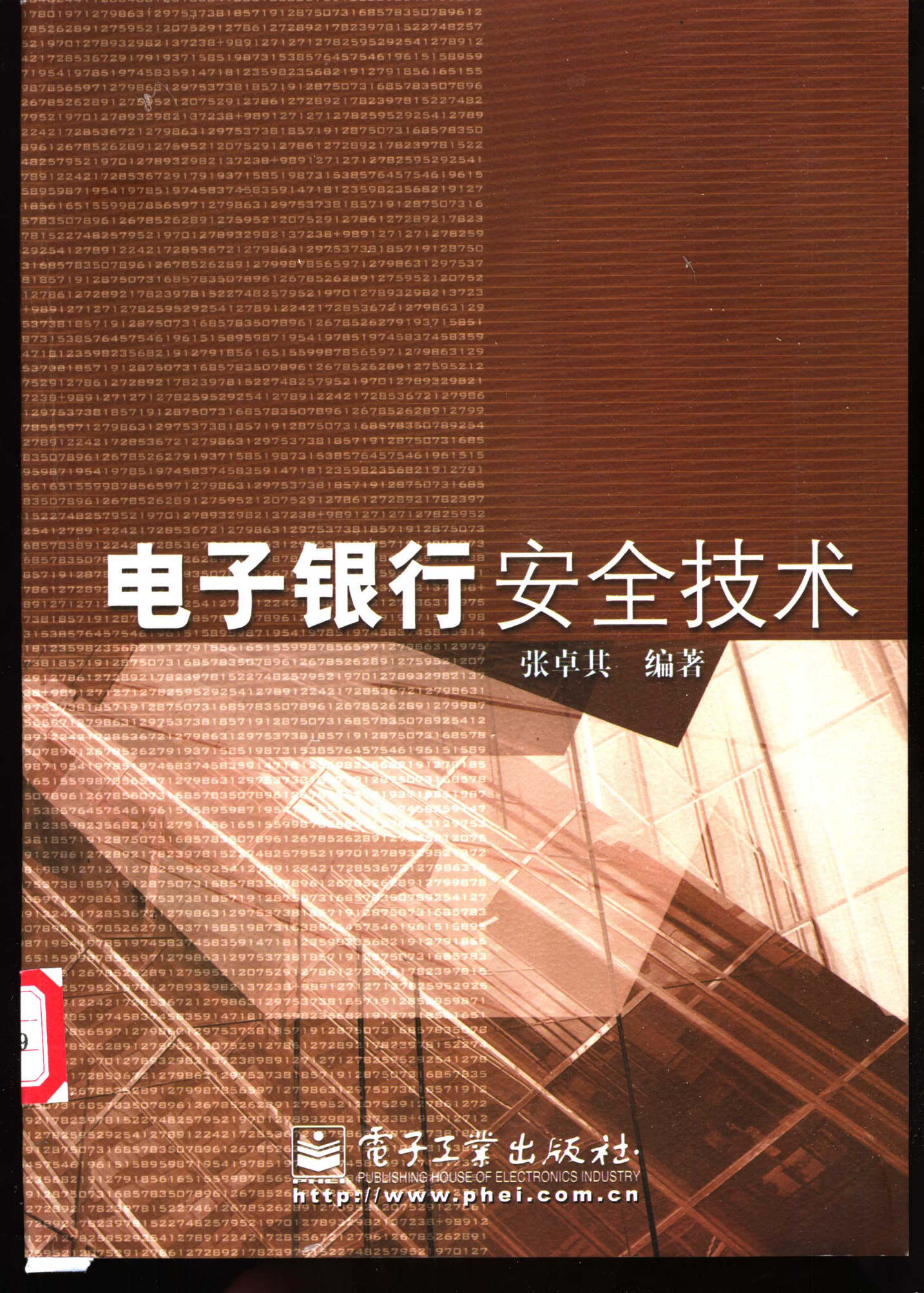
# 电子银行安全技术

张卓其 编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

# 电子银行安全技术

张卓其　编著

電子工業出版社
Publishing House of Electronics Industry

## 内容简介

本书系统介绍电子银行安全的基本原理及其核心技术。重点介绍:电子银行的网络体系结构、运行环境和安全需求;电子银行系统中存在的不安全因素、预防策略和评价准则;电子银行系统的备援配置以及所采用的容错机制和冗余技术;电子银行系统的安全管理、经营风险管理、金融预警系统和安全设计等。

