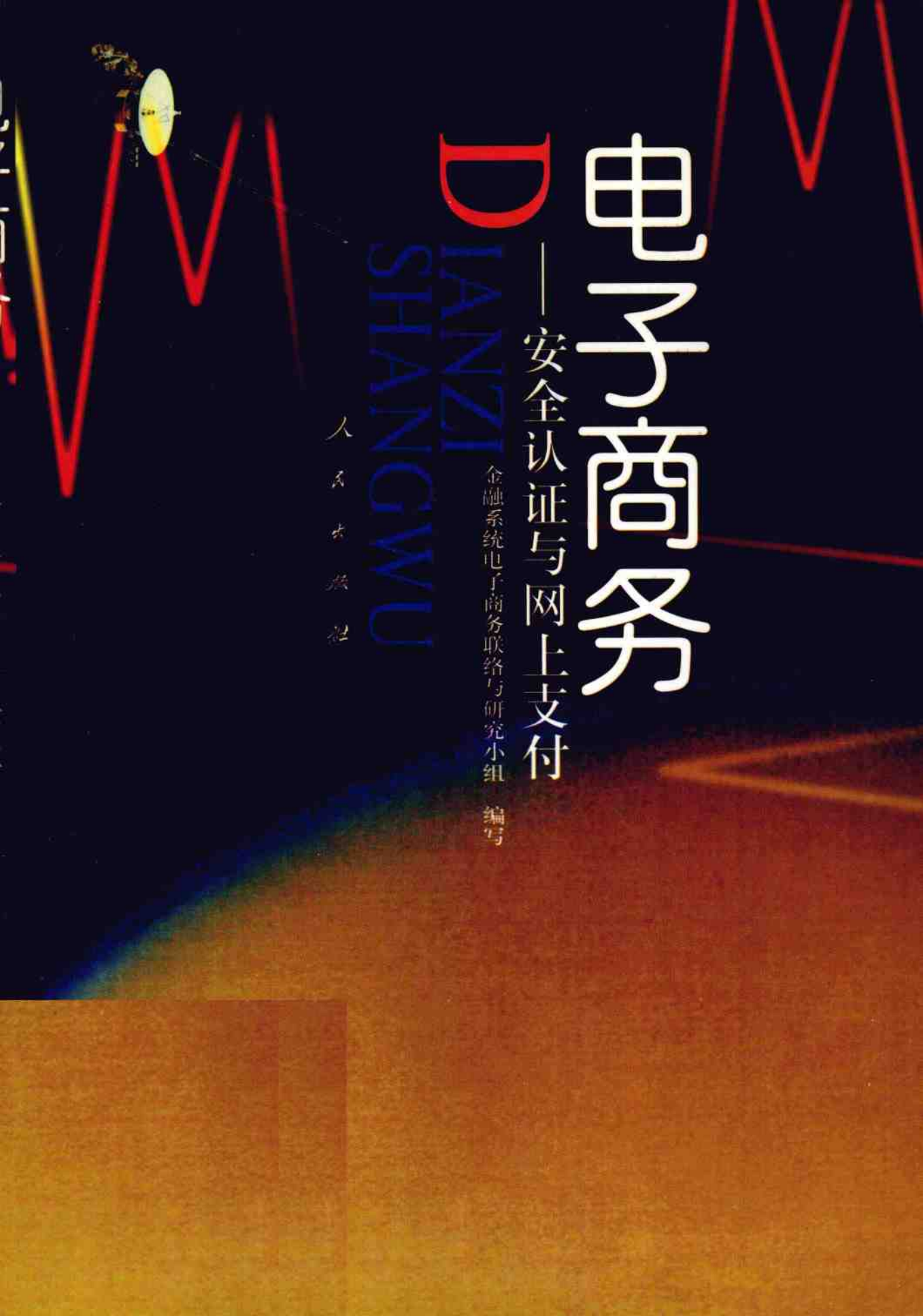

电子商务

——安全认证与网上支付

DIANZI SHANGWU

金融系统电子商务联络与研究小组 编写

人民出版社

电子商务

——安全认证与网上支付

DIANZI SHANGWU

金融系统电子商务联络与研究小组 编写

人民出版社

策划编辑:李春生
责任编辑:郑丽萍
装帧设计:曹　春
责任校对:李兰亭

图书在版编目(CIP)数据

电子商务——安全认证与网上支付/金融系统
电子商务联络与研究小组　编写.
-北京:人民出版社,2000.4
ISBN 7-01-003175-4

Ⅰ.电…
Ⅱ.金…
Ⅲ.①结算业务-计算机网络-安全技术
②计算机网络-计算机应用-商务-结算业务
Ⅳ.F830.49
中国版本图书馆 CIP 数据核字(2000)第 05324 号

