[19]中华人民共和国专利局

[51]Int.Cl[6]
G07F 7/08
G06F 17/60

[12] 发明专利申请公开说明书

[21] 申请号 96194231.2

[43]公开日 1998 年 6 月 24 日

[11] 公开号 CN 1185851A

[22]申请日 96.4.19
[30]优先权
[32]95.4.21 [33]US[31]08/427,287
[86]国际申请 PCT/US96/05521 96.4.19
[87]国际公布 WO96/33476 英 96.10.24
[85]进入国家阶段日期 97.11.27
[71]申请人 国有花旗银行
地址 美国纽约州
[72]发明人 肖伦姆S·罗森

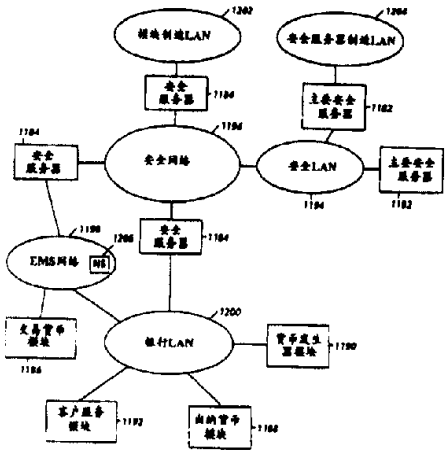
[74]专利代理机构 上海专利商标事务所
代理人 张政权

权利要求书 19 页 说明书 32 页 附图页数 54 页

[54]发明名称 电子货币系统

[57]摘要

一种电子货币系统，包括（1）与货币发生器装置耦合的银行或金融机构，为认购客户产生和发行电子货币，包括被活期存款和电子信用权威机构返回的电子货币；（2）接受和分配电子货币的代理银行；（3）被认购者使用的多个交易装置，用于存储电子货币、与参与银行的联机系统进行货币交易或者在脱机交易中与类似于交易装置的其它装置兑换电子货币；（4）与发行和代理银行有关的出纳装置，用于交易装置与发行和代理银行的手续处理和接口，以及发行与代理银行自身之间的接口；（5）平衡不同发行银行的电子货币帐户的清算银行；（6）给系统的所有部件提供通信服务的数据通信网络；以及（7）维持系统的完整性，探测系统中伪造和篡改的安全性配置。本发明的一个实施例包括处理遗失货币索赔和将帐户与货币模块联系起来以提供银行存取的客户服务装置。



权 利 要 求 书

1.一种在基于处理器的电子模块之间转移电子票据的系统，包括:

基于处理器的电子模块，每一个模块能够产生一个加密的安全通道并通过所述的加密安全通道转移和接收电子票据，所述的每一个电子模块有一个存储所述电子票据的存储器;

其特征在于：存储的每一个电子票据包括:

一组实体数据字段，它包含与所述电子票据有关的货币价值的数据指示;

一组转移数据字段，它包含一列转移记录，每一个转移记录是由转移者的电子模块产生的，包括一个区分被转移电子票据与从所述转移者电子模块转移的其它被转移电子票的流水号。

2.如权利要求 1 所述的系统，其特征在于：所述的货币价值是一个与所述电子票据有关的原始货币价值，所述的转移记录进一步包括一个被转移的货币价值。

3.一种利用第一货币模块把货币的电子表征转移到第二货币模块的支付方法，包括下列步骤:

(a)在所述的第一货币模块与所述的第二模块之间建立一个加密的安全对话，所述的第一和第二货币模块是防篡改的模块;

(b)所述的第二货币模块提示第二认购者交易项目，所述的第二认购者将交易项目提供给所述的第二货币模块;

(c)所述的第二货币模块通过所述的加密安全对话把所述的交易项目送给所述的第一货币模块;

(d)所述的第一货币模块提示第一认购者核实所述的交易项目，所述的第一认购者提供所述交易项目的核实;

(e)所述的第一货币模块通过所述的加密安全对话把所述的货币电子表征转移到所述的第二货币模块;

(f)所述的第一货币模块通过记录所述的电子货币转移委托所述电子货币转移，从而使所述的第一货币模块不再能够通过重新还原其状态而中止所述电子货币转移;

(g)所述的第二货币模块通过记录所述的电子货币转移委托所述电子货币转

移，从而使所述的第二货币模块不再能够通过重新还原其状态而中止所述电子货币转移；

4.如权利要求 3 所述的支付方法，其特征在于：所述的交易项目包括所述货币电子表征的货币金额，所述第一认购者提供核实的所述步骤包括在信用与通货之间指定所述货币金额的分摊。

5.一种在基于处理器的电子模块之间转移电子票据的方法，包括下列步骤：

在转移者电子模块与受移者电子模块之间建立一个加密安全对话；

通过把转移记录添加到存储在所述转移者电子模块中的电子票据上，创建一个转移电子票据，所述的转移记录表示所述电子票据的全部或部分货币金额是否正在被转移；

把所述的转移电子票据从所述的转移者电子模块转移到所述的受移者电子模块；以及

其特征在于：所述的转移记录包括一个区分所述转移电子票据与所述转移者电子模块的另一转移电子票据的流水号。

6.一种在具有将所述电子模块与安全服务器联系起来的网络服务器的电子货币系统网络上签字的电子模块方法，包括下列步骤：

所述的电子模块将其证书发送给所述的网络服务器；

所述的网络产生一个随机密钥和一个随机核实数，将包含所述证书、所述随机密钥和所述随机核实数的加密信息发送给所述的安全服务器；

所述的安全服务器对所述的加密信息解密，存储所述的随机密钥和随机核实数，并核实所述证书的有效性；

所述的安全服务器建立与所述电子模块的安全通信对话；

所述的安全服务器将更新的安全信息发送给所述的电子模块，该信息是由所述安全服务器的加密密钥以数字方式签字的；

所述的电子模块核实所述数字签字更新安全信息的有效性，用所述的更新安全信息更新所存储的安全信息；

所述的安全服务器将所述随机密钥和所述随机核实数发送给所述的电子模块，并结束所述的安全通信对话；

通过用所述的随机密钥对所述随机核实数和终点加密，所述的电子模块产生一个终点信息，把所述的终点信息发送给所述的网络服务器；

所述的网络服务器对所述的信息解密，并核实所述的随机核实数；

所述的网络服务器建立与所述终点的联系。

7.如权利要求 6 所述的方法，其特征在于：所述的电子模块是交易模块、客户服务模块、货币发生器模块或出纳模块。

8.如权利要求 6 所述的方法，进一步包括下列步骤：

所述的电子模块将其日期和时间信息发送给所述的安全服务器；

所述的安全服务器检查所述的日期和时间信息，确定它是否在可接受的预定参数的之外；以及

所述日期和时间信息在所述可接受预定参数之外，所述的安全服务器将新的日期和时间发送给所述的电子模块，以便与所述的电子模块实现同步。

9. 如权利要求 6 所述的方法，其特征在于：在所述网络服务器与所述安全服务器之间的所述加密信息是利用存储在所述网络服务器中和所述安全服务器中的局部对称密钥提供的。

10. 如权利要求 6 所述的方法，其特征在于：所述的更新安全信息包括不好的电子模块和安全服务器识别数的更新表、公共密钥的更新表以及更新的密钥长度。

11. 如权利要求 6 所述的方法，其特征在于：所述安全服务器建立与所述电子模块安全通信对话的所述步骤包括向所述安全服务器和所述电子模块提供对话公共密钥的公共密钥交换协议。

12. 如权利要求 6 所述的方法，其特征在于：进一步包括所述安全服务器重新证明所述证书的步骤。

13. 如权利要求 12 所述的方法，其特征在于：响应于所述安全服务器将重新证明请求信息发送给所述电子模块，产生所述的重新证明步骤。

14. 如权利要求 12 所述的方法，其特征在于：所述的证书包括期满时间；响应于所述电子模块确定所述证书已经期满，发生所述的重新证明的步骤。

15.一种基于电子模块的货币交易系统，包括：

一个主要安全服务器；

多个次要安全服务器，每一个次要安全服务器有一个由所述主要安全服务器数字签字的唯一安全服务器证书；

多个防止篡改的电子模块，每一个模块有一个由所述次要安全服务器中的一

个数字签字的唯一模块证书；一个存储货币电子表征的存储器；以及一个用于给转移和接收所述货币电子表征提供加密安全通道的处理器；

其特征在于：所述的安全服务器证书是根据所述次要安全服务器与所述电子模块或者与所述主要安全服务器相互作用而生效的；

所述的模块证书是根据所述电子模块与所述其它电子模块或者与所述安全服务器相互作用而生效的。

16. 如权利要求 15 所述的系统，其特征在于：所述模块证书和所述安全服务器证书具有期满时间；所述电子模块不适合与具有已期满证书的其它电子模块或次要安全服务器交易。

17. 如权利要求 15 所述的系统，其特征在于：所述多个电子模块中的每一个、所述主要安全服务器、以及所述多个次要安全服务器中的每一个都有一个唯一的服务器类型或电子模块类型的标识符指示。

18. 如权利要求 17 所述的系统，其特征在于：所述的电子模块类型包括：交易模块、客户服务模块、货币发生器模块、以及出纳模块，所述的服务器类型包括：所述的主要安全服务器和所述的次要安全服务器。

19. 如权利要求 17 所述的系统，其特征在于：所述的每一个服务器类型和所述的每一个电子模块类型是与一个类型变量的唯一范围相联系的；所述的每一个唯一标识符在所述的唯一范围内映射到所述类型变量的一个值，根据安全地存储在每一个所述电子模块、每一个所述次要服务器以及所述主要服务器中的映射机制，分配所述服务器类型或者电子模块类型。

20. 如权利要求 19 所述的系统，其特征在于：所述的每一个唯一标识符是一个小于预定素数的唯一整数值；所述类型变量的所述值是根据在对预定素数取模运算下将所述素数的本原根升幂所述唯一标识符而产生的；所述多个电子模块中的每一个、所述主要安全服务器、以及所述多个次要安全服务器中的每一个安全地存储所述的本原根和所述的素数。

21. 如权利要求 15 所述的系统，其特征在于：所述的主要安全服务器维持不好的电子模块和不好的次要安全服务器的所述唯一标识符的表；所述的表提供给所述的次要安全服务器和所述的电子模块。

22. 如权利要求 15 所述的系统，其特征在于：所述的安全服务器证书是由所述主要安全服务器加密的，所述的模块证书是由所述次要安全服务器加密的。

23. 如权利要求 22 所述的系统，其特征在于：所述的安全服务器证书包括：

用所述主要安全服务器的专用密钥加密的第一和第二数据字段，所述的第一数据字段包括：所述次要安全服务器的唯一标识符、所述安全服务器的公共密钥、以及所述安全服务器证书的期满时间；所述的第二数据字段包括：由所述主要安全服务器数字签字的所述第一数据字段；以及

第三数据字段，所述的第三数据字段包括所述主要安全服务器的唯一标识符。

24. 如权利要求 23 所述的系统，其特征在于：所述主要安全服务器的所述唯一标识符是加密的。

25. 如权利要求 22 所述的系统，其特征在于：所述的模块证书包括：

用次要安全服务器的专用密钥加密的第一和第二数据字段，所述的第一数据字段包括：所述电子模块的唯一标识符、所述电子模块的公共密钥、以及所述模块证书的期满日期；所述的第二数据字段包括：由所述次要安全服务器数字签字的所述第一数据字段；以及

第三数据字段，所述的第三数据字段包括所述安全服务器证书。

26. 如权利要求 15 所述的系统，其特征在于：所述主要安全服务器和所述次要安全服务器共享一个公共对称密钥，利用公共密钥的密钥交换，周期性地改变该公共对称密钥。

27. 如权利要求 15 所述的系统，其特征在于：所述主要安全服务器有选择地发出所述安全服务器证书和所述模块证书的全部重新证明的命令。

28.一种利用第一货币模块把货币的电子表征转移到第二货币模块的支付方法，包括下列步骤：

在所述的第一货币模块与所述的第二模块之间建立一个加密的安全对话，所述的第一和第二货币模块是防止篡改的模块；

所述的第一货币模块通过所述的加密安全对话把货币的电子表征转移到所述的第二货币模块；

所述的第二货币模块将准备委托的消息发送给所述的第一货币模块；

响应于所述的准备委托消息，所述第一货币模块把收悉消息发送给所述第二货币模块，然后委托所述的电子货币转移，从而使所述第一货币模块不再能够通过重新还原其状态中止所述的电子货币转移；以及

所述第二货币模块在接收所述收悉消息后进行委托，从而使所述第二货币模块不再能够通过重新还原其状态中止所述的电子货币转移。

29. 如权利要求 28 所述的支付方法，其特征在于：所述的每一个货币模块通过遵循所述货币模块中所编的中止程序，可以在委托所述转移前中止。

30. 如权利要求 28 所述的支付方法，其特征在于：所述中止程序包括以下的货币模块执行的步骤：

检查所述的准备委托的消息是否发出；

发出所述的准备委托消息，记录与从所述第一货币模块接收的所述货币电子表征有关的信息，与所述货币电子表征有关的所述信息能够被用于索赔遗失电子货币。

31. 如权利要求 30 所述的支付方法，其特征在于：所述的中止程序包括下列货币模块执行步骤：

将表示所述电子货币转移未能够完成的消息发送给其它的所述货币模块；以及

响应于所述的信息，所述的其它货币模块使其有关所述电子货币转移的变化重新还原并记下所述的电子货币转移被中止。

32. 如权利要求 31 所述的支付方法，其特征在于：进一步包括步骤：所述的其它货币模块是指第二认购者使用的将所述电子转移被中止的消息发送给所述第二认购者的交易货币模块。

33. 如权利要求 31 所述的支付方法，其特征在于：进一步包括步骤：所述的其它货币模块是与银行有关的通知所述银行倒转所述电子转移已进行的记帐交易的出纳货币模块。

34. 如权利要求 30 所述的支付方法，其特征在于：进一步包括所述货币模块使其变化重新还原以及记录所述交易被中止的步骤。

35. 如权利要求 30 所述的支付方法，其特征在于：进一步包括步骤：所述的货币模块是认购者使用的交易货币模块，所述的准备委托消息没有发出，所述电子转移被中止消息发送给所述的认购者。

36. 如权利要求 30 所述的支付方法，其特征在于：进一步包括步骤：所述的货币模块是认购者使用的交易货币模块，发出所述的准备委托消息，所述电子转移被中止以及可能出现货币转移差错的消息发送给所述的认购者。

37. 如权利要求 30 所述的支付方法，其特征在于：进一步包括步骤：所述的货币模块是与银行有关的出纳货币模块，发出准备委托的消息，通知所述银行倒转所述电子转移进行的记帐交易。