本书可作为大专院校相关专业的教材或教学参考用书。对于从事金融电子化和计算机应用软件开发的科技人员、银行信息管理人员、银行计算中心运行维护人员以及计算机爱好者,也是一本有价值的参考书。



**图书在版编目(CIP)数据**

电子银行安全技术/张卓其编著. —北京:电子工业出版社,2003.1
ISBN 7-5053-8282-9

Ⅰ.电… Ⅱ.张… Ⅲ.计算机应用—银行业务—安全技术 Ⅳ.F830.49

中国版本图书馆 CIP 数据核字(2002)第 094920 号

责任编辑:王沈平　　特约编辑:李盛沐　陈碧凤
印 刷 者:北京兴华印刷厂
出版发行:电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销:各地新华书店
开　　本:787×1 092　1/16　印张:21.25　字数:525 千字
版　　次:2003 年 1 月第 1 版　2003 年 1 月第 1 次印刷
印　　数:4 000 册　　定价:29.00 元

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。
联系电话:(010)68279077

# 前　言

银行电子化建设经过近半个世纪的发展，实现了三次飞跃。第一次飞跃是将计算机与通信(C&C)技术融入银行业务，使银行业务的手工操作实现了电子化，并推出了自助银行服务。第二次飞跃是将信息技术(IT)融入银行业务，使银行业务在提供支付服务的基础上，还能为客户提供金融信息增值服务，从而使传统银行发展成为了电子银行。第三次飞跃是将万维网(Web)技术融入银行业务，使实体银行向着虚拟银行发展。

电子银行的建立和发展，使银行真正体现了以客户为中心，为客户提供更多、更好的银行服务产品，把银行建设成为高效、安全、低成本、多功能、全天候的现代化综合金融体系的发展目标。现在，电子银行系统已经成为了银行赖以生存和发展的基础。电子银行强化了银行的信用中介作用，成为整个社会商品生产、流通和消费体系的命脉和支柱。银行电子化有力地推动着国民经济信息化的发展，推动着全球经济一体化和全球金融一体化的发展进程。

C&C、IT 和 Web 技术的引入，使银行与往来银行、企事业单位、商业部门、政府管理部门以至每个家庭都建立了紧密的联系，使银行的服务深入到了社会的各个角落。电子银行的建立和发展，除了给客户带来方便、给银行和国民经济带来巨大的发展机遇之外，也给他们带来了许多新的技术风险，同时还加剧了金融业内部以及金融业与非金融业之间的竞争，从而加大了银行的经营风险。这些风险与传统金融业务中的信用风险、市场风险、环境风险、行为风险一样，都属于必须防范和化解的金融风险。随着经济全球化和全球金融一体化的迅速发展，中国在加入世界贸易组织后，国内金融业将逐步全面对外开放，将经受国外金融业的严峻挑战。如果电子银行的安全管理体系不完善，在电子银行系统的设计、集成和操作运营管理中疏于风险防范的话，其负面效应所形成的破坏力是难以估量的。当一个银行、一个金融企业连上互联网，面对无限的信息和商机的时候，也将自己暴露于竞争对手和蓄意破坏者的视线之内。电子银行体系中的任何缺陷和不安全因素，都可能使银行面临巨大的风险，以致给银行和整个国民经济带来巨大的损失与灾难。一个重要的电子银行系统一旦崩溃，还可能使整个国家以至全球的支付体系陷于瘫痪。