电子商务——安全认证与网上支付
DIANZISHANGWU ANQUANRENZHENG YU WANGSHANGZHIFU

金融系统电子商务联络与研究小组　编写

人民出版社 出版发行
(100706　北京朝阳门内大街 166 号)

北京师范大学印刷厂印刷　新华书店经销

2000 年 4 月第 1 版　2000 年 4 月北京第 1 次印刷
开本:787 毫米×1092 毫米 1/16　印张:21.75
字数:331 千字　印数:1-3000 册

ISBN 7-01-003175-4/F·700　定价:60.00 元

编写委员会成员

陈　静　中国人民银行支付科技司司长
刘永春　中国人民银行支付科技司副司长
　　全国银行卡办公室主任
单怀光　中国工商银行技术保障部总经理
苗玉峰　中国农业银行科技部副总经理
陈　皓　中国银行科技部副总经理
武　青　中国建设银行科技部总经理
徐　捷　中国建设银行科技部副总经理
周禹相　中国交通银行电脑部总经理
王学良　中信实业银行电脑部副总经理
武　健　中国光大银行信用卡部总经理
贾振陆　华夏银行电脑部总经理
熊文森　招商银行电脑部总经理助理
梅　庆　广东发展银行北京分行电脑部副总经理
陈增圭　深圳发展银行电脑部总经理
刘大隆　全国银行卡信息交换总中心总经理
关振胜　金融认证中心技术总监

编写人员：李永清　徐文胜　叶　林　杨　倩　潘　松
　　马　雁　齐　煊　乔　东　史润生

序　言

中国人民银行副行长　高福林

近几年，电子商务在世界范围内得到了迅速的发展，政府部门对电子商务给予了高度重视和支持。在许多部门，电子商务已经成为战略上的需要。

电子商务对银行业产生了深远的影响，极大地推动了金融创新。商业银行在积极寻求变革，以在未来的网络环境中生存和发展，比如努力向客户提供网上银行服务、适应电子商务网上支付要求而建立网上支付系统等。

网上支付是电子商务的重要组成部分，是传统支付系统的发展和创新。不兼容的网上支付系统无疑会阻碍电子商务的健康发展，因此，支付方式的变革依赖于中央银行的支持。中央银行应对网上支付问题进行研究，规范网上支付系统的发展，积极防范、化解与网上支付相关的金融风险。除此之外，中央银行还应着手对金融行业的安全认证体系进行规划、监督和管理，研究与解决电子商务带来的与金融相关的立法问题。

我们国家对电子商务的发展十分重视。江泽民主席指示不仅要重视私营、工商部门的推动作用，同时也应加强政府部门对发展电子商务的宏观规划和指导，为电子商务的发展提供良好的法律法规环境。江泽民主席同时还要求各级领导干部认真学习和掌握有关知识，以适应社会主义建设新形势的需要。

自1998年初以来，人民银行就积极开展有关的工作。1998年6月，人民银行参加了由北京市政府牵头的“首都电子商务工程”建设，并承担了建设金融认证中心和支付网关的重任。

为了探讨金融CA工程的组织形式，全面规划支付网关建设，并对网上银行、电子商务相关立法问题进行研究，1998年10月，人民银行支付科技司组织工商银行、农业银行、中国银行、建设银行、招商银行科技（电脑）部共同成立了“金融系统电子商务联络与研究小组”。一年来，该联络小组开展了积极有效的工

作,《电子商务——安全认证与网上支付》一书就是他们辛勤工作的成果之一。

《电子商务——安全认证与网上支付》这本书站在银行的角度,对电子商务安全认证、网上支付系统以及网上银行的发展作了系统的、较为全面的介绍。对于在银行科技、信用卡、支付结算等部门工作的同志来说,本书可以作为电子商务培训教材和不可多得的重要参考。

在中国电子商务刚刚起步的今天,本书的出版无疑是十分及时和十分有益的。

1999 年 9 月 21 日

目　录

序　言 …… 中国人民银行副行长　尚福林(1)

