第3章

电子货币与网上支付

学习要点

电子货币；

电子支票；

电子现金的实现手段；

电子现金的特点；

电子现金的安全防范；

网络银行；

网上支付；

第三方支付。

3.1 电子货币

3.1.1 电子货币概念

电子货币是指用一定金额的现金或存款从发行者处兑换并获得代表相同金额的数据，通过使用某些电子化方法将该数据直接转移给支付对象，从而能够清偿债务。按支付方式可将电子货币分为储值卡型电子货币、银行卡型电子货币、电子支票和电子现金。网上常用的电子货币有后三种。

3.1.2 电子货币的发行和运行

电子货币发行和运行的流程分为三个步骤，即发行、流通和回收，如图 3-1 所示。

① 发行：电子货币的使用者 X 向电子货币的发行者 A(银行、信用卡公司等)提供一定金额的现金或存款并请求发行电子货币，A 接受了来自 X 的有关信息之后，将相当于一定金额电子货币的数据对 X 授信。

② 流通：电子货币的使用者 X 接受了来自 A 的电子货币，为了清偿对电子货币的另一使用者 Y 的债务，将电子货币的数据对 Y 授信。

③ 回收：A 根据 Y 的支付请求，将电子货币兑换成现金支付给 Y，或者存入 Y 的存

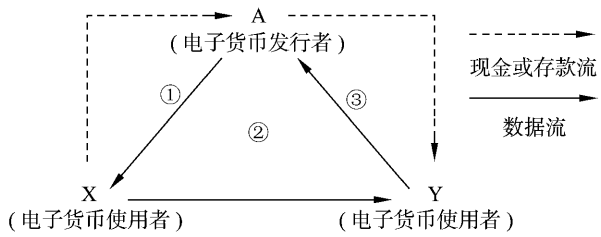

图 3-1　电子货币的发行

款账户。

在发行者与使用者之间有中介机构介入的体系是常见的体系。例如,在图 3-1 中的 A、X、Y 三个当事者之外,A、X 之间介入了银行 a,A、Y 之间介入了银行 b,如图 3-2 所示。

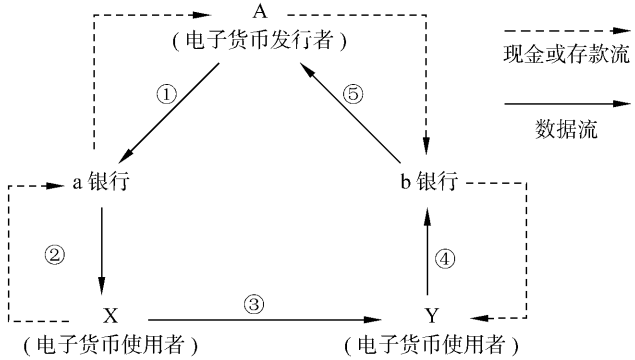

图 3-2　有中介机构介入的电子货币体系

有中介机构的电子货币体系的运行分五个步骤,涉及五个当事者:

① A 根据 a 银行的请求,与现金或存款交换发行电子货币;

② X 对 a 提供现金或存款,请求得到电子货币,a 将电子货币向 X 授信;

③ X 将由 a 接受的电子货币用于清偿债务,授信给 Y;

④ Y 的开户银行 b 根据 Y 的请求,将电子货币兑换成现金支付给 Y(或存入 Y 的存款账户);

⑤ A 根据从 Y 处接受了电子货币的银行 b 的请求,将电子货币兑换成现金支付给 b(或存入 b 的存款账户)。

3.1.3　储值卡型电子货币

储值卡型电子货币就是功能得到进一步提高的储值卡。储值卡是指某一行业或公司发行的可代替现金用的 IC 卡或磁卡。例如,移动通信公司发行的电话充值卡,超市、百货商店发行的购物卡,石油公司发行的加油卡,交通部门发行的交通卡等。