除了计算机犯罪、黑客和计算机病毒攻击层出不穷外，各种“电子战”、“信息战”的呼声鹊起，日益成为国与国、企业与企业之间重要的攻击和防卫手段。未来的战争，可能是先进行信息战，以破坏敌国的金融、经济和军事指挥信息系统，使敌国整个国家的国民经济、人们的日常生活和网络通信陷入瘫痪，从而可轻易地赢得战争。因此，强化和保障中国金融信息网络安全，迎接国外同业的竞争和国内外犯罪分子的挑战，是关系国家安全的大事，是我国金融业面临的紧迫任务。

在面临信息犯罪、信息战威胁的严峻形势下，金融电子化建设应从国家安全的高度出发，以保守国家金融信息秘密、严防高科技犯罪、确保银行金融资产安全、维护客户利益和隐私为基本目标，使核心安全设备实现国产化。因此，自主开发网络安全监控和预警系统，成功地构造基于 PDR 模型的集保护、监测、反应为一体的动态自适应的金融安全体系，是我国

金融业当前面临的重大使命。

鉴于以上情况，我国的金融界在加快金融电子化建设的同时，要十分重视金融信息安全体系的建设，高度重视信息安全组织的建设和信息安全人员的培养，高度重视在职职工的信息安全培训，以适应电子银行环境下的安全要求。因此，相关各界人士迫切需要具有较全面、系统地介绍电子银行安全技术方面的书籍，本人愿在这方面尽自己的微薄之力。

本书内容力求较系统地介绍电子银行安全的基本原理及所采用的主要技术。全书内容共分9章。第1章和第2章是本书的出发点和纲，主要介绍电子银行的运行环境和安全需求，包括电子银行的发展、电子银行体系和网络结构，并从电子银行的安全特点和安全需求出发，总结了电子银行的不安全因素及其预防策略，信息系统的安全理论和评价准则。第3章介绍电子银行软件和硬件系统的备援配置，重点介绍电子银行普遍采用的容错机制和冗余技术。第4章和第5章介绍电子银行信息安全的基础理论和核心技术，包括密码技术以及采用密码技术的安全密码系统和协议技术。安全密码系统主要介绍数据加密标准算法(DES)和RSA算法，协议技术主要介绍数字签名、电文识别码(MAC)及电文识别技术、密码分配协议、身份识别协议等。第6章介绍数据库数据安全保护技术，包括数据库的安全性、数据的完整性、并发控制和数据库数据的恢复。第7章至第9章是本书内容的重点，主要介绍银行专用网络、基于IP网络的网上银行的通信安全体系和主要的通信安全技术，电子银行的网络安全管理、经营风险管理、金融预警系统和安全设计等问题。

本书在多年从事电子银行、电子银行安全学等课程教学的基础上写成，除了重点介绍电子银行安全的基本知识、基本原理和基本技术外，也力求反映信息安全领域的新进展和新技术。

本书可作为大专院校相关专业的教材和教学参考书。对于从事金融信息安全工作的科技人员、银行的安全稽核人员、从事金融电子化及计算机应用软件开发的科技人员、银行信息主管、银行计算中心的运行管理人员，希望本书也是一本有益的参考书。

电子银行及其安全领域技术的发展，建立在C&C、IT、Web等科学技术，现代金融理论和现代管理理论基础之上，所涉及的学科非常广泛，而这些学科的发展又非常快，限于本人的水平和能力，书中的错误和缺点在所难免，恳请读者批评指正。

张卓其

2001年6月于北京

# 目　录

# 第1章　电子银行的发展概况

银行是经营货币的机构，是社会商品生产、流通和消费体系的命脉和支柱。银行信息化是国民经济信息化的基础。因此，世界各国都特别重视银行的电子化和信息化建设。

银行电子化使银行同往来银行、企事业单位、商业单位、政府管理部门以至每个家庭，都建立了紧密的有机联系，使银行的支付服务和信息增值服务深入到社会的各个角落。电子银行系统已经成为银行赖以生存和发展的基础，成为国民经济的大动脉。银行的电子化和信息化，不仅使银行本身发生了革命性的变革，还大大促进了国民经济信息化、全球金融一体化和全球经济一体化的进程。

