电子商务交易协议理论与验证方法

王茜 著

DIANZI SHANGWU JIAOYI XIEYI LILUN YU YANZHENG FANGFA

中山大学出版社

电子商务交易协议理论与验证方法

王茜 著

DIANZI SHANGWU JIAOYI
XIEYI LILUN YU YANZHENG FANGFA

中山大学出版社
·广州·

图书在版编目（CIP）数据

电子商务交易协议理论与验证方法/王茜著．—广州：中山大学出版社，2010.7

ISBN 978-7-306-03500-4

Ⅰ．电…　Ⅱ．王…　Ⅲ．电子商务—研究　Ⅳ．F713.36

中国版本图书馆 CIP 数据核字（2009）第 181622 号

出 版 人：祁　军
策划编辑：嵇春霞
责任编辑：王　睿
封面设计：林绵华
责任校对：陈　霞
责任技编：何雅涛
出版发行：中山大学出版社
电　　话：编辑部 020-84111996，84111997，84113349，84110779
　　发行部 020-84111998，84111981，84111160
地　　址：广州市新港西路 135 号
邮　　编：510275　　传　真：020-84036565
网　　址：http://www.zsup.com.cn　E-mail：zdcbs@mail.sysu.edu.cn
印 刷 者：广州中大印刷有限公司
规　　格：787mm×960mm　1/16　11.875 印张　210 千字
版次印次：2010 年 7 月第 1 版　2010 年 7 月第 1 次印刷
定　　价：23.00 元
印　　数：1-1500 册

前　言

随着全球经济一体化进程的加快，电子化的交易方式在世界范围内逐渐得到普及与应用。其中，电子商务交易协议既是电子商务交易安全的重要保障机制，又是进行电子商务交易的过程标准，同时还是电子商务交易顺利完成的关键。鉴于电子商务交易协议的研究在经济活动中的重要意义和广阔的应用前景，一直吸引着世界各国政府、学术界和经济界的极大关注，成为全球范围内具有前瞻性的研究课题。

本书是对国家自然科学基金资助项目“基于离线可信第三方的电子现金交易系统理论与方法”的一个全面总结。全书围绕电子商务交易协议相关理论和协议验证方法展开，从保护交易双方利益的角度出发，针对电子商务交易协议，尤其是电子现金支付理论研究和实际应用中存在的瓶颈问题，以电子商务交易安全框架为主线，对电子商务交易协议的底层安全技术、交易协议属性、交易协议的模型以及交易协议验证的理论和方法进行了系统的阐述。全书通过对电子商务交易协议核心理论的梳理，建立了较为直观的研究体系。该体系具有理论层次清晰、逻辑结构合理的特点。同时，本书对传统核心理论存在的问题进行了剖析，并通过构建模型、设计协议、验证方法改进等取得了一系列的研究成果，是对相关理论的有益补充，该书是电子商务交易协议理论和方法阐述较为系统深入的一部著作。

全书共分为六章，第一章对电子商务交易系统安全体系及典型交易协议需要满足的基本属性进行了综览与梳理，提出并分析了各属性间在协议设计机理上的制约关系。第二章、第三章和第四章详细论述了电子支付协议的模型、协议设计等基本理论。第五章和第六章则分别系统阐述了电子商务交易协议的分析验证方法。

本书围绕电子商务交易协议理论与方法展开，可作电子商务安全、网络金融、电子支付等课程的研究生和本科生教学参考书，亦可作为从事电子商务安全的科技人员、网络金融管理人员的参考书。

