(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101923754 A
(43)申请公布日 2010.12.22

(21)申请号 200910087315.3

(22)申请日 2009.06.17

(71)申请人 中国工商银行股份有限公司
地址 100031 北京市西城区复兴门内大街55号

(72)发明人 李兴双 史大鹏 刘洋 周新衡

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 周国城

(51)Int.Cl.
G07F 19/00(2006.01)
G07F 7/10(2006.01)
G07F 7/12(2006.01)

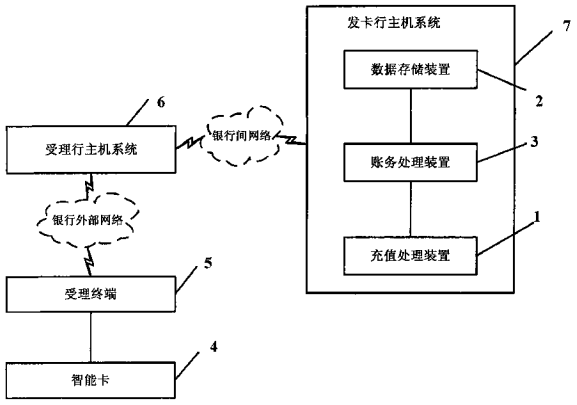
权利要求书 3 页 说明书 8 页 附图 5 页

(54)发明名称

基于银行智能卡实现快速支付的系统及方法

(57)摘要

本发明公开了一种基于银行智能卡实现快速支付的系统，包括：发卡行主机系统(7)、受理行主机系统(6)、受理终端(5)和具备快速安全支付功能的智能卡(4)，其中，发卡行主机系统(7)与受理行主机系统(6)之间通过银行间网络连接，受理行主机系统(6)与受理终端(5)之间通过银行外部网络连接，受理终端(5)与智能卡(4)之间通过接触式或非接触式连接。本发明同时公开了一种基于银行智能卡实现快速支付的方法。利用本发明，克服了传统银行卡支付在支付速度、通讯成本以及安全风险方面的不足，并且交易迅速、安全性高、实施简便。



CN 101923754 A

1. 一种基于银行智能卡实现快速支付的系统，其特征在于，包括：发卡行主机系统(7)、受理行主机系统(6)、受理终端(5)和具备快速安全支付功能的智能卡(4)，其中，发卡行主机系统(7)与受理行主机系统(6)之间通过银行间网络连接，受理行主机系统(6)与受理终端(5)之间通过银行外部网络连接，受理终端(5)与智能卡(4)之间通过接触式或非接触式连接。

2. 根据权利要求1所述的基于银行智能卡实现快速支付的系统，其特征在于，所述发卡行主机系统(7)包括依次连接的充值处理装置(1)、数据存储装置(2)和账务处理装置(3)，其中：

充值处理装置(1)，用于对智能卡(4)进行可用余额充值处理，并将一定金额的账户余额予以冻结保留，且该保留金额会被记录智能卡(4)的芯片中；

数据存储装置(2)，用于登记并存储银行卡账户资料信息，至少包括银行卡的账户可用余额和冻结金额信息；

账务处理装置(3)，用于发卡行的卡账户资金的入账处理，当脱机快速支付后，所有支付信息数据会传递到发卡行主机系统(7)的账务处理装置(3)，账务处理装置(3)判断支付数据的有效性，并完成卡账户资金的入账处理，包括解除账户冻结金额和扣减账户余额处理。

3. 根据权利要求1所述的基于银行智能卡实现快速支付的系统，其特征在于，所述受理行主机系统(6)用于完成智能卡(4)交易的转发以及与发卡行主机系统(7)的资金清算。

4. 根据权利要求1所述的基于银行智能卡实现快速支付的系统，其特征在于，所述受理终端(5)是能够受理智能卡的交易终端，包括但不限于是POS机或IC卡读卡设备，由并联连接的第一通讯单元、第一安全单元、第一运算单元、第一输入输出单元和第一存储单元构成，其中，第一通讯单元用于与智能卡进行通讯，第一安全单元用于与智能卡进行安全认证，第一运算单元用于对交易金额进行计算处理，第一输入输出单元用于交易信息的录入以及交易结果的反馈，第一存储单元用于记录交易信息以便定期上传至受理银行主机系统。

5. 根据权利要求1所述的基于银行智能卡实现快速支付的系统，其特征在于，在联机交易过程中，所述受理终端(5)扣减智能卡(4)上的可用余额，并判断智能卡(4)的可用余额的大小，通过与受理行主机系统(6)及发卡行主机系统(7)的交互，实现智能卡(4)上可用余额的自动充值，同时发卡行主机系统(7)冻结保留智能卡(4)主账户的可用资金，以保证智能卡(4)脱机支付金额不超过账户限额；

在脱机交易过程中，所述受理终端(5)扣减智能卡(4)上的可用余额，并生成日终入账记录文件，通过受理行主机系统(6)定期上送到发卡行主机系统(7)，实现银行卡账户资金的处理与清算。

6. 根据权利要求1所述的基于银行智能卡实现快速支付的系统，其特征在于，所述智能卡(4)包括依次连接的第二通讯单元、第二安全单元、第二运算单元和第二存储单元，其中：

第二通讯单元，用于实现智能卡与受理终端之间的信息交换，其通讯形式是以智能卡上的芯片触点进行，或者是通过第二通讯单元中的天线与受理终端上的电线进行无线电通

信；

第二安全单元，用于实现智能卡与受理终端之间的安全认证，验证受理终端的有效性，保证智能卡存储单元中的数据不会被非法篡改，并在交易完成之后生成数字签名，增强交易的不可抵赖性；

第二运算单元，用于对交易金额、交易货币种类以及智能卡中存储的可用余额、货币种类信息进行判定和比较，决定是否允许继续对交易进行处理；

第二存储单元，用于存储智能卡的基本信息，包括帐号、持卡人姓名、智能卡有效期、持卡人个人标识号 PIN、可用余额和智能卡自动充值阈值信息，供第二运算单元读取和更改。

7. 根据权利要求 6 所述的基于银行智能卡实现快速支付的系统，其特征在于，所述第二存储单元受第二安全单元的控制，在通过安全验证之后，方可被有条件的读取和修改。

8. 根据权利要求 1 所述的基于银行智能卡实现快速支付的系统，其特征在于，所述智能卡 (4) 是银行发行的芯片卡。

9. 根据权利要求 8 所述的基于银行智能卡实现快速支付的系统，其特征在于，所述银行发行的芯片卡是借记卡，或是贷记卡。

10. 根据权利要求 1 所述的基于银行智能卡实现快速支付的系统，其特征在于，所述受理终端与所述智能卡之间采用如下相互认证的安全机制：由证书签发机构来定义根 CA 的公私钥，利用根 CA 的私钥对发卡行公钥签发发卡行证书；发卡行生成 IC 卡上公私钥对、按照一定的规则指定敏感的应用数据，作为需要被认证的静态行业数据；利用发卡行私钥对 IC 卡公钥和静态行业应用数据签发 IC 卡证书，并将 IC 卡私钥、IC 卡证书和发卡行证书被保存于 IC 卡内；交易受理银行主机系统将由证书签发机构签发的根 CA 公钥部署于 IC 受理终端内，在实际应用时，受理终端利用其内的行业根 CA 先验证发卡行证书，通过后获得有效的发卡行公钥；受理终端利用发卡行公钥认证 IC 卡证书，通过后获得有效的 IC 卡公钥及静态行业数据；受理终端再发送动态数据给智能卡，该动态数据是随机数，智能卡利用 IC 卡私钥对指定数据和终端动态数据进行签名，并送给受理终端；IC 受理终端利用获得的 IC 卡公钥对 IC 卡生成的签名进行确认。