38.第一装置与第二装置建立对话的一种方法，所述的第一和第二装置是电子货币系统中的一个电子模块或一个服务器，所述的方法包括下列步骤：

(a)所述的第二装置接收所述第一装置的证书；

(b)所述的第二装置核实所述第一装置所述证书的有效性；

(c)所述的第二装置向所述的第一装置发送一个信息，所述信息包括用所述第一装置公共密钥加密的部分，以及所述第二装置的证书，所述的部分包括第一随机数、第二装置时间信息、以及第一核实信息；

(d)所述的第一装置核实所述第二装置所述证书的有效性，确定所述第二装置的时间信息是否在第一装置时间信息的预定范围内；

(e)所述第一装置向所述第二装置发送用所述第二装置公共密钥加密的第二信息，所述的第二信息包括：由所述第一装置产生的第二随机数、由所述第一装置产生的第二核实信息、由所述第二装置产生的所述核实信息、以及所述第一装置的时间信息；

(f)所述第一装置从所述第一随机数和所述第二随机数的组合，形成对话密钥；

(g)所述第二装置核实所述第一核实信息；从所述第一随机数和所述第二随机数的组合，形成所述的对话密钥；确定所述第一装置的时间信息是否在所述第二装置时间信息的预定范围内；

(h)所述第二装置向所述第一装置发送一个用所述对话密钥加密的收悉消息，所述的收悉消息信息包括所述第二核实信息；以及

(i)所述第一装置对所述收悉消息进行加密并核实所述第二核实信息。

39. 如权利要求 38 所述的方法，其特征在于：所述第一装置连接到具有网络服务器的电子货币系统，步骤(a)包括：所述第一装置向所述网络服务器发送一个包含用对称密钥加密的所述第一装置所述证书的信息；所述网络服务器对所述信息进行解密并将所述第一装置的所述证书发送给所述第二装置。

40. 如权利要求 38 所述的方法，其特征在于：每一个证书包括一个唯一标识符，对于每一个装置而言它是唯一的，所述的方法进一步包括下列步骤：所述第

二装置确定所述第一装置的唯一标识符是否包含在存储在所述第二装置中的第一表中，所述第一装置确定所述第二装置的唯一标识符是否包含在存储在所述第一装置中的第二表中，所述的第一和第二表是不好装置的所述唯一标识符的表。

41. 如权利要求 40 所述的方法，其特征在于：每一个装置是多种类型中的一种，每一个所述的类型与一个类型变量的唯一范围有关；给定装置的所述唯一标识符映射到所述唯一范围内所述类型变量的一个值，根据安全地存储在每个所述装置中的映射机制，指定所述给定装置的所述类型，步骤(b)包括：把所述第一装置的所述唯一标识符映射到第一装置类型变量以及确定所述第一装置的类型变量是否对应于所述第一装置的预期类型；步骤(d)包括：把所述第二装置的所述唯一标识符映射到第二装置类型变量以及确定所述第二装置的类型变量是否对应于所述第二装置的预期类型。

42.一种把预定的总货币价值的电子票据从转移者货币模块转移到受移者货币模块的方法，所述的方法包括下列步骤：

(a)所述的转移者货币模块选择一个或多个电子票据，从这些票据提供所述的预定总货币价值；

(b)所述的转移者货币模块通过把所述转移者货币模块的各个转移记录和数字签字添加到所述的一个或多个电子票据上，创建一个或多个转移电子票据，对于所述的一个或多个转移电子票据中的每一个，所述的各个转移记录表示所述一个或多个电子票据的货币金额的全部或一部分是否正在被转移；

(c)所述转移者货币模块将所述的一个或多个转移电子票据发送给所述受移者货币模块；

(d)所述受移者货币模块核实所述的一个或多个转移电子票据的有效性；

(e)所述的受移者货币模块在票据目录下存储所述的一个或多个转移电子票据；

其特征在于：所述的转移者和受移者的货币模块存储票据记录信息，该信息包括：所述一个或多个电子票据中每一个的票据实体和转移记录；以及

步骤(d)包括：对于所述一个或多个转移票据的每一个转移票据，检查所述票据目录中票据实体和所述票据记录与所述转移票据匹配，创建已确认匹配的票据转移树并检查复制。

43. 如权利要求 42 所述的方法，其特征在于：所述的转移记录包括一个顺序

识别数，对于所述一个或多个电子票据中的每一个，所述的顺序识别数可区分由此产生的所有转移电子票据。

44. 如权利要求 42 所述的方法，其特征在于：对于所述的一个或多个转移电子票据中的每一个转移电子票据，步骤(d)包括检查所述的转移记录以及由其它转移者货币模块添加的所有其它转移记录，确证对于每一个转移，被转移的货币金额不大于先前转移中所转移的货币价值。

45. 如权利要求 42 所述的方法，其特征在于：所述一个或多个转移电子票据中的每一个转移电子票据包括在所述转移电子票据历史上每一个转移者货币模块的数字签字和证书；步骤(d)进一步包括核实每一个数字签字和证书的有效性。

46. 如权利要求 42 所述的方法，其特征在于：所述一个或多个转移电子票据的每一个包括期满日；所述的受移者货币模块是交易货币模块，步骤(d)进一步包括所述受移者货币模块核实每一个电子票据的期满日。

47. 如权利要求 42 所述的方法，其特征在于：所述的电子票据是一种具有期满日和货币价值的货币电子表征；步骤(a)包括：

(a)所述转移者货币模块确定提供预定总货币价值的所有可能的替换以及利用最少的电子票据数目；

(b)确定所述的所有可能替换中哪一组包括最少的转移数目；

(c)所述的组包括一个以上的要素，选择所述组的一个要素，它包括在该要素所有票据上求和的最少数目的货币单位日；货币单位日表示在电子票据的期满日之前的天数与电子票据剩余货币价值的乘积。

48. 如权利要求 42 所述的方法，其特征在于：步骤(d)包括所述的受移者货币模块核实被转移的预定货币价值对应于预期价值。

49.一种把预定总货币价值的电子票据从转移者货币模块转移到受移者货币模块的方法，所述的方法包括下列步骤：

(a)所述的转移者货币模块选择一个或多个电子票据，从这些票据提供所述的预定总货币价值；

(b)所述的转移者货币模块通过把所述货币模块的各个转移记录和数字签字添加到所述的一个或多个电子票据，产生一个或多个转移电子票据，对于所述的一个或多个转移电子票据的每一个，所述的各个转移记录表示所述一个或多个电子票据的货币金额的全部或部分是否正在被转移；

(c)所述转移者货币模块将所述的一个或多个转移电子票据发送给所述受移者货币模块;

(d)所述受移者货币模块核实所述的一个或多个转移电子票据的有效性;

(e)所述的受移者货币模块在票据目录下存储所述的一个或多个转移电子票据;

其特征在于:所述一个或多个转移电子票据中每一个转移电子票据包括在所述转移电子票据历史上每一个转移者货币模块的数字签字和证书,所述的每一个证书包括识别有关转移者货币模块的唯一标识符,所述的转移记录包括受移者电子模块的所述唯一标识符;以及

步骤(d)进一步包括:对于所述电子票据历史上的每一个顺次的转移,检查所述转移记录的所述唯一标识符对应于所述证书中的所述唯一标识符。

50.一种把预定总货币价值的电子票据从转移者货币模块转移到受移者货币模块的方法,所述的方法包括下列步骤:

(a)所述的转移者货币模块选择一个或多个电子票据,从这些票据提供所述的预定总货币价值;

(b)所述的转移者货币模块通过把所述货币模块的各个转移记录和数字签字添加到所述的一个或多个电子票据,产生一个或多个转移电子票据,对于所述的一个或多个转移电子票据的每一个,所述的各个转移记录表示所述一个或多个电子票据的货币金额的全部或部分是否正在被转移;

(c)所述转移者货币模块将所述的一个或多个转移电子票据发送给所述受移者货币模块;

(d)所述转移者货币模块核实所述的一个或多个转移电子票据的有效性;

(e)所述的转移货币模块在票据目录下存储所述的一个或多个转移电子票据;

其特征在于:所述一个或多个转移电子票据中每一个转移电子票据包括所述转移电子票据历史上每一个受移者货币模块的唯一标识符;以及

所述的受移者货币模块是一个交易货币模块,步骤(d)进一步包括:对于存储在所述受移者货币模块中的不好的货币模块,检查所述的每一个唯一标识符是否在唯一标识符的表中。

51.第一认购者将存储在第一交易模块中的第一外币的电子表征兑换为存储

在第二交易模块中的第二外币的电子表征的一种方法，包括下列步骤:

(a)在所述的第一交易模块与所述的第二交易模块之间建立一个加密的安全对话;

(b)所述的认购者利用所述的第一交易模块选择出售所述第一外币的第一金额;

(c)检查所述第一交易模块是否具有足够的资金;

(d)所述的第一交易模块通过所述的加密安全对话把所述的第一金额发送给所述第二交易模块;

(e)所述的第二交易模块提示其所有人选择兑换率或所述第二外币的第二金额;

(f)检查所述第二交易模块是否具有足够的资金;

(g)所述的第二交易模块通过所述的加密安全对话把所述的第二金额或所述的兑换率的消息指示发送给所述的第一交易模块;

(h)所述的第一认购者确认所述的第二金额或所述的兑换率;

(i)所述的第一交易模块通过所述的加密安全对话在所述的第一金额中把所述的第一外币的电子表征送到所述的第二交易模块;

(j)所述的第二交易模块通过所述的加密安全对话在所述的第二金额中把所述的第二外币的电子表征送到所述的第一交易模块；以及

(k)委托所述的第一交易模块，把所述的第一外币转移到所述的第二交易模块，以及所述的第二交易模块从所述的第一交易模块接收所述的第一外币；委托所述的第二交易模块把所述的第二外币转移到所述的第一交易模块以及所述的第一交易模块从所述的第二交易模块接收所述的第二外币，其次序不是预知的。

52. 如权利要求 51 所述的方法，其特征在于：步骤(k)包括下列步骤:

(a)所述的第一交易模块和所述的第二交易模块共享一个公共随机二元值，或是取第一值或是取第二值;

(b)所述的第一交易模块进行有条件记录，或是把所述的第一外币转移到所述的第二交易模块，或是从所述的第二交易模块接收所述的第二外币，这里所述的公共随机二元值分别具有所述的第一值或第二值，从而可以发生重新还原;

(c)所述的第一交易模块把表示所述的第一交易模块已经完成有条件记录转移的消息发送给所述的第二交易模块;

(d)所述的第二交易模块响应于所述的消息有条件记录，或是从所述的第一交易模块接收所述的第一外币，或是把所述的第二外币转移到所述的第一交易模块，这里所述的公共随机二元值分别等于所述的第一值或第二值，从而可以出现重新还原;

(e)所述的第一交易模块把开始委托的消息发送给所述的第一交易模块，这里，所述的公共随机数的值等于第一值;

(f)所述的第一交易模块响应于所述的开始委托消息，将所述的有条件记录设定为无条件记录并对委托协议初始化，这里所述第一交易模块委托其未付转移，从而所述第一交易模块不再能够通过使其状态重新还原而中止所述转移；所述第二货币模块通过记录所述转移和接收，委托所述转移第二外币和所述接收第一外币，从而所述第二货币模块不再能够通过使其状态重新还原而中止所述外币的兑换;

(g) 所述的第二交易模块将所述的有条件记录设定为无条件记录并对委托协议初始化，所述公共随机数的值等于第二值，这里所述第二交易模块委托其未付转移，从而所述第二交易模块不再能够通过使其状态重新还原而中止所述转移；所述第一货币模块委托所述转移第一外币和接收第二外币，从而所述第一货币模块不再能够通过使其状态重新还原而中止所述外币的兑换。

53. 如权利要求 52 所述的方法，其特征在于：在建立加密安全对话的所述步骤期间，所述的公共随机数是作为一个对话密钥产生的。

54. 如权利要求 51 所述的方法，其特征在于：相对另一个货币模块对于未付货币转移由一个指定货币模块对所述委托协议初始化，包括下列步骤:

所述的指定模块将准备委托的消息发送给所述的另一个货币模块;

所述的另一个货币模块响应于所述准备委托的消息将收悉消息发送给所述的指定货币模块;

所述的指定货币模块通过记录所述未付货币转移进行委托，从而使所述指定货币模块不再能够通过使其状态重新还原而中止所述未付货币转移；以及

所述的另一个货币模块通过记录所述未付货币转移进行委托，从而使所述另一个货币模块不再能够通过使其状态重新还原而中止所述未付货币转移。

55. 如权利要求 51 所述的方法，其特征在于：在步骤(b)中，所述的认购者选择以票据类型出售的所述第一外币的所述第一金额。

56.在基于处理器的电子模块之间转移电子票据的系统，基于处理器的每一个电子模块是多个模块类型中的一种，所述的系统包括:

基于处理器的电子模块，基于处理器的每一个电子模块存储一个唯一模块标识符，每一个电子模块能够产生一个加密的安全通道以及通过所述的加密安全通道转移和接收电子票据，这里，所述的每一个电子模块有一个存储所述电子票据的存储器；其特征在于:

所述多个模块类型的每一个类型与模块类型变量的一个唯一范围有关，根据安全地存储在每一个所述电子模块中的映射机制，所述的每一个唯一模块标识符映射到指定所述模块类型的所述唯一范围中的所述类型变量的值。

57. 如权利要求 56 所述的系统，其特征在于: 所述的每一个唯一标识符是一个小于预定素数的唯一整数；所述类型变量的所述值是在所述的预定素数上取模运算下将所述素数的本原根升幂到所述唯一标识符产生的；所述多个电子模块中的每一个、所述主要安全服务器、以及所述多个次要安全服务器中的每一个安全地存储所述的本原根和所述的素数。

58. 在拥有出纳模块、货币发生器模块以及联机记帐系统的发行银行，认购者利用交易模块更新所述认购者的银行帐户的信用票据的方法，所述的方法包括下列步骤:

(a)所述的认购者通过所述的交易模块选择所述的银行帐户，从该帐户更新所述的信用票据和所述信用票据的所请求总信用金额的请求信用金额指示;

(b)所述交易模块建立与所述出纳模块的第一加密安全对话;

(c)所述交易模块通过所述第一加密安全对话将信用请求消息发送给所述的出纳模块，所述的信用请求消息包括与所述信用票据的净信用金额相对应的信用更新金额以及与所述银行帐户相对应的银行帐户信息;

(d)检查所述的银行帐户信息，核实其有效性;

(e)检查与所述认购者的银行帐户有关的信贷限额，提供所述请求信用金额的足够资金;

(f)存在所述认购者的银行帐户的当前信用票据，所述的交易模块将所述的当前信用票据发送给所述的出纳模块;