如何通过银行电子化和信息化建设，体现以客户为中心，为客户提供更多更好的银行服务产品，把银行建设成为高效、安全、低成本、多功能、现代化的综合金融体系，为国民经济的发展和信息化建设发挥更大的作用，是银行界面临的重大课题。

## 1.1　电子银行的产生背景

半个多世纪以来，计算机和通信技术(C&C)被引入银行，使银行传统业务的处理开始实现电子化，银行从此开始了革命性的变革。接着，银行为充分发挥电子化处理的效率，开发出了大量新型的自助银行服务项目。在实现支付服务电子化的基础上，信息技术(IT)也融入到了银行业务之中。银行从交易数据中提取有用成分，开始向客户提供金融信息增值服务，强化了银行的经营管理，完善了银行的电子监控体系，银行因此从传统银行时代进入了电子银行(E-banking)时代。从20世纪90年代开始，因特网(Internet)的发展，电子商务的兴起，全球经济从传统经济向数字经济过渡，为电子银行的进一步发展开辟了又一个广阔的发展空间。电子银行与万维网(Web)技术的结合，推出了网上银行(Internet banking)服务，并开始从实体银行向虚拟银行发展。

### 1.1.1　金融交易中的支付和支付系统

传统银行同其环境的关系，表现在各种金融交易过程中，也体现在银行为其客户提供的各种与金融交易有关的支付服务产品上。

#### 1. 支付和支付系统

金融交易，是指在商品交易、证券交易和货币交易中产生的各种支付活动。所有这些金融交易，都在不断地更新着金融机构的各种用户文件和管理文件。

任何买卖活动都伴随着资金的往来。交易双方的资金往来，称为支付。在自然经济和手工业经济为主的社会里，只有少量的商品交换，主要是以物易物，用实物作为货币。在商品经济社会里，纸币和票据代替了实物货币。这样做的结果，一方面加速了货币的流通速度，大大促进了商品生产的发展；另一方面，由于出现了现金交易之外的票据交易，使得商品

交易双方的收付款活动变得复杂了。银行的“信用”中介作用使商品交易双方的收付活动，扩展为交易双方开户银行之间的资金收付活动；而银行之间的资金收付交易，又必须经过政府授权的中央银行进行资金清算，才能最终完成商品交易双方的资金往来。

如图 1-1 所示，如果客户甲和客户乙在不同的商业银行开户，客户甲向客户乙购买商品，用支票支付。那么，由于甲乙双方进行的商品交易而引发出的支付全过程，将在两个层次上进行。低层面向客户，即银行与客户（包括商业银行甲与其客户甲，商业银行乙与其客户乙）之间的支付与结算。高层面向往来银行，即中央银行与各商业银行之间的支付与清算。在如图 1-1 所示的支付系统里，整个支付过程始于从客户乙，经商业银行乙和中央银行，到商业银行甲的支票流。然后，商业银行甲将客户甲的资金经反向拨付到客户乙在商业银行乙的户头上，从而才最后完成该笔商品交易的资金支付。在上述的资金流动过程中，往来银行之间的资金流动，必须经过中央银行的资金清算才能实现。

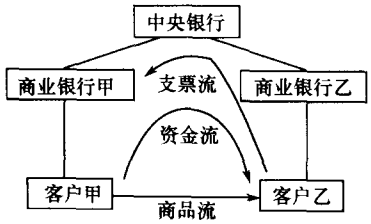



图 1-1　商品交易的支付过程

整个支付过程将各个经济交往的双方和银行维系在一起，组成了一个复杂的整体，这就是支付系统。

在上述两个层次的支付活动中，银行与客户之间的支付与结算是银行向客户提供的一种金融服务，是支付系统的基础。中央银行与商业银行之间的支付与结算，使商品交易中的支付活动得以最终完成。