3.1.4　银行卡型电子货币

银行卡型电子货币是实现了电子化应用的信用卡。信用卡 1915 年起源于美国,至今

已有 80 多年的历史，目前在发达国家及地区，如美国、日本、英国、法国等地，信用卡使用得非常广泛，已成为一种普遍使用的支付工具和信贷工具。它使人们的结算方式、消费模式和消费观念发生了根本性的改变。

信用卡的最大特点是同时具备信贷与支付两种功能。持卡人可以不用现金，凭信用卡购买商品和享受服务，由于其支付款项是发卡银行垫付的，银行便对持卡人发生了贷款关系，而信用卡又不同于一般的消费信贷。一般的消费信贷只涉及银行与客户二者之间的关系，信用卡除银行与客户之外，还与受理信用卡的商户发生关系，这是一个三角关系。按卡的信用性质与功能可分为借记卡（属于广义信用卡）和贷记卡（属于狭义信用卡）。

借记卡的特征是“先存款，后支用”，持卡人必须先在发卡机构存款，用款时以存款余额为限不允许透支。贷记卡的特征是“先消费，后还款”，持卡人无须先在发卡机构存款，就可享用一定信贷额度的使用权。目前我国发行的信用卡主要是两种功能结合又偏重于“借记”的信用卡。此外，各商业银行也在逐步发行、推广贷记卡。

银行卡支付通常涉及三方，即消费者（持卡人）、商户和银行。支付过程包括清算和结算，前者指支付指令的传递，后者指与支付相关的资金的转移。资金支付必须由发卡银行通过适当的网络进行授权来完成，流程如下所述。

（1）持卡人用卡购物或消费，结账时交验银行卡，将银行卡插入 POS 终端，输入的数据（卡号和支付金额）通过通信线路传到银行，请求授权支付。

（2）发卡行经过核实持卡人账户的合法性和可用余额（或受信额度）后，告诉特约商户（POS）同意交易，然后从持卡人账户上扣除相应金额，划入特约商户的开户银行账户。

（3）商户向持卡人提供商品或劳务，并要求持卡人在签购单上签字。

（4）发卡行定期将对账单给持卡人。

当上述基于银行卡的支付在互联网上进行时，环境发生了实质性变化，因为这里有一个基本的前提，就是传统的银行卡支付是在银行专用网络上传输的数据，是足够安全的，而且消费者与商家是面对面交易。在互联网上支付时，信息会在完全开放的网络上传输，对支付的安全性提出了更高的要求。核心问题是消费者、商户和银行之间的支付信息的安全传输和身份认证。这部分内容请参考第 5 章。

3.1.5 电子支票

1. 什么是电子支票

电子支票是将支票的全部内容电子化，然后借助于互联网完成支票在客户之间、银行客户与客户之间以及银行之间的传递，实现银行客户间的资金结算。一个电子支票支付方案包括消费者和他的银行、商户和他的银行、不同银行之间支票的清算处理三个部分。电子支票中包含有与纸支票完全相同的支付信息，如收款方名称、付款方账户、金额和日期。同时电子支票包含有数字证书和数字签名，它们连同加密解密技术一起，用来防止对银行和银行客户的欺诈，提高电子支票的安全性，以保证信息的真实性、保密性、完整性和不可否认性（请参考第 5 章）。

电子支票将整个处理过程自动化，帮助银行舒解银行处理支票的压力，节省了大量的人力和开支，极大地降低了处理成本；可以在任何时间、地点通过互联网进行传递，打破了地域的限制，最大限度地提高支票的收集速度，从而为顾客提供了更方便快捷的服务且减少了其在途资金；通过应用数字证书、数字签名以及加密解密技术，提供了比使用印章和手写签名更加安全可靠的防欺诈手段。电子支票在这三个方面的巨大进步无疑会使其成为支票发展史上的一次革命。

