服务端写入 ES 集群。Airport 提供对这些监控数据的可视化展示如图 7-1 所示。

八、结语

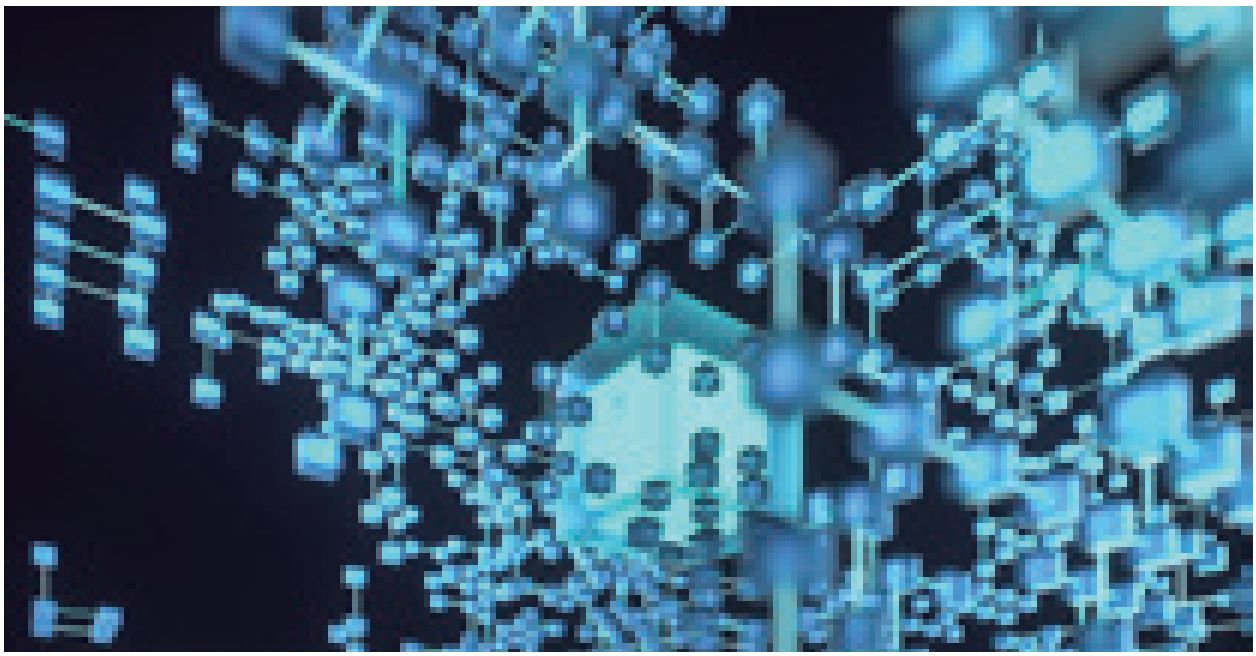
本项目基于 Gateway 实现了许多基本功能，简化了后续应用的开发，提高了开发效率。同时通用功能的变更和迭代，只需要在 Airport 中进行修改即可，提高了版本更新效率。

Airport 还提供了可视化监控服务，填补了目前没有服务指标监控的空白。后续会对相应指标提供告警功能，帮助用户更早的发现服务异常，减少事件产生。

在安全防护上，Airport 也提供了基础的 XSS 防护和 IP 拦截，后续会针对不同的攻击手法增加必要的安全防护。

基于分布式调用链框架证券业务系统应用研究

罗明伟、曾利、任荣、王东、王洪涛 / 海通证券股份有限公司 信息技术管理部



世界经济一体化和全球信息网络的发展浪潮中，各国金融市场日益联结成一个统一整体，复杂庞大金融数字化的深入发展为金融市场一体化奠定了坚实基础。证券行业 IT 体系也浪潮的推动中，在数字化方向的发展上也呈现上升泰势，传统的集中式系统正往分布式系统的方向逐步演变，分布式系统的引入为复杂证券业务的快速变化提供了灵活支撑，但同时也增加了业务调用深度，深度的增加导致一个业务请求可能涉及到几十个应用系统，对链路跟踪的缺乏，无法快速定位出问题系统，最终导致解决问题的效率低下。为了解决分布式系统架构下快速定位问题难的现状，基于对原业务系统侵入尽可能低的目标下，本文提出了一种分布式调用链框架设计方法。

该框架主要包含调用链信息采集、指标处理、链路展示、指标分析等几大模块，能够实现端到端的调用信息监控和跟踪，给生产环境问题排查、接口性能分析带来了很大的便利性，该框架成功运行于海通证券的相关应用系统，并且取得了良好的实际效果。

一、引言

随着互联网的不断发展以及国家信息化建设步伐的加快，迫切要求企业要跟上信息化建设的步伐，其中对于在国家金融发展中有着举足轻重的证券行业也显得尤为迫切。证券公司 IT 体系的快速民展，应用系统业务复杂度增大、系统数量的快速增多，系统与系统之间的信息交互越来越多，这些方面都加剧了系统的维护成本，往往一个业务场景会涉及十几个乃至几十个系统的共同协作才能完成。一旦业务过程中发生问题，对问题的定位将是一种高难度挑战，定位问题占用了开发人员的很多精力，使开发部门幸福感变低，工作效率变差，为此，设计分布式调用链框架，辅助业务系统快速定位问题，则显的非常有必要。

二、相关概念

1) 分布式调用链

在广义上，一个调用过程代表了一个事务或者流程在分布式系统中的执行过程

图 1 中 A-E 五个节点表示五个服务。用户发起一次请求到前端服务 A，该请求依赖后端服务 B 与 C，因此服务 A 分别通过发送 RPC 请求到服务 B 和服务 C，B 处理完 A 的请求后将响应返回给 A，但是服务 B 还依赖服务 D 和 E，B 再发起两个 RPC 请求分别到 D 和 E，D 和 E 处理完毕后回到 B，B 才继续应答到 A，最终 A 将调用结果返回给用户。分布式调用链的目的，就是将用户一个入口请求及相应的其它后续请求进行网络拓扑汇制，最终生成表示调用关系的调用图。

2) 分布式调用链 Span

分布式请求调用会触发多个系统的之间的请求和响应，而将两个服务之间的请求 / 响应过程叫做一次 Span，一个多层次调用过程由多个 Span 组成，其调用过程可以用以下表达式构成：

分布式调用链 = Span A+ Span B+ Span C+.....

图 1：分布式调用过程

图 2：Span 的结构图

图 1 的 span 的结构图如图 2。

上图中，包含了 5 个 span（非 RootSpan），其中 B 和 C 是 A 的子节点，D 和 E 是 C 的子节点，某次请求调用过程的 Span 关系时间轴关系图如下所示：

```
--|-------|-------|-------|-------|-------|-------|-------|-> time

 [Span A···················································]

   [Span B·····························································]

     [Span D·····························]

     [Span E·····························]

   [Span C·····························]

     [Span F·····]
```

图 3：Span 的时间轴关系图

分布式调用链记录每次发送和接受动作的标识符和时间戳，将一次请求涉及到的所有片段服务串联起来，以此实现对一次请求的完整调用跟踪。

三、分布式调用链框架简介

前文介绍了分布式调用链的相关概念，后续将对分布式调用链框架进行介绍，从框架的整体设计而言，整个分布式调用框架主要由以下几个部分构成：调用链日志生成器、数据采集器、采集数据处理器、数据存储器以及调用链可视化组件构成，其中调用链日志生成器负责对整个业务请求过程中所涉及的应用进行卖点并且格式化输出到日志文件中，数据采集器负责对各个应用的日志文件数据进行采集上报，数据存储器需要对数据采集器上报的数据进行存储，并且对采集的数据进行相关指标运算，为系统告警或者相关的应用的性能分析做出参考，调用链可视化组件主要为相关调用链日志查询提供可视化界面查询，并且在查询速度上有比较高的要求。分布式调用

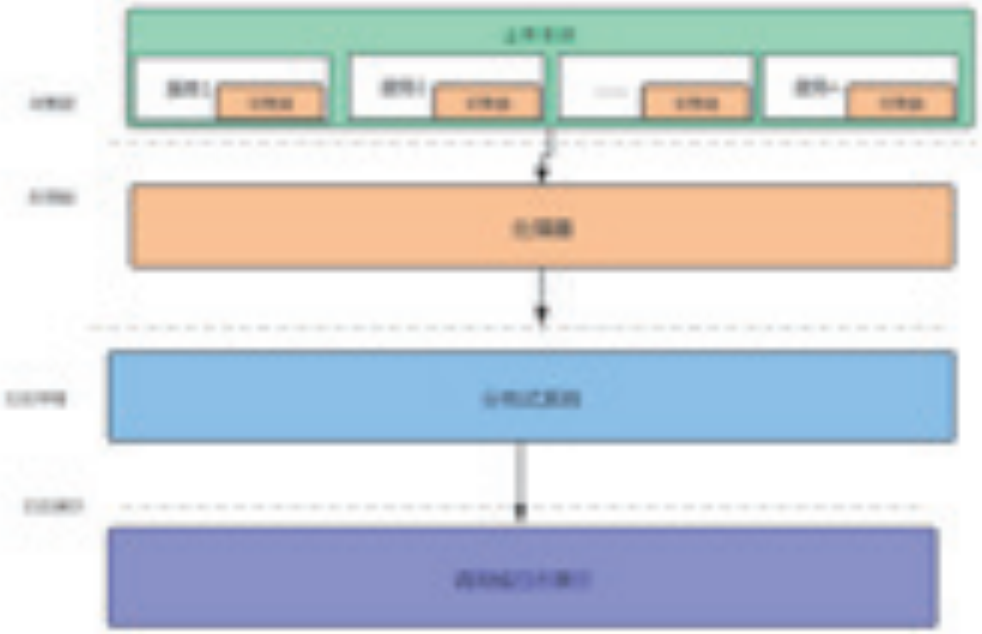


图 4：调用链整体设计示意图

链框架的核心设计图如图 4 所示。

四、调用链框架评估分析

针对调用链框架给系统带来的效果进行评估，主要采用了以下几种评估标准用于评估调用链框架效果，评估的维度如下：

- 系统入侵性
- 接口性能排查
- 出错问题排查
- 可复用性

下面通过几个维度的对比，以列表的形式展现了特点。

五、分布式调用链框架的设计

本节会重点阐述一下分布式调用链整体的设计与实现，分布式调用链从功能实现上来说，有两大核心模块：调用链日志生成模块、日志采集与展示，下面将针对这两大模块的设计方案展开描述。

1) 调用链日志生成模块

首先介绍几个核心概念：Tracer(跟踪器)、Span(跨度)、SpanContext(上下文)、Carrier(承载器)

► Tracer(跟踪器)

表 1：调用链框架给系统影响

是否使用框架 / 维度	调用链框架	传统方式改造
系统入侵性	存在代码入侵，但是入侵性性小	自主实现埋点
接口性能排查	排查容易，基于接口耗时计算，容易分析慢接口	排查困难，难以分析接口性能
出错问题排查	排查容易，通过 TraceId 串联，容易分析出错问题系统	排查困难，难以分析出错问题系统
可复用性	复用效果比较好	自主实现，个性化强，无特别复用效果

分布式系统调用链 Trace 代表一个完整的请求调用过程，Trace 由多个服务系统请求 / 响应组成，一个 trace 可以认为是多个 span 的有向无环图。Tracer 用来创建 Span，以及处理注入和抽取 Carrier，用于跨进程边界传递，为了跟踪一个请求的全部路径，往往通过生成 TraceId 方式进行跟踪。

► Span(跨度)

表示分布式调用链条中的一个调用单元，主要为服务提供方内部两个独立片段服务之间的调用。一个 span 一般会记录这个调用单元内部的一些信息，比如日志信息 , 标签信息 , 开始 / 结束时间。调用链中通过 spanId 来标注一个 Span, 但是日志展示过程中，如果要将两个独立片段服务之间的调用完整的展示出来，必须还要通过 ParentSpanId 来标识两个服务之间调用的层级关系。对于 ParentSpanId 而言，首次请求的时候，父 Span 不存在，因此默认为 -1，后续进行分析的时候只要遇到某个 Trace 节点的父 Span 为 -1，则表示这个请求是首次请求，也就是 Trace 树形结构中的根节点。

► SpanContext(Span 上下文)

表示一个 Span 对应的上下文，Span 和 SpanContext 是一一对应的关系，上下文存储的是一些需要跨越边界的一些信息，比 SpanId（当前这个 Span 的 id）,traceId（这个 Span 所属的 TraceId）即：该次调用链条的唯一 id。SpanContext 可以通过某些媒介和方式传递给调用链的下游来做一些处理（例如子 Span 的 id 生成、信息的继承打印日志等）。

► Carrier(承载器)

用来在 Span 过程中，将 SpanContext 上下文在多调用单元传递，包括 Span 的标识信息、Span 中的深度计数器、时间戳等。

2) 调用链日志采集与展示

海通日志平台是集日志存储、分析和可视化为一体的分布式日志平台，包括日志采集模块、存储模块和日志搜索等功能，采集模块通过 FileBeat 进行采集，之后通过 Kafka 推送至 LogStash 集群进行日志解析、打标，经过日志标准化解析后存储在 ElasticSearch，并生成相应的指标结果，日志平台平台支持图形化展示指标趋势、日志内容模糊快速检索，其架构如图 6。

要实现调用链在日志平台图形化展示，需要对日志格式改造：

1.TraceId 的生成和 MDC 埋点

图 6：调用链日志采集框架

TraceId 的生成方式采用的是 UUID 的生成方式，保证了 TraceId 的唯一性。MDC 是 log4j 和 logback 提供的一种方便在多线程条件下记录日志的功能，将 TraceId 放在 MDC 中，可以保证当前线程下所有的日志输出都有相同的 TraceId，同时当前线程的子线程也和父线程共享相同的 TraceId，从而保证了一次请求的所有调用 TraceId 的唯一性。

2. 日志格式改造

要实现在日志输出时打印出生成的 TraceId，需要对日志格式中增加对 TraceId 的日志配置支持，对 PatternLayout 进行配置，具体配置如下：

```
<PatternLayout>
    <pattern>[%d{yyyy-MM-dd HH:mm:ss SSS} %-5p] [%t] [%X{traceId}] [%X{spanId}] (%c:%L) - %m%n</pattern>
</PatternLayout>
```

六、实际运用

日志平台支持 traceId 的快速检索，支持对日志的链状上下文快速过滤，串联整个调用过程，从而对整个调用进行跟踪。以海通集中运营管理系统为例，详细介绍调用链技术如何串联集中运营管理系统的前端请求和后端子系统，通过对基于 request 请求生成的链路 ID 进行统计，能够有效的监控系统的吞吐量。另一方面基于链路能够对系统的异常报错进行跟踪，从而快速定位到报错系统，大大减少了定位出错问题的时间。通过链路数据的耗时数据实现对系统接口的耗时监控，从而找出系统高耗时的应用接口，再结合整个链路中的各个部分耗时的统计数据，能够具体定位到应用哪个部分出现性能问题，从而进一步对系统的性能问题进行优化。

以集中运营管理系统开户为例，截取了部分开户的日志调用链展示，详细展示了调用链如何对系统的各组件（数据库、缓存以及外部系统）进行串联，其部分调用链图 7 所示。

从上图的链路图可以看出，该图完整的展示了系统连接 DB2，Memcache 的数据组件的完整过程，并且详细记录了查询 DB2，Memcache 的耗时，并且在执行业务代码发生报错，从报错信息能够看出完整的出错原因，减少了排错时间。

以下从线上问题排查，基于链路跟踪的流量监控、耗时监控来说明调用链给系统排障、性能分析所带来的的好处。

▸ 线上问题排查

当线上应用出现问题，传统的模式下需要对各个服务节点的日志用开户的关键字进行日志搜索，如果线上服务节点众多时，难以排查出问题的节点或者找出相关报错信息，当用 TraceId 对各个调用系统进行串联，比如开户，通过资金号或者相关关键信息信息找出业务请求的 TraceId，

图 7：系统开户调用链路图

通过 TraceId 能够将完整的调用日志信息展示出来，找到异常报错日志，找出报错原因，大大提升了排查问题时间。通过集中运营管理系统排查报障的所花费的时间来看，排查报障的时间总体减少了 70%。

► 链路监控

通过调用链的拓扑图式链路监控，可以看到 Span 的有向环形图，并且能够每个 Span 的耗时、吞吐量等指标。

1. 流量监控

根据接口请求进行流量监控，通过流量监控，能够对集中运营管理系统负载情况进行整体评估，从而根据流量情况对服务器进行扩容和预测一些流量峰值，从而提前防范由于流量突然冲高带来的系统风险，实现服务器的动态扩容。图 8 是接口的流量监控，从而图中能够清晰的看到请求的峰值在 10 点左右。

2. 请求耗时统计以及性能优化

对接口请求耗时统计，能够发现慢的请求 / 响应，借助耗时统计分析，发现系统在复杂列表页面、报表页面等请求处存在性能优化空间。图 9 的 Top 接口耗时统计，通过 Top 接口耗时能够看出耗时慢的接口，从而定向优化接口性能。

七、总结

针对证券系统分布式部署下难以快速定位出问题的系统的问题，引入了分布式调用链框架，通过在请求端生成 TraceId 的方式绑定请求，后将 TraceId 在各调用端透传，实现了各个调用服务端的串联，为快速定位线上问题提供了很好的分析手段。该系统具有低入侵性，而且接入方案简单，能够快速接入业务系统，实现了对调用请求的完整跟踪，并且将该框架接入海通集中运营管理系统，实现了对海通集中运营管理系统开户等全业务的调用请求追踪，实现了对集中运营管理系统流量跟踪和请求耗时跟踪，基于耗时跟踪，进一步对系统性能分析，从而为系统性能优化提供好的分析基础。

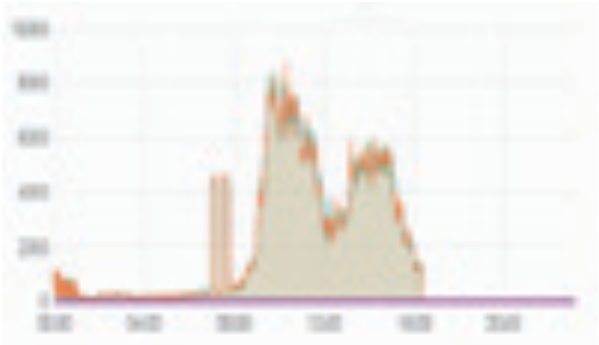


图 8：流量监控图

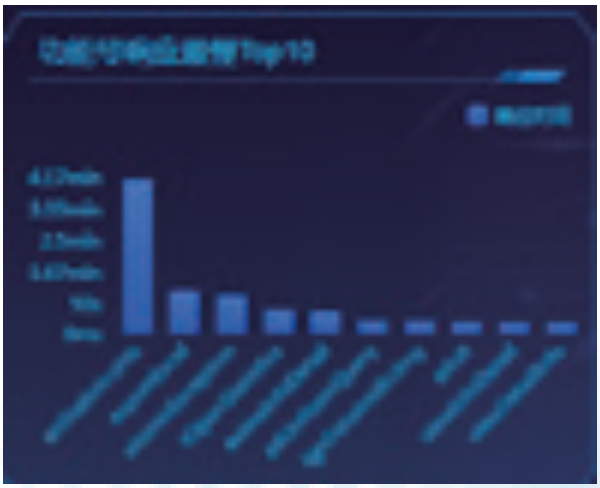


图 9：接口耗时监控图

安信证券服务化平台，助力业务系统云原生架构转型

段苏隆、周巍、沙烈宝、李银鹰 / 安信证券股份有限公司信息技术中心

互联网应用的海量用户、快速迭代、不间断服务和流量突增等业务特征促进其技术架构从传统集中式到分布式 SOA 和微服务架构方向逐步演进。随着敏态业务的逐渐增多，对业务连续性、交付效率和故障处理效率等方面提出了更多的挑战，安信证券服务化平台实践，以赋能业务为中心，积极拥抱微服务、容器和云原生等新兴技术来解决业务系统研发过程中的实际问题。本文描述了安信证券服务化平台实践之路，包括对微服务、容器和云原生等技术的理解、业务系统研发过程中面临的实际问题、服务化平台路线规划、解决方案和实践案例，最后展望平台的未来发展方向。希望能够将实践内容和思考与读者呈现，共同探索这一领域的演进方向。

1. 系统简介

近年来微服务架构因其具有松耦合、敏捷迭代、去中心化和弹性架构等优点，在帮助公司实现业务敏捷、IT 敏捷方面发挥重要作用。在基础设施方面，随着以 Docker 和 Kubernetes 为代表的容器技术的成熟，工程师不再需要应对各种迥异的运行时环境，Docker 通过集装箱式的封装方式，让应用能够以“镜像”的标准化方式发布和交付。当前微服务落地的最佳载体是以容器和 Kubernetes 容器编排引擎为基础，为拆分后的服务提供弹性伸缩、资源调度等一系列标准化和自动化的能力。在微服务治理方面，诞生了一系列的基础框架支撑微服务的敏捷迭代、自动化发布和服务治理等特性。如 Apache 开源的 Spring Cloud、Dubbo 等框架，通过嵌入 SDK 的方式实现如服务注册与发现、负载均衡、认证授权、限流熔断、运行状态等服务治理功能。同时，也有新一代如服务网格等无侵入式的服务治理方案，通过对服务间的通信流量进行代理，能够在不修改源代码的情况下实现上述服务治理功能。

随着微服务、容器等技术的发展以及应用和基础设施的云化，云原生的概念也应运而生，云原生计算基金会 (Cloud Native Computing Foundation，CNCF) 对云原生的定义为：帮助企业和机构在公有云、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。云原生的代表技术包括容器、服务网格、微服务、不可变基础设施和声明式 API。这些技术能够构建容错性好、易于管理和便于观察的松耦合系统。结合可靠的自动化手段，云原生技术使工程师能够轻松地对系统作出频繁和可预测的重大变更。

1.1. 平台架构

安信证券服务化平台，从业务系统的实际需求出发，积极拥抱微服务、容器和云原生等技术，以低侵入甚至无侵入模式实现应用运行状态可观测、服务治理等功能，另一方面，为业务系统的研发提供云原生工程脚手架、并和 DevOps 流水线对接，是整个云原生架构版图中的核心内容。服务化平台的架构图如下所示，其中门户提供运行状态展示、观测告警以及服务治理等功能；模块与组件是用于对业务系统数据收集和服务治理的组件集合，与投资秀、高手社区、Leve2 行情和用户中心等业务系统对接。

1.2. 解决的问题

尽管微服务和容器等技术已广泛使用，但它

图 1

们仍然需要结合具体的业务场景落地。因此，我们从实际出发，针对 15 个具有代表性的自研业务系统负责人进行问卷调查和访谈、同时对近两年的生产事件进行归类，梳理出不同优先级的服务化相关需求。

内部调研结果

从业务系统建设方角度，期望平台提供如下能力项：使用手册、配置中心、服务网关、负载均衡、链路分析、熔断限流、注册中心、工程脚手架、指标监控等。

生产事件分析

平台研发团队对近两年来 1800+ 生产事件分析，归纳整理出中间件配置、外部调用、监控、环境差异、突发流量 5 类共性问题，对应能力项需求包括：中间件最佳实践、开发规范、指标监控、灰度发布、限流熔断等内容。

1.3. 服务化探索

针对上述能力项需求与架构演进方向，安信证券服务化实践主要包括以下几个要点：

（1）演进式架构设计。实际的研发过程中，大部分业务系统的服务拆分并不是一蹴而就，当出现有多个功能模块紧耦合、不同模块需要根据业务需求独立演进等情况下才会考虑适当拆分，否则，单体架构或者“小服务”（拆分粒度相对微服务低）更能简化系统的开发、测试和运维等阶段中的复杂度。

（2）解决实际问题。从应用的全生命周期考虑，在研发阶段提供脚手架、开发规范并约定服务间通信协议、结合 CICD 流水线和容器云平台等基础设施赋能业务系统；在运行阶段，以应用的可观测性（主要包括指标、链路和日志数据）为中心收集并展示其运行状态数据，同时提供多种规则实现异常状态的告警。

（3）结合容器云落地。随着安信证券容器云平台建设的完善，并规划全部自研业务系统“上云”，微服务架构基于容器云平台落地，有效解决运行环境和操作系统的标准化、应用灰度发布和弹性伸缩等复杂操作。在服务治理方面，优先考虑 Kubernetes 和 Service Mesh 等无侵入模式，而不是以 SpringCloud、Dubbo 为代表的 SDK 嵌入模式，主要原因是这类服务治理框架会带来一些额外的负担：

注册中心提供动态的注册与发现功能，但不解决网络权限等问题。例如原本两个服务 A 和 B 间的通信，确保 A 和 B 之间的通信正常即可，引入注册中心 C 后，需确保 A 和 B、B 和 C、A 和 C 之间的通信正常，同时，在高可用模式下，还需考虑服务 A 和 B 与多个注册中心实例的通信状态。在金融行业严格的网络防火墙限制下，也削弱了注册中心的动态弹性伸缩功能；

注册中心内外调用容易混淆。服务 A 和 B 间的通信，服务 A 必须明确服务 B 是否注册在同一注册中心，如果是，则使用注册名进行调用（通过注册名动态发现服务 B 的多个实例地址，并进行负载均衡），否则，需要使用 IP 或者域名进行调用。实际使用中，很难在短期内让所有业务系统在同一注册中心注册（一般也不会这样做，风险较大）这两种调用模式往往同时存在，这对开发者极不友好。尽管能够通过一些约定和封装将二者统一，但也增加了复杂性，不利于故障快速分析。

SDK 耦合问题。如果是通过传统 SDK 等方式实现的服务治理功能，则与业务耦合，当服务端升级且对低版本不兼容时，将不得不面临所有业务系统需升级的大量工作。同时，SDK 的耦合也意味着对具体开发语言有要求，无法实现像 Kubernetes 完全与开发语言解耦合。

1.4. 规划路线

结合微服务、容器等技术的演进和业务系统面临的实际问题，制定服务化演进路线如下：

POC（2018-2019）

针对各类低迟延、高并发的业务应用场景，

调研 Dubbo、SpringCloud 等服务治理框架和 Consul、Eureka、Zookeeper 等注册中心方案，探索以 gRPC 通信协议为基础的低侵入服务治理框架 axsi（AnXin Service Infrastructure，安信证券服务化基础平台），支持多种开发语言接入，并提供服务注册发现、负载均衡、容灾容错、服务治理、服务度量等一系列开箱即用的解决方案。

阶段一（2019–2020）

建设配置中心 Apollo、基础框架 SpringBoot、链路追踪 Skywalking 和运行指标 Prometheus、脚手架等基础设施，打通指标、链路与日志等数据以提升应用系统的可观测性，提供数据展示的服务门户、用户对接的详细文档；试点 3 套业务系统，并对接容器云平台。

阶段二（2020–2021）

推动全部自研类业务系统进行服务化改造，根据用户反馈进一步完善基础设施，部分业务系统改造后部署上云，探索基于 Service Mesh 的限流熔断、灰度发布等功能；同期 Nginx/Redis 等常用中间件最佳实践、JAVA/C++/VUE 等一系列开发规范同步发布，进一步提升业务系统的交付质量。

阶段三（2021–）

全面推广基于 Service Mesh 的服务治理体系，将服务治理功能与业务完全解耦，真正实现开发人员只关注业务。

2. 解决方案

为了有效落地阶段一规划内容，安信证券和博云合作研发，基于开源组件 Apollo、Spring Initializr、Skywalking、Prometheus、Grafana、Alertmanager 等进行个性化定制，实现链路追踪、拓扑绘制、用户管理、应用管理、服务管理、配置中心、指标收集、告警规则和历史等功能；规范化服务间通信协议 Restful HTTP（普通场景）和 gRPC（高性能场景）；制定 JAVA 等开发规范并通过 CICD 流水线检查项落地。

2.1. 以应用为中心，整合统一门户

对用户、系统、角色和权限等元数据统一管理，按系统 - 服务 - 运行实例三个层次对应用运行状态描述，提供以应用为中心的服务画像、服务治理和观测告警等功能；展示接口慢响应、吞吐量、接口调用异常等关键运行数据，并根据预定规则进行告警；动态生成服务间链路拓扑图、系统间链路拓扑图；支持中间件指标收集自服务配置；集成审计日志、用户手册等常用功能。

图 2

图 3

2.2. 标准化开发框架，规范化应用环境

标准化开发框架、基础依赖库、配置管理、日志输出等基础组件；结合 CI/CD 流水线提升开发测试和部署效率；实现开发工程脚手架的功能，通过代码自动生成达到基础框架和版本、工具、脚本等进行规范和标准化。

2.3. 横纵交叉，立体展示业务系统运行状态

在传统对应用使用资源的监控基础之上，在业务系统可观测性方面，对链路追踪数据的展示以及和日志数据的联动，同时也收集了 Spring Boot 应用及中间件的运行指标，多维度展示业务系统运行状态，并基于收集的指标二次计算，形成特定场景的告警，例如应用日志错误率、堆内存使用率、HTTP 错误响应码占比、GC 频率等指标超过设定的阈值。

在每个交易日，平台会通过邮件将当日的系统运行简报发送至各个业务系统负责人，使其对

图 4

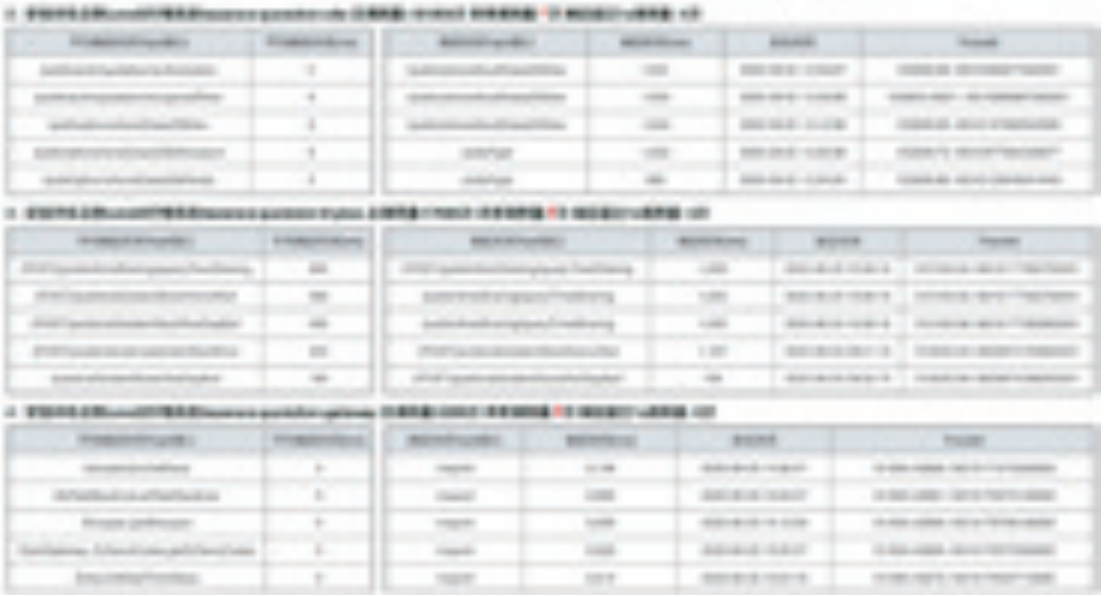


图 5

每天的运行状态了然于心。

2.4. 链路追踪，故障分析之利器

链路追踪，通过自动埋点 TraceId 方式将一次请求完整串联起来，并记录每个环节的耗时，对于接口响应慢等常见故障的排查非常实用，往往能够将一些未发生告警的潜在问题提前发现；另一方面，应用将 TraceId 输出至日志文件，再通过日志收集器统一收集至日志大数据平台，并提供日志查询接口，实现链路和日志数据的关联，更进一步方便用户通过链路和日志数据综合判断故障原因。

3. 实践案例

3.1. 系统介绍

投资秀系统作为早期的试点项目也是改造的标杆项目，积极配合并极大推动了基础设施建设的完善。该业务系统是面向移动互联网用户，线上展示投顾相关产品、观点、以及安信研究报告的窗口，同时也是公司投顾产品的主要营销渠道。主要的功能模块有：组合产品、资讯产品、股票池产品、投顾观点、安信研究、十大金股、策略回顾、模拟下单等。

