



黄红元 主编

上海证券交易所联合研究报告 2014

证券信息前沿技术专集



黄红元 主编

上海证券交易所联合研究报告 2014

证券信息前沿技术专集

图书在版编目(CIP)数据

上海证券交易所联合研究报告.2014:证券信息前沿技术专集/黄红元主编.—上海:上海人民出版社, 2015

ISBN 978-7-208-13409-6

I. ①上… II. ①黄… III. ①资本市场-研究报告-世界-2014②证券交易所-经济信息-研究报告-世界-2014 IV. ①F831.51

中国版本图书馆 CIP 数据核字(2015)第 266043 号

责任编辑 吴书勇

封面装帧 王小阳

上海证券交易所联合研究报告 2014

——证券信息前沿技术专集

黄红元 主编

世纪出版集团

上海人民出版社出版

(200001 上海福建中路 193 号 www.ewen.co)

世纪出版集团发行中心发行 上海商务联西印刷有限公司印刷

开本 720×1050 1/16 印张 19 插页 4 字数 335,000

2015 年 12 月第 1 版 2015 年 12 月第 1 次印刷

ISBN 978-7-208-13409-6/F·2334

定价 52.00 元

本书编委会

主 编：黄红元

副主编：白 硕

执行编辑：王 泊 黄寅飞

编 委 会：刘 凯 张佳岭 郑凌云 金 鑫 黄俊杰

楼晓鸿 唐 忆 石丹妮 程婉芸

目录

1	证券行业数据交换硬件转码技术研究
121	证券风控监察业务复杂事件处理应用研究
189	证券行业关键业务系统及云平台安全性研究
245	证券业高性能实时软件的多核与并行计算研究与应用
268	证券电子商务及支付模式分析研究

证券行业数据交换硬件转码技术研究^{*}

上海证券交易所—中国科学院信息工程研究所联合课题组

第一节

金融领域硬件加速技术综述

术语表

术 语	解 释
FIX	金融信息交换协议(Financial Information eXchange, FIX),适用于实时证券、金融电子交易开发的数据通信协议
STEP	证券交易数据交换协议(Securities Trading Exchange Protocol, STEP)
FAST	FIX Adapted for Streaming 的缩写(适流 FIX)
HFT	High Frequency Trading,高频交易
FPGA	Field Programming Gate Array,可编程门阵列,一种硬件芯片
Xilinx	世界上最大的 FPGA 供应商,产品主要面向高端客户

一、硬件加速技术

硬件加速是指在计算机中通过把计算量非常大的工作部分或全部分配给专门的硬件来处理以减轻计算机主处理器(CPU)的工作量的技术。相对处理器而言,这些专门的硬件都具有高并发、高性能等特性,通过合理的设计使算法的可并行特性与硬件本身的并发结构相结合,可以实现相比于软件方法的几倍甚至几个数量级的性能加

^{*} 课题主持:戴琼;协调人:黄寅飞;课题组成员:姜磊、唐球、杨嘉佳。

速比。随着多年的硬件加速技术的发展与变迁,目前主流的硬件加速平台有图形处理器(Graphics Processing Unit, GPU)、网络处理器(Network Processor, NP)、数字信号处理器(Digital Signal Processor, DSP)、专用集成电路(Application Specific Integrated Circuit, ASIC)、现场可编程门阵列(Field Programmable Gate Array, FPGA)。

(一) 图形处理器

图形处理器(GPU)又称显卡内核、视觉处理器,是一种专门在个人电脑、工作站、游戏机和一些移动设备(如平板电脑、智能手机等)上图像运算工作的微处理器。最初用于加速图形处理,尤其是 3D 图形处理。尤其一颗 GPU 包含了成千个小的、高效的计算单元,现在 GPU 广泛应用于计算机密集型的应用中。GPU 加速计算是指利用一颗 GPU 以及一颗 CPU 来加速科学、工程以及企业级应用程序。与 CPU 的区别是,CPU 由专为顺序串行处理而优化的几个核心组成。而 GPU 则由数以千计的更小、更高效的核心组成,这些核心专为同时处理多任务而设计(原理如图 1 所示)。