11. 一种基于银行智能卡实现快速支付的方法，其特征在于，包括：

步骤 1：受理终端与智能卡之间进行相互认证；

步骤 2：认证通过后，受理终端发起指令扣减智能卡中保存的可支付余额，并保存和记录支付信息；

步骤 3：受理终端定期将所有支付信息传递到受理行主机系统，由受理行主机系统与发卡行主机系统进行资金往来清算。

12. 根据权利要求 11 所述的基于银行智能卡实现快速支付的方法，其特征在于，所述步骤 1 具体包括：

步骤 100：在受理终端输入交易金额，受理终端与智能卡进行通信连接并向智能卡发送交易请求；

步骤 101：智能卡接收受理终端的交易请求；

步骤 102：智能卡对交易请求信息进行校验和判别；

步骤 103：智能卡检查受理终端是否支持快速安全支付功能、受理终端的安全报文是否能通过认证；如果通过检查，则执行步骤 104；如果不能通过检查，则向受理终端返回交

易失败，结束本流程；

步骤 104：智能卡将交易处理情况返回受理终端；

步骤 105：受理终端接收智能卡的返回信息；

步骤 106：受理终端对智能卡的返回信息进行判别，校验智能卡的真实有效性，智能卡有效则继续处理，否则拒绝交易，结束本流程。

13. 根据权利要求 11 所述的基于银行智能卡实现快速支付的方法，其特征在于，所述步骤 2 具体包括：

步骤 107：受理终端判断智能卡中的快速支付可用余额是否足够支付，如果足够支付，则继续处理；否则，退出支付交易处理，对智能卡进行充值；

步骤 108：受理终端处理完毕后，向智能卡发起扣款指令；

步骤 109：智能卡接收扣款指令；

步骤 110：智能卡扣减自身可用余额，并生成当前交易的数字签名信息；

步骤 111：智能卡将扣款结果、交易数字签名返回受理终端；

步骤 112：受理终端接收信息，并将其在存储单元中保存；

步骤 113：受理终端显示支付交易完成，并根据实际需要，打印支付交易凭证。

14. 根据权利要求 13 所述的基于银行智能卡实现快速支付的方法，其特征在于，步骤 107 中所述对智能卡进行充值，具体包括：

步骤 201：受理终端将智能卡充值请求上送给受理行主机系统，并最终传送到发卡行主机系统，由发卡行主机系统对银行卡账户进行资金冻结，扣减主账户可用余额；

步骤 202：受理终端接收发卡行主机系统返回的充值请求处理结果，

步骤 203：受理终端向智能卡发起充值指令；

步骤 204：智能卡接收充值指令；

步骤 205：智能卡增加可用余额至自动充值最大金额，并生成当前交易的数字签名信息；

步骤 206：智能卡将充值结果、交易数字签名返回受理终端；

步骤 207：受理终端显示充值交易完成，并根据实际需要，打印充值交易凭证，充值处理结束。

15. 根据权利要求 11 所述的基于银行智能卡实现快速支付的方法，其特征在于，步骤 3 中所述受理终端定期将所有支付信息传递到受理行主机系统，是通过网络或其他移动存储设备实现的。

基于银行智能卡实现快速支付的系统及方法

技术领域

[0001] 本发明涉及银行卡支付技术领域，特别是涉及一种基于银行智能卡实现快速支付的系统及方法。

背景技术

[0002] 日常生活中，人们经常会进行一些小额消费支付，如在餐饮、便利店、电影院、收费停车、公交、地铁等场合的支付，这类支付要求支付过程能快捷、安全、方便。

[0003] 然而，传统的银行卡支付过程中，一般是由销售点终端通过公共电话网 (PSTN) 以拨号连接的形式将交易送入银行主机系统。这种方式存在交易时间长、通讯费用高等弊端，严重制约着支付电子化的发展。

[0004] 电子钱包技术可以解决传统支付中存在的问题，但是对受理银行而言，需要在终端部署销售点安全访问模块 (PSAM 卡)，在安全、管理等方面存在较大的隐患。另外，从安全角度考虑，电子钱包技术使用对称密钥体系，所有的密钥都是保密密钥，其交换、传递、更新都面临着较大的问题；对客户而言，需要到银行网点对账户进行手工充值，使用很不方便，且无法像信用卡账户那样做到先消费、后还款。

[0005] 近些年，随着欧陆卡、万事达卡、维萨卡 (Europay、MasterCast、Visa，EMV) 智能卡的发行推广，实现了智能卡的安全认证和脱机支付，但在 EMV 卡的脱机认证支付机制下，由于没有进行脱机消费金额与账户余额信息的核对，很可能导致持卡人账户透支超限，从而增加银行的业务经营风险。

[0006] 综上所述，迫切需要一种好的支付方法，该方法能很好地解决支付中的快捷、安全、方便的等问题。

发明内容

[0007] （一）要解决的技术问题

[0008] 有鉴于此，本发明的主要目的在于提供一种快捷、安全、方便的基于智能卡实现快速支付的系统及方法，以克服传统银行卡支付在支付速度、通讯成本以及安全风险方面的不足。

[0009] （二）技术方案

[0010] 为达到上述目的的一个方面，本发明提供了一种基于银行智能卡实现快速支付的系统，包括：发卡行主机系统 7、受理行主机系统 6、受理终端 5 和具备快速安全支付功能的智能卡 4，其中，发卡行主机系统 7 与受理行主机系统 6 之间通过银行间网络连接，受理行主机系统 6 与受理终端 5 之间通过银行外部网络连接，受理终端 5 与智能卡 4 之间通过接触式或非接触式连接。

[0011] 上述方案中，所述发卡行主机系统 7 包括依次连接的充值处理装置 1、数据存储装置 2 和账务处理装置 3，其中：

[0012] 充值处理装置 1，用于对智能卡 4 进行可用余额充值处理，并将一定金额的账户余

额予以冻结保留，且该保留金额会被记录智能卡 4 的芯片中；

[0013] 数据存储装置 2，用于登记并存储银行卡账户资料信息，至少包括银行卡的账户可用余额和冻结金额信息；

[0014] 账务处理装置 3，用于发卡行的卡账户资金的入账处理，当脱机快速支付后，所有支付信息数据会传递到发卡行主机系统 7 的账务处理装置 3，账务处理装置 3 判断支付数据的有效性，并完成卡账户资金的入账处理，包括解除账户冻结金额和扣减账户余额处理。

[0015] 上述方案中，所述受理行主机系统 6 用于完成智能卡 4 交易的转发以及与发卡行主机系统 7 的资金清算。

[0016] 上述方案中，所述受理终端 5 是能够受理智能卡的交易终端，包括但不限于是 POS 机或 IC 卡读卡设备，由并联连接的第一通讯单元、第一安全单元、第一运算单元、第一输入输出单元和第一存储单元构成，其中，第一通讯单元用于与智能卡进行通讯，第一安全单元用于与智能卡进行安全认证，第一运算单元用于对交易金额进行计算处理，第一输入输出单元用于交易信息的录入以及交易结果的反馈，第一存储单元用于记录交易信息以便定期上传至受理银行主机系统。