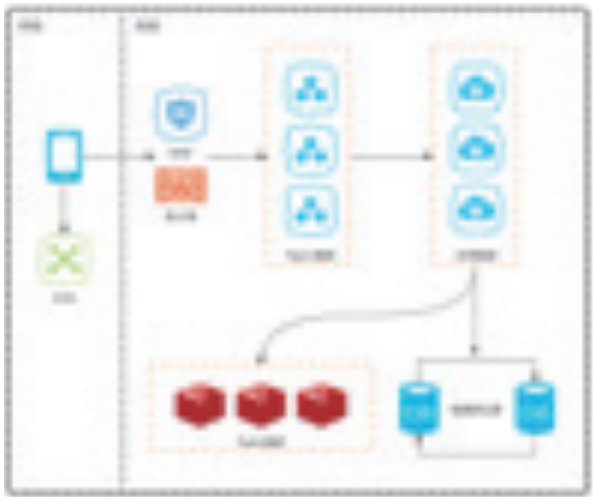
随着业务的发展，对系统的稳定可靠性的要

图 6

求也在逐步提高，同时业务需求的迭代效率也有新的要求，以投资秀系统原有的系统架构已经不能适应当前的要求。

为提升系统的可用性，提高服务能力，提升需求迭代效率，按照平台研发部的指引，引入统一的工程脚手架开展系统的服务化改造。改造完成后将为后续的系统服务拆分，微服务化打下基础。

造前的系统架构图如下：



改造后的系统架构图如下：

3.2. 改造过程

改造步骤：

1. 引入平台服务化的工程脚手架，快速构建 Spring Boot 工程；应用配置分离、多环境配置，为云原生改造打下基础；

2. 开通配置中心、调用链、监控告警等的相关网络权限；

3. 集成 Apollo 的客户端到工程当中，把原有的配置迁移到 Apollo 配置中心；

4. 服务器安装 Skywalking agent，应用日志添加 TraceId；

5. 工程引入 Prometheus 相关依赖包；

6. 工程代码修改通讯接口协议 gRPC 或 Restful HTTP。

实施过程中的问题与困难：

1、gRPC 服务通讯改造的工作量大，或多或少会影响业务需求的迭代；

2、Skywalking 调用链日志埋点 TraceId 为空的问题，该问题还是费了一点时间，经过服务化项目组的通力协助才得以解决。

3.3. 实施效果

改造完成后，我们可以通过配置中心快速便捷的统一配置应用服务，通过服务门户可以非常直观的监控应用服务的健康状态，通过 Skywalking 可以监控接口的调用情况状态，而 Prometheus 则有服务相关的各种状态仪表。

服务门户见图 7。

应用案例：

2020 年 5 月 25 日，10 时 15 分 Skywalking 调用链告警，tzx-manage 服务接口响应延时达 400ms+。

tzx-manage 是内部的消息接收应用服务，经排查，是从非金融订单系统接收 kafka 消息后的业务处理逻辑较复杂导致，排除非故障后，计划在项目后续的版本进行复杂业务的拆分来优化。

3.4. 后期规划

目前投资秀系统已经完成服务化改造，根据业务边界进行了业务拆分，并已将部分服务迁移至容器云平台，前期以虚拟机与容器并行的方式，

图 7

保持系统平稳过渡；后期对新业务功能需求直接以云原生架构方式进行建设，并部署于逐步完善的容器云平台基础设施，同时将存量虚拟机部署的服务逐步迁移至容器云平台，最终下架原虚拟机的应用服务。

在服务治理方面，依托容器云和 Service Mesh 等基础设施实现无侵入式的限流、熔断和灰度发布等功能，逐步将业务代码中耦合的非功能性需求代码下层至平台。远景效果见图 8。

4. 总结与展望

4.1. 总结

服务化基础平台的建设，是以“赋能业务”为第一目标，以“规划先行、逐步迭代”为建设思路，以“产品化建设”为原则，以“建设 + 运营”双路线来促进功能的完善，不重复造轮子，解决用户实际痛点，在平凡中创新。经过近 1 年的投产使用，在平台能力建设方面已逐步完善，并推动自研类业务系统进行改造升级。目前已顺利上线 29 套业务系统、99 个服务和 319 个运行实例，接口调用次数日峰值超过 2 亿次。

本项目的实施，为提升业务系统研发效率和故障定位能力奠定了坚实基础，在平台建设和业务推广两个方面积累了大量的经验，是整个云原生架构版图的重要组成部分。主要的创新点包括：

1. 无侵入式调用链可视化

如何实现从用户请求到应用、中间件、数据库、以及关联系统的全链路展示一直是个工程难题，原因在于各系统有各自不同的用户请求处理机制，有效识别同一用户请求往往需要各系统做代码上的改造，成本相当高。

服务化基础平台通过无侵入插件方式实现对各业务系统方法调用埋点及数据收集，通过全局请求跟踪标识实现跨系统的调用日志聚合，极大提升了跨系统的故障定位能力。根据系统间 API 调用情况，动态生成系统拓扑图，实时显示上下游系统的运行状态、调用频次、调用时长等关键信息，为评估跨系统调用瓶颈提供最有力数据依据。

2、统一技术栈打造云原生快速开发平台

云原生技术生态发展迅速，涉及的概念和可选技术栈庞大，对于传统金融企业，如何打造适

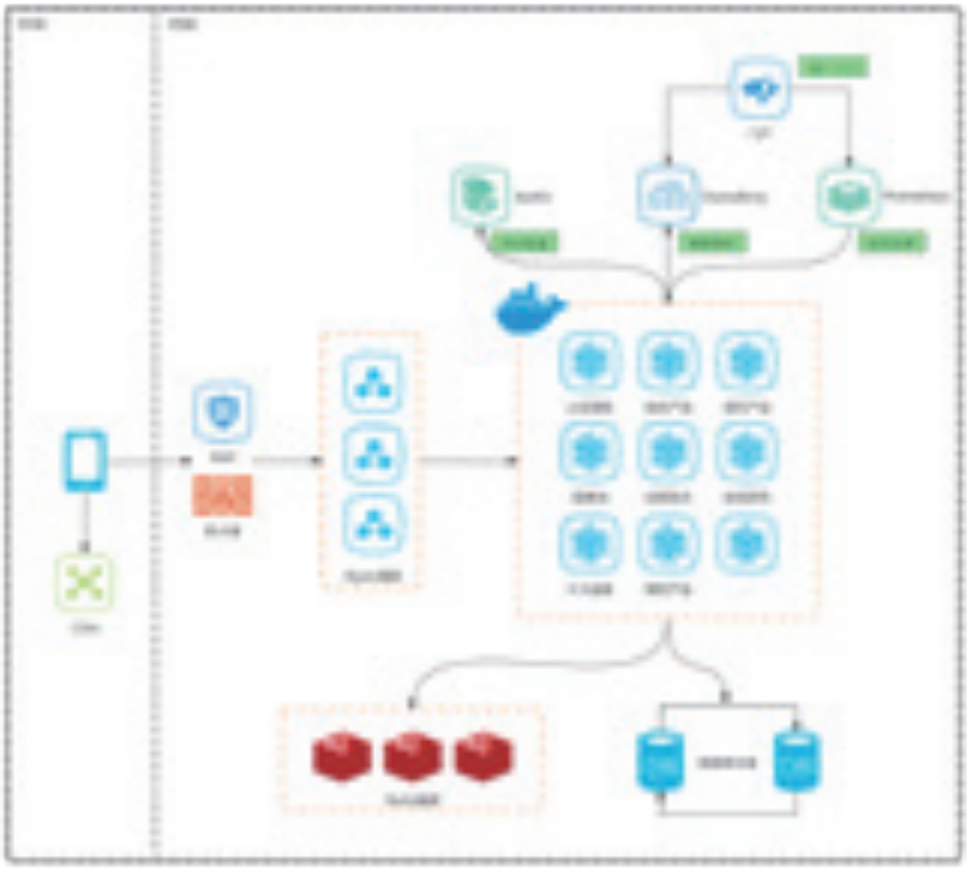


图 8

合自身的企业级落地的云原生基础设施，是一件有技术难度的事情。

基于开源组件定制的云原生应用脚手架，实现一键生成云原生项目工程，能够将项目构建从小时级缩短至秒级。通过将云原生基础能力项标准化，以代码模板的方式固化到脚手架中，实现了所有新建项目的框架统一、配置统一和构建及部署方式统一；通过插件化设计，实现管理平面与业务平面有效分离，平台功能与业务功能升级互不影响。对于已有项目，采用脚手架新生成项目工程、迁移业务代码至新项目，同样可快速升级为云原生应用。

3、基础设施平台化赋能业务系统

服务化平台实现服务治理、运行指标、链路追踪、告警规则等一体化管理，结合配置中心、容器云平台、DevOps 流水线，组成云原生基础设施平台，已成为重要的 IT 基础依赖。通过制订接入规范，各业务系统可按需对接能力项，提升应用可观测性。根据已上线的项目实施过程统计，除少数需要完全改造通信协议项目以外，普通项目 1 至 2 周时间即可完成首次平台对接及验证，后续逐步形成约定沉淀下来。相比之前各业务系统各自实现上述非功能性需求，无论是建设效率还是建设质量，都有大幅的提升。

4.2. 展望

当前，服务网格是云原生架构的关键技术之一。关于服务网格的概念，借用 Linkerd 维护者 William Morgan 的一段定义：

服务网格（Service Mesh）是处理服务间通信的基础设施层。它负责构成现代云原生应用程序的复杂服务拓扑来可靠地交付请求。在实践中，Service Mesh 通常以轻量级网络代理阵列的形式实现，这些代理与应用程序代码部署在一起，

对应用程序来说无需感知代理的存在。

服务拓扑交互和治理功能是微服务框架中最复杂的技术特性，以前需要 SDK 来承载，意味着对应用是有侵入性的。服务网格就是尝试将治理功能进行物理分离，做到无侵入性，对比 Spring Cloud、Dubbo 这类基于 SDK 实现治理的框架，最重要的区别是治理实现的复杂度全部由代理 (Sidecar，也称为边车) 来承担，使得业务程序层面能彻底放飞自我，甚至连开发语言也不限制了，完全解除了业务功能与治理功能的耦合。只要通讯协议是标准的 HTTP/gRPC，Sidecar 总能捕获到这些流量，进行动态控制。因此，也有人将它称为：微服务 2.0 时代。

服务网格有多种实现，其中 Istio 是当前最为流行的一种，从 2018 年 6 月发布 v1.0 至今 v1.7 才 2 年，发展趋势上虽然也有过曲折，但也渐渐步入被大家广泛接受的阶段。在 ThoughtWorks 2020 最新的技术雷达 Vol. 22 中，Istio 终于挺进了采纳区，对其具体描述如下：

如果正在构建和运行规模化的微服务架构，且已采用 Kubernetes，那么使用服务网格来管理所有架构切面，应当是一个默认选择。在众多服务网格实现中，Istio 是最主流的。它的功能十分丰富，包含服务发现、流量管理、服务到服务以及源到服务的安全性、可观测性 (包括遥测和分布式追踪)、滚动发布及韧性机制等。其最新版本易于安装，并提供了控制面板架构，用户体验得到了改善。尽管我们承认维护自己的 Istio 和 Kubernetes 实例，不仅需要足够的指示，还需要一定的内部资源，可能并不适合能力不足的团队，但在我们的诸多项目中，Istio 在保证运维质量的同时，的确降低了大规模微服务的实现门槛。

随着自研类业务系统逐步地迁移上云，以容器云和服务网格等云原生技术为基础的无侵入式服务治理是未来演进的重要方向。服务网格是安信证券服务化实践下一阶段的主要方向，期望实现开发人员只关注业务，更进一步提升业务系统的研发效率和交付质量。

T 低时延技术 echnology

基于FPGA的超低延时硬件加速行情解析系统

环宇翔、崔建军、郑立荣 / 复旦大学信息科学与工程学院微纳系统中心
高昀、王嘉晨 / 上证所信息网络有限公司

对于瞬息万变的证券交易市场，即时的行情信息是行情系统的基础。快速获取行情信息可以给市场参与者提供更宽裕的交易决策时间窗口，交易者获取的行情信息延时越低，往往意味着越多的交易机会和越大的决策空间。传统的基于软件的行情信息系统，信息的解析一般经过网络层数据获取、协议层数据解析、应用层数据处理等过程，在操作系统和协议层面，存在毫秒级别的上下文切换和软件处理延时，由于操作系统的进程调度和 CPU 主频的动态调整机制，这种延时还具备一定的不确定性。为实现纳秒级超低延时行情解析处理，本文针对上海证券交易所的行情发布系统，采用 Verilog 硬件描述语言，在 FPGA 加速卡上开发了对行情信息流的以太网，IP 和 UDP 以及 FAST 协议的硬件解码，设计了支持指令集编程的微指令加速引擎。与传统的基于软件的方法相比，本文提出的专用硬件处理方案延时可降低 10 倍以上。

一、引言

随着量化高频交易在世界范围内的兴起，超低延时的行情信息已经逐步成为高频交易中不可或缺的环节，对于行情信息延时的优化也从软件层次的优化逐步转移到基于硬件实现的加速方案。现场可编程门阵列（FPGA），作为一种可重配置硬件，为超低延时行情解析提供了定制化硬件设计的技术基础。FPGA 相较 CPU，硬件电路并未完全固定，支持硬件的重构编程，可提供深入到底层硬件电路层次的逻辑优化，因而兼具更大的优化空间和足够的灵活度。FPGA 一般需采用硬件描述语言（HDL）（例如 Verilog 或 VHDL）来进行逻辑电路设计描述，通过专门的编译综合工具，转化成包含逻辑门和电路连接的网表，最终在 FPGA 芯片中载入运行。FPGA 的开发门槛较高，周期较长，因此主流 FPGA 厂商均开始支持 OpenCL 等高层次可综合语言（High Level Synthesis，HLS）的编程，开发风格上更接近 C++ 等高层软件编程语言，屏蔽硬件实现细节，从而加速可编程硬件的开发，但 HLS 无法做到精确到单时钟周期级（Clock Cycle Level）的逻辑优化，无可避免的会带来至少 15%-20% 的性能损失。

为了充分发挥 FPGA 的专用硬件加速特性，本文基于 Verilog 硬件描述语言，设计开发了面向证券行情信息的超低延时专用硬件解析系统。该系统通过 Verilog 实现了低延时以太网通信，支持 UDP/IP 协议的硬件解析，及 STEP-FAST 数据流的硬件解码。相比基于 HLS 的硬件设计，本文采用了流水线硬件设计优化，通过 Verilog 实现了 FAST 的硬件并行解码，解码延时可低至 33 ns，最终包含 UDP 收发及行情解码的整体穿透延时可低至 847 ns。

二、技术背景

（一）行情发布系统

FAST（FIX Adapted forStreaming，适流 FIX）是 2005 年全球金融企业联盟组织 FPL 提出的一种面向消息流的压缩、编码和传输方法。主要是利用消息流中先后传到的消息之间字段数据的逻辑联系压缩需要传送的数据内容，针对不同类型的二进制字段进行高效的二进制编码使得压缩率提高，传输数据大小降低。上海证券交易所现有的 Level-2 行情系统就部分采用了 FAST 技术来优化实时消息的传输，在优化消息尺寸、节省带宽、降低行情延迟等方面都获得了良好的实际应用效果。但对于下游用户来说，开发解码程序有一定的难度。目前的行情解析，主要依赖于基于传统服务器 CPU 的软解析模式，通过调用 mFAST、openFAST 进行 FAST 码流的解码。由于 FAST 数据的流式排布特征，数据前后相关性大，很难利用 CPU 的多线程实现处理并行化。同时，CPU 相对固定的处理模式，无法提供底层更细颗粒度的操作调度，所以 FAST 的软解码延时较高，对 CPU 的负载占用较大，乃是现有行情解析系统的痛点所在。为此，我们提出了基于 FPGA 的超低延时硬件行情解析系统，将 CPU 的重负载解析任务迁移至专用硬件处理，进行电路层次的并行操作优化，并支持模版化配置，降低 CPU 负载，实现行情通讯和解码的整体加速。

（二）行情解析相关协议

在当前的行情信息系统中，行情数据流需要跨过多层的协议才能从物理通信端口，这些层主要由网络通信和 STEP-FAST 数据流交换协议组成，具体包括：

1、以太网层

协议栈的最底层为以太网层。该层提供了网络发送数据包的物理实现（PHY）和媒体访问控制（MAC），可以通过定义数据包的发送者和接收者的媒体访问控制（MAC）地址来识别网络中的端点，并提供循环冗余校验（CRC）以确保数据完整性。

2、IP 层

以太网层之上是 Internet 协议（IP）层。该层将计算机分为逻辑组，并为该组内的每个终端节点分配一个唯一的地址，可用于多播向多个端点发送消息。

3、TCP/UDP 层

IP 层之上为传输层协议，主要有 TCP 和 UDP 两种代表性协议。TCP 协议全称是传输控制协议是一种面向连接的、可靠的、基于字节流的传输层通信协议。UDP 协议全称是用户数据报协议，在网络中它与 TCP 协议一样用于处理数据包，是一种无连接的协议。

UDP 协议相比 TCP 协议，首部开销小，无需多次握手建立连接，因而实时性更高，且支持单播、多播、广播等多种通信方式，虽然其可靠性稍差，但可通过上层应用设计实现可靠传输机制，是低延时通信的理想选择，本文的验证系统即采用了 UDP 协议。

4、STEP–FAST

我国金融信息行业，交易所行情数据目前主要采用 STEP（Securities Trading Exchange Protocol）协议，并基于国际主流金融信息交换标准的 FIX（Financial Information eXchange protocol）协议，根据行情数据的流式处理特征，进行了 FAST（FIX Adapted For Streaming）编码压缩。一方面，该协议定义了各种字段和运算符，用于标识特定的股票及其定价。另一方面，FAST 编码带来的流式数据压缩机制，可大幅减少带宽，但也显著增加了数据解析的复杂度。

（三）行情解析处理方案

目前行情数据流的解析延时主要就来自于以上协议层的处理。因此，现有的行情解析方案也着重于围绕通信和数据流解码两方面展开优化，主要存在以下三种主流解决方案：

1、高性能 CPU

行情解析的延时优化主要集中于软件层对 FAST 解码的优化，结合 mFAST、openFAST 等经过软件优化的 FAST 解码库加速 FAST 解析，从而实现 1ms 级的行情解析处理。

2、高性能 CPU + 基于 ASIC 的智能网卡

此方案在软件层优化 FAST 解码的基础上，通过采用如 Solar Flare、Mellanox、Intel 等公司的专用低延时网卡，配合 kernel bypass 技术，进一步降低通信延时开销，从而达到亚毫秒级的行情解析处理。

3、高性能 CPU + FPGA 加速卡

此方案通过基于 FPGA 的专用硬件电路设计，在硬件层面实现了对网络通信和 FAST 码流解析的处理，CPU 仅需进行上层业务逻辑的处理，占据行情解析延时的数据通信和解码被完全从 CPU 上 offloading，最大程度地降低了延时且减少了 CPU 占用，可实现低至亚微秒级的超低延时行情加速，已逐步成为未来的金融信息交换技术的发展趋势。

三、系统架构

本文针对上海证券交易所的 LDDS 系统行情源，提出了一种基于 CPU+FPGA 加速卡的超低延时行情解析方案。行情数据的通信和解析均在高性能 FPGA 加速卡上进行了 RTL 电路设计实现，该硬件系统主要包括网络通信和 FAST 解码两大部分：

（一）低延时万兆以太网接口实现

不同于传统采用网卡实现网络通信的方式，本文在 FPGA 加速卡上直接实现了高速万兆以太网接口。基于 FPGA 的高速以太网接口采用了如上图所示的架构，物理层采用 Xilinx 公司提供的 PHY IP，MAC 层采用 Xilinx 公司的万兆以太网 MAC IP 实现传输协议的 CRC32 校验码的填充与检测，并通过 Verilog 定制设计了 UDP/IP 协议解析电路。如图 2 所示，数据流模拟电路信号经由

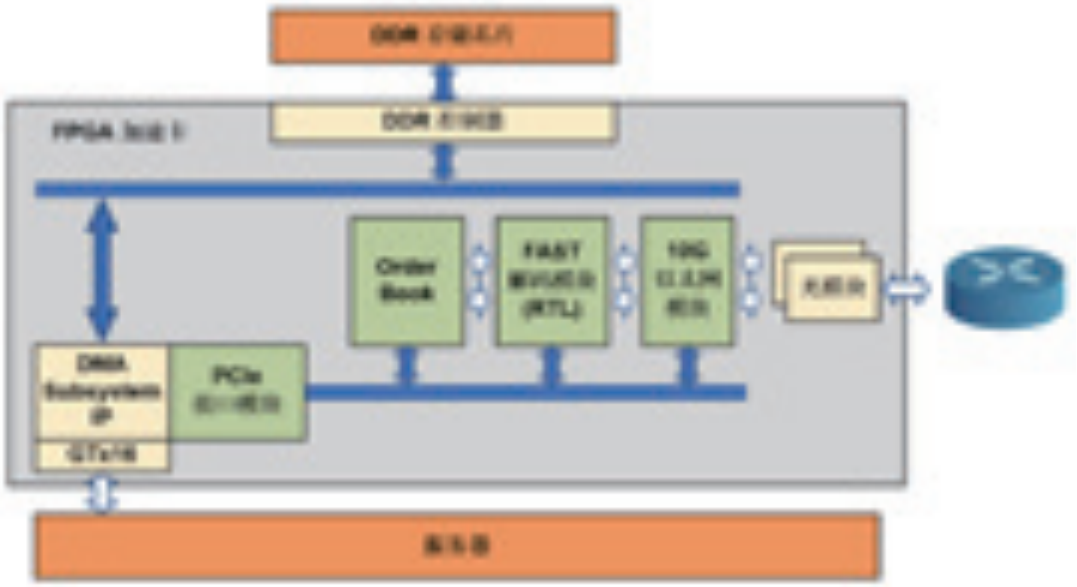


图 1: 基于 FPGA 的硬件行情加速系统框架图

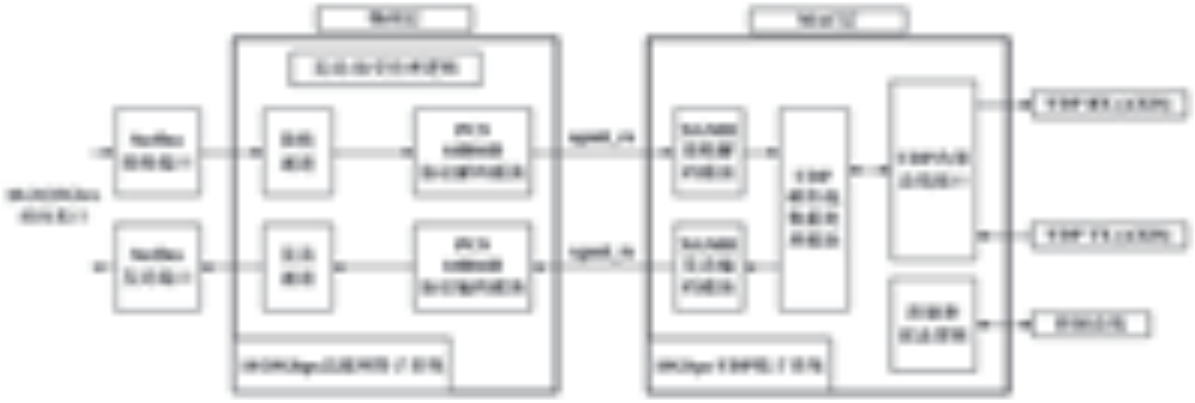


图 2: 低延时以太网架构

高速串行接口 SerDes，配合 PHY IP，实现了对电信号的接收端时钟恢复 / 发送预加重、编解码、通道绑定、数据缓存等，解析出的数字信号数据，将通过 XGMII 接口和 MAC 模块进行数据传递，对发送的数据帧进行编码，对接收的数据帧进行解码。本文中设计的以太网高速通信电路中采用了 64-bit 位宽的单速率 XGMII 总线接口和全双工 10 Gbit /s 的以太网媒体控制器，支持万兆以太网数据的前导码过滤与增加、CRC 校验码的填充与验证，以太数据帧长最小为 64 byte，最大为 1518 byte。发送端在传输数据之前，MAC 控制器会先发送 7 byte 的同步码和 1 byte 的帧首定界符，并在 1 帧传送结束时填充 4 byte 的 CRC32 校验码，如果数据长度小于 46 byte，则会自动在数据字段填充 PAD 字符，即补 0。在接收端，MAC 层去掉前导码和帧首定界符，并对帧进行 CRC32 校验。MAC 层获取的数据将进一步经过 UDP/IP 解析模块的处理，最终转化为实际的 Raw Data。

(二)STEP-FAST 硬件解码

通信接口获取到 Raw Data，仍然不是能直接读取的行情信息，必须遵循行情信息编解码的规范加以解析，本文即在 FPGA 上实现了相应的硬件解析器。

1、STEP 解析器

STEP 协议采用 tag=value，将 FAST 编码的数据流附加额外信息进行了封装，可提供交易行情之外的业务会话信息。为了最大程度降低行情数据解析的延时，本文采用 verilog 定制设计了 STEP 协议的硬件解析器，该解析器模块每个周期从 AXI 总线获取经由网口传递来的 64-bit 数据段，64-bit 的数据段将以 8-bit 为单位进行处理，通过检测“=”和 SOH 的 ASCII 码，自动判定当前数据段所属的 tag 或 value 属性，并发往指定的缓存空间，留待后续的信息读取或进一步的 FAST 解码。

2、FAST 解析器

当 STEP 中的 FAST 数据作为 tag96 的 value 被剥离后，数据将被送入定制设计的 FAST 解码器进行硬件解码。如图 3 所示，原始的行情信息遵循了 FIX 的协议格式，采用了 <SOH> 作为分隔符进行字段切割，字段内的信息则以类似于赋值的 Tag=Value 的形式加以组织。单纯的 FIX 格式的数据码流仍存在较大的存储空间占用，比如每个字段需包含的“=”和 <SOH> 字符、重复的 Tag、Value 类型定义造成的位宽浪费等。针对这些问题，FAST 编码为 FIX 数据流提供了更紧凑的比特流级别的压缩方法，在三个方面实现了数据流压缩：

template 定义减少了重复出现的 Tag 数据。特定类别的数据往往格式相对固定，一般由一组相对通用的 Tag 组成，比如行情快照、逐笔、指数等信息，因此，可以将特定组的 Tag 转换为一套收发双方共同约定的 template 模版来解析数据。在双方都获得数据解析模版的情况下，码流无需再保存 Tag 信息，而只需要按照模版定义的字段顺序和操作组织数据，从而省去了 Tag 数据的传输。

数据操作和数据类型定义减少了 Value 数据的存储开销。此方法主要利用了数据上下文的相关性来减少不必要的数据存储，包括但不限于 Value 数据中可能存在的：数据当前值相教前值保持不变、当前值相教前值差值较小、不定长数据等情形。根据数据的前后关联和 Value 值实际长度，便只需记录历史数据、变化情况、有效数据等相对精简的信息，即可通过反演操作恢复原始数据，能够极大地降低数据码流的存储开销。

单 bit 停止位替代 <SOH> 分隔符。FIX 中 <SOH> 分隔符的使用将导致每个字段无可避免的会附加 1 byte 的存储占用，FAST 编码将字段的分隔改由 byte 数据的最高 bit 位来体现，能够进一步优化码流的压缩比。

采用了上述压缩优化的 FAST 编码，可以大幅降低数据码流的空间占用，数据量可压缩

图 3:FAST 数据流的编码特征

>70%，但同时也对解码提出了较高的要求。软件方案虽然可以一定程度上利用 CPU 处理特性进行解析优化，但 CPU 本身不具备足够灵活的硬件算子或操作来支持精确到 bit 位的解码优化。本文提出的基于 FPGA 的专用硬件解码方案，使用 Verilog 硬件描述语言设计了专门支持 FAST 码流解析的硬件操作算子，通过微指令编码方式提供了底层硬件算子级别的重构能力，不同的 template 可以映射为算子对应的微指令操作，并进行了 FAST 解码过程的操作流水线优化，最终实现了纳秒级别的超低延时 FAST 解码。FAST 解码的硬件设计核心模块包括：

(1) 停止位检测和字段分割单元

该单元以 byte 为单位，在单个时钟周期内完成最高 bit 位检测，判断出当前字节是否为字段停止字节，并根据判断结果，同步更新后续微程序的跳转指令指针，使得已检测的字节能够被立即发往指定的操作算子，在微指令控制下进入解析流水线执行连续的操作。

(2) FAST 解码操作算子

硬件实现的操作算子是 FAST 解码的关键部件，这些操作算子包括：存在图的字段选择、数据移位、计算、复制、尾部更新、字节向量计数、Sequence 字段循环控制等算子，这些硬件经过专门的电路设计优化，可以运行在较高的时钟频率，并且在 1-2 个时钟周期内即可完成对应算子操作（计数和循环控制操作除外）。所有算子模块的控制信号，均由微指令统一整合加以控制，为解码提供了足够的硬件调度灵活性。

(3) FAST 模版解析引擎

FAST 码流解析的规则主要由 template 来定义，因此本文基于微指令技术实现了粗粒度可重构的硬件解析框架。微指令解码器会在每个时钟周期获得当前周期的硬件控制指令，同时翻译为并行的多路控制信号，指示相应模块执行匹配操作。在此框架下，XML 格式的 template 将被翻译为连续的字段数据类型定义、字段操作和流程控制的微程序，FAST 码流将持续的通过数据总线传输给硬件解析流水线通道，在微程序的并行控制下，完成解码操作。虽然各算子模块并行执行操作，但由于 FAST 数据存在前后关联，直接地并行解码难以实现。前后关联的数据遵循相对固定的处理流程，但所处的处理阶段不尽相同，所需占用的硬件算子也并不一样。因此，FAST 数据能够以 byte 为单位，在微指令控制下并行地被调度给当前空闲的硬件算子模块，一方面保证了解析流程的顺序，另一方面仍提高了硬件算子处理的并行度，可进一步提升硬件解析性能。

四、测试结果

（一）测试环境

为评估硬件方案相对软件方案的性能优势，本文在完成了 FPGA 超低延时行情解析系统设计

表 1: 行情加速软硬件对照测试系统环境配置

	发送端	接收端
服务器	Dell s740	WorkStation
系统	CentOS 7.5.1804	Ubuntu 18.04.4
CPU	Intel Xeon Gold 6132 @ 2.60GHz	Intel Core i9-9900KS @ 4.00GHz
通信接口	Intel XL710 10GbE	Intel XL710 10GbE
		Xilinx U200 FPGA

图 4: 行情加速软硬件对比测试系统示意图

的同时，还搭建了软件实现的对照测试系统。测试系统的软硬件环境如表 1 所示。

发送端服务器将读取上海证券交易所的行情源 VDE 中截取的行情数据，通过 Intel 高性能万兆以太网卡，经由光模块同时发往接收端高性能工作站的万兆以太网卡和 FPGA 专用加速卡。本文在接收端同时部署了基于万兆以太网卡的软件接收解码方案和基于 Xilinx U200 FPGA 加速卡的专用硬件行情解析方案，两台测试服务器的通信连接示意图如图 4 所示。两台服务器调用 socket 进行基于 UDP 的行情数据传输，并在接收端完成数据接收和解码。

(二) 测试结果

本测试以 Intel 高性能专用网卡作为对比测试基准，在发送服务器同时发送同样数据给专用网卡和 FPGA 加速卡，进行收发和行情解码的处理延时实测，软硬件对比测试方案架构如下图所示，分别进行了方案整体延时实测和穿透延时测试。

1、整体行情解析延时测试

T_H 为硬件方案总延时，T_S 为软件方案总延时，T_D 为硬件解码延时。测试数据以上海证券交易所 level1 行情的一条 step 数据为例。测试的 STEP 包数据长度为 1515 Byte，其中包括 98byte 的 STEP 头、181 byte 的 FIX 头、1221 byte 的 20 条 FAST 消息，以及 8byte 的 FIX 尾和 7byte 的 Step 尾。VDE 重复发该条 STEP 包，测得软硬件解码的平均解码延时如表 2 所示。

其中 STEP 解码部分的延时在 150us-250us，时间有波动，取决于 CPU 负载；而硬件解码时间固定，无波动。硬件解码延时相比于软件解码缩短了 10 倍以上。

2、穿透延时测试

本文对 FPGA 加速卡上实现的网络通信和行情流解码的穿透延时进行了评估测试，穿透延时从数据到达 FPGA 端的以太网口接收开始计算，截止到 FPGA 端以太网口开始发出经过 STEP-FAST 解码得到的行情数据，包含了 FPGA 端硬件实现的的以太网接收、数据解码和以太网发送三部分，各部分具体延时测试结果如表 3 所示。测试结果显示，FAST 单个字段的解码延时如图 6 的 T1 所示，为 33ns。测试结果显示，FPGA 端的行情穿透延时可低至 847ns。