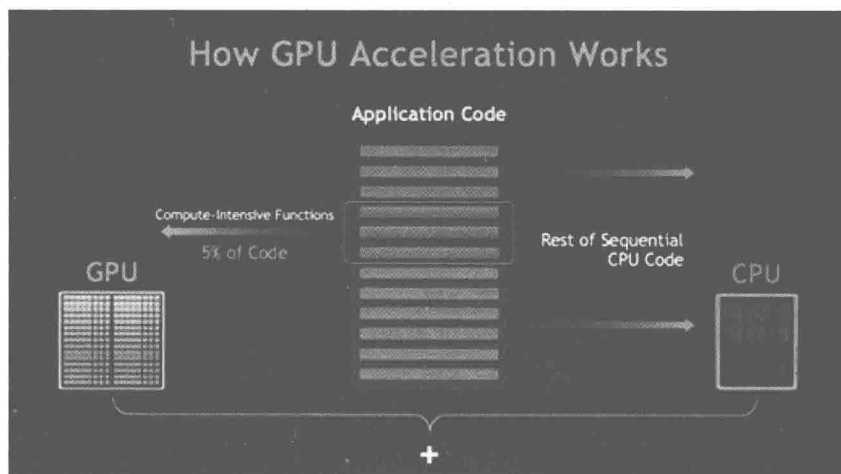


图 1 GPU 加速的原理

(二) 网络处理器

网络处理器(NP)是一种可编程器件,它特定的应用于通信领域的各种任务,比如包处理、协议分析、路由查找、声音/数据的汇聚、防火墙、QoS 等^①。网络处理

^① Liljeqvist, Bjorn, "Visions and Facts—A Survey of Network Processors", *Electronic Engineering*, Chalmers(2003).

器器件内部通常由若干个微码处理器和若干硬件协处理器组成,多个微码处理器在网络处理器内部并行处理,通过预先编制的微码来控制处理流程。而对于一些复杂的标准操作(如内存操作、路由表查找算法、QoS的拥塞控制算法、流量调度算法等)则采用硬件协处理器来进一步提高处理性能,从而实现了业务灵活性和高性能的有机结合。NP 顾名思义,它很适合网络通信领域的数据处理。因为它既有微码处理器可编程的灵活性,又有专用协处理器的高性能的特性。它的不足之处就是微代码的开发相对复杂,导致灵活性较差,难以满足复杂多变的市场需求;另一方面,固定大小的微码空间也限制了应用的丰富性;不同的网络处理器对业务应用的适应性也存在各种各样的限制,对于真正的灵活业务应用,网络处理器还是缺乏必需的灵活变通的能力。

(三) 数字信号处理器

数字信号处理器(DSP)是一种专用于(通常为实时的)数字信号处理的微处理器,有自己的完整指令系统,是以数字信号来处理大量信息的器件^①。一个数字信号处理器在一块不大的芯片内包括控制单元、运算单元、各种寄存器以及一定数量的存储单元等等,在其外围还可以连接若干存储器,并可以与一定数量的外部设备互相通信,有软、硬件的全面功能,本身就是一个微型计算机。DSP 采用的是哈佛设计,即数据总线和地址总线分开,使程序和数据分别存储在两个分开的空间,允许取指令和执行指令完全重叠。也就是说,在执行上一条指令的同时就可取出下一条指令,并进行译码,这大大提高了微处理器的速度。另外还允许在程序空间和数据空间之间进行传输,因为增加了器件的灵活性。其工作原理是接收模拟信号,转换为 0 或 1 的数字信号,再对数字信号进行修改、删除、强化,并在其他系统芯片中把数字数据解译回模拟数据或实际环境格式。它不仅具有可编程性,而且其实时运行速度可达每秒数以千万条复杂指令程序,远远超过通用微处理器,是数字化电子世界中日益重要的电脑芯片。它的强大数据处理能力和高运行速度,是最值得称道的两大特色。由于它运算能力很强,速度很快,体积很小,而且采用软件编程具有高度的灵活性,因此为从事各种复杂的应用提供了一条有效途径。DSP 作为专门的为处理器,主要用于计算,DSP 通过汇编或高级语言(如 C 语言)进行编程。因此,它的优势是具有软件的灵活性,编程速度快,软件更新速度快,适用于计算复杂的多算法任务。DSP 的缺点是它受

^① Lyons, Richard G., *Understanding digital signal processing*, Pearson Education, 2010.