第一篇　电子商务

第一章　电子商务概述 …… (3)
第一节　电子商务基本概念 …… (3)
第二节　电子环境中的风险 …… (4)
第三节　纸基商务与电子商务 …… (6)
第四节　电子商务支撑环境 …… (7)
第二章　电子商务与银行业 …… (11)
第一节　概述 …… (11)
第二节　银行业发展环境的演变 …… (13)
第三节　家庭银行的历史 …… (16)
第四节　家庭银行的实现方式 …… (19)
第五节　开放模式与封闭模式 …… (31)
第六节　在线银行业的管理问题 …… (32)
第七节　总结 …… (41)
第三章　电子商务在中国的发展 …… (42)
第一节　概述 …… (42)
第二节　我国信息技术的发展 …… (43)
第三节　首都电子商务工程 …… (51)
第四节　金融认证中心 …… (53)

木雕 …… 162
最普及的泥塑和石雕 …… 165
酥油花及其他雕塑 …… 171
雪域雕塑的艺术风采 …… 174

世人惊叹的工艺
金属工艺 …… 179
非金属工艺 …… 188
纺织染色工艺 …… 192

雄浑多姿的建筑艺术
政教合一的宫殿 …… 198
王宫的建筑艺术 …… 202
佛殿·寺院风格 …… 205
碉楼·官寨·民宅 …… 217
桥梁 …… 221

花团锦簇的文学原野
格言诗 …… 228
仓央嘉措情歌 …… 230
道歌 …… 231
长篇小说 …… 232
史诗《格萨尔》 …… 239
叙事长诗 …… 245

第一节　SET 信任模式 …… (158)
第二节　用户注册 …… (160)
第八章　认证相关规定与立法 …… (165)
第一节　与 PKI 相关的立法 …… (165)
第二节　认证机构责任的保证和限制 …… (171)
第三节　CPS 条款:限制和条件 …… (173)
第四节　互联网服务提供商(ISP)协议 …… (175)

第三篇　电子商务网上支付

第九章　网上支付系统 …… (185)
第一节　概述 …… (185)
第二节　电子支付技术回顾 …… (186)
第三节　银行卡 …… (187)
第四节　电子现金 …… (188)
第五节　电子支票 …… (190)
第十章　银行卡支付 …… (191)
第一节　概述 …… (191)
第二节　邮寄定单/电话定单(MOTO)交易 …… (191)
第三节　非安全的网络支付 …… (192)
第四节　第一虚拟(FV)系统 …… (192)
第五节　CyberCash …… (195)
第六节　安全电子交易(SET)协议 …… (199)
第十一章　电子支票 …… (217)
第一节　概述 …… (217)
第二节　FSTC 电子支票概念 …… (217)
第三节　Netbill …… (224)
第四节　NetCheque …… (230)
第十二章　电子现金 …… (233)
第一节　概述 …… (233)

第二节　Ecash …… (233)
第三节　NetCash …… (242)
第四节　CyberCoin …… (253)
第五节　Mondex …… (255)
第六节　EMV 现金卡 …… (256)
第十三章　微型支付系统 …… (258)
第一节　概述 …… (258)
第二节　Milicent …… (259)
第三节　PayWord …… (271)
第四节　MicroMint …… (279)
第十四章　电子支付系统的立法问题 …… (287)
第一节　数字签名的法律效力 …… (287)
第二节　电子支付系统的立法问题 …… (288)
附录 A　信息安全技术 …… (292)
第一节　信息安全基础 …… (292)
第二节　密码技术介绍 …… (297)
第三节　数字签名 …… (304)
第四节　密钥管理 …… (309)
第五节　确认 …… (316)
第六节　系统信任 …… (324)
附录 B　Entrust 白皮书——认证策略与认证实务声明 …… (325)
第一节　背景 …… (325)
第二节　概述 …… (325)
第三节　结构与组成 …… (326)
第四节　开发及应用 …… (329)
第五节　总结 …… (330)
附录 C　电子商务政策和立法问题 …… (331)
第一节　契约和法律安排 …… (331)
第二节　电子商务的立法框架 …… (333)

第一篇

电子商务

第一章　电子商务概述

第一节　电子商务基本概念

电子商务起源于计算机电子数据处理(EDP)技术,它代表了计算机应用从科学计算到文字处理和商务统计报表处理的转变。随后出现了电子数据交换(EDI)的开发与应用,并随着网络技术的发展,通过专用的增值通讯网络来传送。银行间电子资金转账技术和企业间 EDI 技术相结合,便产生了早期的电子商务。

电子商务是一个意义十分广泛的术语,它描述了自动化的商业交易。电子商务代表了广泛的技术、处理和实务,它通过大量的无纸化机制使交易自动化。通常,它包含经由 E - mail、电子数据交换(EDI)或万维网(WWW)的信息交换。电子商务包括私营和公共部门内部及其之间的交易,也包括各种国内和国际交易。