2. 电子支票应用过程

电子支票的应用过程如图 3-3 所示。

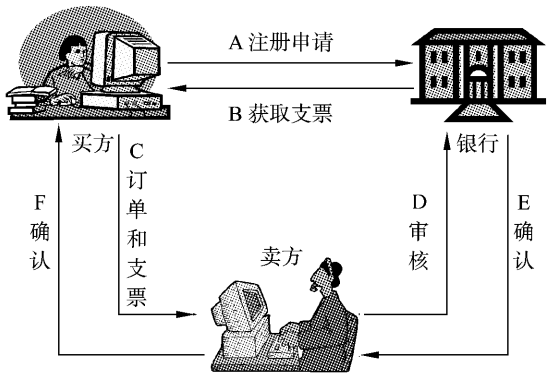

图 3-3　电子支票支付过程

(1) 购买电子支票

买方首先必须在提供电子支票服务的银行注册，开具电子支票。注册时需要输入银行账户信息以支持开设支票。电子支票应具有银行的数字签名。

(2) 电子支票付款

一旦注册，买方就可以和产品/服务出售者取得联系。买方用自己的私钥在电子支票上进行数字签名，用卖方的公钥加密电子支票，使用 E-mail 或其他传递手段向卖方进行支付；卖方收到用卖方公钥加密的电子支票，用买方的公钥确认买方的数字签名后，可以向银行进一步认证电子支票，之后即可发货给买方。

(3) 清算

卖方定期将电子支票存到银行，支票允许转账。不同银行之间的支票清算由金融网络完成。

3. 电子支票的特点

- 电子支票与传统支票工作方式相同，易于接受；
- 加密的电子支票易于流通，买卖双方的银行只要用公共密钥认证确认支票即可，数字签名也可以被自动验证；
- 降低了支票的处理成本，同时减少了在途资金，提高了银行客户的资金利用率；
- 第三方金融机构带的收益，第三方金融服务者不仅可以从交易双方处抽取固定交

易费用或按一定比例抽取费用，它还可以作为银行身份，提供存款账目，而且电子支票存款账户很可能是无利率的。

3.1.6 电子现金

电子现金又称为数字现金，是一种表示现金的加密序列数，它可以用来表示现实中各种金额的币值。电子现金带来了纸币在安全和隐私性方面所没有的计算机化的便利，电子现金的丰富性开辟了一个全新的市场和应用，电子现金正在尝试取代纸币作为网上支付的主要手段之一。电子现金是最接近实体现金的电子货币，一旦得到普及，则对国家的货币体系影响很大。

1. 现金支付的特点

现金在人们日常生活中不可缺少，扮演着重要角色。现金支付具有以下几个特点。

(1) 现金是最终的支付手段

现金之所以具备支付手段的功能，在于所有的经济主体相信现金的经济价值具有不变性和稳定性，相信通过对现金的授受，在付款人和收款人之间进行支付，可以使结算完全终结。目前，存款和现金作为支付手段之所以能在相当广的范围被普及应用，是由于社会对“存款无论何时均可兑换现金”的认识已经根深蒂固的结果。存款作为支付手段能被放心使用的原因在于所有的经济主体对现金价值的信任。因此，从现金在支付中具有不可缺少的“提供价值源泉”的意义上，可以说，现金是最终的支付手段。

(2) 现金支付具有“分散处理”的性质

现金支付在付款与收款当事人之间，只需授受现金即可使支付完全终结，无须任何第三者的介入，也无须改写和记录保存在任何地点的账目。即完全不必集中于某地才可以处理，也不必与某人或某机构联络。因此，从现金支付只是在当事人之间即可完成的意义上，可以说，现金支付是完全分散处理的结算方式。

(3) 现金支付具有“脱线处理”的性质

以现金授受进行支付时，若支付人已预先持有了现金，结算过程中，则完全无须银行帮助。收款人若对接受的现金通过亲眼辨认和亲手触摸能够确认是“真实的现金”，则支付即时完成。所以，从现金支付不必与银行联系，脱离银行也可完成的意义上，可以说，现金支付是完全脱线处理的结算方式。