限于串行指令流的限制,采样率低。

(四) 专用集成电路

专用集成电路(ASIC)是为特定用户或特定应用制定的专用集成电路^①。ASIC拥有悠久的历史,为汽车、医疗、工业、军事、航空和通信等众多应用市场的领先制造商提供混合信号及数字 ASIC 解决方案。由于是集成电路,所以 ASIC 的性能很高,但是它的开发周期长、开发成本与风险高,设计流片生产之后,将不能对 ASIC 进行任何更改。因此,ASIC 适合对专用芯片有大批量需求、应用稳定、要求处理速度快且在很长一段时间内无更新需求的应用场景。

(五) 现场可编程门阵列

现场可编程门阵列(FPGA)是在 PAL、GAL、CPLD 等可编程器件的基础上进一步发展的产物。它是作为专用集成电路(ASIC)领域中的一种半定制电路而出现的,既解决了定制电路的不足,又克服了原有可编程器件门电路数有限的缺点。对比其他的硬件技术,FPGA 最大的特点是可以对电路进行重复烧写,根据需求更改电路的功能。

FPGA 由可编程逻辑单元阵列、布线资源和若干分散的块内存构成,一个 FPGA 的资源包含丰富的逻辑门、寄存器、块内存和 I/O 资源。FPGA 的结构灵活,其逻辑单元、内部连线、块内存和 I/O 单元都可以由用户编程,可以实现任何逻辑功能,满足各种设计需求。其速度快,功耗低,通用性强,特别适用于复杂系统的设计。使用 FPGA 还可以实现动态配置、在线系统重构(可以在系统运行的不同时刻,按需要改变电路的功能,使系统具备多种空间相关或时间相关的任务)及硬件软化、软件硬化等功能。

如图 2 所示,CLB 代表了可编程的逻辑单元,Switch Blocks 表示了内部的连线节点,通过控制 Switch Blocks 的打开与关闭,可以改变 FPGA 内部逻辑单元的连通状态,从而让 FPGA 实现不同的功能。I/O Cells 表示 I/O 管脚,一个 FPGA 中,管脚资源是非常珍贵的,直接决定了 FPGA 可以外接的器件数量。管脚资源数是固定的,因此其可以连接的外部存储器,高速接口的数量也是有限的,要注意充分利用。

^① J. Wolkerstorfer, E. Oswald, and M. Lamberger, "An ASIC implementation of the AES SBoxes", in *Topics in Cryptology—CT-RSA*, Springer Berlin Heidelberg, 2002, pp.67—78.

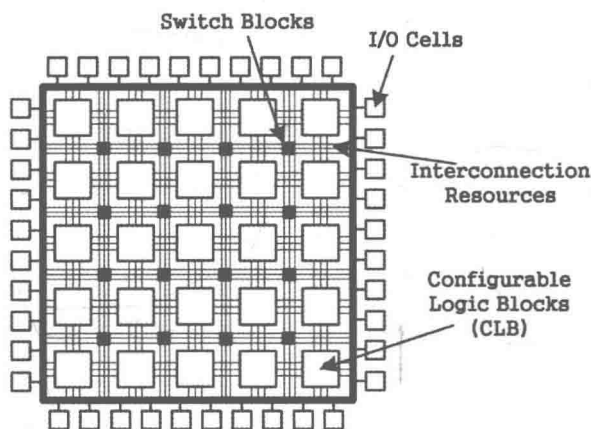


图 2 FPGA 内部结构示意图

目前主要的 FPGA 厂家有 Xilinx、Altera、Actel 等^①。其中 Altera 作为世界老牌可编程逻辑器件的厂家,是 可编程逻辑器件的发明者,开发软件主要有 MaxPlusII 和 QuartusII。Xilinx 是 FPGA 的发明者,主要提供高端的 FPGA 产品,开发软件为 ISE 和 Vivado。Actel 主要提供非易失性 FPGA,产品主要基于反熔丝工艺和 FLASH 工艺,其产品主要用于军用和宇航。从市场份额来看,Xilinx 公司占有的市场份额最大,拥有全世界一半以上的市场份额,其次是 Altera 公司。