[0017] 上述方案中，在联机交易过程中，所述受理终端 5 扣减智能卡 4 上的可用余额，并判断智能卡 4 的可用余额的大小，通过与受理行主机系统 6 及发卡行主机系统 7 的交互，实现智能卡 4 上可用余额的自动充值，同时发卡行主机系统 7 冻结保留智能卡 4 主账户的可用资金，以保证智能卡 4 脱机支付金额不超过账户限额；

[0018] 在脱机交易过程中，所述受理终端 5 扣减智能卡 4 上的可用余额，并生成日终入账记录文件，通过受理行主机系统 6 定期上送到发卡行主机系统 7，实现银行卡账户资金的处理与清算。

[0019] 上述方案中，所述智能卡 4 包括依次连接的第二通讯单元、第二安全单元、第二运算单元和第二存储单元，其中：

[0020] 第二通讯单元，用于实现智能卡与受理终端之间的信息交换，其通讯形式是以智能卡上的芯片触点进行，或者是通过第二通讯单元中的天线与受理终端上的电线进行无线电通信；

[0021] 第二安全单元，用于实现智能卡与受理终端之间的安全认证，验证受理终端的有效性，保证智能卡存储单元中的数据不会被非法篡改，并在交易完成之后生成数字签名，增强交易的不可抵赖性；

[0022] 第二运算单元，用于对交易金额、交易货币种类以及智能卡中存储的可用余额、货币种类信息进行判定和比较，决定是否允许继续对交易进行处理；

[0023] 第二存储单元，用于存储智能卡的基本信息，包括帐号、持卡人姓名、智能卡有效期、持卡人个人标识号 PIN、可用余额和智能卡自动充值阈值信息，供第二运算单元读取和更改。

[0024] 上述方案中，所述第二存储单元受第二安全单元的控制，在通过安全验证之后，方可被有条件的读取和修改。

[0025] 上述方案中，所述智能卡 4 是银行发行的芯片卡。

[0026] 上述方案中，所述银行发行的芯片卡是借记卡，或是贷记卡。

[0027] 上述方案中，所述受理终端与所述智能卡之间采用如下相互认证的安全机制：由

证书签发机构来定义根 CA 的公私钥，利用根 CA 的私钥对发卡行公钥签发发卡行证书；发卡行生成 IC 卡上公私钥对、按照一定的规则指定敏感的应用数据，作为需要被认证的静态行业数据；利用发卡行私钥对 IC 卡公钥和静态行业应用数据签发 IC 卡证书，并将 IC 卡私钥、IC 卡证书和发卡行证书被保存于 IC 卡内；交易受理银行主机系统将由证书签发机构签发的根 CA 公钥部署于 IC 受理终端内，在实际应用时，受理终端利用其内的行业根 CA 先验证发卡行证书，通过后获得有效的发卡行公钥；受理终端利用发卡行公钥认证 IC 卡证书，通过后获得有效的 IC 卡公钥及静态行业数据；受理终端再发送动态数据给智能卡，该动态数据是随机数，智能卡利用 IC 卡私钥对指定数据和终端动态数据进行签名，并送给受理终端；IC 受理终端利用获得的 IC 卡公钥对 IC 卡生成的签名进行确认。

[0028] 为达到上述目的的另一个方面，本发明提供了一种基于银行智能卡实现快速支付的方法，包括：

[0029] 步骤 1：受理终端与智能卡之间进行相互认证；

[0030] 步骤 2：认证通过后，受理终端发起指令扣减智能卡中保存的可支付余额，并保存和记录支付信息；

[0031] 步骤 3：受理终端定期将所有支付信息传递到受理行主机系统，由受理行主机系统与发卡行主机系统进行资金往来清算。

[0032] 上述方案中，所述步骤 1 具体包括：

[0033] 步骤 100：在受理终端输入交易金额，受理终端与智能卡进行通信连接并向智能卡发送交易请求；

[0034] 步骤 101：智能卡接收受理终端的交易请求；

[0035] 步骤 102：智能卡对交易请求信息进行校验和判别；

[0036] 步骤 103：智能卡检查受理终端是否支持快速安全支付功能、受理终端的安全报文是否能通过认证；如果通过检查，则执行步骤 104；如果不能通过检查，则向受理终端返回交易失败，结束本流程；

[0037] 步骤 104：智能卡将交易处理情况返回受理终端；

[0038] 步骤 105：受理终端接收智能卡的返回信息；

[0039] 步骤 106：受理终端对智能卡的返回信息进行判别，校验智能卡的真实有效性，智能卡有效则继续处理，否则拒绝交易，结束本流程。

[0040] 上述方案中，所述步骤 2 具体包括：

[0041] 步骤 107：受理终端判断智能卡中的快速支付可用余额是否足够支付，如果足够支付，则继续处理；否则，退出支付交易处理，对智能卡进行充值；

[0042] 步骤 108：受理终端处理完毕后，向智能卡发起扣款指令；

[0043] 步骤 109：智能卡接收扣款指令；

[0044] 步骤 110：智能卡扣减自身可用余额，并生成当前交易的数字签名信息；

[0045] 步骤 111：智能卡将扣款结果、交易数字签名返回受理终端；

[0046] 步骤 112：受理终端接收信息，并将其在存储单元中保存；

[0047] 步骤 113：受理终端显示支付交易完成，并根据实际需要，打印支付交易凭证。

[0048] 上述方案中，步骤 107 中所述对智能卡进行充值，具体包括：

[0049] 步骤 201：受理终端将智能卡充值请求上送给受理行主机系统，并最终传送到发

卡行主机系统，由发卡行主机系统对银行卡账户进行资金冻结，扣减主账户可用余额；

[0050] 步骤 202：受理终端接收发卡行主机系统返回的充值请求处理结果，

[0051] 步骤 203：受理终端向智能卡发起充值指令；

[0052] 步骤 204：智能卡接收充值指令；

[0053] 步骤 205：智能卡增加可用余额至自动充值最大金额，并生成当前交易的数字签名信息；

[0054] 步骤 206：智能卡将充值结果、交易数字签名返回受理终端；

[0055] 步骤 207：受理终端显示充值交易完成，并根据实际需要，打印充值交易凭证，充值处理结束。

[0056] 上述方案中，步骤 3 中所述受理终端定期将所有支付信息传递到受理行主机系统，是通过网络或其他移动存储设备实现的。

[0057] （三）有益效果

[0058] 本发明提供的这种基于银行智能卡实现快速支付的系统及方法，其与传统的银行磁条卡交易相比，有如下几方面的优势：

[0059] （一）交易迅速

[0060] 一般情况下，为了对银行卡真伪以及账户资金情况等信息进行验证，受理终端都会将录入的信息（含从银行卡磁道获取的信息）通过电话拨号网络送至发卡银行后台主机系统进行验证，之后才能决定是否允许交易。这样，在交易过程中需要由销售点终端 (POS) 机具通过电话网络拨号的形式与银行后台连接进行数据信息传递交换，通常，完成一个交易在网络传输上所花费的时间在 10 秒左右。

[0061] 而在本发明中，先对持卡人银行卡资金账户中的一部分金额进行保留（冻结），然后将这个金额写入银行卡的智能芯片中。当客户交易时，直接由 POS 机具扣减智能卡芯片中保存的余额，不需用和银行主机系统进行连接。这样，可以极大的缩短交易时间。

