网络交易风险控制理论

Risk Control Theory of Online Transactions

蒋昌俊　于汪洋　著

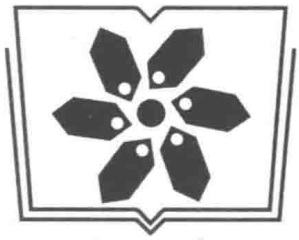
科学出版社

网络交易风险控制理论
Risk Control Theory of Online Transactions

蒋昌俊　于汪洋　著

科学出版社

北京



中国科学院科学出版基金资助出版

作者简介

蒋昌俊，男，教授，博士生导师，国家杰出青年科学基金获得者，973 项目首席科学家。1986 年和 1991 年于山东科技大学分别获得计算数学学士学位和计算机软件与理论硕士学位，1995 年于中国科学院自动化研究所获得控制理论与工程博士学位，1997 年于中国科学院计算技术研究所博士后出站。2008 年至 2015 年任同济大学副校长，现任东华大学校长、同济大学嵌入式系统与服务计算教育部重点实验室主任、上海市电子交易与信息服务知识服务平台主任。

主要学术职务有：国家自然科学基金委员会信息学部咨询委员会委员（2014-2016）、中国人工智能学会副理事长（2015-）、中国自动化学会常务理事（2006-）、中国自动化学会网络信息服务专业委员会主任（2015-）、中国计算机学会理事、中国云体系产业创新战略联盟副理事长（2014-）、上海市科学技术协会副主席（2012-）、美国电子电气工程师学会（IEEE）上海分会副主席（2007-）、中国人工智能学会会士（CAAI Fellow，2017-）、英国工程技术学会会士（IET Fellow，2014-）。被授予英国 Brunel University 荣誉教授（2016-）等。担任《Big Data Mining and Analytics》《计算机学报》《软件学报》《电子学报》《人工智能学报》《应用科学学报》《计算机研究与发展》等编委。担任国际学术会议主席、程序委员会主席等 20 余次。目前与香港城市大学、澳门大学、法国国立高等电信学校、芬兰奥尔多大学，美国阿贡实验室、科罗纳多大学、新泽西理工大学、德克萨斯理工大学和德国基尔大学等开展合作。

主要从事网络并发理论、网络风险防控、网络计算环境和网络信息服务的研究。担任国家重点基础研究发展计划（973 计划）项目“信息服务的模型与机理研究”首席科学家。先后主持国家自然科学基金重大研究计划集成项目、国家自然科学基金重点项目、国家高技术研究发展计划（863 计划）项目和国际重点科技合作项目等 10 余项。在《中国科学》《ACM Transactions on Embedded Computing Systems》《ACM Transactions on Autonomous and Adaptive Systems》《IEEE Transactions on Computers》《IEEE Transactions on Parallel and Distributed Systems》《IEEE Transactions on Mobile Computing》《IEEE Transactions on Services Computing》《IEEE Transactions on Automation Science and Engineering》《IEEE Transactions on Systems, Man, and Cybernetics》等国内外重要刊物和会议文集上发表论文 300 余篇，论文被国内外同行引用 2800 余次。独立完成著作 2 部，分别由科学出版社（中国科

学院科学出版基金资助）和高等教育出版社（教育部优秀博士论文出版基金资助）出版。获国家授权发明专利和澳洲创新专利 60 项、国际 PCT 专利 19 项，行业技术标准 17 项。承担的 2 项国家自然科学基金面上项目的结题评价为“特优”，973 计划项目、国家自然科学基金重大研究计划集成项目和重点项目等结题评价均为“优秀”。