(g)所述的出纳模块建立与所述的货币发生器模块的第二加密安全对话;

(h)根据所述信用票据的请求总信用金额，对与所述认购者的银行帐户有关的

所述信贷限额进行更新;

(i)所述的出纳模块通过所述的第二加密安全对话将产生票据请求发送给所述的货币发生器模块，所述的产生票据请求包括请求信用票据的值;

(j)所述的货币发生器模块产生一个所述请求信用票据值的信用票据;

(k)通过所述的第二加密安全对话，把所述的信用票据转移到所述的出纳模块;

(l)通过所述的第一加密安全对话，把所述的信用票据转移到所述的交易模块;

(m)委托所述的交易模块与所述的出纳模块对话；以及

(n)所述的出纳模块用所述的货币发生器模块进行委托。

59. 如权利要求 58 所述的信用更新方法，其特征在于：存在所述的当前信用票据，在步骤(c)中，所述信用票据的所述净信用金额代表所述当前信用票据的请求总信用金额与当前信用金额之间的差。

60. 如权利要求 58 所述的信用更新方法，其特征在于：所述的银行帐户信息包括具有客户服务模块数字签字的银行帐户号码的帐目分布；检查所述银行帐户信息的有效性的步骤包括用所述客户服务模块的公共密钥检查所述帐目分布上数字签字的步骤。

61. 如权利要求 58 所述的信用更新方法，其特征在于:

步骤(f)进一步包括所述交易模块把存储在所述交易模块中的任何流通票据和任何被转移信用票据发送给所述出纳模块的步骤;

步骤(f)是接着所述出纳模块根据所述流通票据和被转移信用票据更新所述联机记帐系统的步骤之后;

在步骤(i)中，所述的产生票据请求包括与存储在所述交易模块中的所述流通票据和所述被转移信用票据的值相对应的请求流通票据的值;

用所述的请求流通票据的值把发行货币的帐户记录所述联机记帐系统中的贷方;

步骤(j)包括所述货币发生器模块产生所述请求流通票据值的流通票据的步骤;

步骤(k)包括通过所述第二加密安全对话，把所述流通票据转移到所述出纳模块的步骤；以及

步骤(l)包括通过所述第一加密安全对话，把所述流通票据转移到所述交易模块的步骤。

62.认购者借助于与接入一家或多家银行的主机相关的客户服务模块，在拥有出纳模块、货币发生器模块以及联机记帐系统的银行，将交易货币模块与所述的认购者银行帐户联系起来的方法，所述的方法包括下列步骤:

(a)所述客户服务模块的所述主机根据接收的所述认购者的识别信息，从所述的一家或多家银行接入所述认购者的银行帐户信息;

(b)核实所述的银行帐户信息，所述的认购者识别连接到所述交易货币模块的所述认购者银行帐户;

(c)在所述交易货币模块与所述客户服务模块之间建立对话;

(d)所述客户服务模块产生所述认购者银行帐户的帐目分布;

(e)所述客户服务模块将消息发送给所述的交易货币模块，所述的消息包括:所述帐目分布和用所述客户服务模块的专用密钥签字的所述帐目分布的数字签字;

(f)所述的交易货币模块核实所述的数字签字;

(g)所述的交易货币模块将所述客户服务模块的证书添加到所述的帐目分布上;

(h)所述的交易货币模块存储所述的帐目分布；以及

(i)委托所述交易货币模块与所述客户服务模块对话。

63. 如权利要求 62 所述的方法，其特征在于: 步骤(f)进一步包括所述认购者核实所述帐目分布的步骤。

64. 如权利要求 62 所述的方法，其特征在于: 步骤(h)包括所述交易货币模块用所述帐目分布代替所述银行帐户的现有第二帐目分布的步骤。

65. 在拥有出纳模块、货币发生器模块以及联机记帐系统的银行，认购者借助于与接入一家或多家银行相关的客户服务模块，使交易货币模块与所述认购者银行帐户的联系重新生效的方法，所述的方法包括下列步骤:

(a)所述的认购者借助于所述的交易货币模块选择所述的银行，所述银行使所述的联系重新生效;

(b)所述的交易货币模块建立与所述客户服务模块的加密安全对话;

(c)所述的交易货币模块给所述的客户服务模块发送存储在所述交易货币模

块中的所述银行帐户的帐目分布;

(d)所述客户服务模块核实所述帐目分布的有效性;

(e)所述客户服务模块检查所述的银行，所述帐目分布中所包含的认购者银行帐户是否有效的;

(f)所述客户服务模块产生所述认购者银行帐户的帐目分布;

(g)所述的客户服务模块将消息发送给所述的交易货币模块，所述的消息包括所述的帐目分布和用所述客户服务模块专用密钥签字的所述帐目分布的数字签字;

(h)所述的交易货币模块核实所述的数字签字;

(I)所述的交易货币模块将所述客户服务模块的证书添加到所述帐目分布；以及

(j)委托所述交易货币模块与所述客户服务模块对话。

66. 如权利要求 65 所述的方法，其特征在于：所述的帐目分布包括特定客户服务模块的数字签字和所述特定客户服务模块的证书，核实所述帐目分布有效性的步骤(d)包括检查所述客户服务模块数字签字以及使所述特定客户服务模块的所述证书生效的步骤。

67.一种电子货币系统，包括

拥有联机记帐系统的发行银行;

发行货币的协调系统;

在所述联机记帐系统中记帐的货币电子表征;

与所述发行银行关联的货币发生器模块，产生所述的货币电子表征;

与所述发行银行关联的出纳模块，能够存储所述的货币电子表征;

能够转移所述货币电子表征的交易货币模块;

根据任何两个所述模块之间的每一个转移，将转移记录添加到所述的货币电子表征中，所述的电子票据周期性地被传送到所述发行货币的协调系统;

拥有一个分析每一个票据所述转移记录的处理器的所述发行货币协调系统，识别遗失或复制的货币的电子表征；以及

指定交易货币模块的认购者将一份鉴别遗失的货币电子表征的遗失货币索赔提交给所述的发行银行；对于所述的每一个遗失货币电子表征，所述的发行银行根据所述的遗失货币索赔以及所述发行货币的协调系统确认所述遗失货币索

赔的有效性，赔偿所述的认购者。

68. 如权利要求 51 所述的电子货币系统，其特征在于：所述的交易货币模块，每一个都适于存储与中止交易中所涉及的货币电子表征有关的信息；所述的遗失货币索赔包括所述的信息。

69. 如权利要求 51 所述的电子货币系统，其特征在于：所述的交易货币模块，每一个都适于把所述的遗失货币索赔存储在一个独立的存储装置中；所述的遗失货币索赔是由所述交易货币模块的转移密钥数字签字的。

70. 如权利要求 51 所述的电子货币系统，其特征在于：遗失货币索赔包括与存储在所述交易货币模块中的所有货币电子表征有关的信息。

71.认购者创造一个查明与认购者交易货币模块有关的遗失电子票据的遗失货币索赔的方法，所述的方法包括下列步骤:

(a)所述的认购者利用所述的交易货币模块选择产生一个遗失票据索赔;

(b)所述的交易货币模块产生一个唯一的索赔流水号并以数据包构成所述的遗失票据索赔，数据包包含所述的唯一索赔流水号、存储在所述交易货币模块中的所有可转移电子票据的信息、与所述交易货币模块失效委托有关的任何电子票据的失效委托信息、以及所述交易货币模块的数字签字和证书；以及

(c)将所述的遗失票据索赔存储在一个独立于所述交易货币模块的存储介质上。

72. 如权利要求 71 所述的系统，其特征在于：所述的遗失票据索赔包括:

用所述交易货币模块的专用密钥加密的第一和第二数据字段；所述的第一数据字段包括所述的唯一索赔流水号、存储在所述交易货币模块中的包括每个可转移电子票据的当前值和副本的所有可转移电子票据的信息、以及未索赔失效委托的所述失效委托信息；所述的第二数据字段包括用所述交易货币模块的专用密钥数字签字的所述第一数据字段；以及

第三数据字段，包括所述的索赔流水号、所述遗失票据索赔的总货币价值金额以及所述交易货币模块的证书。

73.认购者借助于接入一家或多家发行银行的客户服务模块，利用所述交易货币模块，索赔与交易货币模块有关的遗失票据的方法，所述的方法包括下列步骤;

(a)所述的认购者给所述客户服务模块的主机提供鉴别信息;

(b)建立所述交易货币模块与所述客户服务模块之间的加密安全对话;

(c)所述客户服务模块接收所述认购者的所述主机鉴别信息;

(d)所述交易货币模块将消息发送给所述客户服务模块,所述消息包括与存储在所述交易货币模块中的未索赔失效委托记录有关的未索赔失效委托信息;以及

(e)所述的客户服务模块从所述的未索赔失效委托信息构成一个索赔,并通过所述的主机将所述索赔发送给与一家或多家发行银行有关的发行货币的调查系统。

74. 如权利要求 72 所述的索赔遗失票据的方法,其特征在于:进一步包括所述客户服务模块根据所述消息将索赔标识符发送给所述交易货币模块以及所述交易货币模块用所述索赔识别符作出每一个所述未索赔失效委托信息记录的步骤。

75. 如权利要求 72 所述的索赔遗失票据的方法,其特征在于:在(d) 步中将所述的未索赔失效委托信息发送给所述客户服务模块,该信息只与以前还未索赔的未索赔失效委托记录有关。

76. 如权利要求 72 所述的索赔遗失票据的方法,其特征在于:在(d)步之前,所述认购者借助于所述交易货币模块在失效委托记录的表中选择所述的失效委托的记录。

77. 认购者借助于接入一家或多家发行银行的客户服务模块,利用一个包含从所述交易货币模块存储的遗失票据索赔的存储装置,索赔与交易货币模块有关的遗失票据的方法,所述的方法包括下列步骤:

(a)所述认购者给所述客户服务模块提供鉴别信息;

(b)所述客户服务模块存取所述存储装置中存储的所述遗失票据索赔;

(c)所述客户服务模块从所述存储装置接收所述遗失票据索赔;

(d)所述客户服务模块核实所述遗失票据索赔的有效性;以及

(e)所述客户服务模块从所述的未索赔失效委托信息构成一个索赔,通过所述主机将所述索赔发送给与所述一家或多家发行银行有关的发行货币调查系统。

78. 如权利要求 77 所述的索赔遗失票据的方法,其特征在于:所述的索赔遗失票据包括所述交易货币模块的证书;所述客户服务模块核实所述遗失票据索赔的有效性的(d)步骤包括核实所述证书的有效性。

79. 如权利要求 77 所述的索赔遗失票据的方法,其特征在于:所述遗失票据

索赔包括遗失票据的复制件，所述遗失票据复制件中的每一个遗失票据复制件具有数据字段组成的一个证书组，它包括一张转移所述遗失票据复制件的原件的每个转移者货币模块的表；以及包含各所述转移者货币模块的数字签字和证书；步骤(d)进一步包括核实各转移者货币模块的证书和数字签字的有效性的步骤。

80. 如权利要求 77 所述的索赔遗失票据的方法，其特征在于：所述的遗失票据索赔包括遗失票据的复制件，所述遗失票据复制件的每一个遗失票据复制有一个转移记录数据字段，它包括一张在所述遗失票据复制件的原件在每次转移中转移的各个货币价值金额的表；步骤(d)进一步包括检查所述转移记录数据字段，确证每一次转移的货币金额不大于前一次转移中所转移的货币价值的步骤。

81. 如权利要求 77 所述的索赔遗失票据的方法，其特征在于：在步骤(b)中，在所述客户服务模块与所述存储装置有关的主机装置之间建立通信链路，所述客户服务模块通过所述通信链路存取所述遗失票据索赔。

82.一种基于电子模块的货币交易系统，包括：

多个安全服务器；

多个防篡改的电子模块，每个模块有一个由所述安全服务器中一个服务器数字签字的唯一模块证书、一个存储货币电子表征的存储器以及一个适于给转移和接收所述货币电子表征提供加密安全通道的处理器；

其特征在于：所述的模块证书是根据所述电子模块与所述其它电子模块或与所述安全服务器的相互作用而生效的；以及

所述的多个安全服务器有选择地命令所述模块证书的全部重新证明，请求与所述安全服务器中一个服务器相互作用的任何电子模块重新证明所述的模块证书。

说　明　书

电子货币系统

本申请是1994年4月28日申请的美国专利申请No.08/234461的部分继续申请。

发明领域

本发明涉及以现金、支票、信用卡和债务卡以及电子存款转移的另一种经济交易媒体执行电子货币交易的电子货币系统。

发明背景

目前，每年在个人与机构之间大约发生3500亿笔硬币与纸币的交易。硬币与纸币交易的广泛使用已经限制了诸如购物、车船费和银行帐户存款取款等个人交易的自动化。每一次现金交易由于需要进行正确的计算或找零会加重负担。此外，无论是对个人还是对金融机构，纸币和硬币的处理和管理(包括警卫)也是不方便的、消耗成本和时间的。据估计，仅在美国，货币管理人员单单搬移货币一年就花费600亿美元。另外，纸币的安全性受到比较容易伪造的威胁，例如，可以利用容易获得的高质量的彩色复印机。

尽管支票可填写任何指定的金额，直到最高可达到帐户中可用总金额，但是支票对汇兑能力一直有非常严格的限制，必须是从实地盘存提供的。基于纸质的支票系统不能足够地缓解对现金交易的限制。同样存在许多处理货币的不便并增加了与处理支票有联系的固有的延时。为此，经济交易一直力求以较低的成本获得更大的便利，同时也力求提高安全性。

通过计算机化的电子资金转移(EFT)系统，对于大宗交易已经实现某种程度的自动化。电子资金转移基本上是一个通过金融系统的集中化的计算机交易实现的价值交易手续。EFT服务是利用电子“支票”支付的一种转移，这种电子支票主要被大的商业机构所采用。

自动票据清算所(ACH)和出售点(POS)系统是电子资金转移系统的例子，近年来这些系统实际上已经开始被零售和商业机构所采用。然而，通过这类EFT系统

作出的支付是受到限制的，没有金融系统它们不能进行支付．此外，在营业时间以外的时间里，通常不能进行 ACH 交易。

家庭银行票据支付服务是个人采用电子资金转移系统作出支付的例子。目前，家庭银行的创始人员只找到很少的用户。在已经提供支付服务的银行中，帐户转移和信息是利用个人计算机在电话线上进行的，不到百分之一的银行客户利用这一服务。家庭银行一直不是一个成功的产品的一个原因是，因为客户在这类系统中不能按需要存钱和取钱。

