

THE FORELAND OF
TRADING TECHNOLOGY

交易技术前沿

2018年 第四期 总第33期

本期主题

数字化实践

No.4



上海证券交易所
SHANGHAI STOCK EXCHANGE

ITRDC
证券信息技术研发中心 (上海)

内刊 2018 年第四期 (总第 33 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、蒋凯、陈治纲、唐忆
责任编辑 :
黄俊杰、朱立、徐丹、孙增、陆伟

上海市浦东南路 528 号
邮编 : 200120
电话 : 021-68813289 021-68800293
投稿邮箱 : ftt.editor@sse.com.cn



扫描在线浏览

篇首语

在信息革命、移动互联网革命正深刻改变世界的今天，智能革命的大潮已汹涌而来，伴随着数据化、网络化和智能化实践的深入推进，数字世界、智能城市、数字身份等从概念变为现实。本期《交易技术前沿》聚焦“数字化实践”主题，从数字化发展和转型的核心价值，监管和创新的内在平衡，探索以技术引领推动行业健康蓬勃发展的路径。

其中，《科技赋能 重塑价值 论数字化转型的探索实践》分析了对数字化发展阶段的理解，并介绍了上交所技术的数字化转型战略与实践，阐述了赋能行业的价值观体现。《交易系统低延时测试与分析》通过对交易系统的延时测试，再次强调“低时延技术”成为各大交易所竞争的核心，同时提供具备普适性的延时度量方案。《基金行业数据安全保障体系建设探析》关注不容忽视且越来越重要的问题：数据安全；结合当前基金行业的业务和数据特点，就如何保障数据安全性展开分析。《基于开源架构的任务调度系统在证券数据处理中的探索和实践》利用跨平台、支持多种部署模式的任务调度系统，应对批处理时间窗口逐步缩小带来的挑战。《人工智能+知识图谱：如何规整海量金融大数据？》一文指出多元异构数据的整合，是未来金融机构将要长期面临的一个局面，提出面向人工智能的大数据治理步骤，试图打破存在的信息孤岛。

我们可以预见，未来行业数字化转型的成果，将以“算法+数据”的形式呈现，监管机构、经营机构以及行业各类参与者均从中受益，形成监管科技和业务创新协调共赢、融合互动的良好发展局面。

《交易技术前沿》编辑部

2019年1月3日

目录 Contents

本期热点 Focus

- | | |
|---|----|
| 1 科技赋能 重塑价值 论数字化转型的探索实践 / 王泊 | 2 |
| 2 交易系统低延时测试与分析 / 魏畅 陈冬严 张鸿晔 | 6 |
| 3 低时延网络构建 / 何志东 余鹏飞 | 14 |
| 4 基于开源架构的任务调度系统在证券数据处理中的探索和实践 / 蔡丰令 樊玮 张培乐 田肖 杜小静 | 21 |
| 5 基于改进卷积神经网络在商品指数预测中的应用研究 / 崔闯 胡天华 钟利明 | 30 |

实践探索 Explore

- | | |
|---------------------------------------|----|
| 6 容器云在华泰证券的探索与实践 / 管文琦 朱凯 | 43 |
| 7 海通证券金融云思考与实践（下） / 王洪涛 王朝阳 纪飞 魏勇 张真真 | 49 |
| 8 金融科技在国内外券商 PB 业务中创新实践与思考 / 邓维 | 57 |
| 9 基于证券业信息安全等级保护的应用系统安全实践 / 晏强 杨超 王磊 | 67 |
| 10 基金行业数据安全保障体系建设探析 / 宋晓刚 朱林 杨志明 | 75 |

行业观察 Observation

- | | |
|---|-----|
| 11 券商业务规则体系统一建设的实现与探讨 / 潘聪 刘丽 | 83 |
| 12 智能化多模金融数据质量监控平台实现路径 / 覃剑钊 刘佳茜 张汉林、蒋荣 | 89 |
| 13 基于区块链技术构建可信仓单系统的研究 / 李博 潘文锋 | 99 |
| 14 美式期权价格计算的 FPGA 实现 / 刘超凡 王卓 邹经纬 马辉 钟浪辉 陈敏 | 106 |
| 15 人工智能 + 知识图谱：如何规整海量金融大数据？ / 齐伟 | 113 |
| 16 如何打造健壮的分分布式系统 / 唐刘 | 118 |

资讯采撷 Information

- | | |
|-------------------------------------|-----|
| 17 “聚智赋能，携手共赢” 2018 上交所技术行业用户大会成功举办 | 125 |
| 18 监管科技全球追踪 | 127 |



F 本期热点 ocus

- 1 科技赋能 重塑价值 论数字化转型的探索实践
- 2 交易系统低延时测试与分析
- 3 低时延网络构建
- 4 基于开源架构的任务调度系统在证券数据处理中的探索和实践
- 5 基于改进卷积神经网络在商品指数预测中的应用研究

科技赋能 重塑价值 论数字化转型的探索实践

王泊 / 上交所技术有限责任公司 总经理兼首席技术官



当前，全球都处在数字化发展的重要时期，各个行业都在加速数字化转型。2018年11月乌镇举办了全球互联网大会，可以发现，这几年互联网关注的主题，从首届提出的“命运共同体”到“互联互通 共享共治”，再到“发展数字经济，促进开放共享”，直到今年的“创造互信共治的数字世界”。数字化被赋予了越来越多的含义。传统经济正在向数字经济转型，从统计数据看，去年我国数字经济对经济增长的贡献率为55%，接近甚至超越了某些发达国家水平，可见数字化已经成为带动经济增长的核心动力。数字化和数字经济已日益成为国家谋求竞争优势的制高点，

同时科技和实体经济的深度融合，也为资本市场发展带来新的空间。

1 对于数字化发展阶段的理解

资本市场天然就具有数字的属性，正如上交所第一任总经理尉文渊在《改革开放40年》的访谈中所提到：“上交所从开业的第一笔交易开始就跨入了电子交易时代，这对中国证券市场的发展产生了深远的影响。可以说，没有电子交易的技术基础，中国证券市场不可能以这样快的速度扩张，也无法支持现在遍及全国城乡、数

千万投资人参与、每天几千亿的成交规模。”例如上交所现有的这一代交易系统，在 2009 年上线的一周内，峰值交易笔数就已超过 13 万笔每秒。也就是说，每天开盘对于交易所来说都是一个双 11。

同样全球信息技术也在日新月异地发展与进步，从最早把模拟信号转变为数字信号，就是一个技术上的突破。到现在，Facebook 用户每天会上传 20 亿张图片，特斯拉为了实现全自动驾驶收集了超过 20 亿公里的驾驶数据信息。正是因为信息技术的发展，才使我们可以触及以往所无法探知的信息广度与深度。因此，数字化发展的第一个阶段，就是“信息的数据化展现”，即信息以电子形式的流转与呈现。我们通过把周围产生的数据、想要做的事、想表达的逻辑，变成计算机能处理的 0 和 1，实现数据的采集、传输、存储与展示，才能为后续的分析处理、交互反馈提供资源基础与可能性。

而数字化发展的第二个阶段，可以理解为“数据的智能化分析”，即通过分析创造数据价值，让数据真正活起来。这个阶段主要以大数据、人工智能的落地应用为主线，具体来说可以分为三个发展层次：第一层次首先是对数据的简单统计分析，这也是信息数字化后最直观的体现，我们可以将其理解为一维的；第二层次是在数据分析基础上的预测预判，涉及到数据的整合、算法的运用，这相当于在第一层次基础上提升了一维；第三层次进入到数据的智能化分析，通过大数据处理及人工智能技术挖掘数据的内在价值并做出智能反馈，应用服务于实际场景，这属于高阶多维的数据能力体现。在不断升维的过程中，我们开始逐步探索数据如何对业务产生影响。

因此数字化的第三个阶段，就是“业务的数字化驱动”，即通过打通不同层级的数据壁垒，实现对业务变革、流程更新的快速响应与处理，从而提高业务与服务整体运营效率。这一过程

中，一方面应当注重并支持业务模式的探索与创新。另一方面，需要真正去思考如何让技术赋能，如何通过平台化、规模化、公共化的发展趋势输出技术能力，同步提升算力、算法和数据，推进技术与业务的深度融合，使技术起到引领业务变革的作用。

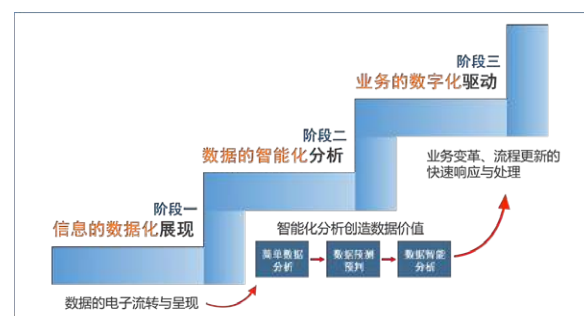


图 1: 数字化发展的三个阶段

这三个发展阶段，其实相当于数字化发展成熟度的一个渐进过程。在数字化转型实践的路径中，首先通过扩展数据来源、优化展现形式，可以使认知范围变得更广；其次通过充实智能分析能力、挖掘数据价值，可以使发展思路变得更加清晰；最后通过整合提升效能、优化业务流程，可以使变革与行动变得更为迅速。这就如同人的双眼、大脑和四肢，三者缺一不可，相互配合协调，才能快速奔跑。

2 上交所技术关于数字化转型的战略规划

数字化转型的实现需要有清晰的顶层设计，才能使得定位准确、执行高效。而制定战略规划时，首先需要明确规划的目标。对于上交所而言，应当履行优化金融监管，提高市场效率的职责，同时也要强化推动自身以及行业技术力量的构建。结合自身实际发展现状，上交所技术提出了五大重点战略，其中前四项都是实实在在为推动行业基础设施与服务完善而展开，主要包括：行业基础设施资源提供、交易系统升级改造、智能监管体系打造以及行业移动互

联推进。而最终的目的，就是推动数字化技术引领业务发展。

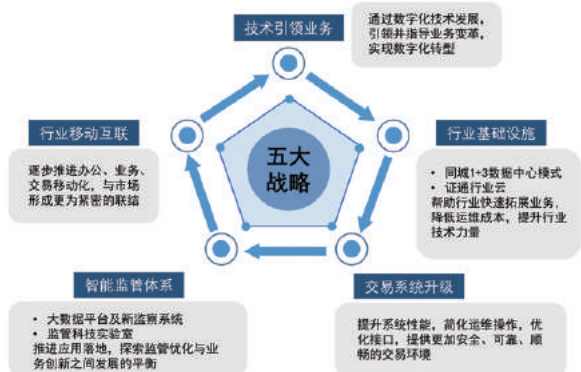


图 2: 上交所战略科技发展规划五大战略

2.1 提供完备的行业基础设施与服务

未来随着金桥数据中心的落成，上交所在上海将围绕金融交易广场，形成陆家嘴、外高桥和金桥的同城 1+3 数据中心模式，并在深圳建立异地灾备中心。金桥数据中心是一个 T3+ 等级的数据中心，通过集约化的管理，可以帮助行业快速拓展业务，降低运维成本，提升行业技术能力。同时，通过启动“证通”行业云，能够更有效为行业用户提供安全、合规、高效的云服务，充分提升数据中心资源利用率，有效降低全行业成本。

2.2 完善交易系统改造升级

目前全球范围内，交易系统都在日新月异地提升和发展中。证券行业有其一定的特殊性，因为证券交易的性能处理是通过两层结构实现的，第一层由终端用户联接行业机构券商，第二层由证券机构联接交易所。也可以说，我们是集聚整个行业的力量一起来提供高效、顺畅的交易服务。通过自主轻型化改造无缝衔接现有交易系统，不仅能让系统性能达到一个新的高度，同时能够使得运维操作更加自动、高效和便捷，接口更加优化，从而为全行业各类型证券的交易过程提供更加安全、可靠、顺畅的环境。

2.3 打造智能化监管体系

在持续完善大数据平台和监察系统的基础上，上交所也正在探索打造智能一体化的监管平台，以画像、舆情、市场波动分析、机器学习平台等为切入点，逐步推进监管领域的应用落地。目前大数据平台已经完全承接了数据仓库的职责，并已正式上线运行，其上的智能监管应用服务业正在逐步落地中。而另一方面，上交所依托证券信息技术研究发展中心（上海）的行业平台，组建了监管科技、低时延技术等不同方向的实验室，组织开展前沿研究，鼓励技术、业务的应用以及监管的创新，力求去探索优化监管与业务创新之间发展的平衡。

2.4 推进行业移动互联

根据最新的调研数据显示，券商线上开户比例绝大部分已超过九成。可以说目前的移动互联，已经不仅仅是移动通信和互联网二者简单的技术结合，而是移动技术、平台、商业模式以及应用的有机结合与深度融合。到今天，全球已经有了超过 50 亿的在网移动终端设备。未来随着 5G 技术发展、物联网时代的到来，全世界的联网设备数量将超过百亿，移动化的发展趋势必将爆发更大能量。移动设备的高便捷性，可以让用户在碎片化时间随意操作，处理日常办公、业务、甚至交易。而通过互联网移动化服务的推进，交易所可以和机构及市场之间形成更为紧密的联结。

2.5 推动技术引领业务发展

通过前四点的开展手段，最终的目标是希望通过技术发展引领业务，从而形成对我们整个资本市场的数字化业务改造，实现行业真正的数字化转型。目前其实行业整体对技术的重视程度可能还不够，或者说还不是特别理解技术所能带来的价值，而更多的把科技作为后台，或是作为服务支撑的部门。实际上我们仅仅拥有技术可能并不够，科技只有实现了商业化，才能改变未来，才能体现 IT 的价值。印证这个说法的一个很好的例子，就是著名的亚马逊公司。现在我们的概

念里都认为亚马逊是一个科技企业，但是当初亚马逊刚开始在美国上市的时候，只是一个在互联网上卖书的平台。但是其通过海量的数据积累与自动化算法的探索，优化并实施执行运营任务，将每日政策制定、运营管理、甚至长期战略决策等若干行动领域整合在一起，形成了以技术为驱动力的业务模式转型创新。可以说，通过技术的正确运用，引领并指导业务变革，才可以在资本市场的支持下不断发展壮大，成为真正的科技创新企业。

3 关于赋能行业的价值体现

从基础设施的不断完善、业务场景的不断丰富，从技术创新到数据治理，数字基因对于金融领域的影响是在对其做质的改变。而数字化转型发展中一个重要的价值体现，在于数字的平台化和服务化，即对数字价值的挖掘以及如何将其通过平台或服务输出将是未来竞争力的关键。可以想象，新技术的发展将重新定义业务形态，智能系统将成为新的核心竞争力，通过智能服务、智能营销等手段可以增强与用户的交互与沟通质量，继而推进产品转型升级，金融服务可以变得更个性化。



图 3: 上交所技术核心价值观

同样，上交所技术在寻求探索数字化转型发展之路的同时，也在重新思考着自身的价值定位。首先，从用户角度来定义，我们秉承的是以用户为中心的理念，用户是我们核心价值创造的根源，我们需要快速响应并满足用户需求。证券

交易的系统结构是由交易所与行业机构共同组成的。因此第一步最核心是要服务好交易所，而后通过交易所服务市场机构，进而服务整个资本市场。

其次，从商业模式角度来定义，我们是以赋能行业为目标。通过提高市场的运营效率，降低整个行业成本，甚至形成对行业的反哺作用，这是我们想得到的真正的价值收益。通过不同角度的携手合作方式，比如与互联网 IT 企业合作提供行业基础设施、与行业的头部机构合作共建平台服务实现技术输出等，通过多样化的合作形式，不仅可以辐射整个行业，服务好长尾客户，更能输出平台能力，提升行业技术水平。

最后，作为技术公司，对技术先进性的追求与自主掌控始终是立身之本。对于交易低延时技术、行业云、移动化、监管科技等方面，仍然需要集中力量开展研究攻关。同时，对于 IT 投入的重视程度，也体现在人才队伍与价值观念中。以高盛为例，目前其员工比例的三分之一是拥有 IT 背景的专业人才。上交所目前 IT 人员的比例是将近四分之一，并且 IT 团队规模仍在增长中。在资本市场及金融证券行业的特定领域内，很多时候我们的对比是局限的。如果放眼到行业外、甚至到全世界的范围下，其实能够感觉到我们距离互联网行业、距离国际一流水平的大型投行，尚还有一定的差距。所以这也要求我们重视技术的作用，通过技术的发展引领实现业务的提升，充分发挥数字化的价值。

数字化转型不仅需要仰望天空，制定前瞻性的目标，也更需要脚踏实地，一步一个脚印去实践与试错。科技创新就好比是一粒种子，市场是创新成长的土壤。良好的运行机制以及我们对待创新的正确态度，是刺激创新成长的最好环境。资本市场的健康发展，需要整个行业一起来携手共建。

交易系统低延时测试与分析

魏畅 陈冬严 张鸿晔 / 证券期货行业测试中心 (中金所)



摘要：订单延时 (Latency) 是衡量交易系统性能的重要指标。本文利用交换机端口流量镜像功能 (Port Mirroring) 和低延时交换机产生的纳秒级时间戳，实现了高精度的交易系统逐笔订单延时测量。通过分析逐笔订单延时数据，验证了交易系统性能微笑曲线，获得了交易系统的最佳表现区间（舒适区），同时也对比了逐笔订单延时与现有日志采样方案的优势。

关键词：低延时交换机；时间戳；交易系统；逐笔订单延时

1 前言

证券期货交易系统具有交易时间相对集中、交易指令和数据密集的特点，对交易系统处理速度具有很高的要求^[1]。近年来，全球各大交易所都在不断对交易系统升级改造，其中“低延时”成为各大交易所竞争的核心^[2]。几所典型国外交易所交易系统性能数据如表 1^[3]所示，可见交易系统延时竞争已经进入微秒量级。目前，国内交易所交易系统延时性能与国外顶级交易系统还存在一定的差距，需要进一步加大投入进行研发、建设。在建设“低延时”交易系统过程中，也就必然少不了对交易系统“低延时”性能的测试。

2 方案介绍

交易系统延时有多种维度定义，参照 Cinobber 公司白皮书^[4]，定义端到端（End-to-end）、门到门（Door-to-door）、撮合器（Business logic）三个延时指标，参见图 1。对于交易所，重点关注的是门到门（Door-to-door）延时指标，以及整个门到门链路上的分段延时指标，分段延时指标不是本文讨论的重点，故不做具体讲解、分析。后文涉及的交易延时指标，如果不作具体说明，都是指门到门（Door-to-door）延时指标。交易延时指报单进入交易前置，经交易系统处理，返回交易系统接入点的总时长。交易延时反映了

交易系统处理报单的速度，延时越小，订单处理越快，性能越好。

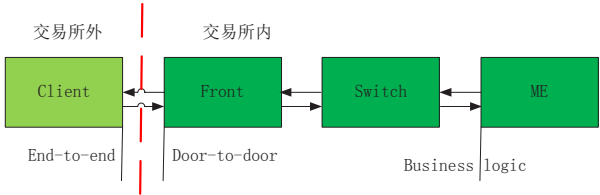


图 1 延时指标定义图

目前市场针对系统延时度量与分析方法众多，如图 2 所示，主要分为软件时间打戳和硬件时间打戳两大类。

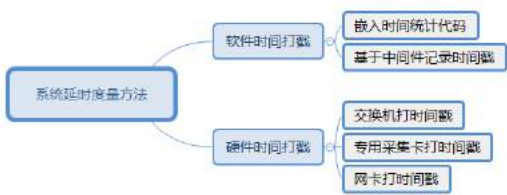


图 2 系统延时度量方法分类

2.1 软件时间打戳，

软件时间打戳通常采用嵌入式时间统计代码或者基于 Weblogic 等中间件记录时间戳。该方案实施简单，缺点也很明显，比如精度差，会增加系统负担从而增加系统延时波动幅度等。目前，很多交易所通过在交易系统中直接加入探针，对交易指令进行采样计算延时，通过系统日志输出，从而得到订单延时。但是，通过该方法获得延时

表 1 典型国外交易所交易系统

交易所	新一代交易系统	性能	时间
纳斯达克市场	Genium INET	小于40 微秒，1 百万笔订单/ 秒	2010 年10 月
德国交易集团T7 衍生品交易平台	T7	延迟220 微秒，	2012 年2 月
BATS 交易所	BATS 交易系统	82 微秒，55 万笔订单/ 秒	2013 年
纽约证券交易所	UTP	375 微秒，32 万笔订单/ 秒	2013 年6 月
伦敦证券交易所	Turquoise	100 微秒	2010 年10 月
港交所	AMS/3.8	2 毫秒，15 万笔订单/ 秒	2011 年12 月
东交所	Arrowhead	1 毫秒	2011 年11 月

存在一些问题，比如：时间戳取自服务器，导致精度无法满足测量需求；只能获得少量采样订单延时，具有一定的偶然性，不能完全反映采样周期内全部订单延时性能。因此，无法满足交易系统“低延时”性能测试的需求。

2.2 硬件时间戳，

硬件时间戳顾名思义是利用硬件打时间戳，目前主流网络流量采集、打时间戳和分析的解决方案有三种：交换机打时间戳、专用采集卡打时间戳、网卡打时间戳。

2.2.1 交换机打时间戳

交换机打时间戳方法是在网络包通过交换机时采用 SPAN 技术（交换机端口镜像方法）将网络包实时异步镜像至可以打精准时间戳的交换机，然后将带有时间戳的网络数据转发给分析服务器，网络拓扑图如图 3 所示。该方案优点是部署简单、灵活，对现有拓扑结构和系统环境影响小^[5]；缺点是成本高，需要特定低延时交换机支持，比如 Cisco Nexus 3548 交换机就是典型的带硬件时间戳的低延时交换机。

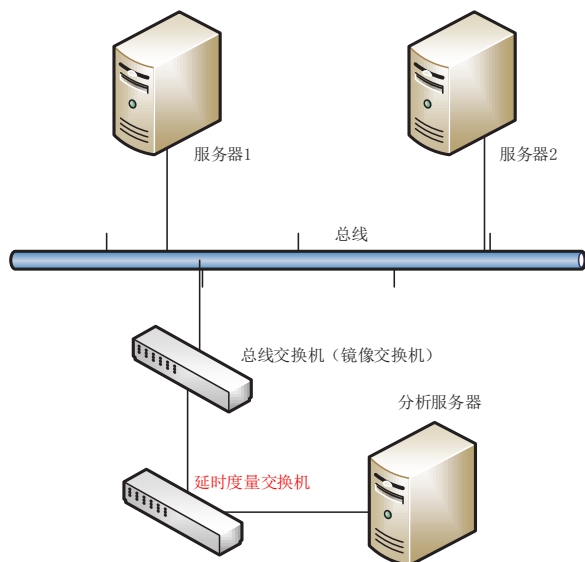


图 3 交换机打时间戳拓扑图

2.2.2 专用采集卡打时间戳

专用采集卡打时间戳方法直接将专用网络采

集卡部署在分析服务器上，交换机将网络包镜像至采集卡后，由采集卡完成打时间戳和解包分析等工作，网络拓扑图如图 4 所示。该方案的优点是部署简单，可容纳吞吐量大，能够实时分析和观测；其缺点是需要绑定厂商的采集卡，通用性不强，扩展性较差，受到厂商限制^[5]。

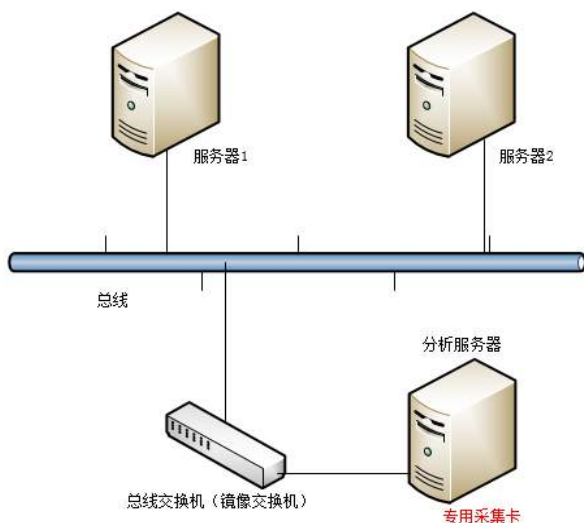


图 4 专用采集卡打时间戳拓扑图

2.2.3 网卡打时间戳

该方案使用专用网卡打时间戳并旁路路由至分析服务器，网络拓扑图如图 5 所示。优点在于更精确的应用延时分析（除去了网络延时），但是也存在每台主机必须部署专用网卡、多网卡间需 PTP 精确对时等问题^[5]。

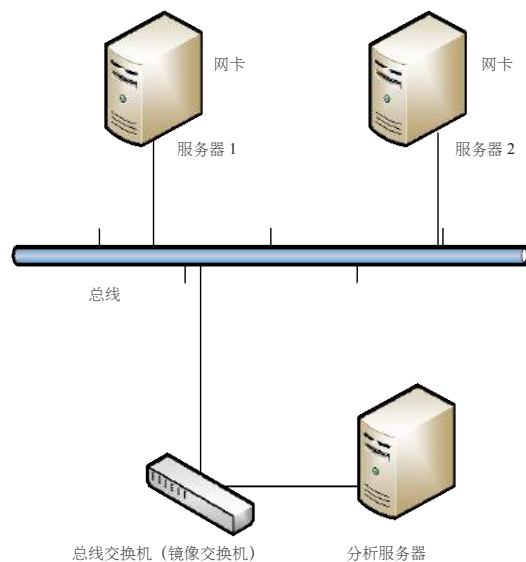


图 5 网卡打时间戳拓扑图

表 2 延时度量方法比较

时间打戳方案	优点	缺点
软件时间打戳	实施简单、成本低	精度低、抖动大、对系统有一定的影响
交换件打时间戳	部署简单、灵活、精度高、对系统无影响	成本高、需要特定交换机
专用采集卡打时间戳	精度高、吞吐量、对系统无影响	可扩展性较差，受厂商限制
网卡打时间戳	精度高、对系统无影响	部署复杂、需要PTP精确对时

综上所述，几种延时度量方法优缺点比较，参见表 2。

我司对项目需求进行详细分析，包括拟度量的网络和业务时间段，度量所需的技术和难度，对现有系统的影响大小，项目成本，以及项目后续可能存在的需求，结合上述方案的比较，最终选择了交换机打戳的方案。该方案结合我们的应用场景，有如下优点：

- 1) 高精度，如采用超低延时交换机，精度可提高 1-2 个数量级；
- 2) 逐笔测量，而现有监控系统 / 性能测试的结果采集采用日志采样方式获取；
- 3) 旁路测量，对交易系统无侵入；
- 4) 通过订单的关联，可以实现前置以及撮合核心的分段延时统计。

3 方案实施

通过上节的对比，本次交易系统低延时测试最终确定为交换机打戳方案。

3.1 部署架构

网络拓扑图如图 6 所示，客户端为压力服务器，用其进行报单发压力；交易前置是外界连接交易的“窗口”，客户端通过交易前置连接交易系统；交易核心是交易系统最重要的部分，用来处理客户订单；交易总线交换机是一台万兆交换

机，负责客户端、交易前置以及交易核心三台服务器之间的数据交换；延时度量交换机选择的是 Cisco Nexus 3548，将交易总线交换机镜像过来的数据打上高精度时间戳，然后分发给分析服务器；通过分析服务器上的应用程序对数据进行解析、处理，实现订单的逐笔追踪以及各个节点的延时度量。

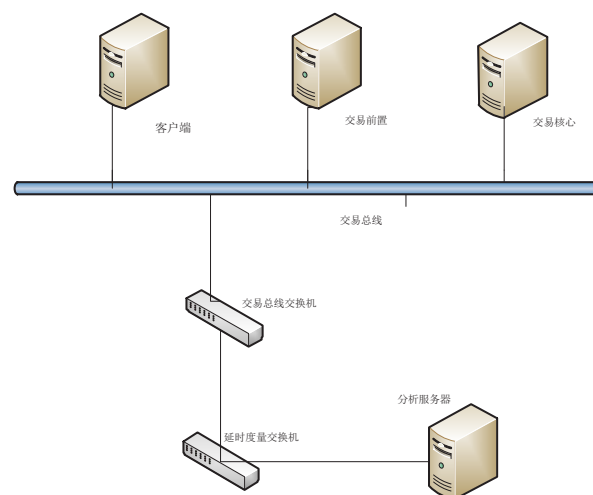


图 6 交易系统低延时测试网络拓扑图

客户端、交易前置、交易核心以及分析服务器四台服务器硬件配置，参见表 3。

3.2 数据流向

订单数据流如图 7 所示，客户端、交易前置以及交易核心通过交易总线传输交易数据。

- 1) 客户端申报订单首先进入交易前置，再到交易核心，交易核心处理完毕后，再将订单的

表 3 服务器硬件配置

主机	型号	操作系统	内存	Cpu 主频	Cpu 数量	Cpu 型号
客户端	DELL R730	RHE6.3	128G DDR3	3.5G	24	Intel Xeon E5-2643 v2
交易前置	DELL R730	RHE6.3	128G DDR3	3.5G	24	Intel Xeon E5-2643 v2
交易核心	DELL R730	RHE6.3	128G DDR3	3.5G	24	Intel Xeon E5-2643 v2
分析服务器	DELL R730	RHE6.3	128G DDR3	3.5G	24	Intel Xeon E5-2643 v2

处理结果信息发送至前置。

2) 部署的另外一台延时度量交换机，它将交易总线上的交易数据打上精准时间戳，然后转发至分析服务器上。

3) 分析服务器上部署了用于解析交易数据包的应用程序，从而实现订单的逐笔追踪以及各个节点的延时度量。

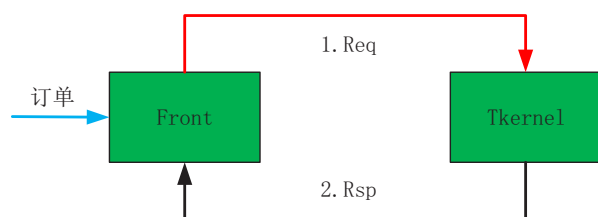


图 7 订单数据流

4 测试案例与结果分析

本节共进行两个案例的测试与分析：1) 寻找交易系统最佳表现区间；2) 对比采样方式和逐笔方式的结果差异。本文数据都已做了脱敏处理，不代表真实结果。

4.1 最佳表现区间

交易系统存在一个舒适区，即延时最佳表现是一个区间。当报单速率从小到大递增的过程中，交易系统由冷变热，由热变烫，交易系统的延时也由大变小，再由小变大。

测试方法：用报单工具在某一合约下以同一价格重复报“买卖开平”单，所有订单均被成交，且价格无变化。报单速率从 1 笔/秒逐步上升至 20k 笔/秒，逐笔延时数据采用稳定报单后 60 秒的报单数据。

根据获取的不同报单速度下的延时数据，绘制相应速度下的交易系统延时帕累托图，如图 8、图 9 所示。根据图 8、图 9 可以看出，在测试环境下，交易系统延时最佳表现在 1k 笔/秒的报单速率下。

根据获取的不同报单速率下的延时数据，绘制各报单速率下的交易系统延时分位图，如图 10。从图 10 中可以看出，在测试环境下，交易系统的最佳表现区间如表 4 所示。从表 4 中可知，报单速度在 100 笔/秒~3k 笔/秒时，符合三种分位数要求，表现最优。

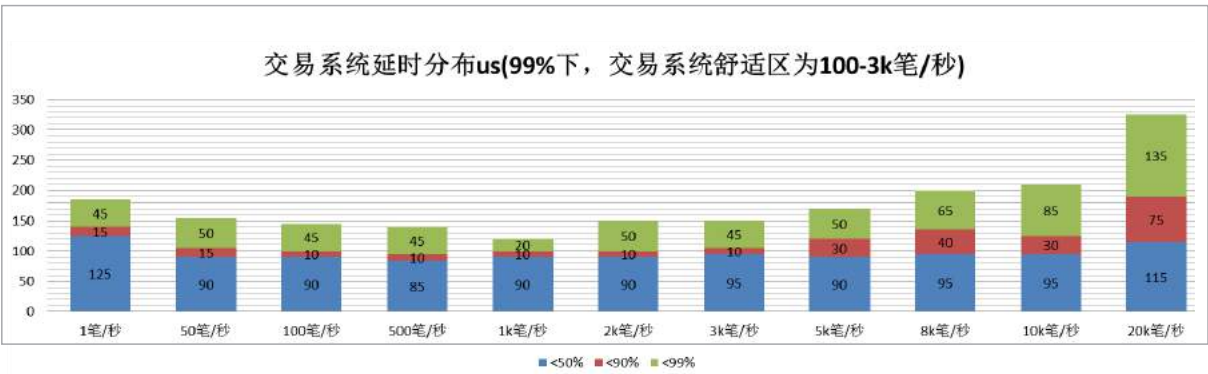
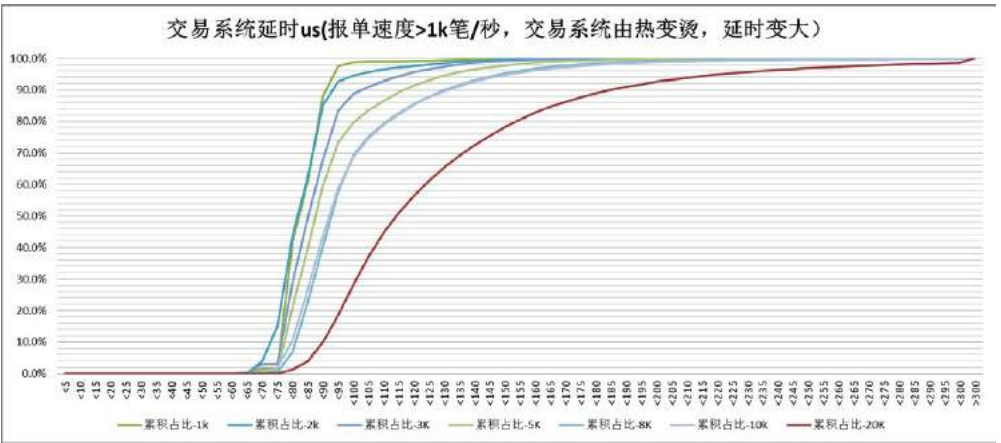
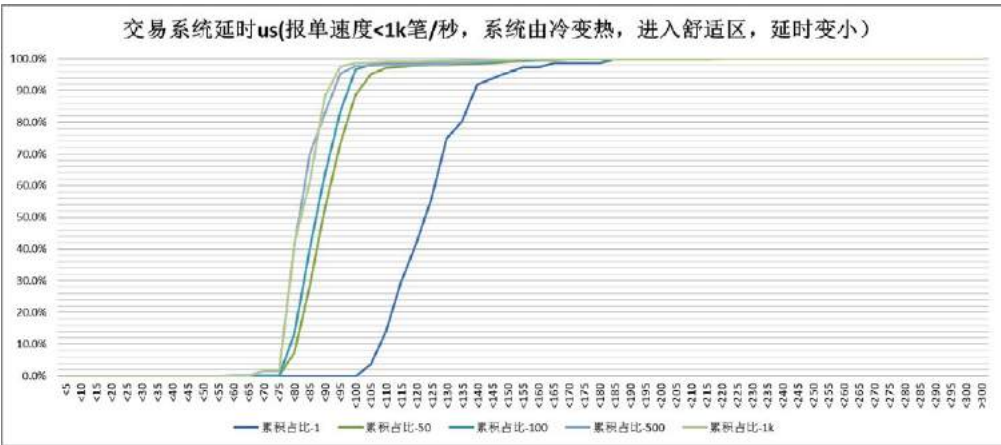
表 4 交易系统最佳表现区间

分位	分位数	最佳表现区间
50	95us 以下	50 笔/秒-10k 笔/秒
90	105us 以下	50 笔/秒-3k 笔/秒
99	150us 以下	100 笔/秒-3k 笔/秒

4.2 与采样方式对比

采样方式获取延时存在问题，但以往都是从定性方面来分析，本案例将从定量方面来比较采样方式和逐笔方式的结果差异，证明采样方式的局限性。

测试方法：用报单工具在某一合约下以同一



价格重复报“买卖开平”单，所有订单均被成交，且价格无变化。报单速率保持在 10k 笔 / 秒，逐笔延时数据采用稳定报单后 60 秒的报单数据；采样数据选取该段时间对应的 Syslog 里面的延时数据。

根据获取的逐笔延时数据和采样数据，绘制

相应交易系统延时帕累托图，如图 11。根据图 11 可以看出，测试环境中，在 10K 笔 / 秒报单速度下，通过 Syslog 获取到的采样数据显著比逐笔的数据要小，特别是延时小于 100us 时，延时越大，差距越大，表示采样数据失真度越大。

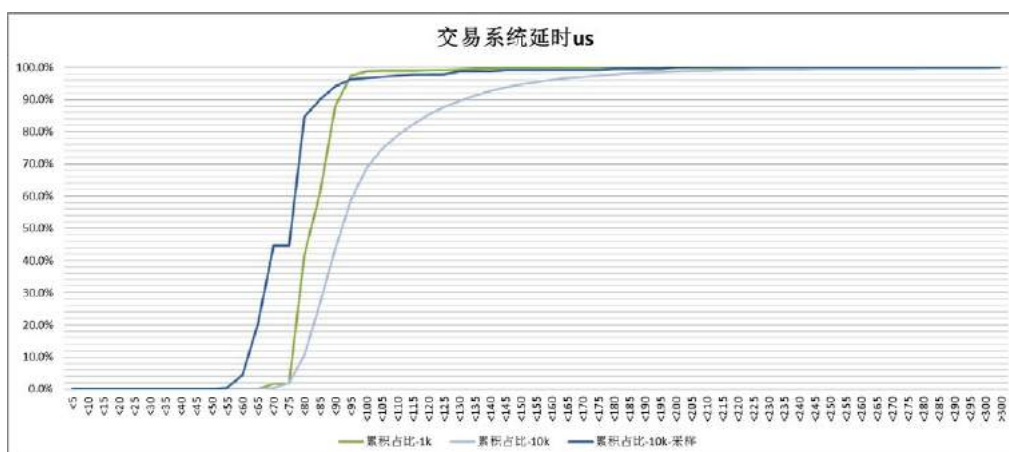


图 11 交易系统延时帕累托图

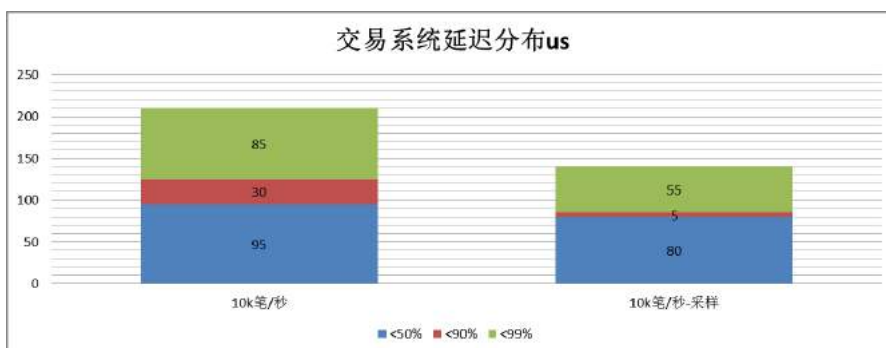


图 12 交易系统延时分布分位图

表 5 延时数据占比

延时 (us)	累计占比-10k	累计占比-10k-采样
<200	98.74%	1
<210	99%	1

根据获取的逐笔延时数据和采样数据，绘制相应交易前置延时分布分位图，如图 12。根据图 12 可以看出，50 分位下，Syslog 采样数据比逐笔数据小 10us；99 分位下的数据要小 55us。

根据获取的逐笔延时数据和采样数据，统计分析得到小于 200us 和小于 210us 的数据占比如表 5 所示。从表中可以看出，通过采样方式获取到毛刺数据不全，在 10K 笔/秒报单速率下，采样得到的最大延时在 200us 以内，遗漏了 1% 左

右的大于 200us 的订单。

4.3 结论

根据前面两个案例，可以得到以下三点结论：

- 1) 交易系统存在一个最佳报单速率，此速率下系统延时状况最佳；
- 2) 根据对交易系统不同的延时要求，存在不同最佳表现区间，要求越严格，最佳表现区间范围越小；

3) 采样数据和逐笔数据对比, 存在失真的情况, 因此只能用来粗略了解系统运行状况; 想要全面掌握系统运行状态, 需要通过逐笔数据来观测。

5 展望

本文在多种延时度量方案中选择了一种相对

较好的方案, 针对交易系统进行了两个案例的低延时测试, 获得了一些测试结果。虽然该项工作是围绕交易系统进行的, 但是该方法具有一定的普适性。同时, 本次测试是在测试环境下进行的, 绝对数据存在一定的失真, 希望以后能在生产环境进行尝试, 获取更加真实的数据给开发运维同事提供一定的参考。

参考文献:

- [1] 徐广斌, 武剑锋, 白硕. 低延时证券交易系统关键技术研究 [J]. 计算机工程, 2011, 37(18):28-31.
- [2] 杨明秋. 论全球证券交易系统七大发展趋势 [J]. 世界经济研究, 2010(11):31-38.
- [3] 徐广斌. 高效率证券市场基础架构研究 [J]. 交易技术前言 201506:4-10.
- [4].Cinober 公司. A Cinnober white paper on: latency. 2009
- [5] 章庆. 使用交换机度量系统超低延时的实践 [J]. 测试技术与质量管理 201706:58-62.

低时延网络构建

何志东 / 华锐分布式技术实验室 广东 深圳 518040

余鹏飞 / 上交所技术公司 上海 200120

摘要：低时延网络技术是交易技术中重要环节，本文围绕低时延网络的设计思路、关键影响因素等进行阐述，提出解决思路和建议方法，希望能为行业机构建设低时延网络提供一些参考。自底向上构建低时延的交易系统，首先需要构建低时延的网络基础设施，低时延网络在国外证券交易所以及大型券商的核心系统都已有成熟的应用，也让系统的整体性能获得了很好的基础设施支撑。本文就如何构建低时延的网络给出了明确的方案思路，也希望抛砖引玉，与同行共同探讨低时延网络的建设思路，促进行业技术升级发展。

关键词：低时延；交易系统；证券交易；以太网；InfiniBand



1 引言

近年来,金融和资本市场通过业务和技术双轮驱动持续高速发展,全球交易所趋向集中整合和互联互通,交易产品和业务多元化创新。信息技术创新日新月异,推动交易系统不断更新换代,交易系统由集中式转向分布式是国内证券行业交易技术发展的趋势。

证券交易系统的交易竞价原则是价格优先、时间优先,即同等价格下,先到先得。目前国内主流券商的集中交易系统委托上行时延从几十毫秒级到上百毫秒不等,面对日益激烈的竞争需求,新一代分布式架构的交易系统已经向百微秒级的时延迈进,时延大小是衡量交易系统性能最重要的指标。

如何构建证券期货经营机构到交易所的端到端低时延网络,成为一个热门的话题。本文就低时延网络技术及构建方案进行阐述,供相互探讨。

2 低时延网络

全球交易所是以微秒级时延来进行度量和竞争的。为满足市场要求,采用先进的高性能网络设备和技術,构建高可靠、低时延、高吞吐网络的需求日益迫切。

每年 6 月和 11 月,Top500 Supercomputer 网

站 [1] 公布超级计算机世界 500 强名单、性能指标、技术架构等,其中网络互联技术作为高性能网络技术的标杆。2018 年 11 月,超级计算机前 500 强名单显示,最流行的互连技术是以太网(252 个系统),然后是 InfiniBand(135 个系统),自定义互连(64 个系统)和 Intel Omni-Path(43 个系统)。各种技术占比情况见图 1:

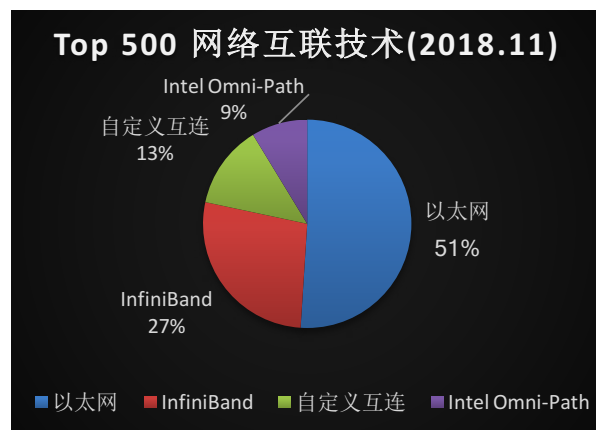


图 1 TOP 500 超级计算机网络互连技术 (2018 年 11 月)

对 2016 年至 2018 年 Top500 超级计算机的网络互连技术变化趋势进行统计,得出如下图 2 的折线图:

通过分析,可以得出高性能网络技术的应用和发展趋势:

- 1、以太网和 InfiniBand 是两种主要的网络协议,万兆以太网是最广泛使用的系统互联技术;
- 2、近两年来,随着融合以太网技术快速发展及以太网带宽大幅提升,以太网的份额逐渐扩

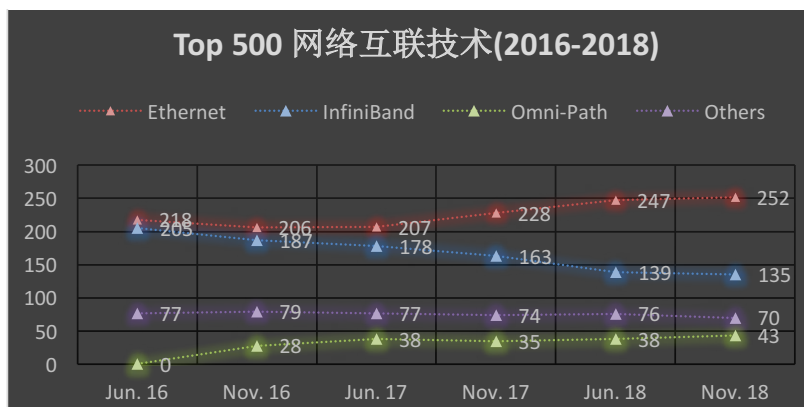


图 2 TOP500 超级计算机网络互连技术 (2016 年 -2018 年)

大至 51%，快接近 InfiniBand 份额的 2 倍；

3、Intel 主推 Omni-Path 高性能计算架构，提供交换机、管理软件、HFI 卡、线缆等一体化解决方案。Omni-Path 作为 InfiniBand 在超算高性能网络领域的主要挑战者，从 2016 年 11 月至今，采用 Omni-Path 的系统数量呈现平缓上升的趋势，目前总体占比为 9%。

2.1 以太网

以太网在 70 年代初期推出，以简单、易用、经济、易扩展等优势得到普遍应用。至今 40 多年的时间里，以太网技术和协议仍在持续演进发展，满足当今高性能网络融合创新的需求。近年来，为满足云计算、统一存储等多样业务，新型以太网通过 DCB、VXLAN、FCoE 等技术，丰富存储和虚拟化支持能力；通过 RoCE^[2]、拥塞控制优化、流控管理优化等技术，大幅降低网络转发时延。以太网带宽从早期的 10M 速率提升到 10G/25G/40G/50G/100G，近期以太网带宽进一步提升到 400G，满足超大规模数据中心和云计算等带宽密集型需求。

高性能以太网技术的快速发展，使得国内、外主要发达市场的交易所积极投入资源升级更新网络基础设施，如纽约证券交易所 (NYSE)、纳斯达克证券交易所 (NASDAQ)、伦敦证券交易所 (LSE)、东京证券交易所 (TSE)、香港证券交易所 (HKEX) 均采用万兆以太网，并提供万兆的托管机房接入。

2.2 InfiniBand

InfiniBand 在 1999 年首次提出，是一个为大规模、低时延的高性能服务器集群而设计的网络技术，通过大带宽链路实现服务器、存储设备互联。其特点一是超大带宽的连接。带宽支持 56Gb/s、100Gb/s 及 200Gb/s；二是极低的网络时

延。InfiniBand 在可比数据速率下具有比以太网更低的时延；三是可靠无损的网络。基于链路层的流控机制和先进的拥塞控制机制防止拥塞和丢包；四是完全的 CPU 卸载功能。基于硬件的传输协议实现高可靠、无丢包的网路数据传输。通过远程直接内存存取 (RDMA) 和内核旁路技术，可以直接对远程节点间预分配内存读和写，无需涉及操作系统内核、无需数据多次复制，大幅降低 CPU 工作负载和网络时延。五是卓越的可扩展性和灵活性。一个子网可以支持 48,000 个节点，一个网络即可支撑大规模服务器的部署。

一套完整的 InfiniBand 系统由服务器、交换机、子网管理器、主机通道适配器 (HCA) 组成。高性能服务器集群最广泛使用的网络架构为胖树 (Fat-Tree)，非阻塞网络下，该架构可以达到大规模服务器的最优性能。典型的胖树架构如下图示：

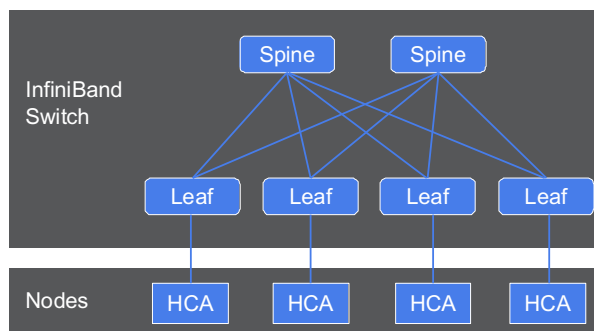


图 3 胖树架构示意图

部分交易系统的内部通信为了达到最小的时延，核心网络采用 InfiniBand，其他网络采用以太网，如德国证券交易所和新加坡交易所的交易系统内网采用 InfiniBand，德国证券交易所的 T7 交易系统 6.1 版本委托回报回路时延少于 52us，新加坡交易所的平均订单回报时延为 90us。

3 构建低时延网络

系统端到端时延主要由网络设备转发时延、网络连线的传输时延、网卡数据收发时延、操作系统处理时延、中间件处理时延及业务处理时延等构成。网络时延由网络设备转发时延、网络连