研究成果获得 2016 年国家科学技术进步二等奖（第 1 位）、2013 年国家科学技术进步二等奖（第 1 位）、2010 年国家技术发明二等奖（第 1 位），省部级三大奖（自然科学、技术发明、科技进步）一等奖 5 项（均为第 1 位）等。此外还获得首届全国百篇优秀博士论文、国际离散事件动态系统（discrete event dynamic system，DEDS）领域何潘清漪奖（每两年一次，每次奖励 1-2 位优秀论文作者）、国际期刊《International Journal of Distributed Systems and Technologies》2010 年度最佳论文、11th IET Innovation Awards、15th ACM MobiHoc Best Paper Awards（国内学者首次获得）等。指导的研究生撰写的论文中，1 篇获得全国优秀博士论文提名、1 篇获得计算机学会优秀博士论文、5 篇获得上海市优秀博士论文。2007 年所带领的“嵌入式服务计算”团队获得教育部优秀创新团队的荣誉。

于汪洋，男，副教授，博士。2013 年毕业于同济大学电子与信息工程学院，现就职于陕西师范大学计算机科学学院，2016 年 12 月至 2017 年 12 月在英国德比大学进行学术访问。主持国家自然科学基金青年基金项目等，在《IEEE Transactions on Automation Science and Engineering》《IEEE Transactions on Systems, Man, and Cybernetics》等国内外重要刊物和会议文集上发表论文 20 余篇。主要研究兴趣为 Petri 网理论及应用、可信软件、网络交易系统等。

序

随着互联网的迅猛发展，我国网络交易等新兴产业迅速发展，已成为国民经济稳定与可持续发展的重要组成部分。然而，与行业高速发展相比，我国网络交易的关键技术仍较落后，监管能力及手段明显不足。近年来，互联网交易遭受恶意攻击、木马劫持、网络钓鱼以及信用卡诈骗等愈加严重，各类交易欺诈、走私逃税等违法经营行为层出不穷。

传统的交易风险控制以法制为主，在相应法律约束下通过监管、监控实现控制。然而受限于新兴业态的发展不完善与研究数据储备不足，即有的法律规范难以满足，因此出现了新的技术，如交易的认证机制、第三方托管机制、参与者的认知能力分级机制、交易中的地域分级机制等。通过细分交易参与者信息，针对不同场景制定详细的交易规则，实现风险控制。但是，以“欺诈”为主要特征的网络交易安全威胁是现有以身份认证为核心、以规则检测为手段、以防御攻击为目标的风险防控技术难以防范的！

蒋昌俊教授带领同济大学的研发团队率先提出了网络交易风险防控的行为认证技术，建立了用户行为数据挖掘的要素路径与标准规范；通过采集和分析用户在系统中留下的蛛丝马迹，构建了表征用户特征和习惯的“行为纹理”和“交易模式”；设计了基于模型的行为认证机制，突破了在线交易规则审核实时性差、放行率低的技术瓶颈，有效克服了交易欺诈的高辨识和强实时的难题。相关成果发表在国内外重要学术期刊上，并被国际同行专家高度评价。

该书是作者研究成果的体现，也是基于信息学科研究网络交易风险控制的第一本学术专著，同时对互联网金融风险控制方面的学习和研究具有重要参考价值。特此推荐给相关领域的各位读者。

中国工程院院士 郑纬民

2017 年 11 月于上海

前　言

网络交易已成为新的经济金融重要组成部分之一，对国民经济的可持续健康发展具有重大战略意义。与此同时，交易支付欺诈问题也呈现爆炸式增长趋势。网络交易犯罪逐渐呈现出规模化、体系化的特点。面对逐渐形成的黑灰色产业链，保障网络交易的安全性变得越来越复杂，网络交易流程和行为的可信问题也变得越来越突出，已逐渐成为网络交易发展面临的瓶颈问题。可信的网络交易系统不仅需要成熟的、合适的理论基础，还依赖于先进的信息技术所实现的网络交易认证与分析平台，并提升网络交易的安全管理水平和管理效率。

本书从信息技术角度，介绍网络交易风险防控的理论和相关技术，首次将行为认证方法引入网络交易的可信保障，开展行为认证技术在网络交易系统中的应用研究。科研团队历时 20 多年的研发，持续得到上海市、国家自然科学基金委员会、科技部等单位的项目支持，形成了网络交易支付系统风险防控关键技术的整套理论与方法，研制了大规模网络交易风险防控系统平台，并在支付宝（中国）网络技术有限公司等进行了应用示范。