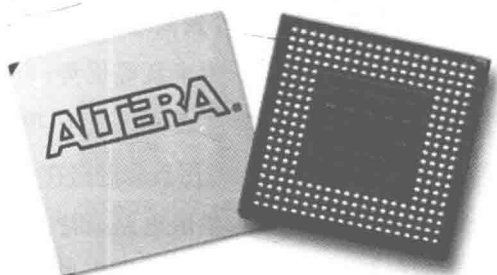


图 3 Altera 公司的一款 FPGA 芯片

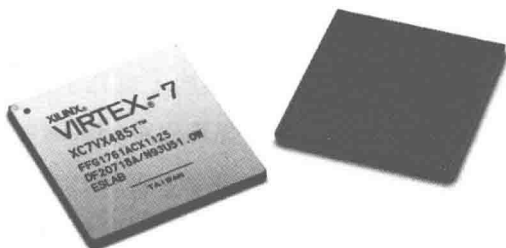


图 4 Xilinx 公司的一款 FPGA 芯片

^① J.J.Rodriguez-Andina, M.J.Moure, and M.D.Valdes, “Features, design tools, and application domains of FPGAs”, *Industrial Electronics, IEEE Transactions on*, vol.54, 2007, pp.1810—1823.

（六）硬件加速技术对比

以上五种硬件加速平台都有各自的特色与优势,有适合其发挥作用的场景,也有混合使用的场景,因此不能一概而论,绝对化地比较优劣之势。不同的研究和设计方案,在速度、面积、成本、灵活性等方面都有很大的差别,在实际应用中,应当根据应用需求,扬长避短,在某些应用领域中选择特定的硬件平台达到最优的加速方案。GPU 适合计算密集型的应用,编程相对简单,但是它往往受限于存储带宽;NP 处理器专门为网络数据处理而设计,它特别适合网络数据处理,如高性能路由器、交换机等,但是它的微代码开发相对复杂,对开发者要求高,开发灵活性较差,同时固定大小的微码空间也限制了应用的丰富性;不同的网络处理器对业务应用的适应性也存在各种各样的限制,对于真正的灵活业务应用,NP 处理器还是缺乏必需的灵活变通的能力;DSP 很适合做信号处理,浮点计算。它采用高级编程语言编程,因此它的开发门槛较低、开发灵活、开发速度快,它的不足是采样频率低、受限于串行指令流的限制;ASIC 最大的优势是速度快、集成度大、芯片尺寸小等,但是它最大的不足就是灵活性差、芯片不可重新编程、开发周期长、开发成本与风险高。ASIC 适合对专用芯片有大批量需求、应用稳定、要求处理速度快且在很长一段时间内无更新的需求的应用场景;FPGA 则既具有 ASIC 的高性能特点,又克服了 ASIC 的灵活性上的不足,具有可编程、开发周期短等优势。FPGA 开发的编程灵活度很大,它具有天然的并发性、逻辑资源丰富等优势;FPGA 是集成电路中设计周期最短、开发费用最低、风险最小的器件之一。此外,单个专用集成电路芯片的生产成本很高,如果出货量较小,则采用专用集成电路在经济上不太实惠。这种情况下可以使用 FPGA 作为目标硬件实现集成电路设计。但是,FPGA 也有自己的缺点,由于兼顾了可重编程的灵活性,FPGA 在面积、速度方面的优化程度不如全定制的集成电路。

随着技术的发展,一些硬件出现了融合的趋势,如最新的一些 ASIC 也具有简单的可编程功能,而最新推出的 FPGA 性能上也几乎接近 ASIC,NP、FPGA 内也都包含了 DSP 模块。2010 年,德州仪器公司(Texas Instruments, TI)推出了一款基于 KeyStone 架构的网络协处理器^①,NETCP,就是一个典型的 DSP 与 NP 结合的芯片产品。该处理器专门用于处理以太网数据包,集成了多个 TMS320C66x 数字信号处理 DSP 模块,并包含了一个数据包加速器和安全加

^① Texas Instruments, “Key Stone Architecture Multicore Navigator”, 2011.9. Website: www.ti.com.