线的传输时延和网卡数据收发时延组成，构建低时延网络，就需要在以上各个环节降低时延损耗。

3.1 转发时延压缩

随着行业低时延、高性能交易场景及数据中心托管业务发展的需求，对网络设备的性能提出了更苛刻的要求。无论数据包大小和流量类型，所有网络端口之间应提供稳定的低时延传输，并保持足够低的时延抖动。2012 年 9 月，思科公司发布了自研芯片和算法的 Nexus3548 交换机，正常路径转发时延为 250 纳秒，抖动在 5 纳秒左右。2013 年，Metamako 公司发布了超低时延的、可配置的一层交换机 MetaConnect，时延仅为 4 纳秒，如此低的时延速度意味着使用者可以获得最大的竞争优势。2014 年，Exablaze 公司发布 ExaLINK Fusion 交换机，通过精简功能和协议并集成 Xilinx Ultrascale FPGA，二层转发时延为 110 纳秒，一层交换时延为 5 纳秒。Arista、Juniper、华为等网络厂商大部分采用 Broadcom、Intel 的商用 ASIC 芯片解决方案，根据官网的数据，Arista 7150s-52 的时延为 380 纳秒，Juniper 的 QFX 5110 的时延为 550 纳秒。Mellanox 采用自研的 Spectrum 芯片，以太网交换机 SN2410 的时延为 300 纳秒，InfiniBand SX6036 FDR(56Gb/s) 交换机的时延为 200 纳秒，InfiniBand SB7800

EDR(100Gb/s) 交换机的时延为 90 纳秒。

从上面的数据可以看到，低时延网络设备的制胜高地竞争异常激烈，超低时延交换机的转发时延已经慢慢接近光传输速度的物理极限。实际上，业务处理时延和系统开销远大于网络设备时延，网络设备的转发时延、性能表现等指标可作为一个对比参考项。尤其是在核心交易系统，我们首先应该关注高可用网络架构以及网络在复杂故障场景下的表现，其次才是尽可能地降低时延。

3.2 网络架构简化

传统的大型数据中心的网络架构，通常分为核心层、汇聚层、接入层，随着云数据中心、分布式计算快速兴起，数据中心内的服务器交互流量激增，数据流向模型由南北向变成东西向。传统的网络架构是为了南北向流量设计，已不能满足高性能、低时延分布式系统部署的要求。目前，构建低时延网络架构的方法是尽量简化传统网络的层数，减少数据经过网络设备的次数，将传统集中交换、垂直的网络架构变为水平的、易扩展的分布式架构。

根据服务器的数量进行分类，交换机按 48 个接入端口计算，一个数据中心小于 40 台服务器的低时延网络架构通常只有一层（核心层），两台交换机互联既作为核心交换机，也作为接入

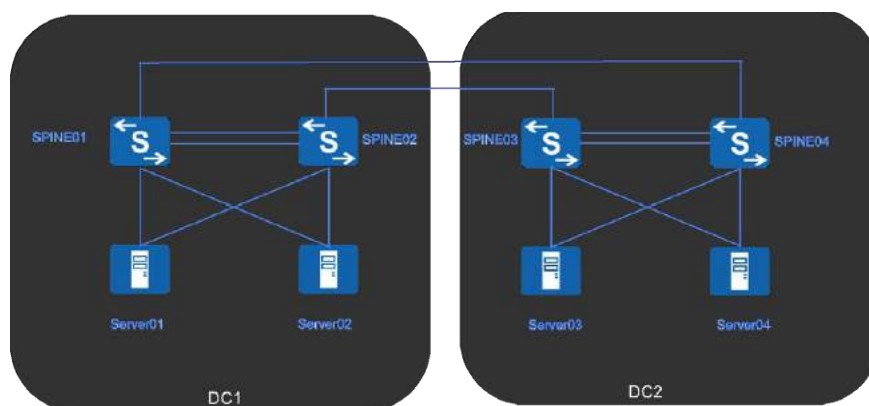


图 4 小规模服务器低时延网络架构

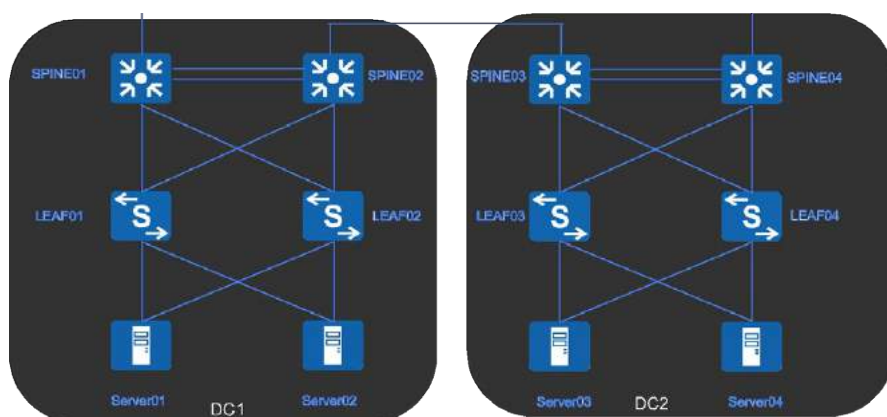


图 5 大规模服务器低时延网络架构

交换机。交换机之间运行 M-LAG 或 vPC 或堆叠，确保不产生环路。同数据中心 1 跳网络可达，跨数据中心 2 跳网络可达，网络架构如图 4 示。

一个数据中心多于 40 台服务器的低时延网络架构通常有两层（核心层、接入层），两台交换机互联作为核心交换机，其余交换机作为接入交换机。核心交换机之间运行 M-LAG 或堆叠，确保不产生环路。同数据中心 1 跳网络可达，跨数据中心 4 跳网络可达，网络架构如图 5 示。

3.3 传输时延优化

网络传输时延是数据在网络链路传输时产生的延迟，网络传输时延与系统部署位置、长途线路的长度及传输介质密切相关，选择最短路径和最佳质量的链路，可确保最小化链路的网络传输时延。

为便于市场参与者能灵活、快速接入，交易所提供托管机房、数据专线甚至互联网等多种接入方式。技术基础设施和系统部署的位置就近接入交易所，在交易所托管机房部署系统可有效缩短网络接入时延，有利于构建点对点直连交易所的快速交易通道。为保证公平性，交易所在托管机房提供几乎完全等长的布线、及统一带宽的接入端口。市场参与者为获得最小的网络通讯时延，应建设低时延的局域网，同城跨数据中心的通讯尽

量采用高速光纤链路进行通讯，通讯链路上尽可能少使用中继器、连接器、防火墙、路由器等设备。

3.4 低时延万兆网卡

低时延网络设备转发时延是百纳秒级的，在同一数据中心内部网络连线的传输时延也是百纳秒级的，相比之下，网卡数据收发时延则占据了主要的比重。下表是几个主流系列网卡的时延参考值：

表 1 主流系列网卡时延参考值

网卡类型	UDP RTT 参考区间 (us)
普通千兆网卡	50-100
普通万兆卡	20-40
低时延万兆卡	10-15

备注：以上测试结果采用标准 X86 PC Server 测试，主频 3.0GHz

即使是同为万兆网卡，不同系列网卡的性能差距甚远，低时延万兆的传输时延是普通万兆网卡的一半。网卡收发数据时延占如此高的比重，因此在构建低时延网络过程中，选择低时延万兆网卡非常有必要。

3.5 网络带宽提升

串行化时延是指一个数据帧或信元被一个接

收者接收并开始处理的时间。串行时延与传输速率成反比，速率越高，接收数据帧的时间越短。提升网络接入带宽是减少串行时延的最有效办法，低时延网络建议最低的接入带宽为 10G，推荐采用 25G 或更高的接入带宽。

现阶段，大多数数据中心基于 10G 以太网规划和建设。随着 25G 交换机和网卡的成本大幅降低，目前 25G 的总体拥有成本基本接近于 10G，网络布线不需要变动便可直接升级演进到 25G 带宽。根据 Dell'Oro Group 预测：随着支持 25G 的网络交换机和网卡不断增加，更多的云用户或大型企业升级到 25G。2019 年至 2020 年，25 G 将成为云和企业服务器的主流速度，25 G 端口的出货量预计将在 2021 年达到峰值。

华锐分布式技术实验室联合上交所技术公司低时延技术实验室，使用 Qperf 对某主流品牌低时延万兆网卡在 10G 和 25G 模式进行 TCP、UDP 时延基准测试，分析对比结果显示：25G 各种不同数据包长的 TCP 和 UDP 时延，均低于 10G 的时延。

时延结果如图 6、图 7 示：

进一步分析发现，即使网卡端口占用带宽远未达到 10Gb/s 的水平（如百兆 b/s 的流量带宽），以上测试结果仍然成立。为进一步分析带宽对应用系统的性能影响，实验室使用华锐的 ATP 交易系统在一个测试环境，基于网卡的不同带宽

模式进行测试，结果表明，系统时延降低超过 20% 的，应用的处理性能也得到了提升。

3.6 网卡加速

网卡作为服务器的一个重要部件，网卡的性能好坏会直接影响系统总体性能。通过网卡加速技术，可以大幅有效减少系统总体时延。近年来，以太网不断融合创新，发展推出 RoCE 协议。RoCE 在数据链路层支持标准以太网协议，在网络层上支持 IP 协议；也无需改变数据中心的原有基础设施，节省大量成本；还使得大带宽以太网的性能快速向 InfiniBand 靠拢。

除了 RoCE 的网卡加速技术，行业比较常用的是 Onload 加速技术，Onload 提供的高性能 POSIX 兼容网络堆栈，可显著减少网络时延、提高吞吐量和降低 CPU 利用率。Onload 提供标准的 BSD 应用程序编程接口支持以太网网络协议，最终用户不需要对应用程序进行修改。Onload 技术通过内核旁路、减少数据复制次数等技术将传统的内核堆栈约 7us 的时延降低至不到 2us。

3.7 无损网络

传统的以太网络采用的是尽力而为的转发模式，它对时延、丢包率等性能不提供任何保

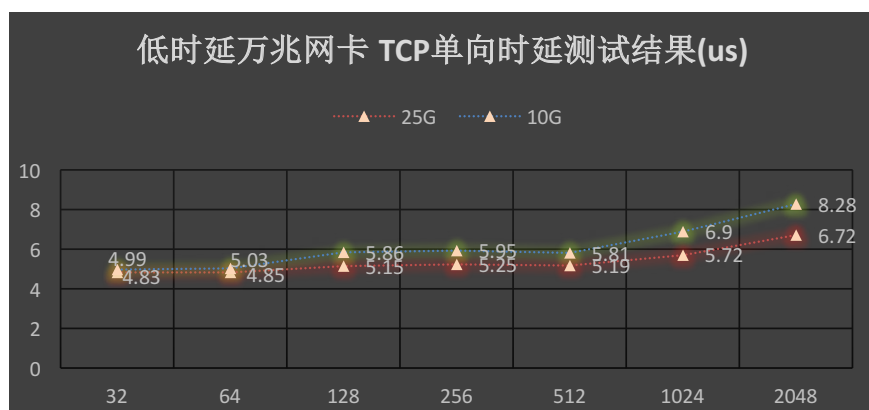


图 6 低时延万兆卡 10G&25G TCP 单向时延对比图

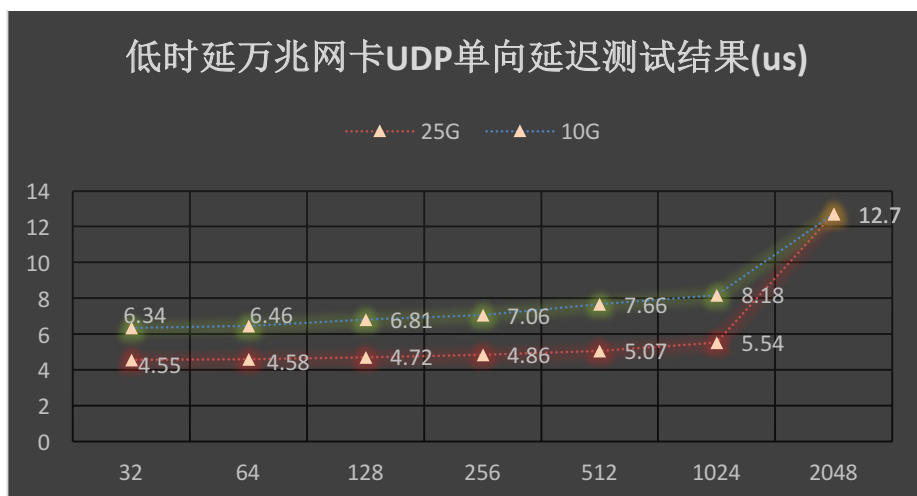


图 7 低时延万兆卡 10G&25G UDP 单向时延对比图

证。当网络中出现多台服务器同时与一台服务器通讯的时候，往往会造成网络数据的拥塞甚至丢包。网络拥塞丢包导致重传，增加网络时延，严重时会让业务性能也受到影响。减少或者避免网络拥塞和丢包现在通用的解决方案是：PFC(Priority-Based Flow Control) 和 ECN(Explicit Congestion Notification) 的流控技术。PFC 可以对链路上队列的流量进行控制，并在交换机入口出现拥塞时对上游设备流量进行反压。ECN 技术可以实现端到端的拥塞控制，在交换机出口拥塞时，对数据包做 ECN 标记，并让流量发送端降低发送速率。通过在网络中组合部署 PFC、ECN 功能来实现无损传输保障，

确保网络保持低时延运行。

4 总结

低时延网络技术是低时延技术的重要组成部分，也是未来网络技术发展的重要分支，在国内外核心金融机构核心金融系统的普及应用也预示着低时延网络技术在证券行业的发展前景。本文就如何构建低时延的网络给出了明确的构建方案，也希望抛砖引玉，与同行共同探讨低时延网络的建设思路，促进行业技术升级发展。本文也是低时延技术系列文章的第一篇，下一篇将会探讨低时延网络的度量方案及测试方法。

参考文献：

- [1] Top 500 supercomputer site[ER/OL]. <https://www.top500.org>
- [2] <https://community.mellanox.com/s/article/rdma-roce-solutions>

作者介绍：

何志东，hezhidong@archforce.com.cn，华锐分布式技术实验室主任，具有丰富的交易系统、消息总线和高可靠架构设计与开发经验，目前主管华锐分布式技术实验室，对分布式系统架构、高性能计算基础设施、低时延技术、系统性能调优等领域有深入研究。

基于开源架构的任务调度系统在证券数据处理中的探索和实践

蔡丰令, 樊玮, 张培乐, 田肖, 杜小静 / 上交所技术有限责任公司 技术开发总部,
上海 200120 (E-mail: flcai@sse.com.cn)

摘要：为了应对证券行业盘后批处理业务复杂度上升带来的批处理时间窗口逐步缩小和运维越来越困难的挑战，上交所技术积极拥抱开源技术，结合上交所批处理的生产经验教训，以零人工介入、自动化运维为目标，开发了一种跨平台、支持多种部署模式的任务调度系统。本文从上交所批处理系统面临的实际挑战出发，通过调研几类典型的批处理架构，选择以开源软件 Spring cloud dataflow 为基础，设计并研发了上交所批处理任务调度系统。目前，该系统已经在交易系统生产环境上平稳试运行半年有余，为该系统在上交所各技术系统的推广打下了坚实的基础。

关键字：任务调度、批处理、Spring cloud dataflow、上交所技术



1 背景和挑战

随着证券交易市场的快速发展，交易业务种类和待处理数据量也随之不断增加，核心应用系统的批处理业务越来越复杂。不同的批处理业务不但内部批处理单元相互依赖，而且与上下游对接系统的交互也越来越繁杂，导致留给批处理业务的处理时间窗口和应急时间窗口越来越小，这些都对新的批处理架构的高效性、高可用性和易维护性等方面提出了更高的要求。针对上交所批处理业务目前的实际情况，面临着如下问题和挑战。

首先是上交所各系统业务类型和数据量的增多对批处理架构的调度性能和功能提出了更多的要求。目前，上交所的核心交易盘后批处理业务类型越来越多，比如 A/B 股、综合业务、期权、沪港通等，对任务类调度的性能都有严格的要求。

其次是核心交易系统批处理业务的上下游交互越来越频繁，应急时间窗口越来越短，这对批处理架构的操控鲁棒性和预警系统的及时性都有了近乎严苛的要求。在证券系统中，不同的系统都有不同的分级，比如上交所核心系统为四级系统，对故障恢复时间要求极为严苛。如何能及时发现问题和解决问题，这不仅需要及时的预警系统，稳定的系统架构，更需要完善的应急操控功能。

第三、目前上交所技术公司业务系统、大数据系统和核心交易等系统都有各自的批处理框架，不同的批处理框架技术栈，各方面要求迥异，这都对新批处理架构选型造成了较大挑战。因此选择一个不同系统通用的任务调度系统，可以大大避免人力和资源的浪费，为软件的持续维护打下坚实的基础。

最后，软件技术、语言、系统等日新月异，软件的生命周期也是不可忽视的方面。比如，目前交易系统核心批处理是基于 OPENVMS 自主研发的批处理框架，虽然极其稳定高效，但是受限于操作系统生命周期将尽，升级或者重构都困难重重。

综上，已有的批处理架构在应对目前面临的各种挑战时就显得捉襟见肘，如何选择和研发一套满足证券业务处理高效性、鲁棒性和监控友好性的批处理架构越来越迫在眉睫。

2 批处理调度系统的探究和选型

目前批任务的处理根据调度控制的不同，分为资源调度和任务调度，资源调度是指为单个批步骤分配各种资源，比如 CPU、内存、磁盘甚至主机，目的是为了提高批步骤利用资源的效率。典型的资源调度系统有 Cloud Foundry、Yarn、Mesos 等；任务调度是指一系列的批步骤按照批编排的顺序及时准确的执行。典型的任务调度系统有 Elastic-job、Spring Batch、TaskCtl、Airflow 等。具体如何选择技术方向，还需要根据实际的需求确定。

批处理调度系统的选型主要有三个方向：自研架构、基于开源软件二次开发和采用商用软件。自研批处理调度架构对人力成本、时间成本都耗费巨大，从零开始，是否经得起大数据量的考验都是不得不考虑的风险；商业软件，成熟稳定，但是一方面不能完全自主掌控，一旦出现问题，难以应急；另一方面，上交所业务复杂，批处理特殊需求较多，难以及时满足各种需求。基于开源软件二次开发，不但可以保证项目进度，而且开源软件经过多年验证，具有一定的可靠性，同时能满足不同业务的独特需求。所以选择开源项目并进行消化改造不失为一种便捷可靠的方向。

由于目的不同，资源调度和任务调度并不冲突，一个调度系统中既可以支持批步骤的资源配置，也可以支持不同批步骤间的流程编排。目前上交所核心批处理调度系统由于历史和稳定性要求等原因，暂时不会采用资源调度的方式，仅将资源调度能力作为系统扩展能力的一部分。目前已知的开源任务调度架构较多，比较有代表性的有 Elastic-job、Airflow、Spring Cloud Data flow（以下简称 Dataflow）等。

Elastic-job 是当当网开源的定时分片类任务调度系统，目前很多公司基于该开源项目二次开发了自己的任务调度系统，比较有名的有唯品会的 Saturn、数人云的 Octopus 等。但是 Elastic-job 对任务间的依赖关系支持较弱，支持的任务类型比较单一，监控的范围和粒度都不能满足证券交易业务的需要。

Airflow 是 Airbnb 开源的 DAG（有向无环图）类优秀的任务调度工具。Airflow 主要由 PYTHON 实现，job 的定义无法通过 XML 或者界面定义，只能依靠 PYTHON 定义，所以无法做到调度架构和应用业务的解耦合；另外，Airflow 开源时间较短，调度性能较低，比较适用于简单的 ETL 类的编排。所以从易用性，稳定性和性能等方面都无法满足当前和未来证券业务的发展。

Dataflow 是 Pivotal 公司开源的支持 ETL、批量运算和持续运算的统一编程模型和托管服务。根据批任务的生命周期长短不同，Dataflow 把应用处理分为流处理和任务处理，并且为基于微服务的分布式流处理和批处理提供了一系列的模型和最佳实践。

但是 Dataflow 也有一些不足：首先云调度性能不足，一个微服务的调度达到了分钟级；其次整体架构比较庞大，如何取其精华是必须面对的挑战。但是结合上交所盘后批处理的实际情况，还有如下几方面优点：

1、Dataflow 强大的编排能力可以支持关系复杂，数量庞大的交易业务。

2、Spring/Spring Cloud 技术栈在上交所技术公司内部使用越来越广泛，这都为后期的 Spring 系列功能维护升级提供了保障。

3、Dataflow 支持本地调度、云调度等部署方式，可以满足不同系统的等级要求，方便以后的系统升级和维护。核心交易系统为了安全性和稳定性的考虑，采用 Dataflow 本地版本可以规避 Docker 等新技术的稳定性风险，也方便了后续云调度功能的完善，核心系统的平滑升级。而大数

据系统却可以采用云调度等部署方式，支持微服务，Docker 等新技术满足自己弹性伸缩、灰度发布等方面的需求。

4、Dataflow 天然支持流处理业务和批处理业务。证券交易业务既有实时交易数据流的同步处理需求，也有报表、对账等盘后处理需求。

5、Dataflow 支持各种类型的批任务，比如 EXE、SHELL、PERL、PYTHON、JAR 等，可以实现调度架构和批应用开发完全解耦。

综上所述，选择以 Dataflow 开源框架为基石，开发出符合上交所数据处理实际需求的调度架构不失为一个可行、可控且符合安全运行需求的方案。

3 面向证券交易的任务调度系统的设计

虽然 dataflow 有诸多优点，但是其作为开源软件，也有开源软件的通病，比如：

1、开源软件只实现了基本功能，且侧重通用性，但是一个完整的企业级软件需要满足各种定制化需求。

2、开源软件一般性能不足，并且实战检验会有各种缺陷，需要不断优化。

3、开源软件需要消化学习成本较高，需要深入学习，才能融会贯通。

所以，结合核心系统的实际情况，我们开发了新一代任务调度服务架构（简称 EzTS），它是基于 Dataflow 深度开发，支持跨操作系统（Linux 和 Windows）运行，满足不同的部署场景（本地、分布式、云调度），具有框架和批应用低耦合，强操控，自动化运维等特点的批处理调度系统。

3.1 总体架构

EzTS 主要由三部分组成：监控网关、调度服务和执行器。核心交易系统批处理采用多活的部署方式保证系统的可靠性。监控网关负责监测

数据的汇聚和操控指令的转发。调度服务主要负责批配置的管理，流程的触发、调用和监控等功能。调度服务可以根据服务提供接口（SPI）的不同，支持不同的部署方式，比如 local 版和 cloud 版。执行器可以根据逻辑的不同分为流程和批组，通过流程和批组的配置编排运行批步骤。所有执行器和批步骤的状态都会存储在状态数据库（核心系统以 MySQL 作为状态数据库）中，其总体架构如图 1 所示。

虽然 dataflow 提供了非常强大的任务编排功能，但是还远远达不到企业级调度服务的要求，必须深入的改造才能适合上交所不同业务盘后批处理的需求。下面就从批应用配置、调服模式、操控方式、依赖处理和监控可视化五个方面介绍新一代任务调度服务的优化设计。

3.2 极简的应用配置导入

目前任务调度领域应用配置导入方式主要有

三大类：XML/JSON 配置式、程序配置式和拖拽配置式。XML/JSON 格式的应用配置方式比较复杂，比较适合业务数量较少，关系简单的系统；应用通过程序配置的方式，对框架侵入性太大，变更难度大，不够灵活，同样难以适合大规模的批处理应用系统；拖拽式的应用配置方式是最近比较流行的配置方式，虽然上手简单，但是实用性不足，难以满足大规模的应用配置。

为了将应用批步骤配置简单化、应用和架构完全解耦合，EzTS 采用了 EXCEL 文件作为应用的配置文件，应用的配置流程如图 2 所示。

应用的配置升级，只需要如下三步骤：

- 1、应用开发者从任务调度服务 web 操控端下载配置模板。
- 2、应用开发者填写应用配置。
- 3、应用配置升级。目前应用配置升级支持两种升级方式：方式一是通过任务调度服务的 web 操控端一键导入，提前检测配置的正确性；另一种升级方式需要把 excel 配置文件放置于公共目

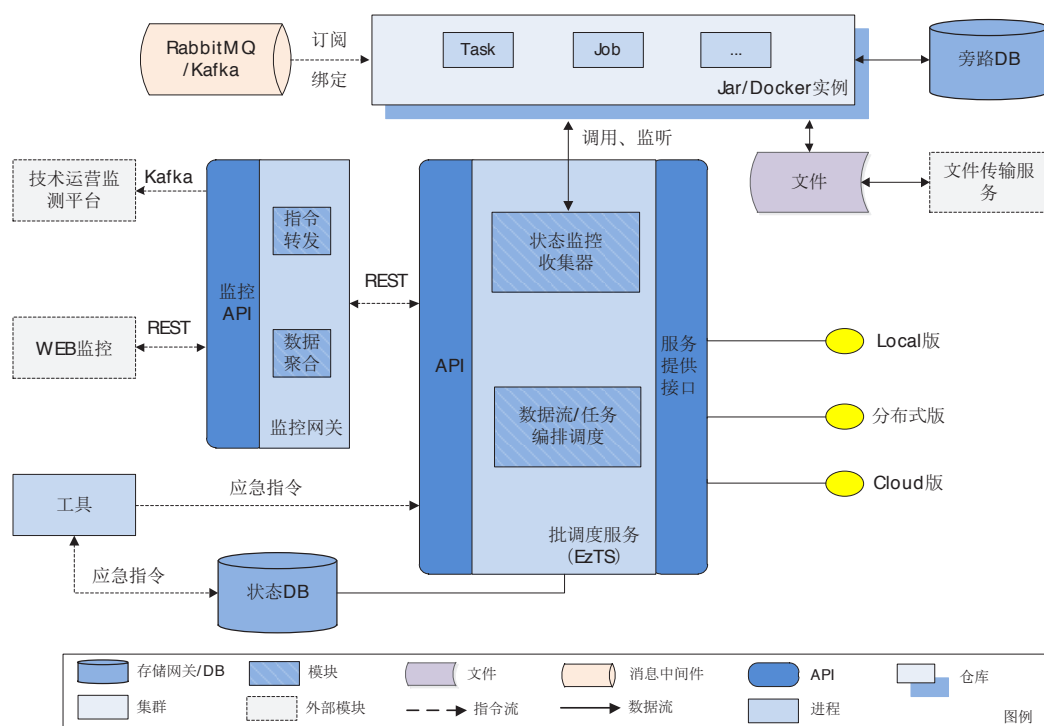
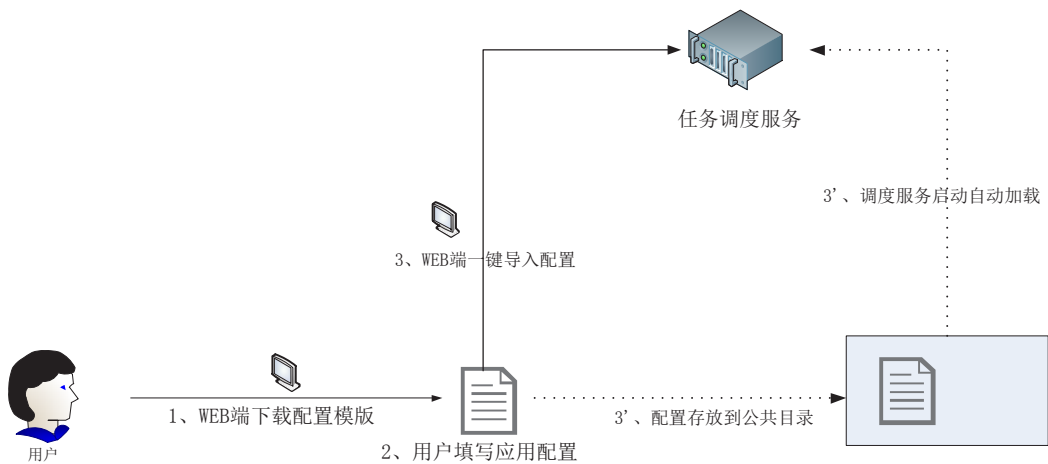


图 1 任务调度系统总体架构



录，调度服务启动时会自动加载应用配置。

这种应用配置的方式一方面大大的简化了应用配置的复杂度，应用开发者更容易上手。另一方面，调度架构和批应用测试升级完全解耦，增加了批应用开发的灵活性。

3.3 灵活的三层调度模式

随着交易业务的多样性，同一业务类型内部处理单元错综复杂，这些都对调度层级提出了更高的要求。为了更好的支持不同业务类型，不同的批处理逻辑单元的关系，EzTS 采用了三层调度架构的设计，根据层级的不同，分为流程、批组和批步骤，如图 3 所示。

目前，业界大多调度系统都支持基于 UNIX 的 CRONTAB 的定时任务，一方面 CRONTAB 为周期性的任务提供了极大的便利，但是却存在着明显的局限性。往往批步骤之间都有极大的耦合性，如果仅仅依靠定时的方式，所有的批步骤均和时间相关，一旦批步骤出现问题，未必能保证批步骤的执行顺序。

另外，目前部分较完善的批处理框架虽然也支持批步骤的串并行配置，但是却无法满足交易业务中天然具有分组概念的内部逻辑。所以为了区分不同业务批处理，不同处理组和不同批的处理先后关系，EzTS 采用了三层的调度架构：

第一层：流程的定时调度或者手工触发运行。一个流程可以为一个业务的所有批的组合或者一

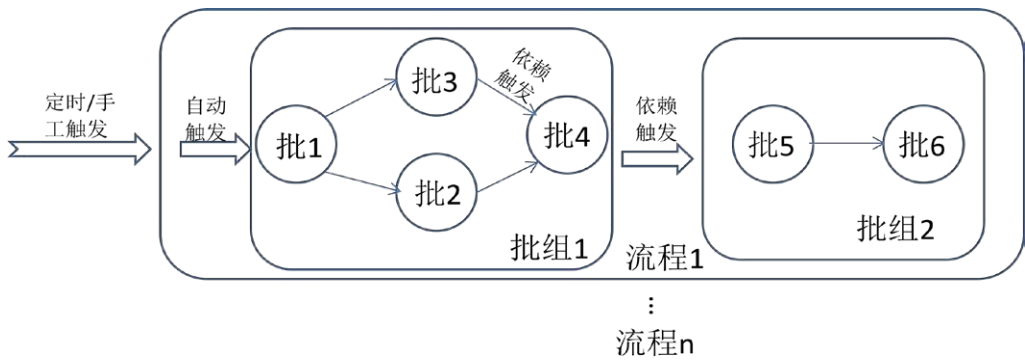


图 3 三层调度模式

类业务的组合。流程和流程之间完全解耦合。

第二层：批组的自动触发和依赖触发。当一个流程触发运行时会自动触发第一个批组，该批组完成，会触发依赖于该批组完成的批组。

第三层：批步骤的自动触发和依赖触发。批步骤作为最基本的处理单元，当批组触发运行，会自动触发第一个批步骤，该批步骤完成，会触发依赖于该批步骤完成的批步骤。

三层调度模式不但使不同的业务处理完全解耦合，而且能够清晰的划分同一业务内部的不同处理组的关系。极大地方便了批步骤的分类和管理。

3.4 多样的操控方式

随着交易业务越来越多，批处理业务的复杂度也越来越高，批步骤关联的上下游系统也越来越多，造成了批处理的应急窗口不断缩小，如何快速的解决批处理中遇到的问题，就显得愈加重要。

在实际的盘后批处理运行过程中，批步骤需要人为干涉的原因各种各样，比如上游数据迟到、错误或者数据处理出错等，这些不同的问题对任务调度服务的操控提出了更高的要求。根据批步骤操控方式的不同，可以简单归为两类：重跑操控和置状态操控。

下表列出了目前支持的操控方式如表 1 所示。

在批应用的生命周期中，往往不是一个人在开发和运维，随着时间的推移，一个批步骤的前后依赖关系逐渐变得模糊。一旦一个批步骤出错，哪些相关联的批步骤需要重跑，除非对该应用十分熟悉，否则很难抉择，这大大增加了应急的难度、时间和风险。所以针对这一类情况，特别加入了相关批重跑的操控类型。当批应用开发的过程中，配置相关批步骤的信息，这样再碰到这样的应急场景时，可以通过相关批重跑功能快速解决问题，这样可以大大减少应急的时间和风险。

多样的操控方式不仅增加了问题处理的灵活性，而且大大缩短了批处理系统恢复处理的时间。

3.5 完善的依赖方式

所有的批步骤都必须依赖满足才能被调起运行，否则，一方面会造成有限资源的浪费，另一方面造成程序进度的不可预知。根据上交所批处理业务的实际，将批步骤的依赖分为三大类：时间依赖、文件依赖和状态依赖。

在交易系统的批处理应用中，时间依赖的应用场景主要有两类，一类是某一批步骤不能早于某一时间点运行，比如期权结算价计算不能早于

表 1 操控类型

操控类型	操控名称	描述
重跑	从头重跑	流程从头开始运行
	错误重跑	流程从错误处开始运行
	单组重跑	单个批组从头开始运行
	单步重跑	单个批步骤重新运行
	相关批重跑	某个批步骤的所有相关的批步骤按配置的方式重跑
置状态	挂起/解挂	流程在某个批步骤上挂起等待
	跳过/解跳	流程运行时跳过某一批步骤继续执行
	置完成	将某一批步骤置为完成状态
	置未运行	将某一批步骤置为未运行状态

实时收盘时间。另外一类是某一类批步骤只能一周或者一个月运行一次。

目前，不同的证券系统之间盘后处理主要依靠文件来交互数据，这就造成了批处理的文件等待处理越来越重要。一方面，文件就绪后，调度服务立即调起批步骤应用程序可以大大缩小批步骤运行的时间，另一方面，批应用运行结束后，文件是否正确生成也可以通过批配置文件依赖反馈到批的运行状态。

另外，随着证券业务类型越来越多，批步骤之间的逻辑划分在实际开发的过程中越来越不清晰，导致不同批步骤之间的关系越来越错综复杂。出于配置和展示的需要，流程图的节点依赖逻辑不能太过复杂，这样完善的批状态依赖设计就显得特别重要。在流程图上能够表示出来不同批步骤间依赖关系称为显式状态依赖，否则称为隐式状态依赖。显式状态依赖可以快速定位批步骤在流程中的位置。隐式批状态依赖可以灵活的配

置任意批 / 批组和流程的等待关系，最大程度的节省批程序的整体处理时间。

3.6 监控的可视化

随着证券业务的发展，批步骤越来越多，批处理的运行时间也越来越长，批处理的运维变得更加困难，这都给批处理的监控提出了更高的要求。

批处理的监控由两部分组成：批处理的展示和操控。批处理的展示的难点在批步骤之间的关系和预警；批处理操控的难点在安全可靠。目前批处理的展示主要有两种：流程图展示和列表展示。两种展示方式各有优缺点，例如：流程图可以直观看到批步骤的关系，但是很难查找某一个批步骤，并且展示信息有限，列表反之。

EzTS 采用了流程图和列表相结合的方式，扩展了流程图的功能，也发挥了列表的优点。流

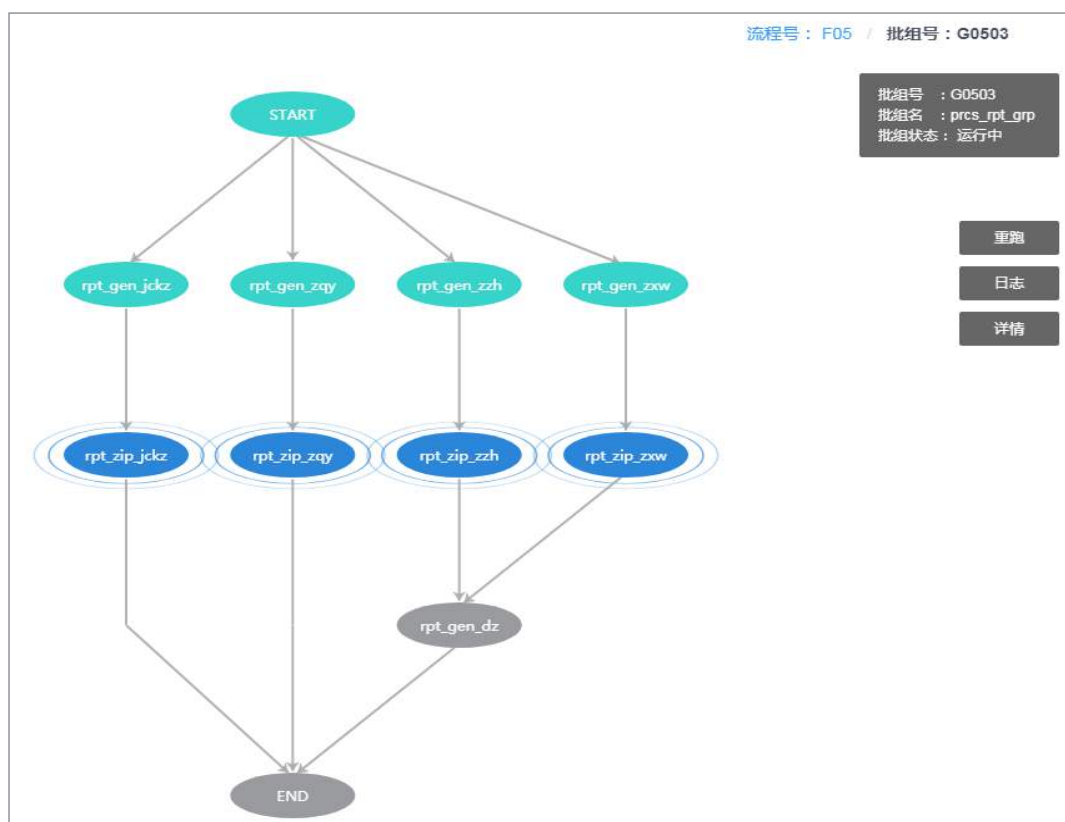


图 4 流程示意图

流程图	列表	46 全部	35 已完成	1 错误	0 超时	0 挂起	0 运行中	0 等待中	10 未运行	0 跳过
-----	----	----------	-----------	---------	---------	---------	----------	----------	-----------	---------

批/批组/流程号		展开		查询	刷新
----------	--	----	--	----	----

ID	名称	状态	依赖条件	起止时间	已耗时 (s)	进度	操作
▼ F05	rpt_gen_ctr	已完成	就绪	14:20:03/14:20:55	00:00:52	100.00%	批组 日志
▼ Q0501	procsolic_grp	已完成	就绪	14:20:03/14:20:18	00:00:15	100.00%	批组 日志
050101	rpt_gen_cv	已完成	就绪	14:20:07/14:20:18	00:00:11	100.00%	批组 批状态 日志
050102	rpt_gen_ndly	已完成	就绪	14:20:07/14:20:18	00:00:11	100.00%	批组 批状态 日志
050104	rpt_gen_zdly	已完成	就绪	14:20:07/14:20:18	00:00:11	100.00%	批组 批状态 日志
050105	rpt_gen_ntscrz	已完成	就绪	14:20:07/14:20:18	00:00:11	100.00%	批组 批状态 日志
▼ Q0502	procsgh_grp	已完成	就绪	14:20:03/14:20:41	00:00:38	100.00%	批组 日志
050201	rpt_gen_gh	已完成	就绪	14:20:08/14:20:19	00:00:11	100.00%	批组 批状态 日志

图 5 列表示意图

程图和列表展示示例如图 4 和图 5 所示。

在流程图页面可以快速的定位有问题的流程、批组和批步骤。不同的节点不但可以展示批名、批描述等信息，还可以点击批步骤直接操控，快速修复批处理中遇到的问题。

在列表页，则可以快速的搜索流程、批组和批步骤，直接定位操控。同时还支持根据不同维度快速分组批步骤，比如可以快速搜索出哪些批步骤为跳过状态。

在流程图的绘制过程中，如何合理的展示批步骤的节点成为了必须要面对的问题。

在流程图展示方面，目前只有商用软件

TASKCTL 宣称支持无流程图交叉，但是也有不足，比如所有批步骤必须完全属于某一串行或者并行组中，但是实际批步骤的关系很复杂，不一定满足这一设定。针对上交所批步骤实际的耦合关系，特别设计了流程图的坐标算法，计算流程如图 6 所示。

第一步：批处理调度服务通过读取数据库的流程图配置，获取流程图的串并行信息，例如 $A \& \& \langle B \parallel C \& \& D \rangle \& \& E$ 。

第二步：根据流程图中的串并行配置信息（备注：配置为 DSL 语言，例如 A 串行 B 用 $A \& \& B$ 表示，A 并行 B 用 $\langle A \parallel B \rangle$ 表示）转换为有向无

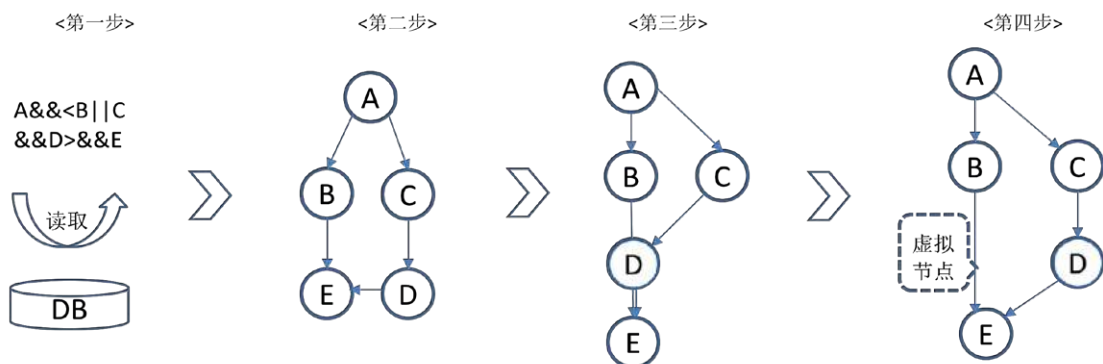


图 6 流程图坐标算法

环图。

第三步：为了使流程图从开始到结束只有一个运行方向（例如从上到下，或者从左到右），对有向无环图进行拓扑排序，这样使不同批步骤的层次更加明显。

第四步：通过第三步的拓扑排序，节点分布在不同的层级上，但是却无法保证批步骤依赖关系连线和批步骤节点不重合，所以加入虚拟节点，实现流程图无点线交叉。

这种流程图显示坐标算法一方面通过简单的串并行配置规则实现了流程图的描述，另一方面实现了任意有向无环图的分层无点线交叉显示。

4 总结与展望

虽然在新一代任务调度系统的实际开发的过程中碰到了各种各样的问题，比如开源软件底层架构的缺陷，高并发度时数据库死锁，线程和内存资源占用过多等问题，但是经过上交所批处理中心的不懈努力，这些问题都得到了优化和解决，完全达到了核心系统上线的要求。EzTS 系统 1.0

版本于今年 5 月份在核心系统生产环境上线运行以来，经历了多种业务，多种场景的检验，整体运行平稳。新一代调度系统在核心系统生产环境上线，不但开了上交所核心系统使用开源软件的先河，而且也说明了核心系统采用基于开源软件二次开发的方式具有可行性。EzTS 系统上线半年来的经验教训不但为批处理调度系统的进一步优化提供了方向，而且为 EzTS 系统在其他系统中的使用打下了坚实的基础。

未来，EzTS 批处理调度框架一方面将在使用过程中不断完善，不断提高可靠性和调度性能，另一方面，要不断的打磨新功能，比如使用流处理、资源调度、微服务、Docker 等，最终打磨出一款适用于上交所技术系统通用的调度服务框架，进一步地结合上交所金融云，推出云调度服务产品。

自动化运维、微服务、云调度一直是互联网技术研究的热点，上交所技术将会充分利用积累的运维经验，以开放的心态，拥抱、研究、落地新技术，不断打磨证券数据的处理能力，进一步提升自己对证券业务的研发、安全保障和运维的能力。

基于改进卷积神经网络 在商品指数预测中的应用研究

崔闯 / 大连飞创信息技术有限公司, 邮箱: cuichuang@dce.com.cn

胡天华 / 大连飞创信息技术有限公司, 邮箱: hutianhua@dce.com.cn

钟利明 / 大连商品交易所, 邮箱: zlm@dce.com.cn



摘要：本文创新地将传统的经济学自回归与深度学习模型结合用于时间序列预测，在保留了自回归模型变量关系可解释性的基础上，增加了卷积神经网络进行回归系数的迭代计算。基于改进卷积神经网络模型具有较高的预测准确度，同时结合了时间序列分析原理又保持了模型的可分析性，适用于多维度时间序列的输入分析并进行未来值的预测。本文利用改进卷积神经网络对飞创煤焦矿指数分别进行了分钟级和日度数据指数值的预测，其预测效果明显优于线性模型与全连接神经网络模型。此外由于模型中使用的卷积神经网络注重于短期序列的多因素相关性研究，对于近期因素对数据影响更大的序列，预测的准确度会更高。

关键词：卷积神经网络，时间序列，预测

1 概述

在预测时间序列的问题上, 计量经济学上通常使用的是自回归 (Auto-regression, AR) 等线性模型, 这类模型清晰地显示了变量之间的因果关系和变化规律, 具有良好的可解释性, 但由于其模型较为简单, 导致预测的准确度有所欠缺。随着计算机技术的迅速发展, 深度神经网络模型广泛应用于预测领域, 具有深入的分析能力和较高的预测精度, 但是其包含的多层网络通常是难以解释的, 直接将其应用于金融领域的交易具有一定的风险性。经济学强调变量之间的清晰因果关系, 期货交易则重视价格预测的准确性, 量化模型需要在可解释性和预测准确性之间进行平衡。本文将卷积神经网络与时间序列分析的 AR 模型进行结合, 保留了变量关系可解释性, 同时增强了模型的预测性。

文章共分为三部分, 首先对国内外卷积神经网络研究现状进行描述, 其次对模型原理进行了具体阐述, 最后使用改进卷积神经网络对分钟频率和日频率的指数值进行预测。

2 国内外文献综述

卷积神经网络 (Convolutional Neural Network) 在计算机科学中越发重要, 在不同的领域逐渐发挥越来越多的作用。由于卷积神经网络处理复杂数据的优越性, 目前国内外常见的卷积神经网络多应用于图像分类中并取得了很好的效果。时间序列预测在金融经济等领域具有重要意义, 部分研究者尝试将卷积神经网络应用于时间序列预测, 能够大大提高预测的准确性。

Jakob (2016) 通过创新将通常应用于文本预测与人工智能等方面的 LSTM 模型用于时间序列的预测, 并取得了较好的效果。将数据在输入神经网络之前先将数据进行多种方式的转换和处理是一种常见的做法, 通过对每个特征进

行深入学习, 可以精简神经网络的自动学习过程。Yi Zheng, Qi Liu (2014) 在研究中引入多元时间序列分类的深度学习框架: 多通道深度卷积神经网络 (MDCNN), 在该框架中, 多元时间序列被分为多个单变量, 并分别对每个单变量序列进行特征学习, 最后通过一个普通的多层感知机连接起来进行分类。其中, 该框架中使用两层卷积神经网络和两层全连接来代表分类多层感知机。Zhiguang Wang, Weizhong Yan(2016) 通过叠加卷积块来构建全卷积神经网络对时间序列进行预测, 该模型中不包含任何池化操作, 这样可以防止过度拟合的发生。此外, 模型应用了批量标准化来加速收敛速度, 提高泛化速度。在卷积完成后, 所有特征被输入到一个全局平均池层中, 而不是一个全连接层, 这在一定程度上减少了权重的数量。Iran Roman(2016) 在研究中分别对多个 CNN 卷积神经网络进行不同的数据转换训练, 包括整个数据集的空间聚类 and 主成分分解等, 训练后的数据应用于 RNN 循环神经网络的隐藏层有助于在隐藏层中保持高时间分辨率记忆的特点, 同时有助于解决在其他循环神经网络中出现的消失梯度的问题。Jan Koutník(2014) 对标准 RNN 体系结构进行了修改形成了一种新型的 CW-RNN 网络, 其中隐藏层被划分为单独的模块, 每个模块在其自身时间粒度上进行处理, 始终只按规定的频率进行计算。该模型减少了传统 RNN 的参数数量, 显著提高了网络的性能, 其中在音频信号处理预测方面的效果超过了传统的 RNN 与 LSTM 网络。Lukasz Romaszko(2015) 通过着重分析多个时间序列的相关性指出, 时间序列处理的深度学习方法和其他方法比较起来具有进一步改进的广阔空间, 并对预测序列数据的卷积神经网络进行了代码优化。

另一种时间序列的研究方法在深度学习中逐渐兴起, 即将数据编码为神经网络的图像, 从而有利于使用计算机的视觉技术进行数据分类。Z Wang(2015) 将时间序列数据编码成为 GAF/MTF

等不同类型的图像，并在标准数据集上使用卷积神经网络来对两种图像进行学习，得到的测试结果与原始数据相比较，MSE（均方误差）均低于普通时间序列分析模型，具有较好效果。Xiaolei Ma(2007) 提出了一种基于图像的卷积神经网络方法，将交通问题转换成通过二维时间空间矩阵来描述时间与空间关系的图像，并以较高精度预测了大规模范围的交通速度。

国内部分学者进行了应用神经网络进行时间序列预测的探索，张贵勇（2016）建立基于卷积神经网络的股票指数预测模型并在此基础上进行改进，提出基于卷积神经网络—支持向量机的混合预测模型用于股票指数预测，并证实了改进模型的有效性。黄卿，谢合亮（2018）分别采用神经网络、支持向量机和 XGBoost 对股指期货一分钟价格变动方向进行预测，研究结果表明，三种机器学习方法均具有较好的预测能力。

3 模型原理

3.1 原理背景

3.1.1 卷积神经网络起源

1962 年，Hubel 和 Wiesel 等通过对猫的大脑视觉皮层系统的研究，提出了感受野的概念，并进一步发现了视觉皮层通路中对于信息的分层处理机制，由此获得了诺贝尔生理学或医学奖。

80 年代中期，Fukushima 等基于感受野概念

提出的神经感知机（Neocognitron），可以看作是卷积神经网络的第一次实现，也是第一个基于神经元之间的局部连接性和层次结构组织的人工神经网络。

此后，研究人员开始尝试采用多层感知器（实际上是只含一层隐含层节点的浅层神经网络模型）来代替手工提取特征，并使用简单的随机梯度下降方法来训练该模型，1986 年，Rumelhart, Hinton 和 Williams 发表了著名的反向传播算法，这一算法随后被证明十分有效。

1990 年，Lecun 等在研究手写数字识别问题时，首先提出了使用梯度反向传播算法训练的卷积神经网络模型，并在 MNIST 手写数字数据集上表现出了相对于当时其他方法更好的性能。

至此形成了第一个真正意义上的卷积神经网络，早期的卷积网络被用于人脸检测、人脸识别、字符识别等各种问题。但并没有成为主流的方法，其原因主要是训练样本数和计算能力的限制等因素。随着科技发展，计算机的计算能力和数据存储能力迅速提高，深度卷积神经网络逐渐受到广泛关注，现代意义上的深度卷积神经网络起源于 AlexNet 网络，它是深度卷积神经网络的鼻祖。这个网络相比之前的卷积网络最显著的特点是层次加深，参数规模变大，在这之后各种改进的网络被不断的提出，卷积神经网络开始广泛的应用于多个领域。