电子商务对现代社会和经济的发展是十分重要的,因而这一领域的大规模发展是不可避免的。在私营部门和公共部门的业务中,电子商务已经成为战略上的需要。人们认为,这种交易方式能够有效地削减成本、增强竞争力,并能适应对速度、精确性和商业情报的要求。对我们这个正在发展的社会来说,电子商务将成为一个重要的标志。它是为迈入 21 世纪而进行商业重组的工具,也是商业重组的结果。

在我们这个经济和社会发展的重要时期,电子商务也是各种分散技术综合的标志。电子商务利用了个人电脑、数据通讯网络、先进的计算机应用、全球化的政治和经济环境的广泛性和整体性,旨在不断地、大幅度地削减成本。简而言之,电子商务不仅变得低成本和应用方便,并且还为社会所广泛接受,人们也会越来越多地应用它。

然而,据我们所知,对于电子商务概念到目前为止并没有形成明确的定义。

下面引用几个有关的论述：

1. 经济合作与发展组织(1997)

电子商务一般指与商业活动(包括组织和个人)有关的、基于数字化的数据(包括文字、声音和视觉图像)处理和传输的各种形式的交易。

2. 欧盟(1997)

电子商务是以电子的方式经商。它基于包括文字、声音和图象在内的数据的电子处理和传输。它包括很多不同的活动：物品和服务的电子交易、在线数字内容的传递、电子资金转账、电子股票交易、电子提单、商业拍卖、合作设计与操作、在线资源化、公共采购、直接消费者推销以及售后服务等。它包含产品(消费者物品、特殊医疗设备等)和服务(信息服务、金融和法律服务)、传统活动(健康咨询、教育)和新型活动(虚拟购物中心)。

3. 日本国际贸易和产业部(1996)

电子商务应用当前仍局限于一些固定的公司，但现在正步入一个新的时代，很多不固定的人们，包括普通消费者都参与到网络中来。另外，其内容不仅仅是有关发送定单和接受定单的数据的简单交易，而且也包含一般的商业行为，例如宣传、广告、协商、合同和资金转账。

4. IBM

电子商务是指利用互联网提供的通讯手段和传统信息技术的丰富资源在网上进行的商务活动。当企业利用网络，把与企业命运息息相关的关键业务系统和顾客、供应商、销售商的协同工作以及其商贸环节联为一体，直接在网上完成从进货到销售的完整商业行为，才是真正实现了电子商务。

5. "大西洋两岸商业对话"电子商务白皮书(1997)

电子商务，简单地定义，就是以电子形式进行的有关服务的商业交易。

6. 欧洲信息技术观察台(1997)

电子商务是指借助通讯网络完成的商业活动，并由此产生价值交换。

第二节　电子环境中的风险

在降低商业成本、改善客户服务、为新的客户服务创造机会等方面，电子商

务都是非常有用的。然而，也存在着一种潜在的负面影响。支持电子商务的电子系统和基础设施很容易以多种方式被误用、滥用或失效。这将可能对电子商务的参与者造成巨大的损失，包括商业交易方、金融机构、服务提供商以及客户等。

从商业的角度来看，这些误用、滥用或失效的后果包括：

1. 由欺诈而造成的直接经济损失

例如，某人（内部欺诈人员或外部攻击者）可能错误地将资金从一个账户转移到另一个账户，或损坏财务记录。

2. 窃取有用的机密信息

许多组织都存储和交换各种信息，这些信息的机密性对其是生死攸关的。这包括专有的技术和营销信息，以及为其客户保存的机密信息。外部攻击者的侵入可能会将这些机密泄露给非授权方，从而对有关各方造成重大的损失。

3. 由于服务中断而丧失商业机会

由于蓄意攻击（来自内部不满者或怀有恶意的外部人员）或意外事故，电子服务可能中断很长时间，或中断的时间让人不能接受，从而丧失许多商业机会。这种损失将是灾难性的。

4. 资源的非授权使用

外部攻击者可以获取对资源的非授权访问，并为其自身的目的而使用这些资源。通常来说，电脑黑客会利用某个被攻破的计算机系统作为攻击其他系统或网络的升级点。

5. 丧失客户信任

给客户带来的不便，或者由侵入、失败及其历史而产生的负面影响等，可能会对业务造成重大的损失。由于假扮内部人员的入侵者的违法行为或可疑行为，可能会对企业的形象造成损害。