速器,可以快速进行以太网数据包交换,数据流分类和数据包加解密操作。现在市场上的 Xilinx、Altera 的 FPGA 芯片都含有 DSP 模块。例如,最新的 Xilinx 推出的 Zynq-7000 平台^①中的 Z-7100 就提供 2 020 片 18×25 MACCs DSP 模块。

总体而言,FPGA 架构天然的并发性和可重定制架构适合高吞吐量数据处理和灵活的硬件加速程序设计,最为贴合本项目的实际需求。以 Xilinx 28 nm 芯片工艺的器件为基础,集成 HKMG 技术以更低的功耗将系统性能实现最大化。最新的 Xilinx FPGA 的 HPC 平台能以单芯片提供高达 2 TFLOPS 的高处理性能,且功耗远低于 GPU 和多核 DSP,如图 5 所示,最新的 Xilinx 7 系列的芯片与最新的 GPU、DSP 的功耗对比图。

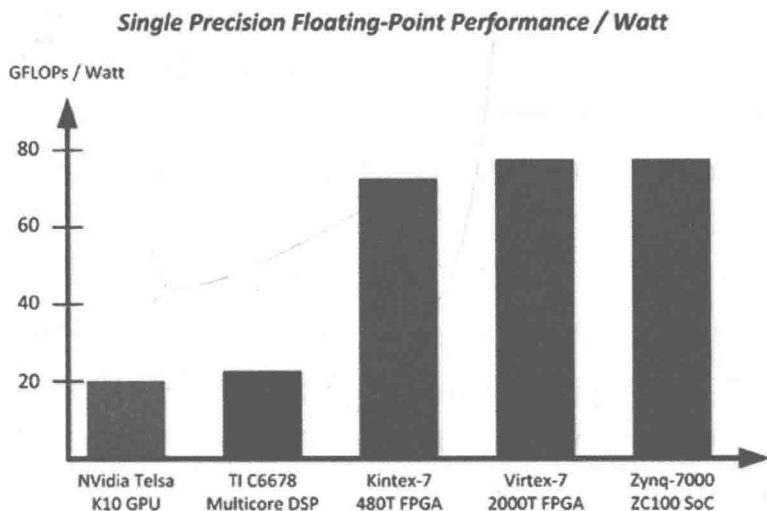


图 5 FPGA 与 GPU、DSP 的功耗对比图

二、数据处理 FPGA 加速技术

随着 FPGA 集成逻辑门数量的增加、性能的提升、功耗的不断优化,而且加入高性能 DSP、高速串行收发器、处理器微处理器软/硬核等模块,现在 FPGA 芯片已经广泛应用于信息处理与航空航天、军用、科学、医疗、金融、汽车电子以及生命科学等领域,并为这些应用提供低功耗高性能的解决方案。目前最新 28 nm 工艺的

^① M.Santarini, "Zynq-7000 EPP sets stage for new era of innovations", *Xcell J*, vol. 75, 2011, pp.8—13.

Xilinx 器件的高性能处理平台能以单芯片提供高达 2 TFLOPS 的高处理性能,且功耗远低于 GPU 和多核 DSP。

FPGA 在数据处理方面,其速度高出 CPU 几个数量级,加之它低功耗的优势,目前 FPGA 开始进入传统的服务器计算领域,Intel 与 AMD 等传统的 CPU 制造公司也已开始研发基于 CPU 与 FPGA 的集成处理芯片。

(一) 密码处理 FPGA 加速技术

2006 年由德国的鲁尔大学与基尔大学的工作组建立 COPACOBANA 项目成功地暴力破解了 DES 密码^①,使用了 120 片并行的 Xilinx Spartan3-1000 的 FPGA,120 个 FPGA 分为 20 个 DIMM 模块,每个模块包括 6 个 FPGA。总造价大约是 10 000 美元,是同等破解能力的服务器系统的 1/25。使用可重配置的 FPGA,使得这种设备也可以用于其他密码的破解。2008 年,改进版本的 COPACOBANA RIVYERA 将破解 DES 的时间减少到了 1 天以内,使用 128 片 Spartan-3 5000 型 FPGA。目前,项目 RIVYER 保持着使用暴力破解法破解 DES 的纪录。