3.1.2 卷积神经网络原理

卷积神经网络（Convolutional Neural Networks,

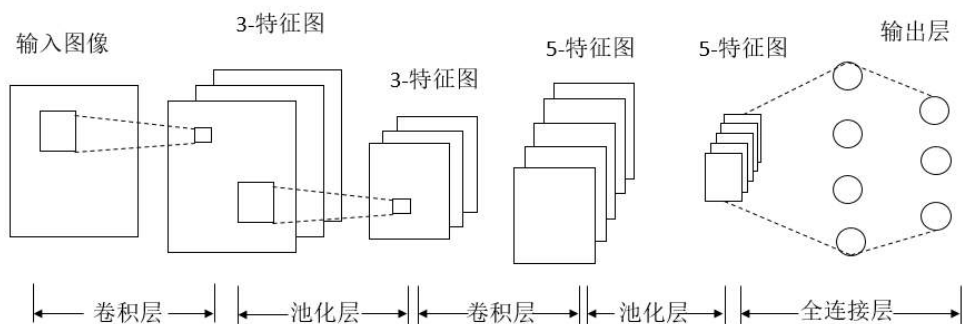


图 1 卷积神经网络构架图

CNN) 是一种常见的深度学习架构,受生物自然视觉认知机制启发而来,具有一定的生物学理论支持,是神经科学的新事物。

如图 1 所示,一个卷积神经网络由若干卷积层、池化层、全连接层组成。通过各层的组合可以构建各种不同的卷积神经网络,它的常用架构模式为:

输入层 \rightarrow [[卷积层]*N \rightarrow 池化层]*M \rightarrow [全连接层]*K

即 N 个卷积层叠加,然后(可选)叠加一个池化层,重复这个结构 M 次,最后叠加 K 个全连接层。图 1 展示的卷积神经网络:按照上述模式可以表示为:输入层 \rightarrow [[卷积层]*2 \rightarrow 池化层]*2 \rightarrow [全连接层]*1,即 N=2、M=2、K=1。

传统的全连接神经网络具有大量参数,部分参数的权重被赋予了极小的值,尽管网络层数越多其表达能力越强,但是通过梯度下降方法训练深度全连接神经网络是非常困难的,因为全连接神经网络的梯度很难传递超过 3 层。因此,我们不可能得到一个很深的全连接神经网络,这也限制了神经网络的扩展能力。综上,全连接神经网络模型的扩展性较差。

与全连接神经网络不同,卷积神经网络具有局部连接的属性,即每个神经元不再和上一层的所有神经元相连,而只和一小部分神经元相连,一组连接可以共享同一个权重,而不是每个连接有一个不同的权重,这样减少了大量的参数。此外,卷积神经网络可以使用池化的方式来减少每层的样本数,进一步减少参数数量,同时还可以提升模型的鲁棒性。因此卷积神经网络在扩展性和预测准确性上都具有更好的效果。

3.1.3 时间序列分析原理

时间序列分析是根据客观事物发展连续规律性,运用过去历史数据,通过统计分析进一步推测未来发展趋势。时间序列中每个观察值大小,是影响变化的各种不同因素在同一时刻发生作用的综合结果。常见的时间序列模型有自回归

AR(p) 模型、移动平均 MA(q) 模型、自回归移动平均 ARMA(p,q) 模型、自回归综合移动平均 ARIMA(p,d,q) 模型等。本文将卷积神经网络与时间序列分析的 AR 模型进行结合,保留了变量关系可解释性,同时增强了模型的预测性。

3.2 模型简介

3.2.1 模型介绍及特点

在预测时间序列的问题上,计量经济学上通常使用的是自回归(Auto-regression, AR)、自回归移动平均(Auto-regressive moving average)与向量自回归(Vector auto-regression, VAR)等线性模型。这类模型的优势是模型参数是可观测的,回归模型显示了变量之间的结构关系,通过检验系数在统计上的显著性就可以分析出变量之间的动态变化规律,从而找到经济变量直接的因果关系。传统的经济学模型虽然具有良好的可解释性,但是由于其简单的线性关系,模型的复杂度不够,导致预测的准确度有所欠缺。

随着计算机技术的迅速发展,深度神经网络模型广泛应用于预测领域,这类模型在图像和自然语言处理等多个领域均取得了较好的预测效果,但是神经网络模型包含的多层网络通常是难以解释和理解的,相当于一个黑箱,直接将其应用于金融领域的交易具有一定的风险性。经济学强调变量之间的清晰因果关系,期货交易则重视预测的准确性,量化模型需要在可解释性和预测准确性之间进行平衡。

本文创新地将传统的经济学自回归模型与深度学习模型结合用于时间序列预测,在保留了自回归模型变量关系可解释性的基础上,增加了卷积神经网络进行回归系数的迭代计算。基于改进卷积神经网络模型具有较高的预测准确度,同时结合了时间序列分析原理又保持了模型的可分析性。利用改进卷积神经网络对飞创煤焦矿指数分别进行了分钟级和日度数据指数值的预测,其

预测效果明显优于线性模型与全连接神经网络模型。此外，由于金融时间序列预测与传统的神经网络处理图像所需序列的特征有所不同，将经典的深度学习模型应用到时间序列预测中需要对其进行一定的改进。

3.2.2 模型原理

改进卷积神经网络模型的基本架构如图2所示，模型同时结合了AR（Autoregressive）自回归模型与卷积神经网络用于处理多维度时间序列，在保留了自回归模型的时间序列可解释性基础上，通过卷积神经网络确定时间序列的权重。

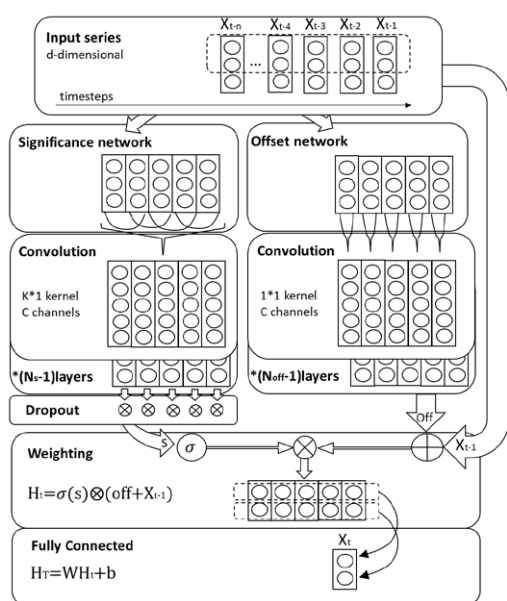


图2 改进卷积神经网络模型概览图

模型架构如图所示，多维时间序列会同时输入到两个卷积神经网络中，分别为显著网络（Significant network）和偏置网络（Offset network），显著网络与偏置网络分别包含了体现卷积网络与时间序列模型特点的卷积层。模型进行预测的主要原理如下：

$$H_t = \sigma(s_{t-1}) * (\text{off}_{t-1} + X_{t-1}) + \sigma(s_{t-2}) * (\text{off}_{t-2} + X_{t-2}) + \sigma(s_{t-3}) * (\text{off}_{t-3} + X_{t-3}) + \dots + \sigma(s_{t-n}) * (\text{off}_{t-n} + X_{t-n})$$

其中， H_t 为经过显著网络与偏置网络加权后的输出，显著网络的输出 $s_{t-1}, s_{t-2}, s_{t-3}, \dots, s_{t-n}$ 为多层卷积后提取的一维特征变量；偏置网络通过大小

为1的卷积核进行一层卷积，输出值 $\text{off}_{t-1}, \text{off}_{t-2}, \text{off}_{t-3}, \dots, \text{off}_{t-n}$ 作为过去时间序列变量的调整偏置值。通过将 $s_{t-1}, s_{t-2}, s_{t-3}, \dots, s_{t-n}$ 作为经过偏置调整后变量的系数并加和得到 H_t ，最后通过一个全连接层得到待预测指数值输出 H_T ，其中 w, b 分别为全连接网络的权重系数与偏置值，公式如下：

$$H_T = wH_t + b$$

与经典的卷积神经网络相比，用于时间序列预测的改进神经网络模型没有使用池化层（pooling layer），用以保证输入的时间序列长度能够保持到最后的全连接层，从而保证了神经网络最终输出模型的可解释性，即通过最终得出的预测公式能够将时间序列各个变量对最终预测结果的贡献进行解释和分析。

3.2.3 模型适用性

在金融系统运作过程中，投资者非常关心某种经济模式的发生状况和时间，以便采取相应对策。而神经网络有很强的识别能力，其学习能力可对环境的变化进行学习。采取神经网络信息处理技术能够对快速变化的市场环境进行深入分析，增强对经济金融领域的预测能力。

通过结合传统自回归模型的可解释性与神经网络的准确性，改进卷积神经网络模型适合于处理多维度时间序列输入进行预测，模型预测可有效应用于积累了大量历史数据需要对未来状况进行预测判断的行业如金融、经济与商业等领域。此外由于模型中使用的卷积神经网络注重于短期序列的多因素相关性研究，因此对于近期因素对数据影响更大的序列，预测的准确度会更高。

4 实证分析

指数预测模型的实证过程包括数据预处理、预测模型结构初始化、预测模型参数调整、预测模型训练、测试以及预测结果统计分析等，即首先建立基于卷积神经网络与经济学传统自回归的预测模型结构，并通过实验结果分析网络结构各

参数对于预测结果的影响，最终确立适用于商品指数预测的改进卷积神经网络模型并分别进行分钟频率指数值与日频指数值的预测。

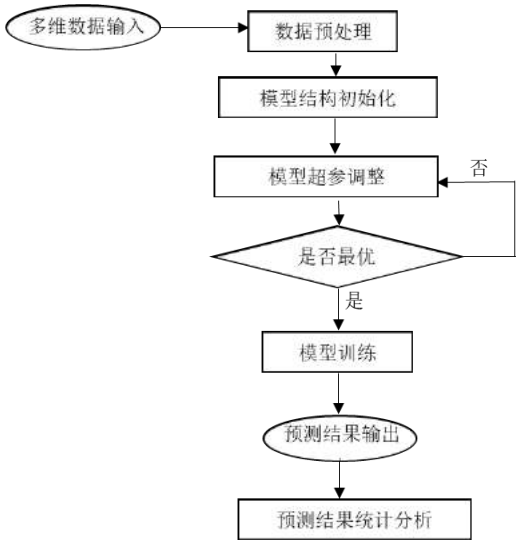


图 3 实证分析流程图

4.1 实证数据样本

在样本的选取上，以飞创煤焦矿指数的分钟频率指数值与日度频率指数值为主要预测对象，模型的输入序列包括分钟频率与日频的指数均价、最高价、最低价与指数所包含品种（焦煤、焦炭、铁矿石）的持仓量、成交量与最新价等多维时间序列。此外，本文还创新添加了包括粗钢、钢铁、钢铁企业、焦炭、焦炭期货、螺纹钢、煤炭、生铁、铁矿石等钢铁相关词条的每日百度搜索指

数值作为预测模型的输入变量。

本文对分钟频率数据采用 2017 年 5 月 16 日 9 点至 2018 年 4 月 27 日 23 点 29 分的时间跨度作为样本区间，数据采样间隔为每分钟，对日度频率数据采用 2013 年 8 月 9 日至 2018 年 4 月 27 日作为样本区间，数据采样间隔为每天，各个频率的数据均剔除了非交易日的数据。煤焦矿指数分钟走势如图 4 所示，可见样本期间煤焦矿指数处于较大的波动中，这说明样本时间的选取存在市场波动，处于适合进行神经网络预测的市场环境。

4.2 预测模型结构及参数介绍

改进卷积神经网络模型具体超参选择情况如图 5 所示，显著网络（Significant network）和偏置网络（Offset network）主要由卷积层、dropout 层、激活层、Flatten 层与全连接层构成。不同的卷积层数、卷积核大小和个数以及 dropout 的概率选择均可以构成不同的卷积神经网络模型，同时也会在一定程度上影响到预测的最终结果。由于显著网络与偏置网络分别继承自深度学习与传统经济学自回归模型，其中前者应用了卷积神经网络的多层卷积处理，后者保留了变量关系的可解释特征，此处对两个网络的卷积方式分别进行规定。

对于显著网络来说，由于商品指数时间序列数据历史值的影响范围较小，因此输入样本应当

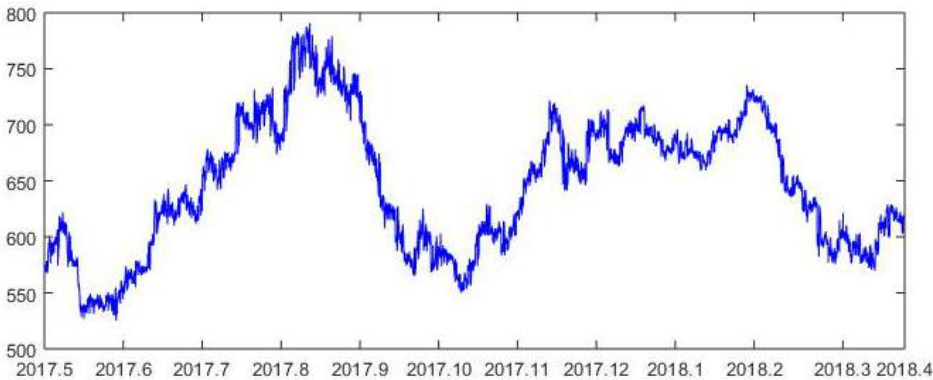


图 4 煤焦矿指数分钟走势图

选择相对较短的数据长度,这对显著网络的深度有所限制,即卷积层数不能过多。本文对改进卷积神经网络模型的显著网络采用3层卷积,在保证神经网络学习深度的同时,也增加了卷积神经网络对时间序列数据的适应性。

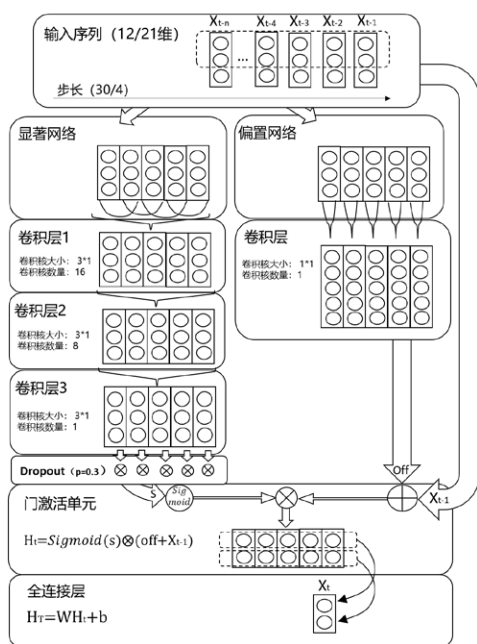


图5 模型超参选择情况示意图

在卷积维度的选择上,由于本文只考虑历史指数相关数据对某个时刻的指数值影响,因此只使用一维卷积,这简化了卷积神经网络的结构,在减小卷积核大小的同时降低了网络计算的复杂度。考虑到如果多次卷积过程中每个卷积核的大小不同会导致模型过于复杂,且不利于模型的训练,因此本文显著网络在每次卷积过程采用相同大小的卷积核,且各层卷积核个数呈递减趋势。经过参数的多次调整和尝试,本文模型的显著网络最终采用的卷积核大小为3,且卷积核个数每层递减,分别为16、8、1,其中,最后一层需要卷积核个数为1来保证输出与待预测时间序列具有相同的维度。

对于偏置网络来说,采用一个卷积层且卷积核大小为1可以保留变量关系的可解释特征。偏置网络将卷积后的输出与指数值序列的输入进行

加和,起到了偏置修正指数输入值前值的作用,以便模型结合偏置网络与显著网络进行综合计算。

过拟合是深度神经网络的常见问题,dropout通过按照一定概率在网络中暂时丢弃部分神经网络单元,可有效的防止神经网络过拟合并提高预测的效果。本文对显著网络三次卷积后的输出结果通过dropout层随机断开部分输入神经元,防止了过拟合现象的出现。经过对参数的调节和验证,对dropout的概率P选择为0.3,即卷积神经网络以0.3的概率舍弃部分神经元,其他神经元以概率0.7被保留,舍去的神经元输出都被设置为零,用以防止模型的过拟合和保证预测效果最优[15]。

显著网络与偏置网络在最后输出层应用了神经网络门激活单元(GATED ACTIVATION UNITS),本模型选用的激活函数为Sigmoid函数。显著网络和偏置网络经过神经网络门激活单元机制后的输出通过Flatten层将数据一维化后,通过全连接层构成单层感知机,输出指数预测值。

4.3 模型预测

4.3.1 分钟预测模型

(1) 参数初始化

本节尝试使用改进卷积神经网络模型预测煤焦矿指数分钟指数值,预测主要是基于煤焦矿指数相关的多维时间序列包括每分钟指数均价、最高价、最低价、指数所包含品种的持仓量、成交量与最新价共计12个因子与粗钢、钢铁、钢铁企业、焦炭、焦炭期货、螺纹钢、煤炭、生铁、铁矿石等9个钢铁相关词条的每日百度搜索指数值。其中,由于百度搜索指数只有日频率的数据,为了将其应用于分钟预测模型中,本文创新将日频的百度搜索指数数据分钟化,即维持当日每分钟的相应百度搜索指数值不变,与每分钟煤焦矿指数一起作为输入变量用于煤焦矿分钟指数值的

预测中，从而实现了不同频率数据的同步输入。

分钟预测模型的训练样本长度为 30 分钟，训练集、验证集与测试集的样本数量分别为 80000、5270 与 2000，迭代次数为 200，在训练中采用小批梯度下降（mini-batch gradient decent）的形式，即把数据分为若干批，按批来更新参数，分钟预测模型中设置每批数据数量为 128，在降低梯度下降的随机性的同时减少了计算量。本部分分别对仅包含期货市场相关 12 个因子，与在此基础上添加了 9 个钢铁相关词条的每日百度搜索指数值共计 21 个输入因子作为模型输入进行煤焦矿指数值的预测。此外还增加了线性回归¹预测（Linear Regreesion）、岭回归（Ridge Regression）与全连接（Rully Connected）模型作为预测情况的对比，验证本文建立的改进卷积神经网络模型的有效性。

以添加百度搜索指数后共计 21 个因子的输

入数据模型为例，改进卷积神经网络分钟预测模型具体如图 6 所示：

其中，InputLayer 为输入层，模型分批次输入了长度为 30 的 21 维因子，分别经过显著网络与偏置网络的一维卷积（Conv1D）进行处理，其中显著网络经过三层卷积核大小为 3，卷积核数量分别为 16、8、1 的卷积后的输出经过 Dropout 层进行概率为 0.7 的神经网络单元随机丢弃得到 dropout_6，偏置网络经过一层卷积核大小为 1 的卷积后的输出结果与指数值序列进行加和得到 add_6。两个网络的输出经过神经网络门激活单元（GATED ACTIVATION UNITS）进行处理：

$$\text{Multiply_6} = \text{Activation}(\text{dropout_6}) \otimes \text{add_6}$$

Multiply_6 经过 Flatten 层将数据一维化后，通过全连接层 Dense 构成单层感知机，最终输出指数预测值。

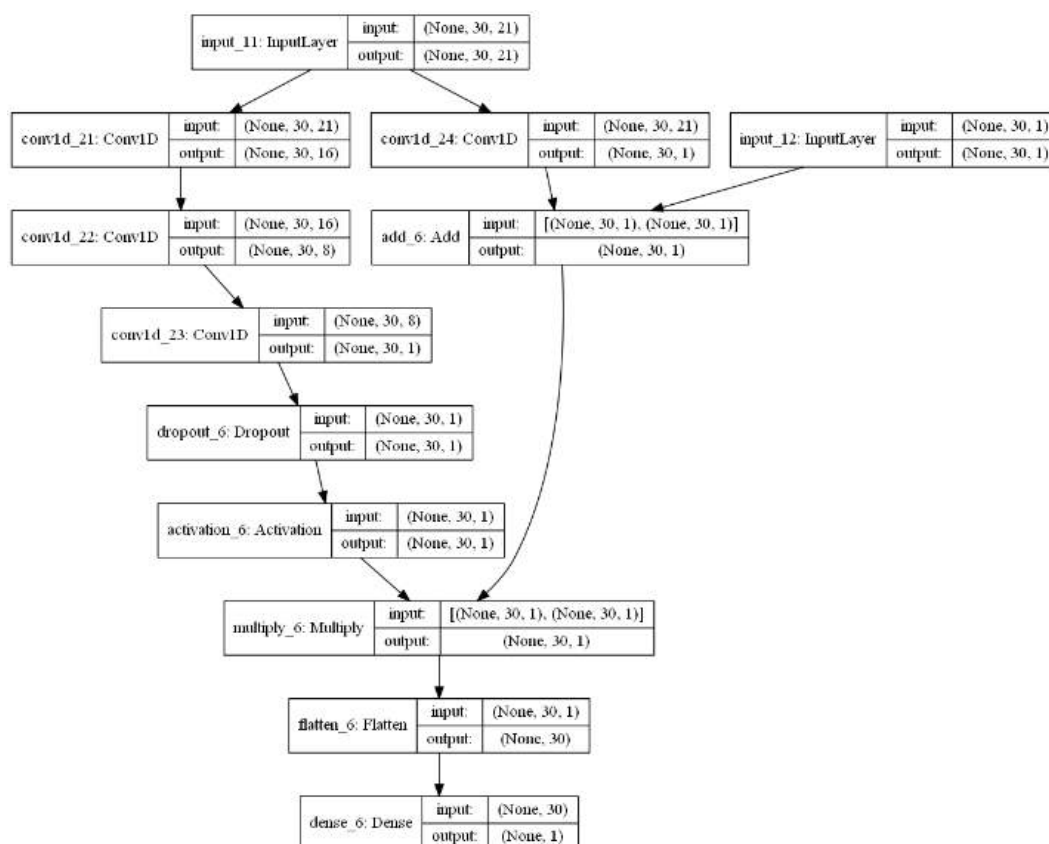


图 6 改进卷积神经网络分钟预测模型（以添加百度搜索指数数据为例）

(2) 预测结果统计

本文分别对是否添加百度搜索指数作为输入因子的输入数据使用各个模型进行指数值预测,各个模型的输出结果如图 7、图 8、表 1、表 2 所示,其中图中蓝色线为模型输出的预测值,红色线为真实指数值。

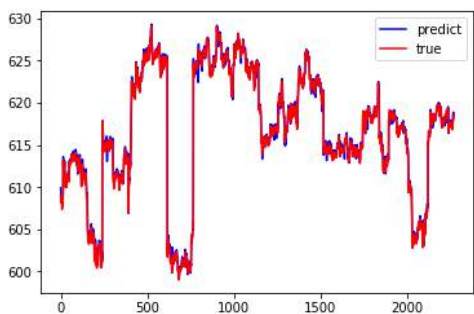


图 7: 未添加百度搜索指数输出结果图(12 维输入因子)

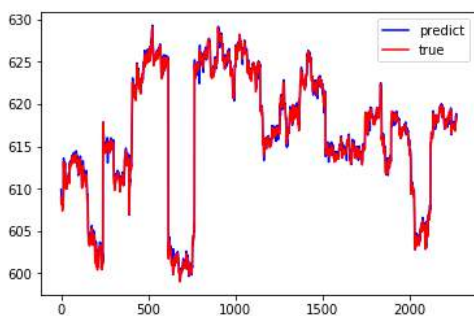


图 8: 添加百度搜索指数输出结果图(21 维输入因子)

通过图 7 可以初步看出改进卷积神经网络模型预测值接近于真实值,模型具有较好的预测效果。根据表 1,基于改进卷积神经网络模型预测结果具有远低于线性回归模型与岭回归模型的均方误差与平均绝对误差,最大误差与其他两个回归模型相差不大,因此,可以看出改进卷积神经网络模型具有较高的预测准确度,是较好的预测模型。

通过表 1 与表 2 的对比可以看出,在输入因子中添加了百度搜索指数后,改进卷积神经网络模型预测效果得到了一定的提升,并仍优于线性回归模型与岭回归模型。但添加了百度搜索指数作为输入因子后,线性回归模型与岭回归模型的预测效果有所下降,这说明线性模型在进行多维数据输入的综合预测时具有一定的局限性,改进卷积神经网络模型更能处理多维信息并提取出有效信息进行时间序列的预测。

4.3.2 日频预测模型

(1) 参数初始化

与分钟预测相似,日频模型应用部分主要是尝试使用改进卷积神经网络模型预测煤焦矿指数日频指数值,预测主要是基于煤焦矿指数相关的多维时间序列包括每日指数均价、最高价、最低

表 1 未添加百度搜索指数输出结果表(12 维输入因子)

	模型	均方误差 Mse	平均绝对误差 Mae	最大误差 Max error
1	线性回归模型	36.7187	3.6983	23.9338
2	岭回归模型	36.6448	3.6950	23.9325
3	全连接神经网络模型	2.9707	1.2264	23.3205
4	改进卷积神经网络模型	0.9080	0.4536	23.1028

表 2 添加百度搜索指数输出结果表(21 维输入因子)

	模型	均方误差 Mse	平均绝对误差 mae	最大误差 Max error
1	线性回归模型	43.4143	4.1333	22.9407
2	岭回归模型	43.3218	4.1293	22.9391
3	全连接神经网络模型	2.3864	1.0682	22.7448
4	改进卷积神经网络模型	0.7583	0.3649	22.8740

价、指数所包含品种的持仓量、成交量与最新价共计 12 个因子与粗钢、钢铁、钢铁企业、焦炭、焦炭期货、螺纹钢、煤炭、生铁、铁矿石等 9 个钢铁相关词条的每日百度搜索指数值。与分钟预测模型不同的是，日频模型的输入变量均为相同频率的数据，同时数据量和数据变动幅度较大。以添加百度搜索指数后共计 21 个因子的输入数据模型为例，改进卷积神经网络日频预测模型具体如图 9 所示：

由图 9 可知，日频预测模型与分钟预测模型保持了相同的结构，不同的是日频预测模型的训练样本长度为 10 天，训练集、验证集与测试集的样本数量分别为 1000、50 与 100，迭代次数为 200，小批梯度下降（mini-batch gradient decent）训练中设置每批数据数量为 8。日度预测同样分别对仅包含期货市场相关 12 个因子、包含期货市场相关 12 个因子与 9 个钢铁相关词条的每日百度搜索指数值共计 21 个因子作为模型输入进

行煤焦矿指数值的预测，此外，本文也同样增加了线性回归预测（Linear Regreesion）、岭回归（Ridge Regression）与全连接（Rully Connected）模型预测作为预测情况的对比。

（2）预测结果统计

分别对是否添加百度搜索指数作为输入因子的输入数据使用各个模型进行日频指数值预测，各个模型的输出结果如图 10、图 11、表 3、表 4 所示：

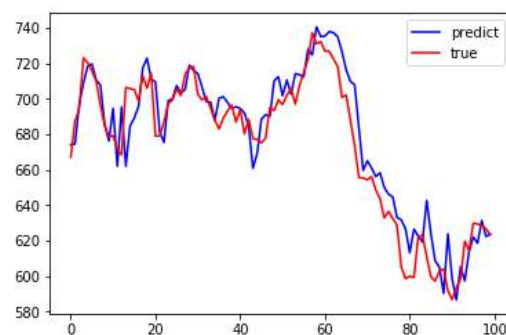


图 10：未添加百度搜索指数输出结果图

（12 维输入因子）

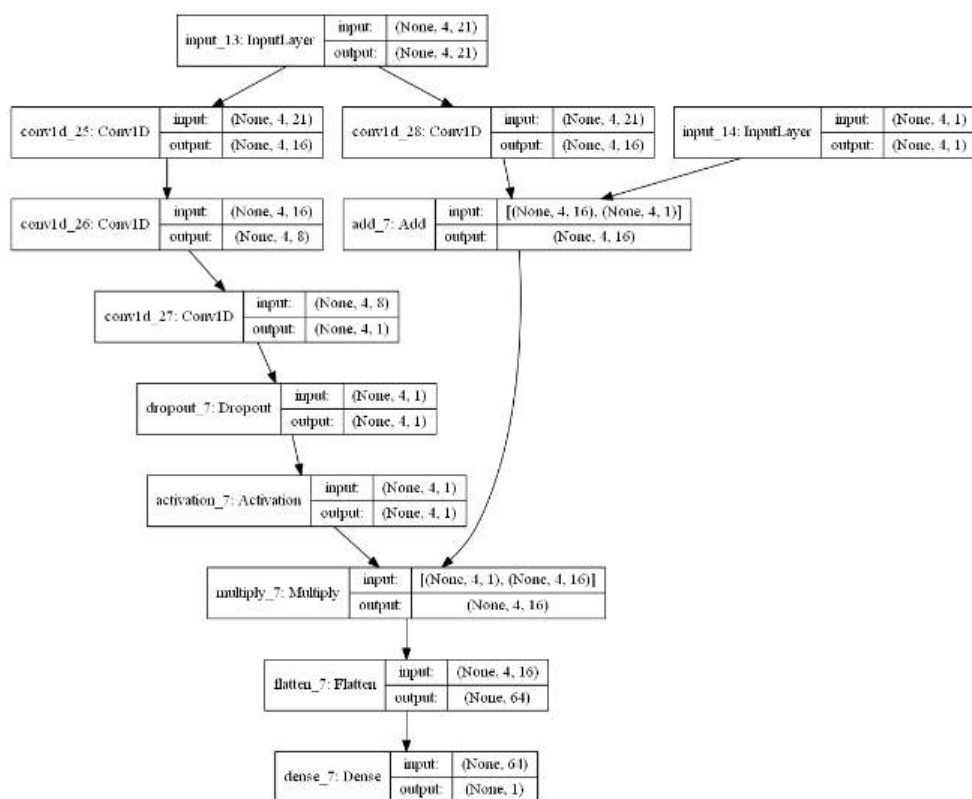


图 9 改进卷积神经网络日频预测模型（以添加百度搜索指数数据为例）

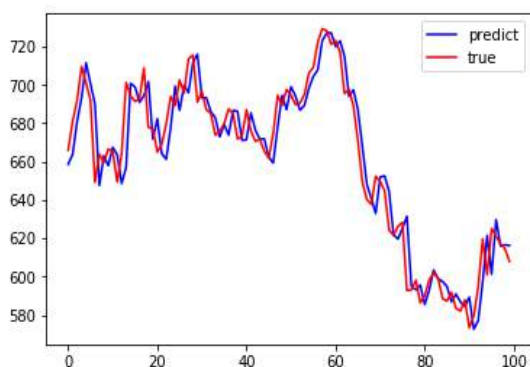


图 11: 添加百度搜索指数输出结果图(21 维输入因子)

由图 10、图 11 可以看出, 添加百度搜索指数的改进卷积神经网络模型预测结果更接近于真实值。根据表 3、表 4, 基于改进卷积神经网络模型的预测结果均方误差、绝对平均误差与最大误差均低于其他三个模型, 在输入数据中添加了百度搜索指数后, 改进卷积神经网络模型预测效果明显提升, 但其他几个模型的效

果有所下降。这与分钟预测模型的结论一致, 即线性模型在进行多维数据输入的综合预测时具有一定的局限性, 而全连接模型由于包含了大量参数, 在大量增加了输入数据维度后, 会导致模型中大量权重被赋予过小的数值, 从而降低了预测精度。因此, 改进卷积神经网络模型在多维输入的日度数据预测上仍具有一定优势。

综上, 改进卷积神经网络模型更能在多维信息中提取出有效信息, 对于高频与低频数据都具有更好的预测效果。此外, 本文使用多重卷积网络对时间序列进行特征提取, 计算时间序列上各个时间节点的权重, 构造出的模型是部分可解释的。一方面为重视可解释性的投资者引入了神经网络工具, 提高了投资的有效性, 另一方面又保证了模型的部分可解释性, 为基本面的量化研究提供了一个新的思路。

表 3 未添加百度搜索指数输出结果表(12 维输入因子)

	模型	均方误差 Mse	平均绝对误差 mae	最大误差 Max error
1	线性回归模型	299.7273	11.3396	54.7982
2	岭回归模型	229.2303	11.3297	54.7429
3	全连接神经网络模型	231.4660	12.4293	41.6515
4	改进卷积神经网络模型	199.1018	10.7687	44.4222

表 4 添加百度搜索指数输出结果表(21 维输入因子)

	模型	均方误差 Mse	平均绝对误差 Mae	最大误差 Max error
1	线性回归模型	306.6457	13.1793	53.6953
2	岭回归模型	305.2636	13.1505	53.4558
3	全连接神经网络模型	579.9800	19.8074	51.4073
4	改进卷积神经网络模型	167.9174	9.8391	44.3006

注释：

1 线性回归预测假设输入的 X 和 Y 是线性关系，预测的 y 与 X 通过线性方程建立机器学习模型，并通过选择合适的算法来求出使得预测 y 和实际的 Y 之间的差值尽量的小的参数，形成最终的预测模型。

参考文献：

- [1] Jakob, Lstm neural network for time series prediction[EB/OL],<http://www.jakob-aungiers.com/articles/a/LSTM-Neural-Network-for-Time-Series-Prediction>.2016-12-21.
- [2] Yi Zheng, Qi Liu, Enhong Chen, Yong Ge³, J. Leon Zhao, Time Series Classification Using Multi-Channels Deep Convolutional Neural Network [J].WAIM, 2014: 298-310.
- [3] Zhiguang Wang, Weizhong Yan, Tim Oate, Time Series Classification from Scratch with Deep Neural Networks: A Strong Baseline [C]. Cornell University Library, 2016(12).
- [4] Iran Roman, Assessing Neuroplasticity with Convolutional and Recurrent Neural Networks [C] Stanford University,2016.
- [5]Jan Koutník, Klaus Greff, Faustino Gomez, Jürgen Schmidhuber, A Clockwork RNN [C] Cornell University Library,2014(2).
- [6] Lukasz Romaszko, Signal Correlation Prediction Using Convolutional Neural Networks [J]JMLR: Workshop and Conference Proceedings 46:45–56, 2015
- [7] Z Wang, T Oates, Imaging time-series to improve classification and imputation[J] International Conference on Artificial Intelligence 2015,1043(1):3939-3945.
- [8] Xiaolei Ma, Zhuang Dai, Zhengbing He, Learning Traffic as Images: A Deep Convolutional Neural Network for Large-Scale Transportation Network Speed Prediction [J] sensors 2017,12(4),818.
- [9] 张贵勇 . 改进的卷积神经网络在金融预测中的应用研究 [D] 郑州大学 ,2016(5).
- [10] 黄卿 , 谢合亮 . 机器学习方法在股指期货预测中的应用研究基于 BP 神经网络、SVM 和 XGBoost 的比较分析 [J]. 数学的实践与认知 ,2018,4:287-307.
- [11] Hubel DH, Wiesel TN. Receptive fields, binocular interaction and functional architecture in the cat' s visual cortex. Journal of Physiology. 1962;160(1):106-154.
- [12] Fukushima K, Miyake S. Neocognitron: A new algorithm for pattern recognition tolerant of deformations and shifts in position. Pattern Recognition. 1982;15(6):455-69.
- [13] Rumelhart DE, Hinton GE, Williams RJ. Learning representations by back-propagating errors. Nature. 1986;323(6088):533-6.
- [14]Alex Krizhevsky, Ilya Sutskever, Geoffrey E.Hinton. ImageNet Classification with Deep Convolutional Neural Networks.
- [15] Geoffrey E. Hinton, Nitish Srivastava, Alex Krizhevsky, Ilya Sutskever, Ruslan R. Salakhutdinov. Improving neural networks by preventing co-adaptation of feature detectors. Cornell University Library. 2012;3.

E 实践探索 xplore

- 6 容器云在证券行业的探索与实践
- 7 海通证券金融云思考与实践（下）
- 8 金融科技在国内外券商 PB 业务中创新实践与思考
- 9 基于证券业网络安全等级保护的应用系统安全实践
- 10 基金行业数据安全保障体系建设探析

00001		0.45	▲	+0.45%
00002		-0.23	▼	-2.34%
00003		-1.01	▼	-1.89%
00004		0.02	▲	+0.21%
00005		+2.58	▲	+3.05%
00006		-0.14	▼	-1.42%
00007		-0.73	▼	-0.90%
00008		+1.08	▲	+5.12%
00009		-0.87	▼	-3.88%
00010		-0.65	▼	-1.37%

容器云 在证券行业的探索与实践

管文琦 / 华泰证券 guanwenqi@htsc.com

朱凯 / 华泰证券 zhukai012131@htsc.com

摘要：随着证券行业的发展，支撑业务的 IT 系统也在逐渐壮大。为了快速响应业务需求，敏捷交付成为了 IT 系统建设新的要求。容器技术作为敏捷交付的最佳拍档，已经深刻影响了持续集成和持续交付，也改变着 IT 系统的开发、交付和运维。

关键词：敏捷；容器；持续集成；持续交付



1 背景

金融市场瞬息万变，高效的业务支撑能力离不开与时俱进的 IT 系统。随着公司业务的发展，IT 系统数量在不断增多，同时每个系统的复杂度也在不断提高。即便在微服务改造之后，IT 系统的开发、交付和运维依旧面临着以下难题：

- 开发

代码量不断增加、协同开发难度加大
多样化的编译和运行环境

- 交付

更快的交付频率
按时发布、按需发布

- 运维

微服务化后带来的架构复杂度提高
产品整体部署和运维难度增加

这再次印证了软件工程的世界里“没有银弹”。微服务化解决了 IT 系统紧耦合、强技术依赖、难维护的问题，但是却同时带来了新的问题。在我们看来，这是一个螺旋上升的过程。

随着容器技术的发展，容器技术与微服务逐渐碰撞出火花，业界也普遍认为容器技术和微服务是“天生一对”。在 2017 年，容器化微服务成为了我们新的选择，优化了开发、交付和运维方式和流程，并一直推动着公司敏捷和 DevOps 的发展。

2 华泰容器云简介

2017 年，随着容器和容器编排技术的日趋成熟，我们建设了符合实际应用场景的“容器云平台”。容器云平台采用时下最流行的容器技术 Docker 和已成行业标准的容器编排工具 Kubernetes 建设而成，通过构建、服务、流水线、监控、日志等功能有效承载了微服务、CI/CD、DevOps。

2.1 微服务

现在越来越多的金融企业使用微服务架构，以应对快速变化的互联网金融挑战。通过微服务改造把应用拆分成很多细小的服务，每个服务专注于单一的功能，服务和服务之间有明确的边际，使用轻量级的通讯协议进行沟通，实现某个相对单一的功能。微服务的到来降低了巨大单体式应用复杂度、每个服务的开发技术自有选择、每个服务可独立扩展、每个服务可独立部署。但使用微服务架构不要低估细粒度分布式应用治理与运维的复杂度。而结合容器技术的微服务则可以给企业带来更高的资源使用率，更加快捷的迭代变更，更加方便的快速扩容能力。

2.1.1 容器是微服务的最佳载体

通过容器将微服务的运行时标准化，每个容器承载一个服务，然后像搭积木一样组合起来，让彼此通信，从而就能很轻松地模拟出复杂的微服务架构。

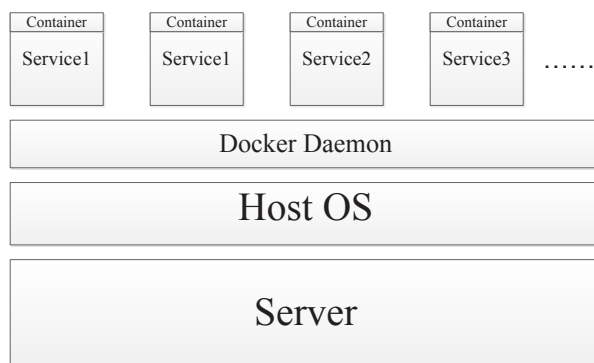


图 1 容器中的微服务

1. 容器天然做到了应用之间相互隔离，在保证安全隔离的同时，可以有效提高资源使用率
2. 为微服务的快速扩容提供有效的支撑，容器启动非常快速，秒级实现，通过镜像可以快速启动多个微服务
3. 对软件和其依赖环境的标准化打包，保证了微服务多个副本之间的绝对一致性，使得我们可以方便运维管理更多的微服务

4. 容器占用资源少、部署快，每个微服务应用可以被打包成一个容器镜像，每个应用与容器间成一对一关系也使容器有更大优势，为每个微服务单独构建镜像，通过镜像可以独立发布一个微服务，不依赖于生产环境基础结构，这使得从研发到测试、生产能提供一致环境。

2.1.2 利用 Kubernetes 支撑微服务

Kubernetes 在支撑容器平台和微服务的竞争中依然胜出。传统的应用部署方式是通过插件或脚本来安装应用。这样做的缺点是应用的运行、配置、管理、所有生存周期将与当前操作系统绑定，这样做并不利于应用的升级更新/回滚等操作。Kubernetes 是 Google 开源的一个容器编排引擎，它支持自动化部署、大规模可伸缩、应用容器化管理。在生产环境中部署一个应用程序时，通常要部署该应用的多个实例以便对应用请求进行负载均衡。

在 Kubernetes 中，我们可以创建多个容器，每个容器里面运行一个应用实例，然后通过内置的负载均衡策略，实现对这一组应用实例的管理、发现、访问，而这些细节都不需要运维人员去进行复杂的手工配置和处理。

2.1.3 微服务运营管理

1. 配置管理

相同的微服务，部署在不同的环境，如不同的生产中心、灾备中心、测试迭代环境、并行测试环境等，需要有不同的配置，容器云平台通过 Kubernetes 特有的 PV/PVC 功能，结合配置中心的统一管理，方便实现配置管理，真正实现“一次打包，到处运行”。

2. 自动扩缩容和灰度发布

利用 Kubernetes 和容器，华泰容器云平台可以很好的实现治理微服务需要的自动扩缩容和灰度发布。根据实际的业务需求和策略，容器云平台通过 Kubernetes 自动“调整”其“弹性资源”的管理服务。通过弹性伸缩功能，业务团队可设置定时、周期、自定义的监控策略，敏捷快速地

增加或减少“弹性资源”，并完成实例配置，保证业务平稳健康运行。在满足业务需求高峰增长时无缝地增加“弹性资源”，并在业务需求下降时自动减少“弹性资源”以节约成本。同样结合负载均衡软件，我们可以让流量逐步指向新扩容出来的新版本的微服务，快捷的实现灰度发布全过程。

3. 健康检查

当微服务数量不断增加后，健康检查和服务自动修复是一项重要工作，华泰容器云平台利用容器的特性，提供了容器健康监控和服务自动修复的功能，减少了微服务过程中运维的压力。

2.2 CI/CD

2.2.1 持续集成

持续集成是一种软件开发实践，开发人员通过经常性地自动化集成他们的工作，从而尽早地发现 IT 系统集成错误。持续集成通常包括如下过程：统一的代码库、自动触发、自动构建、单元测试、自动化部署、自动化集成测试等等，这些工作通过 Jenkins 虽然也能完成，但是需要大量编码工作，而且强依赖底层资源和环境，这使得开发和测试人员花费了大量精力在流程的对接上，而容器云平台的建成大大改善了这种情况。开发和测试人员在容器云平台通过图形化的界面操作便可以完成持续集成的整套流程，将精力聚焦在软件开发细节和测试用例上。使用容器云平台不仅屏蔽了底层资源，大大简化了运行时环境准备工作，结合容器的弹性，还大大提高了资源利用率。图 2 展示了容器云平台的持续集成流程。

2.2.2 持续交付

持续交付是持续集成的自然延续，它完成了产品从开发测试到生产的“质的蜕变”。利用容器云平台上的流水线，我们完成了从提交代码自动化触发构建到最终自动更新生产环境某个微服务版本的整套交付流程。在开发测试环境构建出

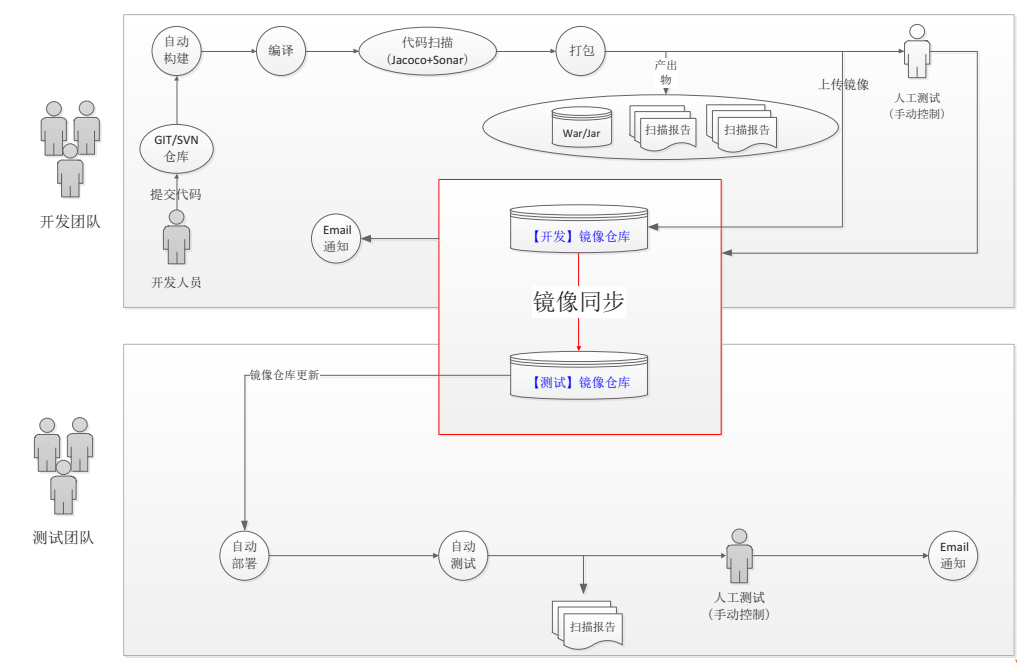


图 2 持续集成

的应用镜像通过流水线同步至预发布环境，经过测试后再同步至生产环境部署，我们做到了在保证交付质量的前提下，加快交付速度，从而更快地反馈市场需求，赋能业务发展。下图是持续交付流程图：

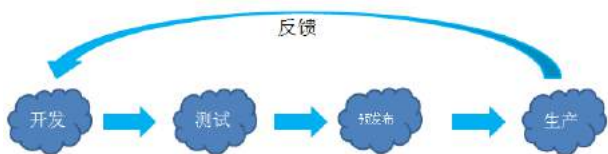


图 3 持续交付

2.3 DevOps

DevOps 主要用于开发、测试以及运维之间的协作管理，并且通过自动化流程，更加快捷、频繁、易重复且可靠的构建软件、测试及发布部署。持续集成和持续交付是实现 DevOps 的一部分，但不等于 DevOps。DevOps 应该还包括一套完整的持续部署以及持续运营的完整开发测试运维一体化的 DevOps 方法和工

具。DevOps 不是一定要用容器，但是有了容器，DevOps 变得更加简单。可以说容器云平台的建设既是 DevOps 实践，也推动了华泰证券 DevOps 的落地：

1. 借助容器云平台提供敏捷开发能力，让开发端更加敏捷；
2. 通过容器云平台，实现开发测试生产环境一致性，逐步建立标准化、一致性的开发、测试、运维环境，专注于业务应用开发，不分心于资源管理；
3. 实现应用全生命周期管理，满足应用开发、自动化部署、自动化运维等应用服务全生命周期管理需求；
4. 基于容器云平台的能力，实现应用服务的弹性伸缩、灰度发布等能力，满足多种业务需求。

3 华泰容器云的落地路径

容器云平台的落地凝聚了很多特色功能，这些功能经过设计、验证和实践，有效支撑了容器



图 4 容器云平台上的 DevOps

云平台稳定、高效地运行，下面简单介绍 4 个落地路径：网络模式、弹性伸缩、有状态服务、应用市场。

3.1 网络模式

为了让用户应用平滑地迁移至容器，比如一些传统应用或者监控应用需要直接使用 Host 的物理网络，也为了保障网络管理的一致性与网络性能的高效，我们选用了 Macvlan 网络模式。Macvlan 本身是 linux kernel 的模块，本质上是一种网卡虚拟化技术。其原理是在宿主机物理网卡上虚拟出多个子网卡，并分配独立的 IP 地址和 MAC 地址，把子网卡分配给容器实例来实现实例与物理网络的直通，并同时保持容器实例的隔离性。Host 收到数据包后，则根据不同的 MAC 地址把数据包转发给不同的子接口。在网络上看起来容器直接连接到物理网络，和物理机和虚拟机没有区别。Macvlan 共有 4 种模式，我们使用的是高性能的 Macvlan Bridge, 如下图所示：

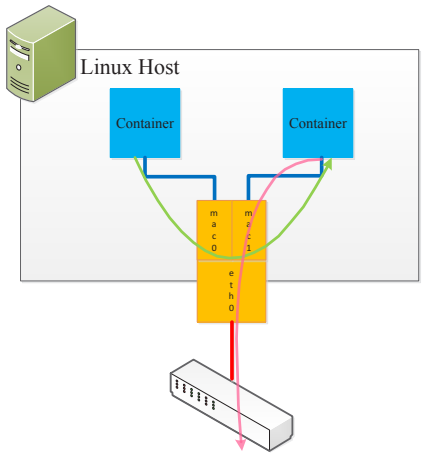


图 5 Macvlan Bridge

3.2 弹性伸缩

弹性伸缩是容器云的重要特性和业务场景。容器的封装性使其横向扩展非常方便，但是想做好弹性伸缩这还远远不够。比如要做到基于 CPU 和内存负载的弹性伸缩，不仅要做好容器的监控，还要配合负载均衡、灰度发布等功能，最重要的是弹性伸缩的时机，这里面有些是技术问



图 6 弹性伸缩

题，而有些需要根据不同业务做定制化处理。还有一点实践经验，善用 Kubernetes 的 Liveness 和 Readiness Probes 对增加应用程序的稳定性很有帮助。通过健康检查保障微服务之间的启动顺序，当应用程序准备好的时候，它们才会开始服务通信，这使得自动调度、滚动更新和弹性伸缩运行得十分顺利。

3.3 有状态服务

众所周知，因为容器本身的磁盘空间不大，而且容器的可写层数据在容器重启后会丢失，所以容器没办法很好地承载有状态服务，而是被广泛应用于无状态的服务。但是我们的容器云平台基于容器和容器编排技术，并结合分布式存储技术，有效支撑了有状态服务，比如容器化 RDS。其核心思想是计算与存储分离，将数据库运行于容器中，而将其数据在外部分布式存储中持久化。结合多种调度策略以及快照功能，可按需创建满足不同业务场景的数据库服务。