[0062] （二）安全性高

[0063] 传统的银行磁条卡中，所有的信息都以规定的格式存放在智能卡磁道中。受这种信息存储方式的制约，磁道中所有信息都可以被任意读取、写入。因而，以智能卡克隆为作案手段的伪卡案件时有发生。在本发明中，数据存储在智能卡芯片中，并采用一整套完善的安全加密体系，一方面智能卡不能被复制、另一方面受理终端可以和智能卡进行相互认证，保证了交易双方的真实、有效性。同时，交易完成之后智能卡可以生成数字签名，降低了抵赖的风险。

[0064] （三）实施简便

[0065] 与目前广泛使用的以对称密钥 (DES、Data Encryption Standard) 加密体系的智能卡不同，本发明中提出的支付系统中，将引入非对称 (RSA、Rivest、Sharmir 和 Adleman 提出的一种非对称密钥算法）加密体系以及动态数据认证 (DDA、Dynamic Data Authentication) 技术，在充分保证安全性的同时，安装实施也比较简单。因为，在对称密钥体系下，所有的终端都需要保存完整的密钥信息，一旦密钥信息被不法获取，那么就可以轻易的制作出伪冒卡；然而，在非对称密钥安全体系下，终端仅保存公钥，因而对终端密钥保存的要求就相对比较宽松。一般的，传统模式下为了防止终端上存储的密钥被不法获取，密钥一般都保存在一张特殊的智能卡 --SAM 卡（安全存取模块、Secure Access Module) 上，

并且需要对该智能卡进行严格的管理；而采用本发明中所述的方法后，由于终端仅保存公钥信息，那么对终端密钥安全性的要求就降低了很多，例如，密钥可以以文件的形式存储在终端存储器上，也可以通过网络或者其他方式灵活的更新、下载。

附图说明

[0066] 图 1 是本发明提供的基于银行智能卡实现快速支付系统的结构示意图；

[0067] 图 2 是本发明中具备快速安全支付功能的受理终端的结构示意图；

[0068] 图 3 是本发明中具备快速安全支付功能的智能卡的结构示意图；

[0069] 图 4 是本发明中安全认证体系的结构示意图；

[0070] 图 5 是本发明提供的基于银行智能卡实现快速支付方法的流程图；

[0071] 图 6 是依照本发明实施例提供的基于银行智能卡实现快速支付的方法流程图；

[0072] 图 7 是依照本发明实施例对智能卡进行充值的方法流程图。

具体实施方式

[0073] 为使本发明的目的、技术方案和优点更加清楚明白，以下结合具体实施例，并参照附图，对本发明进一步详细说明。

[0074] 本发明提供了一种基于智能卡实现快速支付的系统及方法，基于银行智能卡与受理终端的安全认证，在智能卡联机交易环境的过程中，实现智能卡上可用余额的自动充值，同时冻结保留银行卡主账户的可用资金，以保证智能卡脱机支付金额不超过账户限额；在智能卡脱机消费过程中，快速扣减智能卡上的可用余额，并生成日终入账记录文件，定期上送到银行主机，完成银行卡账户资金的处理与清算。

[0075] 如图 1 所示，图 1 是本发明提供的基于银行智能卡实现快速支付系统的结构示意图，该系统包括：发卡行主机系统 7、受理行主机系统 6、受理终端 5 和具备快速安全支付功能的智能卡 4，其中，发卡行主机系统 7 与受理行主机系统 6 之间通过银行间网络连接，受理行主机系统 6 与受理终端 5 之间通过银行外部网络连接，受理终端 5 与智能卡 4 之间通过接触式或非接触式连接。

[0076] 在联机交易过程中，所述受理终端 5 扣减智能卡 4 上的可用余额，并判断智能卡 4 的可用余额的大小，通过与受理行主机系统 6 及发卡行主机系统 7 的交互，实现智能卡 4 上可用余额的自动充值，同时发卡行主机系统 7 冻结保留智能卡 4 主账户的可用资金，以保证智能卡 4 脱机支付金额不超过账户限额。在脱机交易过程中，所述受理终端 5 扣减智能卡 4 上的可用余额，并生成日终入账记录文件，通过受理行主机系统 6 定期上送到发卡行主机系统 7，实现银行卡账户资金的处理与清算。

[0077] 发卡行主机系统 7 包括依次连接的充值处理装置 1、数据存储装置 2 和账务处理装置 3。其中：充值处理装置 1，用于对智能卡 4 进行可用余额充值处理，并将一定金额的账户余额予以冻结保留，且该保留金额会被记录智能卡 4 的芯片中；数据存储装置 2，用于登记并存储银行卡账户资料信息，至少包括银行卡的账户可用余额和冻结金额等信息；账务处理装置 3，用于发卡行的卡账户资金的入账处理，当脱机快速支付后，所有支付信息数据会传递到发卡行主机系统 7 的账务处理装置 3，账务处理装置 3 判断支付数据的有效性，并完成卡账户资金的入账处理，包括解除账户冻结金额和扣减账户余额等处理。受理行主机系

统 6 用于完成智能卡 4 交易的转发以及与发卡行主机系统 7 的资金清算。

[0078] 如图 2 所示，受理终端 5 是能够受理智能卡的交易终端，包括但不限于是 POS 机或 IC 卡读卡设备等，由并联连接的第一通讯单元、第一安全单元、第一运算单元、第一输入输出单元和第一存储单元构成，其中，第一通讯单元用于与智能卡进行通讯，第一安全单元用于与智能卡进行安全认证，第一运算单元用于对交易金额进行计算处理，第一输入输出单元用于交易信息的录入以及交易结果的反馈，第一存储单元用于记录交易信息以便定期上传至受理银行主机系统。

[0079] 如图 3 所示，智能卡 4 包括依次连接的第二通讯单元、第二安全单元、第二运算单元和第二存储单元。其中：

[0080] 第二通讯单元，用于实现智能卡与受理终端之间的信息交换，其通讯形式是以智能卡上的芯片触点进行，或者是通过第二通讯单元中的天线与受理终端上的电线进行无线电通信。

[0081] 第二安全单元，用于实现智能卡与受理终端之间的安全认证，验证受理终端的有效性，保证智能卡存储单元中的数据不会被非法篡改，并在交易完成之后生成数字签名，增强交易的不可抵赖性。

[0082] 第二运算单元，用于对交易金额、交易货币种类以及智能卡中存储的可用余额、货币种类信息进行判定和比较，决定是否允许继续对交易进行处理。

[0083] 第二存储单元，用于存储智能卡的基本信息，包括帐号、持卡人姓名、智能卡有效期、持卡人个人标识号 PIN、可用余额和智能卡自动充值阈值信息，供第二运算单元读取和更改。第二存储单元受第二安全单元的控制，在通过安全验证之后，方可被有条件的读取和修改。