目前的 EFT 系统、信用卡或债务卡与联机系统一起使用进行帐户之间的货币转移，如一个批发商的帐户与一个顾客的帐户之间的货币转移，该系统不能满足对提供银行系统以外普遍接收的经济价值的转移的自动交易系统的需要．此外，信用卡和债务卡系统对于欺诈行为通常是不安全的，不能提供适当的保密性。

为了实现不需要银行系统介入转移、能够分发某些形式的经济价值的、自动的、更方便的交易系统，发展的趋势一直是向脱机的电子资金转移。例如，对于在非现金支付交易中能够作为替代传统支付系统中的货币和支票使用的某些形式的“电子货币”，已经提出许多设想。见美国专利号 No.4977595，题目为“实现电子现金的方法和装置”和美国专利号 No.4305059，题目为“模块资金转移系统”。

更多的为人们所熟知的技术包括：一定金额的购货磁卡，从购货磁卡可以扣除特定用途的预付值。当经济价值用完，就可扔掉该卡。其它的例子包括：存储卡或者所谓的智能卡，这种卡能够重复地存储代表价值的信息，同样可以扣除特定用途的价值。

然而，提出的这些系统存在一个缺陷，没有完全认识到银行货币存款的重要性，它们必须返回到可以发行的广泛接受的货币代表的任何形式。在这些系统中，发行经济价值的代表，无论是电子的还是纸质的，没有得到与其资产相对的等价值债务能力的支持。

提出的这些无纸化支付系统中没有一个具有足够的综合能力，以实现一个不仅包括允许认购者在没有任何中间系统的情况下转移他们之间的电子存款或货币的自动装置而且还包括整个银行系统的多用途电子货币系统，银行系统产生电子货币所代表价值以及结算银行和金融机构的电子货币帐户，维持系统中的货币平衡。

因此，所需的系统允许在没有银行系统中介的情况下进行公共支付人到受款人的经济兑换，控制个人的支付手续。此外，需要提供一种可被大机构用来进行任何规模的商业支付的经济兑换系统，该系统不具有目前 EFT 系统的限制。

在 1991 年 11 月 15 日请求的美国专利请求流水号为 No.07/794112 的专利请求中，这里引作参考，介绍了一个克服上述限制和其它一些现有技术限制的电子货币系统，该系统提供一个采用可以与传统现金互换的并被广泛接受的电子货币的完全电子货币系统。本发明的 EMS 提供安全可靠地转移经济价值(包括认购者之间、金融机构之间以及认购者与金融机构之间的通货和信贷)的方法和系统。EMS 还以多种通货的形式提供电子货币。此外，安全性和可靠性胜过一切，从而产生了对 EMS 作进一步增强的需要。

因此，本发明的一个目的是提供一个强化的 EMS 系统以及有关安全地防范重复使用、复制和伪造的经济兑换方法。

本发明的另一个目的是提供一个索赔遗失钱款的系统和手续。

本发明的再一个目的是提供一个用户友好的支付系统和方法，从货物的买主到零售商实时转移，可以安全可靠地采用该系统和方法。

本发明的以上目的和优点是说明本发明能够达到的，并不是试图对能够实现的可能优点加以限制。因此，从这里的介绍中将能够看出本发明的这些及其它目的和优点，或者可以从本发明的实践中掌握，既如这里所例举的，又如对于本领域的专业人员来说显然可以看出的任何改进和变化。因此，这里所给出和描述的发明属于新颖的方法、装置、组合以及改进。

发明概要

为了实现上述的以及其它的目的，本发明的方法和装置采用一个具有电子货币系统形式的较佳的实施例，包括：(1)与货币发生器装置耦合的银行或金融机构，向认购客户产生和发行电子货币，包括活期存款和电子信用权威机构返回的电子货币；(2)接受和分配电子货币的代理银行；(3)认购者使用的多个交易装置，用于存储电子货币，与参与银行的联机系统进行货币交易或者在脱机交易方式中与类似于交易装置的其它装置兑换电子货币；(4) 与发行和代理银行有关的出纳员装置，用于交易装置与发行和代理银行的手续处理和接口，发行与代理银行自身之间的接口；(5)平衡不同发行银行的电子货币帐户的清算银行；(6)给系统所有

部件提供通信服务的数据通信网络；以及(7)维持系统的完整性、探测系统中伪造和篡改的安全性配置.

在较佳的实施例中，通过将防止篡改的计算机硬件与可以实现网络化的应用软件模块组合，执行货币产生装置、交易装置以及出纳装置的功能。以加密形式发射信息，以防止未经核准的检查，提供安全性。电子货币是用数字签字发射的，提供核准和防止改动或伪造的安全性。

由这些装置兑换的电子货币可以是一种通货或存款的电子表征。电子通货的一个重要方面是与银行票据等价，通过在发行银行中索赔存款可以与一般的纸币互换，但是在发行银行和在代理银行可以进行提款和存款。然而，只有发行银行能够产生电子通货，发行银行对其兑换成现款将负有责任。

发行银行以后利用银行内部结算和结帐手续维持银行系统的货币平衡，正如目前银行业所实践操作的那样。

电子货币表征是代用的、为人们广泛接受的、可以从发行银行无可辩驳地换成现款，即它们具有货币交易的特征。为了维持电子货币系统的完整性，电子货币的每一次兑换包括：与其它信息一起识别存款或货币(即美元、元等)的货币单位、存款或货币单位的金额、发行电子存款或货币的银行以及几个数字签字的数据。

根据本发明的一个较宽的方案，电子货币系统利用电子货币提供交易，包括银行中活期存款返回的电子货币以替代现款交易，以及电子信用核准。在本发明的一个较佳实施例中， EMS 包括：一个产生电子货币的货币模块；一个发行、分配和接受电子货币的货币模块；以及一个接受、存储和转移其它接受货币模块之间以及接受货币模块与发行货币模块之间的电子货币的货币模块。

根据本发明的进一步的一个方案，提供一个执行和维护电子货币的电子货币系统，该电子货币包括通过在银行中索赔存款可与一般货币互换的电子货币以及电子信用核准。

在本发明的一个较佳实施例中， EMS 系统包括：多个发行银行，一个产生电子货币的发生器模块；与发生器模块耦合的，进行出纳交易和与其它出纳模块相互作用，包括电子货币接受和分配的交易的出纳模块；提供电子货币系统整个完整性的安全系统；平衡各个发行银行电子货币帐户以及结算发行银行发行电子货币的结算和结帐手续；由经过核准的用户所有的多个交易模块，进行交易模块

之间、交易模块与出纳模块之间的电子货币的转移；以及处理遗失钱款索赔的客户服务模块，将帐户与货币模块联系，提供银行进入。

根据本发明的另一个方案，通过将防止篡改的计算机硬件与可以与网络一起工作的应用软件相组合，将能执行发生器模块、出纳模块以及客户服务模块的功能。

由这些模块兑换的电子货币可以是在发行银行由活期存款帐返回货币的电子表征或者是信用核准，可以一数字签字发射，提供防止未经核准的改动或伪造的安全性。在一个较佳的实施例中，通过对模块和电子货币的各个单位进行周期性的更新，也可以提供防止伪造和篡改的安全性。较佳地，模块之间的票据转移包括一串识别数，以便于票据转移历史的协调。一旦发现不好的模块或伪造电子货币，能够尽可能快地从流通中剔除掉。

此外，根据本发明的进一步的方案，提供一个索赔遗失钱款的手续，交易模块的所有者或持有者通过客户服务模块可以向银行系统提出索赔，接下来进到银行系统的票据转移历史协调，所有者或持有者可以恢复索赔的任何遗失票据。

本发明的进一步的方案提供对交易模块更新存款的手续，在一个货币模块中对于每一个信用帐仅有一个信用票据。

此外，根据本发明的一个较佳实施例，给交易模块的所有者或持有者提供从零售商那里安全可靠地购买货物提供一个手续。

附图的简述

根据以下的描述并结合附图考虑本发明时，将会理解本发明的另外一些方面、特征和优点，本发明的这些方面、特征和优点也将会变得更加清楚。其中：

图 1A 是表明 EMS 安全性等级体系的示意图。

图 1B 是表明主要安全服务器与普通安全服务器之间的安全网络信息传递的示意图。

图 2 是表明 EMS 安全网络结构的示意图。

图 3A 示出安全服务器的功能部分。

图 3B 示出网络服务器的功能部分。

图 4A 示出客户服务模块的功能部分。

图 4B 示出主要安全服务器的功能部分。

图 5 示出网络签字接通程序的概要。

图 6A-6K 示出网络签字接通协议。

图 7A-7E 示出 EMS 中建立对话协议。

图 8A-8B 示出转移票据协议。

图 9A-9D 示出外汇兑换协议。

图 10 示出 EMS 中模块的委托协议。

图 11A-11B EMS 中模块的中止交易协议。

图 12A-12C 示出出售点(POS)支付协议。

图 13A-13B 示出从发行银行更新信用协议。

图 14 示出建立信用的协议。

图 15A-15B 示出请求信用的协议。

图 16 示出一个票据转移历史的例子。

图 17 示出票据转移树。

图 18A-18C 示出货币模块与银行存取的银行帐户联系的协议。

图 19A-19C 示出使货币模块与银行帐户联系重新生效的协议。

图 20 示出有效帐户号码的协议。

图 21A-21B 示出创建遗失票据索赔的协议。

图 22A-22E 示出索赔遗失票据的协议。

发明的详细说明

本发明提供一种利用电子媒体安全可靠地兑换经济价值的改进货币系统。该系统是通过把新颖的数据处理系统同能够被当前世界上银行系统所使用的其它过程相集成而实现的。根据本发明，对这里引作参考的 1991 年 11 月 15 日请求的美国专利请求流水号为 07/794112 的请求所公开的电子货币系统作了几方面的改进，这几方面的改进包括安全性的一系列改进，它又包括：外汇兑换(F/X)和转移票据交易过程、索赔遗失钱款的过程、连接到银行货币模块的过程、出售点支付的过程、以及更新信用的过程等方面的改进。

安全性

货币系统的有效安全性具有三个特征：即禁止伪造、侦查伪造和遏制伪造。

所述的 EMS 就设计成具有以上三个全部特征的模块系统。

为了禁止伪造，货币模块是利用对称和非对称密钥的密码术进行通信的。任何消息都不是明文的。模块的协议也是通过防篡改的硬件加以保护的。

通过票据协调过程来探测伪造。全系统的定时协议(例如票据期满期)迫使对电子票据进行定期协调。在进行金融交易时也对电子票据进行更新(即用具有新期满日期的新票据来取代)。

如果复制或伪造的票据返回到货币模块的话，货币模块就会被停用(例如放在不好的 ID 表上)。此外，已经通过这些模块的票据将不允许转移。由于票据期满或最终存入银行，将遏制复制或伪造票据的转移。另外，在系统安全存在严重问题的情况下， EMS 可以请求全部协调，因而要求对所有的模块(包括下一次在 EMS 网络上签字接通的交易货币模块)进行重新证明。

以下所列的改进期望能隔断窃听者偷听模块交易的所有信息。对所有的信息加以隐匿，甚至是公共密钥和模块识别符。列出的改进安全性的特征包括如下:

1)保证网络签字接通的安全，从而使得任何人不能欺骗货币模块或者截取任何明文信息，参考图 5 以及如下所述。

2)创建一种指定安全服务器、货币发生器和出纳识别符的方法(见模块编号方案)。对这些识别符进行检查:

a)建立一次对话(见图 7);

b)转移票据-检查转移记录(见图 8)。

3)实现两层安全服务器结构(见安全分级体系和安全网络)，包括主要安全服务器(所有模块带有主要安全服务器的公共密钥)和安全服务器(对所有其它模块进行证明)。

4)改进转移票据，在接受支付或外汇(F/X)票据前针对所有转移检查不好的 ID 表以及检查复制的票据(见图 8)。

5)利用安全服务器的专用密钥对所有的证书加密(见证书结构和有效性)。

6)动态地改变公共密钥的尺寸(见安全网络和图 6)。

7)改变委托协议，从而使故障不会复制货币(见图 10)。

8)改变 F/X，从而使任何当事人都不能通过接收货币而不发送任何货币而中断对于带有必然性的欺骗行为委托(见图 9)。

9)如果付款人委托而接收人中止，改变中止，记录停止委托的信息(见图 11)。

10)如果需要的话，允许全部重新确认(见安全网络和图 6)

以上所列的安全性的改进重点强调了本发明强化的安全性系统所提供的一部分安全特征．从 EMS 安全性系统的另一个较佳实施例的详细描述中可以进一步理解这些以及其它的改进。

安全性等级体系

根据本发明，以下将提供 EMS 系统安全性的另一个实施例。参考图 1A，EMS 必须有两类安全性服务器，主要的 1182 和一般的 1184．主要安全服务器 1182 证明一般安全服务器 1184．安全服务器 1184 证明系统中所有的其它模块(交易货币模块 1186、出纳货币模块 1188、货币产生模块 1190 和客户服务模块 1192)。

主要服务器 1182 只与其它的主要服务器 1182 或其它的安全服务器 1184 进行相互作用．参考图 2，主要安全服务器 1182 被封在一个安全装置中，通过一个安全的 LAN 1194 相互连接。LAN 1194 通过一个安全网关连接到安全网络 1196．所有的安全服务器都是加保护的装置。

安全服务器 1184 还与 EMS 网络 1198 和银行局域网 1200 相连。安全服务器处理得似乎它们能兼顾并服在与其他模块的所有交互作用中是生效的。

只有安全服务器 1184 和模块具有证书。这些装置带有主要安全服务器的公共密钥．证书有两类型：即安全服务器和模块。

证书的结构和有效性

证书的结构如下:

证书(SS) = E_{PSS}[SS(id)||SS(PK)||期满日||σ_{PSS}(X)]||[PSS(id)异或 C]

--X----------

证书(M)=E_{SS}[M(id)||M(PK)||期满日||σ_{SS}(Y)]||证书(SS)

--Y----------

证书有效性协议是:

1)使证书(SS)生效

a)PSS(id) = [PSS(id)异或 C]异或 C

b)$D_{PSS}(E_{PSS}(X||\sigma_{PSS}(X)))=X||\sigma_{PSS}(X)$

c)检查 SS(id)是否是纯正的(见模块编号方案)

d)检查日期是否有效

e)检查是否为 $D_{PSS}(\sigma_{PSS}(X))=h(X)$

2)使证书(M)生效

a)使证书(SS)生效

b)$D_{SS}(E_{SS}(Y||\sigma_{SS}(Y)))=Y||\sigma_{SS}(Y)$

c)检查 M(id)是否是纯正的(见模块编号方案)

d)检查日期是否有效

e)检查是否为 $D_{SS}(\sigma_{SS}(Y))=h(Y)$

式中

PSS = 主要安全服务器

SS = 安全服务器

|| = 串接

M = 模块

id = 识别数

h = 杂凑函数

C = 所有模块共享的不变随机数

PK = 公共密钥(包括密钥的长度)