(二) 网络处理 FPGA 加速技术

2009 年,由欧洲 CESNET 设计的具有多种速率接口的开放硬件平台:COMBO 系列网络分析卡^②。COMBO 系列网络分析卡的核心是利用一个或者多个 FPGA 来搭建,并在其外围配置存储以及连接器等部件。COMBO 系列网络分析卡支持千兆到 10 Gbps 的各种网络接口速率,且板卡和主机之间,板卡与板卡之间可以实现互连。研究者们试图利用 COMBO 系列网络分析卡来实现独立的网络分析功能。基于这个开放的硬件平台,研究者们实现了高性能网络监测适配器 Scampi,用于网络数据采集和监测的网络探针 FlowMon,入侵检测系统 IDS,网络应用通用开发平台 NetCOPE 等项目。目前,COMBO 系列网络分析卡已经用于 6NET,SCAMPI,GN2 等欧盟主要的网络测量和分析项目。

① S.Kumar, C.Paar, J.Pelzl, G.Pfeiffer, and M.Schimpler, "Breaking ciphers with COPACOBANA—a cost-optimized parallel code breaker", In proceedings of the 8th international conference on Cryptographic Hardware and Embedded Systems. Springer-Verlag, 2006, pp.101—118.

② J.Novotny, Z.Martin, "COMBOv2-Hardware Accelerators for High-Speed Networking." XILINX Academic Forum, 2008.

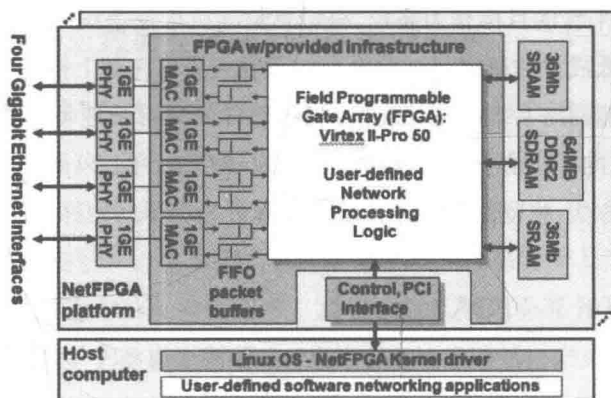


图 6 NetFPGA 板卡架构图

2009 年,斯坦福大学的研究人员推出了 NetFPGA 平台^①,最初是设计用于网络硬件和路由器设计教学的实验平台,现在则被世界各地的研究者们用于验证在高速网络上的新思路。NetFPGA 硬件的结构框图如图 7 所示,整个平台的核心是基于 Xilinx Virtex-2 FPGA 芯片搭建的,NetFPGA 具有 4 个千兆以太网接口以及片外的存储资源。在这个平台上,研究者们实现了开放的 Openflow 交换机和路由器,并将其应用部署在斯坦福大学的校园网和 Internet 骨干网上,用于进行新的网络实验和新协议的验证。2010 年,又推出了 NetFPGA-10G 版本^②,对比旧的 NetFPGA 板卡 (NetFPGA-1G),新的板卡采用了更高性能的 FPGA 芯片,更加丰富的硬件资源。相对第一代 NetFPGA 平台 (NetFPGA-1G) 而言,第二代平台 (NetFPGA10G) 搭建引入了四个 10 Gbps 光纤接口的光纤网络以便进行更高性能的网络研究。NetFPGA-10G 平台是一种 40 Gb/s、以 Virtex-5 FPGA 为核心构建的板卡,拥有庞大的 FPGA 架构,并且能够最大限度地支持各种服务与应用,并提供了网卡、交换机、路由器等参考设计。