商品交易时支付过程的复杂程度，随商品交易双方开户银行之间的关系不同而异。若图 1-1 中所示的商业银行甲和商业银行乙是同一个银行，或是同一银行下属的两个分行，则情况最简单，该银行自己就能完成商品交易的全部支付过程。若商业银行甲和商业银行乙是本地的两个不同银行，则需通过中央银行的同城资金清算，才能完成商品交易的支付过程。若商业银行甲和商业银行乙是异地的两个银行，则需通过中央银行的异地资金清算才能完成商品交易的支付过程。若商业银行甲和商业银行乙是隶属不同国家的银行，则属于国际性支付，需经过同业的多重转手才能完成商品交易的支付过程。

### 2. 电子支付系统的建立和发展

自从出现纸币和票据以来，伴随着商品交易的上述两个层次的资金支付活动就一直存在着。当时，资金支付活动中的各方通过各种票据的流动相互维系在一起，完成商品交易时的资金往来。纸质票据的流通速度慢，处理工作量大，影响了商品交易的发展。通过纸质票据流通而维系在一起的资金支付活动的各方，无法形成有机的整体。因此，严格地说，这时还没有形成现代意义的支付系统。

在商品经济高度发展的市场经济社会里，纸币和票据的流通速度已不能满足急速发展

的商品生产和流通的要求，这就促使银行研制开发新的支付工具和新的处理方法。银行卡的出现，各种电子资金转账(EFT)系统的建立和推广应用，促使货币从纸币发展为电子货币。电子货币的出现和推广应用，促使货币实现了又一次革命性的转变，从而对商品生产和商品交易的高速发展产生了深远的影响。

银行卡的推出，计算机和通信技术的引入，电子资金转账系统的建立和推广应用，使涉及资金支付活动的各方能真正有机地联系在一起，形成各种电子支付系统。在电子支付系统中，存在频繁流动着的两种方向相反的信号流：资金流和与之相关的信息(支付指令)流。在这里，传统的票据流被支付指令信息流所代替，即在电子支付系统中，支付指令信息流和资金流都是电子流。这样，不管支付系统多复杂，一笔支付活动瞬间就可完成，大大加快了资金的流通速度。

早期建立的电子资金转账系统，是银行同其客户进行数据通信的一种电子系统，用于传输同金融交易有关的信息，主要包括电子资金和相关的数据，为客户提供支付服务。

通过电子资金转账系统，银行可把支付服务从银行的柜台延伸到零售商店、超级市场、企事业单位以至家庭，总之可延伸到社会的各个角落。现代的电子支付系统是一个庞大、多功能和全天候的金融综合业务处理系统，是金融业参与竞争和赖以生存的基础。

由于电子支付系统在国民经济中所起的重要作用，因此可认为它是国民经济大动脉中的一个核心系统，在商品生产、流通和消费过程的社会经济活动中起着枢纽作用，维系着整个社会的经济活动。

进入20世纪80年代后，特别是电子商务的兴起，由于经济和金融的国际化发展，使电子支付系统进一步发展成为全球性的支付系统和全球性的金融信息系统，有力地促进了全球经济一体化和全球金融一体化的快速发展。

### 1.1.2 电子银行的产生和发展

银行的电子化建设始于20世纪50年代。经过20多年的发展，到20世纪80年代后期银行才开始逐步进入电子银行时代。

近半个世纪以来，商品生产的规模和交换方式都发生了很大的变化。科学技术的发展，促进了劳动生产率的迅速提高。此外，全国性和国际性贸易的急速发展，无论是从规模还是从速度上来看，都使商品流动量和货币流动量急速加大。除了与商品流动有关的货币流动外，在现代银行业务中，还有大量与实物商品流通没有直接联系的货币流动，如存取款、贷款、证券交易、货币交易等产生的货币流动。其中，仅储蓄和信贷就可使货币流动的强度增大10倍。

如此急剧增长的货币流动强度使银行界陷入困境，整个银行界日益为堆积如山的金融纸票(现金、支票和各种凭证)所困扰。有远见的银行战略家清醒地认识到，单靠增加人力不能解决银行困境，根本的出路在于采用新技术，引入新发明的计算机和通信技术来改造传统的银行业。计算机和通信技术的引入，开始了银行电子化的发展进程。用计算机来处理银行业务，可在网络上以电子的速度传输数据，从而使银行界结束了手工处理票据业务的历史，开始了革命性变革进程。这个变革过程现在仍然没有完成，而是正在向变革的深度和广度发展。