网络交易风险控制技术的研究，不仅从理论方法上建立行为认证理论和面向业务过程的建模和分析技术，推进可信网络交易过程的研究，而且从应用上研制大规模网络交易风险防控平台，实现大规模、强实时网络交易监控和管理，使用户的网络交易过程更安全，为在线非可信交易筑起一道坚固的防线，未来还有望应用于互联网金融工程、自贸区离岸结算等更多领域中。

本书着重介绍网络交易系统的建模、软件系统的风险防控、用户行为的风险防控、网络交易系统的在线监控、征信分析等技术。研究团队发表了数 10 篇 SCI、EI 等高质量论文，获得了数 10 项专利授权，培养了 20 多名博士、硕士及博士后。网络交易风险防控相关研究成果先后获得了上海市科学技术进步一等奖和国家科学技术进步二等奖。

感谢邬江兴院士对本书提出了许多宝贵的意见，并为本书撰写了序言。感谢同济大学嵌入式系统与服务计算教育部重点实验室的老师、博士生、硕士生及博士后的大力支持与帮助，感谢他们为本书提供了写作素材。

本书不仅适合信息技术领域相关研究人员参考，而且适合可信软件和网络交易领域相关人员阅读。

由于时间仓促，水平有限，书中不妥之处在所难免，敬请读者批评指正。

作　者

2017 年 4 月

目　录

第一章 绪 论

1.1 引 言

近年来，随着网络技术的发展，以及“互联网+”相关政策的支持，网络交易作为新的商业模式发展异常迅速。据中国互联网络信息中心统计，截至 2016 年 12 月，我国网络购物用户规模达到 4.67 亿[1]。团购、网上支付、互联网理财和在线旅游全面增长。然而，网络交易的安全可信问题也越发凸显。在各行业网站系统中，电子商务类网站存在高危因素比例最高，为 26%[2]。2014 年因网络消费遭遇安全问题的网民达 8000 万人，占网民总数的 12.6%。49%的网民表示互联网不太安全或非常不安全[3]。国内外各大电子商务网站也频频出现各种技术问题、业务问题、安全事件等[4]。比如，众多的开源电子商务系统与第三方支付平台的流程缺陷[5-7]；2012 年某第三方支付平台存在的安全隐患导致用户资金损失[8]；某 B2C 充值平台的缺陷使该商务网站受到重大损失[9]；2013 年出现了“授权支付”及新形式的交易劫持[10]；2014 年各大电子商务平台所暴露的各种安全问题也给网络购物带来了新的威胁，利用服务器程序与应用程序的接口实施恶意行为已成为新的趋势[2]。同时，近年来以网络钓鱼为典型的社会工程学方法正在大面积地危害网络交易的健康发展。

在动态、开放的网络环境下，分布式网络交易系统之间的协作是通过各个主体的业务交互来实现的。网络交易系统结构多样，参与的主体众多，比如银行、第三方支付平台、买方客户端、购物网站等。交易主体之间通过应用程序开放接口进行交互和通信，如应用程序接口(application programming interface，API)、Web 服务接口、软件即服务(software-as-a-service，SaaS)、现金即服务(cash-as-a-service，CaaS)等，将其各自复杂的业务流程组合成完整的、松耦合的、更复杂的混合网络应用。在开放的网络环境下，这种整合和交互带来了更多的不确定性，从而产生了新的安全挑战。不同主体、会话之间的交互复杂，业务逻辑难以一致，内部数据状态难以协调；业务流程之间数据流、控制流和资金流的复杂联动会导致非常严重的问题，比如交易属性的违反和巨大的经济损失。加之复杂多变的人为因素，不同主体的业务流程之间、不同会话之间、客户端和服务器之间交互所带来的业务逻辑错误，可以被恶意用户所发掘，即使传统的安全需求