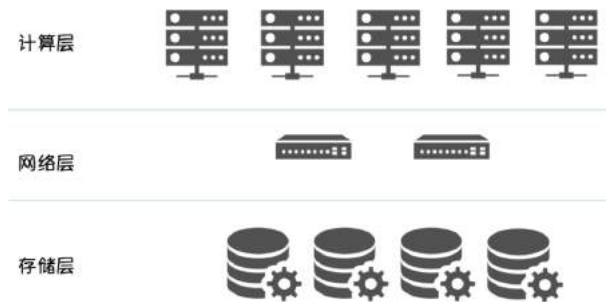


图 7 计算与存储分离

3.4 中间件市场

随着越来越多的应用系统相继建设，对一些公共中间件的需求越来越强烈，例如 redis、kafka 等等。同时这些中间件的运维工作也越来越繁重，申请底层资源、安装配置中间件、调试等繁琐、重复性的工作占据着中间件运维人员的大部分时间，容器化的中间件出现大大降低了中间件维护人员的工作量，无需关心底层资源和界面化的配置操作显著提高了中间件的发放效率。后续中间件的自服务是我们的努力方向。

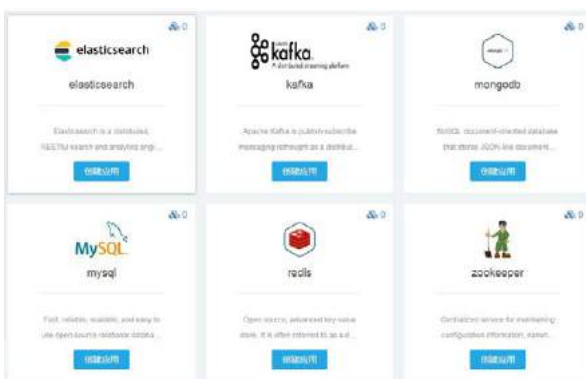


图 8 中间件市场

4 总结和展望

容器云平台在敏捷转型之下应运而生，也很好地支撑了 IT 建设的敏捷转型。开发、测试和运维人员通过容器云平台真正实现了高效协作，形成了 DevOps 的最佳实践。我们打算在后续的容器云平台建设上更多地考虑云原生的思路，推动以容器为中心的云原生生态，赋能金融科技发展。

海通证券 金融云思考与实践(下)

王洪涛、王朝阳、纪飞、魏勇、张真真 / 海通证券信息技术管理部

上一期《海通证券金融云思考与实践(上)》一文中讲述了 OpenStack 架构设计和多类型底层存储资源池相关的内容,这篇文章将会重点讲述海通金融云 SDN 实践、CMP 纳管异构资源池实现资源统一交付和海通证券金融云的未来规划等相关内容。



1 云网联动、融合业务 (SDN)

海通证券研发测试云一期项目中，金融云团队充分的使用并发挥了软件 SDN 的优势，为了进一步提升网络性能及管控能力，在研发测试云二期和生产云一期项目中引入了基于硬件 SDN 的网络架构，并与 OpenStack Neutron 组件对接，形成云网联动。

通过云平台对接硬件 SDN 控制器，云环境下的网络管理入口统一由 CMP 操作界面发起，用户对网络环境的创建、变更和维护均通过云平台驱动硬件 SDN 控制器完成，不但可以对金融云的网络集中管控，形成统一的操作视图，实现计算资源和网络资源的高效联动；同时网络管理员也可以在 SDN 控制器上查看业务访问视图、网络逻辑视图、物理连接视图，快速定位故障点，极大的提高工作效率。

1.1 SDN 部署模式：软件 SDN vs 硬件 SDN

根据 VxLAN 中 VTEP¹ 部署的形态不同，可以分为软件 SDN 和硬件 SDN 两大类：

1、软件 SDN：在软件 SDN 方案中，网络功能是通过软件层面的 Linux 协议栈以及相关的 vSwitch 技术实现的。它的优点是可以避免对硬件网络设备的过度依赖，同时降低了组网的成本。同时此方案的缺点也比较明显：1) 一是性能较低，由 vSwitch 负责 VxLAN 隧道的建立以及报文封装转发，VxLAN 网关转发性能低，同时会降低服务器业务数据的处理性能；2) 运维较复杂，vSwitch 与 Hypervisor 的操作系统耦合，网络故障定位困难，同时要求网络运维人员有较高的运维能力（比如精通 Hypervisor）。

海通证券研发测试云一期项目中采用了此种方案，业务和管理均采用万兆网络平面，随着云平台中租户逐渐增加（目前约 400 租户），对网络节点性能的要求也在不断提高。

2、硬件 SDN：在硬件 SDN 方案中，网络功能是通过专用的硬件交换设备与 SDN 控制器来实现的。SDN 控制器作为网络的大脑，对硬件设备进行策略的下发，将传统的各自为政的网络变为了一个整体，进行网络策略的灵活调配和控制。它的优点是 VxLAN 网关吞吐量高、时延低，用户操作简单，有更高可靠性和可扩展性的架构；而缺点是价格高、厂商锁定。

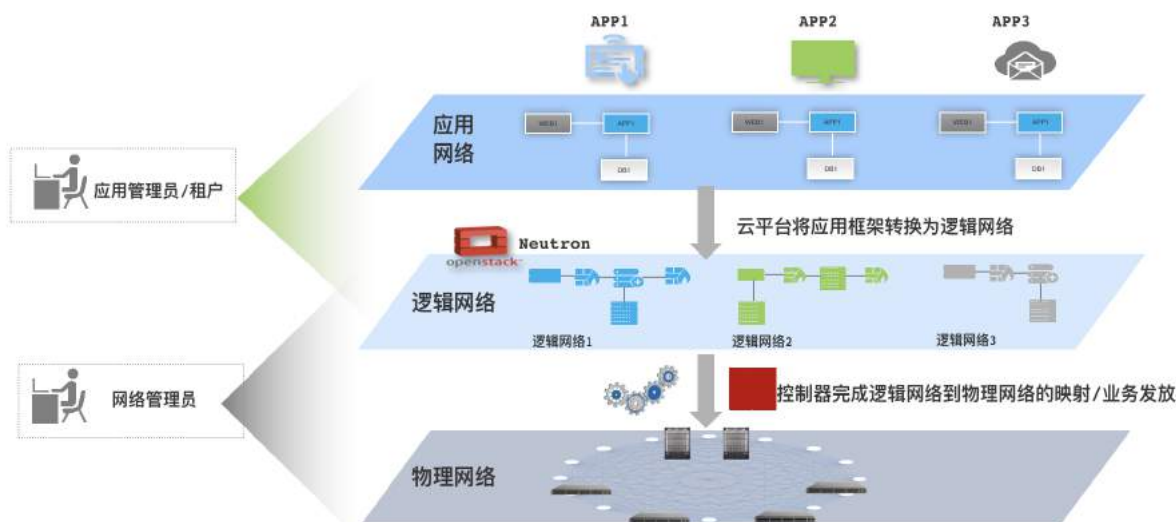


图 1：SDN 业务模型

海通证券研发测试云二期和生产云一期均采用了此种方案，通过与 OpenStack/CMP 集成，所有的网络业务都由 CMP 发起，然后调用 OpenStack 的 API 接口，把相应的网络业务转换为 SDN 控制器可识别的逻辑网络，最终由 SDN 控制器完成逻辑网络到物理网络的映射 / 业务发放。

1.2 硬件 SDN 物理架构设计

此次硬件 SDN 物理架构设计亮点较多，主要介绍以下几个：

1、分布式 VxLAN 网关：硬件 SDN 方案分为集中式 VxLAN 网关和分布式 VxLAN 网关，集中式 VxLAN 网关受限于网关设备的虚拟路由器的规格限制，无法满足大规模业务场景的扩容需求。分布式 VxLAN 网关的虚拟路由器是按需分布在不同的 Server Leaf 上的，组网规模不受限，容易实现平滑扩展。

2、VxLAN 控制层协议：利用扩展路由协议 MP-BGP EVPN 协议完成 VxLAN 控制平面的地址学习后，VxLAN 隧道会自动建立并自动关联。利用 EVPN 的 BGP RR（Spine 作为 RR 反射器）实现邻居发现，每个设备都通告自己的 VxLAN 信息，每个 VTEP 设备都有全网的 VxLAN 信息以及 VxLAN 和下一跳的关系。VTEP 设备会和那些跟自己有相同 VxLAN 的下一跳自动建立 VxLAN 隧道，并将此 VxLAN 隧道跟这些相同的 VxLAN 关联。相较于使用 OpenFlow 协议统一下发配置带来的优势有：1) SDN 控制器只负责下发服务策略，不下发控制流表，可靠性更高；2) 实现控制器与网络设备之间的松耦合，提供更高可靠性的 Fabric 网络；3) 标准化：控制面使用 EVPN，属于标准协议；4) 减少广播报文泛洪，地址通过 EVPN 自动同步。

3、M-LAG 部署：OpenStack 中所有节点都双归接入到两台不同的交换机设备上，当两块网卡处于负载分担模式时，为避免远端交换机设备

出现基于 VTEP IP 的 MAC 漂移问题，节点接入的两台不同交换机需配置唯一的虚拟 VTEP IP。使用 M-Lag 技术基础上配置虚拟 VTEP IP，实现流量一致性。M-LAG 技术可以在两台物理交换机上配置相同的 VTEP IP，但从管理面角度看两台设备依然彼此独立，可独立升级部署，进一步提高接入可靠性。

1.3 SDN 控制器对接 Multi-Region OpenStack

海通证券金融云支持 7x24 小时持续运行的业务应用，通过设计 Multi-Region 架构，使应用分别部署在物理隔离的两个 Region 里，从而业务实现跨 Region 级别的高可用。这就需要在物理的 SDN Fabric 中部署两套云平台，海通证券率先使用此架构设计，引领证券行业金融云发展的同时，也在多方面进行了创新。

1、对接标准 OpenStack（华为 SDN 方案）：SDN 控制器与 Neutron Server 进行对接：AC² Agent 通过 ML2 MetaData、L3 Plugin、FW Plugin、VPN Service Driver 和 QOS Notification Driver 等对接 SDN 控制器。AC Agent 北向通过 API 上报对象状态，AC Agent 南向通过 JSON RPC 和 SDN 控制器进行通信。

2、对接 Multi-Region OpenStack：传统方案下，SDN 控制器对接多个 OpenStack 云平台时，使用的是不同的 Keystone 组件进行对接。海通证券金融云项目的两套 OpenStack 云平台共用一套 Keystone 和 Dashbord 管理界面，用户使用同一账号系统进行认证，并对两个 Region 分别进行资源管理和使用。区别于传统对接方案，此次项目中，SDN 控制器专门增加租户多因子识别校验，用户登录云平台进行网络资源调度时，SDN 控制器不仅会识别用户的账户信息，还会额外识别业务租户所携带的 Region 标识，进而实现同一用户操作不同 Region 的网络资源时，

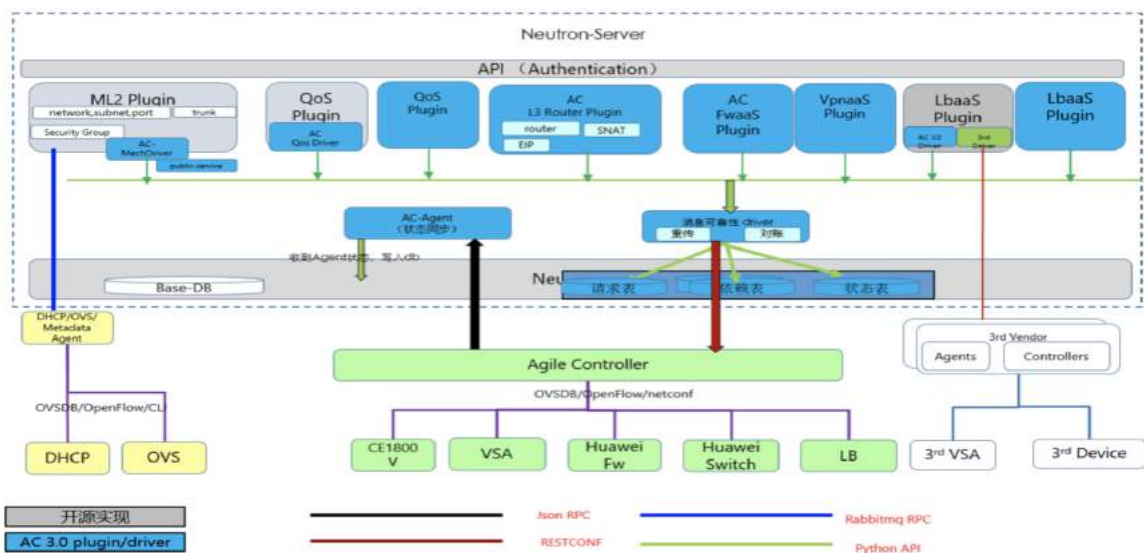


图 2：华为 SDN 对接标准 OpenStack 架构

配置编排正确下发。

3、多业务区域网络隔离：云平台内的多个业务区域（比如：互联网交易区、大数据业务区等等）可以按照需求实现计算物理隔离和网络物理隔离。

按照传统数据中心的习惯，多个业务区域是互相隔离的，不通区域之间的互访需要经过相应的防火墙。这样的隔离在 SDN 网络中是相对容易实现的，可以在 Spine Leaf 上扩展多对 Border Leaf，每一对 Border Leaf 上分别一个外部网关来服务于相应业务区域；也可以在一对 Border Leaf 上创建对多个外部网关来服务于相应的业务区域，两种方案各有优缺点，可以根据业务和后续的扩展方式不同确定。

4、FWaaS 实现防火墙策略自动下发：SDN 控制器纳管了 Fabric 内的防火墙，通过 FWaaS 和 OpenStack 云平台对接，用户可以直接在 OpenStack 云平台上给防火墙基于业务需求进行 NAT、IPsec VPN、安全访问策略等功能配置，进而可以在云平台上实现网络、安全、计算、存储资源统一管理。

1.4 硬件 SDN 提升海通证券金融云平台业务价值

海通证券金融云平台通过集成硬件 SDN 构建了一个弹性可扩展、敏捷自动化、稳定高可用、可智能运维的基础设施服务平台，从而提升云平台的业务价值。

1、弹性可扩展：打破了竖井式架构中网络对资源共享的区域限制，实现网络资源池整合与灵活共享；支持跨机房模块部署，服务器接入与物理位置解耦；优化数据中心内部各物理分区的划分，提高服务器、存储、安全等资源池化共享能力；支持多租户隔离，可以为不同的租户分配不同的网络资源。

2、敏捷自动化：将 OpenStack 所使用的网络平面通过逻辑网络映射到物理网络，并自动化完成业务语言到网络语言的转换和配置下发，动态调配整个数据中心网络资源与安全资源，让网络更敏捷地为业务服务；SDN 控制器通过网络服务、负载均衡、防火墙的策略自动部署和回收，实现服务器节点资源分配的动态绑定网络服务，

将很大程度上帮助网络工程师避免繁杂的手工操作，大幅提升网络运维效率。

3、稳定高可用：网络接入层使用 M-Lag 技术，可以在两台接入层交换机上实现服务器双归接入，但保留管理的独立性，可独立升级部署，消除网络接入层单点故障隐患；结合 SDN 控制器分布式集群部署和网络设备硬件全热备设计以及链路层的 ECMP 多路径负载均衡设计，稳定性进一步提升。

4、智能运维：物理网络和逻辑网络图形化呈现和管理，实现所见即所得；网络运行质量的关键指标包括丢包、时延、抖动等可视化呈现，实现网络风险提前预警，帮助运维人员及时规避网络重大故障。

1.5 实施过程中的经验分享

在金融云建设过程中，网络是最复杂也是关键的一部分，需要更深入的了解 SDN 的原理、软件技术细节和硬件的规格。

1、硬件 SDN 的规格问题：跨租户之间的互访是需要经过 SDN 防火墙的，每创建一个 VRF³，都会在 Border Leaf 旁挂的 SDN 防火墙中创建一个对应的虚拟防火墙；同时一组 Border Leaf 支持旁挂多组 SDN 防火墙，新建 VRF 时，SDN 控制器会随机创建虚拟防火墙到某一组 SDN 防火墙中。

至少需要考虑几个方面的规格：1) Border Leaf 支持的 VRF 数量；2) SDN 防火墙能创建的虚拟防火墙的数量；3) 一组 Border Leaf 能够外挂的防火墙数量等。不同级别的设备支持的规格大小不尽相同，而最终云平台能够使用的资源规格是一个综合计算的结果，这些需要根据云平台支持业务规模的大小来决定。例如：如果一对 Border Leaf 支持的 VRF 上限为 512 个，一组 SDN 防火墙能支持的虚拟防火墙数量为 100 个，而 Border Leaf 最多可以外挂 4 对 SDN

防火墙，则最终能够使用的虚拟防火墙数量是 400。

2、是否开启重启自动对账功能：重启自动对账功能的主要作用是：当业务正常下发时，一台 Server Leaf 因为故障导致了重启，此时策略只下发到了一组 Server Leaf 的一侧，重启之后，会以控制器数据为准，同步差异的策略。

优点是管理方便，差异策略自动同步；缺点是手动添加到 AC 的策略会被覆盖掉。如果开启此功能的话，尽量能够配合一系列的管理规定，比如：不允许手动添加配置等。

2 异构纳管、统一管理 (CMP)

在海通证券金融云的整体架构中，云管理平台 (CMP, Cloud Management Platform) 作为独立的一层而存在。这一层主要承担着异构纳管，统一管理的职责，具体来说，其职责可以分为以下几个方面：

1、作为海通证券金融云面对最终用户的门户，提供简单、一致、高效的云资源操作及管理的界面。金融云最终用户通过云管理平台可以获得标准的服务目录，通过自助服务平台自助高效的获取云资源，并对属于自己的云资源进行生命周期内的管理。

2、作为海通证券金融云建设规划及最佳实践的承载平台，将金融的整体规划以及使用云平台的最佳实践固化到平台内，让最终用户可以按规划、以最佳实践的方式使用云平台。

3、作为海通证券金融云运营平台的重要组成部分，提供面向最终用户的云服务日常运营（如计量计费、使用分析、报表汇总等）和面向平台运维团队的云服务日常运维（如监警告警、巡检、大屏展示等）。

海通证券金融云建设过程中持续投入资源，根据实际需要，经过两年的联合研发，并逐步形成具有自身特色的金融云云管理平台。

2.1 整体架构介绍

云管理平台处于 IaaS/PaaS 与最终用户之间，提供一系列的面向最终用户和平台运营方服务，整个云管理平台主要由以下几个部分组成：

1、基础设施对接层：该层完成对于底层 IaaS/PaaS 层服务能力的对接。目前，海通证券金融云云管理平台已经完成对基于 VMware 的资源池、基于 OpenStack 的资源池、以阿里云和腾讯云为主的公有云资源池的对接。

2、服务运营层：该层是云管理平台的核心能力所在，具体分为运营分析、服务运营以及自服务三个独立模块。其中，运营分析提供对被纳管的云资源的数量、利用率、成本等方面进行跟踪分析，并以丰富的可视化图标方式展示出来；服务运营则是提供给平台管理端来进行资源池规划设置，服务目录定义，配额管理等工作；自服务模块则面向金融云最终客户，提供服务自助申请，云资源自助管理等服务的。

3、基础管理层：该层主要提供云管理平台最基础的配置界面，具体包括用户管理、组织管理和工作空间管理。云管理平台管理员需要基于这些基础管理界面搭建出来整个金融云对外服务

的用户租户体系结构。

4、安全管理层：该层主要提供配合云管理平台使用而建设的安全管理能力，包括不同角色的操作权限，系统云资源访问的运维审计（即堡垒机）能力以及平台日志审计能力。

5、金融云门户：云管理平台的统一 UI 框架，按不同角色定义不同视角的门户界面，目前主要包括服务运营门户、自助服务门户和大屏展示等几个模块。

2.2 CMP 提升海通证券金融云平台业务价值

海通证券金融云的云管理平台具有多种核心能力可以提升云平台的业务价值，比如：异构纳管能力、资源池管理能力、自动化交付能力和运营支撑能力等。

2.2.1 异构纳管能力

异构纳管能力是云管理平台建设的一个基本能力，简单来说就是它需要提供一种机制可以快速对接不同的基础设施平台，同步基础设施平台的基本配置、存量资源，管理数据，并以此为基础对上支持平台的各种服务能力。目

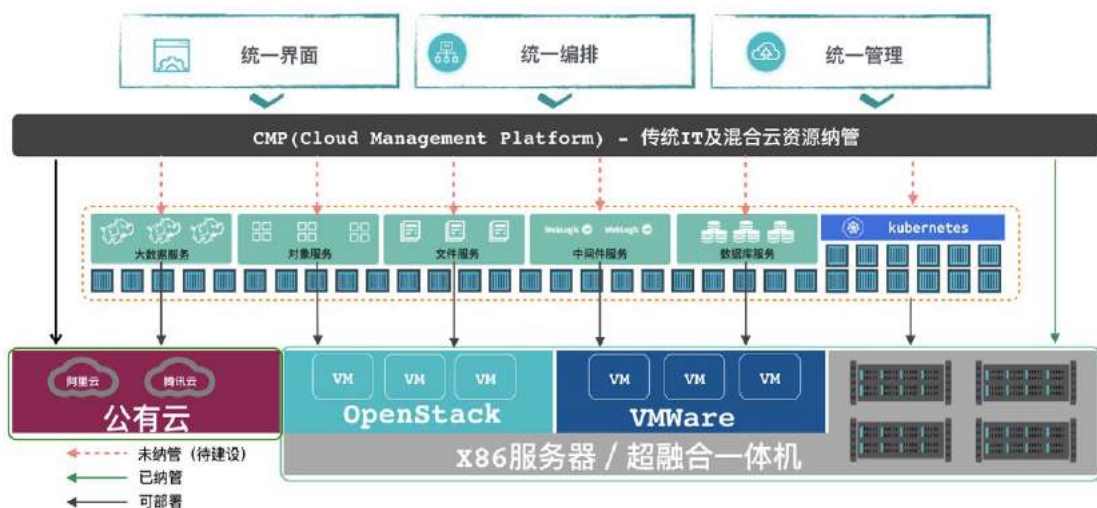


图 3：CMP 异构资源池纳管和资源统一交付

前，海通证券金融云云管理平台已经完成对基于 VMware 的资源池、基于 OpenStack 的资源池、以阿里云和腾讯云为主的公有云资源池的对接。以 OpenStack 环境为例，可以完成：

- 1、完成对于 OpenStack 物理层环境的感知和展示，获取物理层宿主机的列表、配置以及使用情况。

- 2、完成对于 OpenStack 上存量租户及资源的自动化发现，并提供将相关云资源纳管到云管理租户体系内，交付给最终用户的能力。

- 3、完成对于 OpenStack 上主机生命周期，网络以及存储资源控制面的对接，为通过云管理平台对其进行进一步操作提供基础。

为了保证云管理平台整体架构的稳定，实现云管理平台与 IaaS/PaaS 平台的解耦。当前平台中异构纳管能力的建设采用平台插件的模式进行开发。通过独立插件将不同 IaaS/PaaS 平台的异构纳管能力进行适配并对上提供一致的能力接口：1) 可以非常灵活的接入不同的 IaaS/PaaS 层的能力；2) 也可以向上屏蔽不同基础设施的差异。

2.2.2 资源池管理能力

作为基础设施资源的管理平台，资源池管理能力是其必备的核心能力。一般来说，云管理平台资源池管理能力需要支持数据中心资源的全生命周期，即规划阶段 (Day0)、部署阶段 (Day1) 和变更阶段 (Day2)。需要在云管理平台通过资源池的管理能力支撑以上三个阶段的日常运维管理的原因是：

- 1、金融云 IaaS 层不但需要关注标准基础设施服务层面的建设和交付，也需要关注使用 IaaS 层资源的业务规划，例如：不同网络区域支持不同业务，不同存储类型支持不同业务角色等。

- 2、要实现云资源面对最终业务用户全自助、自动化的交付，需要有一层平台能够将用户定义在文档中的各种业务规划“程序化”，可以在云资源最终业务交付过程中自动化获取并应用。

- 3、云管理平台处于最终用户和 IaaS 平台之

间，一方面可以通过 IaaS 平台的 API 灵活控制 IaaS 平台的配置、获取信息以及实施操作。另外一方面，云管理平台面对的最终用户为业务用户，可以关联和预配置好业务相关信息，从而在一个平台上具备“前”和“后”两端数据，从而有可能建立好兼顾后端平台实际和前端业务需求的资产池管理模型。

基于以上分析，海通证券金融云云管理平台引入了“逻辑资源池”的概念，并通过对于逻辑资源池的定义、使用和跟踪实现了云管理平台资源池管理的能力。具体来说，整个实现包括以下几个方面：

- 1、定义由计算资源和存储资源组成的逻辑资源池：通过 OpenStack API 读取当前物理资源池上计算和存储资源，并按资源池类型及 IaaS 平台的规划定义出逻辑资源池。

- 2、为所有逻辑资源打上相关的标签：这些标签包括地理位置、IaaS 平台属性、资源池级别、业务属性等，并将其向最终业务用户开放，供业务用户按实际需求进行选择，进而通过标签选择来定位出合适的逻辑资源池进行业务部署。

- 3、定义独立的网络资源池并与计算存储资源池进行关联：结合公司的实际情况，以 OpenStack 中 Floating IP 为代表的网络资源为例，预先为每个租户分配好网络资源池，与计算资源、存储资源相匹配，则最终用户则可以按照自己的需求自助服务（注：对应访问公网的业务，还需要按照公司规定走网络开通的流程）。

- 4、实现对不同组合逻辑资源池定向授权的能力：平台能够细粒度得控制不同业务组合可以使用的资源池，从而灵活为不同环境、不同业务场景授权合适的可选资源池。

通过以上逻辑资源池的建设，海通证券金融云云管理平台基本能够实现 IaaS 层物理资源的逻辑抽象，并在云管理平台对其进行细粒度的运营和控制，同时能够完全支持业务资源交付的完全自助模式。

2.2.3 自动化交付能力

云管理平台通过异构纳管能力完成和 IaaS/PaaS 平台的能力对接，可以通过 API 实现 IaaS/PaaS 层资源的创建、变更、查询和销毁。但是，IaaS 平台的 API 层仍然只能提供 IaaS 资源层面的管理，对于如云主机这样资源内部的管理和自动化仍然无能为力。而从业务角度看，业务用户希望对于云主机这样的资源能够提供“由外而内”的全栈自动化能力。因此，云管理平台一个重要的能力就是提供云资源的全栈自动化交付。

在海通证券金融云云管理平台中支持对云主机启动后的基础 OS 环境初始化，包括用户、密码、OS 安全加固、系统初始化等工作，也支持在云主机创建过程相关中间件的自动化安装或者初始化，包括如对于 DB2、Oracle 的自动化安装部署。

除此之外，全栈自动化交付能力还体现在对于很多常规长流程操作的封装和自动化，以业务租户的全流程初始化为例：当用户需要为一个业务申请一个独立租户并服务业务，在 IaaS 平台上需要做的工作内容较多且有一定的技术门槛，云管理平台可以将这个初始化流程标准化并全自动化的完成，将用户开启使用金融云的门槛大幅度降低；海通证券金融云业务租户全流程初始化

（由云管一键自动完成）包括 IaaS 租户创建、用户资源池授权、默认私有云网络创建、默认私有网络路由器初始化、分配路由器 Floating IP、配置租户防火墙等。

自动化交付能力与逻辑资源池相结合，则会衍生出来更为强大的服务能力，实际业务中集群化部署（比如：数据库主-备节点部署）环境需要指定不同主机的放置策略，云管理平台在逻辑资源池层面提供了放置策略能力（集中放置、均衡放置、指定放置），这样，云管理平台就可以在一次批量资源申请中将多台机器按用户选择的放置策略进行跨资源池放置。

3 持续创新、引领发展

海通证券金融云建设的过程中，通过实施 Multi-Region 架构、集成 SDN 控制器、提供多种类型存储资源池完成多项行业内云计算方案的创新应用。

后续还会持续进行比如容器云平台建设、DevOps 实践、应用微服务化等多项创新，从而能够进一步引领云计算技术在证券行业的应用和发展。

参考文献：

- 1 VTEP(VxLAN Tunnel End Point): 为 VxLAN 隧道的端点，封装在 NVE 中，用于 VxLAN 报文的封装和解封装，形态可以是物理交换机，也可以是虚拟交换机，如：Open vSwitch。
- 2 AC(Agile Controller): 华为的 SDN 敏捷控制器。
- 3 VRF(Virtual Routing Forwarding): VPN 路由转发表，也称 VPN-instance (VPN 实例)，用于隔离路由表，实现虚拟路由的。

金融科技在国内外券商PB业务中创新实践与思考

邓维 / 招商证券股份有限公司

邓维，博士，现任职于招商证券托管部，曾任职于中国证券登记结算公司、长江证券股份有限公司。

邮箱：foreverdengwei@163.com，手机：13927415060。



金融科技是指由技术创造的金融创新，它通过变革业务模式、流程、应用或产品，以创新金融机构、金融市场或金融服务的提供方式²。在金融科技浪潮下，以移动互联网、云计算、大数据、人工智能和区块链为代表的前沿技术迅速渗透金融机构各个领域，其中证券行业更是方兴未艾。大型证券公司（本文简称券商）纷纷将“金融科技”作为战略性业务或核心竞争力在公司战略中进行描述。然而，券商金融科技大多应用在零售经纪

业务^[1]。其实，主券商业务（Prime Brokerage，简称PB），作为券商的一项机构业务，是指券商为专业投资者提供交易结算、资产托管、后台运营、研究支持、杠杆融资、资金募集等一站式综合金融服务，早已真正将金融科技应用到实践中解决实际问题并获得巨大效益的业务³。由于国内通常以基金托管与运营（外包）服务业务作为PB业务的鉴定标志，因此本文以基金托管与外包服务为主详细分析券商PB业务的金融科技实践。

1 金融科技是券商 PB 业务核心竞争力

随着以私募基金为代表的机构投资者快速发展，PB 业务成为券商“朝阳业务”，预计 2018 年 PB 业务收入可达券商总收入 10%^[2]。PB 业务运营和业务创新的前提和结果均在于技术系统的落地与支持。金融科技能力是券商 PB 业务提高核心竞争力的驱动力⁴。

1.1 技术系统支撑 PB 业务生存环境

券商 PB 业务涉及的投资交易、份额登记、估值核算、投资清算、投资监督、基金销售等业务环节也都是通过专门的系统来完成。PB 业务每日需处理机构客户上百万笔投资交易和上万项业务流程，依靠人工几乎不可能完成。随着监管法规不断颁布，创新业务不断推出，以及私募基金个性化需求不断丰富，PB 业务的支持、创新、改革都需要依靠技术系统的提质增效和升级完善来完成。

1.2 金融科技突破 PB 业务发展难题

券商 PB 业务发展面临最大的问题就是大规模化产品运营与客户个性化需求满足之间的矛盾，导致业务人员运营负荷巨大。由于人力成本高昂和专业人士匮乏，采取“人海战术”来满足 PB 业务需求的外延式粗放型发展模式已难以为继。目前行业已形成普遍共识，金融科技成为券商化解 PB 业务发展瓶颈制约因素的唯一出路，即采取内涵式集约型发展路线，构建先进的科技系统方案、科学的业务流程来提升效率。

1.3 金融科技推动 PB 业务战略创新

金融科技能力已成为衡量 PB 行业创新发展水平的一个重要标志。在面对逐渐饱和的市场和日益

激烈的竞争，大型券商纷纷提出“依靠科技扩展服务边界”的 PB 业务发展战略。例如，如果确立国际化 PB 发展战略，那么就必须在技术系统方面建设全球资本市场信息管理能力和外币管理功能等。大数据记录了历史信息与风险偏好，云计算提供了关联交互、深度学习和精准挖掘，人工智能具有强大的数据分析与计算能力，而区块链、量子等技术不断刷新行业想象极限，由此券商可以充分运用金融科技提供增值服务和创新业务发展。

1.4 金融科技树立 PB 业务品牌声誉

既然金融科技是券商 PB 业务生存、发展与创新的核心驱动力，那么金融科技自然将构建券商 PB 业务服务品牌。而良好金融科技的知识产权保护工作将是实现 PB 业务品牌和声誉持续优势的保障。目前券商的 PB 业务核心系统以直接购买模式为主，该模式极容易导致技术系统落后于业务发展创新，而且行业创新迅速被“复制和趋同”。因此，金融科技创新应用及其知识产权保护程度成为 PB 业务差异化竞争力度的保障。

2 国内券商 PB 业务金融科技创新实践

国内不少先进券商已通过金融科技实践为客户“募集、投资、管理、退出”等全生命周期提供高效优质 PB 服务。

2.1 销售募集

2.1.1 适当性管理

基金募集环节是风险高发“地带”。目前券商均在基金销售系统中增加了适当性管理模块，按照监管法规要求、应用金融科技自动贯穿基金销售售前、售中、售后环节全流程合规管理。在售前了解客户环节，通过对接公安身份证接口对身份证要素进行认证，同时对接最先进的人脸识

表 1：国内券商 PB 业务金融科技实践一览

业务环节	业务场景	金融科技	代表券商
销售募集	适当性管理	人脸识别技术和活体检测技术，移动互联网和云计算技术，大数据分析	全证券行业要求
	电子合同签约	CA 认证，人脸识别，生物识别，移动互联网，RSA/国密算法，区块链技术	中信证券、国泰君安证券、海通证券、华泰证券等
投资交易	极速交易系统	内存数据库技术，并行计算，高速通信技术	国泰君安证券、华泰证券、海通证券、兴业证券等
	量化交易系统	大数据分析技术，云计算，金融工程	国信证券、第一创业证券、恒泰证券等
	智能投研	人工智能，机器学习，大数据分析，自然语言处理，知识图谱	各家券商零售体系均有涉足，但机构客户服务仍在探索中，如中信证券
	智能 PB 管家	大数据分析技术，智能图像容错识别，移动互联网，云计算	恒生、迅策等正在与券商洽谈合作模式
运营管理	智慧运营平台	互联网技术，移动互联网技术，STP（Straight Through Processing）技术	招商证券、国泰君安证券等
	自动化估值	STP 技术，自动化技术	招商证券、国泰君安证券、申万宏源证券等
	电子指令平台	互联网技术，STP 技术，自动化技术	招商证券、广发证券、国泰君安证券、国信证券等
	绩效分析	大数据分析，金融工程	招商证券、国泰君安证券、中信证券、长江证券等
	区块链服务平台	区块链技术	未有实践，招商证券、长江证券等在探索
清盘退出	投后管理	-	通常为管理人自建使用

别技术和活体检测技术，防御各类非真人和人脸攻击；在售中录音录像环节，采用领先的音视频录制技术、移动互联网和云计算技术，支持现场、离线和远程等多种场景，支持手机、平板等多类平台；在售中投资者信息动态管理环节，通过建设投资者适当性评估数据库，即时调整、更新风险评估标准和程序，自动实现风险动态匹配。

2.1.2 电子合同签约

在基金募集过程中，基金管理人、托管人（如有）和投资者需要签署基金合同 / 公司章程 / 合伙协议。目前行业通常是采用线下、纸质、当面签署的方式。然而，这种方式存在“萝卜章”、“阴阳合同”等合规风险和反复寄送、多方轮流签字、扫描等繁琐程序，以及高昂的印刷邮寄费用和合同档案管理成本。2018 年 8 月 16 日，中信证券联合中证机构间报价系统的电子签约平台完成首单电子签约私募基金产品已在中国证券投资基金业协会备案成功，推动我国私募基金进入

电子签约时代⁵。该平台支持机构签署方使用有认证证书的 U-Key 通过网页平台登录进行签署，支持个人签署方使用手机 APP 通过实名认证比对、人脸识别、生物识别等技术进行身份识别和签署。该平台有金融安全级保护：依照金融级安全架构规范，采用中国金融认证中心权威证书，通过 RSA/ 国密等高安全性算法，利用区块链技术确保所有签约数据完整性、准确性及不可篡改性。由此，电子签约方式实现了私募基金募集签约合规化、提升了运营效率、节省了成本。

2.2 投资交易

2.2.1 极速交易

随着创新业务不断推出、程序化交易模式的快速发展，而监管和风控更加严格，尤其是当账户数量较多、风控数量增加时，交易系统的指令、委托延时比较大，已经满足不了客户需求。以私

募基金、信托计划为代表的机构客户对券商 PB 交易系统的性能和稳定性提出了新的要求。因此，不少券商将 PB 交易系统升级为极速 PB 交易系统。极速交易系统采用全内存数据库技术，配合全新的数据通讯机制、多线程并行技术，实现所有业务流程处理均在内存中进行，极大提高了委托确认、成交，以及事前、事中风控的效率。

2.2.2 量化交易

量化交易在欧美等成熟资本市场已经发展近四十年，已成为对冲基金的主要交易手段，交易量占全市场交易量五成以上。而国内量化交易还处于起步阶段。随着私募基金兴起，不少券建设量化交易平台和工具，抢占量化交易型私募基金市场。“科技创新精品券商”第一创业证券的 PB 业务突破口则是量化基金。第一创业证券整合公司在衍生产品研究和量化交易方面优势和条件，于 2016 年作为行业首家推出量化交易平台 MultiCharts Trader，该平台支持全市场实时条件扫描选股、高级图表分析及画图下单、高阶运用的策略编程及自动交易和大数据策略回测与参数优化等高端特色功能。目前第一创业证券 PB 业务中约 50% 的产品规模是量化私募基金类型^[2]。此外，恒泰证券针对量化交易的业务特性，全新打造 U- α 量化极速交易系统，重构了传统的业务流程，全新开发市场上唯一带风控的极速交易接口，更适用于量化交易低延时、大并发的特点⁶。国信证券也联合美国 TradeStation 交易平台为交易型客户实现各种策略交易，该平台部署云端，用户可以用手机监控实时成交情况⁷。

2.2.3 智能投研

传统金融机构仍高度依赖人工搜索资料、处理信息及后期跟踪等投研流程，存在搜索途径不完善、数据获取不完整且不及时、人工分析研究稳定性差、报告呈现时间长等问题。智能投研不仅能改变人工接收和处理信息的深度和广度，快速挖掘数据和资讯，并通过智能搜索、自然语言处理、知识图谱、智能估值等实现信息向决策的

高效转化。目前包括中信证券、招商证券、国泰君安证券、海通证券等多家券商均与专业机构合作推出智能化投研和投顾服务，帮助分析师提高处理信息、快速挖掘投资线索，提供策略的分析和优化建议⁸⁹。但是，大多券商主要停留在初步阶段，而且主要还是面向零售经纪业务。

2.2.4 智能 PB 管家

机构客户通常管理多只产品，而由于资金需求、托管需求、投资经理指定等多种因素，所有产品分布在多家券商，导致机构同时使用十几家 PB 交易系统进行交易，而且投资经理或投资顾问通常通过邮件方式发送投资指令，由此导致日终需耗费大量精力、人力、物力来手工汇集每家 PB 系统中指令执行情况和交易数据，以形成统一的报表上报给投资经理、投资总监用于投资分析等。而且机构产品的二级市场数据分布在多套 PB 系统中，而场外数据在自建交易系统或非标准化交易文件中，由此导致产品系统风控失效，只能人为手工计算。为此恒生、迅策科技等软件服务商打造智能 PB 管家，解决多终端的资产数据整合管理、电子化指令流管理和联合风控问题，协助券商开展差异化主经纪商业务的创新服务模式，为机构客户量身打造多系统、跨系统综合管理服务，开拓人机结合、大数据应用新场景。

2.3 运营管理

2.3.1 智慧运营平台

作为国内众多专业机构投资者的首选主经纪商，招商证券为机构客户打造出业内领先的托管综合金融服务平台，并荣获第六届证券期货科学技术奖三等奖¹⁰。其率先开创了私募基金管理人与托管外包机构之间的交互业务线上化，极大地提高了管理人的运营效率，降低了业务操作风险，在行业内形成了重要的示范效应。其从管理人的实际使用场景 / 角度出发，基于私募基金产

品的“募、投、管、退”全生命周期管理，建立和完善了托管外包业务运营流程和体系，通过科技手段打造的人性化服务平台和推动服务的专业水准。类似地，国泰君安证券为顺应市场需求和监管要求，推进中后台运营创新、完善运营管理体系，推出的“面向未来、智慧运营”的一站式全天候基金运营平台，并载入基金业协会《中国证券投资基金业年报（2015年）》¹¹。该平台覆盖产品管理、账户管理、资金划拨、估值运营、TA运营、基金绩效分析报告、个性化报表、向投资者披露信息、信息披露报告、星期五公开课等全部业务线上办理。该平台的直通式处理方式，极大提升业务办理效率和信息传递效率，资金划拨、估值查询、TA交易等业务运营层面实现了从管理人发起到后端处理的“秒办”。国泰君安证券也是首家推出“微信版管理人服务平台”移动办公，把产品运营装进口袋，用户可实时监控业务办理进度，操作流程清晰可见，后续业务操作流程全透明。

2.3.2 自动化估值

估值核算是资管产品日常运营中最为核心的环节。在资管行业尤其是私募基金行业快速发展的同时，估值核算工作日益繁重、人力成本持续攀升。行业各大券商均在探索如何解决估值效率与成本问题。招商证券、申万宏源证券等券商均通过重新梳理流程、整合系统资源将估值数据准备、数据处理等工作自动执行，构建了一套自动化估值解决方案——估值机器人，使估值人员能够从繁重枯燥且低价值的事务中解放出来。由此，基金会计的主要工作将转移到产品设计和对账处理等关键环节，从而达到提升工作效率，降低人力成本，提升准确率的目标。

2.3.3 电子指令平台

目前大多托管券商与机构客户之间的资金划付交互仍然是通过纸质指令和邮件电话的方式完成。当管理几十只产品、面对几百张指令时，客户运营效率和体验极差。为此，招商证券、国泰

君安证券、广发证券等券商推出一套安全的、便捷的、实时在线的电子指令服务平台，实现各类划款指令电子化，高效解决管理人日常资金业务，包括保证金、场外投资、费用支付、TA类划款、头寸管理、流水与余额查询，以及其他业务资金划转处理。同时，电子指令服务平台通过STP直通式处理模式，与投资监督、投资清算、估值核算等系统进行联动业务处理，加强了资金使用的安全性和服务的便捷性、自动化，并配套提供微信服务，提升业务响应和运营效率¹²。

2.3.4 绩效分析

机构客户具有分析投资运作情况、辅助投后决策分析、研究大类资产配置和展示产品投资表现等诉求，而难以获取所需的基础数据，并且绩效分析系统构建和运维成本高昂。为了解决机构客户这一痛点，招商证券和国泰君安证券等大型券商均推出自建的绩效分析系统，利用规模效应优势免费地为客户服务，客户可享受定制化的、全在线敏捷自助、多维数据分析、直通可视的服务体验¹³¹⁴。绩效评估分析内容包括总体总体情况，净值走势、收益表现、风格特征、收益分布等收益分析，夏普比率、回撤率、换手率、Alpha、Beta、VaR等指标分析，股票、债券、现金等各类资产配置情况、股票行业和个股的分布情况，Brinson分析选股和择时能力、仓位管理能力、资产配置贡献、行业归因、风格归因等等。

2.3.5 区块链服务平台

由于PB业务涉及众多参与方，参与主体间的信息交互并无统一平台，多方的协作存在信用校验难、信息严重不对称、运营成本高、运营风险高和行业监管困难等一系列困境。区块链技术的产生为实现信息信任与共享、提高各机构运营效率、提升客户服务体验、满足全面监管的新型PB业务生态系统提供了技术支撑和解决思路。据公开报道，个别券商正在尝试用区块链的方法管理智能合约，解决合同签署与管理问题和PB业务的综合服务与监管平台^{15[3]}。

2.4 总结分析

机构客户产品在清盘退出阶段，需要特别服务的主要是股权类产品的投后管理，券商目前涉足较少，而券商可提供撮合服务和投行服务，协助其退出。

通过以上分类分析，券商 PB 业务应用金融科技的场景主要是在追求速度、效率、安全、智能等方面，而应用金融科技较为成熟的通常都是 PB 业务发展较好的大型券商或者具有特色业务的中小型券商。这进一步验证了金融科技可以为券商提质增效、优化服务，而且大型券商由于资源、人才、客户等优势，已经将金融科技应用到实践中解决实际问题获得巨大效益，进一步夯实了金融科技能力，提高了 PB 业务竞争壁垒。

3 国外 PB 服务商金融科技应用经验

PB 业务起源于欧美，而国外 PB 服务机构历来重视科技的投入，从技术层面保证业务合规性和良好用户体验。

3.1 高盛集团

作为国外最大的 PB 服务机构，高盛对技术和创新的坚定承诺，引领其开发出许多如今已成为行业标准的作法及技术。高盛一直是电子交易和连接系统方面的先锋，其电子交易平台 REDIPlus 在交易前分析、增值的执行服务、算法交易、组合交易方案及交易后分析方面具有全球领导地位。其中，高盛算法交易（GSAT）是一组涉及全球多种资产的算法程序，包括股票、期货、合成衍生工具和期权，通过与 GSAT 进行交易，客户还可获得高盛的各种资源，包括交易前后及交易期间的分析、交易成本分析和执行策略¹⁶。

除了交易工具外，高盛在各项业务上均大力运用科技促进业务创新发展。在外汇和衍生品交易方面，高盛独创和专有的数据建模技术使客户在投资组合基础上计算保证金，从而高效管理风险及优化资本运用，而且高盛内部技术平台简化了交易确认、组合对账和管理。在托管结算方面，高盛开发了功能强大、范围广泛的全球结算与交收网络。高盛的平台提供了一套完整的工

表 2：国外 PB 服务商金融科技应用一览

PB 服务商	业务应用场景	金融科技
高盛集团	电子交易平台 REDIPlus	互联网技术，STP 技术，大数据分析技术
	算法交易 GSAT	
	外汇和衍生品交易，数学建模技术实现高效管理风险及优化资本运用	
	托管结算，提供功能强大、范围广泛的全球结算与交收网络	
	融资融券，采用技术模型评估客户投资组合和策略的融资方案	
	机构客户网与综合报告平台	
盈透证券	智能交易系统 SmartRouting	STP 技术，自动化技术
	程序化交易编程接口	-
	外汇掉期自动化交易	STP 技术，自动化技术
	全球资产配置平台 Investors' Marketplace	互联网技术，搜索技术
道富银行	全托管服务平台	云计算技术
	直通车式电子指令系统	SWIFT，STP，互联网技术
	流程化会计估值	STP，自动化
	基于区块链的证券借贷方案等	区块链技术

具，允许客户在一个单一的综合账户里跨越多类资产和货币交易。在融资融券方面，高盛运用专有的、采用前沿技术的投资组合风险建模工具，评估客户投资组合和策略的融资方案。在报告服务方面，高盛机构客户网可让客户在线获取高盛的全球在线资源，包括交易理念、投资机会、市场洞察、个性化的投资研究及其它资源。同时，高盛开发了一个可定制程度高的综合报告平台，向客户提供度身定制的涵盖众多产品和市场的业务解决方案。

3.2 盈透证券

盈透证券（Interactive Brokers, IB）是一家以低交易成本和“技术驱动业务”而知名的美国网络券商，机构和个人客户各占一半。PB 业务是 IB 近年来快速开拓的领域。IB 在 PB 服务方面具备两项核心竞争力：一项是 IB 研发的 IB SmartRouting SM 智能交易系统，另一项则是 IB 在成本控制上的绝对优势，IB 可以选择免费为客户提供托管服务^[4]。

受 Basel III、MiFID II 等监管政策的影响，高盛、摩根士丹利等银行控股的主经纪商受到严格的流动性管理约束，被迫抬高客户准入标准和服务定价。IB 则接纳了大型主经纪商不愿服务的对冲基金，同时也吸引了一大批费率敏感型的客户。由于具有出色的技术储备和规划，在面对诸如 MiFID II 等监管新规时，不必被迫进行全面技术升级和增聘一批新员工。IB 为客户研发了一套智能交易系统——IB SmartRouting SM，通过算法寻找全市场最优的价格完成交易。SmartRouting 通过技术手段替代人工化操作，并融入到各个业务流程中改造成自动化的工作流程，从而能极大降低成本。由此，IB 在成本控制上具有绝对优势，进而实现不对客户提出最低管理规模或收入贡献的要求。

此外，IB 拥有一套支持 C++、Java 以及 Python 等语言的编程接口，主要服务于程序化

交易客户。IB 还推出了一套外汇掉期自动化交易程序，使客户以更合理的价格持有外汇头寸。为了满足对冲基金希望只通过一个平台便可以触达全球市场的不同资产，IB 开发了 Investors' Marketplace，为那些配置对冲基金的机构提供搜索工具，该平台上目前有 2911 只对冲基金。

3.3 道富银行

全球金融服务巨头美国道富银行公司一半以上的收入来自于托管业务，覆盖了全球 15% 的资产管理机构。其核心竞争力来自于 IT 实力和先发优势。道富集团每年经营费用中的 20% 至 25% 投入科技方面，在 IT 上的投入每年超过 10 亿美元^{[5][6]}。

3.3.1 全托管服务平台

高盛 PB 业务已开发出领先的前后端全球性技术平台，从而使客户能够在高度自动化的操作环境下管理业务。在 2014 年初，基于私有云技术的全托管服务平台上线。该平台按照分层模式进行架构，分为客户渠道、员工渠道、外部机构直连渠道以及内部产品服务层、数据分析层。在服务层中，包含了核心服务组件、投研与产品组件、客户关系组件、销售与 TA 组件、服务与咨询组件、交易管理组件、财务估值组件、场内管理组件、银行间处理组件、期货处理组件、场外处理组件等。根据不同使用部门需求，全托管平台将组件按需配置出适用于不同业务场景的服务^[7]。此外，道富银行官网 my.statestreet.com 作为客户服务平台的一部分，具有丰富的报表服务，可提供的托管运营报告内容包括：持仓报告、应收应付账款、现金交易报告、投资组合申购赎回报告、变现收益及亏损报告、外汇买卖报告及各种收入报告。用户可以自定义报表格式、种类、产生要素、产生时间以及组合搭配各类报表，从而在信息披露中全方位的实现了电子化和信息化。此外，除了托管运营服务报告外，该平台也提供绩效评估、

投资管理人服务、证券借贷等增值服务和报表^[8]。

3.3.2 电子直通式运营

高效运行的系统可以大大提供 PB 业务运营的工作效率，并且降低人工操作的差错率。在交易抓取和监控工具方面，道富银行的环球交易管理（Global Transaction Management, GTM）可以便捷地接受电子交易，而图像管理和全球直通式（Image Management and Global Entry, IMaGE）可以识别图像并转换成电子交易，交易由接收者授权后直达次托管行系统，由次托管行进行交割处理^[8]。在指令处理方面，道富银行托管部使用直通式电子指令系统替代低效、易出错的纸质指令。该系统使用国际通用的 SWIFT MESSAGE 系统，指令随时可以通过系统直通式自动化传输处理，托管人可以实时收到指令而不会产生延误。在流程化会计估值方面，道富银行建立有数据质量检查中心，通过跨供应商的数据比对检查数据正确性，然后，指令接收人员需要验证客户或投资经理提供的指令是否有效，最后在净值产生与核对过程中严格执行“基金会计 - 复核 - 初级经理 - 高级经理控制审查”全流程^[8]。