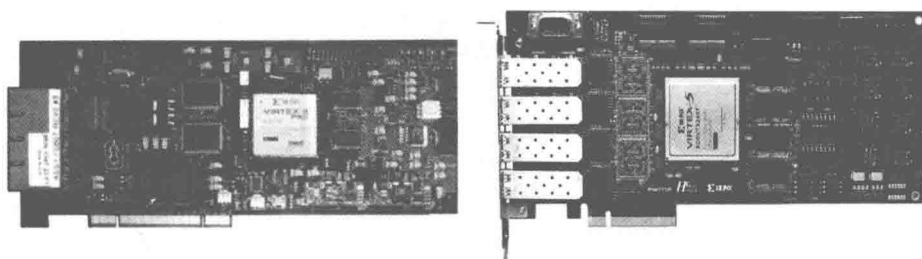


图 7 NetFPGA-1G 及 NetFPGA-10G 板卡图

① J.W.Lockwood, N.McKeown, G.Watson, G.Gibb, P.Hartke, J.Naous, *et al.*, “NetFPGA—An Open Platform for Gigabit-Rate Network Switching and Routing”, in *Microelectronic Systems Education*, 2007, MSE’07. IEEE International Conference on, 2007, pp.160—161.

② NetFPGA-10G, http://netfpga.org/10G_specs.html.

NetFPGA 平台的目标是为高校、科研单位等机构或组织的研究人员提供易扩展、可重配置、低成本的研究与试验平台。研究人员可在其上搭建千兆乃至万兆级别以上的高性能网络系统模型,同时可利用硬件的并行加速特点进行网络流的处理,而复杂多变的网络协议则由软件层来实现与控制。此外,研究人员可以利用模块化的思想与方法,将复杂的硬件模块逐步划分为简单的硬件模块再进行处理。

(三) 超级计算 FPGA 加速技术

2011 年,由英国格拉斯哥大学的范德堡韦德博士和美国马萨诸塞大学卢维尔分校的同行共同研发一款将 FPGA 配置成 1 000 个处理核的 CPU,每个核独立运行自己的指令,测试结果表明其运算速度相比安装普通 CPU 的台式机提升了 20 倍^①。

2012 年,Xilinx 基于其最新的低、中端 7 系列 FPGA 芯片构建了一个高性能、可扩展的软硬协同处理平台:Zynq[®]-7000,它主要由一块 FPGA 芯片(Artix7 或 Kintex7)与一个 1 GHz 双核 ARM Cortex-A9 MPCore 微处理器构成,两大芯片通过 AMBA AXI 互联通信,如图 8 所示。Zynq-7000 通过硬件、软件和 I/O 可编程性实现了扩展式系统级差异、集成和灵活性。通过 Zynq-7000 平台,可以快速地设计出更智能、更高效、低功耗的 SoC 系统。

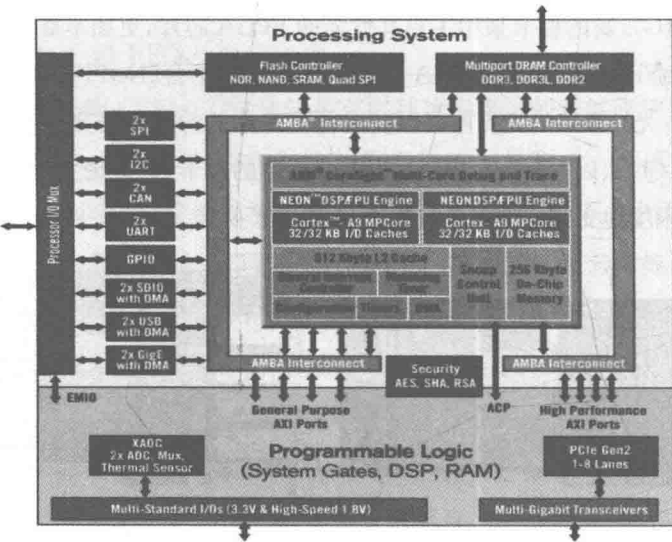


图 8 Zynq-7000 平台

^① M.Lis, P.Ren, M.H.Cho, K.S.Shim, C.W.Fletcher, O.Khan, *et al.*, “Scalable, accurate multicore simulation in the 1000-core era”, in *Performance Analysis of Systems and Software (ISPASS)*, 2011 IEEE International Symposium on, 2011, pp.175—185.