本书在写作过程中参阅与引用了大量中外文献资料及研究成果，主要参考文献已经列在书后。在此，作者对国内外有关作者表示诚挚的敬意与衷心的感谢！

由于作者水平有限，再加之电子商务交易系统领域的研究颇为复杂，因此，书中难免出现错漏之处，恳请读者对此提出批评意见，并能及时反馈给作者。

目　录

第一章　电子商务交易系统

1.1　电子商务交易系统发展

20世纪90年代以来，随着网络技术的飞速发展，网络化和全球化成为不可抗拒的世界潮流。电子商务作为一种新兴的商业模式，突破了传统的时空观念，缩小了生产、流通、分配、消费之间的差距，提高了物流、资金流、信息流的有效传输和处理，在拓展商务空间、降低成本、提高效率、促进经济贸易发展方面发挥着越来越重要的作用，成为国民经济和社会信息化的重要组成部分，代表着未来商务的发展方向。

2010年1月15日，中国互联网络信息中心（CNNIC）在北京发布了《第25次中国互联网络发展状况统计报告》。数据显示，截至2009年12月，我国网民规模已达3.84亿人，较2008年年底增长8600万人，互联网普及率达到28.9%。同时，该调查报告显示，随着互联网用户的增加，商务交易类应用的用户规模增长最快，平均年增幅达到了68%。其中，网上支付用户年增幅80.9%，在所有应用中排名第一。据CNNIC调查，2009年中国电子商务市场规模（交易额）超过35000亿元，同比增长48.5%，高于2008年的41.2%。其中C2C市场增速更是达到97.8%，达到2340亿元。

可见，电子商务在催生新经济和推动经济全球化中所表现出的巨大能量，引发了传统商务的全方位变革，改变着商务活动方式、消费方式以及企业的生产方式，促进了流通网络体系建设，推动了多种流通渠道和流通环节的创新，带动了商业的快速变革和创新。电子商务已经成为改善商务环境、促进商务发展的必要形式和载体。同时，电子商务的应用已经成为决定企业国际竞争力大小的重要因素，而且还是评价一个国家经济发展水平和可持续

发展能力的重要指标。

电子商务的诱人发展前景引起了世界各国政府与国际组织的重视，相继提出了一系列促进电子商务发展的文件。联合国国际贸易委员会于1996年12月通过了《电子商务示范法》，为各国电子商务立法提供了一个范本。1997年美国政府发表了《全球电子商务框架》（*FGEC*），把促进电子商务的发展作为主要任务，不遗余力地推动其在全球的推广和应用。1998年10月，经济合作与发展组织（OECD）召开了电子商务部长级会议，就电子商务发展的重要性、有关原则和下一步工作重点达成了一致意见，并发表了题为《全球电子商务行动计划》的联合宣言。1998年年初，欧盟各国也提出了《欧盟电子商务行动方案》，对电子商务在经济发展中的作用、电子商务的法律框架、电子交易的安全性等问题进行探讨。同样，日本也十分重视电子商务的发展，于1996年成立了“电子商务促进会”，并投入巨资对电子商务项目进行研究。

我国政府也敏锐地意识到电子商务对经济增长和企业竞争力的巨大影响，对电子商务的发展予以高度关注。国家信息产业部信息化推进司、外经贸部、国家经贸委、海关等单位于1998年6月拟定了我国《国家电子商务发展总体框架》。从20世纪90年代起，我国政府在全国推动电子商务的实际运行方面，取得了一系列成绩。例如，银行业的电子化、招商银行的一卡通、中国第一个完整的电子商务中心的成立、中国商品交易市场的大规模的电子商务实践等等。所有这些都说明，电子商务成为不可逆转的潮流，为了促进电子商务的发展，创造一个良好的电子商务运行环境，国际组织和各国政府都在积极进行开拓性的工作。

1.1.1 电子商务交易的网上支付发展

随着Internet和电子商务的迅速发展，特别是信息安全技术的进步，电子支付作为电子商务活动中最为核心和重要支撑体系已经取得长足发展。电子商务交易的关键在于安全地实现网上信息传输和在线支付功能，是伴随着商务活动电子化而形成的支付流程电子化，是电子商务中最为核心和复杂的环节。