3.3.3 区块链技术应用探索

道富银行一直是金融科技的拥趸者，不仅是区块链平台超级账本（Hyperledger）的创始成员之一，也是比特币交易所交易基金（Exchange Traded Funds, ETF）的支持者。道富银行成立了“新兴技术中心”，该中心 70% 项目与区块链技术相关^[7]。其中，基于区块链的证券借贷方案已经进入测试实施阶段。该方案的主要目标是提高证券借贷的操作效率。此外，道富银行正联手加利福尼亚州区块链创业公司 PeerNova 合作开发了另一个区块链项目，用于跟踪投资交易中的资金去向。

3.4 总结分析

虽然国内外 PB 业务金融科技发展路径和范

围类似，但是国外 PB 业务金融科技应用深度和引领性，尤其是交易风控、投资报告和直通式处理等方面，值得国内借鉴学习。

4 国内 PB 业务金融科技发展问题与建议

虽然国内外大型 PB 服务商均已具备一定的金融科技能力，但是由于 PB 业务发展历史较短、不够成熟，仍存在科技滞后于业务、同质化严重、服务深度不足、把控力不强等问题，尤其是中小型 PB 服务商还存在不具备金融科技能力问题。

4.1 存在问题

4.1.1 科技滞后于业务

大部分中小券商开展 PB 业务时，基础设施通常处于“一穷二白”状态。技术系统规划和建设滞后于 PB 业务的快速发展，导致系统的改造升级较为被动、疲于应付和较为艰难满足客户需求。

4.1.2 科技同质化严重

PB 业务严重依赖于信息技术系统，而行业大多券商是购买恒生等少数几家供应商的系统，近似“垄断”的格局导致券商的系统同质化严重，束缚了券商的产品设计和创新能力，偶有系统创新也迅速趋同，最终导致同质化的产品、服务。

4.1.3 科技服务深度不足

金融科技在 PB 业务的应用场景较为单一，主要集中在交易、托管等业务场景，极少券商在金融科技应用在绩效分析、资产管理、合规风控监测、投资报告、客户服务等打造券商长期竞争力的领域。

4.1.4 科技把控能力不强

大多券商在 PB 业务上没有 IT 长远战略规划，IT 投入采用“随大流”策略，金融科技应用大多依赖外部开发商完成，甚至在信息技术基础薄弱的条件下为实现弯道超车而盲目追求流行技

术，风险隐患巨大。

4.2 发展建议

4.2.1 提高 IT 战略定位，引领 PB 业务发展

金融科技应上升到公司发展的战略层面。券商应从战略规划的角度形成切实可行的 PB 业务技术方案，充分发挥战略引领作用，同时应加大科技方面投入。例如，高盛宣称自己是一家科技公司，公司 25% 的人员为技术人员，将科技能力作为公司的核心资源，认为“技术引领业务”^[1]。

4.2.2 践行直通式理念，构建穿透式监管

虽然国内外先进 PB 服务商已采用 STP 方案，但是由于 PB 参与方多、业务环节多、涉及系统多，STP 程度还需进一步深化，实现一站式处理前台（销售、交易）、中台（风险管理、客户服务）、后台（估值、登记结算）各业务环节，无缝对接内外部系统，实现管理的整体化和统一化。此外，金融科技降低了券商的经营成本、提高了效率，但也加速了风险的传播，为风控合规、监管提出了较大挑战，传统的风控合规、监管方式在金融科技应用方面变得苍白无力，利用金融科技构建“穿透式”的合规风险、综合监管变得越发重要和必须。

4.2.3 科技挖掘特色服务，数据驱动智能运营

在存量市场竞争阶段中品牌、体验和服务是

避免同质化竞争关键。金融科技拓展了券商 PB 服务的方式、广度和深度。券商依据自身资源禀赋和优势，技术驱动竞争，挖掘特色服务是取胜之道。例如，利用人工智能技术提供智能营销服务，利用云计算和大数据分析技术提供投资咨询和分析报告服务，利用大数据和人工智能技术提供风险管理、智能预警和 FOF 投顾筛选服务，利用区块链技术实现共识和无差错交互服务等。券商在开展 PB 业务中积累了大量数据，数据除了可以提供大量增值服务外，还将驱动电子化自动化智能化运营。花旗集团便强调实施数据为先文化，除实现了商业效益，也充分运用到平台建设、业务流程优化、风险控制，以及内部运作、内部协同等领域。

4.2.4 丰富科技建设模式，构建行业生态圈

目前券商 PB 业务科技建设通常是以“自主项目管理”+“外包设计开发”为主，以“联合开发”为辅的粗放式开发管理模式，亟需提升自主掌控能力和持续创新能力。国外 PB 服务商除了自身 IT 实力强大外，还与金融科技等企业开展合作，也会通过投资、收购的方式加快提升自身的金融科技实力。国内券商一方面应加强自主设计和开发力量，另一方面可以采取收购、投资金融科技相关企业的方式，或者组建行业联盟，快速实现金融科技能力提升。

注释：

1 本文仅代表作者个人观点，与供职机构立场无关。本文信息均来源于公开渠道。

2 杨涛《金融科技创新需要厘清思路》，中证网，时间：2018-08-17，网址：

http://www.cs.com.cn/sylm/zjyl_1/201808/t20180817_5859448.html，最后访问日期：2018 年 9 月 8 日。

3 参见《招商证券董事长霍达在 2018 年第四届西湖峰会发表主题演讲》，招商证券微信企业号，时间：2018 年 5 月 21 日，最后访问日期：2018 年 9 月 8 日。

4 参见《筑牢基金托管机制 守护投资者合法利益——钟蓉萨副会长在招商银行托管大数据平台发布会上的讲话》，中国基金业协会微信公众号，时间：2018 年 7 月 13 日，最后访问日期：2018 年 9 月 8 日。

- 5 侯捷宁：私募基金进入电子签约时代 首单签约业务完成，证券日报网，2018年8月16日，网址：http://epaper.zqrb.cn/html/2018-08/16/content_336713.htm，最后访问日期：2018年9月8日。
- 6 参见《2018 证券行业创新大奖此刻揭晓！》，恒生官网，时间：2018年8月21日，网址：<http://www.hundsun.com/newsinfo.aspx?id=31ee1a38-f971-4523-9661-0a975dd76b76&sid=15bf3478-809a-4e13-a566-1c18610ebbc4&cid=eab7d121-0401-4174-95da-09227f4745d6&pid=eab7d121-0401-4174-95da-09227f4745d6#aaa1>，最后访问日期：2018年9月8日。
- 7 马庆圆：国信证券联手美国 TradeStation 公司打造交易平台，中证网，时间：2015年3月17日，网址：http://www.cs.com.cn/sylm/jsbd/201503/t20150317_4665707.html，最后访问日期：2018年9月8日。
- 8 参见《国泰君安证券、海通证券两大券商同时携手阿法金融，打造投研投顾智能化》，搜狐网，时间：2018年2月5日，网址：http://www.sohu.com/a/221121611_610473，最后访问日期：2018年9月8日。
- 9 参见《通联数据创始人：智能投研将成为分析师的“得力外脑”》，中证网，时间：2017年11月30日，网址：http://www.cs.com.cn/sylm/jsbd/201711/t20171130_5600143.html，最后访问日期：2018年9月8日。
- 10 参见《第六届证券期货科学技术奖拟授奖项目公示公告》，中国证券业协会官网，时间：2018年2月5日，网址：http://www.sac.net.cn/tzgg/201802/t20180207_134463.html，最后访问日期：2018年9月8日。
- 11 参见《中国证券投资基金业年报（2015年）》，中国证券投资基金业协会官网，时间：2017-01-24，网址：<http://www.amac.org.cn/tjsj/cbw/391701.shtml>，最后访问日期：2018年9月8日。
- 12 参见《广发证券托管指令系统来了》，广发资产托管官方微信，时间：2017-05-15，最后访问日期：2018年9月8日。
- 13 参见《在线绩效系统重磅升级，招证托管只为更好体验》，招商证券托管外包微信公众号，时间：2018年6月5日，最后访问日期：2018年9月8日。
- 14 参见《你家基金“体检”过吗？快来体验国泰君安升级版绩效分析服务吧》，国泰君安托管与外包微信公众号，时间：2017年08月7日，最后访问日期：2018年9月8日。
- 15 参见《招商证券董事长霍达在2018年第四届西湖峰会发表主题演讲》，招商证券微信企业号，时间：2018年5月21日，最后访问日期：2018年9月8日。
- 16 资料来源：根据高盛年报和高盛网站内容整理，网址：<https://www.goldmansachs.com>。
- 17 Malcolm Cannon: State Street Amps up their Blockchain Technology for 2017, BTCMANAGER, 时间: January 6, 2017, 网址：<https://btcmanager.com/state-street-amps-up-their-blockchain-technology-for-2017/>，最后访问时间：2018年9月8日。

参考文献：

- [1] 麻晓勇等．金融科技引领下证券公司的商业模式重构及监管机制研究[J]．中国证券，2018(04): 63-80.
- [2] 邓维．国内外 PB 业务发展现状与中小券商发展路径研究[J]．中国证券，2018(08).
- [3] 邓维．区块链技术在券商 PB 业务的创新应用[J]．上海证券交易所《交易技术前沿》，2018年第2期，总第31期．
- [4] Hedgeweek Special Report. Prime Brokerage 2018[R]. January 2018.
- [5] 申万宏源研究所．银行托管与资管业务的共生繁荣—金融新模式探索系列报告之一：美国篇[R]．上海：2015年．
- [6] 民生证券银行业研究．有数据有分析，为什么海外银行拼命做资产托管业务[R]．北京：2016年．
- [7] 中国建设银行成都开发中心吴磊．全球托管银行业发展启示：大资管的全托管业务创新与平台架构研究．成都：2016年．
- [8] 张哲．国外资产托管业务的发展情况介绍及对我国资产托管业务发展对策[J]．中外企业文化旬刊，2014(2).

基于证券业网络安全等级保护的应用系统安全实践

晏强、杨超、王磊 / 光大证券股份有限公司 wanglei8@ebscn.com



1 前言

信息安全等级保护是我国信息安全保障工作的一项基本制度。国家高度重视信息安全等级保护工作，近年来国家密集发布一系列的信息安全标准体系文件，信息安全等级保护也要跟随着《网络安全法》即将跨入网络安全等级保护 2.0 时代，证券期货业信息系统是国家要求重点保障的重要

信息系统，关系到国家金融安全、社会稳定和广大投资者的权益利益。因此证券期货业更应该促进本行业信息安全建设，增强防护能力，提高业务的运营保障水平。

由于证券期货业有行业内的等保测评标准（JR/T 0060—2010），基本要求虽然是国家标准（GB/T 22239-2008）的细化，但业界还没有一套通用的应用系统网络安全等级保护实践体系，而

网络安全等级保护制度体系中，应用和数据安全在测评控制点上占 4 个技术测评方面比重最大，影响最深，且应用系统的安全测试是系统上线投产前最主要的风险控制手段，可以有效的发现业务安全需求、研发漏洞和系统风险。因此，本文立足于证券期货业的信息系统等级保护，对应用系统的安全实践进行了积极的探索，力求可以构建一个证券业标准化、可推广的应用系统实践体系。

2 应用系统面临的安全威胁及安全需求

应用系统由于存在弱点和漏洞，面临着各式各样的安全威胁，这是一个不争的事实，现阶段对证券行业来说，梳理出一套实用性强、可操作性广、统一标准化的通用安全需求是证券业信息系统安全的首要任务。

本文不求大而全，对安全需求仅取与信息系统等级保护相关的层面来源做阐述，当然国际上也有一些应用开发安全需求类别框架（如 NIST SP 800-53 等），并不太适用于国内的行业现状，这里不予讨论。故本文根据信息系统等级保护的基本要求将应用系统的安全挑战和安全需求，归

纳概括为以下四个方面：标识鉴别、访问控制、内容安全和监控审计。每个方面的具体实践将在下文详细阐述。

3 证券期货业信息安全等级保护中的应用安全测评要求

在网络安全等级保护 2.0 中，应用和数据安全要求通过应用系统、中间件平台系统和数据库管理系统等实现的安全功能来满足。如果应用系统是多层架构的，一般不同层的应用系统都需要实现同样强度的身份鉴别、访问控制、安全审计、剩余信息保护及资源控制等。

网络安全等级保护 2.0 中应用和数据安全是旧版信息系统等级保护应用安全和数据安全及备份恢复合并而来，包括身份鉴别、访问控制、安全审计、软件容错、资源控制、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等 10 个控制点。其中旧版中的控制点“备份和恢复”中部分内容已经调整到“网络和通信安全”和“设备和计算安全”中相应的控制点中。下表 1 是信息安全等级保护、网络安全等级保护和证券期货业信息安全等级保护控制点对照表：

表 1 信息安全等级保护、网络安全等级保护和证券期货业信息安全等级保护控制点对照表

信息安全等级保护 (GB/T 22239-2008)	网络安全等级保护 (等保2.0)	证券期货业信息安全等级保护 (JR/T 0060—2010)
7.1.4 应用安全	7.1.4 应用和数据安全	7.1.4 应用安全
7.1.4.1 身份鉴别	7.1.4.1 身份鉴别	7.1.4.1 身份鉴别
7.1.4.2 访问控制	7.1.4.2 访问控制	7.1.4.2 访问控制
7.1.4.3 安全审计	7.1.4.3 安全审计	7.1.4.3 安全审计
7.1.4.4 剩余信息保护	7.1.4.4 软件容错	7.1.4.4 剩余信息保护
7.1.4.5 通信完整性	7.1.4.5 资源控制	7.1.4.5 通信完整性
7.1.4.6 通信保密性	7.1.4.6 数据完整性	7.1.4.6 通信保密性
7.1.4.7 抗抵赖	7.1.4.7 数据保密性	7.1.4.7 抗抵赖
7.1.4.8 软件容错	7.1.4.8 数据备份恢复	7.1.4.8 软件容错
7.1.4.9 资源控制	7.1.4.9 剩余信息保护	7.1.4.9 资源控制
7.1.5 数据安全与备份恢复	7.1.4.10 个人信息保护	7.1.5 数据安全与备份恢复
7.1.5.1 数据完整性		7.1.5.1 数据完整性
7.1.5.2 数据保密性		7.1.5.2 数据保密性
7.1.5.3 备份和恢复		7.1.5.3 备份和恢复

对比网络安全等级保护（等保 2.0）与旧版等级保护可看出：等保 2.0 应用和数据安全部分由旧版“应用安全”和“数据安全与备份恢复”合并而来；等保 2.0 新增一个控制点“个人信息保护”；合并旧版应用安全控制点“通信完整性”和数据安全及备份恢复控制点“数据完整性”；合并旧版应用安全控制点“通信完整性”和数据安全及备份恢复控制点“数据保密性”；删除旧版应用安全控制点“抗抵赖”（在四级系统中增加了一个要求项，具体为：在可能涉及及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖）。

对比信息安全等级保护和证券期货业信息安全等级保护可以看出：两者在控制点和要求项上保持一致，但要结合证券期货业的实际情况，对国家等保标准进行明确、细化和调整，使其整体防护水平不低于国家标准。

4 基于等级保护制度的证券业应用系统安全实践方案

由于网络安全等级保护（等保 2.0）正式版还未发布，所以我们还是按照证券期货业信息安全

全等级保护标准（JR/T 0060—2010）关于应用安全的测评控制点和要求项来设计整体的应用系统安全实践方案。针对应用系统安全防护领域的常见问题，在流程合理、标准合规的前提下，本文对应用系统安全实践做了三个方面的设计：应用系统安全实践的框架定义、应用系统安全实践的设计方法、应用系统安全实践的全生命周期管理。

4.1 应用系统安全实践通用框架

根据对证券期货业信息安全等级保护测评要求（JR/T 0067-2011）及证券业应用系统的安全的分析，现将应用系统安全通用框架定义如下图 1。

根据证券业应用系统的安全架构，我们对标了证券期货业信息安全等级保护中应用系统的 9 个要求项，将其整合成标识鉴别、访问控制、内容安全和监控审计这四个模块，共同构成了基于信息安全等级保护的应用系统安全框架。此安全框架完整的继承了等级保护应用系统的所有测评要求点，也将证券业最为关注的 web 应用防护、邮件内容侦查、防篡改、防泄漏、虚拟化保护这些技术统归为内容安全大类中，利于完整通用框架的后续设计实践。

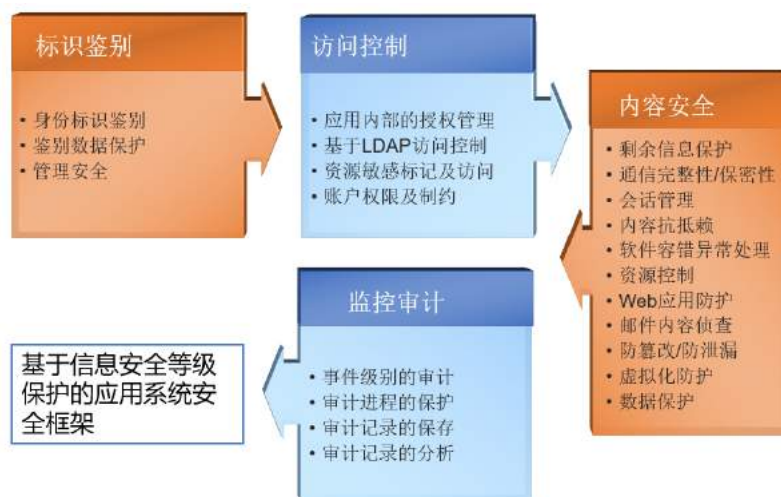


图 1 基于信息安全等级保护的应用系统安全通用框架

4.2 应用系统安全实践的设计方法

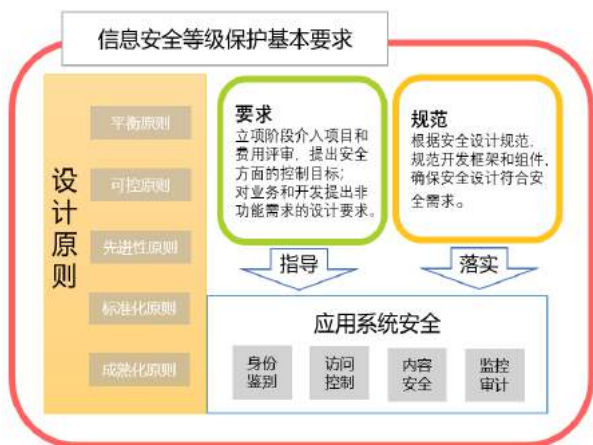


图2 应用系统安全通用框架的设计方法

证券业的信息系统是一个庞杂的工程，既有静态的门户网站，又有核心的交易及资产账户系统，所以安全设计的第一个要务就是平衡原则，要平衡需求、风险和代价。应该全面梳理应用系统安全需求，正确处理需求、风险与投入代价的关系，做到安全性、可用性、可实施性相匹配，

达到技术上可实现、组织上可执行、投入上有保障的设计目标。应用系统安全设计还必须遵循一定可控性规范，以确保各系统安全体系的一致性和风险可控性。同时在标准化和成熟度的基础上，安全体系设计还应具有一定的前瞻性，必须考虑业务安全需求的发展以及安全技术的进步，确保安全体系具备可持续发展能力，能够不断调整和优化安全控制措施，适应新的网络环境，满足新的网络安全需求。

根据我们在3.1中定义的基于信息安全等级保护的应用系统安全通用框架，为保证安全设计符合上述各方面，安全部门需要在立项阶段介入项目和费用评审，提出安全方面的控制目标，并对业务和开发提出非功能需求的设计要求。同时应该根据安全设计规范，《信息安全技术信息系统等级保护安全设计技术要求》(GB/T 25070 - 2010)，规范开发框架和组件，确保安全设计符合安全需求。下面是具体实践的流程图：

图3的流程中上线前安全测试阶段的依据为

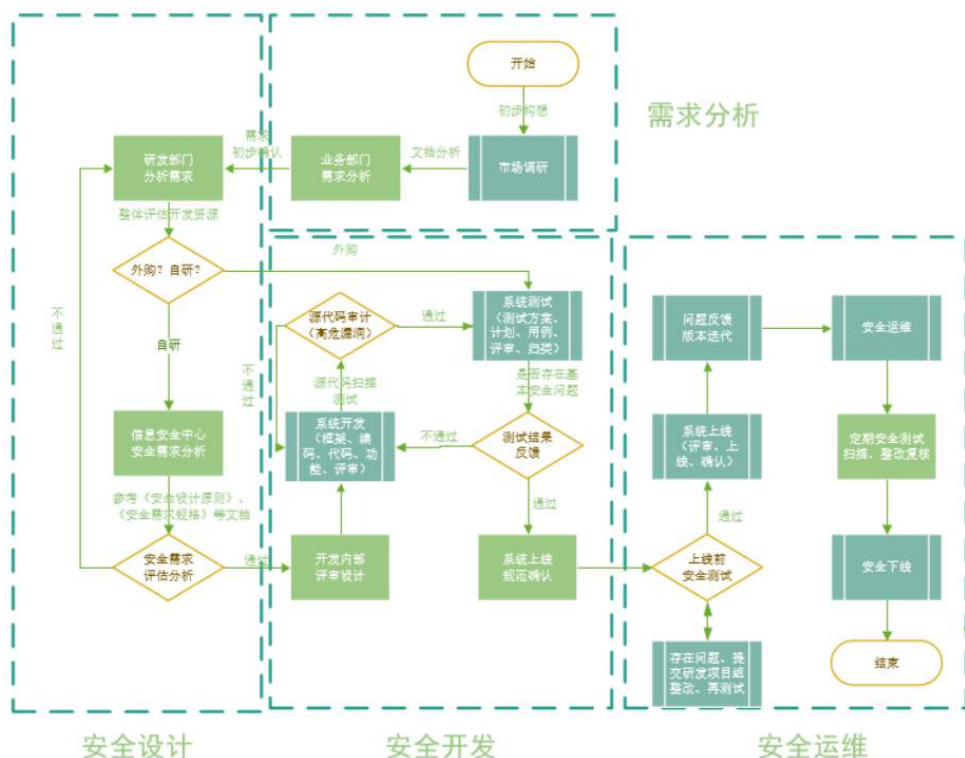


图3 应用系统安全通用框架的具体实践流程

本文在 3.1 中所设计的应用系统安全通用框架，其具体的技术指标要求指标如下（以“标识鉴别”模块为例），通用框架中第一部分为标识鉴别，其中主要包含三个方面：身份标识鉴别、鉴别数据保护、管理安全。

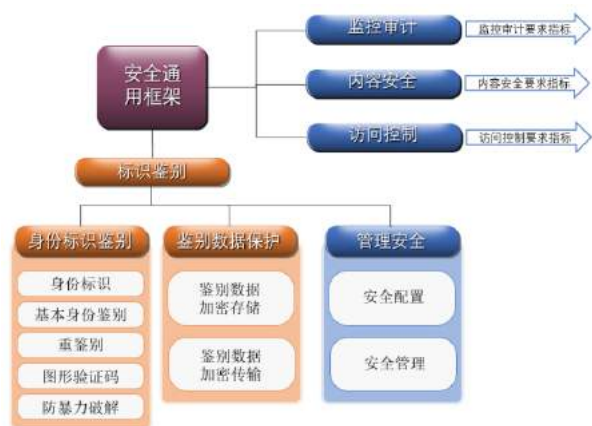


图 4 标识鉴别模块具体要求项

身份标识鉴别主要包括：

► 身份标识：应用系统的管理员和其他操作人员应该具有明确的身份标识。

基本要求项：

- 身份标识应该具有唯一性，保证系统中不存在重复用户身份标识；
- 身份标识应不可预测，如递增序列号等；
- 将身份标识与审计记录关联一致；
- 应支持角色定义、角色权限管理、用户角色管理等；
- 授权管理员能够增加、修改、删除账号和角色；
- 账号异常时（登录过于频繁、长时间未登录等），应该支持后台锁定账号。

► 基本身份鉴别：应用系统对管理员及普通用户的身份进行鉴别。

基本要求项：

- 应该采用至少一种方式对管理员本地控制台登录进行身份鉴别；
- 面对互联网服务的系统，应该采用两种或两种以上组合的方式进行身份鉴别；

• 若通过用户名 / 密码鉴别，则密码应有相关的复杂度策略；

• 若采用 USBKey、动态密码令牌等进行身份鉴别，应该有相关 PIN 保护。

► 重鉴别：执行重要操作或者敏感信息修改时，需队用户进行重鉴别或结合其他途径进行鉴别。

基本要求项：

• 涉及账户交易功能、账户重要关联信息（密码、身份证号、关联的手机号、邮箱等）修改时，应该对用户进行再次身份认证；

• 在密码找回功能中，需要通过账号绑定的手机号发送随机认证的方式再行二次鉴别。

► 图形验证码：通过电脑自动操作可能会带来危害的页面，需采用验证码措施。

基本要求项：

- 以下页面必须使用图形验证码：注册页面、登录页面、短信 / 邮箱认证页面、转账交易页面、限时抢购页面等
- 图形验证码应该采用一定的干扰措施且不可预测，如字体倾斜、加背景噪点等；
- 验证码需有服务器端生成并完成验证，不得在前端页面返回；
- 验证码应该具有一定的有效性，例如：5 分钟。

► 防暴力破解：应用系统应该具备防止密码、验证码等的暴力猜测功能。

基本要求项：

- 防密码暴力猜测：对采用密码进行鉴别的系统，因防止密码暴力猜测，连续失败登录后锁定账号。账号锁定后可以由系统管理员解锁，也可以在一段时间后自动解锁；
- 防验证码暴力猜测：若系统具备验证码功能，应具有防止验证码暴力猜测措施。如验证码连续错误一定的次数后，锁定该主机继续猜测或者锁定主机 IP 地址等。

鉴别数据保护：应用系统应该具备鉴别数据

保护功能，具体要求项如下：

► 鉴别数据加密存储：数据库端对鉴别数据以摘要方式存储，使用 Hash+Salt 方式；

► 鉴别数据加密传输：可采用加密的传输通道，或者对密码以摘要方式传输。

管理安全：身份标识及认证的系统配置，包括这些安全策略的生效准则等。除此之外应用系统的整体安全离不开管理部分，主要集中在信息安全等级保护中的系统建设管理环节，这里不予详述。

以上应用系统通用框架的要求项完全涵盖了信息系统等级保护的具体条款，每一条都对应了测评要求做了细化的具体要求项。信息安全等级保护中身份鉴别具体条款如表 2。

通过逐条比对，本文在综合了监管要求和证券实践的基础上，将上述提出的通用实践框架和信息系统等级保护测评条款一一比对，形成完整的实践要求（表 3）：

除了合规要求以外，本文还在应用安全的身份鉴别方面进行了细化，详细列举了涉及账户交易功能、账户重要关联信息的情景时，需要重鉴别要求项，提出了验证码设计、防暴力破解的详细要求项，以保障应用系统身份鉴别的安全性和实用性。

随着外部威胁的不断变化，金融业务的不断扩展，以及等级保护 2.0 的即将正式启用，本通

用框架还额外的扩展有移动 APP 安全模块（主要针对各 APP 客户端、客户端数据、通信安全做了详细的要求项），微信应用安全模块（对于微信应用，应严格检查提交请求及接口安全）、大数据系统安全模块（大数据主要关注数据筛选、可扩展性、去隐私化及冗余部署等）和云计算安全模块（符合等级保护 2.0 云计算部分的加测项），通用框架中这些拓展模块的细化和落实，以及如何在监管要求和金融实践中找到最优解是我们下一阶段工作的重点。

4.3 应用系统安全实践的全生命周期管理

在以往的信息系统中，安全人员都在测试和运维阶段才接触应用系统，而且只关注应用安全性的管理方式，这样往往治标不治本，而面对现今的安全威胁，安全人员的参与必须从运维阶段大幅度提前，要参与到需求分析、安全设计、安全开发阶段，安全工作介入应用系统越早，潜伏的安全隐患就越少，对漏洞的修复成本就越低。为解决上述面临的难题，本文提出了应用系统安全实践的全生命周期管理，旨在全面的提升应用系统安全的实践能力。针对图 3 的应用系统安全实践的具体流程图，本文提出应用系统安全实践全生命周期模型，具体如图 5：

本文将应用系统安全实践抽象成四个步骤：

表 2 信息安全等级保护中身份鉴别具体条款

7.1.4 应用安全	7.1.4.1 身份鉴别 (S3)	a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
		b) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；
		c) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；
		d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
		e) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

表 3 标识鉴别模块完整实践要求

一级 类目	二级 类目	等级保护要求项	通用安全框架匹配项	测评指导	预期结果
应用 安全	身份 鉴别 (S3)	a) 用户身份 标识鉴别；	1、应用系统的管理员和其他操作人员应该具有明确的身份标识。 2、应用系统对管理员及普通用户的身份进行鉴别。	1) 测试登录控制模块，查看鉴别方式和身份标识； 2) 测试已注册和未注册或错误的用身份登录系统。	1) 普通用户和管理用户有各自的登录界面，管理用户在网动态管理，内外网系统间物理隔离。
		b) 两种鉴别 技术要求；	1、应该采用至少一种方式对管理员本地控制台登录进行身份鉴别 2、面对互联网服务的系统，应该采用两种或两种以上组合的方式进行身份鉴别； 3、若采用USBKey、动态密码令牌等进行身份鉴别，应该有相关PIN保护。 4、若通过用户名/密码鉴别，则密码应有相关的复杂度策略	1) 检查系统管理员登录各类账户的登录过程； 2) 测试使用单独一种登录方式是否能够登录成功。	1) 用户需要采用静态密码、动态密码、生物识别技术中的两种或两种以上的鉴别技术进行登录。 2) 单独使用一种鉴别技术无法实现登录。
		c) 唯一性复 杂度要求；	1、身份标识应该具有唯一性，保证系统中不存在重复用户身份标识 2、身份标识应不可预测，如递增序列号等 3、将身份标识与审计记录关联一致	1) 以已有用户名重新注册，测试系统能否禁止注册？ 2) 新注册用户，测试复杂度是否进行了检查？ 3) 使用扫描工具检测是否存在弱口令或空口令等。 4) 检查防止身份鉴别信息被冒用的措施。	1) 以已有用户名重新注册，系统禁止注册。 2) 新注册用户，口令长度不够、复杂度不满足要求的，设置失败 3) 如果采用口令进行身份鉴别，对口令复杂度的要求：对口令的长度、复杂度、更改周期进行了要求；不存在弱口令和空口令。 4) 所有用户身份标识都是唯一的，并
		d) 登录失败处 理要求；	1、账号异常时（登录过于频繁、长时间未登录等），应该支持后台锁定账号 2、应用系统应该具备防止密码、验证码等的暴力猜测功能，连续失败登录后可锁定账号等。	1) 使用错误的用户名或密码进行登录，测试系统如何响应？ 2) 以超出系统规定的失败次数登录，查看账户是否锁定？ 3) 检查登录系统后在连接超时情况下系统的反应。	1) 登录失败时，系统采取结束会话、自动退出的方式响应。 2) 对登录失败次数有限制，限制次数不是太大，登录失败超过一定次数后，账户会被锁定。具有权限的系统管理员才能给进行解锁。 3) 登录系统后在连接超时，系统可自
		e) 安全配置 要求。	1、应支持角色定义、角色权限管理、用户角色管理等 2、授权管理员能够增加、修改、删除账号和角色 3、验证码有效性设置。 4、鉴别数据加密传输和存储设置。	1) 如果需要进行配置，查看需要配置的实际配置情况，是否按照前3点要求进行了配置，是否已经启用了该功能	1) 没有配置功能的，由系统默认实现的部分，符合前3点要求。 2) 需要配置的，按照前3点要求进行配置，并且已经启动了该功能。

需求分析、安全设计、安全开发和安全运维。这里的全生命周期模型不同于微软的SDL(security development lifecycle 安全开发生命周期),SDL 更加侧重于软件开发过程的管理模式，本文则更偏向于系统，在需求分析阶段安全部门的人员应该和业务部门研发部门一同对软件的安全风险进行评估，建立基本的安全需求；在安全设计阶段安

全人员应该和研发人员共同设计安全方案，并进行威胁建模；在安全开发阶段，安全部门应该提供主流变成语言的安全编码规范、安全函数库以及代码审计方案；运维阶段，安全人员应该基于设计阶段的威胁建模进行系统测试、上线测试等，并对定期维护漏洞威胁库，以动态保障信息系统的全生命周期安全。

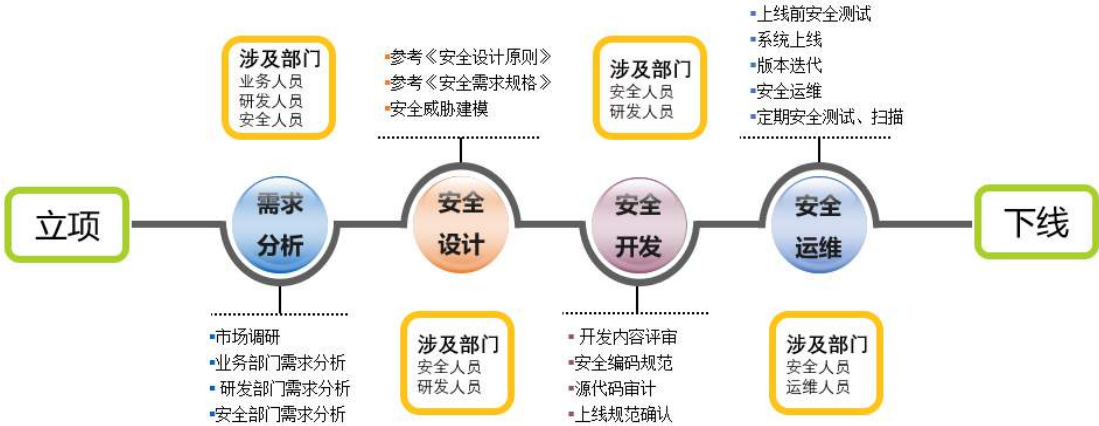


图 5 应用系统安全实践全生命周期模型

5 总结

本文立足于证券业信息安全等级保护的制度要求，对金融业应用系统面临的安全挑战及安全需求做了简要的分析，面对各式各样的安全需求

和挑战，本文旨在探索一套通用的应用系统安全建设实践框架，并对框架的定义、设计方法、实践流程做了详细的阐述，最后提出了应用系统安全实践的全周期管理模型，力求构建一套符合信息安全等级保护测评要求的应用安全实践框架。

参考文献：

- [1] 公安部信息安全等级保护评估中心《信息安全等级保护政策培训教程》，北京：电子工业出版社，2010年；
- [2] 郭启全等《网络安全法与网络安全等级保护制度培训教程（2018版）》，北京：电子工业出版社，2018年；
- [3]《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239 - 2008）
- [4]《证券期货业信息系统安全等级保护基本要求》（JR/T 0060—2010）
- [5] Tyler W. Thomas, Madiha Tabassum, Madiha Tabassum, Bill Chu, Heather Lipford : Security During Application Development: an Application Security Expert Perspective // CHI '18 Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems Paper No. 262; Canada — April 21 - 26, 2018
- [6]《信息安全技术信息系统等级保护安全设计技术要求》（GB/T 25070 - 2010）；
- [7] 安全实践备忘录：应用系统安全通用技术要求，<https://jfsec.org/2017/03/10/appsec-req-std/>
- [8]《信息安全技术信息系统安全等级保护测评要求》（GB/T 28448 - 2012）；

基金行业数据安全保障体系建设探析

宋晓刚 朱林 杨志明 / 银华基金管理股份有限公司信息技术部 邮箱: zhul@yhfund.com.cn

摘要：云计算、人工智能、移动互联为基金行业带来了颠覆性的影响，支撑这些新技术应用的离不开数据的采集和深入利用，围绕数据全生命周期的利用和价值挖掘变成了一个重要的话题，目前大多数基金公司的业务系统每天产生大量的应用数据，其中高价值和敏感数据占据很大比例，这种利用数据开展业务的工作模式已经越来越普遍，但是一个不容忽视的问题越来越重要：数据安全。因此为了提高数据在产生到销毁过程中的安全性，本文结合当前基金行业的业务和数据特点，就如何保障数据安全性展开分析。

关键字：基金行业数据特点 数据分类分级 技术保障 组织保障 制度保障



1 行业数据安全概述

根据证监会官方网站发布的信息,《证券期货业数据分类分级指引》《证券期货业机构内部企业服务总线实施规范》《期货市场客户开户数据接口》《证券发行人行为信息内容格式》等四项金融行业标准已在9月29日发布实施。

目前我国证券期货行业相关数据种类多、数量大,证监会会管单位、证券基金经营机构等各类市场主体沉淀了大量数据信息。各机构因业务发展需要,对数据应用的各类需求也不断衍生和扩展,数据产生、应用、流转、存储等各个环节不断发生变化。在此背景下,证券期货业数据安全,也成为信息安全领域的一个突出问题。

近年来国内外一系列信息安全事件表明,如果基金行业的安全防护措施没做到位,一旦发生重大事故,将给企业造成无法估量的影响,直接威胁到企业生存和发展,造成无可挽回的经济损失,甚至影响整个基金行业的发展和社会稳定。从安全角度看,近年来基金企业内的数据安全已逐步放到首要位置,包括数据的使用范围、流转、复制和篡改等。证监会关于证券基金经营机构信息技术管理办法中明确提出“证券基金经营机构

应当完善网络隔离、用户认证、访问控制、数据加密、数据备份、数据销毁、日志记录、病毒防范和非法入侵检测等安全保障措施,保护经营数据和客户信息安全,防范信息泄露与损毁。”

2 基金行业数据分类分级建议

基金行业业务种类繁多,数据呈现出复杂性高,多样性强的特点。采用规范的数据分类、分级方法,有助于基金公司厘清数据资产、确定数据重要性或敏感度,并针对性地采取适当、合理的管理措施和安全防护措施,形成一套科学、规范的数据资产管理与保护机制。

数据分类是数据保护工作中的一个关键部分,是建立统一、准确、完善的数据架构的基础,是实现集中化、专业化、标准化数据管理的基础。基金公司按照统一的数据分类方法,依据自身业务特点对产生、采集、加工、使用或管理的数据进行分类,可以全面清晰地厘清数据资产,对数据资产实现规范化管理,并有利于数据的维护和扩充。数据分类为数据分级管理奠定基础。

基金行业数据按照分类标准,分类范围包括但不限于:



图1 行业数据分类分级依据

(1) 交易管理类：基金投资成交信息、基金投资委托信息、基金投资组合信息、投资者交易信息、交易业务参数信息、交易日志信息；

(2) 结算管理类：估值清算、资金划转信息、银行账务信息、结算业务参数信息、结算日志信息；行情资讯类：行情数据、资讯信息；

(3) 投资者管理类：投资者基本信息、投资者开户/账户信息、投资者衍生信息、投资者合约信息；

(4) 交易条线：产品信息、合约信息、其他产品信息；

(5) 监管条线：监管信息、合规类信息、风控类信息、稽核类审计信息；

(6) 信息披露条线：披露信息（包含已公开及未公开）、研究报告（包括已公开及未公开）；

(7) 其他条线：客户关系信息、客户服务信息、客户经营分析、渠道信息、市场营销推广信息、服务机构信息、服务人员信息、统计信息、规划类数据、质量管理类数据、开发类数据、测试类数据、安全管理数据、运行数据、人力数据、财务数据、办公数据、经营数据、合同信息、供应

商数据、项目管理数据、战略规划数据、新产品研发、制度章程；

数据分级是以数据分类为基础，采用规范、明确的方法区分数据的重要性和敏感度差异，并确定数据级别。数据分级有助于基金公司根据数据不同级别，确定数据在其生命周期的各个环节应采取的数据安全防护策略和管控措施，进而提高机构的数据管理和安全防护水平，确保数据的完整性、保密性和可用性。

为了保证数据安全，根据数据资产敏感度建议基金公司将数据划分为4个等级：

(1) 1级：数据敏感度极低或无，数据可被公开或可被公终获知、使用。

(2) 2级：数据敏感度低，数据用于一般业务使用，一般针对受限对象公开，一般指内部管理且不宜广泛公开的数据。

(3) 3级：数据敏感度中等，数据用于重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。

(4) 4级：数据敏感度高，数据用于关键业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。

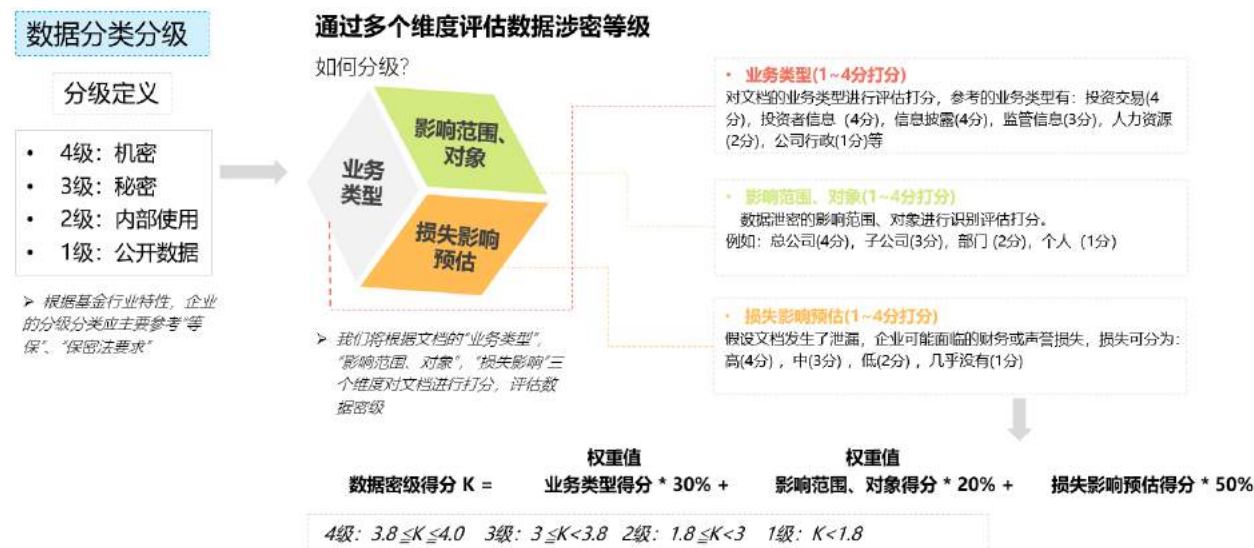


图2 基金公司数据分级思路

数据分级对应业务条线数据说明举例：

参考级别	业务条线	数据子类	数据说明
4 级	交易条线	交易管理	投资成交信息、投资委托信息
		结算管理	持仓信息、估值清算信息
3 级	交易条线	结算管理	银行账务信息、交易日志
		投资者管理	个人投资者基本信息、投资者账户信息、合约合同、客户关系信息、客户服务信息
	其他	技术管理	开发类数据、人员信息（非公开）
2 级	交易条线	交易管理	交易基础信息、交易业务参数信息
		结算管理	资金划转信息、结算日志信息
	监管条线	合规风控	合规类信息、风控类信息
	信息披露		研究报告（未公开）、披露信息（未公开）
1 级	交易条线	结算管理	基金净值
		行情资讯	行情数据、资讯数据、
		产品管理	产品信息、合约信息
	信息披露		研究报告（已公开）、披露信息（已公开）

3 数据安全保障手段

3.1 数据安全能力框架

基于《信息安全技术 数据安全能力成熟度模型》标准能力成熟度等级 3 级要求，数据安全能力建设可参考以下实施框架见图 3：

整体来看，数据安全能力建设是以法律法规监管要求和业务发展需要为输入，结合数据安全组织建设、制度流程和技术工具的执行要求，匹配相应人员的具体能力，组织的数据安全能力建设结果最终以数据生命周期各个过程域来综合体现。下面对合规和业务需求及三个保障维度的框架设计进行概要说明：

合规和业务需求：数据安全最终是为基金公司的业务发展服务的，不能游离于业务之外或独立存在。在满足法律法规要求的前提下，数据安全能力建设须切合业务发展需要来开展。

组织建设：指数据安全组织的架构建立、职

责分配和沟通协作。组织可分为决策层、管理层和执行层等三层结构。

制度流程：指数据安全具体管理制度体系的建设和执行，包括数据安全方针和总纲、数据安全管理规范、数据安全操作指南和作业指导，以及相关模板和表单等。

技术工具：指与制度流程相配套并保证有效执行的技术和工具，可以是独立的系统平台、工具、功能或算法技术等。需要综合所有安全域进行整体规划和实现，且要和组织的业务系统和信息系统等进行衔接。包括适用于所有安全域的通用技术工具，和部分阶段或安全域试用的技术工具。

3.2 组织保障

数据安全能力建设是一个复合型、需多方联动型的工作，在开展组织架构建设时，需要考虑组织层面实体的管理团队及执行团队，同时也要

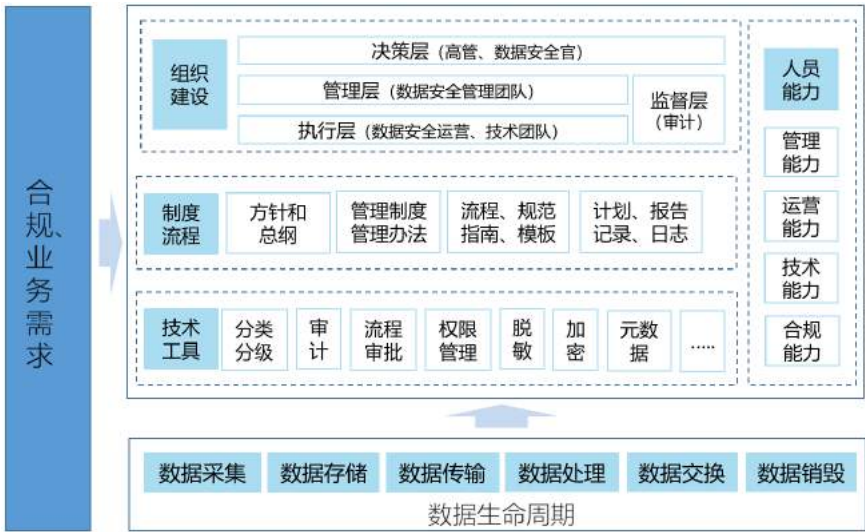


图 3 数据安全能力框架愿景

考虑虚拟的联动小组，其中业务部门、研发部门、HR、IT、法务等部门均需要参与数据安全建设当中。成立数据安全组织其目的是明确数据安全的政策、落实和监督等工作，以确保数据安全能力建设的执行。

同时，需要数据安全管理层制定与各部门之间的数据安全工作机制，目的是为了保障数据安全工作顺利开展，过程中的争议得到解决，如数据安全团队与业务方、法务以及合作伙伴之间的日常工作交流、争议与问题解决等事项。

3.3 技术保障

数据生命周期中所有安全域涉及到的技术工具，可以是独立的系统平台、工具、功能或算法技术等，在规划设计时不用单独针对某个安全域，需要整体考虑。尤其涉及到通用的技术工具，需要整合，且和组织的业务系统和信息系统等进行衔接。

3.3.1 数据脱敏管理平台

数据脱敏 (Data Masking), 又称数据漂白、数据去隐私化或数据变形。指对某些敏感信息通过

脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。在涉及客户安全数据或者一些商业性敏感数据的情况下，在不违反系统规则条件下，对真实数据进行改造并提供测试使用，如身份证号、手机号、卡号、客户号等个人信息都需要进行数据脱敏。

按照数据使用场景，将数据脱敏分为静态数据脱敏 (Static data masking-SDM) 与动态数据脱敏 (Dynamic data masking-DDM)。

3.3.2 数据库审计系统

数据库安全审计系统主要用于监视并记录对数据库服务器的各类操作行为，通过对网络数据的分析，实时地、智能地解析对数据库服务器的各种操作，并记入审计数据库中以便日后进行查询、分析、过滤，实现对目标数据库系统的用户操作的监控和审计。

3.3.3 统一身份认证及权限管理平台

身份认证，就是判断一个用户是否为合法用户的处理过程。最常用的简单身份认证方式是系统通过核对用户输入的用户名和口令，看其是否与系统中存储的该用户的用户名和口令一致，来判断用户身份是否正确。复杂一些的身份认证方式采用一些较复杂的加密算法与协议，需要用户

出示更多的信息（如私钥）来证明自己的身份，如动态口令身份认证、数字证书身份认证等。

权限管理主要功能有：成员站点对用户的权限控制、用户对成员站点的权限控制、成员站点对成员站点的权限控制。用户向某成员站点申请分配权限时，需向该成员站点提供他的某些信息，这些信息就是用户提供给成员站点的权限，而成员站点通过统一身份认证系统身份认证后就可以查询用户信息，并给该用户分配权限，获得权限的用户通过统一身份认证系统身份认证后就可以以某种身份访问该成员站点。

3.3.4 数据防泄漏系统

数据泄密（泄露）防护（DLP），又称为“数据丢失防护”。数据防泄漏系统是以统一策略为基础，采用深层内容分析、对静态数据、动态数据及使用中的数据进行即时的识别、监控、保护的相关技术。

目前，数据泄漏的途径可归类为三种：在使用状态下的泄密、在存储状态下的泄密和在传输状态下的泄密。一般企业可通过安装防火墙、杀毒软件等方法来阻挡外部的入侵，但是事实上97%的信息泄密事件源于企业内部，所以就以上三种泄密途径分析，信息外泄的根源在于：

1、使用泄漏：1) 操作失误导致技术数据泄漏或损坏；2) 通过打印、剪切、复制、粘贴、另存为、重命名等操作泄漏数据。

2、存储泄漏：1) 数据中心、服务器、数据库的数据被随意下载、共享泄漏；2) 离职人员通过U盘、CD/DVD、移动硬盘随意拷走机密资料；3) 移动笔记本被盗、丢失或维修造成数据泄漏。

3、传输泄漏：1) 通过email、QQ、MSN等轻易传输机密资料；2) 通过网络监听、拦截等方式篡改、伪造传输数据。

3.3.5 数据共享传输平台

建立数据共享安全管理平台，或者与在统一的用户认证平台、权限管理平台、流程审批平台，

监控审计平台中支持数据共享的安全控制功能，并结合数据脱敏等数据保护技术保护敏感数据。数据共享安全工具对于共享资源的数据目录或者数据资产进行安全管理，确保共享数据的规范性和安全性。