[0084] 智能卡 4 主要是银行发行的芯片卡，可以是借记卡，也可以是贷记卡。

[0085] 图 4 中，描述了智能卡和受理终端相互认证的安全机制。其中，由证书签发机构来定义根 CA 的公私钥，利用根 CA 的私钥对发卡行公钥签发发卡行证书；发卡行生成 IC 卡上公私钥对、按照一定的规则指定敏感的应用数据，作为需要被认证的静态行业数据；利用发卡行私钥对 IC 卡公钥和静态行业应用数据签发 IC 卡证书，并将 IC 卡私钥、IC 卡证书和发卡行证书被保存于 IC 卡内；交易受理银行主机系统将由证书签发机构签发的根 CA 公钥部署于 IC 受理终端内，在实际应用时，受理终端利用其内的行业根 CA 先验证发卡行证书，通过后获得有效的发卡行公钥；受理终端利用发卡行公钥认证 IC 卡证书，通过后获得有效的 IC 卡公钥及静态行业数据；受理终端再发送动态数据给智能卡，该动态数据是随机数，智能卡利用 IC 卡私钥对指定数据和终端动态数据进行签名，并送给受理终端；IC 受理终端利用获得的 IC 卡公钥对 IC 卡生成的签名进行确认。

[0086] 图 5 是本发明提供的基于银行智能卡实现快速支付方法的流程图，该方法包括：

[0087] 步骤 1：受理终端与智能卡之间进行相互认证；

[0088] 步骤 2：认证通过后，受理终端发起指令扣减智能卡中保存的可支付余额，并保存和记录支付信息；

[0089] 步骤 3：受理终端定期将所有支付信息传递到受理行主机系统，由受理行主机系统与发卡行主机系统进行资金往来清算。

[0090] 图 6 是依照本发明实施例提供的基于银行智能卡实现快速支付的方法流程图，其

具体步骤如下：

[0091] 步骤 100：商户收银员在销售点的受理终端输入交易金额，在受理终端插入具有快速安全支付功能的智能卡（或将具备非接触通讯功能的智能卡放入支付设备的射频感应区），受理终端向智能卡发送交易请求；

[0092] 步骤 101：智能卡接收受理终端的交易请求；

[0093] 步骤 102：智能卡对交易请求信息进行校验和判别；

[0094] 步骤 103：智能卡检查受理终端是否支持快速安全支付功能、受理终端的安全报文是否能通过认证；如果不能通过检查，则向受理终端返回交易失败；

[0095] 步骤 104：智能卡将交易处理情况返回受理终端；

[0096] 步骤 105：受理终端接收智能卡的返回信息；

[0097] 步骤 106：受理终端对智能卡的返回信息进行判别，校验智能卡的真实有效性，智能卡有效则继续处理，否则拒绝交易；

[0098] 步骤 107：受理终端判断卡中的快速支付可用余额足够支付，则继续处理；否则退出支付交易处理，并进行步骤 115；

[0099] 步骤 108：受理终端处理完毕后，向智能卡发起扣款指令；

[0100] 步骤 109：智能卡接收扣款指令；

[0101] 步骤 110：智能卡扣减自身可用余额，并生成当前交易的数字签名信息；

[0102] 步骤 111：智能卡将扣款结果、交易数字签名返回受理终端；

[0103] 步骤 112：受理终端接收信息，并将其在存储单元中保存；

[0104] 步骤 113：受理终端显示支付交易完成，并根据实际需要，打印支付交易凭证。

[0105] 步骤 114：受理终端判断智能卡快速支付余额是否小于智能卡快速支付金额阈值，如小于，则进行步骤 115；否则交易结束；

[0106] 步骤 115：受理终端判断是否具有联机交易环境，是则进行步骤 116，否则交易终止；

[0107] 步骤 116：受理终端将智能卡充值请求上送给受理行主机，并最终传送到发卡行主机系统，由发卡行主机系统对银行卡账户进行资金冻结，扣减主账户可用余额；

[0108] 步骤 117：受理终端接收发卡行主机系统返回的充值请求处理结果，

[0109] 步骤 118：受理终端向智能卡发起充值指令；

[0110] 步骤 119：智能卡接收充值指令；

[0111] 步骤 120：智能卡增加可用余额至自动充值最大金额，并生成当前交易的数字签名信息；

[0112] 步骤 121：智能卡将充值结果、交易数字签名返回受理终端；

[0113] 步骤 122：受理终端显示充值交易完成，并根据实际需要，打印充值交易凭证，充值处理结束。

[0114] 图 7 是依照本发明实施例对智能卡进行充值的方法流程图，详细情况如下：

[0115] 图 7-1：持有具备快速安全支付功能智能卡的客户，假设初始状态下主账户的可用余额（额度）为 1000 元；

[0116] 图 7-2：客户在银行提供的受理终端上发起充值交易（假设充值 200 元），交易成功后扣减主账户可用余额至 800 元，增加快速支付可用余额至 200 元；

[0117] 图 7-3 :客户在支持快速支付的受理终端进行消费（消费 150 元），交易成功后扣减智能卡上储存的快速支付可用余额至 50 元。

[0118] 图 7-4 :银行可以为客户提供自动充值的服务，例如，当智能卡快速支付可用余额小于 60 元时，如果智能卡发生连接发卡行后台主机系统的交易，则自动将快速支付可用余额增加到 200 元，并同时扣减主账户的可用余额 ；