σ = 数字

签字 = $E°h$

Cert = 证书

E = 用于加密和创建数字签字的带有公共密钥的算法

D = 用于解密和检查数字签字的带有公共密钥的算法

注意: 当用在其它的应用中时, E 和 D 也可以分别用于解密和加密。

模块编号方案

给主要安全服务器 1182 、安全服务器 1184 、出纳货币模块 1188 、货币产生模块 1190 、客户服务模块 1192 、以及交易货币模块 1186 指定识别数(id), 从而能够检查识别数的纯正性。产生一个 48 比特的素数 " p " , 通过一个安全过程找出模 p 、本原根 " a " (这里对于所有的 $1\leq n<p-1$, $a^n \neq 1(p)$)。 a 和 p 在制造

安全服务器时就已经被主要安全服务器安全地装载到系统中的所有模块中。

方案工作如下:

如果 $a^n \equiv m(p)$和

(1)$1 \le m \le 99,999$，那么 n 被指定为主要安全服务器的 id。

(2)$100,000 \le m \le 999,999$，那么 n 被指定为安全服务器的 id。

(3)$1,000,000 \le m \le 6,999,999$，那么 n 被指定为出纳货币模块的 id。

(4)$7,000,000 \le m \le 9,999,999$，那么 n 被指定为货币产生模块的 id。

(5)$10,000,000 \le m \le 11,999,999$，那么 n 被指定为客户服务模块的 id。

(6)$m \ge 12,000,000$，那么 n 被指定为交易货币模块的 id。

如果模块或服务器正在使证书生效，通过计算 $a^n \equiv m(p)$，模块或服务器检查识别数 n(例如 M(id)、SS(id)或 PSS(id))的纯正性，然后检查 m 是否在正确的范围内。

安全网络

如图 2 所示，安全网络 1196 和安全 LAN1194 把安全服务器 1184 连接到主要安全服务器 1182。安全服务器 1184 最初在制造时就证明货币模块和客户服务模块。通过一个模块制造 LAN1202 把这些安全服务器连接起来。它们把安全信息(如不好的 id 表和主要安全服务器及其公共密钥的表)送到模块。不好的 id 表包含停止交易的货币模块、客户服务模块和安全服务器的识别数。接下来，在网络签字接通流程图中描述对这些模块的重新证明。

安全服务器 1184 最初在制造时由主要安全服务器 1182 加以证明。这种主要安全服务器可以通过安全服务器制造 LAN1204 连接起来。参考图 1B，安全服务器 1184 接收不同的安全信息，它们将这些信息送到其它模块。安全服务器给 EMS 网络 1198 和银行 LAN1200 提供安全服务，如它们将更新的安全信息送到网络签字接通上。安全服务器 1184 从安全网络 1196 上的主要安全服务器 1182 接收这一信息。交易货币模块 1186 通过网络服务器 1206(NS)与 EMS 网络 1198 通信。参与银行拥有连接到 LAN1200 的出纳货币模块 1188 可能还有货币发生器 1190。

对安全网络 1196 进行链路加密。此外，主要安全服务器和安全服务器共享公共对称密钥(安全网络的加密密钥)。这个密钥由一个指定的主要安全服务器 1182 用公共密钥、密钥交换进行周期性地变化。

由一个指定的主要服务器 1182 维持不好的 id 表。该表是从参与银行、执法当局以及认购者与系统的相互作用中积累的。

安全服务器和模块的公共密钥的长度将作周期性变化。为了维持高的安全水准，密钥的长度通常是增长的。由一个指定的主要安全服务器将新指定的密钥长度传递到主要安全服务器。当新的不好 id 表送出或重新证明时，通过主要安全服务器将新的长度传递到安全服务器。在存在安全性危险的情况下，主要安全服务器能够要求全部重新证明。

每个主要服务器的公共密钥的长度是不改变的。创建一张安排主要安全服务器的执行和解除委托日程的时间表。由于增加了交易量，新的服务器将具有更长的密钥，除非它们被执行。由主要安全服务器创建有效 PSS 公共密钥的表并由该安全服务器用其专用密钥签字。然后将该表传送到其它安全服务器。

图 3A 示出安全服务器 1184 的功能部分。外部接口功能 1208 提供网络接口的通信层。对话管理器功能 1210 控制交易对话的安全方面。网络签字接通功能 1212 管理网络签字接通的安全功能。创建证书功能 1214 证明任何货币模块的证书(在主要安全服务器中这个功能是证明安全服务器)。分配证书密钥功能 1218 将有效主要安全服务器公共密钥的出证机构的表分配给货币模块(主要安全服务器也分配全部重新证明消息)。控制不好的 ID 表功能 1220 控制和分配不好的识别符的表。与日期/时间同步功能 1222 保持货币模块时钟/计时器服务与系统时间同步。时钟/计时器 1224 和密码术功能 1226 与货币模块中的这些功能相同。

图 3B 示出网络服务器 1206 的功能部分。外部接口功能 1228 提供网络接口的通信层。通信对话管理器功能 1230 管理货币模块之间、货币模块与安全服务器之间的通信对话。网络签字接通功能 1232 控制货币模块网络签字接通过程。路由消息功能 1234 给目录服务器提供路由消息，在签字接通期间和货币模块对话期间控制消息路由。银行服务器指导功能 1236 提供参与银行提供的服务信息。密码术功能 1238 提供对称密钥功能 1240 和随机数发生器功能 1242 。对称密钥功能 1240 对网络服务器 1206 与接入网络的模块之间以及网络服务器 1206 与安全服务器 1184 之间的消息加密。随机数发生器功能 1242 为加密密钥和核实消息产生随机数。

根据本发明，较佳地采用另一种安全处理部件，客户服务模块(CSM)1192 。CSM 是一个用于创建和更新帐户分布的防止篡改装置。 CSM 包含一个类似货币

模块中找到的唯一证书。 CSM 能够建立与其它模块(例如安全服务器)的安全对话。 CSM 需要一台主机与客户服务代表和联机金融系统接口。

CSM 有两个主要功能，第一， CSM 创建帐户分布，从而使货币模块能够进入银行帐户，对连接到银行帐户的货币模块重新进行生效，以及使帐户号码生效。参照图 18-20，以下将更全面地介绍这些交易。第二，根据来自主机客户服务器代表的请求， CSM 对索赔遗失票据产生作用，在图 21 和图 22 中将进一步对此作详细介绍。 CSM 具有与货币模块相同的安全功能且其标识符的号码有规定的范围(见“模块编号方案”)。 CSM 这些功能的性能简化了出纳模块使帐户号码生效的过程。

根据采用 CSM 的 EMS 的一个实施例，每个银行的帐户分布结构变为:

期满日||M(id)||B(id)||LA||σ_{CSM}(X)||Cert(CSM)

--X----------

式中:

M(id) = 模块标识符

B(id) = 银行标识符

LA = 帐户号码和帐户类型(存款或贷款)的表

σ_{CSM}= CSM 的签字

Cert(CSM) = 证书(CSM)

|| = 串接

以下参考图 20 介绍这种分布的生效程序。

图 4A 示出客户服务器(CSM)1192 的功能部分。外部接口 3000 将 CSM 与客户服务模块主机(CSMH)处理器中其它处理和通信装置连接；对话管理器 3001 起控制和委托(即终结)或中止 CSM 与交易货币模块或客户服务代表之间的交易对话的作用。创建帐户分布功能 3002 从客户帐户信息构成帐户分布，允许货币模块存取认购者的不同银行帐户。公共密钥功能证明银行帐户分布并签字。由于 CSM 需要一个主机与客户服务代表和联机金融系统接口，至主机功能 3006 介于 CSM 应用与主机应用之间不同责任的中间。索赔遗失票据功能 3008 响应认购者的遗失票据索赔， CSM 使发行银行生效并分配到发行银行。维持安全性功能 3004 管理廉顾的货币模块表、申请证书、与时钟同步化以及管理新数字密钥的创建。时钟/计时器 3012 和密码术功能 3010 与货币模块中的功能相同。

图 4B 示出主要安全服务器 1182 的功能部分。外部接口功能 3020 提供网络接口的通信层。对话管理器功能 3002 控制与安全服务器(把它们处理成似乎能兼顾)和其它主要安全服务器对话的安全方面。创建证书功能 2024 为任何安全服务器创建证书。分配证书密钥功能 3026 将有效主要安全服务器公共密钥的出证机构的表分配给安全服务器。分配安全网络密钥功能 3032 管理主要安全服务器之中的安全网络密钥并分配给安全服务器。设定全部重新证明功能 3030 确定是否需要全部重新证明(例如，由于安全性存在危险)和在必要时请求全部重新证明。分配不好的 ID 表功能 3028 控制和分配不好的标识符的表。时钟/计时器 3034 和密码术功能 3036 与货币模块中的功能相同。

网络签字接通

参考图 5，提供了网络签字接通程序的概要。签字接通协议描述为了重新证明、存款、取款或其它原因，模块 1243 需要接入 EMS 网络 1198 的情况。模块 1234 可以是交易货币模块 1186、出纳货币模块 1138、货币发生器模块 1188 或客户服务模块 1192。(a)建立模块 1243 与网络服务器 1206 之间的通信。(b)将模块的证书送给网络服务器 1206。(c)网络服务器 1206 产生一个随机核实数 V 和随机密钥 K；然后网络服务器将模块的证书 V 和 K 送给安全服务器 1184(用 NS/S 密钥加密)。(d)模块 1243 和安全服务器 1184 建立一个安全通信对话(通过对话密钥(MM/SS))。(e)安全服务器 1184 传送时间/日期，更新不好的 ID 表，更新主要安全服务器公共密钥、公共密钥长度、全部重新证明(如果必要)以及经过重新证明的模块证书(如果必要)的表。(f)结束与模块 1243 的对话，将 V 和 K 送给模块 1243。(g)用 K 对 V 加密并送给网络服务器 1206。(h)网络服务器 1206 确认对模块 1243 的网络签字接通。(i)然后模块 1243 通知终点网络服务器 1206(如有的话)希望与它连接。(j)网络服务器 1206 建立与终点的连接。

设计网络签字接通，是为了使任何人都不能欺骗模块 1243 或者截取其任何明文信息。图 6 描述了网络签字接通程序的详细流程。

通信 A 建立与 EMS 网络 1198 的通信(1244 步)。维持安全性 A 将其证书送给网络服务器 1206(1246 步)。NS 网络签字接通接收证书(1248 步)。NS 随机数发生器产生随机密钥 K 和随机核实数 V(1250 步)。NS 对称密钥用 NS/SS 密钥对模块的证书 K 和 V 加密(1252 步)。NS/SS 密钥安装在网络服务器 1206 和安全服务器 1184 中的局部对称密钥，为网络签字接通进行通信。NS 网络签字接通将证书

K 和 V 送给安全服务器 1184，这类 SS 网络签字接通接收消息， SS 对称密钥对消息解密(1254-1258 步)。 SS 网络签字接通存储 K 和 V，然后将模块证书发送给 SS 公共密钥，进行生效(1260-1264 步)。为了允许重新证明的可能性，在确定模块证书的有效性中， SS 公共密钥不考虑期满日。

如果模块证书是无效的，那么 SS 网络签字接通创建发射到网络服务器 1206 和模块 1243 的否定接入的消息(1266 步)。 SS 公共密钥用模块的公共密钥对送到模块 1243 的消息加密， SS 对话管理器将消息发送给网络服务器(1268-1270)。 NS 网络签字接通接收消息并记下接入被否定。然后将经过加密的消息发送给模块，网络服务器断开连接(1272 步)。对话管理器 A 接收消息，公共密钥 A 对消息解密，对话管理器 A 记下签字接通被拒绝(1274-1278 步)。如果请求签字接通的装置是交易货币模块，那么至认购者 A 通知认购者(1280-1282 步)。否则，至银行 A 通知银行(1284 步)。

另一方面，如果模块的证书是有效的，那么 SS 控制不好的 ID 表检查模块的 id 是否在不好的 id 表上(1286-1288 步)。如果 id 在表上，那么网络接入被拒绝。否则， SS 随机数发生器创建随机数 R 和核实消息(1290 步)。 SS 网络签字接通将 R 和核实消息集合在一个消息中，利用 A 的公共密钥由 SS 公共密钥对该消息加密。通过添加安全服务器的证书，公共密钥 A 也增加这一加密消息(1292-1294 步)。消息被送给 A，这里公共密钥 A 对消息解密并使安全服务器的证书生效(1298 步)。

如果证书是无效的，那么 A 记下对话终止并通知认购者或银行(1304-1306 步)。如果证书是有效的，那么维持安全性 A 检查安全服务器的 id 是否在不好的 id 表中(1308-1310 步)。如果在表上，那么终止对话(1300-1206 步)。如果不在表上，那么随机数发生器 A 产生随机数 R(A)(1312 步)。维持安全性 A 通过运算 R(A) 异或 R 形成对话密钥(MM/SS)，然后存储该对话密钥(1314 步)。

将包含核实消息的消息和 R(A)汇编并用安全服务器的公共密钥加密(1316 步)。对话管理器 A 将消息发送给 SS 网络签字接通， SS 公共密钥对消息解密(1318-1322 步)。

SS 网络签字接通核实该核实消息是否是产生的消息(1324-1326 步)。如果不是，那么安全服务器拒绝网络接入。如果核实消息是正确的，那么 SS 对称密钥用 R(A)异或 R 形成对话密钥(MM/SS)(1328 步)。 SS 对话管理器记下对话开始并

通过发送消息子程序将确认发送给 A(1330-1332 步)。对话管理器 A 接收确认并记下对话开始(1334 步)。

时钟/计时器 A 将时间和日期发送给对话管理器，对话管理器发送给安全服务器(1336-1340 步)。SS 同步日期/时间接收时间和日期并检查它是否在参数之内(1342-1344)。如果不在参数之内，那么 SS 同步日期/时间将新的时间和日期发送给对话管理器 A(1346-1350 步)。然后时钟/计时器 A 调节时间和日期(1352 步)。然后 A 将其日期和时间重新发送给安全服务器，作重新检查。如果时钟企图同步不止一组时间数，那么向认购者或银行报告时钟失灵，然后如果需要的话可以再试(1354-1362 步)。