3.3.6 数据备份系统

数据备份是指为了防止由于操作失误、系统故障等人为因素或意外原因导致数据丢失，而将整个系统的数据或者一部分关键数据通过一定的方法从主计算机系统的存储设备中复制到其它存储设备的过程。当主计算机系统的数据由于某种原因丢失或不可用时，可以利用复制的数据进行恢复，从而保持数据的完整与业务的正常进行。因此，可以说，数据备份主要解决的是数据的可用性问题。

3.3.7 数据加密系统

数据加密的基本过程就是对原来为明文的文件或数据按某种算法进行处理，使其成为不可读的一段代码，通常称为“密文”，使其只能在输入相应的密钥之后才能显示出本来内容，通过这样的途径来达到保护数据不被非法人窃取、阅读的目的。该过程的逆过程为解密，即将该编码信息转化为其原来数据的过程。

文档加密是数据加密中的一种主流技术，采用透明加解密技术，对数据进行强制加密，不改变用户原有的使用习惯；此技术对数据自身加密，不管是脱离操作系统，还是非法脱离安全环境，用户数据自身都是安全的，对环境的依赖性比较小。市面上的文档加密主要的技术分为磁盘加密、应用层加密、驱动级加密等几种技术。

3.4 制度保障

制度流程需要从组织层面整体考虑和设计，并形成体系框架。制度体系需要分层，层与层之间，同一层不同模块之间需要有关联逻辑，在内容上不能重复或矛盾。一般按照分为四级：



图4 数据安全制度体系设计层级

一级文件：方针和总纲是面向组织层面数据安全管理的顶层方针、策略、基本原则和总的管理要求，包括数据安全管理的目标、愿景和方针，数据资产定义、基本原则、违规处理等；

二级文件：数据安全管理制度和办法，是指数据安全通用和各生命周期阶段中某个安全域或多个安全域的规章制度要求，包括数据资产管理、质量管理、安全合规等；

三级文件：数据安全各生命周期及具体某个安全域的操作流程、规范，及相应的作业指导书

或指南，配套模板文件等。

四级文件：指执行数据安全管理制度产生的相应计划、表格、报告、各种运行/检查记录、日志文件等。

4 总结

随着金融行业全面迈入大数据时代，更多的基金公司已经享受到了大数据技术带来的红利。数据是金融行业的命脉，但基金公司面临内部及外部的数据安全风险也将极大的制约对于数据价值的发挥，随着数据量飞速增长，数据管理系统日益复杂，基金公司必将主动引入数据安全管理体系，提升数据安全能力水平，强化数据安全保护意识，完善数据安全管理制度，为数据价值发挥最大化保驾护航；通过本文对数据安全保障体系的分析和建议可以为基金行业提供参考。

参考文献：

- 《网络安全等级保护基本要求》送审版
- 《证券基金经营机构信息技术管理办法》
- 《证券期货业信息系统审计规范》第6部分：基金管理公司
- 《证券期货业数据安全标准规划》
- 《证券期货业数据分类分级指引》
- 《数据安全能力建设实施指南》



0 行业观察 bservation

- 11 券商业务规则体系系统一建设的实现与探讨
- 12 智能化多模金融数据质量监控平台实现路径
- 13 基于区块链技术构建可信仓单系统的研究
- 14 美式期权价格计算的 FPGA 实现
- 15 人工智能 + 知识图谱：如何规整海量金融大数据？

券商业务规则体系统一建设的实现与探讨

潘聪 / 华泰证券 pancong@htsc.com
刘丽 / 华泰证券 liuli@htsc.com



1 现状问题及应对思路

1.1 现状问题

随着券商内部业务复杂程度不断加深，业务运营与监管的规则数量不断增多，在 IT 系统的应用层面普遍出现以下两个方面的问题。

(1) 规则分散，无法独立进行规则管理。

业务规则作为券商的核心资产之一，目前大多基于业务管理部门分割分散于各业务系统中。由于跨部门、跨系统，各业务应用系统管理这些

核心资产的方式各有不同，并且这些业务规则的关联性强、变化十分迅速，无论是业务人员还是研发人员都无法独立对这些规则进行管理，容易在规则执行的时候引发问题甚至会有互相矛盾的情况发生。

(2) 规则多样，无法快速应对监管规定、管理要求和市场竞争带来的持续变化的需求。

近年来，随着监管发布了多项“管理办法”以及营销活动形式的多样化发展，业务规则也发生不断的变化。对于时间紧迫的需求，由于业务规则夹杂在各个应用系统的代码中，改造的和维

护的代价相对较高，不能快速地对变化做出相应的响应。

1.2 解决思路

为此，本文提出了构建券商统一规则体系的理念，通过梳理和分析逐渐将规则从分散走向集中管理，运用流程引擎、规则引擎等成熟的方法实现业务规则的可视化、集中化的统一管理。同时，统一管理后的规则将直观的展示互相之间的关联性，业务人员进行管理的过程中更易发现多项规则之间互相约束的图谱，使得业务处理有径可寻、有据可依，进而引导并协助业务人员形成规范化的业务处理流程。

2 可行性分析

2.1 业务可行性

现有业务无论是营销还是风控、合规等规则较多的场景都是按照业务条线分开管理的，不同业务规则互相影响的现象越发明显，尤其是合规规则天然内嵌到业务流程特点，使得缺乏统一互补的规则管理流程，越来越不适应今后综合客户服务和交叉产品营销的需求。同时营销规则、风控规则的变化会产生互相影响，业务人员往往无法直观的发现，存在既有可能错失了营销的机会又放松了合规管理的风险。因此提炼各业务间统一的规则要素进行信息共存共享，重构各种规则间的逻辑关系，有利于简化公司内部的业务管理流程，提升客户的服务体验，并在此基础上进一步探索更多的业务场景，具有深远的意义。

2.2 技术可行性

针对证券领域的业务规则，变更频率较高，

传统的程序代码难以实现或者过于繁琐。可以考虑引入规则引擎、流程引擎或者多种工具结合的形式来管理这些规则，市面上比较成熟的产品有Drools (JBoss Rules)、iRule等。使用以事件驱动为特征的规则引擎结合规则库、规则语言框架将证券领域的业务规则通过结构化的数据形式表示出来，完全分离实际数据及实现逻辑，从而将业务规则从程序中分离，最终实现业务人员对业务规则的统一管理，例如规则编辑、规则查询、规则生命周期管理等。

3 建设实践

3.1 现状梳理

3.1.1 规则分类

根据证券行业的现状，主要针对以下营销、合规、风控类业务规则进行梳理。

营销的目的主要是为了获客和增加客户粘性，营销活动的规则可以从获客和促活两个方面来进行梳理。

(1) 获客类规则

获客类营销活动主要是针对券商的新客户，获客方式由于受到合规规则的限制，其形式主要有渠道引流、线下引流等。基于此获客类规则主要可由渠道挑选类、资源控制类、执行策略类、效果评估类等原子级的规则点组成，业务人员可以从原子规则点中灵活的挑选出符合活动要求的规则原子通过编排组成一条获客规则执行单元，进而将编辑好的执行单元组成一个获客营销活动。

例如：获客规则执行单元“与日活 ≥ 500 万的第三方平台对接引流，向成功开户的客户发放购物券，总成本 ≤ 20 万”，是由渠道挑选类原子规则点“日活 ≥ 500 万的第三方平台”、资源控制类原子规则点“总成本 ≤ 20 万”、执行策略类原子规则点“发放购物券”组成。一条规则的原子

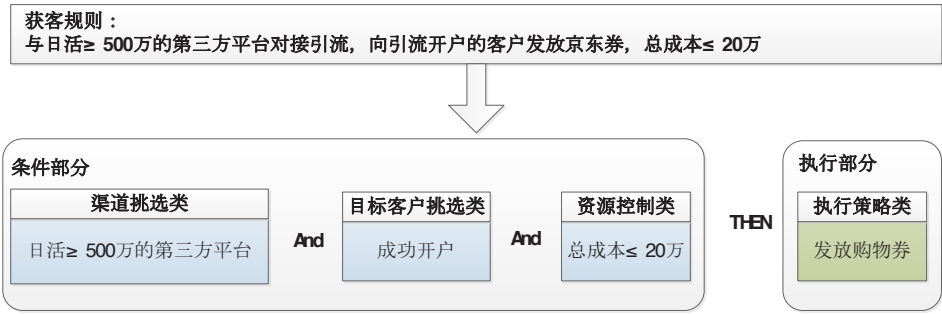


图1 规则梳理的原子化过程

化示意图如图1。

(2) 促活类规则

促活类营销活动主要是针对券商的存量客户，这就需要根据客户的真实情况向客户推荐真正感兴趣内容，提高客户的粘性。促活类的规则主要由目标客户挑选类、资源控制类、执行策略类、效果评估类等原子级规则点组成。目标客户挑选这一类型的规则点大多是由客户画像标签等演变而来，例如：“20 日日均资产 ≥ 5 万”是某一类客户画像标签，同时也可以作为营销活动的目标客户挑选规则点。

合规、风控类的业务规则具有将强的约束性，且必须满足，比较常见的有风控类的异常交易监控规则及合规类的适当性规则。

(1) 异常交易监控规则

异常交易监控大体上可以分为事前监控、事中监控两种方式。将此类规则进行梳理后，可以总结出原子化的规则点有如下几类：买入 / 卖出控制类、指标偏离类、额度控制类等。例如：“对集合竞价期间的委托价格，不得高于前日收盘价的 2%，对连续竞价期间的委托，不得高于市价的 2%”这一条价格偏离度的监控规则，进行原子化拆解后，由买入 / 卖出控制规则点“集合竞价期间”、“连续竞价期间”，指标偏离规则点“委托价格不得高于前日收盘价的 2%”、“委托价格不得高于市价的 2%”。

(2) 适当性规则

适当性管理规则作为外部监管类规则中重要

的部分，其规则涉及到业务办理和产品购买的各个环节，提炼了资质校验、资产校验、黑名单校验、投资经验校验、风险校验等等原子级的规则点，并且让规则在一定范围内可进行动态调整，满足适当性管理的灵活要求。

3.1.2 规则特点

通过对券商业务规则的梳理和分析，原子规则点及其由规则点组成的规则具有如下特征。

(1) 原子规则点复用性强

将规则点原子化后，出现了在不同活动场景下规则点复用的可能性，例如在活动营销时既需要编排好资源控制类、执行策略类规则点又需要考虑将适当性的规则点编排进来减少合规风险；在进行客户服务回访的业务规则设计时既需要目标客户挑选类规则点，又需要加入异常交易监控的规则点对客户进行有针对性的全面的回访服务。

(2) 规则复杂多变，耦合性强

客户的多态性和市场的多变性决定了上述规则的变化必然很频繁，且规则之间存在互相影响、互相制约的管理，例如：营销规则常常受到合规、风控等规则的约束。为了快速响应监管要求同时不错失营销机会，规则上线的时效性要求很高。

(3) 逻辑性

业务规则具有逻辑性，每条业务规则至少包含两个部分：条件部分和执行部分；规则的条件涉及到对业务数据作用的判定，规则的执行涉及到对业务数据的处理。业务规则会根据相应的条

件被触发执行，触发规则执行的“事件”就是业务数据本身。例如营销类规则中，渠道挑选类、目标客户挑选类、资源控制类规则点一般都组成完整规则的条件部分，执行策略类、效果评估类规则点则为执行部分。

(4) 非过程性

每种规则只能定义对一种现象的判断和操作，复杂的业务逻辑应该由多条规则协同处理。非过程性的特点让每条规则的制定变得非常单纯，可以“就事论事”，将复杂的过程处理平摊成一个个有条件的执行单元，实现从简单到复杂的只是累积过程。

(5) 非技术性

业务规则通常是业务人员制定的，业务人员应该使用行业语音而不是专业技术语音（如程序语言、数据库语言、脚本语言等）编写规则。

综上所述，将规则点整理后统一呈现后能够直观的展示规则之间的耦合程度，既使得业务人员可以像搭积木一样独立的完成活动规则设计，又减少了研发人员重复开发的工作量。

3.2 系统功能模块

业务规则决定了证券公司的运营策略，基于上述梳理结果及规则特点建立完整业务规则体系，从而帮助用户发现规则、表现规则、管理规则、自动执行规则、建立规则运行机制，最终实现业务规则管理系统的建设。系统的主要功能模块包含以下部分及流程示意图如下。

• 规则点管理

将梳理的原子化规则点按类型添加到系统中，对特定业务人员开放相关权限，支持对规则点进行增加、删除和修改。并进行上述规则的变化都需要经过规则创建人及使用人的审批。

• 规则编排，形成执行单元

以业务为维度，利用规则引擎进行规则的编排形成规则执行单元，对各业务负责人及相关用

户开放该功能，前端页面利用拖拽的形式自主编排形成个性化的流程图，将编排完成的流程图保存成执行单元。

• 执行单元发布

多条规则组成复杂的执行单元后，可以选择规则发布的渠道和时间，并经规则创建人、业务管理人审批同意后发布，通过测试后再各系统的生产环境中上线。

• 查询功能

对规则及执行单元进行查询，展示被使用的业务场景及规则的使用频率、执行结果等数据报表，便于数据分析人员发现和调整新的规则。

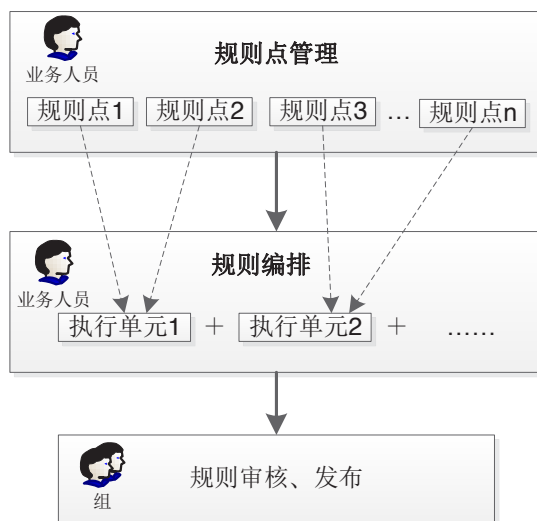


图2 规则编排流程示意图

4 典型业务场景

4.1 合规与风控业务

在券商的适当性管理工作中，业务管理人员可以对业务的适当性管理规则进行自主编排，形成不同的个性化执行单元最终建立该项业务的适当性管理流程。系统中通常通过以下步骤完成一个流程的配置，前端示意图如下图三所示。

• 选择需要进行配置的业务或产品销售的适当性管理种类，系统自动形成配置模板。

- 进行准入规则、办理中规则、办理后规则执行单元的逐一编排，业务人员可以通过拖拽的形式直观的完成执行单元的流程图设计。
- 将各执行单元组合成最终的适当性管理流程，并点击提交审核，发布到应用系统中。

4.2 营销活动

在营销活动开展的过程中必须要满足合规、风控的规则，所以营销规则不是单独存在的，通常是与合规、风控的规则共同组成营销活动执行单元，基于规则体系的统一建设与管理，使业务人员能够及时发现营销活动中的合规问题，并及时的调整使其适用于不同的活动与产品。系统中通常通过以下步骤完成一个流程的配置。

- 选择需要配置的营销活动类型，系统自动形成配置模板。
- 进入营销对象匹配规则、权益发放规则、权益使用规则执行单元的逐一编排，同时在执行单元编排时增加合规、风控规则以及已经编排好的相关执行单元供业务人员选择引用，完成活动

- 营销执行单元的流程图设计。
- 将各执行单元组合成最终的营销活动流程，并点击提交审核，发布到应用系统中。
 - 若需要对营销活动进行效果评估，还可以进行评估规则执行单元的编排和发布。

4.3 业务场景交叉

在营销的过程中有一个典型的应用场景就是“营销欺诈防控”，公司在营销活动的过程中业务人员可以根据之前提炼的经验自定义防控规则，通过在营销活动规则中增加合规规则的配置，如增加用户行为规则、反欺诈规则、黑名单甄别等一系列规则执行单元的配置，对防欺诈进行有效的识别和防范，实现了对薅羊毛行为的实时欺诈拦截，为公司的营销活动保驾护航。

在客户服务的过程中，为了使服务的展开更具有针对性，通常需要为不同的客户制定不同的服务策略，在业务人员形成客户服务策略的过程中，对于交易型客户，除了将营销类的规则考虑进来，还可以将异常交易类规则一并添加到策略

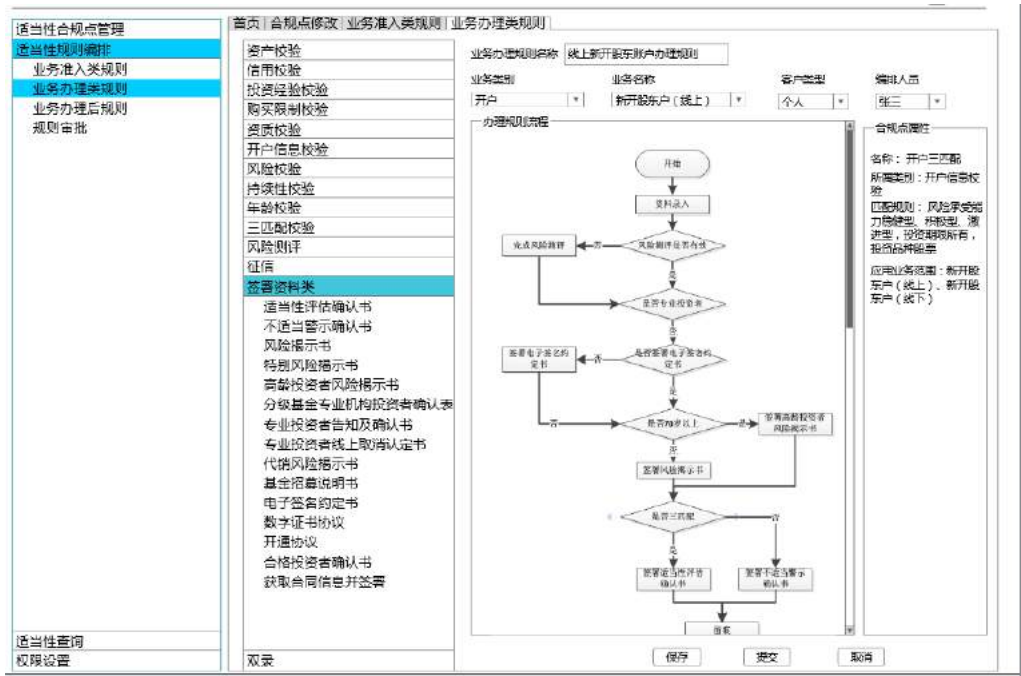


图 3 系统前端线框图

中来，生成策略执行单元，引导业务人员进行后续的客户服务路径。

5 总结

券商规则体系的建设将业务逻辑当做结构化的对象进行处理并统一管理，具有深远的应用意义。

（1）提高企业的核心竞争力

业务规则作为企业的核心资产，常常决定了金融业务的运营策略，是券商核心竞争力的体现。统一规则体系的建设终结了目前业务规则散落在系统内外各处，无法直观统一管理的无序状态，经过不断积累、调整和共享，并对规则进行版本管理，设定规则的有效期，实现业务行为的知识管理。同时在合规的基础上，发现更多的业务机会同时适应业务的创新和发展，提高了券商的核心竞争力。

（2）提升业务规则变更的响应速度

市场竞争及监管要求决定了券商需要不断调整业务策略来适应市场要求。基于业务规则方法使得简单的非技术性的概念容易被技术人员和业务人员所理解，业务人员不必涉及数据模型、处理模型和对象模型即可直接面对业务规则，大大缩短了业务人员的规则制定时间、系统的开发时间及费用。

（3）减轻 IT 部门开发工作量并提高系统运行稳定性

规则体系的建设使应用系统结构及其维护方式发生了巨大的改变，开发者可以直接使用技术语言而无需了解过多的实现细节，规则引擎的引入大大减少了编程的工作量，同时大幅减少了核心系统升级的次数，提高了系统运行的稳定性。

6 未来规划

建设统一的规则体系将来应向运营情况可视

化、规则形成智能化与应用场景多样化不断发展延伸，使得业务规则的统一管理更加具有应用价值。

运营情况可视化：业务人员编排的规则发布运行后，可以对规则的执行结果进行保存分析，并直观的展示在各位环节中提炼的数据指标。例如活动营销类规则，通过对活动效果评估结果分析规则的制定是否可以再次优化，若发现可以优化的环节，业务人员将分析的结果形成新的效果评估规则在进行营销活动编排时添加到规则执行单元中，形成一个闭环、动态调整的营销活动规则，便于业务人员在活动开展的过程中直观的根据活动运营的情况动态的调整活动规则。

规则形成智能化：业务规则最主要的能力是行为约束和知识推理，规则引擎可以进行逻辑判断，建立数据对象和规则之间的映射管理，并且能够动态组织与该数据对象相关联、满足条件的业务规则，自动实现这些规则之间的一致性、时间顺序、相容性等逻辑关系，从而推导出新的业务规则。随着机器学习能力的不断深入，业务人员对于各类规则的形成不再单纯依靠传统经验、口口相传，自动形成新的业务规则将会引导业务人员更快的发现营销线索，更好的规避合规风险。

应用场景多样化：规则的灵活配置让业务场景的选择更加的方便，如业务管理人员可以通过配置不同的营销活动流程进行 A/B TEST，不断优化出最优的营销方案并固化。线下的投顾人员也可以通过规则的配置挑选不同业务及产品营销的目标客户，通过效果评估将转化率较高的执行单元进行分享推广，使得线下投顾人员的能力不断得到标准化的提升。若将业务准入规则、产品画像及购买规则进行整理提炼面向客户端，客户也可以自己配置不同的规则，选择适合自己业务及金融产品提升客户自助理财的体验。

综上，统一规则体系的建设不但能够应对市场、客户、业务纷繁复杂的变化，而且能够延伸出更具价值的应用场景并创造更多的价值，具有一定的推广价值。

智能化多模金融数据 质量监控平台实现路径

覃剑钊、刘佳茜、张汉林、蒋荣 / 广发证券股份有限公司



摘要：金融数据质量是金融公司提供服务的重要基础，也是公司正常运行的前提保障。随着移动互联网、大数据等金融科技的飞速发展，金融公司的数据量及多样性与日俱增。传统的数据质量监控方法与体系已无法满足现代证券公司数据质量监控的需求。本文根据广发证券在智能化数据质量监控系统 X-monitor 的建设与运行经验，阐述一种智能化、自适应的多模金融数据质量监控实现路径。该系统利用自适应机器学习方法，将人工设定的数据质量监控规则与机器自学习生成的监控规则相结合，以提高金融数据质量监控的效率和准确度。系统同时支持监控模型的动态更新，以提高其动态适应性与灵活性。

关键词：数据质量监控；人工智能；机器学习；智能监控

1 引言

高质量的数据是金融证券公司提供服务、正常运行的前提基础。数据不稳定、缺失、异常等数据质量问题如果无法及时发现,将会导致证券公司在投资、理财、清算、风险管理、顾问等业务操作中出现问題,进而造成巨大的经济损失。同时,随着大数据技术、人工智能技术在证券公司各项业务应用的不断深入,大量的系统、业务决策的正确性均需要依赖于高性能的数据质量监督与控制系统。

异常数据的产生原因是多样的,如供应商表结构变化导致后台应用读入不正确的数据、数据读取时意外中止导致的数据缺失等。异常数据的表现形式也有所不同,如数据缺失、数据准确度低、数据的一致性出现异常等。一个完善的金融数据的质量监控系统需要针对各个数据类型、各种数据异常原因提出相应的解决方案。传统的数据监控模式需要开发人员和测试人员对不同数据制定不同的数据质量监控规则并编码实现,而面对海量的金融行情数据以及客户数据,这种人工监控方式不仅难以覆盖所有数据类型,还会消耗大量的人力和开发时间。同时人为制定的监控规则也会存在规则制定不合理,漏报、误报率高的缺点。基于此,本文构建了一种智能化多模金融数据质量监控方法与系统实现方案。该方法提出一种适合于多类型金融数据的智能数据质量监控规则自生成以及自适应更新方法,以此最大限度的减少人工干预水平,提高数据监控效率与成功率。另外,系统也支持人机结合模式,允许将人工设定的数据质量监控规则与机器自学习的监控规则相结合,以提高系统的灵活性和可控性。

本文分六章全面阐述了智能化多模金融数据质量监控的意义与系统实现方案。其中,第二章介绍了数据质量检测的意义及业内常用方法,第三章介绍了广发证券智能金融数据质量监控平台X-monitor的系统架构,第四章介绍了系统的具体

实现方法,第五章中通过实验来验证本文提出的算法可行性以及系统实际应用效果。第六章进行总结和对未来工作的设想。

2 背景

2.1 金融数据质量监控的重要意义

对金融公司来说,高质量数据是公司业务正常运转的前提保障。例如,当数据的正确性与完整性缺失时,将会导致智能投资策略与客户投资建议等重要模块发生错误,进而导致客户投资发生损失。当文本型数据如投资标的资讯、投资标的公告、产品说明等文本内容出现错误、缺失等异常时,将会影响到客户的投资决策,导致客户对公司的忠诚度下降。加强金融数据质量监控具有重大的意义,具体表现如下:

1. 金融数据质量监控有助于提升证券公司数据治理水平的效率和质量。传统的数据监控模式需要耗费较多人力,且对开发人员与测试人员的业务经验有较强的依赖。这种监控模型会消耗大量的人力和开发时间,同时人为制定的监控规则也存在着规则制定不合理,漏报、误报率高等问题。

2. 金融数据质量监控有助于提升证券公司各项业务水平及服务质量。目前证券公司的各条业务线数字化程度越来越高,传统经纪业务在向客户提供交易通道的同时,也向客户提供各种可交易证券的报价、新闻资讯等数据服务。当前蓬勃发展的财富管理业务,包括基于大数据技术及人工智能技术的智能投顾业务均依赖于可靠稳定的行情数据及客户数据。证券自营业务、资管业务的量化交易系统也高度依赖数据产生投资决策。因此,一个高效、可靠的数据质量监控系统,可以提升证券公司各项业务线的业务水平及质量。

3. 金融数据质量监控有助于提升证券公司对内的经营分析质量和风险控制质量。目前证券公

司的经营分析与经营决策正快速向数据驱动型转变，分析与决策越来越依赖于大量的数据统计和分析结果，因此高度自动化、可靠的数据质量监控系统，将有助于提升证券公司的经营分析与决策水平。风险控制是证券公司稳健经验的核心基础，而当前国际、国内成熟的风险控制模型无不依赖于大量的数据建模，因此高度自动化、可靠的数据质量监控系统，将有助于提升证券公司风险控制水平。

2.2 业界常用方法简介

随着各类大数据前沿技术的不断发展与在各应用的不断深入，各领域对数据质量的要求不断提高，数据质量监控的研究也成为业内的热门研究方向。IBM 提出一种数据质量监控的方法^[1]，通过将加载数据的质量与预定的数据质量对比来实现数据监控；格泰科技有限公司提出一种数据质量网络监控管理产品^[2]，该产品提供日常数据质量监控的信息采集、规则监控、问题告警、问题申告处理、质量报告、知识沉淀及任务调度等功能；集奥聚合科技公司提出的数据质量监控方法^[3]主要从四个方面实现：配置监控规则、传递监控规则、识别监控规则与输出监控数据；国家电网公司公开了一种电力大数据质量实时监控方法^[4]，它将企业应用数据流实时输入并对数据流分批，采用 DStreams 与 Spark 分别完成流式计算与批处理执行转换、并使用 Spark 框架实现任务调度、内存管理和结果输出；江苏智通科技有限公司提出了一个包含监测模块、风险预警模块、数据核查模块、决策支持模块和参数配置模块的监测系统^[5]，实现了对交通数据的质量监控。从业界近期公布的方法中，我们可以看到大数据分布式处理技术已经开始引入到数据监控系统中，然而数据监控规则的配置普遍仍然采用纯人工配置的方式，这种方式将无法满足证券公司日益增长的数据监控需求。

3 广发证券智能金融数据质量监控平台 X-monitor 概述

针对传统数据监控方法的不足，我们提出一种“平台化+智能化”的解决方案。该方案具有通用化、智能化、个性化的特点，可以及时、准确、高效的发现数据问题。其创新之处在于：

1. 系统支持多项目管理、多类型数据源接入。具有灵活的监控调度，支持多种时间级别（分钟、小时、日、周等）监控调度和多层级报警，能够及时发现数据的隐患。

2. 系统提供自学习监控策略自主生产监督规则，这不仅能够降低数据监控成本，还可以提高对数据异常问题监控的及时性与数据准确性。

3. 系统支持智能数据一致性检测。金融数据的一致性检测是发现隐藏数据质量问题的重要手段之一。传统数据质量检测方法的实现需要人工对数据的取值范围、数据空缺等参数进行手工设置和编码，但人工设置数据检测规则很容易忽视数据之间的一致性，导致一些数据问题只看单一数据字段没法发现。即便考虑了不同数据字段数据一致性的问题，传统方法需要人工指定待一致性检查的数据字段，然后再定义相应的规则并编码实现。当面对海量的金融行情数据、客户数据，人工指定数据字段进行一致性监控规则将消耗大量的人力。同时，人为设定待一致性检测数据字段需要设置人员具备丰富的业务经验，否则容易产生遗漏。为了解决这些问题，我们的数据质量监控系统支持自动发现需要进行一致性检测的数据字段，并且具备自动学习数据一致性检测规则的能力。

4. 系统支持数值、文本、图像等多模态数据。平台运用文本处理、图像识别等技术对不同类型的待监控数据进行特征提取，将文本类数值、图像类等非结构化数据进行向量化，转化成结构化数据，再利用数值型数据自动监控规则生成与更新方法对向量化后的非结构化数据进行自动监控

与规则更新。

图 1 展示了 X-monitor 界面。首界面除了展示当前的总任务数与成功率外，还给出了各监控项目的状态、任务名、任务类型、运行时间等信息，并允许监控人员对调用接口、监控方向进行调整与配置。

X-monitor 中的“策略”板块下展示了平台目前支持的智能策略。

系统同时支持开发人员根据具体应用情景、反馈结果等信息对监控策略进行调整。如图 3，在“策略”板块中，系统允许开发人员对不同智能策略的超参数进行设置。

4 智能金融数据质量监控系统实现

4.1 系统架构

广发证券的智能数据监控系统 X-monitor 的主体架构如图 4 所示。

基础层主要由容器云、基于 Apache Spark/Flink 的大数据计算平台及各类数据库组成。其中，容器云具有可弹性扩展、容易维护、容易测

试等特点，任务调度、消息推送、数据接口与数据 API 的监控计算任务、部分数据库数据的监控计算任务等后台应用通常运用容器云完成。基于 Apache Spark/Flink 的分布式计算引擎通常负责分布式数据库数据的监控计算任务。而 Mysql、Postgresql、Mongodb 等各类数据库通常用于配置参数、系统参数、部分监控规则的存取。

基础模块层主要由机器学习算法、自然语言处理算法、图像处理算法、任务调度 API、消息推送 API、数据读取接口及 API 等通用模块组成。机器学习算法模块为监控规则自学习功能提供基础机器学习算法支撑；自然语言处理算法模块主要提供 Word2vec、Fasttext、分词等常用自然语言处理算法，为文本数据的特征提取提供算法支撑；图像处理算法模块主要为图像数据的向量化提供算法及模型基础；任务调度 API 模块负责提供任务调动的常用接口；消息推送 API 主要提供短信推送、微信推送、邮件推送等消息推送接口。

应用层由实现系统核心功能的主体模块组成。具体包括数据预处理、监控规则自生成与更新、监控计算、监控结果反馈、数据读取、消息推送等功能模块。

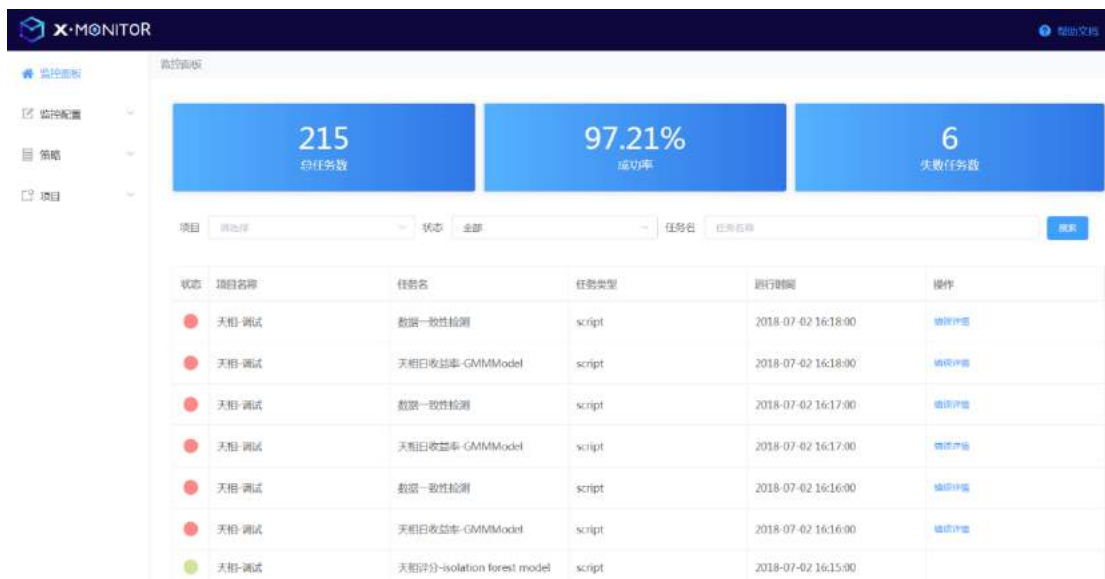


图 1 智能金融数据质量监控平台（X-monitor）界面



The screenshot shows the X-MONITOR web interface. On the left is a sidebar with navigation options: '监控面板' (Monitoring Dashboard), '监控配置' (Monitoring Configuration), '策略' (Strategy), '列表' (List), and '项目' (Project). The main area is titled '策略 / 列表' (Strategy / List) and displays a table of monitoring strategies.

名称	脚本文件	操作
高斯混合模型	GMM_checker.py	编辑 删除
线性相关数据的检测	corr_analysis.py	编辑 删除
高斯模型	GaussianModle.py	编辑 删除
Isolation Forest	isoforest_checker.py	编辑 删除
One-class SVM模型	oneSVM_checker.py	编辑 删除

图 2 智能金融数据质量监控系统使用的模型



The screenshot shows the '策略 / 新增' (Strategy / New) configuration form. It includes fields for '策略名称' (Strategy Name) set to '高斯混合模型', '脚本名称' (Script Name) set to 'GMM_checker.py', and a '默认参数' (Default Parameters) section with a '+ 增加' (Add) button. Below this is a table for parameters with columns '参数名' (Parameter Name), '参数值' (Parameter Value), and '参数描述' (Parameter Description). A '提交' (Submit) button is at the bottom.

参数名	参数值	参数描述
<input type="text"/>	<input type="text"/>	<input type="text"/>

图 3 系统支持对智能策略的配置

用户交互层主要实现 Web 端、移动 App 端的交互功能。

4.2 应用层主体模块

系统主体模块关系图如图 5 所示。
金融数据质量监控系统的主体功能主要由以下模块组成：数据读取配置模块、数据读取模块、数据预处理模块、监控规则生成与配置模块、监控计算模块、消息推送模块、反馈模块。

数据读取配置模块对待监控数据的读取调用进行配置。该模块允许用户通过用户界面（如 Web 或移动 App）对待监控数据的数据源或者待监控数据的前端读取接口进行配置，同时也可以支持用户输入符合系统设计标准的数据读取源代码进行数据读取。当用户在用户界面设置完成并确认后，设置的内容将通过应用服务器将设置内容写入应用数据库，其中应用数据库可选取 mysql、postgresql、mongo 等。

数据读取模块实现对数据的读取。该模块根

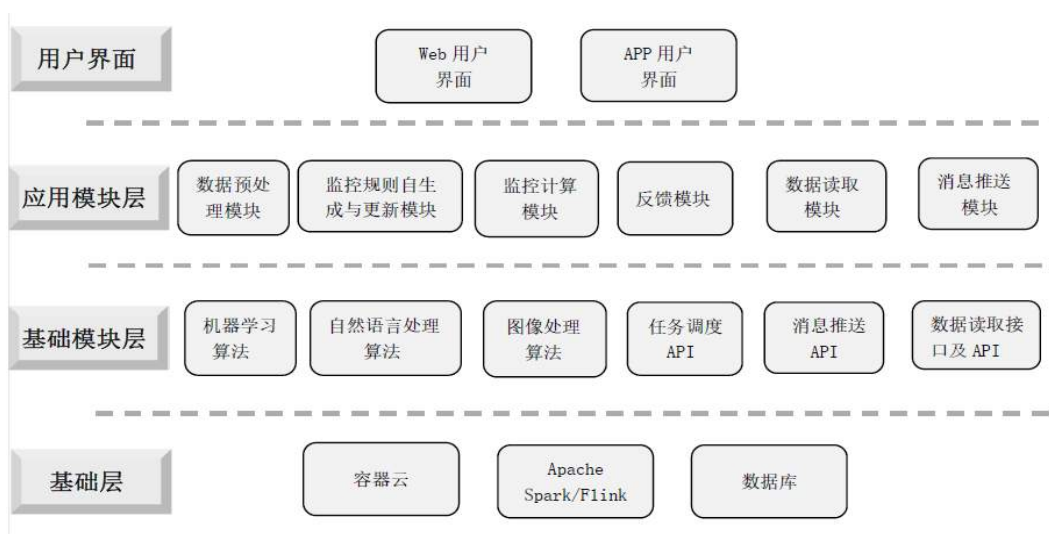


图 4 系统架构图

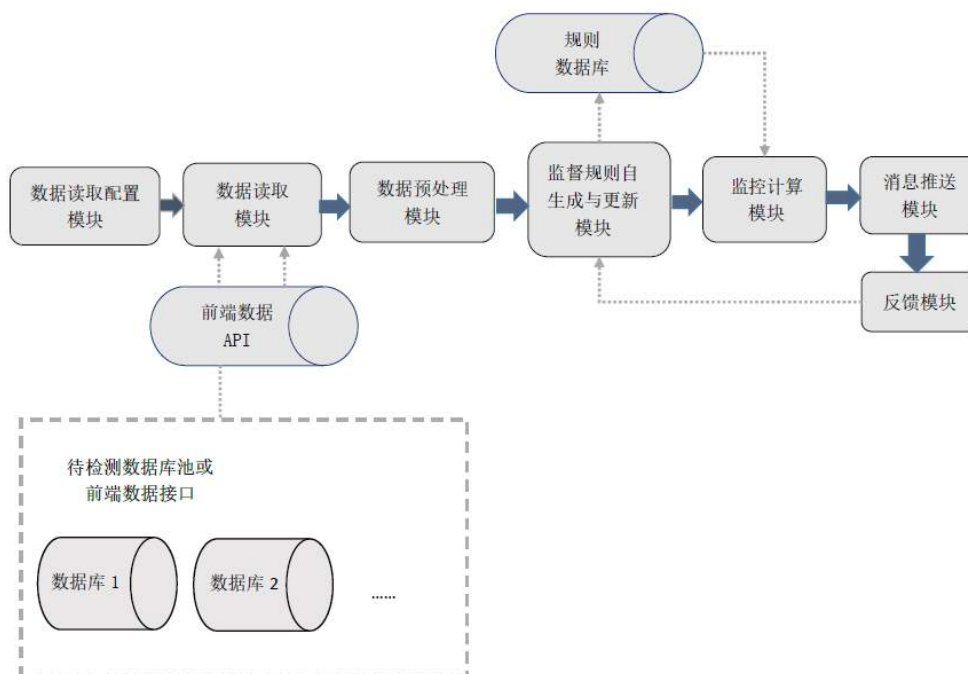


图 5 系统主体模块关系图

据已配置的读取方式对待监控数据、待监控数据的历史正常数据进行读取。数据读取模块根据用户输入的数据库类型、IP 地址、用户、密码、待监控数据所在的数据表、表中字段名等参数对数据进行读取。为了支持更丰富的数据读取方式，该模块也支持用户输入符合规范的数据读代码模块以供计算服务单元调用获取数据。

数据预处理模块利用数据智能预处理层的策略对待监控数据进行处理。该模块将文本类、图像类、音频类等非结构化数据转化成结构化数值后，再标准化成生成监控规则所需要的数据格式。同时该模块也需要自动筛选出强相关的数据字段对，为一致性检测提供待检测数据。

监控规则生成与配置模块将智能策略自动生

成的监控规则与人工规则结合, 以实现监控规则库的不断更新与完善。该模块在对智能监控规则模型的超参数进行配置后, 利用标准化的待检测数据与选定的机器学习方法对监控规则进行自学习, 或者根据更新的待检测数据对监控规则进行自动更新, 最后将学习或更新后的监控规则存入规则数据库。同时, 该模块还支持人工对自生成的监控规则进行修改、调整或添加新的规则。由于机器学习产生的数据监控规则在历史正常数据较少的情况下, 容易出现监控规则不够完善的情况, 故此设计提高了系统的灵活性及适应性。

监控计算模块利用最终配置完成的监控规则对新增待监控数据进行计算, 根据输出的结果判断该新增数据是否触发数据异常报警。

消息推送模块将输出的数据质量监控报警信息利用消息推送系统推送给客户, 消息推送系统可包括微信、短信、应用 App 等渠道。例如: App 推送可通过 MQTT、XMPP 等协议实现, 也可以调用阿里云移动推送、腾讯信鸽推送等第三方平台实现。

反馈模块负责接收运维人员对数据监控报警的反馈信息, 并将该反馈信息反馈给监控规则生成与配置模块。数据开发、测试人员根据反馈结果对监控数据进行人工调整和优化。如果反馈发出报警的信号为假信号, 则需要反馈给监控规则生成与配置模块, 根据具体原因及时进行监控规则调整。

4.3 智能监控规则生成方法

4.3.1 数值型金融数据监控规则

金融产品行情收益率的分布通常可近似认为服从高斯模型或高斯混合模型。因此该类数据的监控规则可利用高斯模型、高斯混合模型来建立。一维数据的高斯模型数学表达式为: $p(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$ 其中参数 μ , σ 分别为训练数据的均值和标准差。多维数据的高斯混合模型的数

学表达式为: $p(x) = \sum_{i=1}^K \frac{\omega_i}{\sqrt{2\pi}\sigma_i} e^{-\frac{(x-\mu_i)^2}{2\sigma_i^2}}$ 。其中, $\sum_{i=1}^K \omega_i = 1$, K 为高斯模型的数目, ω_i , μ_i , σ_i 分别为第 i 个高斯模型的权重、均值和标准差。这些参数可以利用历史正常数据, 采用 EM (Expectation Maximization) 算法进行估计。

当待监控数据的分布模型未知时, 可以采用 One-Class SVM 或 Isolation Forest 对待监控数据进行建模。One-Class SVM 模型在异常数据检测中被广泛使用, 它通过历史正常数据构造支撑超平面, 以此判断待监控数据是否为正常数据。Isolation Forest 模型也是一种无需事先知道数据分布模型的方法, 由于异常数据具有在生成树中经过的路径 (即树的节点个数) 较短的特点, Isolation Forest 利用该特性实现异常数据的检测。

4.3.2 文本型金融数据监控规则

文本数据是金融数据的重要组成部分, 这些数据包括投资标的相关新闻、投资标 公告、金融产品说明以及金融公司内部文档交互等。这些文本数据是金融公司提供客户服务的重要基础, 也是公司正常运行的重要基础。

要完成文本数据监控规则的自动生成, 首先需要把文本数据映射成数值向量, 然后利用上述数值型监控规则自动生成方法完成规则的生成。我们采用以下方法将文本向量化:

首先建立分词模型和词向量模型。由于金融类文本包含了大量金融专业术语和独特的金融产品名称, 采用通用分词模型容易导致文本分词结果错误。因此, 在进行分词模型训练前, 需要人工 (或结合新词发现的方法) 进行词库扩充。完成词库扩充后, 再利用更新后的词库进行分词模型的训练。常用的分词模型有隐马尔科夫 (HMM), 条件随机场 (CRF) 等模型。在进行词向量模型训练时需要采集 wiki、金融资讯、金融公告等文本数据, 并利用训练好的分词模型对这些文本数据进行分词。得到文本数据的分词后, 利用 word2vec 算法或 Fasttext 方法建立词向量模型。其中, Fasttext 中的词向量训练与 word2vec 相似,

主要有两种方案：一种是通过中心词 w_t 来预测周边词 $w_{t-2}, w_{t-1}, w_{t+1}, w_{t+2}$ ，称为 Skip-gram 模型；另一种是通过周边词 $w_{t-2}, w_{t-1}, w_{t+1}, w_{t+2}$ 来预测中心词 w_t ，称为 CBOW (Continuous Bag-Of-Words)，即连续的词袋模型。二者都是通过计算单词之间的共现关系来实现训练，即把相关词汇映射到词向量空间的模型。

得到训练好的分词模型后，需要用该模型对待监控历史文本数据进行分词，接着采用词向量模型把文本数据的分词结果映射到词向量空间。

最后，系统将计算历史文本数据的词向量分布以形成文本数据的数值向量表达。得到文本数据的数值向量表达后，即可采用数值型监控规则自生成方法中采用的高斯模型、高斯混合模型、One-Class SVM 等模型完成监控规则的自动生成。

4.3.3 图像数据监控规则

证券公司投资银行业务在对公司进行实地调研与持续督导过程中，通常会通过拍摄、复印、扫描等方式获取待调研待督导公司相关资料。公司本身也会通过图像方式（如证明材料的扫描件）来提交材料。

图像数据监控规则的自动生成首先需要把图像数据映射为数值向量，然后利用上述数值型监控规则自动生成方法完成规则的生成。

我们在系统实现中采用了以下方法完成图像数据向量化：首先，将大量通用图像数据与证券行业特有图像数据相结合进行深度学习模型 Autoencoder 的训练。然后，通过训练好的 Autoencoder 模型将图像数据映射到数值向量空间。最后，采用数值型监控规则自生成方法中的高斯模型、高斯混合模型、One-Class SVM 等模型完成监控规则的自生成。

4. 智能数据一致性监控

数据内容的一致性指的是两个线性相关的数据字段的数据应该保持其线性相关性。例如，当一只基金的评分越高时，其对应的评级也应该越好。由于金融数据体量庞大，人工设定需要进

行一致性检测的字段是不现实的，所以我们提出一种自动发现需要进行一致性检测的数据字段的方法：(1) 首先计算相关字段数据的协方差矩阵 $\Sigma = E[(x-u)'(x-u)]$ ，得到字段数据间的相关性度量。其中， x 为多数据字段数据组成的向量， u 为这些向量的均值。(2) 然后设置相关度的阈值，以筛选出强相关数据字段。完成字段对筛选后，利用一个字段对另一个字段的线性回归，计算出回归值与待检测值的差值。最后利用数值型检测规则自生成中的高斯模型、高斯混合模型、One-Class SVM 等模型对差值建立监控规则。

5 系统评估

5.1 智能监控规则生成方法实验验证

为验证智能策略在数据监控中的性能，我们设计实验检验三种智能监控规则生成方法 (GMM, Isolation Forest 与 One-Class SVM) 对异常数据的检出效果。实验选取天相基金数据作为数据集，抽取了 100 支基金，共 20100 个净值数据来训练各模型。实验根据各基金的数据分布情况模拟生成异常数据，将其标记后混入正常数据，用训练好的模型输出检测到的异常数据，以此比较各模型的检测性能。测试过程中使用的评估指标包括召回率、准确率与 F1 值。

本实验主要分为两部分：各模型最优参数的确定与模型的对比。前者显示，各模型在其最优参数下对异常数据均有优秀的检测能力。其中，One-Class SVM 与 isolation Forest 的召回率与精确率均可达到 100%，GMM 效果相对逊色，但也达到了 99.8% 的召回率与 100% 的精确率。为对比各模型对异常数据的检测能力，我们调整异常数据的生成方式以增大异常数据的甄别难度。结果显示，One-Class SVM 的综合表现最佳，它在数据检出率与时间效能上都表现突出，其次是 GMM 模型，它在 F1 值与 isolation Forest 相差

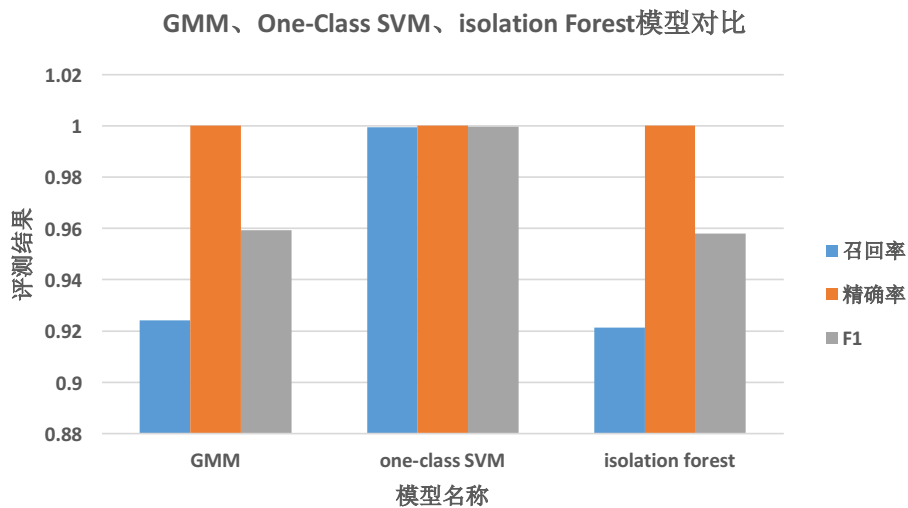


图 6 三种模型在异常数据检测实验中的结果

无几的情况下具有更低的时间复杂度。不过尽管 One-Class SVM 的表现相对较弱，其对异常数据的检测率仍然可达到令人满意的程度。模型对比的统计结果如图 6。

具体数据如下表：

表 1 实验结果

模型 评测指标	GMM	One-Class SVM	Isolation Forest
召回率	0.924235	0.999375	0.921279
精确率	1	1	1
F1 值	0.959276	0.999677	0.957915

实验验证了三种模型在异常数据检测上的优越性能，进而证实了统计模型及机器学习模型用于监控规则生成的可行性，模型生成与更新的高效性更为海量金融数据的处理带来了便利。

5.2 系统应用

目前平台在广发证券贝塔牛、广发证券财富管理平台、交易测试柜台等系统中进行了监控测试，运行了上千次监控任务。初步验证了平台的

有效性与实用性。

6 结论与展望

对金融数据的分析处理一直是金融证券公司提供服务的重要基础。随着大数据技术与人工智能在证券公司的不断拓展应用，金融数据的质量监控成为维系公司业务正常运行的前提保障。本文针对金融数据的质量监控，根据广发证券智能数据监控平台 X-monitor 的实现路径，介绍了一套“平台化 + 智能化”的解决方案。最终搭建的监控平台不仅支持对数据库进行实时数据监控，也允许配置 API 支持与大部分周边系统的对接。与传统的人工设置监控规则不同，该平台利用机器学习方法，将智能监控策略与人工规则结合。这不仅降低了数据监控成本，更提高了对异常数据的监控及时性与准确性。从测试与运行结果来看，该平台具有明显的有效性与实用性。

尽管本文构建的金融数据质量监控系统在性能上已经取得不错的成效，但随着数据规模与复杂度的不断提升，金融公司中各业务对数据质量

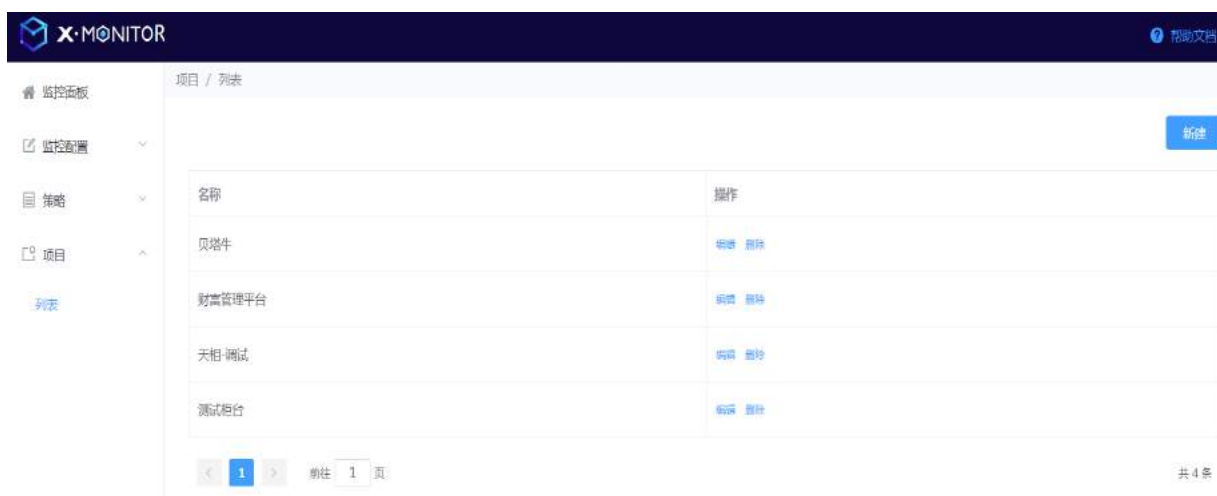


图 7 广发证券 X-monitor 平台应用于贝塔牛、财富管理平台等项目

要求也在不断提高。后续工作中，我们将继续提高平台的智能化水平。本文目前仅在数据质量的监控规则建立时利用人工智能技术，未来将考虑

将智能策略融入数据监控的其他方面，如数据的自动平稳化、数据地图的自动生成、异常数据源的智能定位等方向。

参考文献：

- [1] M• 奥伯霍菲尔 ,J• 塞弗特 ,Y• 赛勒特 ,S• 尼尔克 . 用于数据质量监控的系统和方法 . 欧洲专利 : 201210225743X. 2013-01-02.
- [2] 何万军 . 一种数据质量网络监控管理产品 . 中国专利 : 2015108035291, 2017-05-31
- [3] 何良均, 张翼等 . 一种数据质量监控的方法及系统 . 中国专利 : 2016108322820, 2017-02-15
- [4] 魏智博等 . 一种电力大数据质量实时监控方法 . 中国专利 : 2016104937192, 2018-01-05
- [5] 吕伟韬等 . 交通数据质量监控系统 . 中国专利 : 2016108051886, 2017-01-25
- [6] Krizhevsky A, Hinton G E. Using very deep autoencoders for content-based image retrieval.[C]. the european symposium on artificial neural networks, 2011

作者简介：

覃剑钊，香港大学博士，现任广发证券信息技术部资深工程师。在数据分析、算法设计、人工智能领域有多年研发经验，相关领域国际著名期刊 / 会议发表论文 20 余篇，被引用近 300 次，曾担任 IEEE Transactions on Fuzzy Systems, IEEE Transaction on Cybernetics 等国际著名期刊的论文审稿员，已获授权发明专利 10 多项。Email : qinjianzhao@gf.com.cn。

刘佳茜，广发证券实习生，中山大学在读硕士。Email : jiaxilua@163.com。

张汉林，广发证券信息技术部副总经理。Email: gfzhl@gf.com.cn。

蒋荣，哥伦比亚大学博士、特许金融分析师（CFA），现任广发证券信息技术部总经理。曾任威灵顿管理公司（波士顿总部）董事总经理。Email : jiangrong@gf.com.cn。

作者联系地址：广州市天河区花城大道 667 号美林基业大厦 14 层

基于区块链技术 构建可信仓单系统的研究

李博 / 大连飞创信息技术有限公司 创新实验室, libo@dce.com.cn

潘文锋 / 大连飞创信息技术有限公司, panwenfeng@dce.com.cn



摘要：仓单是大宗商品流通的重要工具，对于节约交易成本，提高大宗商品的流通效率具有重要的作用。但是长期以来,我国非标准仓单市场存在仓单信息缺失、信用担保不足和流动性不佳等问题。为解决这些问题，本文提出了一种基于区块链技术构建可信仓单系统的解决方案，设计了区块链仓单系统模型，使用开源区块链产品 HyperLedger Fabric 进行了概念验证。基于区块链技术构建可信仓单系统对于我国仓单市场的健康持续发展具有重大意义。

关键字：仓单；区块链技术；可信仓单系统

Abstract: Warehouse receipt is an important tool for the circulation of bulk com-

modities, which plays an important role in reducing transaction costs and improving the circulation efficiency of bulk commodities. However, the non-standard warehouse receipt market of China has faced problems such as lack of warehouse receipt information, insufficient credit guarantee and poor market liquidity. In order to solve these problems, this paper proposes a solution to build a trusted warehouse receipt system based on blockchain technology. It designs a blockchain warehouse system model and uses the open source blockchain product HyperLedger Fabric to carry out the proof of concept. The construction of a trusted warehouse receipt system based on blockchain technology is of great significance for the healthy and sustainable development of China's warehouse receipt market.