[0119] 图 7-5 :客户也可以发起减值交易，释放智能卡的快速支付可用余额，增加主账户的可用余额。

[0120] 以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

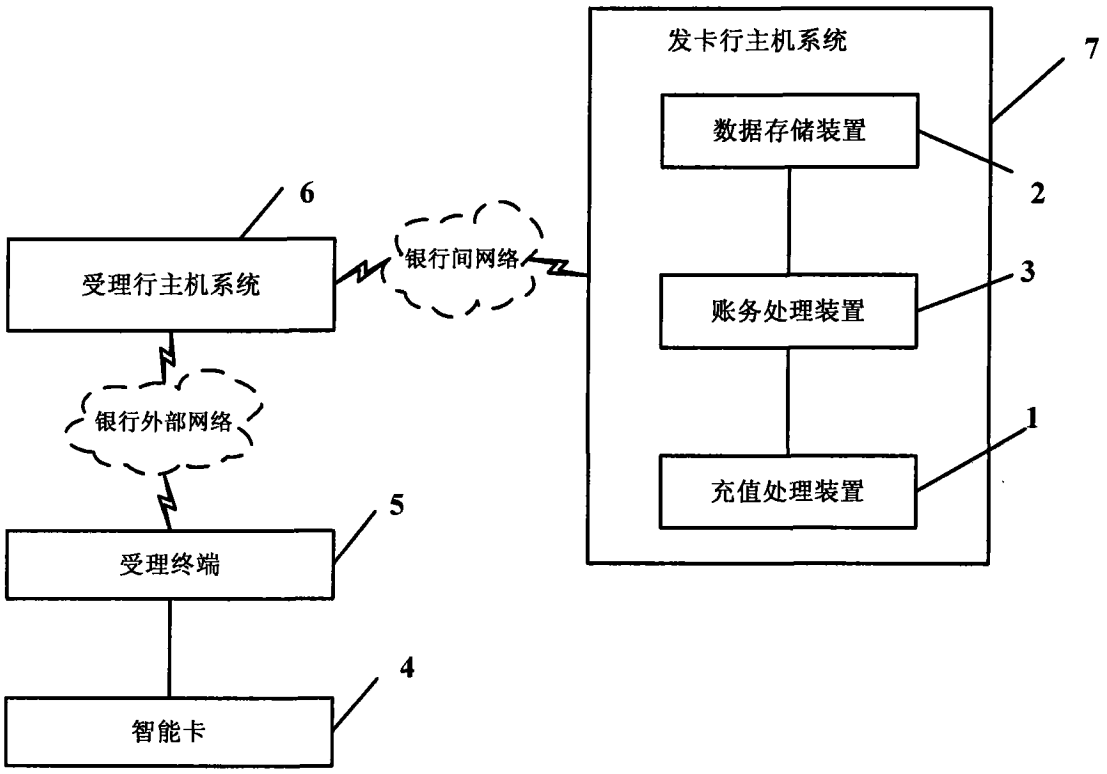

发卡行主机系统
7
数据存储装置
2
账务处理装置
3
充值处理装置
1
6
受理行主机系统
银行间网络
银行外部网络
5
受理终端
4
智能卡

图 1

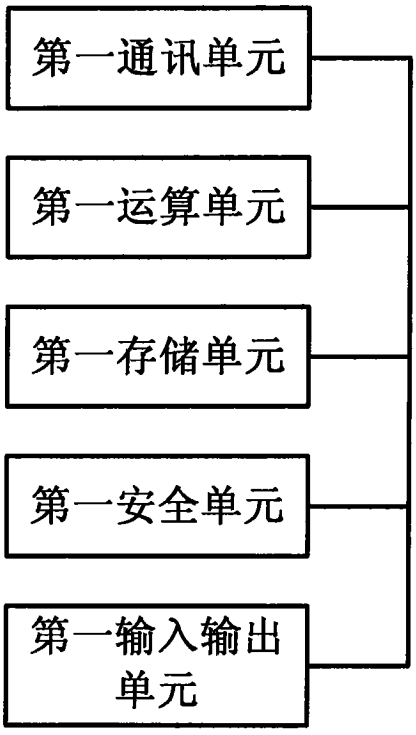

第一通讯单元
第一运算单元
第一存储单元
第一安全单元
第一输入输出单元

图 2

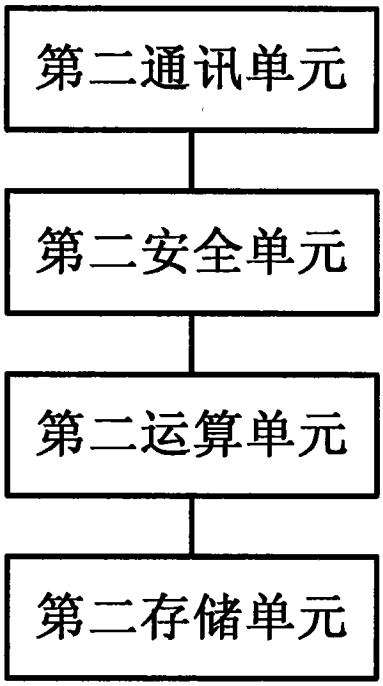

第二通讯单元
第二安全单元
第二运算单元
第二存储单元

图 3

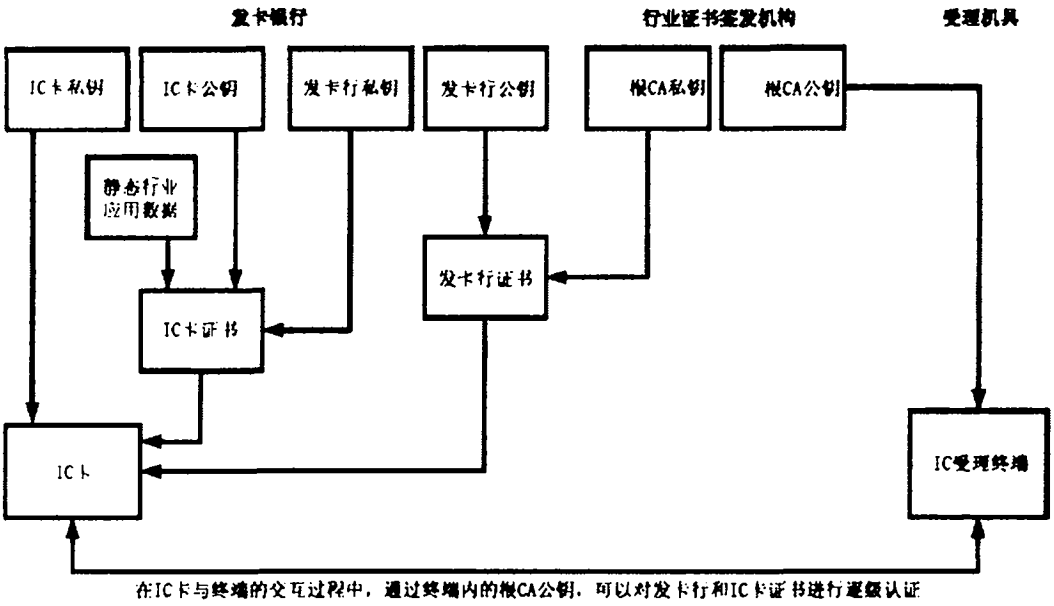

发卡银行
行业证书签发机构
受理机具
IC卡私钥
IC卡公钥
发卡行私钥
发卡行公钥
根CA私钥
根CA公钥
静态行业应用数据
发卡行证书
IC卡证书
IC卡
IC受理终端
在IC卡与终端的交互过程中，通过终端内的根CA公钥，可以对发卡行和IC卡证书进行逐级认证

图 4

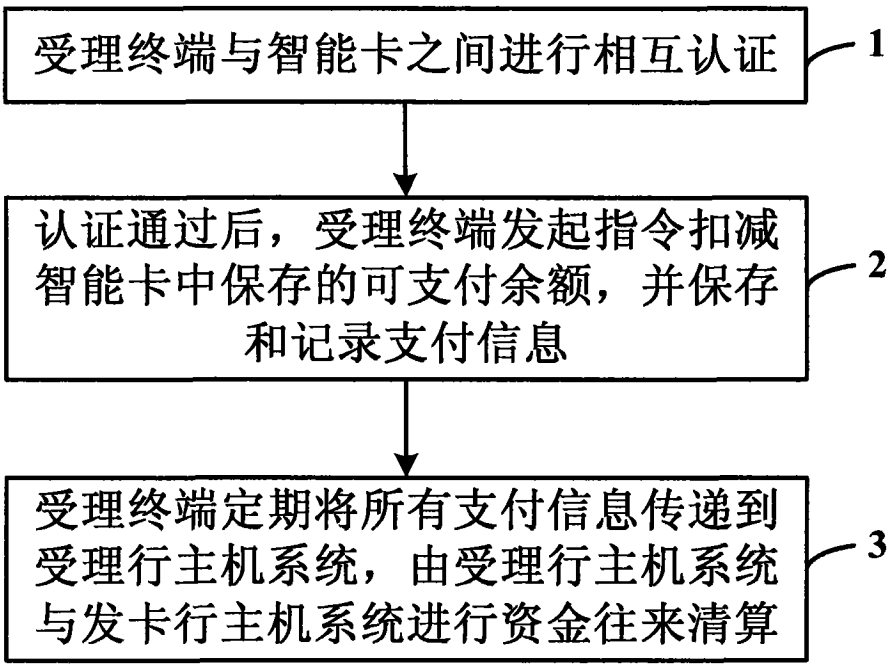

受理终端与智能卡之间进行相互认证
1
认证通过后，受理终端发起指令扣减智能卡中保存的可支付余额，并保存和记录支付信息
2
受理终端定期将所有支付信息传递到受理行主机系统，由受理行主机系统与发卡行主机系统进行资金往来清算
3