然而，如果时间和日期在参数中，那么 SS 网络签字接通将含有不好的 id 表的消息、新的主要安全服务器公共密钥的表(它们来自分配证书密钥功能)、以及公共密钥的长度(周期地改变公共密钥的尺寸)组合起来(1264 步)。SS 创建证书检查是否已经请求全部重新证明以及保证全部重新证明的时间周期没有期满(1366-1368 步)。这个时间周期应当足够长，从而使每个人的证书已经重新证明或者已期满。该功能还应当检查该模块最后重新证明是何时，因为如果模块最后重新证明是在全部重新证明期间证明的，那么不需要重新证明。

如果需要重新证明，那么 SS 创建证书对以前的消息增加：模块应当重新证明(1370 步)。然后，无论是否请求重新证明，SS 公共密钥对消息签字(1372 步)。将消息发送给 A，这里公共密钥 A 检查消息上的数字签字(1374-1378 步)。如果签字是无效的，那么终止对话。那么维持安全性 A 更新不好的 id 表、公共密钥表以及密钥的长度(1382 步)。

然后，模块 A 检查其证书是否需要重新证明(或是因为全部重新证明的指示或是因为是已期满的证书)(1384-1386 步)。如果需要新的证书，那么维持安全性 A 开始产生新的证书(1388 步)。公共密钥 A 产生新的密钥并用其老的专用密钥对新的公共密钥签字(1390 步)。对话管理器 A 将签字的新的公共密钥发送给安全服务器的 SS 创建证书(1392-1396 步)。然后 SS 公共密钥使新的公共密钥上的签字生效(1398-1400 步)。如果不是有效签字，那么安全服务器拒绝网络接入。如果签字是有效的，那么 SS 公共密钥对模块的新的证书签字并将其发送给模块(1402 步)。对话管理器 A 接收证书，维持安全性 A 同意让证书生效，公共密钥 A 使签字生效(1404-1410 步)。

如果证书是无效的，那么对话管理器 A 通过发送消息功能把“证书无效”消息和证书发送给安全服务器(1412-1413 步)。SS 网络签字接通接收消息，SS 公共密钥使签字生效(1414-1418 步)。如果安全服务器确定证书实际是有效的，那么它拒绝模块接入到网络。然而，如果证书是无效的，那么 SS 对话管理器通知网络服务器它将从网络上断开(1420 步)。NS 网络签字接通通知失灵的模块(1422 步)。然后模块询问认购者或银行再试一次(1424-1432 步)。

另一方面，如果模块确定其新的证书是有效的，那么对话管理器 A 把收悉消息发送给安全服务器(1434 步)。同样，如果不需要新的证书，那么维持安全性 A 把收悉消息发送给安全服务器(1436-1438 步)。在两种情况下，SS 对话管理器接收收悉消息并记下其与模块对话结束(1440 步)。SS 网络签字接通则把 K 和 V 送给 A(1442-1444 步)。对话管理器 A 接收消息，对称密钥 A 用 K 对 V 和终点加密并把消息送给网络服务器(1446-1448 步)。NS 网络签字接通接收消息，NS 对称密钥对消息解密并检查 V 是否是与以前产生的 V 相同(1450-1454 步)。

如果 V 不正确，那么 NS 网络签字接通把拒绝接入的消息送给 A，然后断开(1456-1458 步)。如果 V 正确，那么 NS 网络签字接通建立与终点的联系并把收悉消息送给 A(1460 步)。最后，对话管理器 A 接收收悉消息并记下 A 已经签字接通到 EMS 网络 1198(1462 步)。

建立对话

图 7 示出建立对话协议。维持安全性 A 把模块证书发送给对话管理器，对话管理器 A 接收证书并检查货币模块 A 是否连接到网络上(1464-1466 步)。如果货币模块 A 连接在网络上，那么对话管理器 A 把从维持安全性 A 接收的证书送给终点 B(1476 步)。

另一方面，如果货币模块 A 连接在网络上，那么对称密钥 A 用 K 对证书加密，对话管理器 A 把加密的证书送给网络服务器(1468-1472 步)。网络服务器用 K 对证书解密并把证书送给终点 B 。

不管证书是由网络服务器送出的还是由对话管理器 A 送出的，对话管理器 B 接收证书，维持安全性 B(如果 B 是一个安全服务器，那么这一功能是由对话管理器执行的)使证书生效(1480-1482 步)。如果证书不是有效的，那么对话管理器 B 记下对话被终止并通知认购者或是银行(1486-1492 步)(如果 B 是一个安全服务

器，那么 B 仅仅记下交易终止)。

如果证书是有效的，那么维持安全性 B 检查 A 是否在不好的 id 表上(1494-1496 步)。如果 A 在表上，那么终止对话。如果 A 不在表上，那么随机数发生器 B 产生随机数 R(B)和 B 核实消息(1498 步)。时钟/计时器 B 检索时间和日期(1500 步)。维持安全性 R 将 R(B)、B 核实消息、以及消息中的时间和日期组合起来(1502 步)。公共密钥 B 用 A 的公共密钥对消息加密，对话管理器 B 把 B 的证书添加到加密消息中并把消息送给 A(1504-1506 步)。

对话管理器 A 接收消息，公共密钥 A 对消息中加密部分进行解密，维持安全性 A 使 B 的证书生效(1508-1514 步)。如果证书不是有效的，那么对话管理器 A 记下对话终止并通知认购者或银行(1516-1522 步)。如果证书是有效的，那么维持安全性 A 检查 B 是否在不好的 id 表上(1524-1526 步)。如果 B 在表上，那么终止对话，如果 B 不在表上，那么维持安全性 A 检索日期和时间并将其与 B 的日期和时间进行比较(1528-1530 步)。如果日期和时间在范围之外，那么终止对话。

如果日期和时间在范围之内，那么随机数发生器 A 产生随机数 R(A)和 A 核实消息(1532 步)。维持安全性 A 通过运算 R(A)异或 R(B)形成对话密钥(1534 步)。将 A 核实消息、B 核实消息、时间、日期以及 R(A)组合成一个消息并用 B 的公共密钥加密(1536 步)。通过对话管理器 A 把消息送给 B(1538 步)。对话管理器 B 接收消息，公共密钥 B 对消息加密，维持安全性 B 检查 B 核实消息(1540-1546 步)。如果 B 核实消息不正确，终止对话。如果 B 核实消息正确，维持安全性 B 通过 R(A)异或 R(B)形成对话密钥(1548 步)。对时间和日期进行检索并与 A 的时间和日期进行比较，检查它们是否在相互的预定范围内(1550 步)。如果时和日期在范围之外，那么终止对话。如果时间和日期在范围之内，那么对话管理器 B 记下对话开始(1552 步)。

对话管理器 B 把收悉消息和 A 核实消息送给 A(1554-1556 步)。对话管理器 A 接收消息，维持安全性 A 检查 A 核实消息(1558-1562 步)。如果核实消息不正确，那么终止对话。如果核实消息正确，那么对话管理器 A 记下对话开始。

转移票据

图 8 示出转移票据协议。票据目录 X 选择转移的票据和价值，更新票据量和流水号，然后把消息送给票据(1566 步)。选择票据的可能目的是，例如：(1)使数

字签字的数目减至最少(这需要处理时间); (2)使数据包的尺寸减至最小; (3)使交给转移认购者的电子票据的利用率达到最大(即在期满前用最短的时间传送票据)。通过以下的票据转移算法可以实现这些目的: (1)确定包含票据最少号码的所有可能替换物; (2)确定这些替换物中哪一个具有最少转移数; (3)如果从第二步有一种以上的选择，选择具有最少货币单位天数的一个。货币单位日 = 被转移的票据的剩余价值乘上票据期满前剩下的天数，再对数据包中所有票据求和。

票据 X 根据从票据目录 X 接收的消息，产生添加到每一个转移票据上的转移(1568 步)。公共密钥 X 为票据产生签字(1570 步)。数据包管理器 Y 将带有新的转移的票据与数据包中的签字组合起来并把数据包送给 Y(1572-1574 步)。数据包管理器 Y 接收数据包并将其拆开(1576 步)。

核实 Y 使票据中的所有证书生效(例如，货币发生器证书和所有转移证书)。然后，核实 Y 通过电子票据的历史核实转移组中的识别数与签字和证书组中证书的模块识别数匹配。此外，通过保证在整个电子票据历史中，在每一次依次的转移中所转移的量少于上一次转移的量，使每个票据的转移量的一致性生效。此外，检查转移的总量，保证是预计总量(1578-1580 步)。

如果有效并且 Y 是一个交易货币模块。那么核对器 Y 核实票据的期满日(1584-1588 步)。如果任何票据已期满，那么中止交易。如果没有票据期满，那么核对器 Y 针对不好的 id 表检查票据转移的每一个 id(1590-1592 步)。如果任何转移的 id 在不好的 id 表上，那么中止交易。

如果转移的 id 不在不好的 id 表上(或者 Y 不是交易货币模块)，那么公共密钥 Y 核实票据签字的有效性(1594-1596 步)。如果任何签字都不是有效的，那么中止交易。如果签字是有效的，那么核对器 Y 检查票据实体是否与票据应用所存储或者位于交易记录中的票据实体相匹配(1598-1600 步)。对于匹配的每一个票据实体，为了确定是否存在任何重复票据，创建票据转移树(1602-1604 步)。如果任何票据都已经复印一份，那么中止交易。对重复票据的检查(即 1598-1604 步)具体是针对并且也很适合于阻止试图利用兼顾的交易货币模块由内部交易转移票据来产生货币的个人。

如果没有重复票据或者鉴定没有票据实体匹配，那么记录 Y 将票据放在货币持有者中(1606 步)。最后，票据目录 Y 对票据位置和金额进行更新，还设置流水号的初始值(1608 步)。

应当明白，转移票据过程包括对流水号进行更新和初始化以方便票据调节(见“发行货币调节”)、检查任何票据的转移者是否在不好的 id 表中、已经检查重复票据的步骤。这些增加的特征和步骤使得对手难以引人和循环复制票据，增强了在循环中探测复制票据的能力。

外币兑换

图 9 示出利用美元和英镑作为典型货币单位的外币兑换交易的协议。最初，A 同意在$/L 兑换率下与 B 进行美元($)对英镑(£)兑换(1602 步)。然后 A 和 B 在他们的货币模块上签字，模块提示他们的认购者交易的类型(1604-1610 步)。A 选择购买外汇，B 选择出售外汇(1612-1614 步)。A 和 B 建立安全交易对话(1616-1620 步)。

至认购者 A 提示 A 的所有人/持有人他希望兑换的美元票据类型的金额(1622 步)。付款/兑换 A 接收该金额，票据目录 A 检查 A 是否具有足够的资金(1624-1628 步)。如果资金不充足，那么至认购者 A 提示新的金额再次针对现有资金检查(1630-1632 步)。如果没有进入新的资金，那么中止交易(1634 步)。

如果资金充足，那么付款/兑换 A 将美元金额送至 B(1636-1638 步)。至认购者 B 提示 B 的所有人/持有人选择或是他希望兑换美元的英镑数量或是简单地为美元的兑换率(1640 步)。票据目录 B 检查有充足的资金(1642-1644 步)。如果资金不充足，那么至认购者 B 提示新的兑换率并再次检查现有资金充足(1646-1648 步)。然而，如果没有选择新的兑换率，那么付款/兑换 B 通知 A 资金不充足(1650-1652 步)。然后，A 可以选择新的兑换金额或者中止交易(1630-1634 步)。

如果 B 具有充足的交易资金，那么付款/兑换 B 给 A 发送收悉消息和兑换英镑的金额(也发送等价的兑换率)(1654-1656 步)。至认购者 A 提示核实英镑的金额和兑换率(1658-1660 步)。如果金额和兑换率不正确，那么付款/兑换 A 通知 B 金额和兑换率不正确(1662-1664 步)。然后至认购者 B 提示新的兑换率(1666-1668 步)。如果没有选择新的兑换率，那么中止交易(1670 步)。

然而，如果 A 核实交易的金额和兑换率正确，那么付款/兑换 A 把美元金额送给货币持有人(1672 步)。然后美元票据从 A 转移到 B(1674 步)。付款/兑换 A 把英镑金额送给它的持有人(1676 步)。然后英镑票据从 B 转移到 A(1678 步)。

在交易中的这一点上，A 和 B 都暂时持有正确金额的外汇票据。A 和 B 每个人参与两次转移：A 转移：(1)A 把美元转移给 B；(2)A 接收来自 B 的英镑。

B 转移: (1)B 把英镑转移给 A；(2)B 接收来自 A 的美元。为了完成外汇交易， A 现在必须委托其这两个转移(即最终永久记录在其交易记录中)．同样， B 必须委托其这两个转移。注意： A 可以分别委托外汇转移 A→B(美元从 A 到 B)和 B→A(英镑从 B 到 A)．同样， B 可以分别委托外汇转移 A→B 和 B→A 。

外汇兑换协议的下一部分是这样设计的，任何一方都不知道交易货币模块将委托的次序。这种不确定性将可以阻止各方试图篡改交易。作为背景，功能 S(X)是这样定义的， S(0) = A 和 S(1) = B ，这里 A 和 B 指货币模块 A 和 B 。因此，如果 X 随机地选择为 0 或 1 ，那么随机地指示货币模块 A 或 B 。

采用以下程序允许 A 和 B 共同建立一个随机数 X 。 R(A)和 R(B)分别是在建立兑换子程序期间由 A 和 B 产生的随机数。确定 R(A)异或 R(B)的奇偶性(通过 R(A)异或 R(B)的每个位异或)。这个奇偶性是随机数 X 。 $\overline{X}$ 是 X 的补数($\overline{X}$ = X 异或 1)。

再参考图 9 ，交易记录 A 有条件地更新其交易记录，把转移 S(X)记录为 S($\overline{X}$)(1680 步)。如果 X 计算为 0 ，那么有条件地记录转移 A 到 B(即美元转移)。如果 X 计算为 1 ，那么有条件地记录转移 B 到 A(即英镑转移)。由于记录是有条件地记录的，在货币模块 A 中止交易中它可以退回重来。一旦记录更新被设定为无条件的，更新记录变为永久的(或是如流程图明示的或是在委托期间暗示的)。对话管理器 A 把“记录被更新”的消息送给 B(1682-1684 步)。相应地，交易记录 B 也有条件地更新其交易记录，把转移 S(X)记录为 S(X)(1686 步)。

如果 X = 1 ，那么交易记录 B 将记录更新设定为无条件的(1688-1690 步)。因此，在这一点上， B 已经委托其英镑转移给 A 。接着， B 遵循下一步参照图 10 所述的委托协议(1692 步)。在这种情况下， A 将委托其两个转移(即转移美元和接收英镑)， B 将委托其一个未付(未委托)转移，即接收美元。