Key words: Warehouse receipt; Blockchain technology; Trusted warehouse receipt system

1 引言

仓单是仓储物经过“资产证券化”后的流通票据,在降低货物仓储、物流环节的损耗和提高大宗商品的流通效率方面发挥着不可替代的作用。仓单除了具有标识仓储物的所有权的基础功能外,还具有有价证券的属性。近年来,围绕仓单开展的业务创新不断丰富,包括仓单串换、远期和回购、质押融资等业务。这些业务对仓单的信用水平有较高的要求。纵观非标准仓单市场的发展现状,存在仓单信息缺失、信用担保不足、流动性不佳等问题,难以满足仓单业务的要求。

区块链技术的发展,为解决非标准仓单面临的上述问题提供了技术上的新思路。区块链技术具有的去(多)中心化、数据公开透明、数据可溯源和难篡改特性对于构建组织间的互信关系,提高仓单信息的可信度,跟踪和记录仓单流转的完整信息具有重要意义。依托核心机构的权威性建立仓单市场联盟,有利于实现核心企业的信用传递,提高仓单的信用水平。提出区块链与物联网技术结合的建议,有利于把对机器的信任延伸

至物理世界,利用传感器技术、RFID 标签和嵌入式技术打通物理世界与数字世界的信任壁垒,建立可信仓单系统体系。

2 仓单在应用时存在的问题

仓单是在存货人按照仓储合同约定将仓储物交付给保管人后,由保管人向其出具的提取仓储物的凭证。仓单是仓储合同当事人(存货人和保管人)履行仓储合同义务的证明,即存货人已履行了交付仓储物给保管人的义务,保管人履行了对仓储物进行验收的义务。仓单是一种物权凭证,存货人获得仓单,即意味着获取了仓单表示数量和品种的仓储物的所有权,仓单持有人可凭仓单请求保管人给付仓储物。仓单还是一种有价证券,仓单持有人对所持仓单及其标的仓储物拥有处置权,可以通过在仓单上背书并经保管人签字或盖章后转让仓单项下仓储物的所有权,也可以通过质押仓单获取融资服务。

在我国,仓单有标准仓单和非标准仓单的分类。标准仓单是由期货交易所指定交割仓库

签发的实物提货凭证，需要经过规定的流程并经交易所注册后始生效。非标准仓单是标准仓单的补充，凡是不满足标准仓单注册条件的仓单都是非标准仓单。通常情况下，非标准仓单是由仓储机构为货主出具的仓库保管单、入库单等有效凭证。

目前，仓单在我国市场应用中存在以下问题：

2.1 仓单信息孤岛现象严重。

我国仓单业务种类丰富、流程复杂，涉及的参与方众多。通常参与仓单业务的机构间系统相互独立，信息孤岛现象明显，尤其是仓单在经过多次转让、连续交易、质押等操作后，极易发生有效信息的缺失，造成信息链条不完整，权责不明确等问题。这些问题加大了监管部门对当事人道德监控的难度，容易滋生虚开仓单、重复质押等风险事件。

2.2 非标准仓单信用担保不足。

我国仓单的信用水平高低不一，总体表现为标准仓单的信用水平高于非标准仓单的信用水平。标准仓单有交易所对其进行信用背书，具有较高的信用水平。非标准仓单的信用水平则主要依赖于签发主体和第三方信用担保机构，通常签发非标准仓单的机构在规模和抗风险能力方面表现欠佳，能够为非标准仓单提供信用背书的第三方担保机构也十分有限，因此非标准仓单面临信用担保不足的问题。

2.3 仓单的流动性不佳。

标准仓单的持有成本较高，通常只应用于大宗商品外贸现货和国内的期货交易所，市场体量有限。非标准仓单的数量远远超过标准仓单的数量，属于仓单市场中的长尾部分。但是非标准仓

单因为面临信用担保不足的问题，所以其信用水平较低，市场流动性表现不佳。质押融资方面，仓单质押业务活跃度不高，参与银行融资的仓单数量占比不到 5%。

3 区块链技术解决仓单面临的关键问题

区块链的思想诞生于 2008 年中本聪 (Satoshi Nakamoto) 发表的题为《比特币：一种点对点的电子货币系统》的论文。他提出了一种在没有可信任第三方机构参与的情况下，通过点对点网络解决双重支付问题的方案。该方案使用了时间戳、数字加密、分布式共识机制等关键技术，人们把这种揉合了多种信息技术的分布式记账方式叫做区块链技术。区块链本质上是建立了一种公平、公开、公信的交易机制，具有去中心化的特点。它通过创建数据公开透明和不可篡改的交易环境来抑制参与者作恶的心理，通过组织参与机构进行相互监督来规范参与者的交易行为，共建组织间的信任关系。

本文第一部分阐述了我国仓单在应用时存在的问题，分析其原因在于仓单市场缺少有效的仓单信息公示机制和行业公认的仓单信用标准。区块链技术具有的信息公开透明，数据可溯源和难篡改特性对于解决上述问题具有积极的意义。

3.1 建设高可信的仓单信息公示平台。

使用区块链技术建设仓单信息公示平台，解决参与机构间的信息孤岛问题，提高仓单信息的可信度。区块链技术也叫做分布式账本技术，区块链网络中的每个节点都维护着一份相同的账本，联盟成员可以基于本地的账本准确地获取仓单的基本信息，跟踪仓单注册、转让和质押等流转信息，有效地避免因仓单信息缺失导致仓单多重质押等风险事件的发生。

3.2 建立联盟成员公认的仓单信用标准。

使用区块链技术构建仓单市场联盟，依托核心企业的权威性，建立联盟内公认的仓单信用标准。我国仓单业务涉及的参与机构具有种类多、数量大，规模各异的特点，不具备建立中心化信任模型的基础条件。利用区块链技术构建仓单市场联盟，由核心企业组成联盟链的多中心组织，对区块链网络内的仓单业务进行信用背书，有利于核心企业的信用传递，提高非标准仓单的信用水平。

4 模型的设计与构建

4.1 基于区块链技术构建可信仓单系统的模型设计

我国仓单市场缺少有效的仓单信息公示机制和行业公认的仓单信用标准。解决该问题的关键是建立一个信息公开透明，仓单公信度高的仓单市场联盟。本文设计了一种基于区块链技术构建可信仓单系统的解决方案，其逻辑模型如图 1 所示。



图 1 基于区块链技术构建可信仓单系统的逻辑模型

本模型的参与机构包括仓单持有人、仓储机构、信用担保机构和银行。其中，仓单持有人为

仓单的实际所有者，持有人可以基于所持仓单开展多种业务；仓储机构是仓储物的存管机构，拥有仓储物的监管权；信用担保机构可以对仓单的信用做担保，提高仓单的信用水平；银行在仓单质押业务中充当质权人的角色。

模型中将上述参与机构分为核心机构和普通机构，其中，核心机构是指在行业中发展较好、具有权威性的企业，包括核心仓储机构、核心信用担保机构和核心银行；普通机构是指经营规模较小的市场参与者，包括仓单持有人、普通仓储机构、普通信用担保机构和普通银行等。

为每个参与机构搭建专属于自己的区块链节点，这些节点上存储着相同的仓单账本，记录着仓单的信息。在该模型中选择核心仓储机构、核心信用担保机构、核心银行的区块链节点形成联盟链的多中心组织，负责对区块链网络中发生的每一笔仓单业务进行确认和信用背书，普通的节点只需要对与自己相关的仓单业务进行验证和背书签名即可。

基于区块链技术构建的仓单系统模型，其上流转的仓单信息具有公开透明、数据可溯源和难篡改的特点，是一个可信度较高的仓单信息公示平台；经过区块链仓单系统办理的仓单业务不仅由参与双方承认，还得到了核心机构的认可，有利于提高仓单的信用水平，形成行业公认的仓单信用标准。

4.2 基于 HyperLedger Fabric 构建可信仓单系统

HyperLedger Fabric 是一种开源的区块链技术产品，是目前应用最广泛的联盟链产品。Fabric 提供了身份管理、账本管理、交易管理、智能合约（链码）管理等功能，能够快速搭建商业区块链平台。本实验使用 Fabric 1.2.0 版本搭建可信仓单系统原型，以验证上述模型的可行性。基于区块链技术的可信仓单系统架构图如图

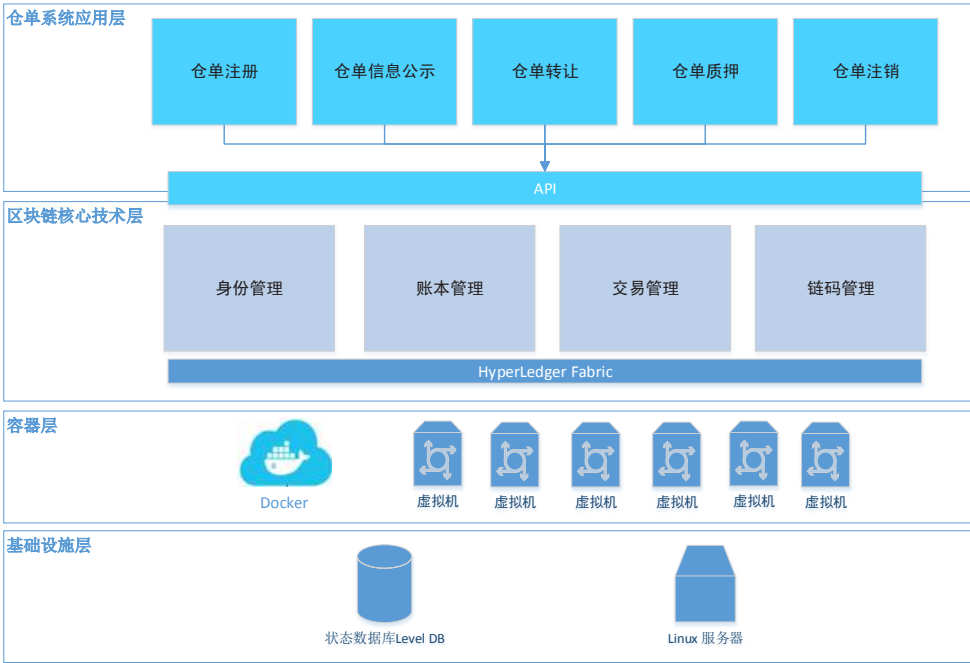


图 2 基于区块链技术的可信仓单系统架构图

2 所示。

该系统的实现分为 4 层结构，自下而上第一层是基础设施层，使用 Level DB 作为区块链的状态数据库，Linux 服务器提供系统服务；第二层是容器层，使用 Docker 技术虚拟化多个 docker 容器来代表不同的网络节点；第三层是区块链核心技术层，使用 Fabric 在 docker 容器之间建立区块链网络；第四层是仓单系统的应用层，通过 Web 应用调用 Fabric 提供的 API 与区块链网络进行交互。

该实验构建了一个包含 1 个 Orderer 排序服务节点和 7 个 Peer 节点的区块链仓单系统，其中区块链系统中各个节点的功能描述如表 1 所示。

该实验的区块链系统中包含两种类型的节点，一种是 Orderer 节点，负责对系统中的交易数据进行排序，生成区块；另一种是 Peer 节点，负责在区块链系统中发起交易，背书交易结果，验证区块和记录账本数据。区块链仓单系统中的核心机构节点与普通机构节点都属于 Peer 节点，但是二者在功能方面存在差异：1、对交易进行

签名背书时，普通节点只需要对和自己有关的仓单业务签名背书，核心节点需要对网络中发生的所有仓单业务签名背书。2、普通机构节点具有发起仓单业务、背书仓单信息、查询和记录仓单账本数据的基础功能，核心机构节点除了具有普通机构节点的功能外，还具有管理同类型普通节点的功能，例如新增节点和运维等工作。

区块链中的 Peer 节点具有不同的功能是通过设计不同的智能合约实现的。智能合约是区块链系统中可以自定义的代码文件，当满足特定的条件时区块链节点就会触发智能合约里的代码，执行相应的操作。本实验中共运行了 7 份不同的智能合约，分别对应 7 种不同角色的区块链节点，决定了它们的功能。

以仓单登记注册业务为例，说明区块链系统内业务流程的特点。区块链仓单系统的仓单注册业务流程图如图 3 所示。

存货人完成仓储物入库工作后，由仓储机构通过区块链系统录入仓单的基本信息并提交仓单注册申请，仓单的基本信息会被保存在仓储机构节点的状态数据库中，并且标记为申请状态。仓

表 1 区块链系统中各个节点功能描述

序号	节点名称	角色描述	功能描述
1	Orderer	排序服务节点	负责排序交易，打包区块。
2	org1.peer0	核心银行节点	背书全部交易结果，验证区块信息。
3	org1.peer1	普通银行节点	背书与自己有关的交易结果，验证区块信息。
4	org2.peer0	核心仓储机构节点	发起交易，背书全部交易结果，验证区块信息。
5	org2.peer1	普通仓储机构节点	发起交易，背书与自己有关的交易结果，验证区块信息。
6	org3.peer0	核心信用担保机构节点	背书全部交易结果，验证区块信息。
7	org3.peer1	普通信用担保机构节点	背书与自己有关的交易结果，验证区块信息。
8	org4.peer0	普通用户节点	发起交易，背书与自己有关的交易结果，验证区块信息。

储机构申请的动作会被记录在区块链系统中不可以修改的区块链上。该仓单注册申请需要得到区块链网络中核心机构节点的背书签名后才能被成功提交，仓单注册申请提交成功后，仓储机构节点的状态数据库中的仓单的基本信息和区块链上的申请信息会被同步到区块链系统中的其他节点上。存货人可以从本地节点获知仓单注册申请的信息，然后通过区块链仓单系统对仓单的基本信息进行确认，存货人的确认动作会被记录到本地

节点的不可以修改的区块链上，确认同样需要获得核心机构节点的背书签名后才能成功。仓单注册申请经存货人确认成功后，区块链系统中的所有节点的数据再一次同步更新。此时，根据仓单是否需要信用担保，决定仓单注册的下一步流程。如果无需要信用担保，则仓单注册申请流程就此完成，区块链的状态数据库中的仓单基本信息就会被更新为流通状态；如果需要信用担保机构进行担保，信用担保机构基于本地节点的信息

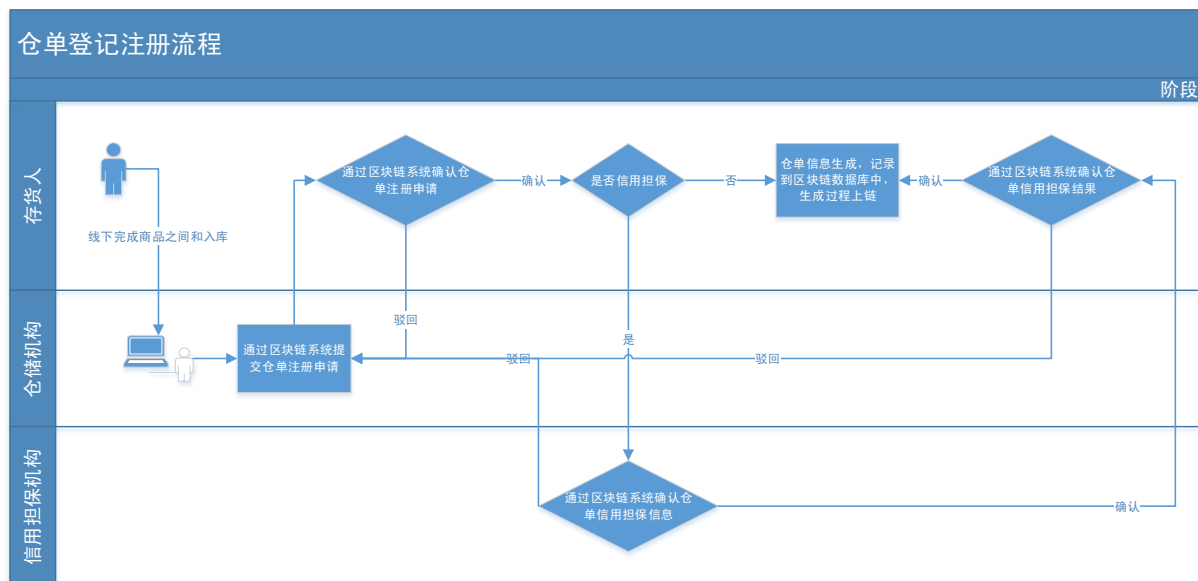


图 3 区块链仓单系统的仓单注册业务流程图

完成担保确认操作，核心机构节点背书签名确认后，将确认操作信息同步到区块链系统中的全部节点，完成仓单的注册流程。上述业务流程看似复杂，但是实际上的背书签名操作、状态数据库和区块链数据的网络同步等工作均由智能合约自动完成，无需人工操作。

基于区块链技术的仓单系统的特点在于仓单的基本信息和仓单业务的全过程都会被记录在不可篡改的区块链上。这些信息在联盟内公开透明，区块链中的每一个节点都可以基于本地账本数据查询仓单的基本信息，获取仓单完整的流转信息。另外，每一个经过核心企业节点背书后的仓单业务不仅由参与双方承认，还经过核心机构的信用背书，仓单的信用水平将得到有效地提升。

5 结论与建议

5.1 结论

使用区块链技术构建可信仓单系统对于建立仓单信息公示机制和制定行业公认仓单信任标准具有重大意义。区块链技术是目前信息公开度最大、可信度最高的信息公示技术。加入联盟链的成员可以基于本地节点准确地获取仓单的基本信息和流转过程，对于仓单的来龙去脉有更全面的了解，从而有效地预防“仓单重复质押”

等风险事件的发生，亦可为事后纠纷提供有效的证据。同时，以核心仓储机构、核心信用担保机构、核心银行节点为多中心的联盟链网络，代表了仓单市场最高的信用水平，经由核心机构节点背书的仓单和仓单业务在联盟范围内具有普遍的公认度，对于建立行业公认的仓单信任标准十分有益。

5.2 建议

虽然区块链可以保证存储在链上的数据不被恶意篡改，但是无法监控线下的欺骗行为，不具有判断初始上链数据的真实性的能力。虚开仓单是仓储物保管人与仓单非法持有人线下勾结产生的欺骗事件，区块链技术并不能覆盖对此类问题的控制。本文在最后提出“区块链+物联网”的技术建议，为解决数据上链环节的真实性问题提供思路。

在仓单领域使用物联网技术，可以实现对仓储物生产、存储和物流环节的监控。区块链和物联网的结合有利于形成有形资产和数字资产的直接映射关系，解决链上链下数据的信任问题，区块链技术保证存储在区块链上的数据不被恶意篡改，物联网技术提高上链数据的真实性，反应仓储物的实际情况，有效防止“一货多用，虚开仓单”等风险事件的发生。

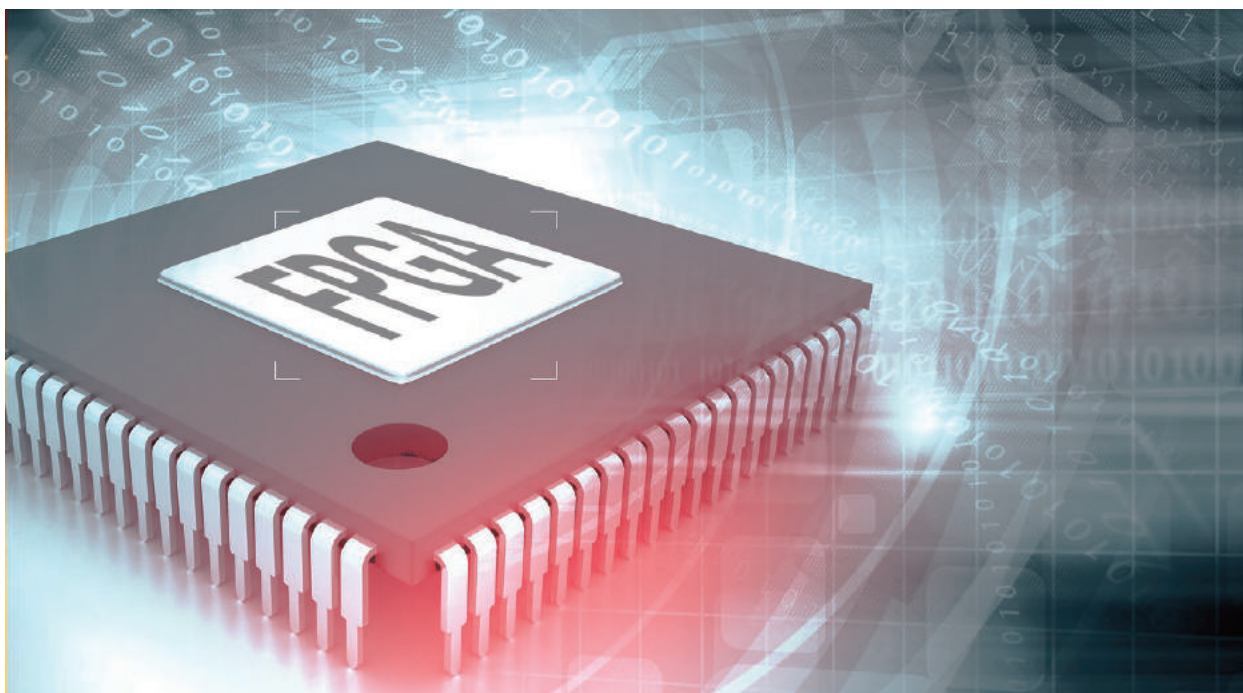
FPGA加速计算应用研究

——美式期权价格计算的FPGA实现

刘超凡、王卓 / 西安子午线智能技术有限公司

邹经纬、马辉 / 国泰君安股份有限公司

钟浪辉、陈敏 / 上交所技术有限责任公司



随着资本市场对外开放的步伐加快，国内的证券期货业核心机构、会员单位等不同的市场参与人都在以不同方式推动金融科技创新，持续助力金融科技在交易、监管等方面的进步。上海证券交易所（简称“上交所”）也一直在深入跟踪、引领交易技术、监管科技的发展趋势，积极将大数据、人工智能新技术运用到自律监管和交易服务中去，进一步提升监管的效率和交易的效率。

现场可编程门阵列（简称“FPGA”）技术是近年来证券期货市场发展得比较快、研究得比较热的技术之一。与证券期货业许多核心机构、会员单位一样，上交所技术公司也积极布局研究

FPGA 应用研究，我们部门在去年研究《FAST 行情硬解码》的基础上，今年又与国泰君安合作研究《FPGA 实现股票期权相关指标》，希望利用 FPGA 的加速计算特性实现快速的期权定价，探索一条利用 FPGA 加速计算任意金融指标的路径。

期权又称选择权，是证券期货市场发展到一定阶段出现的衍生性金融工具，包括个股期权、股指期货、ETF 期权、外汇期权、商品期权、利率期权等。目前国内可交易的有上证 50ETF 期权、豆粕、白糖、玉米、棉花、铜等商品期权，每种期权都有一定的做市商提供流动性。期权交

易中的各个市场参与人都对期权理论价格的确定有着强烈的需求，高精度、低延时的定价也是市场参与人核心竞争力之一。本文描述了 CRR 定价模型的 FPGA 工程实践，希望借助这一工程描述 FPGA 应用的一般过程，特别是反应出 FPGA 加速计算的特质。

1 美式期权的 CRR 定价模型

美式期权是指可以在成交后有效期内任何一天被执行的期权。美式期权允许期权持有人在到期日或到期日前执行购买（如果是看涨期权）或出售（如果是看跌期权）标的资产的权利。

某甲公司突然宣布发放较预期金额高的现金股利时，持有该公司美式期权的人可以立即要求履约，将选择权转换为股票，领取该笔现金股利；而持有该公司欧式期权的人就只能干瞪眼，无法提前履约换股、领取现金股利了。因此，绝大部分市场的股票期权采用美式期权。

美式期权作为最基础的金融衍生产品之一，为其定价一直是金融工程的重要研究领域。和欧

式期权不一样，美式期权价格没有明确的表达式，目前只能通过数值方式进行求解。网络分析法是一种数值求解的办法，主要思想是在风险中性前提下，将标的资产符合的随机过程进行离散化处理，再动态规划对其进行求解，获得标的资产衍生品的价格。网络分析法具体有可以分为二叉树法、三叉树法以及更多的分支模型。

Cox、Ross 和 Rubinstein 三人提出了 CRR 模型，该模型将二叉树与有限差分方法运用于期权定价中，在定价时具有收敛的特性。期权定价基本思想是假设投资者对待风险的态度中性，所有证券预期收益率是无风险利率。风险中性的投资者将期望值用无风险利率折现获得现金流量的现值。

该方法需要计算价格上下波动的概率和数量，主要变量有：股息收益率 q ，贴现率 r ，远期利率 $b=r-q$ ，标的资产连续复利收益率的标准差 σ ，到期时间 t_{cal} ，总分期数 N 。

向上波动

$u = e^{\sigma\sqrt{\Delta t}}, dt = t_{cal}/N$

向下波动

$d = \frac{1}{u} = e^{-\sigma\sqrt{\Delta t}}$

波动的概率

$p_u = \frac{e^{bdt_f-d}}{u-d}, dt_f = \frac{t_f}{N}, p_d = 1 - p_u$

贴现因子

$df = e^{-r dt_{pv}}, dt_{pv} = \frac{t_{pv}}{N}$

表 1

序号	0	1	2	3	4	5	6
时间(年)	0	0.083	0.167	0.25	0.333	0.417	0.5
股票价格	50	56.23	63.24	71.12	79.98	89.94	101.15
		44.46	50	56.23	63.24	71.12	79.98
			39.53	44.46	50	56.23	63.24
				35.15	39.53	44.46	50
					31.26	35.15	39.53
						27.8	31.26
							24.72

表 2

序号	0	1	2	3	4	5	6
时间(年)	0	0.083	0.167	0.25	0.333	0.417	0.5
期权价值	5.3	8.52	13.26	19.84	28.24	38.04	49.07
		2.3	4.11	7.16	12.05	19.21	27.9
			0.61	1.26	2.61	5.39	11.16
				0	0	0	0
					0	0	0
						0	0
							0

为了简化数学描述，下面通过简单的例子说明 CRR 模型的运算过程。

例如：假设股票价格初始为 50 元，期权到期执行价格 52.08 元，无风险利率 4%，股票波动率（标准差）0.4068，到期 6 个月，划分期数 6 期。

首先计算 $u=1.1246, d=0.8892$ 。（如表 1）

按照股票价格二叉树和执行价格，构建期权价值二叉树并计算期权价值。

首先计算 $p=0.4848, 1-p=0.5152$ 。

其次，执行价格大于股票价格时，期权价值为 0。

最后，最右边列的期权价值是股票价格减去执行价格，其他列从右到左分别通过公式计算：期权价值 = (上行概率 * 上行时到期日价值 + 下行概率 * 下行时到期日价值) / (1+r)，例如 $38.04 = (0.4848 * 49.07 + 0.5152 * 27.9) / (1 + 4\%/12)$ 。（如表 2）

2 实现期权定价的困难

由于美式期权没有明确表达式，只能通过数值方式求解，但是以 CRR 模型为代表的各类方

法都存在收敛速度慢的特点，一旦时间节点数增多，树的分枝数将会呈现出指数爆炸状态。

大多市场的期权行情刷新间隔是 500 毫秒甚至 250 毫秒（统一简称 1 个 TICK），这就意味着市场参与者必须在 1 个 TICK 内完成所有股票期权的理论定价，并据此判断套利机会与套利成本，对于明显不合理的报价进行买卖直到市场报价回归合理。理论定价越快，留给投资者实施套利的的时间就越多，投资回报就越高。对期权做市商而言，理论定价越快，向市场提供的报价就越合理、公正，就越能激发市场活力、提高市场效率。

显然，这些业务需求对技术实现提出了苛刻的要求。如果利用通用 CPU 计算价格，计算效果差，不能兼顾高精度与低延时。本文利用 FPGA 实现 CRR 模型，加速了期权定价加速计算，有效地缩短了美式期权的定价时间。

3 实现 CRR 模型的 FPGA 应用工程

我们的 FPGA 应用运行在 Xilinx KCU1500 板卡（图 1）上实现。KCU1500 主要器件是 Xilinx 中端系列器件 Kintex Ultrascale 中最大的

Board Features

Featuring the KCU1500 Board

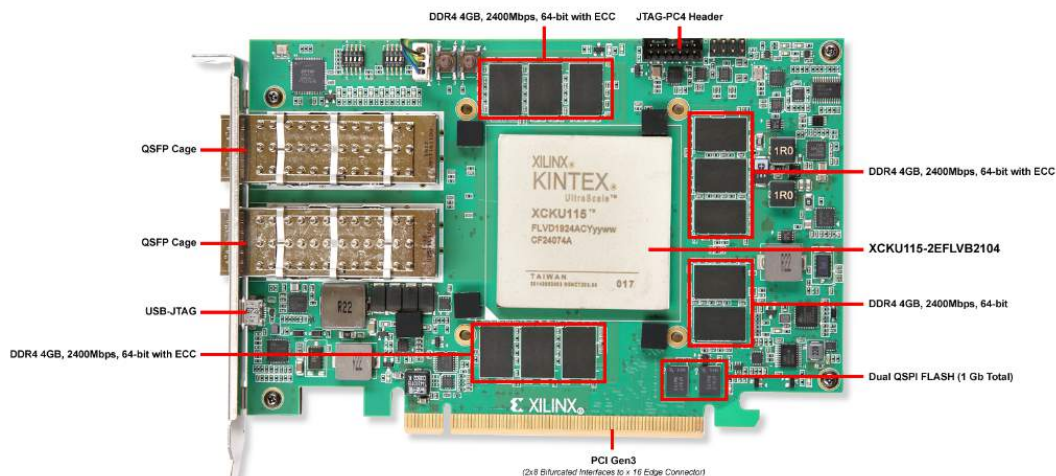


图 1

一颗芯片 KU115, 它有丰富的 LUT 查找表与 FF 触发器资源, DSP 单元高达 5520 个, 适合大吞吐量的算法设计, 性价比较高。

主要接口如图 1 所示, 需要特别指出的是我们使用 10G 网口对外服务, 通过它接收网络上的行情数据并返回定价结果, 板卡所在的服务器 PCIe 只做供电用, 所有运算完全在 FPGA 上独立完成, 服务器其他部件可以处于休眠状态, 实测发现 FPGA 交易期间功耗 40W 左右。

3.1 设计说明：

实际工作环境中, FPGA 作为单独的计算加速单元使用, 配合 Server 端完成指定的计算。

具体工作流程为：

Server 从网口下发计算参数 -> FPGA 网口接收参数 -> FPGA 分配计算任务给空闲的 Channel -> FPGA 内部 Channel 并行计算 -> FPGA 从网口发送计算结果 -> Server 做后处理

整个设计除了接口部分, 算法上重点是单个 Channel 内部的设计

3.2 设计要点：

(1) 充分利用 FPGA 设计的 Pipeline 特点, 在 Channel 内将循环计算中的数据在时间上做好排布, 使得计算单元在时间上的占用率尽可能高

(2) 将一次期权计算中涉及的运算尽可能并行排布, 利用 FPGA 的并行特点, 减小单独 Channel 的算法总时延, 会增加一定资源

(3) 最终整个设计的瓶颈在于单个 Channel 的资源占用与芯片能放下的 Channel 数以及主时钟的频率三者的均衡, 达到尽可能高的性能

3.3 FPGA 开发流程

3.3.1、软件说明

Xilinx 公司的开发工具 Vivado (2017.4 版本), 可以完成从综合, 布局, 布线, BIT 文件生成, 加载到在线调试的全部功能, 而且有 IP 库可以免费或付费使用 Xilinx 的多种 IP, 加速设计。

3.3.2、工程建立

启动 Vivado 后, 选择 Quick Start 中的 Create Project 去新建工程, 在界面中输入工程名称和路径, 如图 2。

然后选择建立 RTL Project, 此时可以勾选 Do not specify source at this time, 先不添加设计文件。

接着按照界面提示选择 FPGA 器件, 由于我们使用 Xilinx 官方的开发板, 直接选择 Boards 后输入“KCU1500”, 会自动匹配出对应的开发板。

3.3.3、设计文件导入

在 RTL 设计做完功能仿真验证后, 运行工程实现前必须将设计文件导入, 包含 Design Sources 和 Constraints 两部分。

Design Sources 通常包含 RTL 设计代码如 Verilog HDL/VHDL 文件以及网表文件如 EDF 文件, 还有调用的 Xilinx 的 IP 文件接口 XCI 文件以及其它 Vivado 工程中综合得到的 DCP (Design Check Point) 文件。需要在 Settings 中指定整个设计的 Top module name 以确定 Top 文件, 根据该文件中的例化调用关系来构建出整个设计的 Hierarchy。

Constraints 只有 XDC 一种文件格式。XDC 是在业界标准 SDC (Synopsys Design Constraints) 基础上, 增加 Xilinx 定制的部分规则而形成的一套设计约束体系, 通常包含物理位置约束与时序约束。物理位置约束需要定义 Top 文件对外的 I/O 在 FPGA 芯片管脚的位置对应以及电平/驱动强度等物理信息, 以及限定内部设计中一些 Cell 或 Primitive 的位置等信息。时序约束通常要约束设计中所有的时钟频率/相位等信息, 进出 FPGA 管脚的时钟与数据相位关系, 以及各时钟时间的例外约束等。

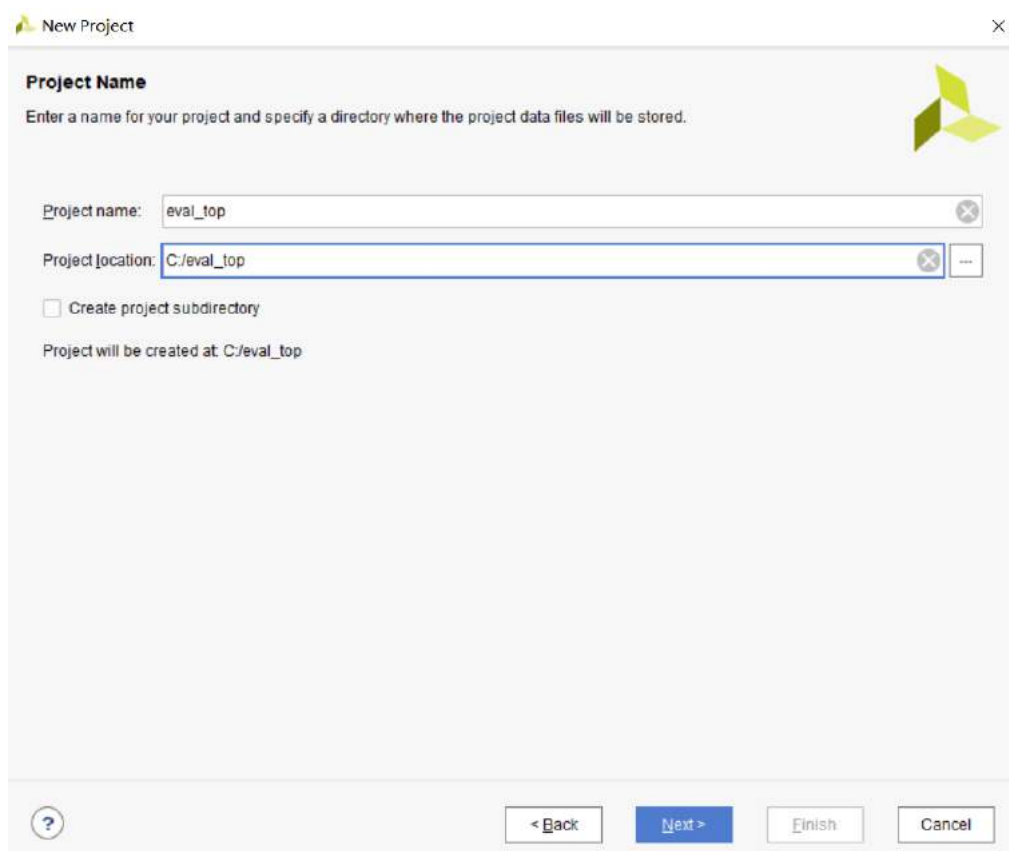


图 2

导入 Design Sources 和 Constraints 后的工程
如图 3 所示。

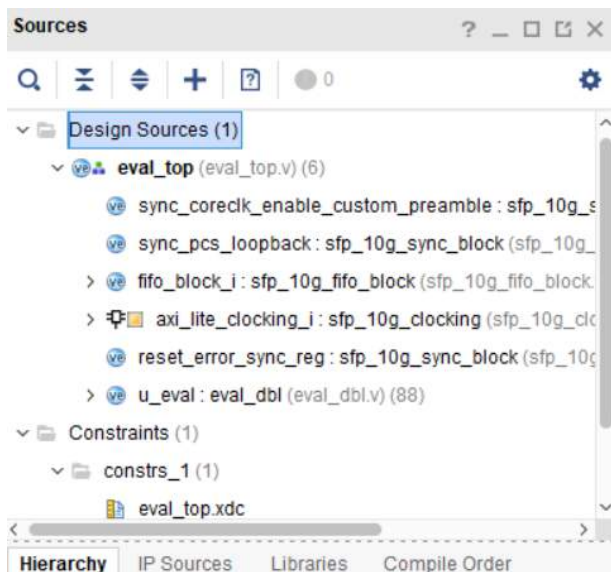


图 3

3.3.4、工程实现

Vivado 工程实现包含 Synthesis 与 Implementation。

Synthesis 是将 RTL 代码与所有被调用的 IP 等综合成一体，相当于生成 FPGA 芯片底层电路 Primitive 的所有配置与连接关系，配合 Constraints 信息，就形成整个设计的 Netlist。

Implementation 是将 Netlist 适配到 FPGA 芯片的流程，主要步骤是 Place 和 Route，通常称前者为布局，后者为布线。Place 选择将 Netlist 中的 Primitive 放置在 FPGA 中合适的位置，而 Route 完成 Primitive 间连线的实现。

Implementation 完成后可以点击按钮 Generate Bitstream 生成最终上板加载的 Bit 文件，但必须检查 Implementation 的 Timing 结果是否正常，通常主要查看整个设计所有时许路径建立保持时间的完成情况，在 Project Summary 中可以查看。

下图是 Setup 和 Hold 的时序结果

Timing	Setup Hold Pulse Width
Worst Negative Slack (WNS):	0.018 ns
Total Negative Slack (TNS):	0 ns
Number of Failing Endpoints:	0
Total Number of Endpoints:	1507117
Implemented Timing Report	

图 4

注意：一个完成实现后可以上板测试的版本的 TWS 和 THS 必须为 0，此时 WNS 和 WHS 一定是大于等于 0 的，这两个值越大意味着时序余量越好。

如果时序不满足或者实现报错，需要返回到设计步骤重新调整设计与约束。

在 Project Summary 中同时可以查看到实现后 FPGA 芯片的资源占用，如下图所示。

Utilization			
Post-Synthesis Post-Implementation			
Graph Table			
Resource	Utilization	Available	Utilization...
LUT	329496	663360	49.67
LUTRAM	32146	293760	10.94
FF	661657	1326720	49.87
BRAM	527	2160	24.40
DSP	3541	5520	64.15
IO	10	702	1.42
GT	1	64	1.56
BUFG	9	1248	0.72
MMCM	1	24	4.17

图 5

本设计占用了 49% 的 LUT，49% 的 FF，24% 的 BRAM 以及 64% 的 DSP 资源。

4 FPGA 加速计算的测试结果与加速计算展望

4.1 设计性能：

因业务精度需要，一个二叉树从根开始合计

需要分叉 200 次(分叉次数因人而异,也许 100 次、50 次分叉就够用。理论上分叉越大越接近全微分方程，精度越高)，详细过程见下图：

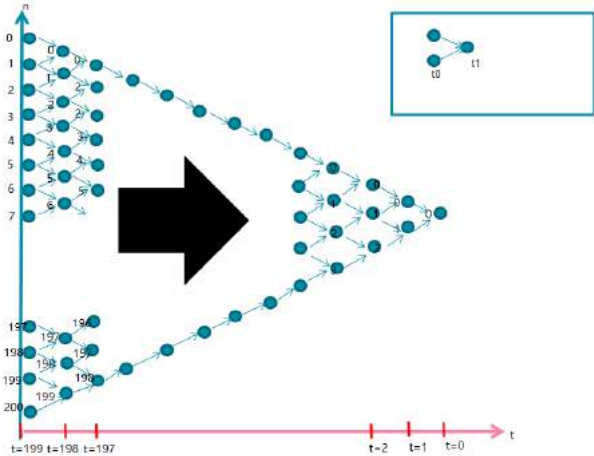


图 6

完成这 200 批次双精度浮点的循环计算即可满足现有期权业务的定价精度需求，实现一次理论价格计算（Operation，简称 op）。由于临近交割等情况下时单精度（float）计算精确度很差，所以业务上必须双精度（double）计算，代价是 FPGA 资源消耗多、延迟拉长，代价大约是单精度的 3 倍。通过逻辑综合与实测确定 FPGA 应用一次理论价格计算耗时（Calculation Latency）大约 14000 时钟周期（cycles）。

不考虑网络传输及 Server 端效率以及其它开销，FPGA 板卡的性能可以用以下公式表达：

$$\text{Operation per second} = \text{Fmax} * \text{Channel} / \text{Calculation Latency}(\text{number of cycles})$$

KCU1500 主频 308MHZ，拥有 80 个通道，理论性能接近 $308\text{M} * 80 / 14000 = 1.76\text{M op/s}$ ，即每秒 176 万次美式期权定价。如果考虑线路开销与软件后处理延时，实际效率为 45% 左右，即实际定价能力大约为 800k op/s。

实盘以及日常测试时因业务需要，KU115 的 80 个通道只分配 60 个做 200 批次双精度浮点循环计算，实盘的实际定价能力大约为 616k op/s。

4.2 测试用例与测试结果：

每个 strike 对应 1 个 call (认购期权) 1 个 put (认沽期权)，以及各自的 greeks (常用的 5 个期权希腊字符)，实际每个 strike 需要 12 颗二叉树的计算量，即每个 strike 需要 12 次 op。

测试中假定有 1000 个 strike (对应一个期权行权价格)，这 1000 个 strike 单次定价计算量是 12000 次 op。迭代 1000 次运算就是 12M 次 op (计算平均延时需要在总耗时基础上除以 1000)。

Model	Time Steps (批次)	Strikes(对应 12 次 op)	Iter Size (迭代次数)
CRR American	200	1000 (*12)	1000

Card Type	Mean(ms)	GPU Usage Avg
GPU(Tesla M40)	43.41	96%
FPGA(Xilinx KU115)	19.45	N/A

一个 TICK 内 FPGA 应用平均耗时 19.45 毫秒处理整幅行情快照 (1000 个 strike 有行权价的期权)。1000 个 strike 需要二叉树计算 12K op，它们被平均分配在 60 个 Channel 内并行计算，每个 Channel 串行 200 个 op 耗时 19.45 毫秒。可以推算每次 op 耗时 $19.45\text{ms}/200=97$ 微秒。97 微秒中包含网络延时、预处理任务时间、FPGA 净计算时间等因素，其中单次 op 的 FPGA 净计算时间需要 14000 时钟周期，根据主频 308M 可以推算所以单次 op 的 FPGA 净计算时间是 $14000/308\text{M}=45$ 微秒，FPGA 净计算时间占单次 op 耗时的比率是 $45/97=46.4\%$ 。未来还可以把预处理任务交由 FPGA 完成，进一步拉长 FPGA 净计算时间、缩短预处理时间，从而提升 FPGA 净计算时间的占比，缩短单次 op 的时间。

考虑到 FPGA 板卡与 GPU 的价格与性能的可比性，GPU 的 M40 型号与 KU115 FPGA 接

近，但是 M40 的美式期权定价耗时比 KU115 大 100%，最重要的是 M40 功耗为 250W (KU115 仅 40W)，各大交易所数据中心在用电约束下明确限制 GPU 的实盘运行。使用 CPU 运行 CRR 模型 (网络上有许多对应的 c++ 代码)，实测发现 1 个 TICK 内无法完成运算，实盘价值小。

4.3 FPGA 应用展望

本文通过一个 FPAG 工程实现了美式期权定价 CRR 模型，它在期权行情刷新间隔内完成了符合业务精度的理论价格计算。未来 FPGA 应用开发在证券期货业大有可为，结合赛灵思、华为、Intel 等主流 FPGA 厂商的最新技术我们发现 FPGA 发展势头很好：