表 2:FAST 解码软硬件方案处理性能对比

软件解码	硬件解码
示例 STEP 数据平均：217us	示例 STEP 数据平均：14us

图 5: 行情加速软硬件对比测试系统架构图

表 3：基于 FPGA 的硬件行情解析方案穿透延时测试

以太网接收（PHY RX + MAC RX）	STEP-FAST 解码	以太网发送（MAC TX + PHY TX）
430 ns	33ns	384ns

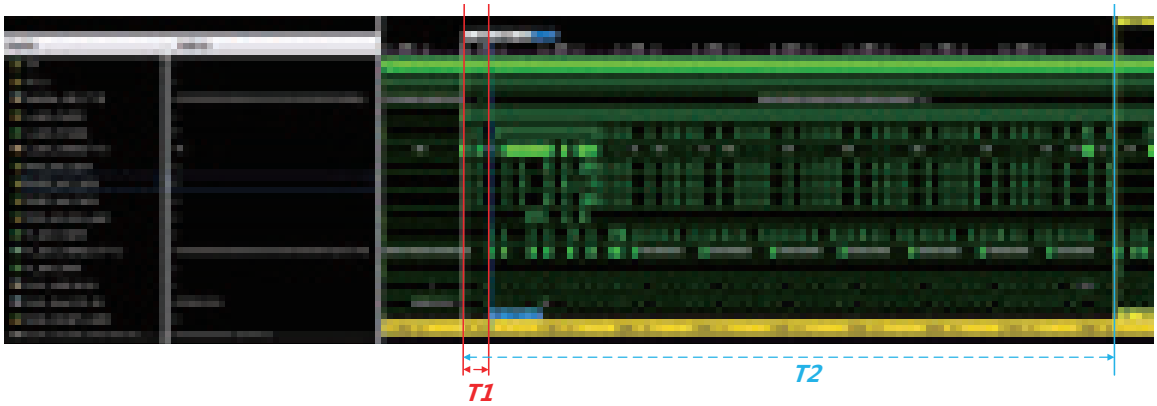


图 6：T1 为 STEP-FAST 解码延时，T2 为单条 UA5302 FAST 数据的解码延时

3、不同模板解码延时测试

从数据流中随机抽取不同模板的一条 FAST 数据测试延时，分别测试了上海证券交易所 Level1 FAST 实时流行情 UA5302，Level2 行情快照 UA3202，Level2 逐笔行情 UA3201 和 Level2 指数行情 UA3113 四种具有代表性的模板数据。测试结果如表 4 所示。对应的延时测试波形图如图 6 T2，图 7 T3，图 8 T4，图 9 T5 所示。

五、总结和展望

行情信息是交易市场运行的基础。及时地获取行情信息，是一切交易发生的前提。随着电子信息技术的飞速发展，高实时的行情信息越来越被市场参与者所青睐，推动着金融信息交换技术向着低延时行情解析的方向不断发展演进。FPGA 以高硬件集成度、高灵活性等优势，越来越受到金融信息开发者的关注。相比较传统的软件实现的行情系统，FPGA 提供了集网络处理、编解码甚至智能算法加速等于一体的集成化可编程硬件开发平台。原有系统中的性能瓶颈功能，均可以转化到 FPGA 平台，进行专用硬件的定制设计和精确到纳秒级时钟的性能优化。本文即面向证券行情信息领域，设计开发了基于 FPGA 的

表 4：基于 FPGA 的硬件行情解析方案不同模板数据解码延时测试

行情 UA5302	快照 UA3202	逐笔 UA3201	指数 UA3113
846ns	716ns	223ns	236ns

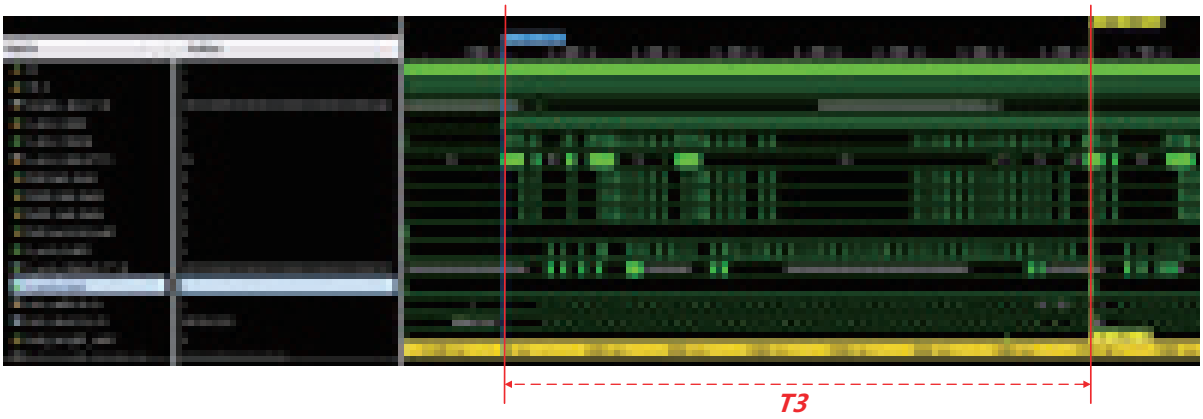


图 7：T3 为单条逐笔 UA3202 FAST 数据的解码延时

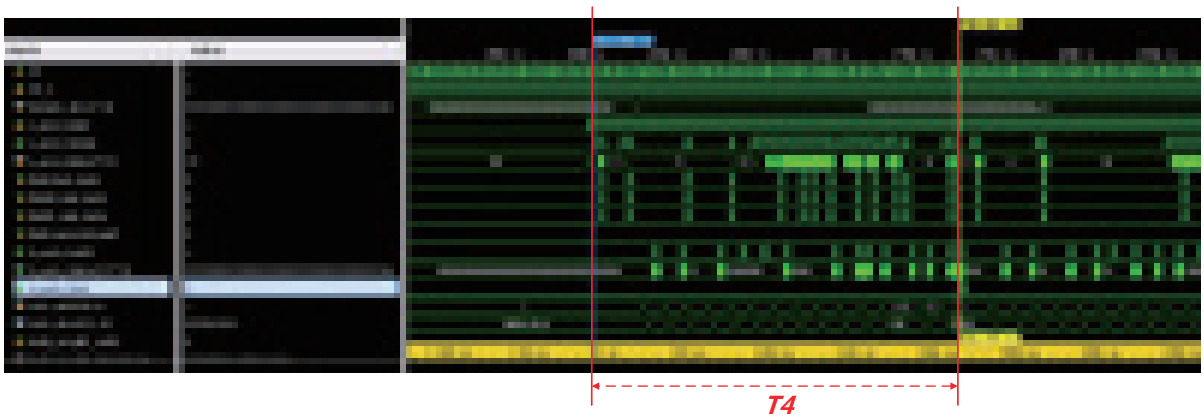


图 8：T4 为单条逐笔 UA3201 FAST 数据的解码延时

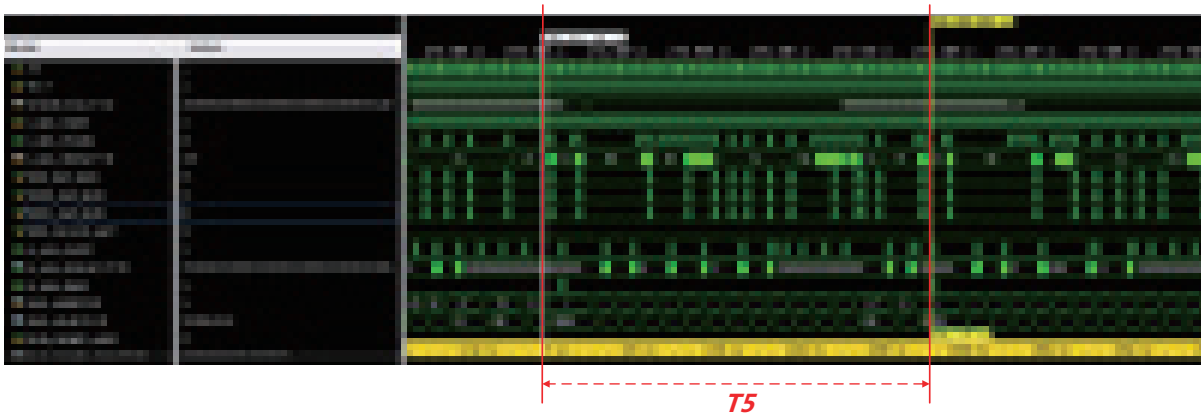


图 9：T5 为单条指数行情 UA3113 FAST 数据的解码延时

超低延时专用硬件解析系统。为了实现超低延时的行情信息解析，本文通过 Verilog 实现了低延时以太网通信，支持 UDP/IP 协议的硬件解析，提出并设计了基于微指令架构的 STEP-FAST 数据流的硬件解码模块，支持根据 template 快速配置解码硬件。通过微指令层次的 FAST 解码流水

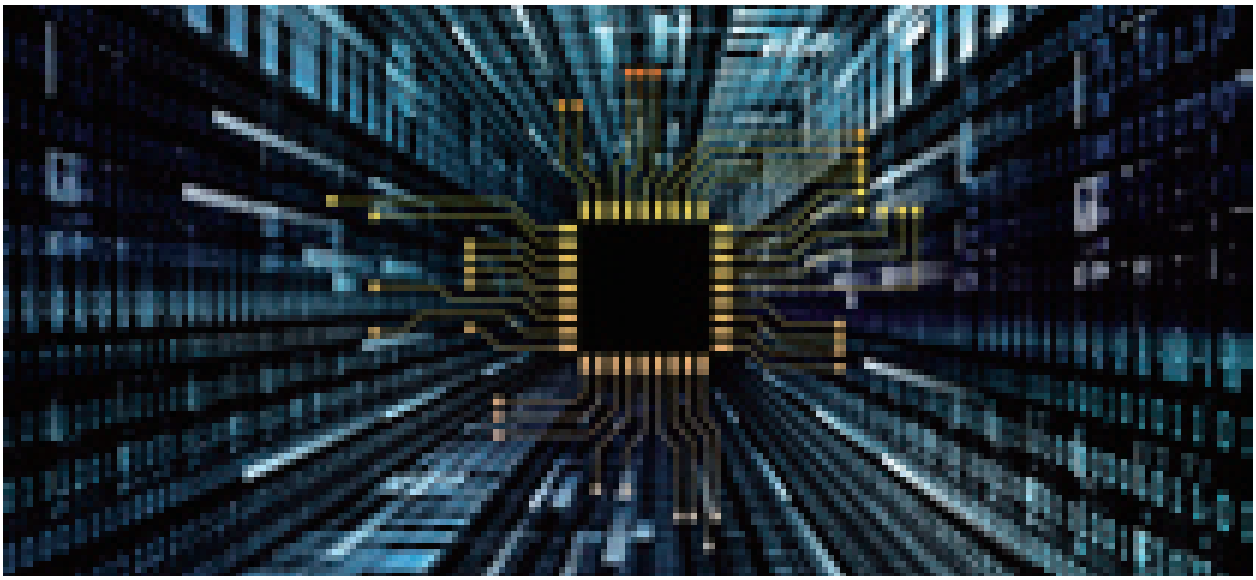
线优化，实现了 FAST 码流的硬件并行解码，解码延时可低至 33 ns，最终包含 UDP 收发及行情解码的整体穿透延时可低至 847 ns。

本文的对行情解析的延时优化主要集中于网络通信和 FAST 解码两大部分的优化，实际的业务系统还会涉及到 FPGA 处理数据与主机 CPU 频繁的数据交互，若未充分优化，则可能由于中断引发频繁的内核态和用户态的切换，大幅提升 FPGA 与主机 CPU 数据交互的延时。针对此问题，未来可在 CPU 端引入 kernel bypass 机制，配合 FPGA 上的高速 DMA 模块，采用轮询方式的 PMD（Poll Mode Drivers）驱动来替代原来 Linux 操作系统的基于中断触发的数据交互机制，使用无中断方式直接操作网卡的接收和发送队列，则可大幅降低系统方案的行情数据解析及业务处理延时，这也将是未来本文系统进一步优化的方向。

本文目前只涉及了行情数据的通信和解码，但行情业务远不止于此。随着大数据、人工智能等技术的飞速发展，行情业务将不只停留在对原始数据的解析，结合新的处理技术和手段，行情信息必定可以被挖掘出更大的价值。FPGA 是传统 CPU 平台的有益补充，提供了丰富的硬件逻辑和计算资源，将是未来新处理业务的良好承载平台。行情硬件解析仅占用了 FPGA 少量的资源，该硬件平台仍存在巨大的空间去承载更为复杂的处理任务，诸如数据库加速、大数据预处理、分布式计算、人工智能算法处理等，为现有信息系统赋能、赋智。行情业务通过 FPGA 实现软硬件结合一体化必将是未来重要的发展方向。

上交所level-2行情OpenCL平台硬件解码

金亭姝 / 国泰君安证券 jintingshu@gtjas.com
马辉 / 国泰君安证券 mahui012430@gtjas.com



随着近年来资本市场的快速发展，投资者对超低延时行情处理、转发系统的需求也越来越迫切。对于算法交易投资者而言，如果能拥有比竞争对手更快的行情，就意味着能在瞬息万变的证券市场里更精准把握买卖时机获取更丰厚的投资回报。FPGA（Field Programmable Gate Array，现场可编程门阵列）以其可编程稳定低延时的特性，成为打造低延时行情和交易系统的理想技术。本文针对上交所 level-2 行情解码转发服务，提出了基于 OpenCL 异构加速平台的 FPGA 硬件解码方案。首先分析了上交所 level-2 行情协议的特点，在此基础上，设计了超低延时的行情硬件解码转发系统的整体架构，详细阐述了解码模块的工作过程和实现难点，最后给出了时延相关的结果和分析。

一、实践背景

上交所 level-2 行情是沪深两地行情中解码难度较大的一类行情。目前业内主要有两种解码方案：一种是基于通用 CPU 的纯软件解码，另一种是基于 FPGA 的定制化纯硬件解码。

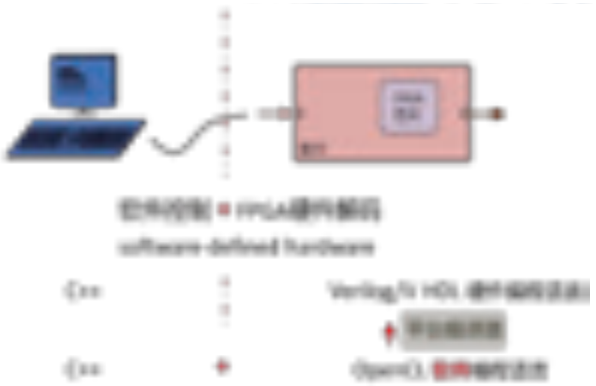


图 1：OpenCL 硬件解码平台

纯软件解码采用 C/C++ 等高级编程语言，开发测试环境友好，开发周期短，在更新迭代上有很大优势。在解码效率上，虽然 CPU 主频远高于 FPGA 时钟频率，但这种基于高级语言 + 通用 CPU 的开发环境，很难完全规避掉编译器编译顶层开发语言至底层机器语言过程中引入的时延不可控。另外，软件解码程序运行在操作系统之上，操作系统的中断机制和线程调度会给整体解码时延带来很大的不稳定性。

基于 FPGA 的纯硬件解码采用底层硬件语言 Verilog/VHDL 来描述解码逻辑，可以严格编程完成特定功能所需的最短延时，但其面向底层的开发逻辑在很大程度上也增加了开发以及维护变更的时间周期（通常以半年计）。

为了结合软件解码和硬件解码各自的优势，我们采用业界 FPGA 主流供应商近年来推出的异构加速 OpenCL 平台对上交所 level-2 行情进行解码开发（图 1）。一方面利用异构平台顶层构建的特性缩短开发周期，另一方面，针对硬件特性，结合平台编译器编译原理，对 FPGA 侧 OpenCL 开发逻辑进行特定优化，成功实现了快速开发、高效解码的异构加速行情链路。

二、上海 lev2 行情协议

2.1. 行情传输协议

上交所 level-2 行情数据采用标准证券交易数据交换协议（STEP 协议）进行封装，即采用标准“tag=value”FIX 消息格式传输行情数据。由于 STEP 数据格式冗余较大，level-2 系统对实时行情的 STEP 数据进行 FAST 压缩编码，并将压缩后的数据嵌入 STEP 消息的 96 号标签（图 2）。

对于一个单独的 STEP 包，35 号标签指示 STEP 消息里行情数据的消息类型，95 号标签指示了 FAST 消息的总长度，96 号标签为实际的 FAST 编码消息数据，这里面可能包含一条或多条同一消息类型的 FAST 消息。

2.2. 协议特点

上证所 lev2 行情这种 STEP 协议内嵌 FAST 压缩的封装格式以及快照行情增量传输的特点，给设计硬件解码程序带来了不小的挑战，具体体现在以下方面：

• 不定长编码

FAST 压缩协议采用停止位编码方式，对于某个行情字段而言，其在行情二进制流里占用字节是不定的，这种不定长编码就意味着不能通过以字节（byte）为单位的内存映射方式获取一个字段的值，而必须深入到二进制流内部，以位 (bit) 为单位对行情数据进行分析。

• 强耦合性

FAST 协议特有的数据类型 + 数据操作的方

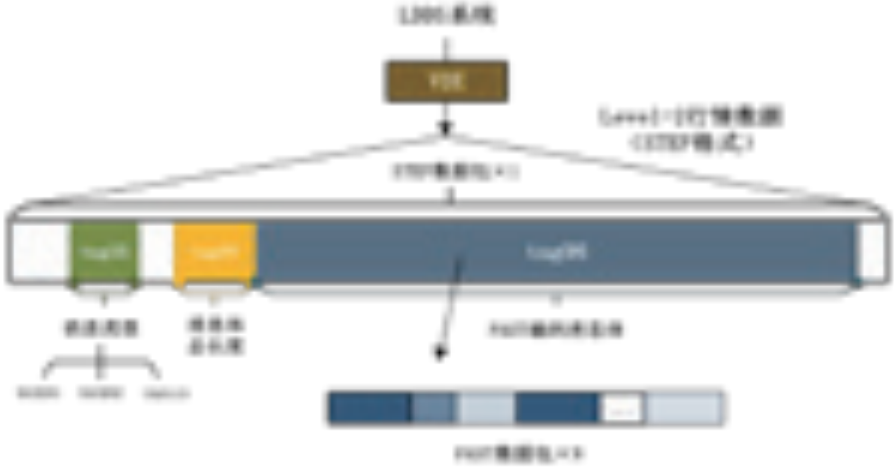


图 2：行情传输 STEP 及 FAST 协议

式导致同一个 STEP 内的多条 FAST 消息有强耦合性，一个 FAST 协议里行情字段在解码时需要依赖上一个 FAST 协议解码完成后的字典值。这种数据流之间的耦合，加大了设计 FPGA 并行解码任务的难度。

• 增量传输

快照行情采用增量传输方式，这就要求解码程序不仅需要正确解出 FAST 压缩的行情，还需要缓存目标行情所有的快照字段并进行正确的更新操作，这对 FAST 解码的正确性、存储空间和读写效率都提出了更高的要求。

三、应用实践

3.1. 总体设计

结合上海 lev2 行情传输协议的特点，在 FPGA 侧，我们设计了图 3 所示架构进行行情解码以及转发。

图 3：总体设计方案

1)TCP_IN

此模块建立与交易所 VDE 程序的 TCP 连接，行情数据经过板卡中集成的 TOE IP 核完成 TCP/IP 协议层解析，提取应用层的行情数据，送至过滤模块。

2) 过滤模块

该模块完成 STEP 消息的解析，根据应用层 35 号标签筛选出 UA3201 逐笔成交行情消息、UA3202 快照行情消息与 UA3113 指数行情消息，并将三种行情消息的 96 号标签内容分别送至对应的解码模块进行 FAST 层协议的解码。

3) 解码模块

此模块是行情解码的核心，主要完成 FAST 协议 pmap 的解析、字段分隔与操作、字典存储、行情字段映射、转发行情协议封装等。

4) 合并分发模块

解码后消息报文统一汇总至消息合并分发模块，由该模块进行调度转发到下一级。

5) UDP_OUT

对转发行情报文进行 UDP 网络协议层封装，最终以组播形式转发至客户。

3.2. 解码模块实现

以 UA3202 消息报文解码为例，图 4 具体指出了解码模块的主要任务。

图 4：解码流程

1)FAST 字段分隔

将过滤模块送进来的 FAST 编码 96 号标签内容按照停止位编码规则进行字段分割，将数据

流以字段为单位进行组织和存储。

2) 状态机嵌套解析

状态机不断根据分割出来的字段和当前所处的解码状态位置进行 pmap 的读取、映射或者内部两层嵌套循环的拆解，将从上一级拿到的字段结合模板操作符进一步匹配到其具体的交易所业务层含义。

3) 量 / 价委托操作

在得到 FAST 解码后的业务字段后，依据证券代码进行当前价格队列及委托队列的增量运算操作，并将运算出来的全量行情进行存储。

对于 UA3201 逐笔成交行情消息与 UA3113 指数行情消息，对应的 FAST 模板不存在二层嵌套以及应用层价位或委托队列的增量运算、维护，通过字段停止位分割与状态机解析，即可得到对应的解码业务字段。

4)RAM 存储性能优化

对于 UA3202 快照行情，因为行情应用层协议包括对买卖十档价上价格、数量以及买卖一档价位上五十笔委托量的操作运算（增加 / 删除 / 更新），所以快照行情解码时不可避免的需要以证券代码为索引存储这些信息。具体而言，在解码模块完成 fast 字段的解压后，需要用证券代码找到关联价格或数量进行增量运算，在增量完成之后，再将增加运算的结果更新到存储。由此可见，快照行情解码涉及到与片上 RAM 进行频繁的数据加载和存储，基于 OpenCL 平台的 RAM 使用和注意事项也成为了解码功能提升以及效率优化的关键。下面列举几点开发过程中成功尝试的优化思路。

• RAM 创建

在创建存储各证券标的行情字段的RAM时，需保证任一证券代码所有行情字段之间 RAM 访问和存储的独立性。对 OpenCL 平台而言，就是让这些需要同时读写的行情字段分配有不同的 Load/Store 逻辑单元。 如图 5 所示，kernel 计算单元在平台编译器编译之后，会有三组 Load/Store 逻辑单元，4 个 RAM Bank 通过 Load/Store 逻辑进行读写，其中 Bank_0 和 Bank_1 可以同时独立的（stall-free）加载或存储数据，而 Bank_2 和 Bank_3 之间有公用的 Load/Store 单元，如果逻辑上需要同时访问 Bank_2 和 Bank_3, 就会造成 RAM 阻塞（stall），降低访问效率。

图 5：独立数据 RAM 存储访问

• RAM 读写

对于增量快照行情，应用层面上的更新逻辑是先从 RAM 读入上一个时间片的行情字段，更新完成后再回写到 RAM，但是平台编译器对 RAM 的读写顺序有默认要求。其为了保证读 RAM 时数据有效，在 OpenCL 语言编译转化过程中，会自动生成相关保护电路保证读操作位于写操作之后。这种默认的优化项不仅会相应增加逻辑资源的使用，更是影响了整个解码效率。针对快照行情解码这类应用，从行情数据接收时间的先后顺序来看，完全可以保证读 RAM 时数据是有效的。因此，可以通过适当的编译指令阻止编译器对 RAM 读写顺序的自动优化，从而进一步提升板卡运行频率和解码延时。

• RAM 空间利用

存储快照类行情增量运算的行情字段需要很大的 RAM 空间，对板卡 RAM 资源提出了很大的挑战。以我们使用的 Intel 中端开发板卡为例，板卡共有 RAM 资源 5.25MB，除去 OpenCL 平

台占用的固定存储空间以及 TOE IP 核所需的存储空间，板卡剩余 RAM 资源可用不足 2MB，存储一只证券行情需要近 800 字节的存储空间，因此，理论上板卡最多能存储约两个代码段的快照行情。而上交所仅股票就有 600/602/603/605/688 五个代码段，这意味着仅支持上交所股票类行情快照的解码就需要 2 块板卡，考虑支持基金和债券的快照行情则需要更多。因此，单从节约成本、系统部署及运维简易性的角度，对 RAM 空间利用率进行优化十分重要。

图 6：离散存储空间哈希映射

针对证券代码分段配置的特点，我们在优化过程中选择合适的哈希映射函数，将离散地址的证券代码存储转化为连续地址的存储映射（如图 6），充分利用了板卡可用存储，容纳了更多代码段的行情信息。目前，经过优化，在我们所用的板卡上，快照类行情可以支持上交所全部股票、ETF 基金、可转债以及部分 LOF 基金。

3.3. 解码延时分析

解码延时采用 FPGA 板卡内部打点计时的方法进行测量。为了保证业务逻辑的完整性，测量计时自行情数据第一个字节进入板卡开始计时，解码行情报文出最后一个字节停止计时，包含完整的 FPGA 应用层解码时间以及业务包发送时间。解码上下游均采用万兆网络进行行情数据收发。

在上述测量方法下，对于只含有一个 FAST 消息的 STEP 行情包，测得指数类行情解码加发送延时 1.5μs，逐笔成交类行情解码加发送延时 1.28μs。针对单个指数类或逐笔成交类行情，解码前输入的 TCP 行情数据包和解码后输出的 UDP 行情报文都较小（不超过 100 字节），上述两类行情包的测量延时可以近似为内部解码延时。

相比于指数行情和逐笔成交行情，快照类行情业务字段多，解码前后的数据包较大。以解码后输出 752 字节 UDP 包体的快照行情包为例，万兆网络满负荷 10Gbps 流速，除去 UDP 层、IP 层以及 MAC 层固定包头，行情净荷数据输出流速理论上不超过 7~8Gbps，相当于每纳秒传输 1 个字节。即对于 752 字节的净荷数据，发送延时在总测量时间中至少占用了 752ns，约 0.75μs。对于输入 221 字节的快照类行情包，测得解码及发送延时 3.1μs，其中输出固定延时约 0.75μs，可以近似认为相当于 TOE 网络层穿透延时。

表 1：快照、逐笔成交及指数测量延时统计

行情包种类	解码延时（含发送）
快照 (752–byte)	3.1us
逐笔成交	1.28us
指数	1.5us

与软件解码线程内串行解码的逻辑不同，硬件解码逻辑并行化的优势在测试过程中得到了进一步的体现。与“工厂流水线”类似，一旦流水线正常运转，则理论上输出每个行情包之间的时间间隔仅仅为发送延时，解码延时作为流水线的级数只在最初影响整体延时的绝对偏移。在图 7 所示测试对比中，测试二为一个 489 字节含有

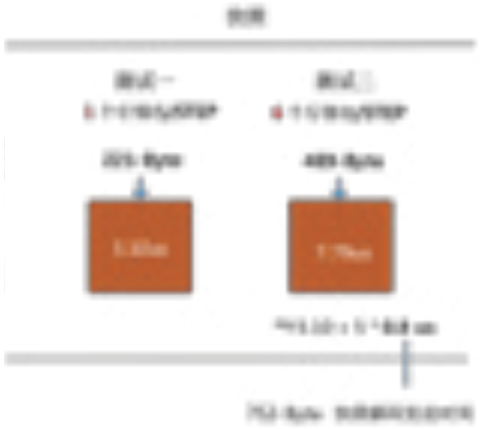


图 7：多 Fast 报文时延测试对比

表 2：压力测试流量统计

测量时间	上游（交易所）TCP 发包个数	下游（客户端）UDP 收包个数
0:00:10	0	0
0:00:20	609633	4254261
0:00:30	553637	3657249
0:00:40	554211	3643970
0:00:50	555131	3580034
0:01:00	555547	3671346
0:01:10	554028	3756451
0:01:20	446910	2443601

6 个同类 FAST 行情的 STEP 包，测量延时 7.79 μs。与测试一相比，测量时间差相当于 5 个行情包发送时延累加。

此外，板卡解码程序经过 20 倍于交易所流量的压力测试。压力测试采用交易所全天实盘行情数据进行 80 秒极速回测，FPGA 板卡平均每十秒向下游发送近 357 万个 UDP 行情包，运行结果正常，下游组播无丢包，行情数据都正确。下表以每十秒为单位，分别统计了上游（交易所）发送及下游（客户端）接收在 80 秒测量时段内每十秒的发 / 收包流量。

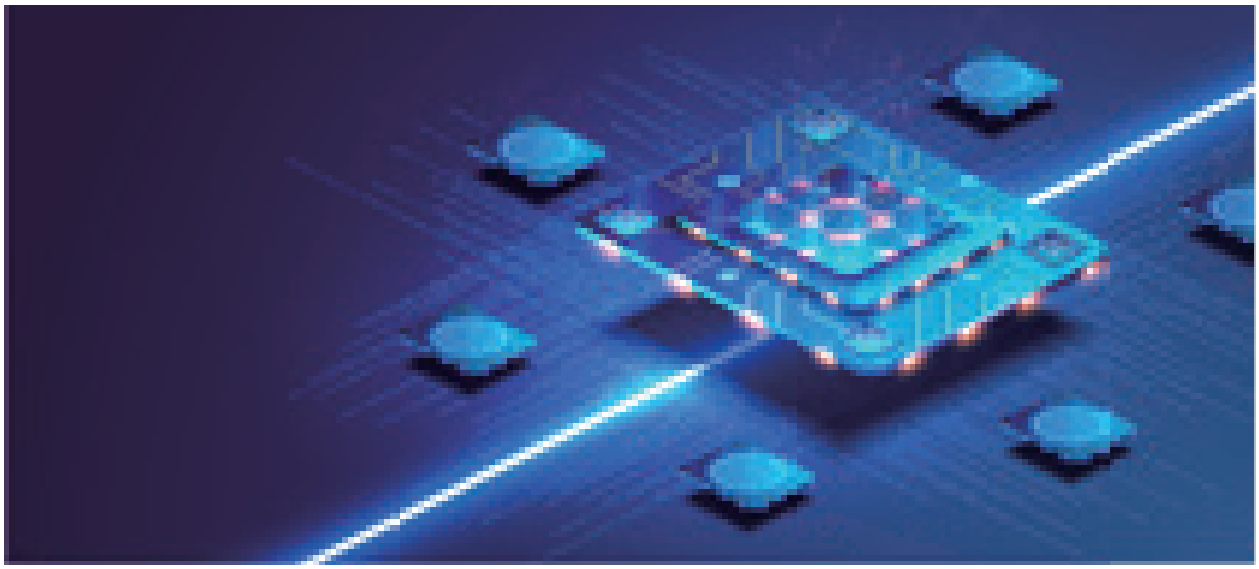
四、总结与展望

本文介绍了在 OpenCL 平台上开发上海 level-2 行情解码转发系统的难点、设计思路、优化与测试方法，这是我们将硬件加速技术运用到复杂金融应用上的一次探索和成功实践，目前我们开发的这套超低延时行情系统已在生产环境稳定运行近半年，客户使用反馈良好。

在异构加速产业化布局的大趋势下，我们希望结合 FPGA 与 CPU 各自的优势，开展更多金融领域加速技术的研究和应用，为行业输出更多的经验。

基于OpenCL的硬件期权风控研究

邹经纬、马辉、金亭烨、孙越 / 国泰君安证券股份有限公司
钟浪辉 / 上交所技术有限责任公司
黄琦、余洋样、朱兆俊 / 英特尔移动通信技术（上海）有限公司



股票期权为证券市场里面非常重要的衍生品之一，也是基础的风险管理工具。由于其 T+0 的属性，市场对其交易速度的要求非常高，竞争到微秒级。期权本身属于高风险的交易品种，因此，期权交易的风控至关重要。当前的软件风控方案大多为毫秒级，一些使用内存数据库实现的可以做到几百微秒。基于软件的方案已经逐渐接近极限，因此，需要研究基于硬件实现的风控方案。我们选择 OpenCL 这一高级语言，进行 FPGA 期权风控的开发。通过快速迭代和深度优化，实现了基本的验资、验券风控的功能，达到了纳秒级的性能，验证了基于 OpenCL 开发硬件风控的可行性并提供了解决方案。

一、研究背景

股票期权是国际市场上成熟的衍生品，也是基础的风险管理工具。上海证券交易所 2015 年 2 月 9 日上市交易上证 50ETF 期权合约品种，能更好发挥证券定价、风险管理、资产配置、流动性中期的功能，提升蓝筹股市场的深度和吸引力，服务上海国际金融中心建设。随着中国股票二级交易市场基础性系统性能的逐渐提高、监管制度的逐渐完善，对于更加丰富的对冲工具也提出了更多的需求。2019 年 11 月 10 日中金所发布“关于沪深 300 股指期权合约及相关规则向社会征求

意见的通知”后。ETF 期权新品种推出的时间线逐渐明朗，随后 2019 年 12 月 13 日深交所发布“深交所全力保障沪深 300ETF 期权于 12 月 23 日平稳上市交易”通知，上交所发布“上海证券交易所开展沪深 300ETF 期权上市交易获批”通知，中金所发布“沪深 300 股指期权将于 12 月 23 日上市交易”通知，三个新期权品种已将在本申请编辑之后一周内上线，变成可交易的实际标的物。

在期权市场上，为维持市场的流动性、满足公众对投资者的投资需求，由具备一定实力和信誉的金融机构作为做市商参与进去，给市场提供连续的双向报价，促进交易的活跃，增加市场的流动性，满足投资者交易的需求，因其参与了价格决定过程，有助于改善投资者的预期，稳定市场情绪。但由于现有系统中风控模块的穿透时延过高，对做市商策略带来大量的延时成本，导致做市商难以对市场提供有效的流动性。