然而，如果 X = 0(1688 步)，那么对话管理器 B 将“开始委托”消息送给 A(1694-1696 步)。然后，交易记录 A 将其交易更新设定为无条件的(1698 步)，因此委托其美元转移。然后要求图 10 的委托协议。在这个协议(接下来介绍)中， B 委托其两个转移(即转移英镑和接收美元)， A 委托其一个未付的转移，即接收英镑。

正如所看到的， F/X 交易委托票据的每个转移，因此阻止票据复制，如果仅有一个委托可能会出现复制。外币兑换协议保证每一方都不知道谁的转移(A 的美

元或 B 的英镑)将首先被委托。这降低了当事人篡改交易的动机。每个转移是分别被委托的，但是委托的次序是由两个模块随机地选择的。试图干预交易的一方具有 50-50 的遗失货币的机会。此外，由于遗失货币可以重新索赔(见索赔遗失货币)，因此，不存在干预委托的动机。

委托

图 10 示出模块的委托协议。对话管理器 X 将“准备委托”的消息送给 Y(1702-1704 步)。这将委托契约传送给接收消息的模块。在常规货币转移情景中，利用首先传送委托重点的技术来保证转移货币的一方首先委托，从而，消除复制货币的可能性。

然后对话管理器 Y 将收悉消息发送给 X(1706-1708 步)并通过更新其交易记录委托给任何未付的交易(1710 步)。此外，如果 Y 是一个交易货币模块，那么至认购者 Y 通知认购者交易成功(1712-1714 步)。对话管理器 Y 记下对话结束(1716 步)。

交易记录 X 从 Y 结束收悉消息并更新其交易记录，因此委托任何未付转移。X 以与 Y 相同的方式完成其委托。

中止交易

图 11 示出模块的中止交易协议。对话管理器 X 使变化重新还原并记下交易被中止(1726 步)。然后对话管理器 X 检查“准备委托”的消息是否已经送出(1728-1730 步)。如果是，那么 X 通过记录在发送准备委托消息后中止 X 以及在转移票据协议期间接收每个票据的票据标识符和金额，更新其交易记录(1732 步)。因此，在未委托子程序期间请求中止子程序时，中止协议记录信息。

如果 X 是交易货币模块 1186，并送出准备委托消息，那么至认购者 X 通知其认购者交易被中止以及可能存在货币转移差错(1734-1738 步)。

如果 X 是出纳货币模块 1188，那么至银行 X 通知银行应当反转其记帐交易(用适当的负债或信贷)(1740-1742 步)。如果 X 是交易货币模块 1186，并且还没有发送准备委托的消息，那么至认购者 X 通知认购者交易被中止(1744 步)。

在任何情况中，对话管理器 X 给 Y 发送交易未能完成的消息(1746-1748 步)。对话管理器 Y 使其变化重新还原并记下交易中止(1750 步)。然后 Y 通知其认购者交易中止(1752-1754 步)或者通知银行反转其记帐交易(1756-1758 步)。

正如所述的，如果交易是在委托协议期间中断的，有可能遗失票据．如果发生这种情况，受移者已经中止，转移者已经委托票据转移。在这种情况中，受移者的货币模块记录有关应接收票据并通知认购者存在潜在问题的信息(即不接收A送出的票据)。注意：在这种情况下，就转移者货币模块而言，它适当地转移了票据。

然后，受移者货币模块的认购者可以向证明机构作出索赔货币的声明。索赔信息包括未交易的记录。然后证明机构与发行银行检查看看票据是否已经协调。在部分时间周期之后，如果票据没有协调，认购者可以重新索赔其货币。

POS支付

图12示出出售点(POS)支付的协议。POS支付协议试图简化购买人的交易货币模块1186与商家的交易货币模块1186之间发生的支付。例如，商家的交易货币模块1186可以位于超市的现金寄存器中。

起初，A同意从B处购买产品或者接受服务(1760步)。交易货币模块A的所有者/持有者在他的货币模块上签字(1762步)。至认购者A提示交易货币的所有者/持有者且A选择进行POS支付(1764-1766步)。与此同时，商家确定总的购买价格(1768步)。至认购者B提示交易，B选择POS支付(1770-1772步)。然后A和B建立安全对话(1774-1776步)。

至认购者B提示支付的金额，支付/兑换B接受该金额并将其送给A(1778-1782步)。然后，至认购者A提示其认购者核实所请求的金额(1786步)。此外，请求认购者选择将要支付的票据和金额，从而使总数等于请求的金额。如果请求的金额不正确，那么支付/兑换A给B发送请求金额是不正确的消息(1788-1790步)。然后至认购者B提示其主机新的金额(1792-1794步)。如果没有选择新的金额，那么交易中止(1696步)。

如果请求的金额正确，那么支付/兑换A接受票据类型的金额(1798步)。票据目录A检查有否充足的资金(1800-1802步)。如果资金不充足，那么至认购者A提示新的票据类型的金额(1804-1806步)。如果没有进入新的金额，那么支付/兑换A给B发送资金不充足的消息(1808，1790步)。至认购者B提示主机新的金额(1792-1794步)。如果没有新的金额，那么交易被中止(1796步)。如果选择新的金额，那么再次开始支付交易。

如果资金充足，支付/兑换 A 把金额传送给货币持有人(1810 步)。然后票据从 A 转移到 B(1812 步)。最后，交易货币模块委托(1814 步)。

正如所看到的，对于购买人来说 POS 支付得到简化，因为这是受款人启动的支付。通常， POS 支付被用于向商家支付货款，而认购者至认购者(STS)支付被用于支付个人或者支付帐单。

从发行银行更新信用

图 13 示出从发行银行更新信用交易的协议，具体描述了用户如何获得信用票据的。信用票据是一种预先核准的信用支付周转。用户能够携带该用户拥有的每个信用帐户的一个信用票据。注意：允许用户接受更新信用票据的每家银行是这些信用的发行银行。

建立更新信用交易的流程是在货币模块 A 和银行的出纳货币模块 B 之间建立信用过程开始的(1854 步)，现在参考图 14 作进一步介绍。

建立信用

当交易货币模块 A 决定进行信用更新，因而与其货币模块签字时开始建立信用撤回过程(1876 步)。例如，用户 A 可以拥有信用票据，但是希望改变信用金额(如增加或减少)，包括金额减至零，或者目前不拥有信用票据，但是希望得到它。至用户 A 提示交易的所有者/持有者， A 选择从特定银行和帐户进行特定金额的信用更新(1878-1880 步)。在执行中，由用户 A 规定的信用更新金额是用户 A 希望携带的总信用金额。然后，交易货币模块 A 通过上述的网络签字接通程序，开始与网络选择的银行通信的程序(1882 步)。

在完成货币模块签字接通交易选择和网络签字接通的步骤后， A 和 B 建立安全对话(1884 步)。然后，交易货币模块 A 根据请求信用程序(参考图 15 更详细地描述)作出从出纳货币模块 B 的信用请求(1886)。

请求信用

现在参考图 15 ，介绍请求信用的过程。应当注意：尽管图中将各方表示为“ X ”和“ Y ”，在下述的过程步骤中，它们可以应用于与出纳货币模块交易的任何货币模块。

开始，如果对于所选的帐户存在信用票据，票据目录 X 将这个信用票据的金额发送给出纳 X(1897 步)。至出纳 X 确定用户 A 所请求的总信用金额与信用票据金额之间的净差值，并将信用更新请求发送给出纳货币模块，请求从规定帐户中核准一定的净信用金额。在其更新信用请求的传输中，帐户号码和帐目分布以及净信用金额将从请求货币模块传送给出纳货币模块(1898 步)。根据发送消息协议发送这一消息(1900 步)。其中利用密码技术对该消息加密。

一旦请求信用撤回和将帐户号码和帐目分布传送给出纳货币模块，开始证实帐户号码的程序(1902 步)。图 20 示出如何证实帐户号码的流程图。以下将更清楚地描述。

有了经证实的帐户信息，至银行 Y 核实具有足够的信用以支持信用更新请求金额(1904 步)。足够的信用将提示至交易 Y，把收悉消息发送给 X，它通过其至出纳应用功能接收收悉消息(1906-1912 步)。

然而，不充足的信用金额将引起提示用户进入新的信用更新数量(1914-1918 步，图 15)。由用户输入的新的信用更新数量导致至出纳应用把新的信用金额送给出纳货币模块的至银行应用，以核实是否存在足够的资金覆盖最新的请求金额(1922-1924 步)，返回到图 15A 的 1904 步。如果用户没有请求新的金额，那么交易被中止(1926 步)。

回过来参考图 14，根据从请求信用撤回过程返回，至出纳 A 请求转移总的流通票据、被转移的信用票据(即在以前交易中接收的信用票据)以及到出纳货币模块的帐户的信用票据(1888 步)。如果在作出信用撤回请求时在交易货币模块中没存有的票据，至出纳 A 应用把不存在票据的消息发送给出纳货币模块(1892-1894 步)。然而，如果在交易货币模块中持有票据，那么根据上述的转移票据程序并参考图 8，电子票据从 A 转移到出纳 B(1896 步)。

回过来参考图 13，至交易 B 检查是否有任何已转移流通票据和被转移的信用票据(1856-1858 步)，以及是否已经将这些票据类型从交易货币模块 A 转移，记帐交易通过至银行应用 B 公布反映这种情况(1860 步)。当票据还没有从货币模块转移以及在 1860 步中公布记帐交易之后，在这两种情况中，在出纳货币模块与货币发生器模块之间建立对话(1862 步)。至银行 B 通过把信用票据的金额增加到可用信贷限额以获得总的可用信用以及通过从总的可用信用中推导出所请求信用金额，更新信贷限额。如果由于所请求信用金额为零以及没有转移流通票

据，没有创建票据(包括流通票据和信用票据)，那么货币模块将根据以上参考图10所述的委托程序结束交易(1865-1875步)。

然而，如果由于非零的信用金额请求和/或被转移的流通票据，创建了票据，那么根据请求票据程序，出纳B从货币发生器模块请求票据(1865-1866步)。利用上述的转移电子票据的转移票据过程(见图 8)将货币发生器模块中的请求票据转移到出纳货币模块B(1868步)。然后，利用相同的转移票据过程将票据从出纳货币模块B转移到交易货币模块(1870步)。最后，为了成功地完成更新信用的程序，根据以上参考图 10 所述的委托程序结束交易。委托过程首先是由交易货币模块委托与出纳货币模块B交易开始的(1872步)。然后在出纳货币模块B与货币发生器模块之间执行委托过程(1874步)。这就完成了从发行银行的一次完整信用更新的过程。

发行货币的协调

参考图16和17，介绍针对票据伪造和复制的票据协调检查的过程。发行货币的协调系统，基于发行货币主文件中存储的信息，构成模块转移票据历史的票据转移树。

图16以图示方式示出具有表示符号“1”的货币发生器模块(称为货币发生器1)、具有表示符“2”的出纳货币模块(称为出纳模块2)、以及具有整数表示符3至6的四个交易货币模块(称为交易模块3-6)之中假设的一系列交易，以及用1：00：00表示日期/时间时由货币发生器模块1产生一个票据。

根据图16中所示的转移历史的例子，图17示出通货的电子表征的转移是如何从货币发生器模块产生的初始票据，产生导出的通货的电子表征的树形结构。根据票据更新，存储票据的各次转移(树枝部分)或返回到发行银行时，由发行货币协调系统建立图17中的票据转移树。在这个例子中，货币发生器1(模块标识包含在数字签字证书中产生一个具有数据字段实体组和数据字段转移组的通货的电子表征 2300 。为了清楚展示，图中只示出其中的一部分。此外，为了方便起见，未示出数据字段的签字和证书组。

数据字段的实体组包括票据的标识符(例如“N12”)、货币发生器模块的标识符(例如“MG1”)、发行银行的标识符(例如“银行名称”)、发行日期(例如1：00：00)、到期日(例如12：00：00)、票据金额、以及货币单位标识符(例如$50)。

为了方便起见，未示出其它的实体组数据字段，如票据类型等。为了表明起见，以天：小时：分的形式示出电子票据的不同日期字段。当然，可以用其它的时间监测形式(例如包括秒)。

数据字段的转移组包括：具有受移者的识别数的转移记录、转移日期、以及转移金额。转移组较佳地还包括每一次转移后转移者的票据目录所增加的流水号。一般，转移的日期/时间和转移 id 应当足以能够唯一地识别转移。然而，如果在转移之间存在时间调节以及将相同的金额转移到相同的模块，就可能会复制转移、受移者 id 、日期/时间、以及金额。因此，为了避免这种可能的问题，较佳地将流水号(seq)增加到转移记录和票据目录中，以唯一地识别转移。在每一次转移后票据目录将会使流水号增加。如果使流水号复位，那么将探测为复制。

因此，当通货的电子表征 2300 被转移到出纳模块 2 时，转移记录 2302 添加到转移组中，包括受移者的识别数(例如 2)、转移日期(例如 1： 00： 00)、转移金额(例如$50)、以及流水号(例如“1”。为了说明方便起见，图 17 中所表示的票据转移仅仅示出被转移票据中新添加的转移记录部分。此外，为简便起见，图中未示出表示转移总次数的转移组数据字段。

来自货币发生器 1 的通货的电子表征存储在出纳模块 2 中。作为用交易模块 3 取款$50 的部分，出纳模块 2 通过将转移记录 2304 添加到转移记录 2302 增加的通货电子表征 2302 中的数据字段的复制，形成通货的电子表征。然后，根据完成取款，将这一票据存储在交易模块 3 中。可以看出，票据转移树的每个节点表示被转移票据中的新添加的转移记录部分。正如票据转移树所表示的，在 1:00:05 时，交易模块 TR3 通过转移记录 2306 支付$10 给交易模块 4 。在 1:01:00 时，交易模块 3 通过转移记录 2308 支付$10 给交易模块 5 。在 3:08:01 时，交易模块 3 通过转移记录 2310 支付$25 给交易模块 5 。在 4:11:08 时，交易模块 3 通过转移记录.2312 将$5 转移给交易模块 6 。

在 2:00:01 时，交易模块 4 通过转移记录 2314 将$5 转移给交易模块 6 。在 2:01:07 时，交易模块 4 通过转移记录 2315 再将$5 转移给交易模块 6 。在 3:07:05 时，交易模块 4 通过转移记录 2321 又将$5 转移给交易模块 3 。

在 2:00:06 时，交易模块 5 通过转移记录 2316 将整个$10 转移给交易模块 3 。从 3:08:01 时通过交易模块 5 从交易模块 3 接收的$25 票据中，在 3:09:12 时交易模块 5 通过转移记录 2318 向交易模块 6 支付$20，在 4:12:05 时通过交易记录 1320