图 5

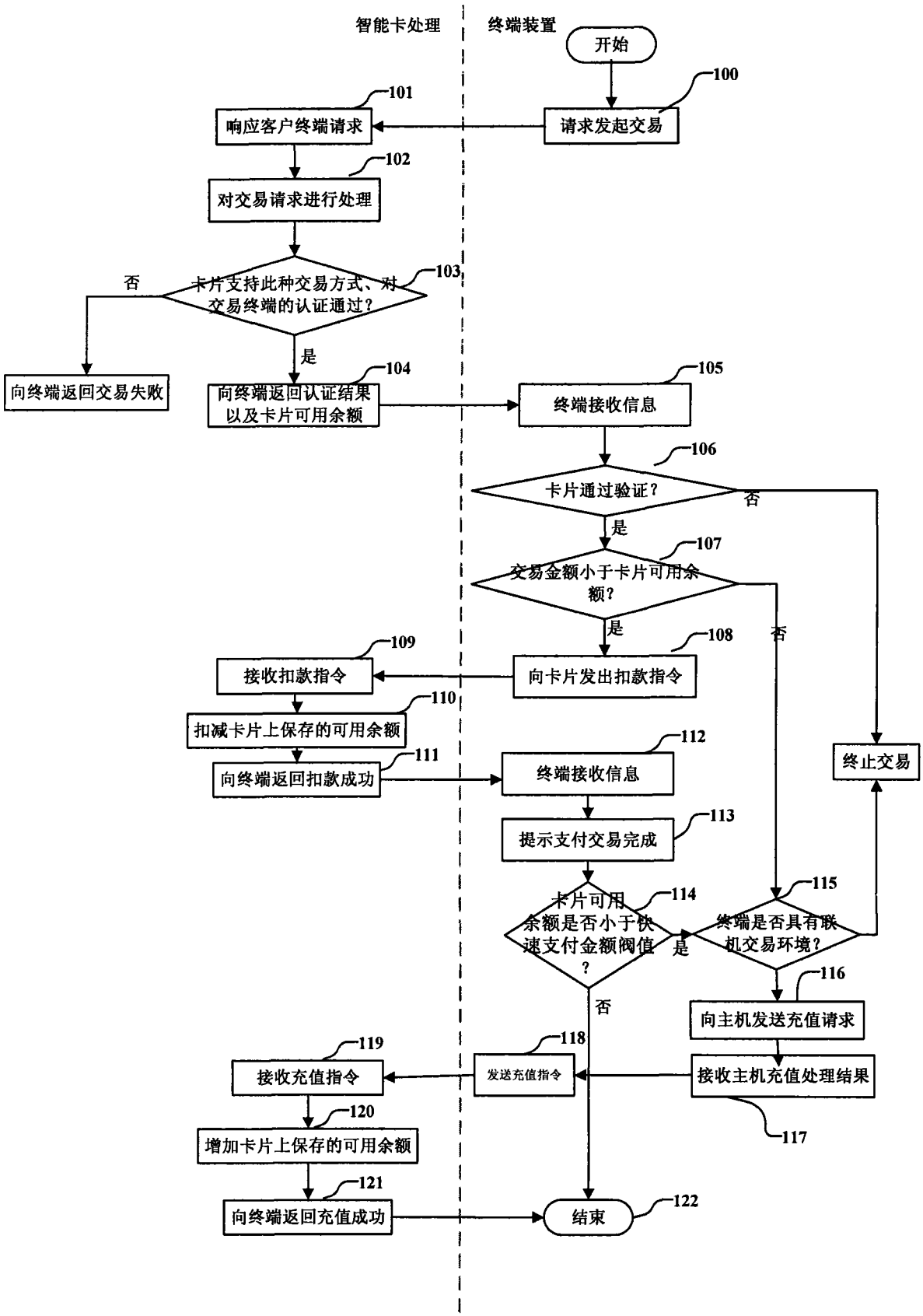

智能卡处理
终端装置
开始
100
请求发起交易
101
响应客户终端请求
102
对交易请求进行处理
103
卡片支持此种交易方式、对交易终端的认证通过？
否
是
向终端返回交易失败
104
向终端返回认证结果以及卡片可用余额
105
终端接收信息
106
卡片通过验证？
否
是
107
交易金额小于卡片可用余额？
否
是
108
向卡片发出扣款指令
109
接收扣款指令
110
扣减卡片上保存的可用余额
111
向终端返回扣款成功
112
终端接收信息
113
提示支付交易完成
114
卡片可用余额是否小于快速支付金额阀值？
是
否
115
终端是否具有联机交易环境？
否
是
116
向主机发送充值请求
117
接收主机充值处理结果
118
发送充值指令
119
接收充值指令
120
增加卡片上保存的可用余额
121
向终端返回充值成功
122
结束
终止交易