被满足(信息完整性、访问控制、安全策略等)，恶意用户仍然可以通过一系列系统允许的行为实现恶意目的，获取非法利益。

网络交易流程的实体和方式不断发生变化，开放、动态的网络环境也使得网络交易系统面临的环境复杂多样。据艾瑞咨询统计，天猫、淘宝服务平台的第三方服务商数量已超过2800多个。阿里巴巴甚至提出“聚石塔”和“阿里无线百川计划”，增强与第三方业务的合作[11]。多样化的系统结构和众多角色参与，使得不同主体之间的流程协作复杂，安全风险必然随之增加。因此，网络交易软件系统的流程设计和构造存在可信隐患会导致以业务流程为核心的网络交易系统在运行时出现不可预期的行为。

众所周知，网络交易已经成为互联网产业的重要组成部分，对于未来信息化时代的生活和经济发展是极其关键的。2015年12月工信部发布的《国务院关于积极推进“互联网＋”行动的指导意见》进一步指出：“推动工业电子商务平台、第三方物流、互联网金融等业务协同创新和互动发展……深化企业间电子商务应用……”，本书的内容符合上述国家重大发展趋求,相关研究成果将具有广泛的应用前景。

1.2　互联网发展

自互联网接入中国以来，中国的网络应用飞速发展。互联网基础设施建设的不断完善、利好政策的持续出台，以及互联网对于各个行业的渗透，共同促进了网民规模的持续增长。2016年上半年，国务院等相关部门相继出台有关“互联网+政务服务”“互联网+流通”“互联网+制造业”等指导意见,推动互联网与各个行业的融合。2016年4月，习近平总书记在网络安全和信息化工作座谈会上提出“推动我国网信事业发展，让互联网更好造福人民”。未来互联网作为信息社会的基础设施，将进一步对中国政治、经济、文化、社会等领域发展产生深刻影响[12]。

2016年，我国个人互联网应用保持稳健发展，用户规模均呈上升趋势，其中网上外卖和互联网医疗是增长最快的两个应用，年增长率分别达到83.7%和28%[1]；网络购物也保持较快增长，半年增长率为8.3%。手机端大部分应用均保持快速增长，其中手机网上外卖用户规模增长最为明显，半年增长率为40.5%，同时手机网上支付、网络购物的半年增长率均接近20%。政府在推动消费升级的同时加大对跨境电商等相关行业的支持，网上购物平台从购物消费模式向服务消费模式拓展[12]。

互联网金融类应用在2016年保持增长态势，网上支付、互联网理财用户规模

增长率分别为 9.3%和 12.3%[12]。电子商务应用的快速发展、网上支付厂商不断拓展和丰富线下消费支付场景，以及实施各类打通社交关系链的营销策略，带动非网络支付用户的转化；互联网理财用户规模的不断扩大、理财产品的日益增多、产品用户体验的持续提升，带动大众线上理财的习惯逐步养成。平台化、场景化、智能化成为互联网理财发展新方向。

2016 年，各类互联网公共服务类应用均实现用户规模增长，在线教育、网约车、在线政务服务用户规模均突破 1 亿，多元化、移动化特征明显。在线教育领域不断细化，用户边界不断扩大，服务朝着多样化方向发展，同时移动教育提供的个性化学习场景以及移动设备触感、语音输出等功能性优势，促使其成为在线教育主流；网约车领域，基于庞大的市场需求和日益完善的技术应用，行业规模不断扩大；在线政务领域，政府网站与政务微博、微信、客户端结合，充分发挥互联网和信息化技术的载体作用，优化政务服务的用户体验[12]。

在网民数量方面，截至 2016 年 12 月，中国网民规模达 7.31 亿，全年共计新增网民 4299 万，增长率为 6.2%。互联网普及率为 53.2%，较 2015 年年底提升了 2.9 个百分点，超过全球平均水平 3.1 个百分点，超过亚洲平均水平 7.6 个百分点。中国网民规模已经相当于欧洲人口总量。我国手机网民规模达 6.95 亿，网民中使用手机上网的人群占比由 2015 年年底的 90.1%提升至 95.1%，较 2015 年年底增加 7550 万。网民上网设备进一步向移动端集中。随着移动通信网络环境的不断完善以及智能手机的进一步普及，移动互联网应用将更加向用户各类生活需求深入渗透[1]。