(4) 现金的稀缺性与信誉性

现金之所以能成为最终的支付手段进行脱线的分散处理完成结算的原因何在呢？究其根本原因，仍然是以所有经济主体对于现金价值的信任为基础的。正是由于相信现金本身具有的价值，认为从付款人手中接受的现金可以用于下一次支付，即自己成为债务人时，债权人也能将该现金当作支付手段接受。债权人相信只要接受现金，此外，无须与任何人联络、无须任何确认手续，即可放心地完全回收债权。

2. 电子现金实现的手段

现金货币是在社会信任纸币和辅币等物理实体具有价值的基础上存在的，人们对实

体现金信任的基础在于实体现金的稀缺性。那么，现金实现电子化即电子现金的出现，同样必须确保稀缺性的特点，才会得到社会的信任，才能具有普遍接受性。为此，在保证稀缺性的基础上，出现了各种实现电子现金的技术手段，其中有代表性的主要有以下两种手段。

(1) 数字信息块实现手段

实现电子现金的第一种手段，是将遵循一定规则排列的一定长度的数字串，即一种电子化的数字信息块，作为代表纸币或辅币所有信息的电子化手段。实际上，这个数字串是非常简单的数字串。例如，可用“99005010”这个数字串表示 50 元人民币现钞、“99010010”这个数字串表示 100 元人民币现钞。如果在某台计算机的硬盘中存储了 5 个“99005010”和 3 个“99010010”，那么则表示该硬盘合计存储了 550 元的电子现金。在电子现金用于支付时，只需将相当于支付金额的若干个信息块综合之后，用电子化方法传递给债权人一方，即可完成支付。

通过上述手段，可以将用纸张、金属制造的实体现金转化为数字信息，是对现金货币的一种纯粹的电子化模拟试验。就目前情况而言，由荷兰的求索现金公司(Dig Cash bv/inc)技术开发的电子现金试验项目(以下称电子现金)是使用这种技术手段的典型代表，已接近于现钞的功能。

但是，数字化的电子信息块也正由于是以数字串排列为特征的数字化信息，所以具备可以完整复制的特点。例如，将数字串“99005010”复制之后，得到的数字串“99005010”与原件完全一致，即复制物与原物不可区别。因此，该手段具有难以确保电子现金稀缺性的缺点。针对该缺点，通过采用特殊的密码技术和其他安全措施，使得合法的发行主体之外的任何个人或组织不可能制造(或复制)出这种数字信息块，成为确保电子货币稀缺性的关键所在。

上述荷兰的电子现金项目，为了克服容易复制的缺点，采用了强度密码技术，而且每次支付时，均要与电子现金的发行银行之间核查是否发生过复制，从而保证了电子现金的稀缺性，不失为有效的安全措施。但是，正因为电子现金支付时必须与银行联系，使得它与完全可以分散处理和脱线处理的支付手段现金货币仍有一段距离，还不能说可以完全模拟实体现金货币。

(2) Mondex 的实现手段

实现电子现金的第二种手段，是被称为“Mondex 型”的电子现金模式。对于在英国进行实用化试验的 Mondex 电子现金项目，外界多有评论称其为“实现了现金的电子化”。Mondex 的系统结构不是像第一种手段在微机的硬盘中根据需要的数量存储相当于一定现钞金额的电子信息块，而是在 IC 卡内保存了货币价值的汇总余额，并且该余额是以二进制数字形式存储的。

Mondex 使用 IC 卡作为货币价值的计数器，即可以将 Mondex 的 IC 卡看成记录货币余额的账簿。在从卡内支出价值，或是向卡内再存入价值时，通过改写卡内的余额记录进行处理。因此，就该点而言，可以说 Mondex 类似于存款货币，Mondex 的专用 IC 卡相当于存款账户。