FPGA 作为可编程硬件，已经在证券期货领域得到了广泛的使用，特别是在期货市场。硬件行情解码、硬件风控系统、硬件柜台系统等已经被充分的验证过，是高效、可靠、极速的解决方案，能极大的降低交易系统延时。

二、研究目的

本研究旨在通过 FPGA 技术，提升千万规模做市单的情况下的风控处理能力，降低交易延时。基于协议对接，方便对接各个现有的交易系统，满足其风控业务需求。通过 OpenCL 开发，探索更高效快捷的 FPGA 开发路径，并将其应用到期权业务中。

三、基于流式协议的 FPGA 期权做市风控方案

3.1 期权风控业务介绍

沪深证券交易所的股票期权风控一般有如下几条。

3.1.1 持仓限额

每个股东账号持有的单个合约品种不得超过交易所持仓规定的限额，又分为总持仓、权力仓、当天买入开仓、当天卖出开仓。而且从严管控。

3.1.2 防对敲

单个期权账号的委托，不能与该账号的未完成委托自成交。

3.1.3 验资验券

针对资金账号，对每笔委托校验资金和持仓。

验资，保证金、权利金、费用占用不能超过结算账号里面的资金，否则被交易所直接打回。

验券，平仓合约数量不能超过剩余可平仓合约数量（累计可平仓合约），否则被交易所直接打回。

3.1.4 涨跌停限制

单笔委托的价格不得超过期权合约的涨跌停价格。期权合约信息文件中有涨跌停信息、合约代码、保证金等信息。

3.1.5 委托参数合法性校验

期权交易的申报数量为 1 张或者其整数倍，限价申报的单笔申报最大数量为 50 张，市价申报的单笔申报最大数量为 10 张。委托的委托方向是否正确合法。还有委托金额是否为最小变动单位的整数倍等等。

3.2 PAC 板卡介绍

Intel 的自主品牌 PAC（Programmable Acceleration Cards），该卡可部署在各种服务器中，适用于许多细分领域，如大数据分析、人工智能、基因组学、视频转码、网络安全和金融交易等。可以和 Intel 的 x86 服务器构建异构加速平台，并采用统一的编程平台进行开发。

该卡主要器件是 Intel Arria 10 GX FPGA，板上有 8GB DDR4 和 128MB Flash，更为关键的是它为开发人员提供了通用的开发接口，包括驱动

程序、应用编程接口 (OPAE[Open Programmable Acceleration Engine] API 以及 Intel Quartus Prime software and the Intel FPGA SDK for OpenCL Application Developers) 和 FPGA 接口管理器，搭配加速库和其他开发工具。纯软件工程师 (C/C++) 就可以开发 FPGA 应用，降低开发人员资质要求的同时还节省了开发人员开发、调试 / 优化的时间。

3.3 OpenCL 介绍

OpenCL（Open Computing Language）是首个开放式、免费许可的统一编程模型，能够在异构系统上加快算法速度。OpenCL 支持在不同的平台上使用基于 C 语言的编程语言开发代码，例如 CPU、GPU 和 FPGA。OpenCL 的主要优势在于它是一个可移植、开放式、免费许可的标准，这是它与专用编程模型相比的一个关键优势。

对于软件工程师而言，OpenCL 是一个编程模型，对于系统架构师来说则是一种方法。它基于支持扩展的标准 ANSI C（C99）来隐藏并行性。此外，OpenCL 还包括一个应用编程接口（API），支持主机与硬件加速器进行通信（一般通过 PCIe）通信。

传统的 FPGA 开发一般选择硬件描述语言（如 VHDL/Veriolog），开发周期长，难度大，对于 C 语言类的软件工程师而言，进入的门槛非常高。

Intel 提供一套非常高效的 Intel FPGA SDK for OpenCL，助力软件工程师更快更有效率的进行 FPGA 开发。OpenCL 这一语言标准基于 C99 标准，进行了扩展，加入了并行指令集和语法，以及异构设备（CPU-FPGA）之间的任务调度。同时，Intel FPGA SDK for OpenCL 还提供了独有的 Channel 指令集，实现任务并行计算。而且，可以很自然的描述在 FPGA 中实现的并行算法，包括数据并行和任务并行两种模式。其功能抽象也远高于硬件描述语言。

使用 OpenCL 开发 FPGA，可以加速 FPGA 开发周期。在开发完 OpenCL 代码之后，使用 Intel FPGA SDK 可以直接利用 gdb 进行 Kernel 代码的调试，仿真速度快，类似于 Linux 下用 gdb 调试 C 程序。在功能调试完成后，还可以利用 Intel FPGA SDK 的性能优化工具和资源查看工具进行进一步优化，例如添加 const 关键字、隐式推导寄存器、合理 unroll 循环等等减少资源消耗，查看代码的流水线图优化流水线结构。保证功能正确性后，可以使用 Intel FPGA SDK 进行编译生成 FPGA 的 aocx 文件（类似于 FPGA 的 bitstream）。SDK 也提供上版运行的性能分析工具，在 FPGA 上运行完 Kernel 程序之后，可以得到每个 Kernel 的运行延时分析报告，方便进一步优化性能。

CPU 与 FPGA 之间的交互一般采用 OpenCL 提供的 C、C++API 接口，底层 BSP（Board Support Package，板级支持包）。这样，在利用 OpenCL 开发 FPGA 程序之后，在 CPU 侧可以使用 API 的方式调用 FPGA 上的 Kernel 进行计算，实现加速。CPU 与 FPGA 之间的调度分为两种，同步和异步。在业务程序运行过程中，还可以利用 FPGA 的 PR（Partial Reconfiguration）部分可重配技术，替换 FPGA 上的加速功能模块，自适应的选择加速功能模块。

3.4 风控方案

3.4.1 方案简述

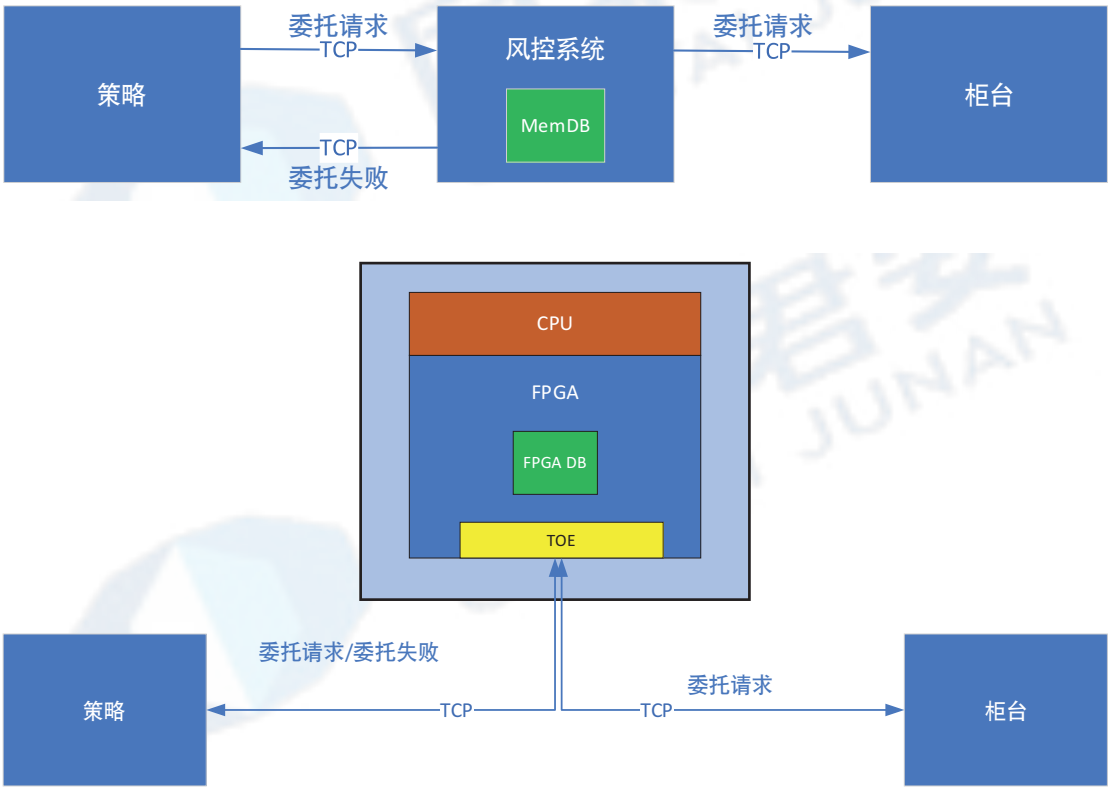
风控是量化交易系统中非常重要的环节之一。风控的速度直接影响委托的速度，因此风控

越快，委托的速度越快，对于量化交易而言成功率就更高。本方案采用 FPGA 负责风控业务的执行，CPU 负责风控业务的控制。

传统的基于 CPU 的风控系统，一般数据都存在内存中，对外提供 TCP 通信的接口。策略通过 TCP 链路委托，该委托经过网卡，到达风控系统的程序内存中，然后风控程序查询风控数据库（多为内存数据库），进行风控项检查，最后返回风控结果。如果通过则转发委托，失败则返回委托失败和失败错误码。一般的风控延时在毫秒级或者百纳秒级。而通过 TCP 通信，搭配低延时网卡，采用内存数据库存储数据，简单的风控延时可以优化到 10us 左右，但是随着委托量的增加，风控延时也会急剧增加。当前证券领域已经进入微秒级甚至纳秒级竞争，需要采用新的方案获取微秒或者纳秒级的风控延时了。

基于 FPGA 的硬件风控方案，就可以获取纳秒级延时。整个风控验证，全部在 FPGA 板卡内进行，无需通过网卡到 CPU 侧内存，节省了这部分的传输延时。而且带有 TOE（TCP Offload Engine）的 FPGA，能够提供远超低延时网卡的 TCP/UDP 低延时通信，因为整个通信链路是通过纯硬件实现。FPGA 本身具备的逻辑资源非常多，可以进行任务并行和数据并行处理，这样可以并行的进行多道风控项目的检查，快速返回结果。相较内存数据库，FPGA 硬件数据库如果使用片内 RAM 作为存储，速度相比 CPU 访问 DDR 更快，并行访问大量数据，在纳秒级完成大量数据的读写。

风控业务方面，本方案支持验资、验券、防对敲等基础风控。在验资时，查找对应客户的可用资金是否足够；验券时，查找客户对应期权标的的持仓数量是否足够。由于账户数量和期权标的数量有限，支持 256 个以内，所以可以利用 FPGA 片内 RAM 存储账户资金和持仓。使用 RAM 存储的有限数据可以在纳秒级完成遍历查找。而委托数据至少万笔以上，RAM 无法存储这么多的数据，PAC A10 的片内 RAM 资源只有



53Mbits，DDR 有 8GBytes，足以存储大量的委托数据。在 FPGA 的委托处理过程中，实时计算着未完成委托的买单最高价和卖单最低价。因此，在检查防对敲时，如果是买入期权，只需要校验委托请求的价格是否超过保存的卖单最低价；如果是卖出期权，只需要校验委托请求的价格是否低于保存的买单最高价。通过这种方式，避免了在委托过程中重新计算未完成委托价格，从而极大的降低穿透延时。而在处理柜台成交和委托应答时，会重新计算出买单最高价和卖单最低价。详细方案设计参看设备程序介绍章节。

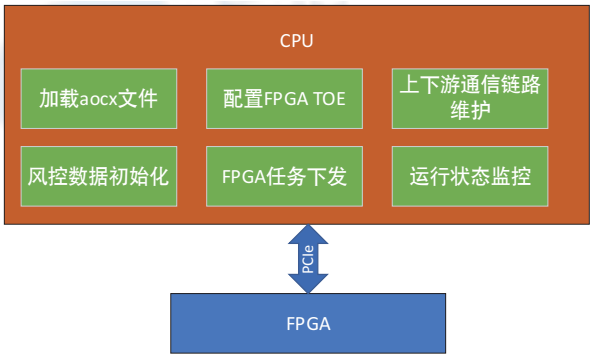
3.4.2 功能描述

硬件风控系统，是采用 X86-FPGA 的异构加速平台实现。风控系统的 FPGA 内部存储了账户每日的账户资金数据、持仓数据、委托记录。每天在开盘前，通过主机程序（CPU 程序）将账户当日的初始资金数据、持仓数据下发到 FPGA 中。FPGA 本身资源有限，因此是限定支持的客户数。而股票期权标的数量一般当日不超过 256 个，活跃的更少，因此本方案限定持仓标的 256 个。由于选择的是 PAC（Arrial 10）的板卡，因此卡上的容量不足以存储百万笔委托，风控的委托表存储在 FPGA 的 DDR 中，不是片内 RAM。

FPGA 内有两个 TOE 模块，可以分别在不同网段工作。客户端或者策略建立与风控系统的 TOE0 的 TCP 连接，风控系统通过 TOE1 建立与。通过这条连接，客户端或者策略，将委托请求发送到风控系统中。如果风控检查通过，验资、验券、防对敲都检查通过，那么就将该委托存储到风控系统中，然后将委托请求通过 TOE1 的 TCP 通道转发到下游柜台系统中。如果风控检查不通过，验资、验券、防对敲任意一个不通过，都会原路（TOE0 的 TCP 连接）返回风控结果，结果中包含风控不通过的原因和对应的错误码。

3.4.3 主机程序

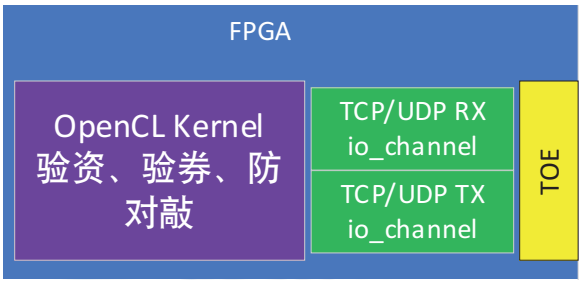
CPU 侧的程序称之为主机程序，一般采用 C/C++ 语言开发，通过调用 OpenCL 主机接口，完成 FPGA 设备的控制。在 FPGA 期权风控方案中，CPU 负责整个风控的控制、风控数据的导入导出等功能。



FPGA 本身没有任何逻辑，依赖于外部给其设计内部逻辑电路。风控业务开发完成后，会生成用于加载到 FPGA 上的 AOCX 文件。该文件包含 FPGA 内部逻辑电路设计。通过主机程序，调用 OpenCL 的接口，可以完成 FPGA 上的业务逻辑的重新配置，即将业务逻辑、TOE 和 PAC 卡本身的静态逻辑加载到 FPGA 中。而 TOE 功能，则需要主机程序先配置 FPGA TOE 的 MAC 地址、IP 地址。风控方案一般是上游连接客户策略，下游连接柜台，上下游通信链路的建立页依赖于主机程序来进行建立和维护。风控本身会需要一些账户初始化资金、持仓、期权基础信息等，这些数据一般只能通过主机程序或者，然后写入 FPGA 内部。FPGA 执行哪些任务，或者执行哪些任务组合，也都是通过 CPU 来控制。最后是整个风控系统的运行状况，FPGA 板卡的状态，也都是交由主机程序来监控。

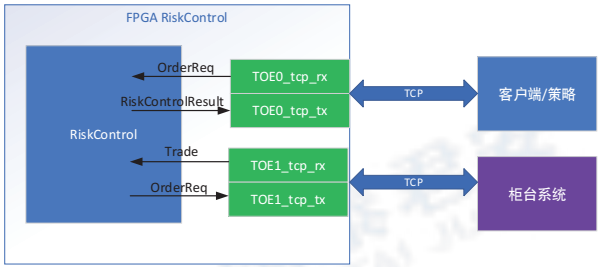
3.4.4 设备程序

FPGA 侧的程序称之为设备程序。采用 OpenCL C 语言开发。不同的任务采用不同的 Kernel 函数来实现。FPGA 内部集成了 TOE(TCP Offload Engine)，通过 TOE 模块，Kernel 代码可以只关注进出的 TCP/UDP 负载数据。本方案所选择的 PAC 板卡和 BSP，将 TCP/UDP 的通道封装成 OpenCL 的 io_channel 形式，提供给开发人员，对接 OpenCL 代码。



FPGA 风控的数据流如下图所示。整个 FPGA 风控系统，通过 TCP 与客户的策略和柜台通信。同时使用两路 TOE，一路 TOE0 处理来自客户或者其他系统的委托单，另一路 TOE1 负责与柜台的通信连接。

客户或者其他接入系统与 FPGA 风控建立连接。在委托时，通过 TOE0 的 tcp_rx 通道传入委托请求 OrderReq。委托请求 OrderReq 进入风控模块后，风控经过一系列风控校验，例如验资、验券、防对敲。如果风控检查通过，将委托请求 OrderReq 转发出去，通过 TOE1 的 tcp_tx 发送到下游连接的柜台中；如果风控检查失败，则将风控检查结果发送到客户或者接入系统，通过 TOE0 的 tcp_tx。



委托报到柜台之后，如果有撤单成交或者普通成交 Trade，这些成交将会通过 TOE1 的 tcp_rx 进入到风控模块。风控模块接收到成交之后更新委托表，重新计算买方最高价和卖方最低价。下图是设备程序的内部 Kernel 逻辑。

四、研究结果

4.1 测试用例

在搭建完系统之后，进行充分测试。本方案简化处理，在测试时只有一个客户，持仓数据 256 条。

经过测试，验证了如下 8 个测试用例，都通过验证。

- 测试用例一，验资通过
- 测试用例二，验资失败
- 测试用例三，验券成功
- 测试用例四，验券失败
- 测试用例五，买单防对敲通过
- 测试用例六，买单防对敲失败
- 测试用例七，卖单防对敲通过
- 测试用例八，卖单防对敲失败

4.2 风控延时及分析

4.2.1 PAC 板卡时延度量

本方案选择的 PAC 板卡和 BSP，带有时延度量工具，可以测试 TOE 进出用户开发的 Kernel 的延时。FPGA 内部有全局计数器，类似于 CPU 的 Cycle 计数器，每次上电复位后，都会持续增长，每个周期增加 1。PAC 卡提供了多个寄存器，用于记录包进出 TOE 时的全局计数器数值。通过读取寄存器的值，可以获取到如下计数器：

TOE0 in: TOE0 输入报文的第一个字节从 TOE0_tcp_rx 通道进入风控模块的计数器数值，对应的是委托请求第一个字节进入风控模块的计数器数值。

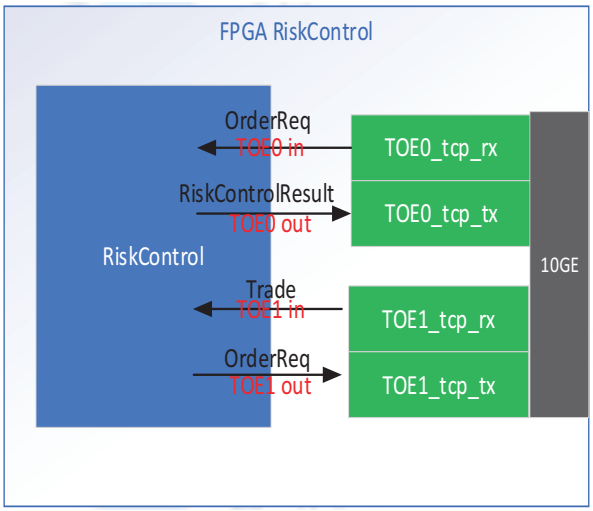
TOE0 out: 风控输出报文的第一个字节进入 TOE0_tcp_tx 通道的计数器数值，对应的是风控结果第一个字节进入 TOE0_tcp_tx 发送通道的计数器数值。

TOE1 in: TOE1 输入报文的第一个字节从 TOE1_tcp_rx 通道进入风控模块的计数器数值，对应的是柜台返回的成交消息进入风控模块的计数器数值。

TOE1 out: 风控输出报文的第一个字节进入 TOE1_tcp_tx 通道的计数器数值，对应的是风控

模块将通过风控校验的委托请求转发到 TOE1_tcp_tx 通道的计数器数值。

TOE 的频率固定为 156MHz，对应周期为 6.4ns，计数器的差值乘以周期即为业务穿透不同点的时延。再加上 TOE 本身进出约 800ns 的延时，就可以得到穿透整个板卡的延时。



风控穿透延时统计方式如下：

1. 风控校验通过时，记录委托请求到委托转发出去的延时：

delay = (TOE1_out – TOE0_in) * 6.4ns

2. 风控校验失败时，记录委托请求到返回风控结果的延时：

delay = (TOE0_out – TOE0_in) * 6.4ns

4.2.2 委托延时分析

通过 PAC 板卡的时延度量工具，测试记录了 8 个测试用例场景下的穿透延时。

测试用例	穿透计数器计算	穿透延时（ns）
验资通过	TOE1 out - TOE0 in	377.60
验资失败	TOE0 out - TOE0 in	326.40
验券成功	TOE1 out - TOE0 in	364.80
验券失败	TOE0 out - TOE0 in	320.00
买单防对敲通过	TOE1 out - TOE0 in	384.00
买单防对敲失败	TOE0 out - TOE0 in	384.00
卖单防对敲通过	TOE1 out - TOE0 in	377.60
卖单防对敲失败	TOE0 out - TOE0 in	332.80

从表中数据可以分析得到，通过合理规划数据存储，可以获得 400ns 以内的风控延时，再加上 TOE 的 800ns 延时，整体穿透硬件风控的延时为 1.2us，而且抖动小，远低于软件风控系统。

五、结论

本研究对 OpenCL 开发数据库进行了探索和研究，以期权风控为业务目标，实现了一套基于协议的 FPGA 期权做市风控系统。该系统主机程序负责控制和调度，FPGA 设备程序负责整个风控业务的处理以及通信的连接。该风控系统可以并行进行多道风控的处理，支持 256 个期权标的的验资、验券和防对敲风控。可以建立多条与客户、柜台的连接，满足多个客户和对接多个柜台的通信需求。整个风控系统支持协议对接，客户可以传输二进制协议进行委托和风控验证，无需额外的 SDK。基于 OpenCL 的硬件风控系统，通过深度优化，可以在 400ns 内完成验资、验券和防对敲业务，穿透延时远低于软件方案，可以获得接近 HDL 开发 FPGA 的性能和延时。

DTP在极低延迟领域的新进展新突破

夏之春 / 上海金仕达软件科技有限公司 zhichun.xia@kingstarfintech.com

本文通过简要的说明方式，对最近几年来金融 IT 领域中交易系统中低延迟领域的研发策略和最新进展进行设计反思和研发解读，同时对系统架构、网络优化路线、性能方法论等方面取得的成果和经验做尝试性的总结分析，希望为同行研究者提供一些参考和启示。

一、技术背景和前景分析

（一）交易系统在分布式服务架构方面的进一步成熟

过去 3 年金融交易系统在分布式领域的进展是全面突出且技术跨越最大的。虽然更早的十年里，金融交易系统已经经历多个演化阶段，出现了基于消息中间件、内存表技术等新交易平台技术的尝试与实践，但在研发投入、成果落地和市场认同方面都无法与近几年的变化相比。不断涌现的新概念、技术和产品促使分布式服务架构的交易体系不断熟化和加速迭代。

过去容错架构的交易平台主要提供 HA 层面的服务保证，无法线性提升扩展服务吞吐能力。但现在，不论是前置、报盘还是交易核心，分布式交易架构都可以通过资源分区的集群模式进行

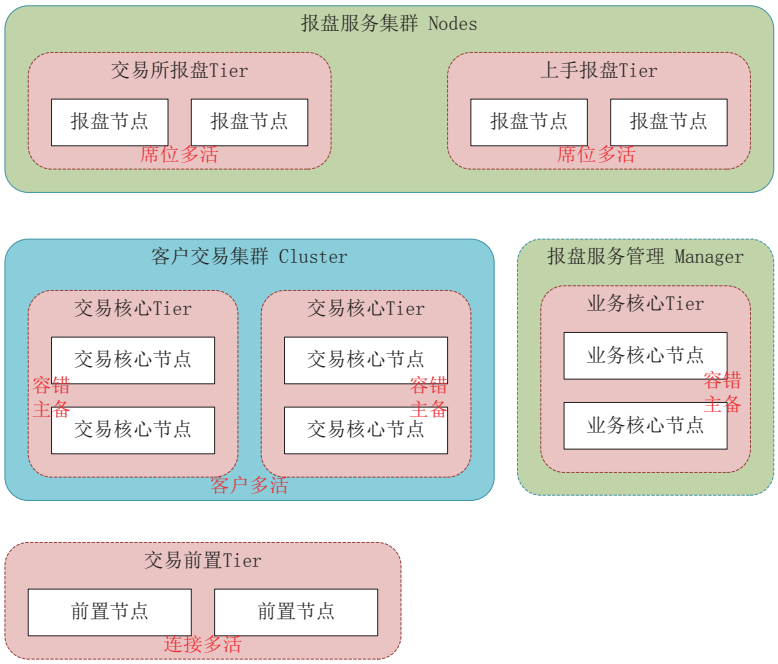


图 1

分布式服务的快速部署，同时不影响应用模块的统一管理，从而彻底解决了服务化资源扩展的问题。

.

(二) 核心处理的极限优化和合作组织化的研发布局

最近几年，期货柜台交易系统的核心处理能力指标的记录不断刷新，出现了递进式相互超越的情况——几乎所有的新交易系统都涌入了微秒级的延迟技术世界。这与软件级内存表或内存库计算技术的普遍掌握和精准使用息息相关。

不断优化突进的核心处理和边缘负载能力将全链路延迟的分析评估目标迅速拉入微秒度量时代。但在实际 IT 环境下，网络和 IO 延迟类成为全链路延迟的高占比部分。为此，在涉及网络交换机、网卡、协议栈、通讯中间件的技术方面，延迟改进工作从未停止，开发方法和度量工具也成为不断取得突破和变革的重点区域。在此趋势下，不同网络设备厂商、交易软件厂商、金融客户，以及客户外围开发组织等主动组队或结伴合作进行多领域技术尝试和共同实践优化。

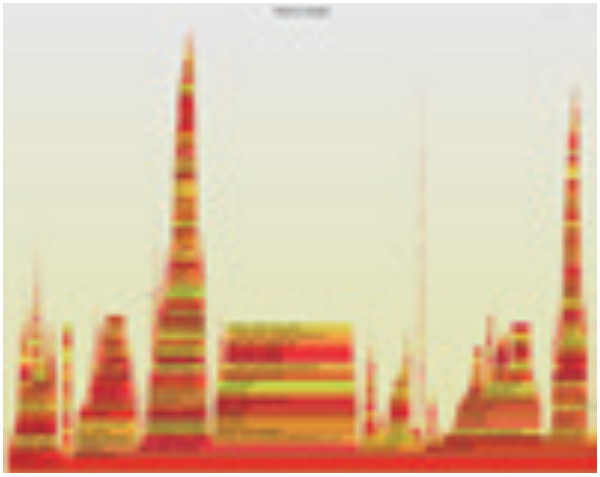
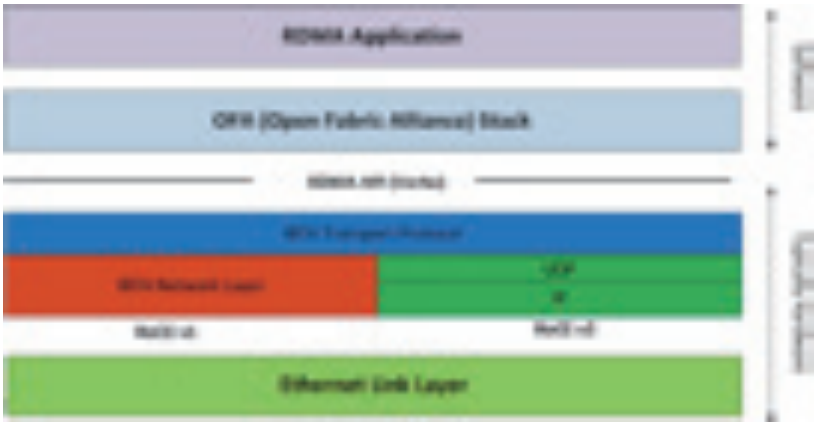


图 2. 某一交易核心应用的运行性能火焰图，其中 IO 延迟类占比多已经显现

(三) 网络吞吐能力和低延迟技术的运用前景

在 IT 部署格局里，网络延迟技术水平一直是影响金融交易系统服务质量水准的核心要素。该要素技术的不断优化发展催生了各种网络特性和部署方案的尝试和实践。鉴于目前金融行业里具备低延迟能力的以太网络交换和网卡技术已经非常成熟和商业化，交易平台开发商必须在此技术条件下，进一步深挖和优化其网络



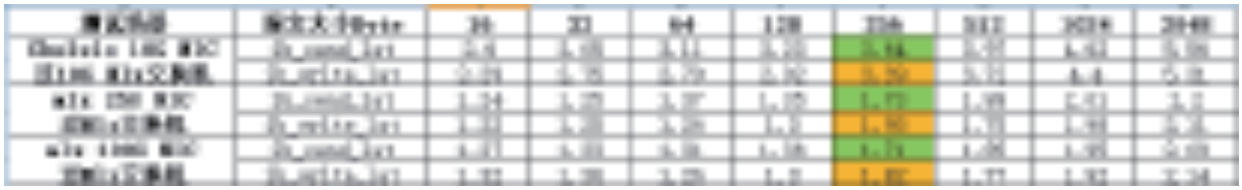


图 3：针对 RoCE 环境进行的不同网络连接条件下的一组评测数据

技术能力在金融交易系统的延迟交换技术方面的实际表现和商业性高回报。RoCE（RDMA over Converged Ethernet）就是在此背景下进入行业的技术视野。

二、RDMA/RoCE 技术的引入和原生开发路线之选

（一）RDMA/RoCE

RDMA（Remote Direct Memory Access）是一种内核旁路技术，它提供了网卡硬件的抽象层 verbs，运行用户空间的进程绕过内核直接访问 RDMA 网卡，实现高效快速通讯。RDMA 源于 InfiniBand 网络技术，由 IBTA 组织对其进行标准化定义和维护。在硬件层面，RDMA 硬件在发送和接收端双方向都通过 DMA 技术直接对用户态内存进行读写，通过使用网卡内置的网络协议卸载引擎，实现数据传输过程中的完整协议处理，不仅大幅降低CPU对网络处理的资源利用率，同时使得时延降至 1μs，网络吞吐量也得到明显提升，是高质量高性能网络通信的首选方式。

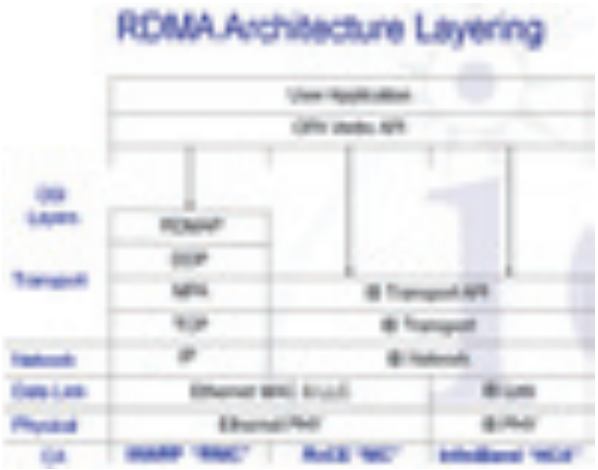


图 4.RDMA 架构布局

RDMA 技术的三个关键技术优势为：

- ▸ CPU Bypass 与 offload
- ▸ Zero-copy 与内存直写 / 读
- ▸ 异步调用与最大化用户态运行

（二）VMA\Onload 和 RDMA/ibVerbs 原生接口的技术对比

在支持 RDMA 接口的开发解决方案里，基于 TCP/Socket 接口的技术方案比较容易被初涉

其间的开发组织关注，因为其开发门槛相对较低，成果变现快，比如 Mellanox 的 VMA 技术。另外，Solarflare 公司的低延迟技术 Onload 也是通过网卡加速技术提供的解决方案，只是其本质不属于 RDMA/RoCE 范畴，尽管如此我们也一并纳入对比分析。关于采用原生 RDMA 接口的想法，是基于我们对各类编程接口和实际环境的实验评测以及对交易系统技术栈的评估而不断演化后产生的，为此我们进行了针对各类交互场景和软件组件以及系统方案级的对比性评测。

在针对标准消息中间件的对比性测试中，VMA\Onload 技术下的指标性延迟表现是比较接近的，相对原有传统网络情况下的延迟优化提升也是非常接近的，但我们在对 RDMA 原生接口情况下的对比评测后发现，原生接口的延迟表现在 VMA\Onload 的表现基础上会有非常稳定和明确的提升，提升比例在 100% 左右。这些因素促使我们更加坚定地采用原生 RDMA 接口技术。

附注：Mellanox 和 OFED

NVIDIA Mellanox 是 InfiniBand 和以太技术世界领先的网络产品供应商。NVIDIA Mellanox 为高性能计算、数据中心、云计算、计算器数据存储和金融服务等市场提供极具竞争力的网卡，交换机，软件，线缆及芯片。公司的 InfiniBand 产品以高吞吐率、极低时延、网络计算等特性牢牢占据了高性能计算领域网络设备的优势市场地位；以太网产品提供 1G/10G/25G/40G/50G/100G/200G/400G 端到端产品解决方案，ConnectX 系列网卡在 25G 及以上速率的高端市场占据过半份额，Spectrum 交换机在全球交换机供应商排名第四，为云客户、运营商、企业网提供极速、弹性优质的数据转发服务。

OFED（OpenFabrics Enterprise Distribution）是 OpenFabrics 联盟的企业发行版。作为是一个传输透明的软件堆栈，OFED 主要用于进行高性能计算和企业数据中心管理。 OFED 虚拟了一个 HCA，安装 OFED 驱动后就可以使用 Infiniband 互联方式，将节点间延迟降低到微秒级，一般的 TCP 通信方式延迟是毫秒级，基本上就相当于本地 PCI-X。

三、DTP 在 RDMA/RoCE 方面的低延迟网络解决方案

端到端全链路网络解决方案的模块布局如图 5 所示。

根据基本适配的延迟层面的阶段分析表格

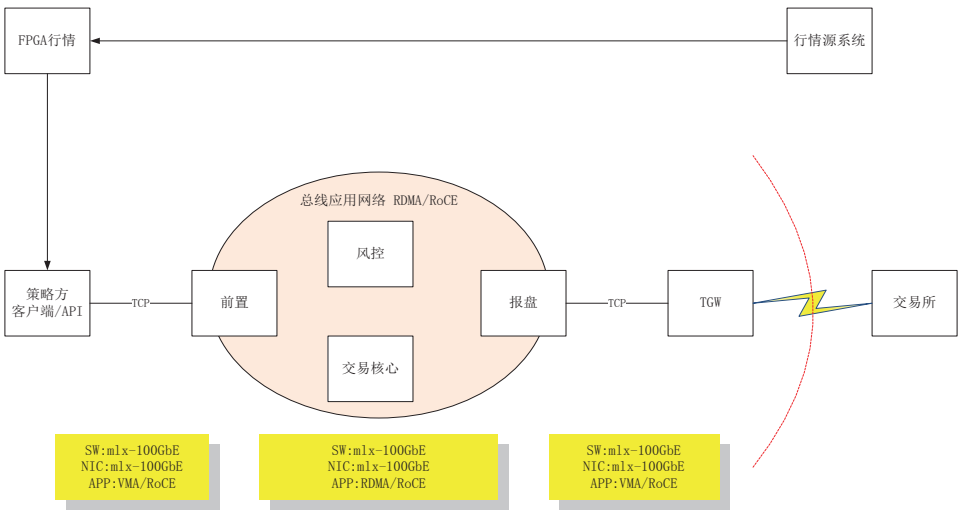


图 5. 端到端全链路网络解决方案布局

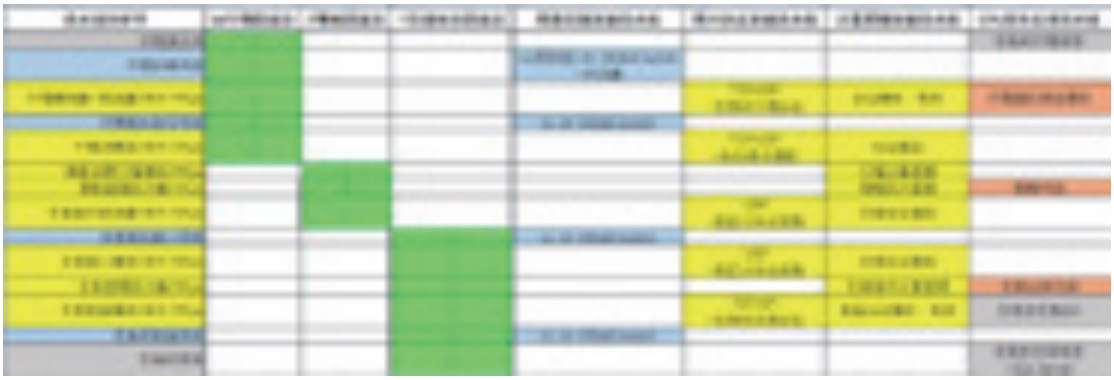


图 6.