在银行电子化初期，不少电子资金转账系统是由大银行自行开发和使用的专有系统，而中小银行由于受资金和人才的限制，则采用联合开发共享电子资金转账系统的方法。随着

银行业务的不断扩大，工业化国家的许多电子资金转账网络，逐步互联成了各种地区性、全国性以至全球性的庞大的金融共享网。

20世纪80年代中期以前，电子资金转账系统基本上是面向单个银行产品进行开发和推广应用的。电子资金转账系统之间相互独立，各电子资金转账系统在进行资金转账过程中，都要进行账务处理工作。为了能为客户提供更好的服务，从20世纪80年代中期开始，发达国家的银行将各种电子资金转账系统进行了集成，使各种电子资金转账系统共用一个账务系统，促使各种电子资金转账系统能进行联动处理，银行因而能为客户提供综合业务服务，大大方便了客户。此外，银行从统一的账务处理系统中能掌握客户全部的业务活动，从而为银行提供信息增值服务打下了重要的基础。

随着银行电子化的深入发展，建立金融综合业务处理系统后的银行，采用信息技术，从各种金融交易数据中提取有用的信息，向各类客户提供金融信息增值服务，并建立以客户为中心的管理体系和科学的金融监控体系。这样，银行的业务处理不仅实现了电子化，银行还能对客户提供金融信息增值服务，并使银行的经营管理和安全监控实现了数字化和现代化。电子资金转账系统因此发展成了电子银行系统，银行也从手工操作的传统银行逐步发展成了高度自动化和现代化的电子银行。

电子银行是数字化和信息化了的高效率、低运行成本的银行。在电子银行里运行着各种电子银行系统，它通过电子传输的办法，向其客户提供全方位、全天候、高品质又安全的银行服务。因此，电子银行从根本上改变了传统银行的业务模式、管理模式和管理体制，建立了以信息为基础的自动化业务处理和以客户关系管理(CRM)为核心的科学管理新模式。电子银行采用电子货币支付方式，取代传统的现金交易和手工凭证传递与交换，大大加快了资金的周转速度。以银行为主的金融业从单一的信用中介部门，发展成为一个全开放和多功能的现代化金融体系。可以说，现代的金融业，是集金融交易服务和金融信息增值服务为一体的金融“超级市场”。银行的业务重点，从单纯的存贷款和资金调拨，转向既提供金融交易服务又提供金融信息增值服务。银行的收入结构，也将因此发生根本性的改变，即银行以传统的存贷款利息差为主要收益来源，将代之由提供金融劳务服务和金融信息服务所得的收入为主要收益来源。

传统银行与环境之间的关系，仅体现在金融交易方面，因此，传统银行只能起到信用中介作用。在电子银行时代，银行同环境之间的关系，表现在进行金融交易和进行金融信息交换两个方面。前者是基础，后者是从前者派生出来的。因此，现代化的电子银行系统，一般都具有支付服务和金融信息增值服务两种功能，或者说电子银行的产品，包含支付产品和信息增值服务两大类产品。只有建立完善的综合支付体系，才能为客户提供有效的金融信息增值服务。这样，电子银行不仅大大增强了传统银行所起的信用中介作用，即资金、货币流通的介质和导体作用，电子银行还起着全新的社会经济信息收集、加工处理和服务中心的作用。银行从传统的单纯信用中介，发展到强化了的信用中介和信息增值服务，使银行发生了革命性的变化，也使银行界真正进入了电子银行时代。

进入20世纪90年代后，随着Internet的爆炸性发展和电子商务的兴起，Web技术引入银行，银行开始通过开放性的Internet提供网上银行服务。网上银行服务和其他电子银行系统的发展，使银行的支付服务和信息服务深入到社会的各个领域，电子银行进入下一个全新的发展阶段，由实体电子银行向虚拟电子银行发展。在网上银行服务中，银行的服务将以