1、支持传统软件编程模式，编译器自动生成的设计甚至比手动编码的 RTL 设计方案的性能还高。支持 OpenCL/HLS 等类 C 语言开发 FPGA 应用。

2、Intel 等厂商提供专业的 OpenCL 版欧洲金融库，效率达到 RTL80% 以上。

3、专业 IP 厂商提供可靠组播、低延时 TCP、压缩、加密、分布式存储等 IP，这些 IP 有硬核也有软核模式，通过集成化的手段提供给开发人员满足不同的应用场景。

4、华为等厂商还提供了 FPGA 与本机用户进程之间低延时传递数据的编程框架，利用 PCIe、共享内存、用户态驱动等技术，从最终用户主机进程的角度进一步降低延时，屏蔽底层技术细节，最终用户只需按照各自金融业务编程即可。

人工智能+知识图谱： 如何规整海量金融大数据？

齐伟 / 恒生电子股份有限公司 邮箱：qiwei@hundsun.com



摘要：人工智能正在迅速改变金融机构，金融机构的数据计算的关注点，正在从企业信息系统内部的计算，转变为关注来自互联网和三方的外部数据的计算和处理上。多元异构数据的整合，是未来金融机构将要长期面临的一个局面。数据难以融合，也就难以做到统一消费，从非结构化数据提取的实体关系、属性等信息，当他们不能融合到企业内部经营数据中去，就会再次形成信息孤岛，随着多元异构数据的量级不断攀升，这个信息孤岛将会呈现越来越严重的局面。在人工智能迅猛发展的今天，如何解决上述问题，是未来企业竞争中体现出来的核心竞争力之一。

关键词：人工智能、大数据治理、知识图谱、金融场景

1 概述：

“The more we know, the less we understand”

21 世纪以来，人类社会信息资源的开发范围持续扩大，经济、社会信息随着经济活动加剧得到空前的开发，信息资源总量呈爆炸式增长，我们从最初的“信息匮乏”一步踏入到“信息过量”时代。

个人如此，行业亦然。随着大数据应用的不断发展，金融机构的经营决策、营销服务越来越依赖于诸如新闻舆情、企业信用、热点概念等企业外部数据，而这些数据的应用场景也愈加需要与金融机构内部的数据打通，形成数据融合计算。再加上人工智能的异军突起，大量非结构化数据正在被人工智能结构化掉，隐藏在文档中的信息价值正在不断的被“机器”发现并加以大规模的使用，大数据、人工智能让金融机构的数据治理工作又重新回到了“混乱”的起点。面向人工智能的大数据治理，已经成为金融 IT 向金融 DT 转型所必须面对的一个严峻课题。

2 人工智能的应用现状

在笔者看来，人工智能就是一种数据服务能力，智能金融本质上就是金融 DT 服务，发展人工智能就等于发展数据技术，人工智能系统智能化程度的高与低，与数据处理能力正相关。为了方便说明这一论点，我们先来看看金融机构在人工智能领域所做的各种探索和尝试。

人脸识别作为最早的人工智能技术在金融机构各种需要身份验证的应用场景中得到广泛的应用，早在 3 年前远程开户、网上营业厅等业务就已经在金融机构中逐步展开，这是人工智能进入金融领域比较早的案例。现如今智能客服也已成了一个极佳的人工智能的切入点：首先通过智能语音技术将客户的语音转化为文字，然后用自然语言处理 NLP 技术进行解析，识别用户意图，

最后用智能问答形式给与相关的解答和服务。

智能客服在大幅降低人工客服的服务压力的同时，还能有效提升服务品质和服务效率，这对那些面临大量客服工作的大型金融机构来说还是非常具有吸引力的。还有一部分金融机构以产业链知识图谱为其人工智能的着眼点，构建上市公司及其产品服务的上下游关系，再通过追踪监控新闻、事件、舆情在产业链中的传导效应，形成具体的投研策略。产业链技术延伸出去就会形成智能投研、智能资管、智能风控等智能金融业务，这类人工智能技术更加贴合金融机构的金融业务的用户场景。也有金融机构，索性把人工智能当作自己的贴身秘书来使用，各类新闻、公告、年报的解读全部交给了人工智能，通过自然语言处理技术，提取公告中的财务数字，做自动摘要，形成正负面相关性的分析。这类数据通过人工智能技术预处理后，大量信息被提炼出来，结合部分人工审核和校对，基本上也可以上生产了。

3 数据智能服务：从感知到认知

有人把人工智能的发展分为三个阶段：计算智能、感知智能、认知智能，对应的 DT 服务的发展就是数据从信息向知识演化并最终生长为数据智能的演变过程。当前大部分金融机构的人工智能还停留在感知智能向认知智能转化这个阶段，而主要工作场景还是在感知这一领域，所谓感知智能就是能听能说，具备一定的表达能力。很显然，人脸识别是图像视频这类非结构化数据的特征结构化的结果，这是让机器看懂人的图像；智能客服仰仗的是 NLP 的分词和意图识别能力，支撑问答系统的是强大的知识库和知识图谱技术，这是让机器理解人的语言；产业链知识图谱主要是传统三方资讯关系型数据转变为 RDF 三元组的一种数据存储形态的改变；各类新闻公告年报等的报告信息提取与加工，代表着非结构化数据结构化的一个过程，这是让机器替代

人脑去读懂文档。

发展人工智能,光有感知能力显然是不够的,最终要能够具备认知推理的能力,从学术界看这个问题,有两条路可以走,一个是机器学习,一个是符号推理。机器学习大家都比较理解了,尤其是深度学习技术已经让语音识别、视频影响处理的能力超越了人类大脑的能力。符号推理,走的是另外一条路,最早指的就是专家系统,大量的知识被存储管理起来,用于检索,现如今,符号推理,是借助语义网络知识管理进行图分析挖掘的一种能力。符号推理在当前工业界落地的就是指知识图谱,基于RDF三元组存储的知识图谱,可以存储管理人类已有的各类知识,而这些知识又因为是一种实体关系属性的图表达,所以基于图的分析挖掘,表现出来的就是知识发现和推理的一种能力。

在我国金融行业,因为大数据本身的积累不够,做过标注的金融数据语料更加匮乏,所以造成一个结果,就是在金融行业,面向具体金融业务场景的机器学习的数据是不够的,更加谈不上深度学习了,结果就是基于机器学习的认知智能的发展必然受限。这里最直接的表现就是我们发现所有金融应用场景里,适合机器学习和深度学习的场景,是比较少的。很多机器学习不得不为NLP、知识图谱这种细节场景服务,或者机器学习和金融工程整合在一起,而主体还是金融工程,机器学习目前只是一种辅助工具,充其量就是多因子的一个加工手段而已。究其原因是金融行业业务相关的大数据的体系还没有完全构造出来。应用场景的数据还没有得到有效沉淀。

而符号推理在金融行业会有所不同,我们知道金融服务本质上就是一种信息服务,而金融对上市公司的公告、年报、新闻等等的资讯数据是天然敏感的,大多数玩金融的人,都是从处理这些信息开始的。很多行业研究员为了能够建立自己的竞争力,领先市场一步,每天加班加点的就是在阅读分析处理这类资讯数据。这类资讯数

据基本上是一种非结构化形式存在的,三方资讯数据厂商通过人工采编的方式能够结构化掉其中一部分,而大多数数据还是需要人脑加工的。这就给了人工智能应用一个空间,通过自然语言理解NLU,再进行自然语言处理NLP,最后通过自然语言生成NLG,有了这几项技术,再结合知识图谱和机器学习的能力,将可以将这类非结构化数据的加工结果进行有效反馈。如果我们将NLP加工获取的金融词林,进一步挖掘获取的实体、关系、属性、概念、事件等信息,加以整理,建立他们之间的各类关系,那么一个基本的金融知识图谱就构造出来了。所以,我们会看到NLP技术在当前的人工智能领域的应用已经成为了热点,而KG是紧随其后的一项技术,大量的非结构化数据的提取达到一定的准确度后,机器就可以代替人,来完成大规模知识发现,最终形成知识计算所需要的“大知识”的数据储备,目前NLP的准确率还只能到60%上下,具体场景针对性优化后才可能到90%以上的水准。

在足够窄的应用领域,NLP技术通过了实战的考验。但面对海量大数据,基于文档互联的互联网体系想要转化为以实体关系为主体的语义网络,还有相当长的一段路要走。但我们还是有理由相信以广义NLP(新视频文字)技术为核心的人工智能将会统治相当长一段时间,直到非结构化数据的处理不再是问题以及非结构化数据和结构化数据能够相互融合,那么届时行业知识图谱、企业知识图谱的数据准备也已由点及面的建立起来,基于知识图谱的人工智能应用将大放异彩,金融领域的人工智能也就从感知智能正式过渡到认知智能阶段。

4 数据的价值演化

人工智能的发展本质上是数据价值的一个演化过程。计算智能对应的就是我们看到的多源异构大数据,我们将这些数据进行采集、清洗、转

化加载到大数据中心后，数据变成各类有用的信息。如果我们将信息进一步提炼，通过知识构建与管理的一系列手段，便可以将信息转化为知识，存储起来。如果我们按照 W3C 的知识管理规范，对知识做 RDF 三元组的存储和管理，我们就能构造出来一系列的知识图谱。有了这个知识图谱，我们就具备了知识计算的能力，那么对于一个具体的金融场景来说，如果我们将金融业务场景的业务模型结合知识计算的能力，以及对大数据平台的数据进行机器学习的能力，就可以形成我们的金融大脑。



图1 从数据到智能

金融大脑 = 金融业务场景的业务模型 + 知识计算 + 机器学习。我们将这类金融大脑，也就是大大小小的智能化场景，开放出去，就形成我们对传统金融的一个智能化变革。

5 面向人工智能的大数据治理

从以上的分析中，我们可以明确感觉到人工智能正在迅速改变金融机构，金融机构的数据计算的关注点，正在从企业信息系统内部的计算，转变为关注来自互联网和三方的外部数据的计算和处理上。

多元异构数据的整合，是未来金融机构将要长期面临的一个局面。数据难以融合，也就难以做到统一消费，从非结构化数据提取的实体关系、

属性等信息，当他们不能融合到企业内部经营数据中去，就会再次形成信息孤岛，随着多元异构数据的量级不断攀升，这个信息孤岛将会呈现越来越严重的局面。在人工智能迅猛发展的今天，如何解决上述问题，是未来企业竞争中体现出来的核心竞争力之一。

以上所述的问题与挑战，就是我们今天所谈到的面型人工智能的大数据治理有待解决的问题。那么我们该如何行动呢？

第一步：多源异构数据源的统一管理。首先，我们要对多源异构数据源进行统一管理。这里既包括金融机构内部的经营数据，也包括来自三方资讯数据厂商的外部数据，以及来自互联网的各种大数据。

为了达到未来的智能化能力，我们需要将金融内部的结构严谨的业务系统数据图谱化，将具有明显关系特征的数据提取出来，再用这些数据对企业内部数据通过实体链接、数据标引等技术进行再组织；同时我们将三方数据中非结构化的那部分 PDF、WORD 等进行知识抽取，也提炼出实体关系属性等数据。最后对那些跟金融机构相关的互联网大数据，通过爬虫技术不断的抓取，并对这些网页半结构化数据进行结构化处理，同样提取其中的实体关系和事件信息。

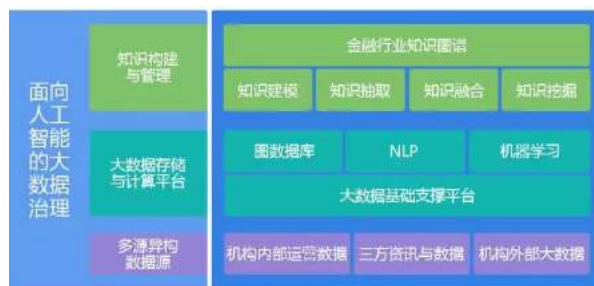


图2 面向人工智能的大数据治理

第二步：大数据存储与计算。对于金融机构而言，无论是采用商业化的软件还是开源软件，都需要一个大数据平台将来自多源异构数据源的数据进行统一管理，可以把这理解为一个大数据中心的建立，只不过这个数据中心的主要构建技

术是人工智能的三驾马车：知识图谱、NLP、机器学习。我们在大数据中心除了保留原始异构数据源的一份拷贝之外，还要对这些数据进行面向人工智能的数据处理，包括通过 NLP 进行实体挖掘、关系抽取、属性提炼；通过知识图谱保存 NLP 提炼出来的具有关系特征的各种数据以及用机器学习来加速这一进程的处理效率提升准确度等。

第三步：构造知识图谱。最后我们需要构造金融行业的一个知识图谱，可以是行业知识图谱，也可以是企业图谱。KG 的建设是有一个完整的生命周期的，包括知识建模、知识获取、知识融合、知识计算以及知识应用的全过程。知识建模依赖与金融机构内部数据和来自三方的结构化数据，将 ER 关系转化为 KG 的 Schema 是这一个工作的重点。构造好 Schema 后，就可以进行知识获取工作了：首先导入关系型数据库的各类实体关系属性数据，然后通过知识抽取技术将各类非结

构化数据结构化掉后，将散落在互联网大数据和三方非结构化数据中的知识进行整理合并到现有 KG 中去；接着通过实体消歧、指代消解等知识融合技术对 KG 的质量进行管理与维护；KG 初步建立后，就可以通过图计算进行知识发现知识推理和挖掘等工作了。

至此，一个完整的面向人工智能的数据治理工作关于基础信息系统层面的建设就告一段落了。

6 结论

之后如果我们据此再逐步建立大数据大知识 (KG) 的管理规范，不断积累其中的业务应用模型，那么一个成熟可拓展的面向人工智能的大数据治理成果就会逐步呈现出来。届时，面向人工智能的大数据治理，势必能有效支撑智能金融从感知智能向认知智能的变革。

如何打造健壮分布式系统

唐刘 PingCAP / 首席架构师 tl@pingcap.com



1 为什么需要『混沌』

对于一个大规模分布式系统来说，我们完全不能预见系统会发生怎样的情况。在里约热内卢的一只蝴蝶扇动了下翅膀，就可能改变大洋彼端的天气，当然也可能直接把我们存放在数据中心的数据给干掉。在任何时候，异常都是可能发生的。

作为下一代分布式 HTAP 数据库，TiDB 从一开始设计的时候，就把用户数据的安全性放到了最重要的位置。因此，我们基于 Raft 一致性算法构建了一套容错系统，对用户的数据复制到不

同的机器上面，保证数据的安全。但是，这又面临了另一个问题，也就是我们如何确定，即使出现了各种各样的异常情况，我们的系统仍然能保证用户的数据安全？

通常，在构建系统的时候，我们会写很多单元测试，但即使单元测试的覆盖率到了 100%，也不能保证系统是健壮的。如果更进一步，我们可能会写非常多的集成测试，通过模拟不同的业务场景，来看整个系统是正常的。但这些都远远不够，我们会遇到各种各样的情况，譬如磁盘突然掉速，NTP 同步不正常，而这些都是常用的测试方法很难模拟覆盖的。

下图是我们实际生产环境遇到的一个 bug：

```
[root@10-180-0-22 data]# ls -lt snap/* | grep 16986
-rw-r--r-- 1 ops ops      58 Jul 18 23:42 snap/rev_1129386_18_16986.meta
-rw-r--r-- 1 ops ops      0 Jul 18 23:42 snap/rev_1129386_18_16986.write.sst
-rw-r--r-- 1 ops ops      0 Jul 18 23:42 snap/rev_1129386_18_16986.lock.sst
-rw-r--r-- 1 ops ops 8499200 Jul 18 23:42 snap/rev_1129386_18_16986.default.sst
```

先简单介绍下上面的异常，对于 Raft 来说，如果一个 Follower 没有追上 Leader 的进度，Leader 就会发送 snapshot 给 Follower。在 TiKV 里面，一个 snapshot 包含三个 column family - default, write 和 lock 的数据（也就是上图的 .sst 文件），另外就是有一个 meta 文件，用来记录一些元信息 - 譬如各个 sst 文件的大小等。

Follower 会首先接受三个 sst 文件，然后是 meta 文件，但我们发现，接受的文件里面 write 和 lock 的文件大小都是 0，但在 meta 文件里面，这些 sst 文件的大小是不为 0 的，也就是说，我们的 sst 数据出现了损坏。

那么这个 bug 是如何出现的呢？我们在 dmsg 里面发现一个异常：

图 1 是 Linux 操作系统在处理 page cache 的时候爆出来的。大家都知道，我们写文件，如果写完之后没有强制 flush 或者是使用 direct IO 模式，要写入的数据都是先写到 page cache 里面，然后由操作系统的后台线程将 page cache 给刷到磁盘。如果这里出现了错误，就会导致我们的数据其实是没写入到磁盘的。悲催的是，之前在 TiKV 里面，我们写 sst 文件是没有 flush 的，所以就出现了丢数据的情况。

可以看到，无论我们的单元测试或者集成测

试写的多么丰富，都很难覆盖到上面出现的情况，所以我们需要一种更好的测试方式，也就是混沌 - Chaos。

2 混沌工程

提到 Chaos，首先不得不提的就是著名的 Chaos Monkey，它是 Netflix 在 2011 年介绍给大家的。这只猴子，在 Netflix 的系统里面，天天上蹿下跳，一会把这台机器的网卡给拔掉了，一会又把另一台机器的磁盘给踩坏了，反正就是能怎么捣乱就怎么来。Netflix 的工程师，想尽了一切办法抓住这只猴子，但无奈它太神出鬼没，根本抓不到，于是只好退而求其次，聚焦到构建更加健壮的系统上面。这样，无论这只猴子怎么捣乱，系统还能稳定的运行。

随着跟猴子不断对抗，Netflix 的工程师们渐渐积累了丰富的经验，形成了一套特有的 Chaos 工程实践方式，提炼出相关的应用原则。在 Principles Of Chaos Engineering 里面，Chaos 的实践方式，主要有 4 个步骤：

1. 定义系统的稳定状态。这个可以通过现在系统正常行为下面的一些输出来衡量。
2. 将系统分成两组 - 控制组和实验组，并且做个假设 - 稳定状态在控制组和实验组会一直一致。
3. 给实验组引入错误，譬如服务崩溃，硬盘驱动故障，网络隔离这些。

```
[17988717.953807] 0 pages in swap cache
[17988717.953808] Swap cache stats: add 0, delete 0, find 0/0
[17988717.953809] Free swap = 0kB
[17988717.953810] Total swap = 0kB
[17988717.953811] SLUB: Unable to allocate memory on node -1 (gfp=0x20)
[17988717.953813] cache: kmalloc-8192, object size: 8192, buffer size: 8192, default order: 3, min orde
[17988717.953815] node 0: slabs: 78, objs: 312, free: 21
[17988717.953816] node 1: slabs: 37, objs: 148, free: 0
[18010253.332261] snapshot worker: page allocation failure: order:1, mode:0x204020
[18010253.332267] CPU: 15 PID: 32283 Comm: snapshot worker Not tainted 3.10.0-327.el7.x86_64 #1
[18010253.332268] Hardware name: Huawei RH1288 V3/BC11HG5C0, BIOS 3.35 10/20/2016
[18010253.332270] 000000000204020 000000008bc746cd ffff882604e8b768 ffffffff816351f1
[18010253.332277] ffff882604e8b7f8 ffffffff8116ef80 0000000000000010 0000000000000000
[18010253.332281] ffff88407ffd7000 000000001fffffff 0000000000000003 000000008bc746cd
[18010253.332285] Call Trace:
[18010253.332295] [<ffffffff816351f1>] dump_stack+0x19/0x1b
[18010253.332300] [<ffffffff8116ef80>] warn_alloc_failed+0x110/0x180
[18010253.332304] [<ffffffff81173708>] alloc_pages_nodemask+0x9a8/0xb90
[18010253.332309] [<ffffffff811b43f9>] alloc_pages_current+0xa9/0x170
```

图 1

4. 尝试在控制组和实验组找到不同的稳定状态，来证明之前的假设是不对的。

可以看到，如果我们能更多的将稳定状态给打乱，对整个系统的行为我们会越有信心。对于 TiDB 来说，我们也是按照上面的方式来进行 Chaos 实践的，简单来说，我们有如下步骤：

1. 使用 Prometheus 监控系统，通过一些关键的 metrics 来定义系统的稳态。譬如在 TiKV 里面，有一个 Busy 的 error metric，正常情况下，这个 metric 是不会有数据的，如果有了，表明系统出现了异常。

2. 对系统进行错误注入，观察 metrics 的变化情况，验证是否符合预期。譬如，我们挂掉了一台 TiKV 节点，正常情况下面 client 的 QPS metric 曲线只会稍微抖动一下，然后正常，但如果 QPS 一直持续为 0，那么一定是哪里出现了问题。另外，我们也会学习相关的异常 metrics，得到异常跟 metrics 的对应关系，这样生产环境中如果出现了异常，我们可以根据相关的 metrics 来快速定位到错误。

3. 构建 Schrodinger 测试平台，将上面的流程自动化处理。

3 错误注入

如果要应用 Chaos，一个重要的工作就是 failure injection。我们会在正常运行的环境中故意注入相关的错误，来看系统的表现。在开发 TiDB 的过程中，我们 team 也积累了非常多的错误注入方式。

最基本的，我们通常会使用如下的几种方式：

1. 使用 kill 关掉某个进程。
2. 直接使用 kill -9 的方式来杀掉某个进程。
3. 给某个进程发送 SIGSTOP 命令来暂停运行，然后再发送 SIGCONT 命令继续执行。
4. 通过 renice 调整进程的优先级。
5. 通过 set thread affinity 的方式调整线程的

优先级。

6. 运行一些程序将 CPU 吃满。

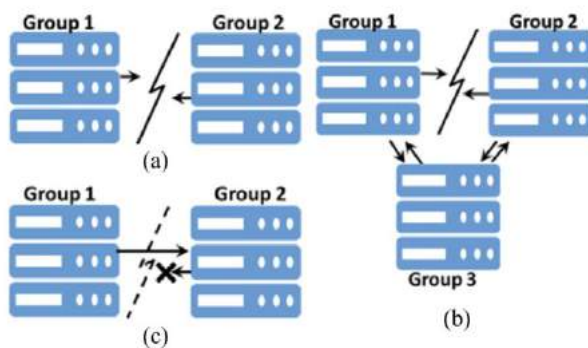
7. 使用 cgroups 来控制进程的 CPU，Mem 等资源。

对于 TiDB 来说，网络和磁盘是我们重点关注的两个地方。毕竟我们是一个分布式的数据库，多个节点之间避免不了通过网络进行通信，然后也需要将数据存储到磁盘，保证不丢失。

4 网络

在 An Analysis of Network-Partitioning Failures in Cloud Systems 这篇论文里面，作者分析了 25 个知名的开源系统，发现有 136 个因为网络隔离出现的错误，而这些错误中有 80% 的都是灾难性的，其中有 27% 造成了数据丢失。可以看看，仅仅是模拟网络故障，我们就能发现很多的问题。下图是论文里面提到了三种网络隔离方式：

1. 完全隔离，Group 1 和 Group 2 完全连接不了。
2. 局部隔离，Group 1 和 Group 2 连接不了，但它们可以通过 Group 3 来中转。
3. 单一隔离，Group 1 能连接 Group 2，但 Group 2 没法连接 Group 1。



在 TiDB 里面，我们也是按照这些方式来模拟的。网络隔离的方式通常就是使用 iptables，但我们还做了更多：

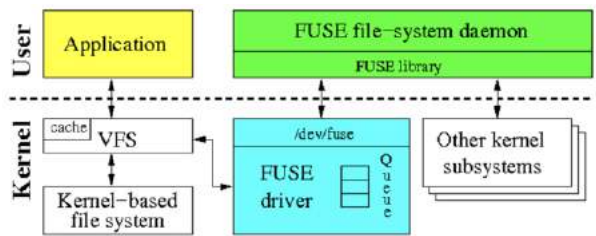
1. 使用 tc 增加网络延迟

2. 使用 `tc` 将网络包乱序
3. 启动一个程序将网络带宽占满
4. 通过 `proxy`，对网络进行更加细粒度的控制

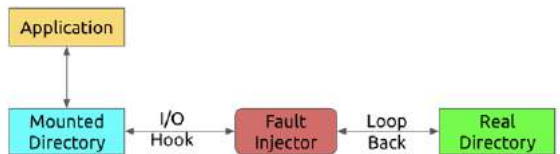
5 文件系统

我们另一个关注的是磁盘，这里主要关注的是文件系统，毕竟我们跟磁盘交互是需要通过文件系统来完成的。在 *All File Systems Are Not Created Equal* 这篇 Paper 里面，作者提到文件系统在有些时候会因为崩溃造成数据不一致，譬如上面提到的 `snapshot` 的例子，就是因为没有 `flush` 出现的问题。

对于文件系统的模拟我们主要使用的是 `Fuse`，在 *To FUSE or Not to FUSE: Performance of User-Space File Systems* 这篇 Paper 里面，介绍了 `Fuse` 的架构：



`Fuse` 包含两个部分 - `kernel` 和用户态 `daemon`。内核部分是一个 `Linux` 的内核模块，它会在 `Linux` 的 `VFS` 上面注册一个 `Fuse` 的文件系统驱动。这个 `Fuse` 驱动可以认为是一个 `proxy`，会将请求给转发到后面的用户态 `daemon` 上面。所以我们要做的事情就是让我们的应用程序跑在我们用 `Fuse` 挂载的路径上面，然后再 `hook` 住文件相关的操作，进行错误注入。大概流程如下：



具体到实际的 `case`，我们可以在某次写入返

回空间不足的错误，看 `TiKV` 在崩溃之后数据是否一致。

6 故障点

有些时候，我们想在一些特定的逻辑触发异常，譬如下面：

```
fn save_snapshot() {
    save_data();
    fail_point!("snapshot");
    save_meta();
}
```

仍然是 `snapshot` 处理，我们先存储 `data`，最后是 `meta`。在实际生产环境中，我们碰到过如下一种情况 - 写 `data` 成功了，但 `meta` 其实并没有写入。但这种错误其实很难在外面模拟的，所以我们引入了 `fail`，在一些代码逻辑上面显示的加入 `fail point`，然后外部进行触发，当程序执行到这个 `fail point` 的时候，就会执行相关的触发逻辑（譬如 `panic`）。

7 故障发现

在前面说的 `Chaos` 实践中，我们提到需要定义系统的稳态，然后注入错误之后，看系统进入不稳定的状态的一些情况。这里其实面临的另一个问题，我们如何去判定系统处于不稳定的状态？如果单纯的人工进行错误注入，然后排查 `metrics`，通过 `metrics` 来判定出现了异常。这个其实比较容易的，但如果每次都是人工来弄，还是很麻烦，我们需要一种更加智能的方式，也就是能自动的去判断系统这时候出现了 `failure`。

要进行 `failure` 判断，一个比较容易的方式就是使用 `Prometheus` 的 `alert` 功能，我们会定义

一些 alert 规则 - 譬如 **error per second** 超过一定阈值, 当规则被触发, 就报警, 这样我们就知道出现了异常。但 **alert** 的方式力度比较大, 有时候, 我们需要更加细粒度的判定。

另一个直观的解决方式是从历史记录中学习, 因为我们有很长一段时间的 **metrics** 数据, 所以可以根据之前的 **metrics** 来推断当前的 **metrics** 是否是正确的。譬如我们知道某个 **metric** 曲线, 但是突然这个曲线出现了一个短时间的抖动, 而这个因为力度太小并没有被 **alert rule** 给捕获。但我们的系统能发现这个异常, 并且发现这种抖动在之前的历史里面也没有, 推测可能出现了错误, 于是报警。

现阶段, 我们还在尝试另一种方式, 来源于 **paper Capturing and Enhancing In Situ System Observability for Failure Detection**。里面的想法很直观, 任何错误都是可观察到的, 一个客户端给某个服务发送了请求, 然后发现请求失败了, 那么我们其实就能推测, 系统出现了故障。对于 **TiDB** 来说, 我们考虑在不同组件交互的地方加上详细的 **log**, 通过外部程序分析这些 **log**, 来判断系统是否出现了问题。

8 薛定谔

在最开始开发 **TiDB** 的时候, 我们就引入了 **Chaos**, 不过那时候, 所有的操作我们都是人工来进行的, 譬如我们提交了一个大的改动, 需要进行测试, 我们会进行如下操作:

1. 找管理员申请几台物理机器, 如果这时候没有可用的物理机器, 那只有等着。这里其实非常的低效, 因为有些同学申请之后, 并不会一直在机器上面进行测试, 这时候机器其实是空置浪费的, 但别人也用不了。

2. 在集群上面编译构建 **TiDB**, 这一步持续时间会比较长, 主要是因为编译 **TiKV** 非常耗时间, 因为 **TiKV** 是用 **Rust** 语言来编写的。

3. 手工将编译好的二进制包拷贝到不同的机器上面, 因为我们是一个分布式系统, 而且有多个组件, 不同机器上面启动的组件是不一样的。

4. 一台一台机器启动不同的组件。

5. 运行测试程序。

6. 手工对不同的组件进行错误注入。

7. 观察结果。

8. 重复上面的流程。

可以看到, 这套流程非常的麻烦, 作为程序员来说, 当然是不能忍受的, 所以我们开发了一套分布式测试框架 - **Schrodinger**。

Schrodinger 是基于 **Kubernetes(K8s)** 的, **K8s** 会帮我们管理物理机器, 帮我们从繁琐的人工操作中解放出来。

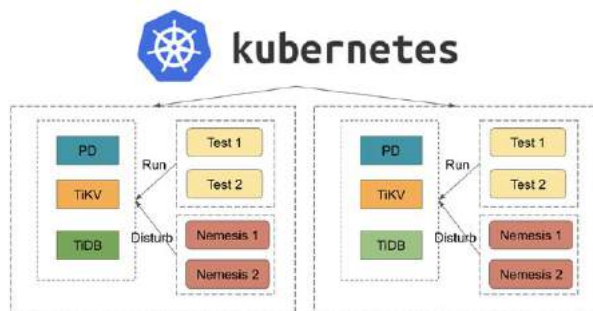


图 2 是 **Schrodinger** 的主界面, 里面详细的列出来现在的资源使用情况:

对于开发的同学来说, 现在, 如果他想对自己最新的代码进行测试, 那么就非常容易了, 主要流程如下:

1. 编写一些测试用例, 当然也可以重用现有的很多测试用例。

2. 创建一只 **Cat**, 这个 **Cat** 就是我们要测试的集群, 在这里面, 我们可以指定要测试的组件的个数, 对应的版本, 以及一些配置等。

3. 创建一个 **Box**, 将想要测试的 **Cat** 和之前的测试用例一起放在这个 **Box** 里面。

当做完了这些, **Schrodinger** 就会帮助我们创建好对应的集群, 编译对应的版本, 部署到集群并且启动, 执行测试程序, 输出测试报告。譬



图 2

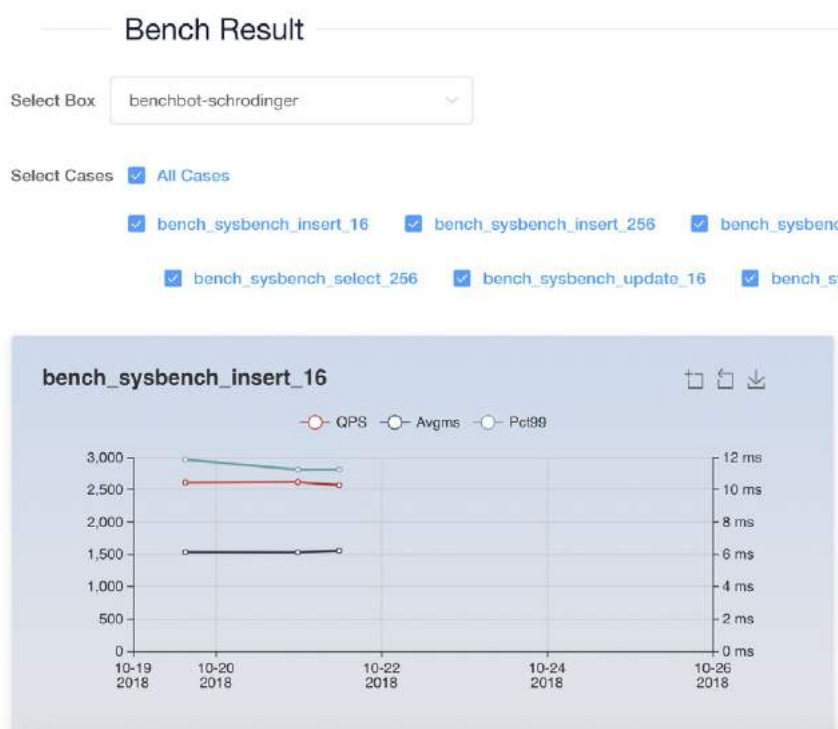


图 3

如下面就是我们的一个自动 sysbench 的 case 报告：(见图 3)

9 写在最后

本文只是简单的介绍了我们在 Chaos 上面的实战，后面我们会重点对 Schrodinger 进行优化以及功能增强，也会不断的吸取外界的优秀经验，应用到 Schrodinger 上面。也特别欢迎有相关想法的团队加入我们一起开发。

从最开始开发 TiDB 的时候，我们就把测试作为我们的最高优先事项来对待，从最初人工进行测试，到现在能自动化的进行 Chaos 实践，我们克服了很多困难，也收获了很多。正因为我们在测试方面做了这么多工作，才让我们更有信心来保证 TiDB 系统的稳定性。

本文分享的 Chaos 实践经验并非智能用于数据库的研发，完全可以用于其他分布式系统的构建，比如用于确保交易系统全序组播或区块链共识算法的可靠实现。



I 资讯采撷 nformation

17 “聚智赋能，携手共赢”

2018 上交所技术行业用户大会成功举办

18 监管科技全球追踪

“聚智赋能，携手共赢” 2018上交所技术行业用户大会成功举办

2018年12月18日，上交所技术有限责任公司举办2018上交所技术行业用户大会，来自证监会信息中心、机构部，各交易所等行业核心机构，行业协会，证券、期货、基金等市场经营机构，以及代表性科技企业在内的200多家机构，300多位嘉宾齐聚一堂，围绕“聚智赋能，携手共赢”的大会主题，就信息技术如何服务证券市场健康发展进行了深入的交流与分享。

会上，中国证监会信息中心副主任刘铁斌对近年来行业技术的发展进行了简要回顾，阐述证监会监管科技3.0的设计理念和建设进展，要求上交所充分运用科技手段服务行业监管，聚集行业力量，积极挖掘行业共性需求，为行业提供完善的基础设施服务，降低行业成本，提升行业效能。

上交所副总经理、上交所技术有限责任公司董事长徐毅林从推进核心技术创新和数字化转型、支持业务创新与发展、拓展市场服务深度和广度等方面进行总结，并强调在技术创新的支撑与支持下，2018年上交所在业务创新、产品链完善、国际化发展等方面取得的进展。

上交所技术有限责任公司总经理兼首席技术官王泊对《上交所科技战略规划》进行全面解读，介绍了上交技术系统向云化、智能化、移动化方



中国证监会信息中心副主任 刘铁斌



上海证券交易所副总经理 徐毅林

向发展的推进情况。

本次大会，上交所面向行业重点推出金桥数据中心和“证通云”等产品和服务。同时面向监管科技 3.0 建设需求，宣布依托证券信息技术研究发展中心（上海）成立监管科技实验室及低时延技术实验室，重点推进大数据、人工智能等在监管领域落地应用，以及核心交易系统低延时技术自主掌控。

大会分享环节，华为云、阿里云、腾讯、360 企业安全集团、Intel、微软等多家国内外科技企业，结合行业发展需要，介绍了云计算、数据安全、人工智能、AI 视觉和硬件性能优化等领域的前沿研究成果，以及证券行业的信息系统部署解决方案。

会议期间组织专题评审会，来自行业监管机构、核心机构和经营机构的 6 位专家，听取上交所“大数据和智能化监管”和“异地灾备中心”建设情况的汇报，围绕数据分享与治理、智能化服务落地、低成本灾备中心建设等话题展开讨论，为相关信息系统建设提供建议。

未来，上交所将进一步汇聚行业智慧，积极构筑安全、稳定、高效、共赢的服务生态圈，在为市场经营机构业务赋能的基础上，推动证券市场健康蓬勃发展。



实验室揭牌仪式



金桥数据中心启动仪式



上交所证通云发布

监管科技全球追踪

国际组织动态

经合组织发布 2018 年监管政策展望报告

10 月 10 日，经济合作与发展组织，简称经合组织 (OECD) 发布《2018 年 OECD 监管政策展望》。OECD 监管政策展望系列报告于 2015 年首次推出，2018 年发布了第二份报告。在对 2017 年广泛的 OECD 监管指标调查 (iREG) 进行分析的基础上，该展望报告强调了良好的法律法规的重要性，突出了经合组织各国良好的监管实践，并以批评视角指出了这些国家可以改善的内容。例如，该报告指出，法规的“生命周期”在很大程度上仍不完整。各国更擅长早期工作，即设计法律法规，而非后期的执行和审查。此外，现在仍然没有系统的方法用于评估法律法规在实践中是否实现了目标。尽管有的法律法规可能已经过时，给企业和监管者带来了不必要的成本，并可能给公民带来风险，各国却未能系统收集证据，监控执行情况，并对结果进行评估。同时，该报告强调，技术变革的速度势不可挡，经济体间的相互关联前所未有的，使得政府监管什么、怎么监管都变得更不确定、更复杂。现有监管体系是否有效，政府是否确实有能力适应变化都遭到了质疑。这就需要公共部门变得越来越灵活，有能力借助技术变革带来的诸多机会更好地制定规则，适应新的实际情况和风险。

国际货币基金组织和世界银行发布《巴厘金融科技议程》

10 月 11 日，世界银行和国际货币基金组织 (IMF) 共同发布《巴厘金融科技议程》。该议程指出，技术的快速发展正改变着经济和金融格局，在带来广泛机会的同时也提高了多种潜在风险。金融科技有助于促进金融业发展，加强金融普惠，提高金融效率，从而支持经济增长和减贫；但它也可能对金融体系的稳定健全以及消费者和投资者保护构成风险。各国政府迫切希望发挥金融科技的益处，同时缓解其潜在风险。《巴厘金融科技议程》旨在帮助成员国稳健发展金融科技，改善金融服务，同时管理新风险。该议程以成员国的经验为基础，将决策者和国际社会对金融科技需要考虑的关键问题总结为以下 12 个要点：1、拥抱金融科技的潜力；2、利用新技术扩大金融服务提供；3、加强竞争，恪守对开放、自由和竞争市场的承诺；4、培育金融科技以促进普惠金融和发展金融市场；5、对持续发展变化的金融体系保持密切监测，深化理解；6、调整监管框架和监管实践，促进金融体系的有序发展和金融稳定；7、保障金融体系的健全；8、实现法律框架现代化，提供有利的法律环境；9、确保国内货币和金融体系的稳定；10、建设稳健的金融和数据基础设施，以维护金融科技的优势；11、

增强国际合作和信息共享；12、加强对国际货币和金融体系的集体监督。IMF 希望它成为各国评估和制定 Fintech 政策的思考框架。对于该议程，

央行行长易纲表示，中国欢迎基金组织和世界银行共同提出的《巴厘金融科技议程》，支持将其作为基金组织关于金融科技的工作框架。

欧美动态

美国证券交易委员会发布 2018-2022 战略规划

10 月 11 日，美国证券交易委员会（SEC）宣布了一项新的战略规划，以指导未来四年的工作重点，即关注投资者、创新和业绩。该计划的目标反映了对其长期使命的承诺，同时利用机遇并应对快速发展的市场、产品和服务带来的挑战。美国证券交易委员会的新战略规划是根据 2010 年政府绩效和成果现代化法案发布的，该法案要求联邦机构概述其任务、计划举措和四年战略目标。这就要求联邦机构概述其使命、行动计划和四年的战略目标。战略规划摘要目标，一是关注普通大众投资者的长远利益。二是认识到我们不断变化的资本市场的重大发展和趋势，并调整我们的努力，以确保我们的资源得到有效分配。三是通过提高我们的分析能力和人力资源，提升 SEC 的绩效。

美国证券交易委员会宣布成立创新 与金融科技战略中心

10 月 18 日，美国证券交易委员会（SEC）宣布成立创新和金融科技战略中心（FinHub）。FinHub 将为公众参与美国证券交易委员会与 FinTech 相关问题和举措的讨论提供资源，主要涉及分布式账本技术（包括数字资产）、自动化投资建议、数字市场融资以及人工智能 / 机器学习等多个领域。FinHub 将以 SEC 几个内部工作组的工作为基础，并取代其功能，代表 SEC 处

理相关事宜。具体而言，FinHub 的职能包括：1. 为行业和公众提供一个门户网站，让他们直接与 SEC 工作人员就创新理念和技术发展进行接触；2. 在 FinHub 网站上公布有关美国证券交易委员会涉及 FinTech 的活动和举措的信息；3. 通过出版物和公共活动与公众互动，包括计划于 2019 年举办的分布式分类帐技术和数字资产的金融科技论坛；4. 作为 SEC 工作人员获取、传播 FinTech 相关知识和信息的平台和交换所；5. 担任其他国内和国际监管机构关于金融、监管和监管系统新兴技术的联络人。

英国三大金融监管部门联合发布加 密资产总结报告

10 月 29 日，英国金融行为监管局（FCA）、英格兰银行和英国财政部联合发布了关于监管加密资产和分布式账本技术（DLT）的总结报告。该报告由英国财政大臣主导成立的由英国财政部、金融行为管理局和英格兰银行组成的加密资产工作组完成，目的是评估新兴的数字资产行业以及 DLT 的潜力。特别工作组的结论认为，虽然 DLT 处于发展的早期阶段，但它有可能在未来为金融服务和其他部门带来“重大利益”。组成特别工作组的三大部门将致力于支持其发展。当然，特别工作组在表达了联合支持的意见的同时，也承认了会有相关的风险存在。这些风险主要与首次代币发行（ICO）、猖獗的欺诈以及市场操纵有关。此外，由于对消费者保护的担忧仍在上升，FCA 可能禁止向零售消费者出售以下数字

资产：所有交易代币的衍生品，如比特币、价差合约、期货、期权和可转让证券。这将不包括符合证券条件的加密资产（也经常作为证券代币引用）。特别工作组指出：“到目前为止，FCA 还没有批准任何以交易代币作为标的资产的交易场所的交易产品上市。”

伦敦证券交易所发布报告《监管科技改变监管未来的 5 种方式》

12 月，伦敦证券交易所集团发布了《监管科技改变监管未来的 5 种方式》报告。该报告简要回顾了近 10 年来监管政策的变化，包括欧盟金融工具市场指导 (MiFID)、多德弗兰克法案、通用数据保护条例 (GDPR)，以及 UnaVista（伦交所集团的子公司，为超过 10 万名用户提供监管报告综合管理平台服务）的发展历程，并分析了数据分析、人工智能、区块链等技术如何改变监管的未来。该报告指出，UnaVista 通过在线网站方便企业提交监管报告，其提供的数据分析服务使得提交监管报告不再仅是企业的负担，相反，企业能从数据分析中获取价值。同时，UnaVista 正在尽可能的简化需要人工参与的流程，使能实

时数据报告，某些企业已经能做到在交易发生 15 分钟之内汇报数据。对于区块链技术，该报告认为，终极的区块链解决方案将完全取代监管报告，因为不可变的分布式区块链将包含所有必要的信息。

瑞士金融市场监管局发布新金融科技许可证的申请指南

12 月 6 日，瑞士金融市场监管局 (FINMA) 发布新金融科技许可证的申请指南，旨在通过简化申请程序来促进金融科技创新。今年 6 月 15 日，瑞士议会通过了新金融科技许可证的相关条款，该许可证将受到修改后的瑞士银行法案 (BA) 和修改后的瑞士银行条例 (BO) 监管。自 2019 年起，申请许可证的机构需准备以下材料：一是申请理由、工商信息、集团信息等基本信息；二是股本、直接或间接持有 5% 及以上股份的股东名单、直接控制人等股权信息；三是个人信息、有效身份证明、高管简历、工作证明等申请人个人基本信息；四是业务流程、未来三个年度经营计划、组织结构、内控管理等业务活动和内部组织信息。

亚太动态

新加坡金融管理局发布智能投顾指南

10 月 8 日，新加坡金融管理局 (MAS) 公布了一份数字咨询服务指南，旨在借此推动新加坡智能投顾服务发展。指南吸纳了公众咨询中得到的反馈以及 MAS 与行业互动中的学习要点。MAS 发布的数字咨询指南依据《证券和期货条例》(SFA) 和《财务顾问条例》(FAA) 对智能投顾服务许可和商业行为提出新要求，指南还对行业改进提出了建议。根据新规定，向散户投资

者提供基金管理服务的数字顾问公司，即使不符合 SFA 的公司业绩记录要求，也可以获得智能投顾服务许可。但是，这些公司需要满足一些安全要求，包括董事会和高级管理层应当拥有基金管理和技术经验，提供包含仅非复杂集合投资计划的投资组合，并在运营第一年结束时对数字咨询业务进行独立审计等。此外，数字咨询无需遵守 FAA 关于收集客户财务状况全套信息的要求，如收入和财务承诺等信息。公司可以通过客户信息调查问卷，确定和拒绝明显不适合数字咨询产品

的客户。同时，作为财务顾问，数字顾问可以将其客户的贸易订单转交给经纪公司执行。他们无需获得 SFA 的额外资本市场服务许可，即可在集合投资计划中重新平衡客户的投资组合。

嘉银研究院与清华大学发布《印度金融科技研究报告》

嘉银新金融研究院与清华大学金融科技研究院互联网金融实验室于 2018 年 10 月联合发布《印度金融科技研究报告》，该报告聚焦印度，全面阐述其宏观环境及金融科技发展状况，重点剖析印度网贷行业、支付行业、征信行业、个人理财行业、众筹行业等细分领域，旨在通过对印度金融科技的全面分析和系统研判，深入了解印度金融科技领域，促进行业发展和交流。印度是世界第二人口大国，GDP 位列全球第六，互联网用户数量位列世界第二。消费升级开始显现，印度正充分享受人口红利。莫迪政府提出“印度崛起”口号，并推出一系列对互联网的友好政策。印度金融科技在区块链、支付、P2P、智能投顾、普惠金融、技术驱动的银行综合服务、互联网金融安全与生物识别方面存在众多亮点和潜力。

香港交易所发布研究报告《金融科技的运用和监管框架》

10 月 18 日，香港交易所发布了题为《金融科技的运用和监管框架》的研究报告。该报告由香港交易所首席中国经济学家办公室和创新实验室联合推出，着重围绕区块链和人工智能这两大技术与证券行业的结合点展开，探寻这些新技术如何与证券业的投资及交易、结算、监管层面等业务具体结合，为金融科技找到在资本市场的具体运用模式，以实际的、可操作的案例来说明金融科技对资本市场和证券交易的影响和意义。该报告介绍了区块链技术在交易结算领域的运用、资产再抵押业务和私人股

权市场的应用，以及人工智能技术在智能投研、智能投顾领域的运用。每个案例亦会比较新技术与传统业务模式的优缺点，以及运用新技术可能面临的难点和挑战。报告强调，作为一个新兴行业，基于金融科技商业模式不断发展并变得越来越复杂。在某种程度上，金融科技的应用可能无助于降低金融体系中的固有风险，反而可能会放大或暴露新形式的金融风险。因此，作为监管机构应考虑如何在适当的监管框架下将金融科技的金融创新应用于证券业。

人民银行发布金融行业云计算相关技术标准

近日，中国人民银行发布了《云计算技术金融应用规范 技术架构》(JR/T 0166—2018)、《云计算技术金融应用规范 安全技术要求》(JR/T 0167—2018)、《云计算技术金融应用规范 容灾》(JR/T 0168—2018) 等三项金融行业标准，《云计算技术金融应用规范 技术架构》规定了金融领域云计算平台的技术架构要求，涵盖云计算的服务类别、部署模式、参与方、架构特性和架构体系等内容。《云计算技术金融应用规范 安全技术要求》规定了金融领域云计算技术应用的安全技术要求，涵盖基础硬件安全、资源抽象与控制安全、应用安全、数据安全、安全管理功能、安全技术管理要求、可选组件安全等内容。《云计算技术金融应用规范 容灾》规定了金融领域云计算平台的容灾要求，包括云计算平台容灾能力分级、灾难恢复预案与演练、组织管理、监控管理、监督管理等内容。此三项标准适用于金融领域的云服务提供者、云服务使用者、云服务合作者等。

新加坡金融管理局发表 FEAT 原则以促进更好地使用 AI 和数据分析

11 月 12 日，新加坡金融管理局 (MAS) 发

布了一套原则，以促进在金融中使用人工智能和数据分析时，确保公平、道德、责任和透明。这套原则被称为 FEAT 原则，它将为提供金融产品和服务的公司负责任地使用人工智能和数据分析提供指导意见，以加强有关数据管理和使用的内部治理。随着越来越多的公司采用技术工具和解决方案来支持商业战略和风险管理，这套原则将增强人们对人工智能和数据分析的信心与信任。MAS 通过 FEAT 委员会与资深的行业合作伙伴密切合作，共同制定了这些原则。这些原则还纳入了金融机构，行业协会，金融科技公司和学术界的观点和反馈意见。

新加坡举办第三届新加坡金融科技节

第三届新加坡金融科技节于 11 月 12 日至

16 日在新加坡成功举办。本届金融科技节由新加坡金融管理局、新加坡银行公会和新加坡展览集团联合主办，赞助商包括了尚乘、GIC、万事达、德勤、毕马威、渣打银行等传统金融领域企业，也包括了谷歌、亚马逊、甲骨文、英特尔等知名科技企业。据悉，本次金融科技节共吸引了来自接近 130 个国家、45000 人参与，是世界最大规模的金融科技盛会。包括印度总理莫迪、国际货币基金组织总裁拉加德、加拿大总理特鲁多、肯尼亚央行行长帕特里克·恩乔罗以及老挝中央银行行长松赛·西帕赛等外国政要也出席了本届新加坡金融科技节。本届金融科技节上开展了众多精彩活动，包括全球金融科技加速竞赛展示日、人工智能（AI）金融峰会、金融科技颁奖典礼、走访创新实验室、研讨会等。

2019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。

2019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），请通过投稿邮箱 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：2019 年 3 月 31 日。

4、投稿联系方式 021-68813289, 021-68800293 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)

关键字：(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)

四、参考文献 (仿宋 GB2312 小四)

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：021-68813289

021-68800293

投稿邮箱：ftt.editor@sse.com.cn

ITRDC

证券信息技术研究发展中心（上海）



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>

内部资料 免费交流

本刊物仅为内部交流使用，本季度刊印1200册，编印单位为上交所技术有限责任公司，面向证券期货行业发送，印刷日期为2019年1月，印刷单位上海长鹰印刷厂。

部分图片或文字来源于互联网等公开渠道，其版权归属原作者所有。如有版权相关事宜，请发送邮件至ftt.editor@sse.com.cn