（如图 6 所示），在将全链路的技术环节按技术类型分解后，我们需要针对不同类型的技术栈进行加速优化。

其中网络层次和环节的优化项占比较大；关于网络技术方面的方案要素包括：

• 在交易平台的总线应用网络中消息容错总线从基于 UDP 组播方式调整为基于 RDMA/RoCE 方式，全面大幅度优化网络吞吐量和低延迟消息，其效果将内部穿透延迟推进到个位数微秒级别；

• 在策略方 API 和交易前置间采用 RDMA/RoCE 方式替代原先的 TCP 通讯模式，不过作为逐步替代方案，初期可以考虑采用 VMA 方式来过渡；

• 在报盘和 TGW 间，采用 VMA 方式以优化仅为 TCP 模式的限制性应用网络环境；

四、未来极低延迟技术方面在 DTP 领域的发展预测

（一）引入 Infiniband 网络

图 7

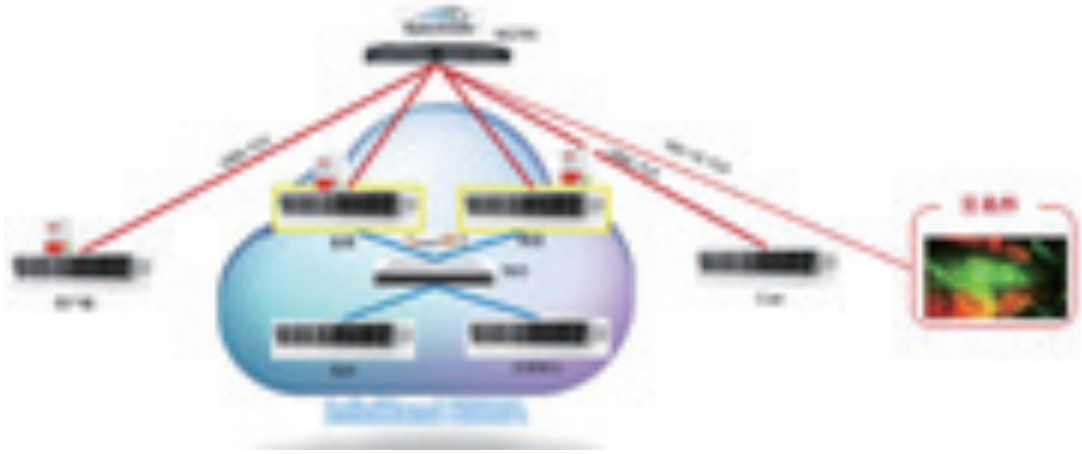


图 8

在支持RDMA的以太网技术世界里，Infiniband是一个传奇般的存在，正是IB的成功历史才真正成就了RDMA的目前地位。在前述网络解决方案里，基于RDMA技术的总线应用网络里，我们希望通过引入IB技术成果，来全面优化和进一步改善极低延迟的技术质量。

图8为我们设想的端到端全链路网络方案中引入IB网络设备/网卡后的系统布局。

（二）引入FPGA网卡和加速产品

在未来的端到端方案中，FPGA技术可以在网络协议加速、业务逻辑加速、甚至柜台整体加速方面提供更加优异和惊人的加速产品解决方案，同时为现有的端到端方案提供更多部署选择和商业模式。

（三）RDMA/RoCE的原生实现RDMA_MSG

RDMA/RoCE的研发技术方面，我们在不断和厂商深入合作的基础上，准备开放性地提供更为基础性的RDMA通信组件RDMA_MSG。该组件通过更为直接和方便的接口方式，为不同通信模式的软件提供统一性的编程接口，用以在替代Socket编程接口向RDMA演化期间，为研发团队提供低门槛高质量的通讯组件。

结语

在过去研发者的基础上推进性能优化的技术工作一向很艰难，尤其是在高层金融产品的技术架构层面。虽然分布式、微服务、高速网卡等面世已有一段时间，但业内在交易系统建设时，牵绊和局限条件依旧很多。在前述的具体工作中，我们充分体会到多层技术栈整合的巨大研发潜力还没有被挖掘出来。这个领域需要不同技术层次的厂商和供应商共同合作才能提供真正完备的高质量高性能的金融交易产品系统解决方案。

0 行业观察 bservation

SD-WAN在证券行业灾备互联应用研究

冯涛、涂鸿安、鲍振华 / 上交所技术 tfeng@sse.com.cn
宋士明、张军、汪洋、周翔 / 南京证券 smsong@njzq.com.cn
刘超 / 思杰公司

证券行业是高度信息化行业，券商作为证券行业的主要参与者，其信息化发展亦是如此。目前券商的核心业务大多数是通过广域网实现的。最近几年，随着券商业务的扩张、数字化转型和云化部署的快速推进，由于 SDH、MSTP、MPLS 等广域网存在价格高昂、开通周期长、运维效率差、管理方式低效等缺点，无法快速、灵活地满足业务需求，致使券商重新评估其 WAN 的设计和部署，并寻求改进措施。

SD-WAN 的诞生满足券商广域网对于扩展性、可靠性和安全性方面的要求。目前，该服务已广泛应用于连接广阔地理范围的企业网络、数据中心、云联网应用及云服务。国内部分大型银行机构在分支网点已有 SD-WAN 应用案例，该技术同样适合为证券行业用户解决广域网互联问题，并基于传统网络提供优化的广域网解决方案。

为验证 SD-WAN 方案在券商广域网应用场景下的技术优势和适用性，上交所技术携手南京证券和思杰公司，探索 SD-WAN 在证券行业灾备互联应用研究。

一、SD-WAN 技术特性

相较于传统组网方案，SD-WAN 组网技术拥有如下特性和亮点：

► 确保业务连续性

SD-WAN 采用数据复制功能，保证关键应用的持续高可用，采用压缩和缓存降低广域网数据传输的带宽，整体上提升应用访问体验。

► 网络与数据安全性

SD-WAN 提供了一种更简单的接入方式，同时提供端到端数据加密，安全验证、防火墙、IPS、防病毒等全方面广域网安全控制措施。

► 云软件部署的适配性

SD-WAN 提供对主流云服务商的支持，可以实现与云市场对接，便于用户快速开通云端 SD-WAN。

► 业务部署快速性

SD-WAN 可以提供零接触部署（ZTD），即通过管理节点或云端推送方式完成，帮助券商以跨数据中心、远程指导、外派人员等方式分钟级快速接入网络。

► 线路接入的多样性

SD-WAN 设备具备接入各种网络介质的能力、路由层面的相应对接能力、根据不同线路的特点来发挥整体 overlay 网络的最大效能。

► 线路感知的实时性

SD-WAN 对于线路的质量具有实时感知能力，进而对流量转发路径做出最佳选择，降低客户扩容频次。

► 流量调度的智能性

SD-WAN 技术可以在广域网线路发生变化的情况下，确保实时应用数据传送的连续性，无需预定义数据流带宽叠加需达到的带宽门限值。

► 应用流量的可视性

SD-WAN 可以实时展示广域网线路质量、具体应用流量统计、网络监控方面的线路情况展现和丰富的报表。

二、证券行业灾备互联组网的现状和痛点

近年来，证券行业网络安全事件呈高发态势，暴露出行业整体备份能力建设覆盖面不全、备份能力等级不达标等诸多问题。为有效解决以上问题，监管机构出台了《证券经营机构信息技术管理办法》、《证券期货经营机构信息系统备份能力标准》等行业指导性的意见，推进证券经营机构开展“两地三中心”等灾备系统的建设。但是，在灾备互联组网方面遇到了一些问题和痛点，主要包括如下：

1、线路资源利用率低。为确保灾备系统之间互联的网络高可用，提高业务连续性，券商普遍申请多条广域网线路采用冷备方式提供网络冗余，备份线路带宽闲置，整体浪费线路资源。

2、业务流量区分保障问题。证券行业对关键业务数据零丢失和关键业务连续性保障要求较高，传统广域网架构和技术，缺乏应用识别并针对关键业务应用提供高级别 QoS 保障。

3、难以适应云转型发展。云灾备中心是证券行业近来非常突出的创新方案，对云网融合提出了更高的要求，传统专线在网络灵活性和弹性等方面不适合云化部署。

4、传统专线部署周期长、价格昂贵，运维成本高。

5、业务可视化问题。缺乏可视化界面，无法图形化实时查看线路的延迟、抖动、丢包、拥塞、应用对于网络资源的使用情况等实时网络状态。

为解决以上业务痛点、提升券商广域网安全运行水平、降低运营成本，上交所技术携手南京证券就 SD-WAN 在灾备互联场景展开应用探索，具体场景以南京证券主中心到上海灾备中心为例。

三、南京证券 SD-WAN 灾备互联组网实践

在跨数据中心灾备互联中，传统组网方案多

图 3–1：改造前多数据中心传统网络对接示意图

数通过点到点专线互联，多条广域网专线形成主、备互备，详细见图 3-1。

传统的灾备互联组网方式对券商业务连续性保障提供了有效支撑，但也带来备份线路带宽闲置等情况。若采用 SD-WAN 技术，多数据中心灾备互联可引入价格低廉，带宽更高的互联网线路替换部分昂贵的专线带宽，通过多线路捆绑来增加总体可用带宽，提升网络稳定性。同时 SD-WAN 内置的安全及路由功能还可代替防火墙和边界路由器的部署，简化运维等。

下文将结合南京证券主备数据中心灾备互联场景，验证 SD-WAN 组网的可行性和应用价值。

图 3–2：改造后多数据中心网络 SD–WAN 对接示意图

图 3.2–1：测试网络拓扑图

3.1. 验证内容

验证内容如下：

1、业务多线路宽带利用率测试；

2、WAN 线路切换情况下业务连续性、可靠性测试；

3、业务自动识别及自动优化测试；

4、业务加密测试；

5、运维可视化测试。

3.2. 测试情况

上交所技术、南京证券通过在跨数据中心场景下对 SD-WAN 网络的部署和测试研究，较好地验证了 SD-WAN 技术价值。总体测试方案为：上海节点 SD-WAN MCN 设备和南京节点 SD-WAN Branch 设备均采用网关模式进行部署，用于传输灾备环境的数据库同步业务数据以及双向打流数据。SD-WAN 设备采用电信与联通双 Internet 线路（电信 50M，联通 100M）和双专线链路（电信联通均为 20M）。测试网络拓扑图如图 3.2-1。

本次测试场景设计了如下线路捆绑组合，分别为两条 MSTP 专线捆绑，一条专线一条互联网捆绑，以及两条互联网线路捆绑。对于每个测试线路组合，均开展了如下几个方面的测试：

1、业务多线路宽带利用率测试：

测试过程：以业务多线路宽带利用率测试为例，在客户端使用 iPerf 测试工具向服务端打流，查看 iPerf 的带宽能达到的最大值远超出单条线路能够提供的带宽。

测试结果：单个业务可以同时使用多条专线带宽资源；总体带宽利用率不低于 80%，峰值总带宽利用率达到 95%。

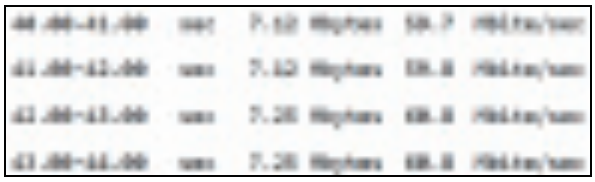


图 3.2–2：20M+50M 线路叠加打流有效带宽记录

2、业务线路切换情况下应用连续性、可靠性测试：

测试过程：测试业务对单个线路的质量变化无感知，单根线路故障不影响业务流量连续传输，模拟线路断网，持续一段时间后专线恢复，SD-WAN 系统自动调度流量。具体测试方法为在断线测试之前，使用 iperf 打流以及向上海异地灾备做数据库同步，同时长 ping；断开任一线路，看设备是否监测到线路中断，业务是否出现中断；重新接上线时，查看设备是否监测到线路恢复，业务是否出现中断。

测试结果：整个测试过程，ping 包不丢，数据库同步业务流也无任何中断，在中断线路恢复后，流量分摊到两条专线，提高了广域网传输业务可靠性。

3、业务自动识别及自动优化测试：

测试过程：测试 SD-WAN 自动识别应用种类，双向实时感知线路状态，能够自动保证实时类应用转发，不出现拥塞。通过同时在 SD-WAN 两端测试机发起 ping 和 iperf 流，以及进行生产数据库同步。

测试结果：在 SD-WAN 管理平台上查看业务流信息，发现流量分别被识别为 icmp、iperf

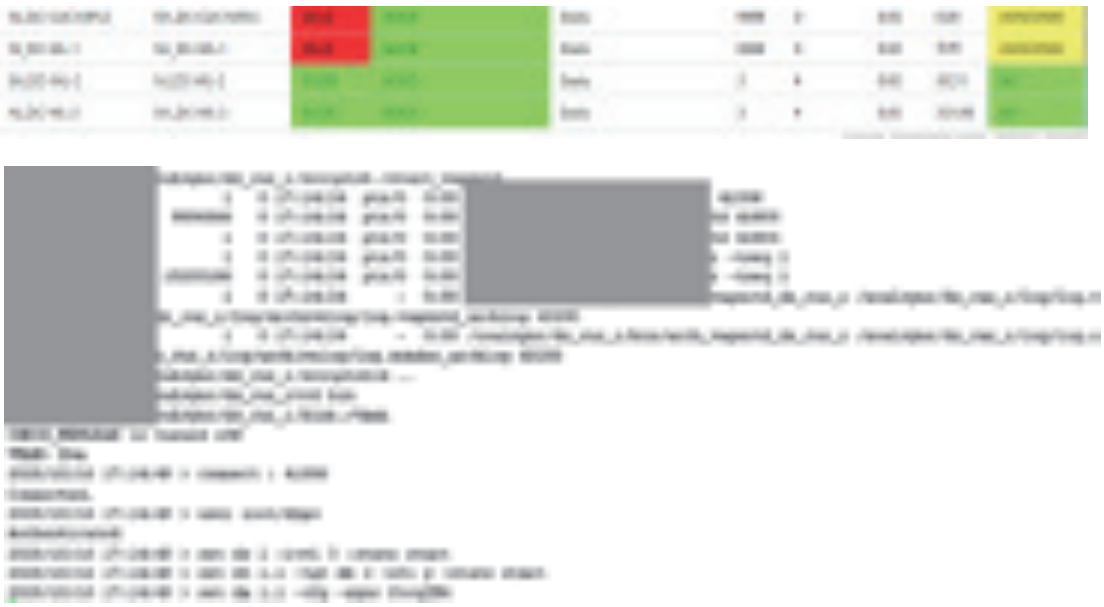


图 3.2–3：专线线路中断，但数据库同步业务流量不受影响

和 Oracle 应用类型，SD-WAN 可以基于应用类型自动选择路径转发，出现拥塞时，优先确保 Oracle 的实时数据库同步业务流量进行转发，确保广域网业务传输可靠性。

4、SD–WAN 的安全性测试：

测试过程：SD-WAN 具有网络防火墙功能，通过对业务流量在 SD-WAN 接口上抓包查看包内容信息。

测试结果：发现每根 WAN 线路上数据报文都经过加密，只能查看到报文的转发端口和数据长度，看不到内部数据，无法获取内层报文内容，保证广域网传输数据安全性。

此外，SD-WAN 还具有内置防火墙功能，可以根据应用来实现安全策略控制。

5、运维可视化测试：

测试过程：SD-WAN 管理平台可视化实时展示 SD-WAN 全网各线路，各方向的网络状态信息。

测试结果：展示的状态数据含有：硬件使用，线路带宽占用，网络抖动、延迟、流表信息、流量的源目地址、协议类型，转发路径等。在 SD-WAN 运维监控方面，支持链路质量明细监控、流量追踪溯源、流量排序索引、QoS 和流量的图像化展示、统一管理等功能，提升了广域网运维的效率。

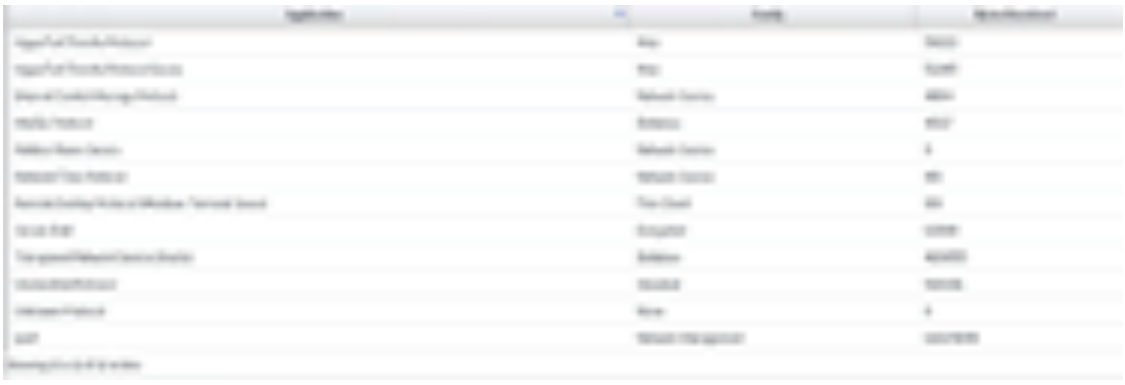


图 3.2–4：SDWAN 应用识别引擎自动识别流量应用类别

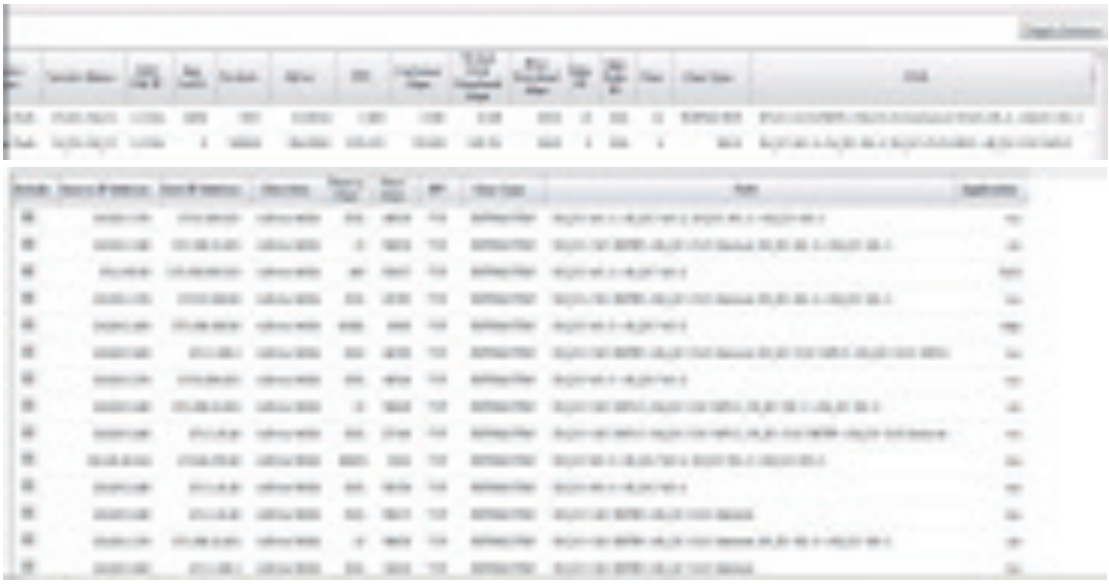


图 3.2–5：基于不同应用类别自动分配不同 QoS 优先级

图 3.2–6：优先保证高优先流量转发（Interactive>Bulk）

3.3. 应用价值

在证券行业的灾备数据中心互联应用研究中，通过 SD-WAN 网络部署，积极探索了证券行业 SD-WAN 网络容灾能力，与券商的传统广域网实践对比，SD-WAN 可为证券行业广域网互联带来如下价值：

1、降成本增效能：SD-WAN 可实现将昂贵专线和价格便宜的互联网线路逻辑捆绑为高可用的混合 SD-WAN 虚拟通道，通过使用性价比高的链路，可有效减少券商网络建设费用支出。根据测算，同比例带宽情况下，SD-WAN 相较运营商专线，每年至少可节省 30% 的成本。基于 SD-WAN 捆绑的专线 + 互联网的虚拟网络通道，可以实现在提供不低于原有专线带宽的情况下，并达到与专线同等的网络服务质量。由于同等带宽的互联网线路相较于运营商专线价格非常低廉，使用 SD-WAN 构建的混合虚拟网络可以进一步降低券商的跨数据中心，尤其是与异地数据中心之间的网络建设费用。

2、网络实时在线：

1）SD-WAN 综合利用多条互联网或专线链路，具有多路由优化及冗余特性，保障券商业务

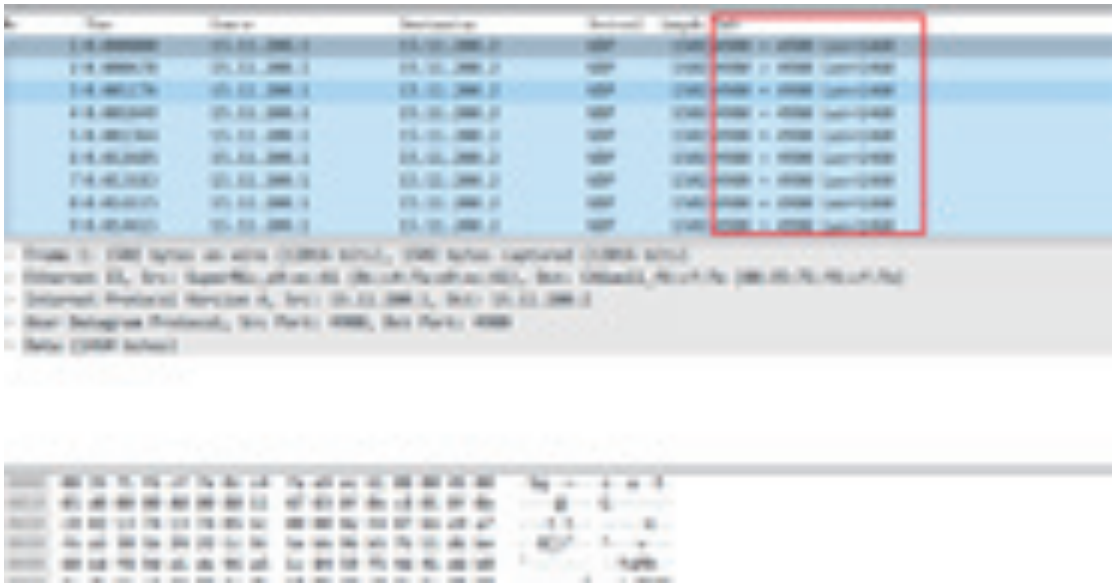


图 3.2–7：数据报文内容展示

图 3.2–8：双向线路状态实时显示（时延 带宽 丢包 抖动 拥塞）

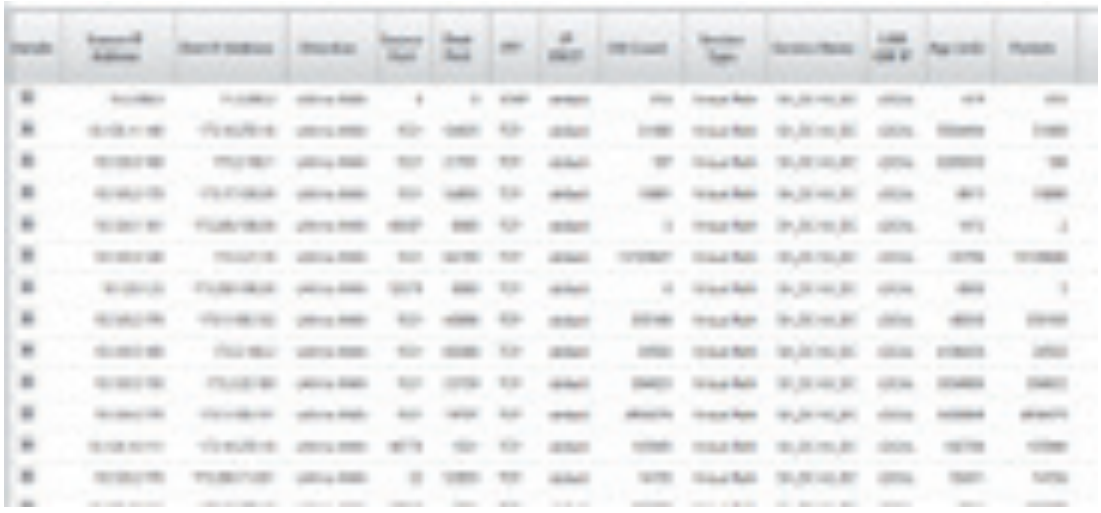


图 3.2–9：流表详细信息

的连续性。

2）SD-WAN 根据业务应用需求和实时链路质量检测以及智能路径控制等特点，为关键业务提供优质的链路，保障券商关键业务的运行质量。

3）SD-WAN 基于数据包级链路探测，毫秒级感知线路质量，基于数据代理级报文收发模式。单条线路出现故障时，同一个会话流量可自动平滑切换，不会造成应用层业务会话中断，保障券商广域网链路实时在线。

3、盘活线路带宽：SD-WAN 将多根独立的甚至不同介质的线路进行逻辑捆绑，叠加多根线路带宽，形成高速通道。拥有基于数据包的带宽聚合，使一组源目 IP 流使用多条通信通道传输，通过智能算法实现带宽叠加利用和线路故障无感

图 3.2–10：应用流量 QoS 信息

图 3.2–11：不同 QoS 流量带宽占用

图 3.2–12：不同应用流量在不同时间段占用带宽的情况

知切换。

4、保障实时应用：通过高可用性、智能服务，算法优化等方案提升用户体验。针对 UDP 或对延迟高敏感的应用（例如：视频会议、VOIP，实时数据同步等），通过数据复制技术并选择优先到达数据来提供用户体验保障，解决卡顿、丢帧、时延过大等问题，可内置 QoS 策略自动双向保障不同业务流量优先级，确保高优先级的关键业务始终保持在优先级高的链路上，实现最高优先的业务运行在质量最优的链路上。

在本课题研究中，券商充分利用 SD-WAN 的技术优势，通过捆绑专线和互联网线路实现了

场景（双线路）	未使用 SD-WAN		使用 SD-WAN		采用 SD-WAN 方案投资回报
	线路类型	预估费用（元）	线路类型	预估费用（元）	
20M MSTP 两根对比 20M MSTP+20M Internet 各一根 + SDWAN	MSTP 1: 20M	218712	MSTP 1: 20M	218712	**宽带：×2 倍 费用节省：170712 元/年**
	MSTP 2: 20M	218712	Internet: 20M	48000	
50M MSTP 两根对比 50M MSTP+50M Internet 各一根 + SDWAN	MSTP 1: 50M	292932	MSTP 1: 50M	292932	**宽带：×2 倍 费用节省：172932 元/年**
	MSTP 2: 50M	292932	Internet: 50M	120000	
100M MSTP 两根对比 100M MSTP+100M Internet 各一根 + SDWAN	MSTP 1: 100M	467724	MSTP 1: 100M	467724	**宽带：×2 倍 费用节省：227724 元/年**
	MSTP 2: 100M	467724	Internet: 100M	240000	

从主中心到异地灾备中心的跨中心的核心数据库实时同步，达到专线的网络服务品质，实现了预期的目标。

5、部署可管可控：

SD-WAN 的典型特征是软件定义，在网络的管理上拥有先天的灵活运维优势：

1）SD-WAN 拥有即插即用、集中运维管理能力。可实现对 SD-WAN 网络设备统一配置管理及相关策略下发等功能，无需专业 IT 人员到异地中心现场安装配置，实现 SD-WAN 快速自动组网。

2）SD-WAN 拥有全网可视化界面、多维度图形报表展示等功能。可实时实现对全网线路、流量和网络设备可视可控、提供智能运维、事件报警等功能。

3）SD-WAN 拥有丰富的 API 接口，可被上层网络集中管理平台集成，进一步提高券商数据中心网络管理的效率，降低网络运维难度。

6、多维安全保障：SD-WAN 管理平台集中管理整网安全策略，实现端到端、全方位网络安全控制。具有状态化防火墙和 IPsec VPN 功能，SD-WAN 内置安全功能还可以包括入侵防御系统、URL 和内容过滤、恶意软件检测和 DDoS 防护等，提供多维度安全保障，丰富报表便于安全事件回溯。

四、总结与建议

4.1. 研究总结

近年来，SD-WAN 发展势头强劲，整个证券行业的热情也持续高涨。SD-WAN 的发展对于网络服务商的组网型业务有一定的影响，特别是对于电信运营商的专线业务。

SD-WAN 广域网互联可提供安全隔离的点到点、点到多点及多点到多点的专享连接服务。可满足证券行业差异化的组网需求，为整个行业提供组网便捷、体验优异、运维便利、质优价廉的广域网互联服务，实现广域网多点间互联，灵活组网以及便捷的远程管理等丰富的增值服务。