不过，为了对卡内记录的货币余额进行转移，又采用了相应的技术手段，从而，使

Mondex 具备了与现金货币极其相似的特性，取得了相当大的成功。具体而言，在两个合法的 Mondex 专用 IC 卡之间转移货币（支付）时，一方的余额减少，另一方的余额只增加相同金额，不可能有非正当的增额出现。由于实现了有效而可靠的余额管理体系，所以 Mondex 确保了货币余额的稀缺性。而且，使用 Mondex 的结算处理，只需在同类的 IC 卡之间进行，无须与银行等 Mondex 的发行主体取得任何联系，因此，实现了作为现金支付特征的分散处理和脱线处理。

以上简要说明了在技术上如何确保电子现金稀缺性的方法。即为了防止发行主体之外的非法主体通过复制的方法任意伪造电子现金，以动摇社会对电子现金的信任，而采取的技术手段。

3. 电子现金的支付过程

（1）购买电子现金

买方在电子现金发放银行开电子现金账号并购买电子现金。要从网上的货币服务器（或银行）购买电子现金，首先要在该银行建立一个账户，将足够资金存入该账户以支持今后的支付。目前，多数电子现金系统要求买方在一家网络银行上拥有一个账户。这种要求对于全球性和多种现金交易非常严格，买方应该能够在国内获得服务并进行国外支付，但需要建立网络银行组织，作为一个票据交换所。

（2）存储电子现金

使用专用软件从电子现金银行取出一定数量的电子现金存在特定的设备上。一旦账户被建立起来，买方就可以使用电子现金软件产生一个随机数，它是银行使用私钥进行了数字签名的随机数，再把货币发回给买方。

（3）用电子现金购买商品或服务

买方同意接收电子现金的卖方订货，用卖方的公钥加密电子现金后，传送给卖方。

（4）资金清算

接收电子现金的卖方与电子现金发放银行之间进行清算，电子现金银行将买方购买商品的钱支付给卖方。这时可能有两种支付方式：双方的和三方的。双方支付方式涉及两方，即买卖双方。在交易中卖方用银行的公共密钥检验电子现金的数字签名，如果对于支付满意，卖方就把数字货币存入它的机器，随后再通过电子现金银行将相应面值的金额转入账户。所谓三方支付方式，是在交易中，电子现金被发给卖方，卖方迅速把它直接发给发行电子现金的银行，银行检验货币的有效性，并确认它没有被重复使用，将它转入卖方账户。在许多情况下，双方交易是不可行的，因为可能存在重复使用的问题。为了检验是否重复使用，银行将从卖方获得的电子现金与已经使用电子现金数据库进行比较。像纸币一样。电子现金通过一个序列号进行标识。为了检验重复使用，电子现金将以某种全球同一标识的形式注册。但是，这种检验方式十分费时费力，尤其是对于小额支付。

（5）确认订单

卖方获得付款后，向买方发送订单确认信息。

三方电子现金支付过程如图 3-4 所示。

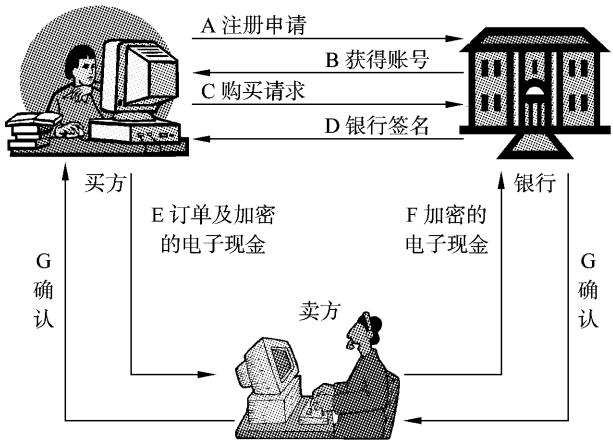

图 3-4　三方电子现金支付过程

4. 电子现金的特点

(1) 匿名性

电子现金与信用卡应用型和电子支票的最大区别在于,可以实现结算的匿名性。首先,对信用卡应用型电子货币而言,因为需要通过第三者授信和垫付行为的介入,所以每次结算的付款人和收款人必须是特定的,该结算数据至少要由第三者保管一段时间。其次,对存款利用型电子货币而言,所有的结算处理均要通过管理存款的银行作改写账目的事务处理来完成。因此,每一次独立结算的资金来源和去向必然被银行所掌握。