1.3 网络交易现状

中国电子商务经过 20 年的发展，市场不断优化，电商巨头阿里巴巴、京东、唯品会等纷纷赴美上市。一方面，电商由综合网络购物不断向母婴、跨境、农村等细分领域发展；另一方面，线上线下结合、企业合纵连横、大数据技术的运用，都象征着中国电子商务走向生态化发展道路。而企业不断打通生态入口、产品、服务和场景，对自身生态体系内的资源重新整合[13]。

截至 2016 年 12 月，我国网络购物用户规模达到 4.6 亿，占网民的 63.8%，增长率为 12.9%，我国网络购物市场依然保持快速、稳健增长趋势。其中，我国手机网络购物用户规模达到 4.41 亿，占手机网民的 63.4%，年增长率为 29.8%。作为 O2O 主要入口，移动端的普及为 O2O 发展起到直接的保障作用，是开展各种形式的线上线下结合的用户基础。2016 年我国购买互联网理财产品的网民规模达到 9890 万，相比 2015 年底增加用户 863 万，网民使用率为 13.5%，较 2015 年

底提升 0.4 个百分点。互联网理财市场历经几年的快速发展，理财产品日益增多，用户体验持续提升，网民的线上理财习惯初步养成。截至 2016 年 12 月，我国使用网上支付的用户规模达到 4.75 亿，较 2015 年底增加 5831 万，增长率为 14%，我国网民使用网上支付的比例从 60.5%提升至 64.9%。其中，手机支付用户规模增长迅速，达到 4.69 亿，年增长率为 31.2%，网民手机支付的使用比例由 57.7%提升至 67.5%[1]。

截至 2016 年 12 月，网上预订机票、酒店、火车票或旅游度假产品的网民规模达到 2.99 亿，较 2015 年年底增长 396 万，增长率为 15.3%。网民使用网上预订火车票、机票、酒店和旅游度假产品的比例分别为 34.0%、15.9%、17.2%和 7.4%。其中，手机预订机票、酒店、火车票或旅游度假产品的网民规模达到 2.62 亿，较 2015 年底增长 5189 万，增长率为 24.7%。我国网民使用手机在线旅行预订的比例由 33.9%提升至 37.7%[1]。

艾瑞咨询最新数据显示，2016 年中国电子商务市场交易规模 5.2 万亿元，同比增长 30.8%，环比增长 12.9%。其中移动网络购物同比增长 56.1%，成为推动电子商务市场发展的重要力量。另外，B2B 市场 13.7%、在线旅游 28.4%的同比增长共同拉动了电子商务市场交易规模增长。网络购物行业发展日益成熟，各家电商企业除了继续不断扩充品类、优化物流及售后服务外，也在积极发展跨境网络购物、下沉渠道发展农村电商。在综合电商格局已定的情况下，一些企业瞄准母婴、医疗、家装等垂直电商领域进行深耕，这些将成为网络购物市场发展新的促进点。移动网络购物市场集中度很高，阿里无线、唯品会、京东、苏宁、国美等企业也大力发展移动端，移动端占比均有提升，市场竞争较激烈[14]。

从宏观政策到企业促销，政府和企业合力推动消费升级。“十三五”规划从顶层设计明确了消费升级方向，强调以扩大服务消费为重点带动消费结构升级，引导消费朝着智能化、环保化、集约化、品质化方向发展。作为传统零售与信息消费相结合的产物，网络购物顺应了这一向新型消费升级的发展趋势。与此同时，电商平台营销方式多元化升级，从购物消费模式向服务消费模式延伸拓展。如在电脑端和移动端引入媒体元素进行兴趣导购，拓展电商媒体化功能；探索视频电商导购模式，以短视频和直播为载体深挖网红效应的经济价值等[12]。