近几年来，西方发达国家在电子支付工具的研发和推广方面投入巨大，大都建成了覆盖全国的电子金融结算网络，如美国的FEDWIRE、国际上的

SWIFT 与 CHIPS 资金支付结算网络等，为电子支付提供了良好的支撑环境。这些国家的电子支付已基本普及，为网络时代电子商务的发展奠定了基础。

20 世纪 80 年代以来，随着信息技术在中国银行业的广泛应用，电子支付业务在中国也得到迅速发展。我国的电子支付建设起步较晚，发展水平同发达国家存在很大差距。但我国近年来推广电子支付的力度较大，自 20 世纪 90 年代以来实施了如“三金工程”等一系列信息化工程和中国国家现代化支付系统的建设，为电子支付的应用提供了良好的基础。经过多年的努力，我国也建成了多个电子支付结算系统。

在政策鼓励及第三方电子支付企业的努力和创新下，近年来电子支付市场发展十分迅速。艾瑞咨询研究显示，2006 年中国第三方电子支付市场交易额规模为 500 亿元，2007 年交易额规模迅速增长并突破 1000 亿元，增幅达 100%。艾瑞咨询数据显示，2009 年网上支付市场交易额规模达 1560 亿元，环比上涨 26.2%，同比上涨 117.3%。2009 年前三季度网上支付市场交易额规模之和为 3892 亿元，同比上涨 119.7%。2009 年国内第三方支付市场交易额规模接近 6000 亿元。

第三方电子支付交易额呈现超过 100% 的高速增长，反映出国内电子支付市场广阔的发展空间。有关分析指出，内部的支付需求、用户基础，外部电子商务的推动，共同促进了电子支付市场的快速发展。一方面，中国经济的快速稳定发展创造了巨大的财富，这是支付需求产生的基础；另一方面，庞大的互联网用户、手机用户群保证了电子支付的巨大市场需求。中国电子商务的快速发展是推动电子支付前进的巨大动力。

（1）网上支付的蓬勃发展。

网上支付是指通过 Internet 完成支付的行为和过程，是构成电子商务的一个关键环节。在此过程中仍然需要银行作为中介，通过交易双方在银行开设的账户实现交易资金的转移，通过传统的支付系统完成跨行交易的清算和结算。电子支付工具通过电子支付渠道实现不同账户间资金所有权的转移，它安全、高效且便利。在当前的第三方支付市场中，网上支付仍为最主要的支付方式，2007 年仅第三方网上支付交易额规模就达 976 亿元。其中，以银行卡为代表的电子支付工具就是信息技术应用于金融领域取得的成功典范之一。

信用卡既是一种电子支付工具，也是一种信贷工具，这两项功能使其愈

益成为人们生活中不可缺少的重要组成部分，被广泛接受和使用；同时，经营信用卡业务的高额利润也使发卡机构纷纷将其作为发展的重点，因此，信用卡在美国等发达国家获得了飞速的发展。正是由于信用卡的发展为电子支付产业积累了丰厚的收益，才有足够的资金用于产业发展所需的大量基础设施投入，使整个产业能够蓬勃发展，因此，信用卡对整个电子支付产业的培育和发展具有举足轻重的作用。

而借记卡必须依托于持卡人的存款账户，具有电子存折的性质，在一定程度上是支票的替代品。借记卡对于持卡人而言，使用安全、方便、快捷；对银行来说没有信用风险，管理方便，成本较低，是一些对风险承受能力较弱的中小银行进入银行卡市场的很好领域。签名借记卡通过核对持卡人的签名进行身份验证，其交易流程和信用卡完全相同，可以在所有能够接受信用卡的商户中使用。