与此相反,对电子现金而言,仅仅在结算的当事人之间进行脱线的分散处理,因此资金的流向不必由第三者管理和把握。这与使用现金的情况类似,所有关于结算的信息均无须第三者管理和掌握,而且现实中是可以实现的。人们社会经济行为的最终结果几乎全部要归结到资金的流动,围绕个人日常活动的资金流、信息流如果必须逐一被他人掌握,相信没有一个人会感到愉快。虽然不能断言结算绝对需要匿名性,但是,人们对具备匿名性的结算方法的偏好是大量存在的。因此,电子现金在这一点上占据优势。

(2) 不可跟踪性

不可跟踪性是现金的一个重要特性。不可跟踪性可以保证交易的保密性,也就维护了交易双方的隐私权。除了双方的个人记录之外,没有其他关于交易已经发生的记录。因为没有正式的业务记录,连银行也无法分析和识别资金流向,也正是因为这一点,如果电子现金丢失了,就会同纸币现金一样无法追回。

(3) 节省传输费用

普通现金的传输费用比较高,这是因为普通现金是实物,实物的多少与现金金额是成正比的,金额越大实物货币就越多,大额现金的保存和移动是比较困难和昂贵的。而电子现金流动没有国界,在同一个国家内流通的费用跟在国际间流通的费用是一样的。

(4) 风险小

普通现金有被抢劫的危险,必须存放在指定的安全地点,在存放和运输过程中要由保

安人员看守。保管普通现金越多，所承担的风险越大，在安全保卫方面的投资也就越大，而电子现金则不存在这些问题。

(5) 节省交易费用

为了货币的流通，普通银行需要设置许多分支机构、职员、自动付款机及各种交易系统，这就增加了银行进行资金处理的费用。而电子现金是利用已有的互联网和用户的计算机，所以消耗比较小，用于小额交易尤其合算。

(6) 支付灵活方便

电子现金的使用范围比信用卡更广，银行卡支付仅限于被授权的商户，而电子现金支付却不必有这层限制。

5. 电子现金的安全防范措施

电子现金在实际应用中，为了确保安全，防止伪造，使用了一些关键性技术。

由于电子现金本身是数字串形式的数字信息，如果他人破译了数字串排列的规律，即可随意制造出新的电子现金。因此，为了防止伪造，对使用中的电子现金，必须能够证明是由取得发行权的银行发行的原件。有如发行纸币时，每张纸币上均需盖有银行的印鉴。实际上，在保证电子现金具备匿名性的同时，可以通过加盖电子印鉴以防伪。其中，使用了称为“盲签名”的密码技术是通过复杂的数学处理实现的，具体说明如下。

假设消费者需要从银行支取金额是 1 元的电子现金。首先，用自己的计算机启动电子现金软件，发出想要支取的指令。然后，计算机内自动产生一个表示序列号的随机数字串，再与表示 1 元金额的数字串合并成一个新的数字串。为了不被他人所知，将该数字串装入电子信封(即加密处理)中，授信给银行。银行收到之后，不开启信封，透过信封对里面的数字串加盖电子印鉴，连信封一起传递给消费者。消费者从信封中取出盖有银行电子印鉴的数字串，保存到硬盘中。这样就得到了 1 元金额的电子现金。

银行加盖印鉴时，银行一方不可能看到每个电子现金的序列号，这是采用“盲签名”密码技术的关键所在。假如银行看到了该序列号，当电子现金用于支付又返回银行时，银行就可以知道：该电子现金曾发行给何人，又传递到何人的手中。这样一来，则不能确保电子现金的匿名性。