未来，SD-WAN +5G 结合将是证券行业广域网互联的重要发展方向。5G 能力和 SD-WAN 终端接入结合起来，实现行业超大带宽、超低时延、高速连接的能力，为整个行业提供更优的业务体验。

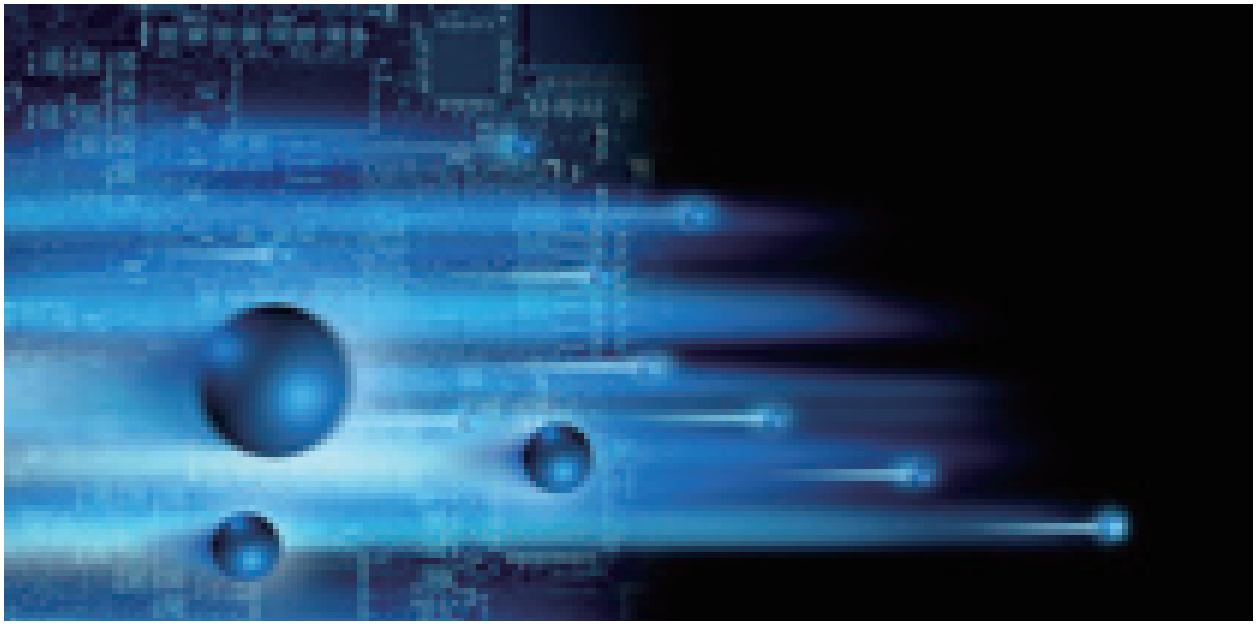
4.2. 政策建议

目前阶段，SD-WAN 作为广域网互联的一种新型连接方式，其技术还在不断发展中。证券行业不可轻易放弃现有业务质量保证的专线，建议可部署混合网络，即在保留原有私有专线的传送关键数据的基础上，根据业务优先级，将部分相对不重要的业务使用 SD-WAN 技术动态迁移到公共宽带网络，甚至是无线 LTE 网络上。

SD-WAN 作为一种具有较高价值广域网技术，目前已逐渐在金融行业有较多的落地案例，部署场景包含但不限于总部与分支机构互联，跨数据中心互联，跨行业机构互联等。SD-WAN 作为证券行业逐步采用一种新兴网络技术，同样需要考虑网络的高性能和高可用，建议主管部门对证券行业应用 SD-WAN 技术采取鼓励的政策，在满足国家及行业监管相关要求的前提下，尽可能允许证券机构采用 SD-WAN 技术更先进，稳定性更高，性能和解决方案更优的产品方案，确保证券业务连续性、加速证券行业数字化转型。

量子密码研究报告

秦体红 / 北京信安世纪科技股份有限公司 qintihong@infosec.com.cn
汪宗斌 / 北京信安世纪科技股份有限公司 wangzb@infosec.com.cn



报告通过调研了量子密码技术的起源，跟踪了解了当前量子密码，主要是量子密钥分发（QKD）最为成熟，调研、分析及研究了量子密码结构模型、理论安全性以及实际安全问题。报告分析了 QKD 技术在实际应用中的性能的影响，调研了当前量子密码的行业应用情况；另外，报告跟踪了解了当前国内外由于量子密码的标准化进程。

1. 研究背景

量子密码的思想源自由美国人 Wiesner 于 20 世纪 70 年代提出的量子货币概念。量子密码是以现代密码学和量子力学为基础、利用量子物理学方法实现密码思想和操作的一种新型密码体制。与当前使用的以数学为基础的密码体制不同，量子密码以量子物理原理为基础，利用量子信号实现。当前所谓的量子密，主要是指量子密钥分发（QKD）。

1984 年 IBM 公司的 Bennett 与加拿大的 Brassard 共同提出了量子密钥分发（Quantum Key Distribution，QKD）的概念，以及第一个量子密钥分发协议 --BB84 协议，从而奠定了量子密码学发展的基础。其后，随着 EPR 协议的发明以及无条件安全性证明的提出，量子密码技术得到了学界的重视，开始蓬勃发展。迄今人们已经提出了多种 QKD 协议方案，其中包括 BB84 协议、EPR 协议、B92 协议、差分相位协议等。随着量子通信以及量子计算技术的逐渐丰富与成

熟，量子密码在未来信息保护技术领域将发挥重要的作用。

报告的结构安排如下：第 2 节回顾了 BB84 协议；在第 3 节中调研了 QKD 的系统模型；调研及分析了 QKD 的安全性和实际系统中安全问题安排在第 4，5 节中；报告的第 6 节分析了 QKD 技术的性能；第 7 节调研了目前已有的量子密码技术的应用；在第 8 部分，调研了国内外有关 QKD 测评技术；第 9 节描述了一些其他的量子密码技术；报告的第 10 节调研了国内外关于量子密码的标准问题；最后，报告的第 11 节阐述了后量子密码算法。

2. BB84 协议

1984 年，Bennett 和 Brassard 最早提出了量子密码协议，通称为 BB84 协议，是第一个量子密码协议，属于量子密钥分发的范畴。在 BB84 协议中，量子通信实际是由两个阶段完成的。第一阶段通过量子信道进行量子通信，进行密钥通信。第二阶段是在经典信道中进行的，进行密钥协商，探测是否存在窃听者窃取信息，从而确定最后的密钥。BB84 协议过程如下：

(1) Alice 准备一个光子序列，每个光子随机处于共轭基$\{|0\rangle,|1\rangle\}$和$\{|+\rangle,|-\rangle\}$中的四个态之一。这四个量子态分别表示光子处于水平，垂直，左旋和右旋偏振态。Alice 记录序列中每个光子所处的状态，并把整个序列通过量子信道发送给 Bob。

(2) 对接收到的每个光子，Bob 从$\{|0\rangle,|1\rangle\}$和$\{|+\rangle,|-\rangle\}$中随机选择一组偏振基进行测量。

(3) Bob 通过公开的经典信道告诉 Alice 他测量每个光子所用的偏振基，而不是测量得到的偏振态。

(4) Alice 告诉 Bob 在哪些光子上他们选择了相同的基，同时双方把选用不同的基的那些光子对应的数据丢弃。

(5) 双方将对应于每个光子的偏振态按约定转换成 0，1 比特，如$|0\rangle\to0$，$|1\rangle\to1$，$|+\rangle\to0$，$|-\rangle\to1$，得到一串密钥。

(6) Alice 和 Bob 从生密钥中随机选择部分比特进行公开比较。若错误率大于安全界限，表示有窃听者存在，抛弃此次得到的所有数据，返回到第一个步骤。反之，协议继续，进入纠错过程。

图 1：BB84 协议示意图

3.QKD 系统模型

3.1 量子密钥分发（QKD）

量子密钥分发（QKD）是一种基于量子力学原理实现的密钥生成技术，通过量子态的制备、传输和测量，在收发双发之间实现无法被窃取的共享随机密钥生成。QKD 根据物理机制和协议类型不同，可以分为基于单光子调制的离散变量协议，如 BB84 协议；基于多光子调制的连续变量协议，如 GG02 协议；以及基于纠缠光子对的纠缠协议，如 E91 协议。

3.2 量子密钥分发系统模型

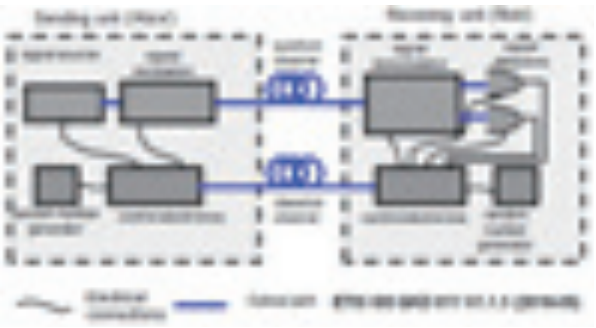


图 2：量子密钥分发模型（QKD）

QKD 系统一般包括发送方、信道、接收方和数据后处理系统。具体如下：

1）发送方是负责制备和发送量子态的用户。主要设备包括光源、调制器（根据系统的不同，调制器可能包括包相位调制器、强度调制器、偏振调制器、衰减器等），还有相应的随机数发生器和协议控制模块等。

2）信道是在用户之间传输量子态的通道。

3）接收方是负责接收和测量量子态的角户。主要设备包括分束器、偏振分束器、分束器 / 耦合器、探测器等，还有相应的随机数发生器和时间校准装置以及协议控制模块等。

4）数据后处理系统是经典数据处理系统。在通信双方完成量子态的发送、接收、测量之后，需要进行基矢对比、随机比特的误码对比，再根据测量、对比过程得到的相关参数来估计可能泄漏的信息的上限；然后通信双方再据此来进行对原来密钥的纠错和隐私放大的操作，最终得到安全的密钥。纠错过程也会泄露部分信息，这部分信息在最终提炼密钥的过程中也需要被剔除。数据后处理系统的经典信息交互还需要进行消息与身份的鉴别。

4. QKD 安全性

量子密码的无条件安全性是指量子密码方案在攻击者具有无限计算资源的条件下仍不可能破译该密码方案的特性。无条件安全又称信息论安全，其基础是信息论。量子密码中也发展了基于复杂性理论的量子密码体制，其安全性依赖于量子计算复杂度。

4.1 QKD 安全性物理原理

一般地，量子密钥分发的安全性都基于以下物理原理：

（1）不可再分性。量子密钥分发若采用单个量子作为信息载体，由于单量子不可再分，则 Eve 无法通过窃取部分单量子并测量其状态的方法来获得密钥信息。

（2）测不准原理。根据量子力学中的海森堡测不准原理，Eve 即使可以截取量子信号，也无法有效同时测量其非对易物理量。这种情况下，如果 Eve 根据测量结果重新制备一个量子发送给接收方，将会改变单量子状态。发送方和接收方可以通过一定的方法检测到 Eve 对单量子的测量行为，并进而检验密钥的安全性。

（3）不可复制性。Eve 也可以试图在截取量子信号后，通过复制单量子的量子态来窃取信息，但量子力学中的不可克隆定理保证了不可能精确复制任意未知的量子态。

4.2 QKD 安全假设

QKD 的无条件安全依赖于以下假设，如果协议能满足下述条件，则证明 QKD 协议是无条件安全的。假设如下：

(1) 可信任的物理安全区，对外界没有不必要的信息泄露。窃听者 Eve 无法直接入侵 Alice 和 Bob 的设备获得密钥信息或者测量基的选择。

(2) Alice 和 Bob 拥有理想的随机数发生器 (可能是量子随机数发生器，也可以不是)，因此双方可以随机选择量子态的制备和测量基。

(3) 可信任的量子设备 (量子态制备和测量设备)、经典设备 (例如存器和计算设备)、存储和处理量子仪器所产生的经典数据。

(4) 经典信道必须是可信认证的，可以利用经典无条件安全的认证方案来保证。

(5) 窃听者的攻击能力可在量子力学允许的范围内。

4.3 QKD 攻击模型

QKD 的攻击模型：

1）个体攻击：个体攻击指的是 Eve 单独攻击每一个从发送方 Alice 发往接收方 Bob 的量子信号，并且每次攻击的攻击策略均相同。Eve 在

Alice 和 Bob 进行基矢筛选之后、其他数据后处理过程之前对自己得到的 量子信号进行测量。

2）集体攻击：集体攻击指的是 Eve 单独攻击每一个从 Alice 发往 Bob 的量子信号，并且每次攻击的攻击策略均相同。但是 Eve 可将从攻击中得 到的量子信号利用量子存储器保存下来，并在 Alice 和 Bob 的数据后处理 过程之后，选择最优测量方式对自己保存的量子信号进行集体测量。

3）相干攻击：量子物理原理容许的任何攻击方法。

1999 年，Shor 等人利用纠缠提纯的思想首先证明了 BB84 协议在集体攻击下的安全性。2005 年，Renner 等人从信息论的角度证明了 BB84 协议在集体攻击下的安全性，并给出了更优的成码率公式。Renner 还利用交换不变性证明了 BB84 协议的相干攻击并不优于集 体攻击，更进一步地还证明了任何一个 QKD 协议只要满足交换不变性，其集体攻击就是最强攻击。2008 年，Scarani 等人给出了有限码长 BB84 协议的安全性证明。

5. QKD 实际安全问题

QKD 安全性证明都基于理想的 QKD 协议实现模型，实际条件下的 QKD 系统所使用的实际器件的性能和理想模型的设定是存在差异的，这带来了一些另外的安全威胁。对于实际条件下 QKD 系统面临的安全威胁主要有离散变量 QKD（DV-QKD）系统面临的实际安全威胁和连续变量 QKD（CV-QKD）系统面临实际安全威胁。

离散变量 QKD（DV-QKD）系统面临的实际安全威胁主要有：1）非理想单光子源：光源可能发出多光子脉冲，信 息在多余的光子上也被编码 造成信息泄露、2）光源强度涨落：诱骗态方法要求发送方引入不同强度的信号，若强度信号的涨落被窃听者掌握，则窃听者可以获得稍多的信息、3）不完全随机化相位攻击：弱相干光源各脉冲之间的相位存在关联，不满足诱骗态方案的要求，可造成信息泄露、4）不同基矢探测效率不匹配：窃听者可能一定程度上控制不同探测器的探测效率，窃取更多的信息、5）解码装置波长选择攻击：若解码装置存在波长相关性，窃听者可以利用波长影响接收方的基矢选择，破坏测量基矢选择完全随机的安全性假设，提高窃听成功的概率、6）测量设备被 Eve 干扰：窃听者通过注入强光控制探测器的响应、7）基相关迭代筛选的安全漏洞：若发送和接收方在每次发送和测量之后都会公布制备基和测量基，则破坏了随机采样的适用条件。窃听者可以干扰采样过程，造成合法通信双方错误率估计不准确、8）木马攻击：窃听者注入强光探测发送方编码器件的状态，获得编码信息、9）调制器误差：调制器件的误差造成量子态的制备、测量和理论协议不能完全一致、10）相位调制器衰减：干涉仪一臂引入的相位调制 衰减，造成编码态和理论协议不一致、11）相位重映射攻击：对于往返式 QKD 系统，光源来自发送方设备的外部。此时窃 听者控制光源，通过调节延时使信号的相位调制发生误差，编码态不符合理论协议的规定。

连续变量 QKD（CV-QKD）系统面临实际安全威胁主要有：1）非理想相干光源：光源非理想相干性会等效引入额外的调制过噪声，会造成 系统性能的降低、2）非理想高斯调制：发送方在实际中调制的高斯调需要进行离散化和截断的处理，实际调制和理想的高斯调制会存在差异。如果攻击者在实际中可以分辨出这样的差别，就会破坏安全证明中的假设，产生安全威胁、3）特洛伊木马攻击：攻击者可以从开发信道发送强光到发送方内部，通过测量从发射端反射出的光可以测量出发送方的相位和高斯调 制信息、4）本振光抖动攻击：如果没有对本振光光强进行检测，收发双方无法察觉对应散粒噪声的变化，如果本振光减小，接收方即会高估了散粒噪声大小，

从而低估过噪声造成安全隐患、5）平衡零差检测波长攻击：由于分束器对波长的敏感性，可借助其他非工作波长伪造相干测量结果，从而掩盖截断重发攻击而泄露密钥信息、6）平衡外差检测波长攻击：由于分束器的波长敏感性，可通过引入其他非工作波长信号并联合校准攻击掩盖截断重发引入的过量过噪声，从而获取密钥信息、7）散粒噪声校准攻击：攻击者通过延时本振光的时钟信号，造成接收方测量的方差不是最优值，收发双方通过预先标定的光强 - 散粒噪声关系会高估散粒噪声，从而低估 过噪声，产生安全隐患、8）有限带宽采样效应：由于对检测器输出模拟信号的采样带宽有限而无法精确获取信号峰值，造成性能降 低、9）饱和攻击：攻击者可以通过开放信道发射强光到接收方探测器，从而造成电子器件饱和，进而造成接收方错误估测截取再发攻击产生的过噪声，造成安全隐患、10）有限码长引起的统计涨落：由于参数评估的数据块长度有限而引入了关键参数统计误差，会降低系统性能和 11）非理想相位补偿：由于系统相位补偿精度有限而等效引入额外的相位噪声，会降低系统性能。

此外，中继站的不可信也导致了 OKD 系统的不安全。

6.QKD 性能

QKD 系统的性能要求主要体现在传输距离、抗信道噪声能力和生成安全密钥率等方面。从 1984 年首次提出实用化的 QKD 协议 --BB84 协议以来，QKD 技术从理论逐步走到产业界应用。根据 BB84 协议的流程，包括以下 5 个步骤：对基筛选（Sifting）、误码估计（Error estimation）、纠错核对（Error correction）、结果校验（Confirmation）和保密增强（Privacy amplification）五个步骤。误码估计和保密增强是保障 QKD 安全性的核心步骤，纠错校验算法效率是限制 QKD 安全成码率的瓶颈之一。

由于协议和关键器件的性能的限制，QKD 传输距离以及密钥生成的速度受其限制，导致整个系统性能下降。验室条件 DV-QKD 超低损光纤单跨段最远传输距离为 421.1 公里（71.9dB 损耗），安全密钥成码率约为 0.25bit/s，使用极低暗记数率（0.1Hz）SNSPD。最高密钥成码率为 11.53Mbit/s 光纤传输距离为 10 公里（2dB 损耗）。

由于量子中继技术尚不成熟，目前 QKD 系统长距离传输只能依靠密钥落地、逐跳中继的可信中继技术。而可信中继战的密钥存储管理和中继转发也是制约了 QKD 的因素之一。

7.QKD 技术应用

量子密码采用 QKD 技术分发对称密钥与对称加密组合对通信数据进行加密。其实现原理如下图所示：

QKD 设备结合光开关、波分复用器等传输辅助设备完成量子态光信号物理层传输和点到点 QKD 密钥生成。量子密钥管理设备负责网元管理、密钥管理和基于可信中继的端到端密钥生成。量子加密应用设备使用 QKD 密钥对业务数据进行加密处理。

图 3: 量子加密示意图

7.1 QKD 和现有密码技术结合

QKD 作为一种新的密钥分发技术，可以广泛应用于现有的信息系统中，或者说与现有的密码技术进行结合。QKD 用于密钥交换，可与网络层的 IPSec 协议结合使用、还可以与传输层的 TLS、SSL 等协议进行集成使用；利用 QKD 技术为通信双方提供共享密钥，可以用于

进行用户的身份鉴别或者用于实现业务数据的加密传输。

7.2 QKD 技术行业应用

QKD 技术可以广泛的应用在各行各业：如关键信息基础设施、移动通信等。

7.2.1 关键信息基础设施中应用

量子保密通信可用于保护政企专网基础设施及其服务的安全性。企业或政府机构通常要求通信服务提供高度的机密性、完整性和真实性，需要 强制性地采用专用的安全系统。当前通常采用基于 IPSec 或 TLS 的安全虚拟专用网络（VPN）技术来对数据中心与分支机构之间的流量进行鉴权和加密，而 QKD 链路加密机可以与这些技术结合来满足企业网各站点之间信息加密需求。如下图所示：

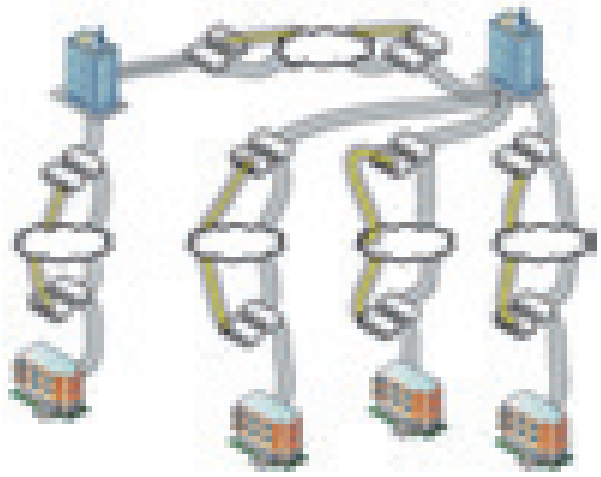


图 4：QKD 应用于关键信息基础设施

7.2.2 QKD 技术应用于移动互联网

随着通信技术的发展，各种智能终端的普及，如智能手机、pad 等，各类移动终端安全问题也随之而来。利用 QKD 技术自身的独特优势，同时结合密钥分发中心可以将 QKD 生成的量子密钥应用于移动终端侧，保护端到端及端到服务器的通信安全性，可在移动办公、移动作业、移动支付、物联网等多种场景进行应用。

如图 5 所示，QKD 网络结合用于管理 QKD 网络产生的量子密钥的量子安全服务密钥分发中心（Quantum secure service KDC），以及用户的量子密钥更新终端设备，可将 QKD 技术产生的量子密钥注入到终端的安全存储介质例如 U 盾、安全芯片等，用于其通信过程中的身份鉴别和通信数据加密。

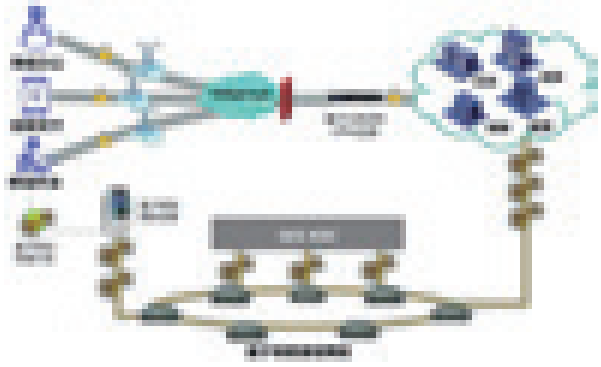


图 5：QKD 应用于移动互联网

8.QKD 测评

随着量子保密通信系统广泛应用，相关测评工作的研究探索也逐步开展。欧洲电信标准化协会 (ETSI) 在 2008 年成立了包括日本东芝公司剑桥大学研究所、英国国家物理实验室和瑞士 IDQ 公司等 16 家成员单位在内的 ISG-QKD 标准化工作组，在量子加密通信和 Swiss Quantum 等试点应用项目的基础上，开展量子保密通信测评和标准化等领域的研究工作。日本多家研究机构和欧洲联合建立 Tokyo QKD 实验床网络，进行了多种量子密钥分发协议的演示和技术验证研究。在国内，随着“京沪干线”的试点，也开始组织量子密码技术相关的测评研究。

在量子保密通信系统中，目前测评重点内容包含以下几个方面：量子密钥分发、量子密钥管理和量子加密。

8.1 量子密钥分发测评

QKD 设备系统功能和性能测试是验证其系统传输能力、密钥生成能力、量子密钥真实性、

安全性和可靠性等系统重要特性的必要手段。通过验证 QKD 协商信道的协议交互和算法后处理流程与诱骗态 BB84 协议要求的一致性，结合量子光信号的准单光子特性，可以为 QKD 设备生成量子密钥的真实性提供佐证。通过 QKD 系统密钥成码率和传输能力测试，能够验证 QKD 系统的性能指标，并为 QKD 系统的实际应用部署提供必要保证。

QKD 系统功能和性能测试内容主要包括协议一致性、密钥成码率和安全性与可靠性等方面。诱骗态 BB84-QKD 协议一致性测试，主要验证系统设备协商信道中的量子态制备检测和协议后处理流程与诱骗态 BB84 协议的基本流程要求是否一致。QKD 系统密钥成码能力测试包括密钥成码速率和传输能力两方面，系统密钥成码速率主要考察指定信道衰减条件下的系统小时平均成码率，系统传输能力主要验证发 QKD 发射机和接收机之间最大的衰减容忍值，以及在指定光纤信道中，密钥成码率降低为零时对应的最大传输距离。

8.2 量子密钥管理测评

量子密钥管理是对量子密码系统中的基本网络管理功能和性能的验证。量子密钥管理是实现网络用户节点间量子密码系统组网的基本条件。密钥管理包含密钥存储归档、输出控制和中继管理等功能，实现系统密钥的存储、交换和中继。量子密钥管理设备和网络管理系统应用接口对量子加密设备输出密钥，是业务用户最终使用量子密码系统系统加密通信服务的基本接口。

8.3 量子加密测试

量子加密测试主要内容包括 : 量子密钥接入功能和更新速率，量子密钥和传统协商密钥的备份和切换，业务加密信道的传输性能，包括吞吐量、丢包率和时延等参数，以及量子加密业务加密长期稳定性。

9. 其他量子密码技术

9.1 量子秘密共享

对量子密钥分发的进一步研究，开始推广到多方密钥分配问题，于是很自然地提出了量子秘密共享这一新的方向。1998 年，Hillery，Berthiaume 和 Buzek 提出了量子秘密共享和量子信息分拆的概念，并基 GHZ 三重态提出了一个量子秘密共享方案和一个量子信息分拆方案。在 Hillery 等人工作的基础上，日本 Soken 大学 N. Imoto 领导的小组采用 Bell 纠缠态亦实现了量子秘密共享，提出了两态量子秘密共享算法。

与经典密码中的秘密共享相比，量子秘密共享还有很多问题有待进一步研究，如参与者增加或者减少后的量子密码方案的适用性问题、量子秘密共享的实现技术、安全性分析等。

9.2 量子认证

与经典密码一样，量子认证是量子密码中的一个重要组成部分，内容涉及量子认证码、量子身份认证、量子签名以及量子信道认证等几个方面。目前，在量子认证方面的研究工作主要集中在基于对称密码体制的认证系统中，例如，针对点对点或者依赖一个可信赖中心，人们设计了一些量子认证方案。在量子身份认证方面，1996 年，以色列密码学者 E. Biham 等人首先提出了量子身份认证协议，该协议可用于具有对称密钥的通信者之间的身份认证问题。2000 年，杨理等基于代数编码理论设计了量子消息认证协议。另外，曾贵华等还提出了量子签名的概念，并研究了基于对称密钥的量子签名方案和基于非对称密钥的量子签名方案在此基础上，国内外一些学者相继开展了一系列的研究，提出了一批量子签名算法。另外，利用连续变量量子信号的特性，一些基于连续变量的量子身份认证方案和量子签名方案得到了初步的研究。

10. 量子密码标准化

量子密码从实用化走向产业化规模应用之路仍然面临不少挑战。 标准化是其中十分重要的一环，对于未来产业健康发展具有奠基石的意义和作用。

10.1 国外量子密码相关标准进展

欧洲电信标准化协会（ETSI）于 2008 年 9 月牵头成立了包括 16 家成员单位在内的 ISG-QKD 标准化工作组，展开前瞻性的标准化研究。ISG-QKD 的研究包括 4 个方面，一是研究技术规范，包括对 QKD 系统的不同协议方案、主要器件、性能参数、设备接口和工作环境等方面进行定义和规范；二是提出测试方法，包括对 QKD 设备的光学器件、密钥系统和协议参数进行可溯源的测试评估；三是推动安全认证，包括对实际 QKD 系统的器件属性、安全漏洞和侧信道进行分析和攻防测试，并推出安全可靠性的认证要求；四是提出应用需求，包括对 QKD 技术的应用场景、与现有网络设备的集成以及应用接口的规范等方面的内容进行研究。计划在 2019 年初进一步发布 QKD 术语、QKD 系统部署参数、QKD 密钥提取接口等规范。

另外，国际标准组织、国际电信联盟等组织研究并发布了部分量子密码相关的标准及研究报告。

10.2 国内量子密码相关标准进展

随着我国量子密码试点应用和产业化快速发展，其系统设备与网络架构、技术规范和测试评价等方面的标准化需求也日益明显。为推动量子通信关键技术研发、应用推广和产业化，CCSA 于 2017 年 6 月成立了量子通信与信息技术特设任务组，旨在建立我国自主知识产权的量子保密通信标准体系，推动 QKD 相关国际标准化进展。

目前，ST7 已制定了完整的量子保密通信标准体系框架，包括名词术语标准以及业务和系统类、网络技术类、量子通用器件类、量子安全类、量子信息处理类等五大类标准。

目前 ST7 已从术语定义、应用场景和需求、网络架构、设备技术要求、QKD 安全性、测试评估方法等方面立项开展 25 项标准编制工作，包括《量子通信术语和定义》、《量子保密通信应用场景和需求》两项国家标准项目，《量子密钥分发 (QKD) 系统技术要求 第 1 部分：基于 BB84 协议的 QKD 系统》、《量子密钥分发 (QKD) 系统测试方法》、《量子密钥分发（QKD）系统应用接口》、《量子保密通信网络架构》、《基于 BB84 协议的量子密钥分发（QKD）用关键器件和模块》等 8 项行业标准。

11. 后量子密码

随着量子计算机的快速发展，其强大的并行计算能力给现代密码体制，尤其是以因子分解和离散对数问题为基础的公钥密码带来巨大的威胁。由于量子计算机对经典密码体制的的重大威胁，多国政府一件意识到量子计算的重要意义，如美国国家标准与技术研究院（NIST）于 2016 年开始启动抗量子计算机攻击的算法，开始在全球公开征集后量子密码算法。

1994 年，贝尔实验室的 Peter Shor 提出了 shor 算法，shor 算法在量子计算机可以高效地解决离散对数问题、椭圆曲线群上离散对数问题以及因子分解问题。随着量子计算机的发展，上述困难问题的 Diffie-Hellman 密钥交换协议、RSA 算法和椭圆曲线密码体制将不再安全了。同样的，基于上述底层算法的实现的密码协议如 IPSec、SSL/TLS 协议、SSH 协议也将不再安全。对于对称密码算法而言，1996 年提出的 Grover 算法使得其比特安全性下降到原来的一半，如密钥长度为 256 比特的 AES 算法，量子计算机上执行 Grover 搜索算法会使其安全性下降到 128 比特安

全性。对于哈希算法，“量子随机行走算法”将影响到哈希算法的抗碰撞性，会使哈希算法的安全性下降为原来的 2/3，如 sha384 算法，在量子计算机环境下其安全性只有 128 比特安全。量子计算机对现有算法的安全性影响如下表：

算法	类型	功能	量子计算机影响
AES/SM4	对称	对称加密	增加密钥长度
SHA1/2/SM3	哈希	哈希	增加输出长度
dh/ecdh/ sm2	公钥	密钥交换	不安全
dsa/ecdsa/ rsa/sm2	公钥	数字签名	不安全
ecies/ rsa/sm2	公钥	公钥加密	不安全

表 1：量子计算机对现有算法的安全性影响

11.1 后量子密码体制

后量子密码体制是指既能抵抗现有经典计算攻击又能抵抗未来量子计算攻击的密码体制。严格来说，后量子密码体制至少应该满足以下三点：

（1）能够抵抗已知经典攻击方法；

（2）能够抵抗已知量子算法攻击，目前主要是抵 Shor 算法、Grover 量算法以及量子随机行走算法的攻击；

（3）尚不存在已知的量子攻击方法无法在多项式时间内成功攻击的密码算法。

11.2 后量子密码算法

后量子密码算法主要包含基于 Hash 的密码体制、基于编码的密码体制、基于格的密码体制和基于多变量的密码体制。它以这四类密码体制为主流，还有其他类的密码体制，如基于同源椭圆曲线密码体制。

11.2.1 基于哈希的后量子算法

基于 Hash 算法构造的签名体制，最经典的是 Merkle-hash 树签名体制。它由传统的 Hash 函数和任意的一次性签名算法，共同构造出一个完全二叉树来实现数字签名。该体制不依赖于大整数分解和离散对数等难解问题，而是依赖于 Hash 算法的抗碰撞性，所以被认为可以抵抗量子计算攻击。