为了适应人们生活和社会经济发展不断产生的新的支付需要，各种新的电子支付工具，如储值卡、EBT 卡、预授权支付、远程支付等纷纷涌现，并取得迅速的发展。

（2）电子支付渠道规模化及集中化的发展。

在信息技术的推动下，支付工具逐渐电子化，并出现了一些全新的电子支付工具。电子支付包含三个基本要素：核心是个人支付账户，载体是电子支付工具，基础设施是电子支付渠道。其中，电子支付渠道的作用就是使购买者在经济交易发生时利用电子支付工具，通过电子支付渠道，与个人支付账户取得联系，经过确认、授权和清算等程序，完成货币所有权的转移，完成支付。因此，没有广泛分布的电子支付渠道，电子支付工具就无从应用，电子支付也无从进行。正是电子支付工具发展的强大需求，推动电子支付渠道的迅速发展，而电子支付渠道的发展，又促进了电子支付工具的迅速普及。由于所基于的个人支付账户及支付工具不同，电子支付渠道也发展为多种，并在电子支付工具快速增长和多样化发展的推动下，不断扩大渠道范围，不断拓宽应用领域，不断扩大所能受理的支付工具。

电子支付渠道的经营具有显著的规模经济效应，因此，在市场竞争中“强者越强”现象明显。规模较大的企业具有明显的竞争优势，这使其能够在竞争中不断地兼并、收购对手，从而经营规模越来越大，形成了庞大的网络体系；同时，市场越来越集中于少数几家大规模运作的企业，电子支付渠

道的发展表现出明显的规模化、集中化的发展趋势。

1.1.2 电子现金交易系统发展

电子支付手段是开展电子商务的必要工具。电子现金（E-Cash）正在取代纸币成为主要的支付工具之一。它保留所有传统现金的基本属性，有极好的安全性、可靠性和匿名性，成为电子支付方式中的一种不可替代手段。

尽管 E-Cash 大范围的应用普及还需以时日，但各个国家和研究机构、公司、银行都意识到其在经济中的重大意义和应用前景的美好，都非常重视 E-Cash 的发展，并积极开展这方面的贮备研究，目前 E-Cash 研究和试验开展得如火如荼。

总部分别设在荷兰和美国的 DigiCash 公司是目前唯一一家在商业上提供专业电子现金系统的公司。1994 年 5 月，该公司提出了著名的无条件匿名的电子现金系统 DigiCash 系统。该系统通过数字记录现金，集中控制和管理现金，允许消费者使用 E-Cash 进行在线交易，是一种足够安全的电子交易系统。第二年，DigiCash 公司又提出了一种名为 CyberBucks 的电子现金系统，并在美国圣路易 Mark Twain 银行试验，目前大约有 50 家 Internet 厂商和 1000 名客户使用这种电子现金。据 Mark Twain 银行的高级副行长兼国际市场主管 Frank Trottert 称："第一阶段是零售商业系统，然而真正的潜力在于形成一个全球性的面向商业的支付网络。"目前，使用该系统发布的银行有 10 多家，包括 Mark Twain、Eunet、Deutsche、Advance 等世界著名银行。

另一个电子现金系统——NetCash 系统是由美国南加州大学信息科学研究所的 B. 科兰德·诺曼和甘那迪·玛文斯基发明设计，它设置分级货币服务器来验证和管理电子现金，是可记录的匿名电子现金支付系统。

E-Cash 系统则是由 DigiCash 开发的另一个在线交易用的数字货币，具有和保留了传统现金的特性和属性，因此，人们称其为"网络现金"。E-Cash 系统已经在美国密苏里州 St. Louisr 的 Mark Twain 银行进行了试验，参加试验系统的使用者约 1 万人，零售商店约 2000 家。同时，美国的 IBM 公司也积极投入资金研究 E-Cash 系统，并提出了 Mini-pay 系统，这是另一种 E-Cash 模式。该产品使用 RSA 公共密钥数字签名，交易各方的身份认证通过证书来完成。