1.4　网络交易风险

网络交易软件系统的安全风险也随着网络购物的迅猛发展而凸显出来。许多电子商务软件的技术不够成熟和可靠，存在安全漏洞，极易被外来入侵者利用，从而导致巨大的经济损失。据有关统计数据，美国每年因为网络安全问题在经济

上造成的损失就达到近百亿美元，而国内的情况也不容乐观[15]。2010 年有超过 1 亿用户曾遭遇过至少一种针对网络购物的安全威胁，带来的直接经济损失突破 150 亿元，网络购物用户的人均经济损失也由 2009 年的 80 元上升至 150 元左右[16]。据中国互联网络信息中心(China Internet Network Information Center，CNNIC)统计，2011 年上半年，有 8%的网民在网络购物时遭受过经济损失，该群体规模达到 3880 万人[17]。此外，网络购物木马与钓鱼网站也严重威胁着网络购物安全。据 2011 年金山网络云安全中心统计，每天监测到的网络购物木马传播量就达到上千次，钓鱼网站更多，与 2010 年同期相比，不管是钓鱼网站服务器主机数与拦截访问次数均增加了 10 倍之多[18]。2016 年第二季度，360 互联网安全中心共拦截各类新增钓鱼网站 37.5 万个，虚假购物类网站占比为 16.2%，假冒银行占比为 8.7%，虚假购物的诈骗案例达到了 862 例，占比为 15.8%，网游交易 658 例，占比为 12.0%，虚拟商品 654 例，占比为 12.0%，金融理财 497 例，占比为 9.1%[19]。

网络交易过程中的典型案例也层出不穷，比如开源电子商务系统 NopCommerce+Paypal 的支付流程漏洞在网络交易软件系统中具有相当的典型性；2010 年 8 月，苹果公司 iTunes 组件程序的漏洞导致 iTunes 用户的 Paypal 账户被攻击，但不通过 iTunes 而直接在线购买是安全的[20]。2010 年出现了针对网络交易的新攻击方式：交易劫持[10]。黑客利用用户的合法身份，在用户正常交易的同时，产生一笔后台交易且收款方为黑客账户。在用户即将支付、付款的环节，正常交易被劫持到黑客后台交易，从而将用户的钱支付到黑客账户。黑客已经就网络购物安全威胁形成了一条完整的产业链条，集团化作战趋势越来越明显，网络购物的危险因素越来越多，欺诈手法也层出不穷，安全形势十分严峻。甚至于安全性很高的银行系统也屡次出现问题。近年来，针对银行、证券等金融行业的高级持续性威胁(advanced persistent threat，APT)不断出现。2016 年 2 月 5 日，孟加拉国央行(Bangladesh Central Bank)被黑客攻击而导致 8100 万美元被窃取[21]。综合 360 互联网安全中心各项大数据分析显示，2016 年“双十一”虚假购物类钓鱼网站制作更加精良，并且有大量钓鱼方式是通过入侵正规政府或大型企业网站制作完成的，从而大大增加了安全软件的防护难度。不仅如此，2016 年“双十一”截获的新增钓鱼网站总量较 2015 年“双十一”增长了 18.7%，360 猎网平台共接到全国用户网络诈骗举报 532 起，人均损失达 9282.8 元。金融行业网站漏洞威胁更加复杂化，不仅传统的银行、保险等金融领域，还包括新兴的第三方支付、互联网 P2P 领域也曝出不少高危漏洞[22]。

针对网络交易系统，微软研究院和印第安纳大学伯明顿分校联合研究团队，以及加州大学戴维斯分校研究团队曾做了大量的案例研究，发现了众多潜在的实

际问题，并提出业务流程中的逻辑缺陷已愈发重要。图 1.1 和图 1.2 为一个真实的案例。图 1.1 为一个分布式网络交易业务流程示意图(完整具体的业务流程细节可参见相关文献)，由客户端、开源电子商务平台 NopCommerce 以及第三方支付平台 PayPal 组成。三方各自的业务流程组合成完整的网络交易流程，这样就容易导致各个主体互不了解内部状态，使整个交易过程的数据状态不一致，从而使得恶意用户有机可乘。图 1.2 为恶意用户行为流程图，在该系统中，具有合法账号的恶意用户可以扮演不同身份，打开多个会话，通过调用分布式网络交易系统的开放接口来实现自己的恶意目的，从而违反相关交易属性，例如交易完整性。最后实现的效果就是：只付一次钱，通过反复发送签名信息，得到任意多个同样价格的物品。