三、面向证券行业数据交换的 FPGA 加速技术

本节综述了使用 FPGA 加速金融证券交易的应该与研究现状,已有的应用中更多的是使用 FPGA 加速高频交易。通过调研综述发现,使用 FPGA 加速金融证券交易还是一项比较新的技术,已有的文献较少。以下综述几个比较有代表性的工作,尤其“硬件加速 FIX 订单取消系统”与“FPGA 加速高频交易”的工作比较有代表性,给出了更多的 FPGA 加速细节。总体上的实现思路从两方面进行加速:(1)使用 FPGA 部分或全部编解码 FIX/FAST 消息;(2)使用 FPGA 加速网络流处理。在 FPGA 实现 TCP/IP 协议栈,使实时市场行情数据流通过硬件直接进行协议解码,跳过操作系统的协议栈,达到加速网路流处理。

(一) 订单取消 FPGA 加速系统

2011 年,Wall Street FPGA 公司的发表了技术白皮书:“Hardware Accelerated FIX Order Cancel System”^①。其主要贡献是采用 FPGA V5 加速 FIX 协议中的订单取消系统,使用开源的 FIX 系统 Quick Fix。加速系统是部署于一块基于 FPGA 实现的网卡上,并优化了 QuickFIX。整个 FIX 4.2 订单取消消息是在 FPGA(不需要借助软件)上快速生成。实验结果表明,从触发取消订单到该消息的第一个字节传输到达网络的时延为 314 ns,从触发订单取消到该订单取消消息全部传输到达网络的时延为 1 874 ns。

当证券交易过程中特定事件出现后,交易商需向交易所发送一系列的取消订单,并且希望尽快得到响应,避免损失。详细介绍如下:

随着信息化的发展,交易量的增加,如图 9 所示。峰值交易周期提供了最有利的投资机会,同时也蕴含了最大的损失风险。因为在峰值交易周期内,必须在交易系统变得开始趋势下滑与无利点到来之前,大量的交易市场数据能够被迅速的分析与处理掉。

高频交易(HFT)正在影响市场动态与产生利益争论。一家公司参与了高频交易的最直接的好处是可以在市场大震荡中最大限度的保护自己的资产。如 2010 年 5 月 6 日美股市场的“闪电崩盘”^②(如图 10 所示)。像这类股市瞬间震荡

^① T.Stratoudakis, “Hardware accelerated fix order cancel system”, Wall Street FPGA, LLC, New York City, 2011. http://assets.tabbforum.com/research2011/WallStreetFPGA_FIX_CANCEL_FPGA.pdf.

^② 李敏波、孟辉、孔哲:《从美股“5.6 闪电崩盘”看高频交易对市场的影响》,《金融发展研究》2011 年第 7 期,第 50—53 页。

期间，一家交易公司可能因为使用了基于 FPGA 加速的订单交易取消系统而且先于其他交易公司成功撤销订单，从而减少损失。



图 9 信息化带来的交易量的增加趋势

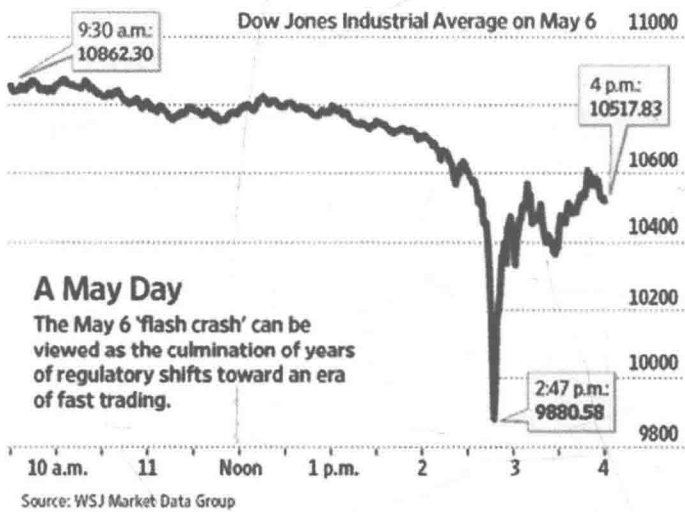


图 10 2010 年美股市场“闪电崩盘”

一个交易商(broker-dealer)连接至一个交易所，二者之间通过 FIX 协议^①进行消息通信。交易商提交订单至交易所等待撮合匹配。所有来之交易商的订单都是

^① Financial Information eXchange(FIX)，website: www.fixtradingcommunity.org.