为什么每个电子现金都需要有一个序列号呢？如果仅仅是为了匿名性的话，一开始就不用序列号也是可以的。实际上，是为了防止通过复制电子现金，从而非正当地、恶意地、重复二次、三次地使用。下面看看使用电子现金支付时的处理过程，进一步说明上述安全措施的作用。

消费者将电子现金授信支付给网上商店。接受电子现金的一方即商店再将电子现金授信给银行。银行受信后，首先，核对电子现金上加盖的印鉴，确认该电子现金的真实性，是否由具备发行权的银行发行；其次，通过核对电子现金上的序列号，确认该电子现金过去是否曾经使用过。因为，银行一方对用过一次的电子现金的序列号均保存在数据库中。电子现金每次返回银行，均需查询数据库。如果数据库中已经保存了同样的序列号，则说明该电子现金是重复使用；若数据库中无此序列号，则作为初次使用对待，并在数据库中保存该序列号。经过以上审查，如果确认了是未经重复使用的合

法的电子现金，银行则将接受的电子现金相应金额存入商店的账户，即增加账户余额。在电子现金用于个人之间的支付时，其审查过程完全相同，也必须核对其真伪以及是否重复使用过。

也就是说，为了防止重复使用，电子现金只能使用一次，而实体现金，同样的纸币或辅币可不断流通反复使用，二者的形态完全不同。就该点而言，电子现金尚未能完全模拟实体现金支付。而且，保存电子现金序列号的数据库中的数据会不断膨胀，这也是电子现金目前存在的缺点。

EC 聚焦——招商银行一网通

招商银行对全行计算机网络进行了改造，推出了“一网通”（又名招商银行网络银行）。招商银行的网络银行（一网通）是指通过因特网或其他公用信息网（如“视聆通”），将客户的计算机终端连接至银行，实现将银行服务直接送到客户办公室、家中和手中的服务系统。它拉近了客户与银行的距离，使客户足不出户就可以享受到招商银行的服务。

“一网通”包括“企业银行”、“个人银行”、“网上支付”、“网上证券”和“网上商城”，为客户提供招商银行信息服务、个人银行、企业银行、网上支付等网络银行业务、利率、汇率、股市行情等金融信息以及网上商城服务。在“一网通”的“个人银行”中，消费者还可以将“一卡通”的资金转换成“一网通”的资金。

招商银行的“一网通”在我国所有的网络银行中，无论在技术上还是从业务量上均处于领先地位，通过“一网通”，客户不再受时间、空间的限制，可以全天候不间断地在世界任何角落享受招商银行提供的服务。

3.2 网上支付

3.2.1 什么是网上支付

所谓支付（Payment），是指清偿商品交换和劳务活动以及金融资产交易所引起的债权债务关系，由银行所提供的金融服务业务。它起源于银行客户之间的经济交往活动，但由于银行“信用”中介的结果，演化为银行与客户和银行客户的开户银行之间的资金收、付关系。而银行之间的资金收、付交易又必须经过银行的银行，即政府授权的中央银行进行资金清算，才能最终完成支付的全过程。因此，支付全过程将在两个层次完成，下层是商业银行与客户之间的资金支付往来与结算；上层是中央银行与商业银行之间的资金支付与清算。两个层次支付活动的全过程将经济交往活动各方与商业银行、中央银行维系在一起，构成复杂的系统整体，被称为支付系统（Payment System）。在国民经济大系统之中，支付系统发挥着重要的宏观经济“枢纽”作用。

在两个层次的支付活动中，银行与客户之间的支付与结算，是银行为客户提供多种金融服务的窗口，其系统特点是账户多、业务量大，涉及客户、银行双方权益，是支付系统的基础，被称为支付服务系统；而中央银行与商业银行之间的支付与清算则是政府授权的中央银行实施货币政策，监督、控制商业银行金融活动，控制国家货币发行，管理国库，管理