由于没有有效的量子算法能快速找到哈希函数的碰撞，因此（输出长度足够长的）基于哈希的构造可以抵抗量子计算机攻击。此外，基于哈希的数字签名算法的安全性不依赖某一个特定的哈希函数。即使目前使用的某些哈希函数被攻破，则可以用更安全的哈希函数直接代替被攻破的哈希函数。

11.2.2 基于编码的后量子算法

基于编码的后量子算法是基于编码理论上的数学困难问题而设计的密码体制。它的数学困难问题包括有界编码解码问题、随机线性编码解码问题、列表解码问题等。1978 年 Robert McEliece 提出的基于编码理论的公钥密码算法 McEliece，该算法基于“随机线性编码解码”数学困难问题，经受至今 30 年的密码分析仍然没有被攻破。基于编码的密码体制主要以加密、签名方案设计为主。该类算法的缺点在于其公钥尺寸过大。

11.2.3 基于格的后量子算法

基于格的公钥密码体制是指基于格理论的数学困难问题构造的密码体制。格理论的数学困难问题主要有：最短向量问题 SVP、最近向量问题 CVP 等。这些问题被认为能够抵抗量子计算攻击。目前，格密码具有较好的扩展性，可以利用格理论为设计基础，设计加密、签名、伪随机发生器、密钥交换协议、基于身份的加密、全同态密码等。

基于格的算法由于在安全性、公私钥尺寸、计算速度上达到了更好的平衡，被认为是最有前景的后量子密码算法之一。与基于数论问题的密码算法构造相比，基于格的算法可以实现明显提升的计算速度、更高的安全强度和略微增加的通信开销。与其他几种实现后量子密码算法相比，格密码的公私钥尺寸更小，并且安全性和计算速度等指标更优。

11.2.4 基于多变量的后量子算法

多变量公钥密码体制（MQ）主要基于有限域上的多元二次多项式方程组的难解性，由于shor 算法、Grover 算法对这类方程的求解问题无法实施有效攻击，因此被认为能够抗量子计算攻击。与 RSA、DH、ECC 相比，多变量公钥密码的安全性很难被证明等价于一个已知的可简单表述的数学难题，因而多变量密码体制不具有可证明安全性。基于多变量的密码体制主要以加密、签名方案设计为主。

与经典的基于数论问题的密码算法相比，基于多变量的算法的计算速度快，但公钥尺寸较大，因此适用于无需频繁进行公钥传输的应用场景。

11.3 后量子密码标准化

美国国家标准与技术研究院 NIST 于 2016 年启动抗量子密码算法的征集工作，NIST 的后量子密码算法标准征集竞赛共征集两类公钥密码算法—公钥加密（密钥交换）和数字签名算法。第一轮征集共有 69 个算法入围，其中，有 26 个算法进入第二轮评估。

12. 总结

自 1984 首次提出量子密码概念以来，量子密码作为一种新型的密码技术为信息安全提供了另外一种不同的解决安全问题的新途径。到目前为止，量子密码研究的主要中在量子密钥分发领域。量子密钥分发技术从理论到产业已经相对成熟，但是在工程应用、标准化方面仍有不少亟待解决的问题。另外，量子密码其他技术如量子密码算法、量子认证等，无论是理论还是工程技术还有待于加强研究。

基于NLP的客服交互数据应用研究

肖钢 / 中信建投证券股份有限公司 xiaogang@csc.com.cn
刘国杨 / 中信建投证券股份有限公司 liuguoyang@csc.com.cn
潘建东 / 中信建投证券股份有限公司 panjiandong@csc.com.cn
王赵鹏 / 中信建投证券股份有限公司 wangzhaopeng@csc.com.cn
刘逸雄 / 中信建投证券股份有限公司 liuyixiong@csc.com.cn

客服系统作为证券公司连接客户的重要渠道，其内部存储了大量有价值的客服交互数据。对于监督服务质量、挖掘客户需求都有重要的意义。过去由于技术手段的不足，对数据的分析主要依赖于人工，无法满足大规模实际应用的需求。近年来自然语义理解技术不断发展并走向成熟，为我们解决该问题提供了重要的思路。本文将围绕着这个课题展开分析应用研究，希望能够给证券行业、客户服务等领域的同行提供一些参考。

一、概述

经过 20 多年的信息化发展，证券公司已经建立起了较为完善的、覆盖多种渠道的客服信息系统。通过这些系统快速触达客户，在第一时间倾听客户的声音，为整体业务发展提供有效的支持。在这个过程中，在每一套客服信息系统中通常保存了大量的与客户沟通的交互记录，这些记录中包含了丰富的、有价值的信息，例如客户意向线索、企业产品满意度等等。但是由于这些交互记录具有形式多样（如文本、音频、视频等）、内容非结构化等特点，利用传统大数据技术对其分析难度较大，因此长期以来主要依赖人工手段进行分析，其价值无法得到深入的发掘。

NLP（Natural Language Processing，自然语言处理）技术是一种利用计算机智能地分析、理解、提取人类语言中表达的真实用意的并将其合理应用的人工智能技术。随着近年来该技术的不断成熟，其已经被广泛应用在智能外呼、在线客服、智能客服质检等领域。在这种情况下，利用机器替代人工实现对客服交互数据的处理已经具备条件。本文将围绕这一方向展开研究实践，希望能够抛砖引玉，为证券行业客户服务领域的同行提供一些参考。

二、现状分析

在证券公司中，围绕着客服业务建立了多种

表 1：常见客服业务对应信息系统

业务分类		客服系统	业务说明
电话呼入业务	电话委托	电话委托系统	提供语音按键导航引导客户进行证券交易委托服务。
	电话客服	呼叫中心系统	提供人工坐席接听客户来电，基于工单系统跟踪客户的投诉和建议。
		智能电话客服	基于智能技术实现 7×24 小时自动应答客服来电咨询服务。
在线客服业务	在线咨询	优问（在线人工客服）	提供在线人工客服。
		智能客服（在线智能客服）	为在线客服（优问）提供问答辅助功能。
		邮件系统	提供客户邮件咨询服务
		社交网络（如微信，QQ）	提供在线人工客服。
	业务办理	优问（在线人工客服）	提供服务插件支持客户业务办理。
		非现场开户	通过在线客服（优问）引导客户进入系统进行业务办理。
		一柜通	
客户回访业务		智能外呼系统	利用智能机器人批量回访客户。
		呼叫中心系统	人工坐席对客户进行电话回访。
营销业务		智能外呼系统	利用智能机器人批量客户营销。
		呼叫中心系统	人工坐席对客户进行营销。
		电销系统	专业的电话营销系统。

客服系统以实现全渠道触达客户。表 1 以中信建投证券为例归纳了主要的客服业务及其对应的信息系统。

每个客服系统为满足监管或自身管理需求，都保留了完整的与客户交互的数据记录。这些记录呈现出多源、异构的特点。如表 2 所示。

这些数据中蕴含着大量的与业务相关的信息，对于指导业务开展、提升管理工作效率都有十分重要的意义。表 3 整理了可以从客户交互数据中挖掘的重要信息。

通常这些数据是由公司的运营管理团队进行收集、整理、分析的。一方面，由于缺少自动化手段，分析方式主要以人工为主，效率不高；另一方面，分析内容主要侧重于客户投诉、合规隐患等常见问题，缺乏对信息多维度、进一步深入地挖掘，遗漏了大量有价值的信息。在当前证券行业竞争日趋激烈的情况下，显然不能够满足业务快速发展的需要。在这种情况下，引入 NLP 技术实现对客服交互数据的自动化分析就成为一个值得研究的课题。

表 2：客服系统产生数据情况

客服系统	数据	格式	说明
电话委托	客户委托指令	文本	来源电话委托日志文
呼叫中心	电话录音	录音	完整记录与客户沟通内容
	坐席日志记录	文本	本次通话日志
	任务工单	文本	跟踪客户投诉建议
智能(电话)客服	电话录音	录音	完整记录与客户沟通内容
	沟通文字	文本	通过语音识别技术将通话转为文字
智能(文字)客服	沟通记录	文本、图片	完整记录与客户沟通内容
优问	沟通记录	文本、图片	完整记录与客户沟通内容
	服务日志	文本	记录本次日志的概要内容
邮件	沟通记录	文本	完整记录与客户沟通内容
社交网络	沟通记录	文本	通过社交网络提供的工具导出日志
智能外呼	电话录音	录音	完整记录与客户沟通内容
	沟通文字	文本	通过语音识别技术将通话转为文字

表 3：客户交互数据包含的重要信息

交互内容分类	蕴含信息	说明
客户咨询业务	客户投资能力	通过交易规则熟悉程度、产品了解程度判断
	产品购买、业务办理意图	如客户询问某项产品或业务，可能代表其对其感兴趣
	投诉建议	识别客户对产品的情绪、态度等，发现不满或者希望的目标
	客户画像	性别、情感、态度、兴趣
	员工画像	包括服务能力、语气等等
主动营销	客户画像	性别、态度、兴趣、投资能力
	员工营销能力	分析员工营销话术要点，结合业绩分析最佳话术实践
投诉建议	突发事件	短时间内客户投诉事件增多（如系统故障、产品缺陷等），可能需要及时预警
	投诉建议	提取客户投诉对象及原因
	客户画像	态度、情绪

三、实现方案

中信建投证券经过近几年在 AI 领域的不断积累，对如何充分利用客服交互数据，进行了大量的探索。我们构建了针对客服交互数据的分析平台。该平台的数据处理流程如图 1 所示。

如图 1 所示，分析平台主要由格式化预处理、数据仓库、分析引擎三部分组成。

格式化预处理平台利用语音识别、声纹识别等技术，对来源于呼叫中心、在线客服等系统的不同类型的数据进行预处理，形成符合规范格式的数据记录，并集中存储于客服交互数据仓库中。

数据仓库采用了“文件对象存储 + 非关系数据库”的混合存储方式，同时存储了客户交互数据原始文件（包括文本、音频文件等）以及客服交互数据的元数据（描述信息）。基于元数据，数据仓库实现了对异构多源的客服交互数据快速检索，为数据分析提供有力保障。

分析引擎基于 NLP 技术构建了大量的数据分析模型，如文本分类、实体分析等等。其主要工作就是通过分析客服交互数据的内容，分析出其中包含的语义、情感或实体等多种维度的信息，为各种类型业务提供数据支持。

四、关键技术

（一）格式化预处理

为了简化后续存储管理工作，便于数据的分析和应用，对于客服交互数据的格式化预处理至关重要。通过格式化预处理，可以将多源、异构的数据（如聊天文本记录、音频流、电话录音等）转换为统一规范化格式，降低后续数据分析、存储的难度。

目前设计客服交互数据的规范格式可包含两部分：交互原始数据和元数据。原始数据一般包括客服电话的原始录音文件、在线客服保存的原始聊天记录文件等。交互记录的元数据是指对原始数据进行描述的信息。这些信息一方面可以从源客服系统中采集获得。例如客服会话发生时间、持续时间、客服渠道、客户标识、坐席标识等，也可以通过对原数据文件的简单分析获取，例如原始数据大小、音频数据采样频率、位速等信息。

对于原始数据存在的大量音频数据，我们采用了语音识别技术（ASR）将转换为文本，与其

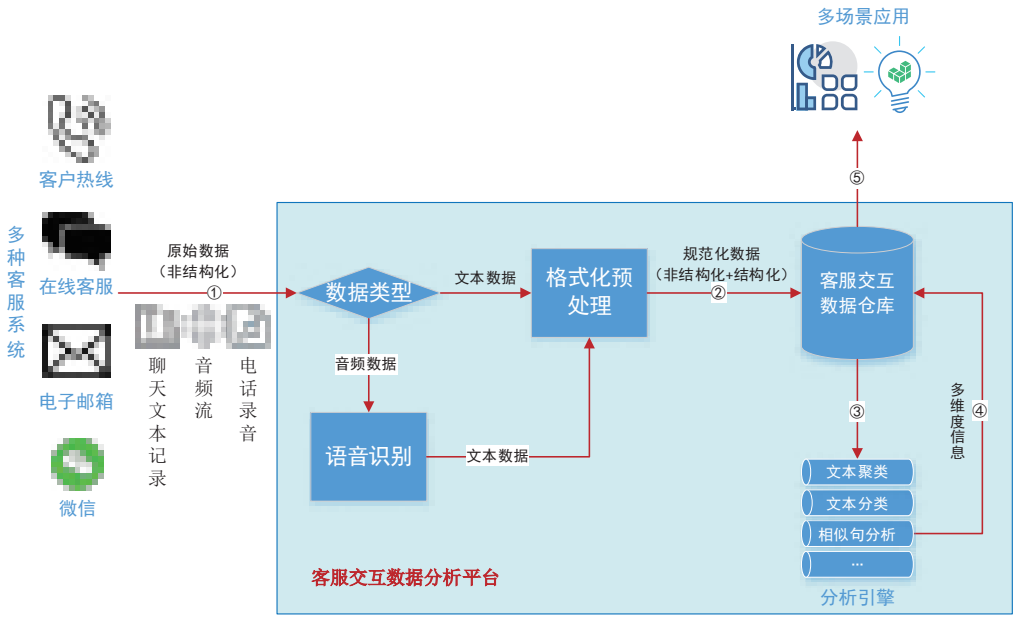


图 1：客服交互数据处理分析流程图

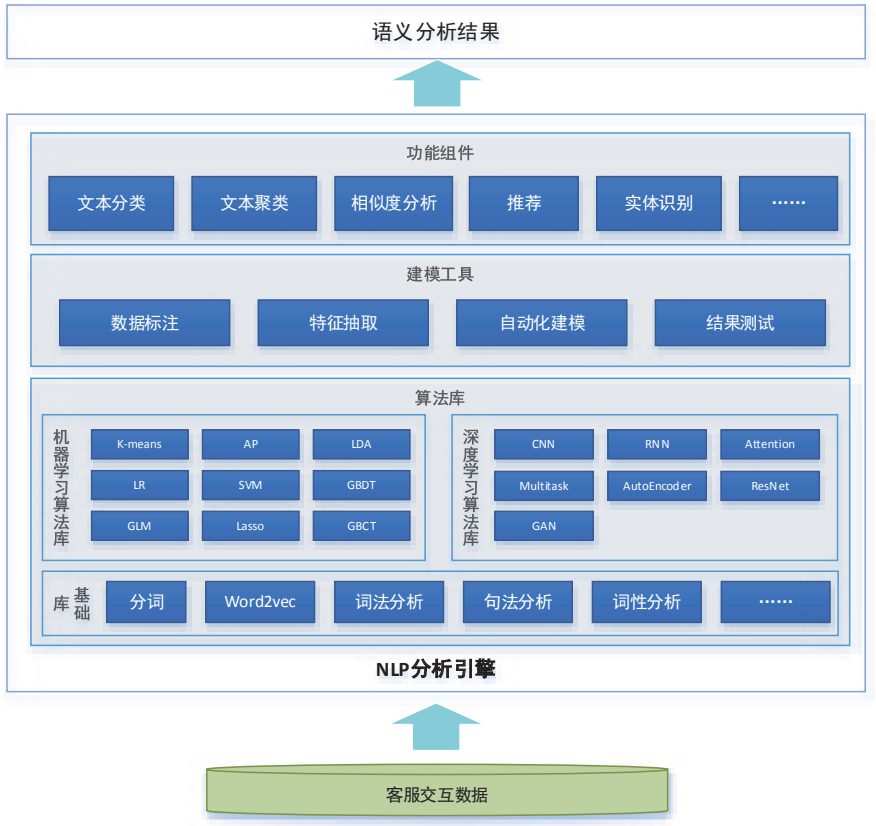


图 2：NLP 分析引擎

他文本格式的客服记录一起进行存储。以此降低后期对数据 NLP 分析的复杂度。

（二）NLP 分析引擎

通过 NLP 技术，我们构建了专门用于分析客服交互数据的 NLP 分析引擎，对数据仓库中分析挖掘隐含的业务线索、语义及要点信息。

图 2 展示了目前我们构建的用于客服交互记录分析引擎架构。整个引擎可以从下到上可以分为三个层次：(1) 基础算法库；(2) 建模工具；(3) 功能组件。

1、基础算法库

分析引擎底层提供了常见的 NLP 基础算法库，如分词、词法分析、句法分析、实体识别等等。以及主流的机器学习和深度学习算法库。机器学习算法库提供 K-means、LDA、GBDT 等算法，深度学习算法库提供 CNN、RNN、AutoEncoder 等。

2、建模工具

在基础算法库的基础上，引擎为分析人员提供了分析建模工具，可以根据具体业务需求定制建模。经过定制的模型可以通过预置的结果评估组件进行性能测试，以此来方便分析人员掌握模型的性能指标（如准确率、召回率等）是否满足实际应用的需求。

3、功能组件

完成训练测试的模型将封装为标准的功能组件。分析引擎建立对功能组件的版本控制，并对其生命全周期（包括发布、升级、下线等）进行管理。

（三）多标签文本分类

对于客服交互记录进行多标签分类是目前 NLP 引擎分析的重要功能组件，也是目前获取、管理、应用交互文本语义的最有效的方式之一。各业务场景的应用大多可以围绕着客服交互数据的一个或若干个标签展开。例如在对客服质检时，

可以通过分析识别对话记录中客户的问题标签以及坐席回答的知识点标签，并对两者的匹配情况来分析判断坐席的服务质量。

目前我们采用的多标签文本分类模型如图 3 所示：

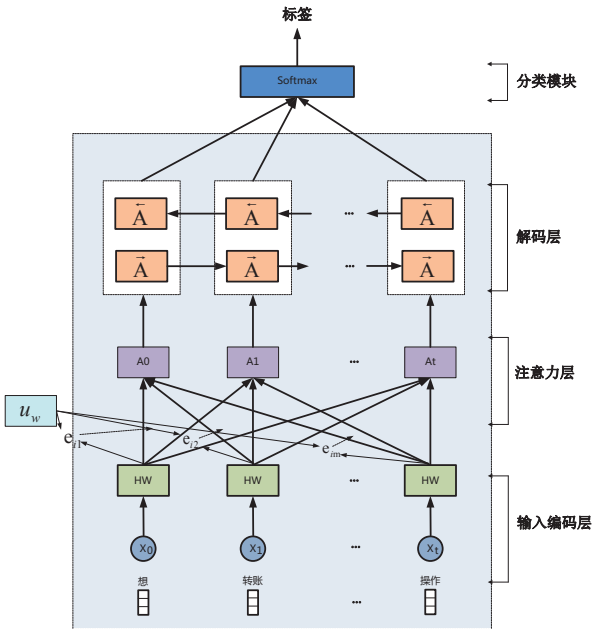


图 3：多标签文本分类模型

分类模型主要分为输入编码层、注意力层、解码层、分类模块组成。其中输入解码层负责对文本词向量特征进行编码，并通过 Highway Network 门控制机制对词向量维度进行调整。注意力层负责对经过编码的文本特征给予不同的权重，并筛选出对类别标签重要的文本特征。编码层使用 LSTM 按顺序生成标签，通过 LSTM 结构处理标签序列之间的依赖性，以此来考虑标签的相关性。最后编码层输出标签序列，经过分类模块找到最优的标签序列。

五、应用实践

围绕着客服交互记录的分析，我们在多个业务领域进行了应用的探索：

（一）客服质量检验

中信建投证券于 2019 年开始进行了客服记录自动化质检系统的建设。前期该系统主要通过规范用语、说话语速、禁用词语等简单、易于判断的维度进行质量检测。但是通过 NLP 技术，使得我们可以进一步对客户服务过程中客户的情绪、坐席的情绪、坐席解答问题的情况等信息进行评估，从而进一步丰富了质检的内容，为公司准确把握客服质量提供了依据。

表 4 列出了我们对电话客服质量主要的检测项。

通过为每一个质检项建立语义标签。质量检测时，通过对交互数据的标签的识别，来进行对服务质量的评估。例如当我们识别出对话记录中出现“客户要求核实信息”的标签时，判断对话记录中否同时出现“坐席帮助客户反馈”的标签，由此来判断服务是否满足客户的需求。图 4 为目前我司质检系统质检项的配置界面：

图 4：质检评估项配置界面

图 5、图 6 展现了目前智能质检系统的运行的情况。目前智能质检系统已经覆盖了公司所有的电话客服的服务业务。

（二）话术辅助训练

2020 年上半年，我们为全公司客户经理构建了一套话术演练系统。客户经理可以在设定的 50 个营销业务场景中与智能对话机器人模拟的客户进行对话沟通，从而实现对自己营销话

表 4 客服质量项

评分维度	评分类别	评分项目
服务规范	规范用语	未使用标准开头语、结束语
	服务禁语	1. 使用口头语、语气词、俗语、内部用语 2. 通话中出现辱骂用户 3. 出现《服务禁语》中相同或类似语句
	服务态度	1. 客户有负面情绪时，未及时安抚，无视客户的抱怨 2. 通话中有不尊重客户的语气、语调、语言，质疑客户、说教客户 3. 语气不耐烦，明显缺乏耐心，敷衍、推脱、搪塞客户 4. 注意力不集中、未认真倾听、正确理解客户意图、答非所问 5. 语速明显过快、不礼貌地打断客户、出现明显抢话的现象
	服务效率	1. 在线查询时间较长，超过 1 分钟未及时回应客户 2. 通话中未告知顾客原因，5 秒钟以上未理会顾客 3. 通话结束后，未及时挂机
业务能力	业务解答	业务解答或信息提供错误
	客户回访	1. 有话术或问卷要求的回访，未按照话术顺序执行 2. 回访过程中遗漏关键话术或遗忘询问问卷中的问题
行为合规	诱导客户	1. 采用不符合实际的煽动性的、夸大的语言或编造虚假信息等方式诱导客户 2. 诱使客户进行不必要的交易 3. 以其他不正当手段推广业务方式招揽客户
	承诺收益	对客户承诺保底、承诺收益、承诺不受损失或约定分享收益
		向客户提供了投资建议或咨询信息，但未向客户说明风险提示
致命错误	被投诉	出现严重的业务差错或服务态度恶劣，可能或已造成重大投诉
	信息保密	未按照规范泄露保密信息

术能力的训练。每一个客户经理在完成话术练习后，演练的过程将通过分析平台进行评估。通过对话的情绪、标准型、语义完整性等多个维度进行量化评分，从而有效的监督指导客户经理的话术学习。

目前话术演练系统已经在公司的企业微信中发布，支持了两融业务的 8 个话术训练场景。系统运行效果截图如图 7、图 8。

(三) 投诉事件监控预警

中信建投证券在线客服优问是公司触达客户的主要途径。上线四年来，历经了多次突发事件，已经成为公司获悉问题、安抚客户、解决问题的重要环节。但是我们注意到，在每次信息系统异常事件出现时，在优问上通常会出现大量客户的集中投诉反馈。但是由于对客户的服务模式采用一对一的方式。当发生问题时，从客服人员

图 5：客服质检统计情况

图 6：客服质检详细信息

反馈后台运营人员，再到运营人员察觉问题，再到故障解决，往往需要很长的时间。这就导致客服人员无法即使安抚客户，给客户带来了不好的体验。

针对上述问题，利用交互数据分析平台，对实时的客户服务记录进行分析，为不同场景下的投诉事件打上标签。在短时间内，如果发现某类投诉事件标签出现陡增的情况，进行实时报警，以便运营人员第一时间跟进解决问题。

图 9 展示了通过交互记录分析系统获得的标签情况。

图 10 展示了我们对公司 2019 年 2 月 26 日的客服交互数据的分析情况。可以看到在当天开市（9:30）以后，在短时间内客服系统接到大量的客户反馈：“手机炒股软件无法登陆”，即标签“咨询 - 无法登陆”的出现频率急剧增加。因此可以预测出：相关系统可能出现异常。通过对此类情况加以监控，一方面可以及时向运维人员提供预警，另一方面，也为客服人员第一时间做好客户安抚工作提供了依据。

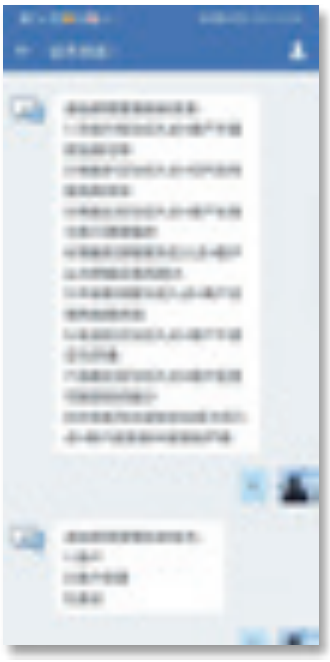


图 7：话术演练场景选择

图 8：话术训练及评估得分

图 9：客服交互记录标签

图 10：客户投诉记录实时分析

六、总结

本文基于 NLP 技术，设计并构建了客服交互数据分析平台。利用该平台对多种渠道客服系统的客服对话记录进行收集、整理、存储、分析，进而充分发掘客服交互数据的价值。目前该平台已经在多个业务场景中开展应用，取得了较好的效果。下一步的研究工作主要有两个方面，一方面是进一步深入研究 NLP、ASR 等技术，优化技术精度和性能，为数据分析工作夯实基础。另一方面是继续探索针对交互记录的新的应用场景，最大化地发挥数据的潜在价值。

海通证券互联网对客数字化运营实践

熊友根、王洪涛 / 海通证券有限公司 软件开发中心

对于目前国内大部分证券公司而言，客户群体主要分为零售客户与机构客户两类。相对以企业法人为主体的机构客户，笔者将零售客户定义为经纪条线的个人客户，通过证券公司提供的移动 APP、网上交易终端等互联网工具进行证券委托、融资融券等业务，部分资金量大的零售客户还可以获得更专业的行情交易工具以开展更复杂的业务。互联网终端是券商零售客户的主要交易平台，与互联网公司相比，券商互联网终端面临着用户规模与活跃度难以提升的瓶颈。本文从金融科技视角，聚焦券商公司互联网零售对客整体的业务生态，通过金融科技整合前中后台能力，从用户运营、内容运营、活动运营、自动运营四个方面，以“运营”为中心，对证券公司数字化运营的结构与机理进行分析与研讨，形成一套完整的数字化运营方法，建立海通数字化运营平台，帮助业务运营团队自主计划、自主配置、自主上下架，实现辅助决策式运营和数据驱动式运营，进一步提升海通互联网对客产品质量，为用户提供更加优质的服务。

一、引言

零售对客业务是证券公司的一种重要业务模式，在中国 30 多年的证券市场发展进程中，广大的个人投资者为企业融资以及资本市场的繁荣发展做出了巨大的贡献。而另一方面，由于证券公司普遍人手不足，绝大部分的零售客户并没有获得良好的服务，特别是在柜台交易和网上交易阶段，证券公司为广大零售客户提供的服务仅限于进行证券买卖委托和查询等交易通道服务。

2013 年 3 月 15 日中国证券业协会发布《证券公司开立客户账户规范》，放开非现场开户限制。随后，零售客户的规模呈现爆发式增长，证券公司原有的网上交易和移动 APP 与互联网公司的自营产品差距越来越大，为了将客户保留在自有的系统内，证券行业开启了在互联网金融领域的全方位竞赛。各券商均投入大量的人力物力完善自己的移动 APP，这也带来了各类应用功能，交互体验和视觉体验的快速提升，客户的满意度普遍得到了改善。但是在用户规模上，与互联网公司的 APP 相比，证券公司 APP 与互联网公司 APP 的用户规模差距似乎并没有缩小，与此同时，用户活跃度等关键指标的差距似乎还越来越大，导致很多证券公司对互联网金融的热情有所降低，出现了撤并、降级或者改名互联网金融部的现象。一些互联网金融发展比较好的头部券商似乎也遇到了发展瓶颈，整个行业处于迷茫的状态中。

另一方面，金融科技的发展日益升温，相对于互联网金融，从技术层面来看，券商互联网金融关注的是移动 APP 等前端业务，赋能的是零售客户，而金融科技关注的是公司整体的业务生态，赋能的是全体客户和内部职能部门，通过金融科技整合前中后台能力，驱动证券公司向数字化转型。作者认为，对于处于迷茫的互联网金融来说，加强数字化运营的能力建设，是提升用户获得感，缩小与互联网公司差距的关键手段。

二、以“运营”为中心的数字化运营

数字化运营是指通过数据化的工具、技术和方法，对运营过程中的各个环节进行科学的分析，为数据使用者提供专业、准确的行业数据解决方案，从而达到优化运营效果和效率、降低运营成本、提高效益的目的。数字化运营的核心是“运营”，通过收集到的各类数据，以个性化的功能、内容、活动等形态，为用户提供用户可能感兴趣或者与用户切身利益相关的信息，引导用户完成相关操作。一套较为完整的运营方法包括用户运营、内容运营、活动运营和自动运营四个部分。

2.1 用户运营

用户运营是以用户为中心，开发用户所需要的功能和产品，策划与用户相关的活动，创造与用户相关的内容，最终达到运营的目标。用户运营通常又包括“拉新”、“留存”、“转化”、“促活”四个方面。

“拉新”：对于一个产品，开源是最重要一环，吸引新的用户使用产品，是产品不断发展壮大的基础，不同的产品拉新的手段或者策略有所不同，同一个产品不同用户群体的拉新策略也有所不同，e 海通财拉新除了采用传统的银行渠道、互联网渠道、分支机构线下经纪人渠道、硬广告和外部链接等手段。还有三个措施：1、提升曝光率，通过提升 APP 的更新频率和质量提升 APP 的曝光概率。我们以每个月两个迭代的固定节奏进行版本发布，每更新一次版本，安卓和苹果应用市场就会增加一次曝光的机会，下载位置就会相对靠前，用户搜索看到的概率就更大。2、提供低风险高收益理财产品，针对新客户提供一定周期的较低风险较高收益的理财产品，为用户带来实实在在的收益。3、持续的运营活动，比如限时送 Level2、竞猜抽奖等，提升用户粘性。

“留存”：很多用户可能是基于一些拉新活动而安装的 APP，并没有很强的使用这款 APP 的

需求，如果将用户拉过来以后不做任何维护，这批用户很容易流失，之前所有的投入都将成为沉没成本。因此，留存率是判断产品价值最重要的标准。在如何提升用户的留存率方面，我们从价值、功能、消息、激励、场景 5 个方面进行了探索。1、价值留存：首先让价值来实现留存，用户使用证券 APP 的核心诉求就是投资一些产品，获得一定收益，我们为用户提供了全品种的投资产品，满足不同用户不同阶段的投资需求，比如银行理财产品、公募基金、私募基金、A 股、港股、融资融券、贵金属、期权等。2、功能留存：通过功能来实现留存，对于大部分股民来说，证券 APP 在熊市和震荡市使用的频率比较低，但是很多股民又想及时了解国家经济走势和重大政策对股市的影响，把握最佳入市时机，我们为适当性用户提供海通首席研究员和投资顾问视频直播服务，每天进行宏观经济阶段性解读、市场趋势分析和行业分析等。3、消息留存：用消息推送来实现留存，我们开发了新股打新的提醒、理财产品到期提醒、新的理财产品发售提醒、市场异常波动提醒等。4、激励留存：通过用户激励体系实现留存，目前很多公司都有一套完整的会员服务体系，为不同等级的会员提供不同的服务，我们也构建了通享会员体系，有白银、黄金、砖石等级别，提供丰富的积分获取和积分兑换渠道。5、场景留存：增加可使用场景实现留存，证券 APP 的核心用户都是交易型用户，有很多交易流水数据，围绕交易账号、交易流水和自选股，我们开发了智能账单、已清仓股票查询、自选股分析、预约打新、场内基金 T+0 套利等功能。

“转化”：对于证券公司 APP 而言，真正能产生营业收入的用户是理财用户和交易用户，所以 APP 运营的最终目的也是要将拉新、留存下来的用户转化为这两类用户。我们针对不同阶段的用户制定了不同的引导方案，通过使用较低的积分就可以兑换咖啡、抱枕、视频会员等权益服务，将下载用户向注册用户转化；通过使用通财钱包、现金赢家、OTC 理财产品等低风险、货币型、固收型、灵活型和结构化等产品，将注册用户向理财用户转化；通过使用国债逆回购、场内货基 T+0 套利、指数估值和预约打新等产品将理财用户向交易用户转化。