图 6

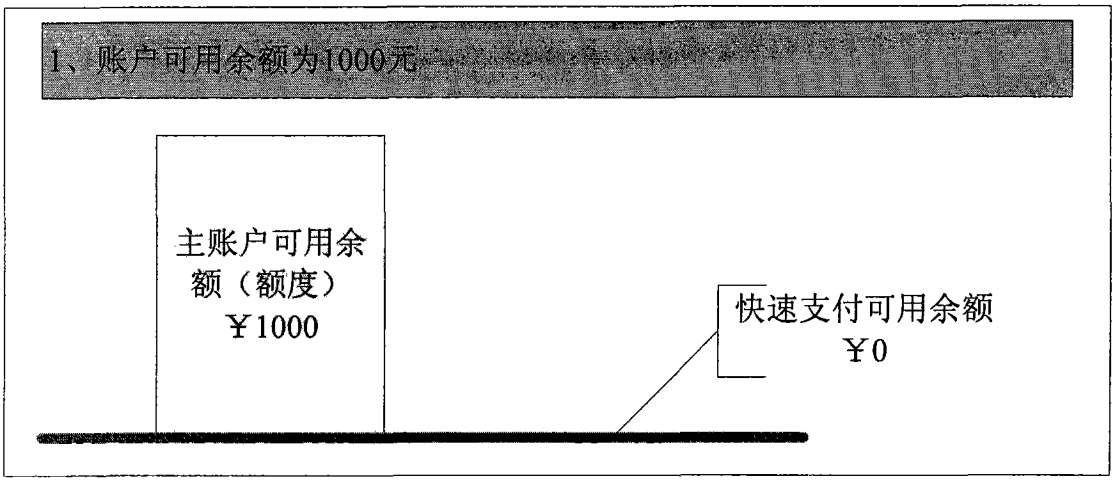

1、账户可用余额为1000元。
主账户可用余额（额度）
￥1000
快速支付可用余额
￥0

图 7-1

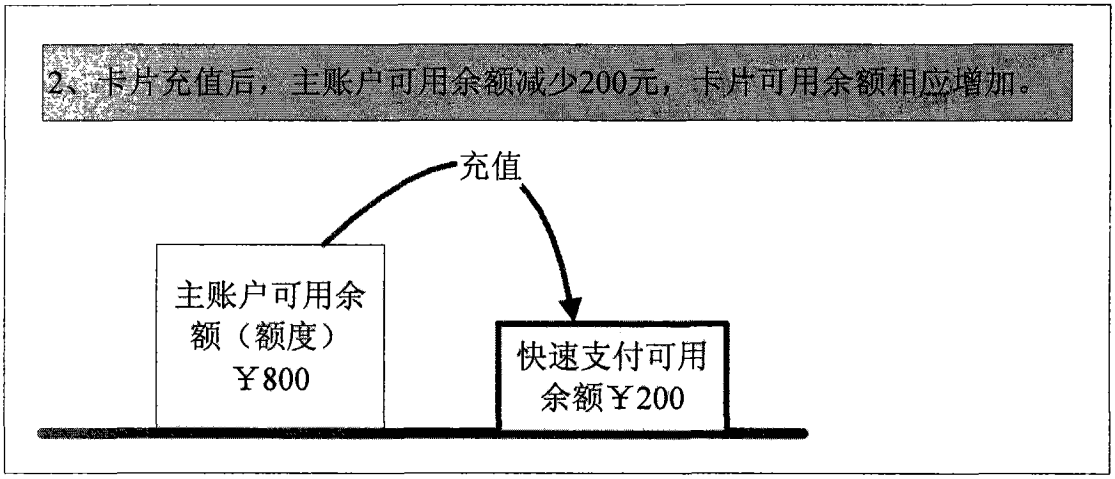

2、卡片充值后，主账户可用余额减少200元，卡片可用余额相应增加。
充值
主账户可用余额（额度）
￥800
快速支付可用余额￥200

图 7-2

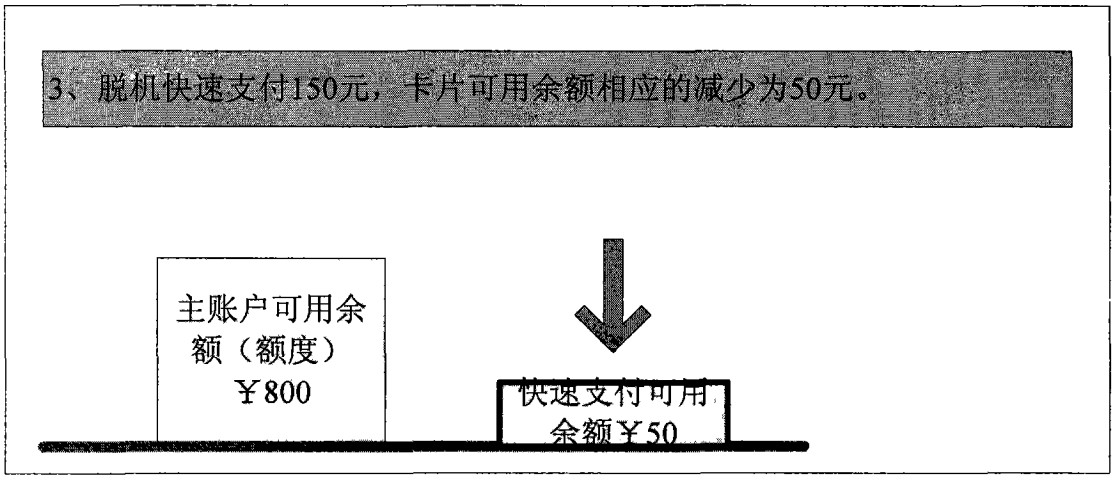

3、脱机快速支付150元，卡片可用余额相应的减少为50元。
主账户可用余额（额度）
￥800
快速支付可用余额￥50

图 7-3

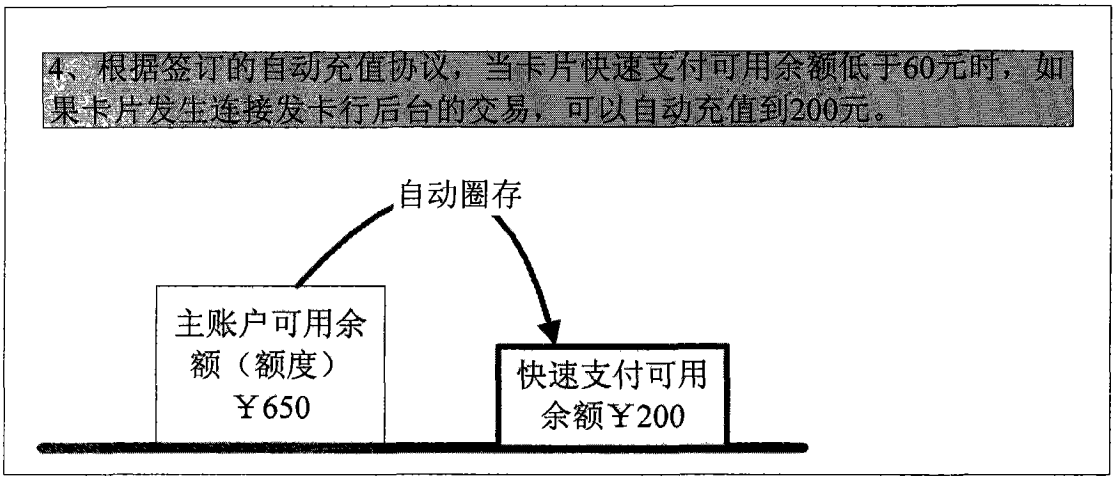

4、根据签订的自动充值协议，当卡片快速支付可用余额低于60元时，如果卡片发生连接发卡行后台的交易，可以自动充值到200元。
自动圈存
主账户可用余额（额度）
￥650
快速支付可用余额￥200

图 7-4

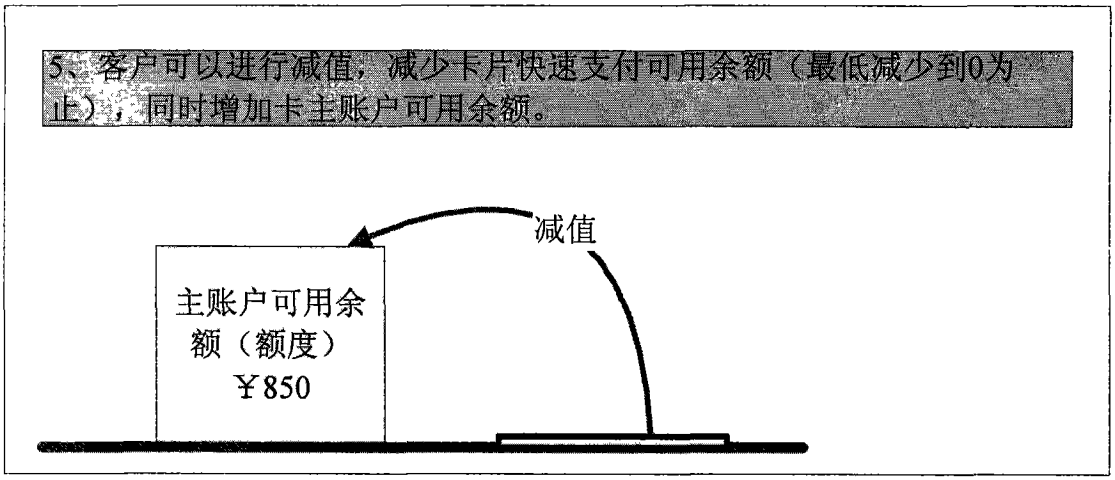

5、客户可以进行减值，减少卡片快速支付可用余额（最低减少到0为止），同时增加卡主账户可用余额。
减值
主账户可用余额（额度）
￥850

图 7-5