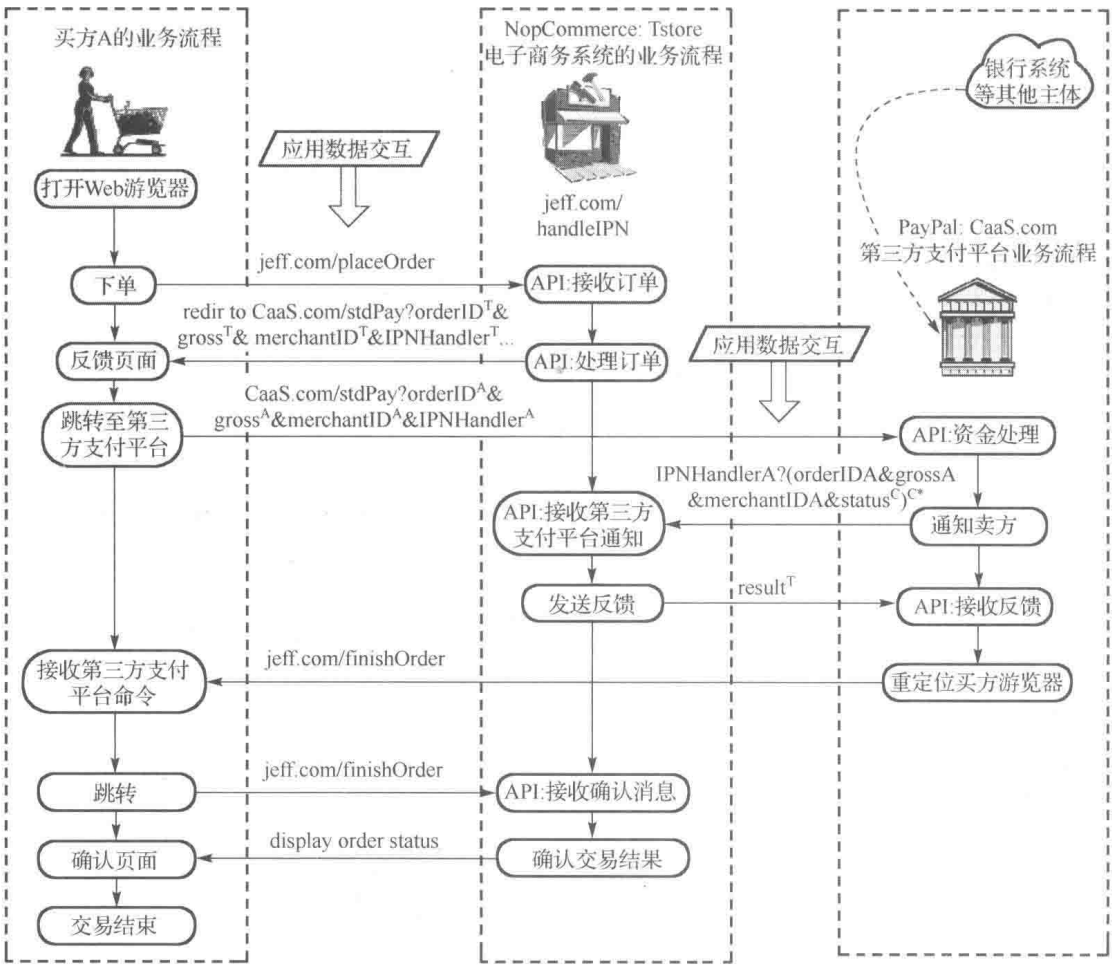


图 1.1　分布式网络交易业务流程