“促活”：在券商的半年报和年报上经常能看到一个叫做“用户数”的数字，这个数字为所有安装过券商 APP 的用户数总和，对于大部分 APP 来说，这个数字与实际活跃的用户数之间存在巨大的差距，因为很多用户安装完以后就再也不使用了，或者使用的频次非常低，所以业务团队有一个重要的指标就是尽可能的通过一些手段将用户激活，提升月活跃率和日活跃率。我们通过用户分类、用户画像、自动化召回与刺激召回四步，建立了一套流失召回体系来促活用户。STEP1、用户分类：梳理用户分类及流失定义，我们将用户分为新用户和老用户，新用户是下载了 APP 但没有注册过社区，也没有登录过交易的用户，老用户是指有交易流水的用户。我们将新用户的流失定义为 1 周内没有再次打开 APP 的用户，将老用户的流失定义为 1 月内没有再次打开 APP 的用户，这个时间可以根据情况自己定义。为了将流失的用户促活，我们需要知道这些用户在 APP 上做了什么，为什么要走。STEP2 用户画像：为了了解用户在 APP 上做了什么，为什么要走，我们需要建立基于用户画像的精细化行为标签。用户画像从四个维度进行绘制，分别是用户的性别、年龄等基础客观属性；用户在 e 海通财上的当前状态；用户的佣金贡献、交易量贡献、资产规模等级别；用户在 e 海通财上发生过的重要行为，比如参与活动偏好等。经过四维画像后，我们基本上清楚了用户最后停留的行为状态。STEP3 自动化召回：建立自动化召回体系，将用户根据状态放在用户池、预警池、维护池和流失池 4 个不同的流量池中，针对不同的流量池触发不同的自动化运营策略。STEP4 刺激召

回：设计有针对性的文案，将预警池用户进行清洗分群以后，推送相应的文案或活动刺激召回。

2.2 内容运营

内容运营主要指通过原创、编辑、组织等手段，创作或重塑产品并予以呈现，从而提高互联网产品的价值，让用户对产品产生一定的黏性。内容主要包括文字、图片、视频、歌曲和游戏等，我们做了大量的内容运营相关的工作，包括盘前、盘中、盘后实时解读、投顾投教内容的编辑推送、视频直播上下架、用户意见回复以及终端功能图标动态调整等。

2.2.1 资讯运营

证券类 APP 最重要的功能是开户、行情、交易、理财和资讯。开户、行情、交易和理财从功能上来说，大部分券商基本上相似，从内容运营的角度来看，基本上可操作的空间不大，但是资讯内容各有千秋。证券公司 APP 与某顺、某东等互联网公司 APP 最大的差异就是在资讯、股吧等方面。在人员配置上，某顺仅资讯运营人员就有 40 多人，而相当多的证券公司是没有资讯运营团队的。海通有一个 10 人以下的资讯运营团队，每天在根据搜集到的材料，编辑整理的同时，从研究所获取最新的研究报告通过数字化运营平台进行录入，审核通过后向用户进行推送。具体的操作和终端展示如图 1 所示。

2.2.2 大 V 运营

大 V（投资顾问）对 APP 等互联网产品具有非常强的吸粉能力，包括社交类的微博，财经类的雪球等。海通也从员工中培养了一批自己的大 V，时常向客户撰写一些投资方面的专业知识，通过数字化运营平台进行上下架，并在 APP 终端专

图 1：海通数字化运营平台 – 资讯运营

图 2：海通数字化运营平台 – 大 V 运营

图 3：海通数字化运营平台 – 投教运营

区进行展示。具体的操作和终端展示如图 2 所示。

2.2.3 投教运营

证券类 APP 是为用户提供各类证券买卖、融资融券等股市业务服务的平台。为帮助股民应对股市风险，需要为股民提供教育。作为一家综合性证券公司的移动投资平台，海通 e 海通财 APP 有一块投教专区，为投资者提供文字、图片和视频等证券市场基础知识、风险教育、投资技巧以及 APP 功能介绍等投教内容。业务运营人员通过数字化运营平台配置相关的内容，并在后端对内容进行管理配置。具体的操作和终端展示如图 3 所示。

2.2.4 终端功能图标运营

由于业务不断变化、不断创新，证券类 APP 需要有一个灵活的终端架构，既可以由用户自己编辑部分终端界面，满足自己的操作习惯，又能满足业务运营人员在后端对终端功能位置和图标进行配置的需求，实现业务快速上线。海通 e 海通财 APP 首页和交易页面的功能图标和位置可以由业务运营人员通过数字化运营平台根据版本动态配置，通过可见及可得的操作体验方便运营人员管理，减少差错。具体的操作和终端展示如图 4 所示。

2.3 活动运营

活动运营与内容运营的一个区别在于内容运营是长期的，而活动是阶段性的。内容运营是形式上基本固定的运营，而活动运营是阶段性的，需要一定的准备、策划、执行、传播和复盘。每个活动都有一个明确的主题，所有的用户围绕着

图 4：海通数字化运营平台 – 终端功能图标运营

图 5：海通数字化运营平台 – 活动运营

这个主题进行活动。海通 e 海通财的活动运营形式非常多，比较大的活动运营有世界杯竞猜大赛、模拟炒股大赛、Leve2 优惠活动、视频直播活动、知识问答活动等等。所有的活动运营都可以在数字化运营平台进行新增与删除，具体操作如图 5 所示。

2.3.1 视频直播活动

视频直播是一种非常直接有效的信息传播方式，抖音、快手等直播平台非常受各年龄段用户喜爱。海通 e 海通财尝试通过视频直播的方式向用户提供广播式投资顾问，从而提升 APP 的活跃度和黏性。

2.3.2 模拟炒股活动

实盘交易毕竟存在一些风险，为了使得用户了解交易规则，体验交易过程，积累交易经验，并且引导用户从低风险交易品种入手向交易用户转化。海通 e 海通财举办了 ETF 模拟交易大赛，规定只允许买卖 / 申购 ETF 基金，通过在规定期限内统计总收入的方式确定比赛名次，并为获奖者颁发奖品。参与 ETF 模拟交易大赛的用户数非常可观，有效的提升了 e 海通财的用户转化率。

2.3.3 知识问答活动

知识问答是近年来开始流行的一种通过回答一系列主题知识获得一定奖励的交互式游戏。海通 e 海通财在数字化运营平台中，将投教类的知识包装成知识问答并提供给用户，供用户在 APP 中进行游戏挑战。

2.4 自动运营

自动运营是根据用户的个性化特征和业务场景进行逻辑设定，当业务数据触发设定条件时，自动为用户执行个性化服务。自动运营的最大特点就是全程由数据驱动，程序自动执行，不需要人工干预。一个完整的自动运营服务包括数据打通、数据整合、运营计划创建、用户触达、运营计划调整五个部分。

STEP1 数据打通：首先需要打通数据。通过打通 CRM、数仓、产品中心、资讯中心等应用系统与运营平台之间的数据，对用户特征、用户行为、交易流水、理财产品、新闻资讯等业务数据进行采集；

STEP2 数据整合：数据打通后，需要进行数据整合，包括标签化处理以及对用户的固定特征进行分群等；

STEP3 运营计划创建：根据业务数据进行运营计划的创建，设置好计划的类型，选择受众客群；

STEP4 用户触达：根据最终的业务场景目标制定用户个性化触达策略，包括触达的方式、触达的消息内容以及触达以后用户的引导等；

STEP5 运营计划调整：根据用户的点击回执以及用户后续的业务办理情况进行自动化运营

图 6：海通数字化运营平台 – 自动运营闭环场景

效果的分析，调整自动运营计划和策略。

在海通数字化运营平台中一个自动运营的闭环场景如图 6 所示。

三、海通数字化运营平台

综上所述，海通证券目前主要的互联网对客运营活动都是基于数字化运营平台来展开。从开始单纯的通过 CRM 筛选出符合各类条件的客户信息，再经过短信平台下发短信的形式或者电话的形式与客户进行信息的传递。数字化运营平台经过了较长时间的摸索逐步成型。截止目前，数字化运营平台已成为建立于大数据平台、人工智能平台、用户行为分析系统、资讯中心、消息中心、产品中心、会员中心等中台系统基础上，对各类数据进行整合关联的一体化、数据驱动的互联网运营能力中心。具备为 APP、PC、微信小程序、微信公众号和基于 H5 的对客终端等终端提供数字化运营支持的能力。海通证券互联网数字化运营能力中心如图 7 所示。

数字化运营平台作为互联网运营能力中心的核心，起到了承上启下、关联整合的作用。海通 2018 年正式立项建设数据化运营平台，包括数据采集、数据清洗、数据整合、数据分析和数据运用五大模块。数据采集实现了 e 海通财 APP、e 海通财 PC、e 海方舟等对客终端的用户行为数据的采集以及后台业务数据和日志数据的采集；数据整合模块复用了大数据平台的存储能力，实现了数据的统一管理；数据分析模块具备可自定义多维度的灵活联合检索功能，实现了托拉拽的灵活界面展示；数据应用模块包括精细化客群管理和个性化消息推送，可实现自动运营。同时，数字化运营平台实现了所有与运营相关的应用模块整合，业务运营人员只需要在数字化运营平台即可完成所有的运营活动。海通数字化运营平台架构图如图 8 所示。

四、总结

券商传统的互联网终端基本上是一个个封闭的应用，无论是技术人员还是业务人员，都难以了解终端客群及其使用偏好，无法为用户提供精

图 7：海通证券互联网数字化运营能力中心

图 8：海通数字化运营平台架构图

细化、个性化服务。这使得业务团队缺乏运营服务的抓手和工具，无法评估运营活动效果，导致用户处于一种自我发展的状态。

海通数字化运营平台通过数据和接口将后台庞大的应用系统关联起来，形成千人千面的标签体系，通过客群分类和运营策略，实现后端配置和前端展现的动态联动，引导面向客户的各项目标执行。

数字化运营平台作为海通证券互联网运营的主要载体，在打通已有多套应用系统、复用已有技术栈、整合各类数据、整合各应用系统运营模块的基础上，已形成集中式、一体化的运营中台，为业务运营团队提供线上用户运营、内容运营、活动运营和产品运营服务。业务运营团队可自主计划、自主配置、自主上下架，达到辅助决策式运营和数据驱动式运营目的。

随着互联网金融的发展进入深水区，功能、交互、视觉、性能等基本的产品要求已不再是瓶颈，证券行业互联网对客产品发展的好坏将取决于券商数字化运营和智慧化运营的能力。海通互联网对客产品将借助于数字化运营平台，一如既往的为用户提供优质服务，通过大数据和人工智能技术，融合数字化运营工具，最大限度的为用户普及知识、揭示风险、实现价值最大化。

I 信息资讯采撷
nformation

监管科技全球追踪

监管科技全球追踪

国际动态

世界经济论坛（WEF）发布首份数字资产报告

近日，世界经济论坛（WEF）全球加密未来理事会发布首份数字资产报告（Crypto, What Is It Good For? -An Overview of Cryptocurrency Use Cases）。报告指出，有关区块链技术的讨论文章很多，但是除了价格和金融投机外，人们对加密货币领域似乎并不太关注。在本次报告中，理事会重点介绍了一系列基础层协议、次级协议和服务提供商，帮助人们了解加密货币在金融服务及其他与金融科技无关领域的服务，使社会经济能够从这种创新的模式中获得更多收益。

国际清算银行（BIS）、瑞士国家银行和 SIX 联合开展央行数字货币实验

2020 年 12 月 3 日，国际清算银行（BIS）宣布，瑞士的一项有关批发央行数字货币（CBDC）的试验显示出央行货币在分布式分类账上的“可行性”。该项目由瑞士国家银行（SNB）与 BIS 创新中心及瑞士证券交易所运营商 SIX 合作发起，研究了使用批发中央银行数字货币结算数字资产以及将 DLT 平台链接到现有支付系统的可行性。根据 BIS 的报告，Helvetia 项目证明了这两种方法的可行性。BIS 表示，在使用仅限于银行和金融机构的 CBDC 时，批发 CBDC 具有潜在优势，尽管它也带来了一些政策和治理挑战。

国际清算银行（BIS）发布 CBDC 基本原理与核心特征报告

10 月 9 日，国际清算银行发布了《央行数字货币：基本原理和核心特征》（《Central bank digital currencies: foundational principles and corefeatures》）。据国际清算银行透露，七个国家的中央银行与之组成的小组共同合作编制了这份报告，旨在为中央银行实现其公共政策目标确定公开发行央行数字货币所必需的基本原则——为了使任何辖区考虑进行 CBDC，所有政府必须满足某些标准：（i）中央银行不应通过发行央行数字货币来损害法定货币或金融稳定；（ii）央行数字货币必须与现有货币形式共存并互补；（iii）央行数字货币应促进创新和效率。严格满足这些标准并提供建议功能的 CBDC 可能是中央银行实现其公共政策目标的重要工具。这批中央银行将继续合作并探讨报告中概述的实际影响。

金融稳定委员会（FSB）就与外包和第三方关系有关的监管问题进行咨询

11 月 9 日，金融稳定委员会（FSB）发布了一份讨论文件，以供公众咨询，内容涉及与外包和第三方关系有关的监管和监督问题。讨论文件借鉴了 FSB 成员之间进行的一项调查的

结果。金融机构数十年来一直依赖外包和其他第三方关系。然而，近年来，与第三方广泛而多样的生态系统的相互作用的范围和性质已经改变，特别是在技术领域方面。金融部门最近对 COVID-19 的回应强调了管理金融机构与第三方互动风险的好处和挑战。新冠可能也加速了对某些第三方技术的依赖的趋势。

国际清算银行（BIS）发布监管沙箱对金融科技融资影响的报告

11 月 9 日，国际清算银行发布了《监管沙箱内部：对金融科技资金的影响》(Inside the regulatory sandbox: effects on fintech funding)。报告指出，2015 年，国际金融市场行为监管局 (Financial Conduct Authority) 率先推出了全球首个监管沙盒。迄今为止，已有 50 多个国家采用了沙盒，有证据表明它们确实有助于创新金融科技公司筹集资金文件分析了进入英国的监管沙箱如何影响金融科技公司筹集资金的能力：他们发现进入沙盒后筹集资金的可能性更高，平均筹集的资金数量增加约 15%。我们的研究表明可能出于以下三个原因：监管沙箱通过减少信息不对称性和监管成本来改善获得资金的途径，沙盒入场对募集资金的积极影响对于规模较小和较年轻的公司尤为明显；首次投资人和英国以外的投资者所占份额增加；拥有具有金融法个人背景的 CEO 的公司从沙盒中受益较少。

欧美动态

美国证券交易委员会（SEC）与金融科技战略中心升级为独立部门

2020 年 12 月 3 日，美国证券交易委员会(SEC)宣布其创新与金融科技战略中心（通常称为 FinHub）将成为独立办公室。Valerie A. Szczepanik 将继续领导这一机构，并直接向 SEC 主席汇报。FinHub 于 2018 年在 SEC 的企业财务部内成立，以鼓励金融部门负责任的创新，涉及分布式账本技术和数字资产、自动化投资建议、数字市场融资以及人工智能和机器学习等多个领域。通过 FinHub，市场和技术创新者以及国内外监管者已经能够与 SEC 员工就联邦资本法范围内的资本形成、交易和其他金融服务的新方法开展有效互动。

欧盟委员会（EC）制定 75 亿欧元预算打造“数字欧洲”，重点关注人工智能与云计算

2020 年 12 月 14 日，欧盟委员会（EC）就“数字欧洲”（Digital Europe）计划的约 75 亿欧元预算达成协议。从 2021 年开始至 2027 年，这项计划希望为数字化转型提供支持，确保民众和企业（特别是中小企业）获得高质量的公共服务，提高欧洲在全球数字经济中的竞争力并实现技术主权。据介绍，本次预算分配比例大致为：超级计算（22 亿欧元）、人工智能（AI）（21 亿欧元）、网络安全（17 亿欧元）、高级数字技能（5.8 亿欧元）和确保广泛使用数字技术（11 亿欧元）。具体细节包括通

过在 2021 年底之前至少收购一台百万兆级超级计算机，使欧洲成为全球顶级超级计算机地区；在健康、环境 / 气候、移动性、制造和能源领域建立并提供用于人工智能的全欧数据空间以及测试和实验设施等。

美国 SEC：创新与金融科技战略中心升级为独立部门

12 月 3 日，美国证券交易委员会（SEC）宣布其创新与金融科技战略中心（通常称为 FinHub）将成为独立办公室。Valerie A. Szczepanik 将继续领导这一机构，并直接向 SEC 主席汇报。FinHub 于 2018 年在 SEC 的企业财务部内成立，以鼓励金融部门负责任的创新，涉及分布式账本技术和数字资产、自动化投资建议、数字市场融资以及人工智能和机器学习等多个领域。通过 FinHub，市场和技术创新者以及国内外监管者已经能够与 SEC 员工就联邦资本法范围内的资本形成、交易和其他金融服务的新方法开展有效互动。

美国证券交易委员（SEC）发布股票市场数据收集、整合和传播规则

12 月 9 日，美国证券交易委员会 (Securities and Exchange Commission，简称 sec) 发布规则对在交易所上市的全国市场系统股票 (“NMS 市场数据”) 收集、整合和传播市场数据的基础设施进行现代化改造。自 1970 年代后期开始实施以来，这一基础设施一直没有重大的更新。新规则对 NMS 市场数据的内容进行了更新和显著扩展，以更好地满足当今股票市场投资者的多样化需求。通过培育竞争环境和提供一种新的去中心化模型，承诺减少延迟和其他新的效率，所采用的规则还更新了网管市场数据的整合和传播方法。“今天的规则是我们更大计划的一部分，也是我们正在进行的努力的一部分，目的是使我们的股票市场监管结构现代化，以应对我们交易市场的重大变化，更好地满足投资者 (包括散户和机构投资者) 和其他市场参与者 (包括发行人) 的需求。特别是，这些规则旨在增加竞争和透明度，这将提高数据质量，并为所有市场参与者提供数据，”主席 Jay Clayton 说。

欧盟数字金融新战略出台

9 月 24 日，欧盟委员会（EC）采用了新的数字金融一揽子计划，包括数字金融和零售支付战略，以及有关加密资产和数字弹性的立法提案。一揽子计划将激发欧洲在金融领域的竞争力和创新能力。它将为消费者提供更多的金融服务和现代支付的选择和机会，同时保护消费者并维护金融稳定。其中，数字金融战略的目标是使欧洲的金融服务更加数字化，并促使欧盟金融服务提供商负责任的创新和竞争。数据管理也是战略的核心。为了与欧盟委员会更大范围的数据战略保持一致，今天措施的目标是促进数据共享和开放金融，同时保持欧盟在隐私和数据保护方面的高标准。最后，该战略旨在确保金融服务提供商之间公平的竞争环境：相同的活动、相同的风险、相同的规则。

英美就人工智能合作研发共同发布宣言

9 月 25 日，美方和英方就人工智能研究和开发合作达成协议发表了共同宣言——《推动人工智能技术突破的共同愿景》(A Shared Vision forDriving Technological Breakthroughs in Artificial Intelligence)，包括：认识到人工智能 (AI) 带来的好处和机会，以及人工智能对我们未来经济增长、

健康和福祉、保护民主价值观和国家安全的重要性；希望利用人工智能技术赋予我们的公民权力，提高他们的生活质量，并促进一个技术生态系统，通过将人工智能融入经济，使创新蓬勃发展；认识到共享公共数据集最佳实践的价值，以促进人工智能创新，并在监管框架上交换信息，以消除创新障碍，同时获得公众信心；认识到基础和早期研发 (R&D) 合作的重要性，以及为持续和未来的人工智能创新和使用建立研究基础的必要性；认识到促进信任和理解对实现人工智能并充分发挥其潜力的重要性；认识到有能力的研发队伍和人工智能相关技术技能的劳动力开发的重要性，包括学徒制、再技能培训、计算机科学和 STEM 教育——这将使当前和未来几代工人获得能力和能力，并改善人民生活质量。

英国金融行为监管局（FCA）推出全新数据收集平台 RegData 取代 Gabriel

11 月 24 日，英国金融行为监管局（FCA）宣布将用新的数据平台 RegData 取代 Gabriel 系统。所有在 Gabriel 定期提交监管报告的 52000 家公司都需要使用 RegData。RegData 更快速、更易使用，并且使用灵活的技术构建来更快地解决问题以持续改善用户体验。RegData 系统相较原有系统有三大优势：访问系统——速度更快导航更清晰且配备更全面的在线资源；查看报告——改进公司时间表和提交历史的布局安排；提交数据——提供更好的指南和更强的数据验证功能。

G7 官员探索中央银行数字货币相关的机遇和风险，强调数字货币监管的必要性

10 月 13 日，七国集团（G7）财政部长和央行行长发表有关数字支付的声明，称七国集团的许多主管部门正在探索与中央银行数字货币（Central Bank Digital Currencies, CBDC）相关的机遇和风险。G7 致力于解决支付系统中现有的摩擦，并继续支持 FSB、FATF、CPMI 和其他标准制定机构的工作，以分析与数字支付相关的风险，确定针对数字支付的适当政策。12 月 7 日，美国财政部长史蒂文·姆努钦与来自加拿大、法国、德国、意大利、日本、英国、欧盟委员会的财政部长和央行行长以及欧元区的财长们主持了一场虚拟讨论会。根据会议声明，与会者谈到了应对加密货币和其他数字资产不断变化的环境，以及政府为防止其用于非法目的所做的努力。“整个 G7 都强烈支持对数字货币进行监管的必要性”，声明称，部长和行长们还讨论了正在进行的国内和国际经济应对措施，以及实现整个全球经济强劲复苏的战略。

30 家机构入选英国 FCA 数字沙盒计划

2020 年 5 月，英国金融行为管理局（FCA）与伦敦金融城联合启动了“数字沙盒”计划，帮助初创企业应对新冠疫情带来的重重挑战。2020 年 11 月 23 日，FCA 发布公告称，计划共收到 94 份申请，最终 30 家机构成功入选。这些入选的机构中，有 8 家专门从事中小企业贷款服务，通过大数据分析、开放银行、区块链、人工智能等技术加速中小企业贷款审批，另有 22 家机构从事反欺诈、财务脆弱性等问题的研究。据悉，这项实验计划将一直持续到 2021 年 2 月 5 日。

德国政府出台新法案，允许区块链电子证券合法化

12 月 17 日，德国政府内阁通过了新的立法，允许使用区块链技术记录所有电子证券。德

国财政部表示，默克尔内阁于本周三通过了引入全电子证券的新立法，这是其更广泛的区块链战略的一部分。该法案放宽了此前强制证券发行人和持有人使用纸质凭证证明交易的规定。财政部长 Olaf Scholz 表示：“出于怀旧情绪，纸质证券可能很珍贵，但未来属于电子版本。”他补充说，电子证券降低了成本和管理负担。现在，纸质凭证可以被中央证券托管机构或私营银行的登记簿所取代，而基于区块链技术的加密证券登记簿也是可能实现的。司法部长 Christine Lambrecht 表示，该法案将提供法律清晰度，并增强新技术的潜力。

亚太动态

联合国开发计划署（UNDP）联合新加坡金管局，帮助中小企业数字化转型

12 月 8 日，联合国开发计划署 (UNDP) 全球技术、创新和可持续发展中心与新加坡金融管理局 (MAS) 合作，帮助中小企业利用技术更好地进入全球价值链，为中小企业提供创新的金融和数字工具，帮助它们更好地利用数据，更有效地获得融资解决方案。它还将为包括金融科技在内的中小企业创造新的机会，使它们能在联合国开发计划署全球 170 个办事处的网络中向发展中国家扩张。合作首先汇集来自联合国开发计划署和 MAS 的三个成功项目，即 Cultiv@te、无国界商业组织和 API 交流。中小企业在全球经济中发挥着至关重要的作用，特别是在发展中国家。然而，这些公司在获得融资以支持其增长方面面临重大挑战。据官方新闻稿称，COVID-19 大流行的影响进一步加剧了这一问题。Cultiv@te 是联合国开发计划署的创新农业技术项目，从全球的初创企业和研发团队中寻找新的解决方案。Business sans Borders (BSB) 是 MAS 和 Infocomm 媒体发展管理局联合发起的一项倡议，旨在为贸易发现和数字商业服务连接提供一个开放的全球数字基础设施。API Exchange (APIX) 是一个 mas 支持的跨境、开放创新 API 平台，为金融机构和金融科技提供策划的全球市场。

阿联酋央行增设金融科技办公室，并与沙特阿拉伯央行发布 CBDC 项目报告

11 月 25 日，阿联酋中央银行（Central Bank of the U.A.E，简称 CBUAE）宣布成立金融科技办公室。这个新机构旨在发展阿联酋内部成熟的金融科技生态系统，并推动阿联酋成为地区和全球重要的金融科技中心。该办公室将支持吸引国际和地区金融科技公司，并为所有市场参与者提供合作和创新的平台。阿联酋、沙特阿拉伯央行发布了 CBDC 项目 Aber 试验报告——CBDC 对于跨境支付不仅在技术上可行，而且在架构弹性方面比集中支付系统有了显著改进。该报告提出了下一步的研究和政策措施，包括采用分布式账本技术来提高现有系统的安全性，并扩大未来项

目 Aber 试验的范围。

韩国监管沙盒新增 15 项服务总量达到 135 项

12 月 22 日，韩国金融服务委员会（FSC）宣布，金融科技监管沙盒新增 15 项创新金融服务，自推出以来总量已达 135 个。本次入选的服务项目涉及在线食品订购、个人健康评估与保险订购折扣、基于面部识别的身份认证、基于数字认证系统的非接触式实名认证、在线商业保险订购、小企业团体保险订购、电子商务平台数字礼品卡、信用卡积分奖励等多个方向。

埃及启动 2021 年数字普惠金融计划

1 月 3 日，埃及金融监管局宣布推出“2021 年数字普惠金融计划”，希望借此为无现金支付系统发展、提高金融普惠率提供支持。计划特别强调，希望增强数字支付工具在非银行金融活动，特别是小微企业活动中的使用率。

阿曼央行推出金融科技监管沙盒

12 月 9 日，阿曼央行 (Central Bank of Oman) 宣布推出金融科技监管沙盒计划，为创新金融科技解决方案提供测试环境。本次公布的计划包括申请的资格标准、流程和期望。阿曼央行希望借助这一机制更好地了解金融科技解决方案的收益和风险，增强金融领域竞争力，为消费者提供更高标准的保护措施，加快合规产品走向市场的速度。据介绍，阿曼央行监管沙盒计划的首期将主要针对支付解决方案相关的创新企业。

数字货币写入十四五年规划建议

近期，数字货币的研发进展一直吸引着市场的目光。《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》中明确提出，“稳妥推进数字货币研发”。央行行长易纲 11 月 2 日表示，数字人民币目前可在 4 个试点内，通过“二维码”或“tap and go”运用。试验阶段运作顺畅，有超过 400 万宗交易，对应逾 20 亿元人民币。易纲指出，中国的数字货币仍在起步阶段，需要更完善的法律框架，以及着重透明度的监管要求，未来会与国际央行及监管部门，就框架以及货币稳定性进行讨论。值得一提的是，为健全金融法治顶层设计，支持金融业稳健发展，央行积极推进《中华人民共和国中国人民银行法》修改工作，起草了《中华人民共和国中国人民银行法 (修订草案征求意见稿)》(下称《征求意见稿》)，于 10 月 23 日向社会公开征求意见。《征求意见稿》规定人民币包括实物形式和数字形式，为发行数字货币提供法律依据；防范虚拟货币风险，明确任何单位和个人禁止制作和发售数字代币。

中国人民银行副行长范一飞：加快金融数字化转型步伐

近日，中国人民银行副行长范一飞出席 2020 中国（深圳）金融科技全球峰会并致辞。他表示，金融业要深入贯彻落实十九届五中全会精神，扎实做好金融数字化转型工作。深挖潜能，实现决策管理的数据驱动；开拓创新，加快运营机制的敏捷重塑；与时俱进，聚焦业务模式的智慧再造；多向赋能，推动生态体系的协同共建。同时，金融业要利用科技赋能，加强金融安全体系和能力建设，扎牢织密金融创新。

2021年一季度《交易技术前沿》征稿启事

《交易技术前沿》由上海证券交易所主管，上交所技术公司主办，以季度为单位发刊，主要面向全国证券、期货等相关金融行业的信息技术管理、开发、运维以及科研人员。

2021 年一季度征稿主题如下：

一、云计算

（一）云计算架构

主要包含但不限于：云架构剖析探索，云平台建设经验分享，云计算性能优化研究。

（二）云计算应用

主要包含但不限于：云行业格局与市场发展趋势分析，国内外云应用热点探析，金融行业云应用场景与实践案例。

（三）云计算安全

主要包含但不限于：云系统下的用户隐私、数据安全探索，云安全防护规划、云安全实践，云标准的建设、思考与研究。

二、人工智能

（一）应用技术研究

主要包含但不限于：语音识别与自然语言处理，计算机视觉与生物特征识别，机器学习与神经网络，知识图谱，服务机器人技术。

（二）应用场景研究

主要包含但不限于：智能客服、语音数据挖掘、柜员业务辅助等。

主要包含但不限于：监控预警、员工违规监控、交易安全等。

主要包含但不限于：金融预测、反欺诈、授信、辅助决策、金融产品定价、智能投资顾问等。

主要包含但不限于：金融知识库、风险控制等。

主要包含但不限于：机房巡检机器人、金融网点服务机器人等。

三、数据中心

（一）数据中心的迁移

主要包含但不限于：展示数据中心的接入模式和网络规划方案；评估数据中心技术合规性认证的必要性；分析数据中心迁移过程中的影响和业务连续性；探讨数据中心迁移的实施策略和步骤。

（二）数据中心的运营

主要包含但不限于：注重服务，实行垂直拓展模式；注重客户流量，实行水平整合模式；探寻数据中心运营过程中降低成本和提高服务质量的途径。

四、分布式账本技术（DLT）

（一）主流分布式账本技术的对比

主要包含但不限于：技术架构、数据架构、应用架构和业务架构等。

（二）技术实现方式

主要包含但不限于：云计算 + 分布式账本技术、大数据 + 分布式账本技术、人工智能 + 分布式账本技术、物联网 + 分布式账本技术等。

（三）应用场景和案例

主要包含但不限于：结算区块链、信用证区块链、票据区块链等。

（四）安全要求和性能提升

主要探索国密码算法在分布式账本中的应用，以及定制化的硬件对分布式账本技术性能提升的作用等。

五、信息安全与 IT 治理

（一）网络安全

主要包括但不限于：网络边界安全的防护、APT 攻击的检测防护、云安全生态的构建、云平台的架构及网络安全管理等。

（二）移动安全

主要包括但不限于：移动安全管理、移动互联网接入的安全风险、防护措施等。

（三）数据安全

主要包括但不限于：数据的分类分级建议、敏感数据的管控、数据共享的风险把控、数据访问授权的思考等。

（四）IT 治理与风险管理

主要包括但不限于：安全技术联动机制、自主的风险管理体系、贯穿开发全生命周期的安全管控、安全审计的流程优化等。

六、交易与结算相关

（一）交易和结算机制

主要包含但不限于：交易公平机制、交易撮合机制、量化交易、高频交易、高效结算、国外典型交易机制等。

（二）交易和结算系统

主要包含但不限于：撮合交易算法、内存撮合、双活系统、内存状态机、系统架构、基于新技术的结算系统等。

投稿说明

1、本刊采用电子投稿方式，投稿采用 word 文件格式（格式详见附件），请通过投稿信箱 ftt.editor@sse.com.cn 进行投稿，收到稿件后我们将邮箱回复确认函。

2、稿件字数以 4000-6000 字左右为宜，务求论点明确、数据可靠、图表标注清晰。

3、本期投稿截止日期：2021 年 3 月 31 日。

4、投稿联系方式 021-68607128，021-68607131 欢迎金融行业的监管人员、科研人员及技术工作者投稿。稿件一经录用发表，将酌致稿酬。

《交易技术前沿》编辑部

证券信息技术研究发展中心（上海）

附件：投稿格式

标题：（黑体 二号 加粗）
作者信息：（姓名、工作单位、邮箱）（仿宋 GB2312 小四）
摘要：（仿宋 GB2312 小三 加粗）

一、概述（仿宋 GB2312 小三 加粗）
二、一级标题（仿宋 GB2312 小三 加粗）
（一）二级标题（仿宋 GB2312 四号 加粗）
1、三级标题（仿宋 GB2312 小四 加粗）
（1）四级标题（仿宋 GB2312 小四）
正文内容（仿宋 GB2312 小四）
图：（标注图 X. 仿宋 GB2312 小四）
正文内容（仿宋 GB2312 小四）
表：（标注表 X. 仿宋 GB2312 小四）
正文内容（仿宋 GB2312 小四）
三、结论 / 总结（仿宋 GB2312 小三 加粗）

杂志订阅与反馈

各位读者，如您想订阅《交易技术前沿》纸质版，欢迎扫描右侧二维码填写问卷进行订阅，同时可以向我们提出关于《交易技术前沿》的建议与意见反馈。如您希望赏阅电子版，欢迎访问我们的电子平台 http://www.sse.com.cn/services/tradingservice/tradingtech/sh/transaction/（或扫描封面尾页二维码）。我们的电子平台不仅同步更新当期的文章，同时还提供往期所有历史发表文章的浏览与查阅，欢迎关注！

扫描在线浏览

联系电话：021-68828590
021-68813289
投稿邮箱：ftt.editor@see.com.cn

ITRDC
证券信息技术研究发展中心（上海）
上海证券交易所 SHANGHAI STOCK EXCHANGE TECH 上交所技术
中国上海浦东南路528号
邮编：200120
公众咨询服务热线：4008888400
网址：http://www.sse.com.cn