英国西敏寺（National Westminster）银行开发了以智能卡为钱包的电子

现金系统。后来，西敏寺银行又与英国的米德兰（Midland）银行合作，共同出资成立了一家经营 Mondex 电子现金的公司，并发明了 Mondex 电子现金支付系统，是世界上最早的电子钱包系统，于 1995 年 7 月首先在有“英国的硅谷”之称的斯温顿（Swindon）市试用。1996 年，Mondex 电子现金系统在世界上许多发达国家和地区进行试用和推广。香港汇丰银行和恒生银行隆重推出电子现金 Mondex；澳大利亚最大的 4 家银行和新西兰的 6 家银行，也都相继建立并推广了 Mondex 电子现金应用系统；1998 年，Mondex 在美国纽约试用，还以合同连锁方式在其他城市进行实验，参加的银行有曼哈顿银行、芝加哥银行和法兰西银行等；同时，澳大利亚的国家银行也引入了 Mondex，南非和以色列等国家也制定了相同计划。

虽然 Mondex 电子现金系统在一些大型银行实验推广，但是如德国、比利时、芬兰和丹麦等国家，并没有直接接受它，都在开发本国独特的 E-Cash 系统。而在美国也并非只有 Mondex 一种电子现金系统，也有其他公司开发的使用不同技术体系的电子现金在研发当中。日本政府也计划投入数以万亿日元的巨资对现有的金融网络进行改造，研究本国特色的 E-Cash 系统。

基于 E-Cash 的诱人前景，著名的 VISA 信用卡集团也开发和推行了一种新型电子现金系统——VISA-Cash，这是世界上使用较早、时间较长，比较成熟的电子现金系统，也在多家银行试验运行。

除 VISA-Cash 和 Mondex 两大电子钱包电子现金服务系统之外，其他著名公司，如 HP 的 VWALLET 和微软的 Microsoft WALLET，在 IE4 里选项中可以选择 6 种电子钱包系统，为世界各地的不同用户提供不同的 E-Cash 服务。此外，还有 IBM 的 IBM WALLET，EuroPay 的 Clip，德国银行业的 Geldkarte 和比利时的 Proton。其他很多软件厂商都在自己开发的软件系统中加入了电子钱包的功能。

其他诸如 CyberCash 公司和康柏等计算机公司及商业机构在 E-Cash 研究方面也都投入大量资金。日本东京 Ecosys 公司还开展了数字现金方式的电子通货实验；美国的 Microsoft 在其雄心勃勃的 NETMYSERVICE 服务中也整合了包含电子钱包、电子邮件、日程簿内容，借 Windows XP 推出挑战主流 E-Cash 的雄心计划一览无遗。

与国外相比，我国的电子现金研究和试验开展相对较晚，但我国政府对 E-Cash的研究工作非常重视，投入了相当数量的资金、人力进行 E-Cash 的

研究。国内的著名科研院所、大学等各科研机构跟踪国外的研究成果，也展开了大量的、更为深入的研究，取得了丰硕成果。同时，国内几乎所有的商业银行都已经行动起来，正在推出或即将推出一些初级 E-Cash 业务。与国外相比，我国的电子现金研究和试验开展相对较晚，但我国政府对电子现金的研究工作非常重视，投入了相当数量的资金和人力。1993 年，国务院启动了以发展我国电子货币为目的、以电子货币应用为重点的各类卡基应用系统工程——金卡工程，为我国电子商务的发展打下了基础。世界第三、欧洲最大的智能卡供应商 Bull 公司曾为深圳城市合作银行设计实施了一种基于智能卡（包括电子钱包及借贷功能）的付款系统，Bull 公司为此提供了数万张卡以及用于向卡中加入电子现金和进行付款的终端。

在北京，北京电信与中国银行北京分行合作推出了利用金融卡（长城卡）可进行电信消费的系统，虽不是严格意义的 E-Cash，但却向 E-Cash 技术迈出了重要的一步，是个良好的开端，这在我国尚属首次，前景广阔。而且，由英国最大的西敏寺银行和米德兰银行推出的电子现金系统——Mondex 的所有者汇丰银行已经获得了在中国经营 Mondex 卡的权力，E-Cash 在我国的推广应用正在飞速发展中。