6. 由不确定性引起的损失

外来入侵、不诚实、不当操作、人为错误或电子系统失效等会打断正常的交易秩序，这将不可避免地使交易在一定时期内处于瘫痪状态。例如，可能没有收到对交易的确认，或交易被其他方所中断。商业损失、可信度和商誉的损失及纠纷解决成本都可能是巨大的。

尽管可能存在保护消费者的各种法律和规定，公众还是很脆弱的，他们的权益很容易受到损害。例如，消费者将钱托付给电子系统，而当该电子系统受到攻击或失效时，他们就会遭受损失。以上所列的所有这些风险最终都会以直接损失、由商业传递的隐形损失、不便利因素等方式来损害消费者的合法权益。

对计算机网络和电子商务服务的攻击及其失效已有大量成文的报告。这里不再具体举例。

要减少电子商务中的内在风险，只有使用合法的安全措施，并建立必要的商业和法律框架。从技术的角度来说，这并没有什么大的问题。信息安全领域多年来一直是政府、高校和一些专家的研究课题，而对其中的多数技术问题，技术专家们也已给出了解决方案。然而，直到最近，除了在国防和银行业的应用之外，这些信息安全解决方案在其他方面很少应用。因此，我们仍需进一步了解，如何把信息安全技术广泛地应用于商业环境中。此外，在运用技术安全措施的同时，还要注意有关的法律和商务惯例等。

第三节　纸基商务与电子商务

20世纪80年代中后期，与计算机有关的信息的特征已经成为人们重新思考的课题，这使人们对其有了更多的认识。例如，为了在纸基数据和电子数据之间建立准确的法律和商务对等性，人们花费了很多精力。但是，大多数努力都失败了。

以纸为基础的技术和以计算机为基础的技术之间存在着基本的、实际的和法律上的差异，这一点是很明显的。经过签名的纸基文件具有其内在的安全特征，而以计算机为基础的记录缺乏这些特征。这些特征包括嵌入纸纤维中的墨水的半持久性、任何特定打印处理的惟一性(例如抬头)、水印和签名的生物学特性(例如压力、形状和运笔方向等特征都是签名者所惟一具有的)、时间印鉴，以及修改、行间书写和删除的可检测性。

基于计算机的信息和记录本质上并不具有这些安全特征。计算机存储的信息仅仅是二进制数字串(0和1)，它们以编码的形式来表示信息，如单词和数字。如果不使用外部的、尤其是所构建的安全机制，这些记录可以被任意地修改而不

被发觉。也就是说，我们必须使用一些附加的控制机制(包括物理的和电子的保护)，使得计算机所存储的信息至少能与纸上信息具有同样的可信度。

另外，基于纸的文件和基于计算机的文件在商业和法律上可能并不具有等价或完全类似的功能。可转让的所有权文件表明了这两种介质之间的差别，因为这种文件需要具有原始性和惟一性。纸基所有权文件的转让在法律上可用作该文件所代表的物品和财产的转让。该文件的接收方相信，这种转让在法律上是被认可的，部分原因是由于这个原始的、惟一的“纸”文件可用作转让的证据。

相反，基于计算机的记录本质上不具有惟一性。事实上，数字数据的一个优点就在于，人们可以制造出任意数目的相同拷贝，而且每一拷贝与原件都是不可区分的。不幸的是，这一特点使得这些记录不能像纸基文件那样提供有力的法律证据。因此，纸基文件和基于计算机的记录之间的这种内在差异要求使用不同的方法和程序来取得可转让性和其他等价的法律功能。

在现实中，电子商务与纸基交易之间很少具有直接的一一对应的法律类比。但是，在考虑数字媒介的独特性质时，有必要去发现相关的一些功能对应。

第四节　电子商务支撑环境

电子商务与传统纸基交易之间存在着本质的不同。电子商务面临的是一种全新的电子环境，交易方式和支付方式都发生了根本性的变化。因此，电子商务的健康发展需要具有良好的支撑环境。

一、要建立健全的法律框架

电子商务涉及到许多方面的立法或法律修正问题，其中主要是涉及电子环境的立法，比如有关信息安全的立法、有关在线交易的立法、电子信息中的权利、在线信息内容的规范化、在线产品的规范化等。如果没有健全的法律保障，电子商务就没有得以健康发展的基础。所以，要发展电子商务，首先要及时地培育法律上的配套支撑环境。

实际上，金融电子化的发展已经给银行界提出了不少难题。比如在支付系统中，票据截留后电子形式票据的有效性、数字签章的合法性等。在电子商务