尽管 E-Cash 的研究及应用前景广阔，然而 E-Cash 在技术及管理上目前都存在许多障碍。例如，E-Cash 对硬件和软件的技术要求高，如硬件基础设施必须具有极高的效率、稳定性和严密的安全措施，而目前各行业的运行环境远未能达到；如果系统升级，不仅耗资巨大而且工作量很大，将在一定程度上阻碍 E-Cash 的发展。其次，目前只有少数商家接受 E-Cash，少数几家银行提供 E-Cash 开户服务，离大范围的普及尚有距离；而且目前的 E-Cash 系统的使用风险较大，在安全保障技术、消费者利益保护方面仍不是非常完善，存在许多需要改进的地方。

尽管存在种种问题，E-Cash 的使用及发展仍增长迅猛。Jupiter 通信公司的一份分析报告称，1987 年，电子现金交易在全部电子交易中所占的比例为 6%，到 2000 年年底，这个比例将超过 40%，在 10 美元以下的电子交易中所占的比例将达到 60%。而实际的发展远远超过预期目标。因此，随着较为安全可行的 E-Cash 解决方案的出台，E-Cash 一定会如商家和银行界预言的那样，因其便利性而成为未来网上贸易主要的交易手段。相信随着技术的成熟，E-Cash 将促进电子商务的发展，也必将在经济活动中扮演越来

越重要的角色。

1.1.3 电子商务交易的个性化推荐系统发展

随着电子商务规模的不断扩大，商品个数和种类快速增长，用户需要花费大量的时间才能找到自己想买的商品。这种浏览大量无关信息和产品的过程无疑会使淹没在信息过载问题中的消费者不断流失，用户迫切需要一种能够根据自身特点组织和调整信息的服务模式，于是个性化服务应运而生。

个性化推荐系统是根据用户的兴趣特点和购买行为，向用户推荐用户感兴趣的信息和商品，是建立在海量数据挖掘基础上的一种高级商务智能平台，以帮助电子商务网站为其顾客购物提供完全个性化的决策支持和信息服务。个性化推荐系统能收集用户特征资料并根据用户特征，如兴趣偏好，为用户主动做出个性化的推荐。系统给出的推荐是可以实时更新的，即当系统中的商品库或用户特征库发生改变时，给出的推荐序列会自动改变。这就大大提高了电子商务活动的简便性和有效性，同时也提高了企业的服务水平。总体说来，一个成功的个性化推荐系统对将电子商务网站的浏览者转变为购买者、提高电子商务网站的交叉销售能力、提高客户对电子商务网站的忠诚度等方面具有重要作用。

个性化服务技术经过10多年的发展取得了很大成就，很多电子商务网站已经开始为用户提供个性化服务并取得了良好的收益，实现了一对一的营销（One-to-one Marketing）。研究表明，电子商务的销售行业使用个性化推荐系统后，销售额能提高2%~8%，尤其在书籍、电影、CD音像、日用百货等产品相对低廉且商品数目繁多的行业，推荐系统能大大提高企业的销售额。目前，几乎所有的大型电子商务系统，如Amazon、eBay等，都不同程度地使用了各种形式的推荐系统。各种提供个性化服务的Web站点也需要推荐系统的大力支持。在日趋激烈的竞争环境下，个性化推荐系统能有效地保留客户，提高电子商务系统的服务能力。成功的推荐系统会带来巨大的效益。

1995年3月，卡内基·梅隆大学的Robert Armstrong等人在美国人工智能协会上，提出了个性化导航系统Web Watcher；斯坦福大学的Marko Balabanovic等人在同一次会议上推出了个性化推荐系统LIRA。同年8月，麻省理工学院的Henry Lieberman在国际人工智能联合大会（IJCAI）上提出了个