将余下的$5 存入出纳模块 2 。

在 4:10:00 时，交易模块 6 根据转移记录 2322 将$10 转移给交易模块 5 ，在 5:00:06 时，通过转移记录 2324 将余下的$10 转移给交易模块 3 。根据本发明的实施例，应当清楚，根据从交易模块到银行的货币存款，交易模块中的所有票据(包括信用票据)被送给金融系统并被更新。因此，与转移记录 2320 表示的从交易模块 5 到出纳模块 2 的上述存款基本同步，转移记录 2326 表示的另一个同时的转移自动地发生。然后，货币模块 1 将产生价值$5 的新票据(假设交易模块 3 没有信用票据)并添加适当的转移记录(未示出)，通过出纳模块 2 将其转移给交易模块 3 。因此，可以知道，通过提供一个将票据返回到金融系统的附加装置，根据基于模块与出纳模块织之间的交易(例如存款或取款)，对交易货币模块中的所有票据进行更新方便了票据协调过程。

在 5:00:10 时，交易模块 3 通过转移记录 2328 将$10 存入到出纳模块 2 。如上所述，对于交易模块 5 的存款，与交易记录 2328 表示的交易模块 3 的存款同时，将交易模块 3 所拥有的所有票据(包括转移记录 2316 和转移记录 2321 表示的)同时附加转移给金融系统(未示出)。然后，金融系统给交易模块 3 返回一张价值等于发送给金融系统进行更新的总票据(例如$15)的票据。

因此，在这时，只有交易模块 6 拥有原始票据 2300 的转移痕迹，如转移票据 2312 和 2314 所表示的。如果交易模块 6 在将这些票据转移给其它交易货币模块前与出纳模块交易(例如，存款或取款)，那么在与原始票据 2300 有关的循环中将没有转移票据；从原始票据 2300 转移而导出的所有票据将被返回到金融系统，从而允许构成图 17 所示的票据转移树。期满日期通过限制票据可以被转移的时间，有效地简化了票据的协调。

从票据转移树，可以看出，如果票据是伪造的，那么则没有与存人的第一原件相匹配的票据实体。如果转移是复制的，那么以下的转移总和值则大于超正常转移金额。例如，如果在 5:00:06 时交易模块 6 将$20 转移给交易模块 3(即转移记录 2324)，那么，转移记录 2318 以下的转移(即 SEQ1 、 3:09:12 、 TR6 、 $20)总和为$30 ，表示交易模块 6 已复制转移。

货币模块与银行帐户相联系供银行存取

图 18 示出将货币模块与银行帐户相联系供银行存取的协议。过程是从认购

者识别他/她自己的客户服务代表(CSR)并请求 CSR 将认购者的帐户与货币模块相连接开始的(1928 步)。 CSR 请求进入 CSM 主机 A(CSMHA)，连接已识别认购者的帐户， CSMHA 从银行系统存取已识别认购者的帐户信息(1930-1934 步)。然后认购者和 CSR 核实帐户信息，认购者选择连接到货币模块的帐户(1936 步)。

在认购者请求他/她的货币模块 B 连接银行帐户， CSR 通过 CSMHA 请求 CSMA 连接银行帐户，在认购者的货币模块 B 与 CSMA 之间建立安全对话(1938-1946 步)。然后，响应 CSMA 的至主机 A 的请求， HCSMA 将帐户信息发送给 CSMA， CSMA 接收帐户信息并构成帐目分布(1948-1952 步)。然后公共密钥 A 给帐目分布签字，创建帐目分布构成帐目分布和签字的消息并将这一消息发送给货币模块 B(1954-1958 步)。维持安全性 B 接收消息，公共密钥 B 检查消息上的数字签字(1958-1962 步)。如果签字是无效的，那么中止对话(1966 步)。

如果签字是有效的，那么至认购者 B 将分布发送给主机，以便客户核实帐目分布。如果客户没有确认帐目分布，那么中止交易。如果客户确认帐目分布，维持安全性 B 将 CSM 证书增加到帐目分布上(1968 步)。

然后，至认购者 B 检查确定帐目分布是否已经由新创建的(新的)帐目分布有关的银行存储。如果银行的帐目分布已经存在在至出纳 B 应用中，那么由至出纳 B 用新的帐目分布替代；否则，至出纳 B 增加新的帐目分布(1970-1974 步)。

重新使货币模块与银行帐户联系生效

图 19 示出认购者重新使认购者的货币模块与银行帐户相连接生效的协议。过程是从认购者在他/她的货币模块上签字，响应至认购者 A 所产生交易的提示，认购者选择重新使客户服务模块(CSM)B 有关银行的银行帐户联系生效开始的(1978-1982 步)。货币模块请求和执行图 6 所述的网络签字-开始的协议，在货币模块 A 与 CSMB 之间建立安全对话(1986 步)。然后，至认购者 A 将银行帐户的帐目分布发送给 CSMB(1988-1990 步)。创建帐目分布 B 接收消息，维持安全性 B 使 CSM 证书和帐目分布的签字生效(1992-1995 步)。如果证书和签字是无效的，那么 CSM 中止交易(2000 步)。如果证书是有效的，至主机 H 将帐目分布的帐目表送给 CSM 主机(CSMH)， CSMH 用联机金融系统检查，确定每个帐户目前是否是有效的(1996-2001 步)。如果任何帐户已经期满， CSMH 将中止消息传送给 CSM(2010 步)， CSM 根据中止过程中止交易(2000 步)。

如果所有帐户是有效的，那么 CSMH 将重新生效指令发给 CSM，创建帐目分布 B 接收消息并由帐目信息构成一个帐目分布(2002-2004 步)。然后，公共密钥 B 给帐目分布签字，创建帐目分布 B 从帐目分布和签字构成一个消息并将该消息送给货币模块 A(2006-2010 步)。公共密钥 A 接收消息并核实数字签字(2012 步)。如果签字是无效的，货币模块 A 中止交易(2018 步)；如果数字签字是有效的，那么将帐目分布签字和 CSM 证书增加到帐目分布(2014 步)，货币模块 A 委托交易(2016 步)。

使帐户号码生效

根据上述的采用客户服务模块(CSM)的本发明的一个实施例，图 20 示出如何使帐户号码生效的流程图。

在这个过程中，维持安全性 Y 接收帐户号码和帐目分布，包括 CSM 证书，以及核实 CSM 证书(2020 步)。无效的证书会引起两个货币模块之间的交易中止(2028 步)。

如果证书是有效的，维持安全性 Y 将帐目分布传送给公共密钥 Y，核实 CSM 签字(2022 步)。无效的签字会引起维持安全性 Y 通知对话管理器帐目分布是无效的(2026 步)，两个模块之间的交易被中止(2028 步)。

如果签字测试确认是有效的签字，过程前进到至银行 Y，至银行 Y 将已接收的帐户号码送给银行的联机计算机系统(2024 步)。无效的帐户将引起维持安全性 Y 通知无效帐户的对话管理器并使交易中止(2028 步)；有效的帐户将引起使帐户号码生效的程序返回到工作流程的下一步，请求使帐户号码生效过程。

正如所看到的，与不包括 CSM 的本发明实施例相比，对于出纳货币模块，简化了使帐户号码生效的过程。

索赔遗失货币

正如已经讨论的，由于以下的任何原因，可能会遗失电子货币，这些原因包括：(1)货币模块被损坏并不再起作用；(2)货币模块被遗失或被偷窃；(3)委托失效。对于货币系统的利用来说，用户对系统感到信任，他们的货币是安全的，这是重要的。因此，受移者能够重新索赔系统故障而遗失的货币，这是重要的。当货币模块受损坏时，能够替换货币将会增进信任度，因为电子故障多半是纸张受

损遗失。由于遗失或被偷窃货币模块的意外事件，替换货币是更成问题的。允许这样的索赔则要在系统上引来广泛的索赔，因为用户会不采取预防遗失的措施。

在任何情况下，本发明中所举实例是在两种替换情况的任一情况中允许货币遗失。在两种情况(即上述的情况(1)和(2))中的第一种情况中，用户必须周期地创建一个遗失票据索赔(见图 21)，该索赔存储在货币模块之外。根据故障，向金融系统提交带有认购者身份的索赔(见图 22)。索赔应当包含认购者的货币模块的最后已知状态。使索赔票据的说明生效并分配给发行银行。如果索赔票据还没有被存入，发行银行在一段时间后可以替换货币。

在委托失效的情况(即第三种情况)中，如果货币模块仍然在起作用，在货币模块与客户服务模块之间交互地创建索赔(见图 22)。如在第一和第二种情况中，这一索赔传送给发行货币的调查系统，该系统针对存入的货币监测索赔。由于发行银行能够针对欺诈应用监测进入货币并有应用者的身份，它们在替换遗失票据中感到信任。

以下参考图 21 和 22 将更详细地描述这些方法。

创建遗失票据索赔

现在参考图 21A，图中示出可以根据本发明一个实施例实践的创建遗失票据索赔的过程。该过程是从认购者在货币模块上签字，至认购者 A 提示认购者交易，以及认购者选择一个创建遗失票据索赔任选方案开始的(2032-2036 步)。

然后，发生整顿所有票据和未索赔失效委托的几步(2038-2042 步)。具体说，票据目录 A 产生一个唯一索赔流水号(该流水号被用作识别一个索赔)并将流水号的票据目录的副本传送给数据包管理器。票据 A 将具有签字和证书的所有票据的副本传送给数据包管理器。然后，交易记录 A 把在中止过程期间记录的所有未索赔失效委托交易送给数据包管理器。

接着，公共密钥 A 利用货币模块的专用密钥给发送到数据包管理器的索赔流水号、票据目录、票据和失效委托签字，数据包管理器 A 将签字添加到汇编的数据中，产生一个汇编数据包(2044-2046 步)，然后用公共密钥 A 对其加密(2048 步)。然后，至已加密索赔、公共密钥 A 添加由索赔流水号、索赔总价值金额和货币模块 A 证书构成的索赔说明(2050 步)。至认购者 A 将这一索赔送给货币模块主机，该主机接收并在与货币无关的介质上存储索赔，供将来使用(2052-2054 步)。

因此，可以看出，索赔遗失票据的过程提供了一种产生和保护潜在的不会由于货币模块损坏或故障而销毁的货币索赔的方法。

索赔遗失票据

图 22 示出索赔遗失票据的协议，该协议是从认购者向客户服务代表(CSR)请求作出遗失票据索赔、向 CSR 揭示认购者的身份开始的(2056 步)。然后 CSR 将认购者的身份传送给客户服务模块主机(CSMH)A ，并检查索赔是由于失效委托造成的还是由于货币模块的遗失或毁坏造成的(2060 步)。如果失效委托是索赔的基础(和认购者的货币模块已经遗失或损坏)，那么根据认购者作出从货币模块遗失票据索赔的选择以及 CSR 从货币模块接收遗失票据索赔的选择，认购者货币模块的对话管理器 B 和与客户服务代表有关的(通过客户服务模块主机(HCSM))客户服务模块(CSM)的对话管理器 A 分别请求建立 CSM A 与货币模块 B 之间的安全对话。

一旦建立安全对话，至 CSM 的主机 A 请求认购者的身份， HCSM A 通过把包含认购者身份的消息送给 CSM 对这一请求作出响应(2072-2074 步)。索赔遗失票据 A 接收这一消息并把表示应当发送索赔的消息送给货币模块 B(2076-2078 步)。

交易记录 B 接收这一消息并检索还未索赔的失效委托记录(2080 步)。如果没有查出失效委托记录，那么中止交易(2083 步)。否则，至认购者 B 把检索的失效委托记录中的信息(例如日期、时间和金额)发送给认购者，用于审查(2082 步)。从这一信息，认购者选择要求索赔的交易(2084 步)。例如，认购者会不选择已经单独解决的失效委托交易。然后，对于认购者所选的每一个失效委托交易，交易记录 B 构成包含这些交易记录信息的消息并将这一消息送给 CSM(2086-2088 步)。

索赔遗失票据 A 接收这一消息并把包含索赔标识符(例如，确认数)的收悉消息送给 B，供将来索赔参考(2092 步)。交易记录 B 接收收悉消息并用索赔的日期/时间和 CSM 提供的索赔标识符标示所选失效委托交易记录(2094 步)。然后， B 委托交易(2096 步)。

在完成委托程序后，从接收的包含失效委托交易信息的消息，索赔遗失票据 A 构成一个发送给发行货币调查系统(MIIS)的索赔，该系统较佳地形成交易调查

系统的一部分。至主机 A 将这一索赔发送给 HCSMA， HCSMA 接收该索赔并进一步将索赔发送给 MIIS(2098-2102 步)。

现在，回到图 22 的 2060 步，如果索赔不是由于失效委托造成的(例如，由于遗失或者损坏货币模块的缘故)，那么，根据以上参考图 21 所述的创建遗失票据索赔过程，认购者可以选择从主机 B 作出遗失票据的索赔，主机 B 可存取任何从货币模块计算环境(例如，在 FLASH 存储器上)产生和卸载的认购者的索赔。 CSR 单独选择对过程初始化，从存储器模块主机接收遗失票据的索赔，主机根据任何已知技术建立通信联系(2104-2108 步)。

然后，认购者主机 B 把包含存储器模块证书的索赔发送给 CSMHA， CSMHA 把索赔发送给 CSMA(2108-2112 步)。索赔遗失票据 A 接收索赔并把索赔发送给公共密钥 A，公共密钥 A 使货币模块证书生效(2114-2116 步)。如果货币模块证书是无效的，那么至主机 A 把表示索赔已经被拒绝的消息发送给 CSMHA，CSMHA 将这一消息送入认购者主机 B，终止索赔遗失票据过程(2120-2121 步)。

如果货币模块证书是有效的，那么公共密钥 A 对索赔解密并核实索赔中所有的票据证书和签字(2118 步)。如果任何票据证书和签字是无效的，那么终止交易(2119-2121 步)。如果票据证书和签字是有效的，那么索赔遗失票据 A 核实转移金额的一致性，保证传送给受移者的货币价值不大于每个票据的转移历史中转移者接收的价值(2122-2123 步)。如果存在不一致，那么将终止交易(2120-2121)。

然而，如果对于所有转移金额是一致的，那么索赔遗失票据 A 构成一个索赔，发送给 MIIS，还产生一个与索赔有关的索赔标识符。至主机 A 把构成的索赔和索赔标识符发送给 CSMHA， CSMHA 接收索赔和索赔标识符并将索赔标识符适当地送入到 MIIS(2124-2128 步)，因此，完成索赔遗失票据过程。

尽管以上的描述提供了许多特征，但是这些细节不应当被认作为是对发明范围加以限制，专业人员将会懂得，在不偏离这一范围以及不减少其伴随优点的条件下，本发明可以作许多改进、适应和等效实现。因此，希望本发明不现有这些公开的实施例而是根据以下权利要求书来限定。

说 明 书 附 图

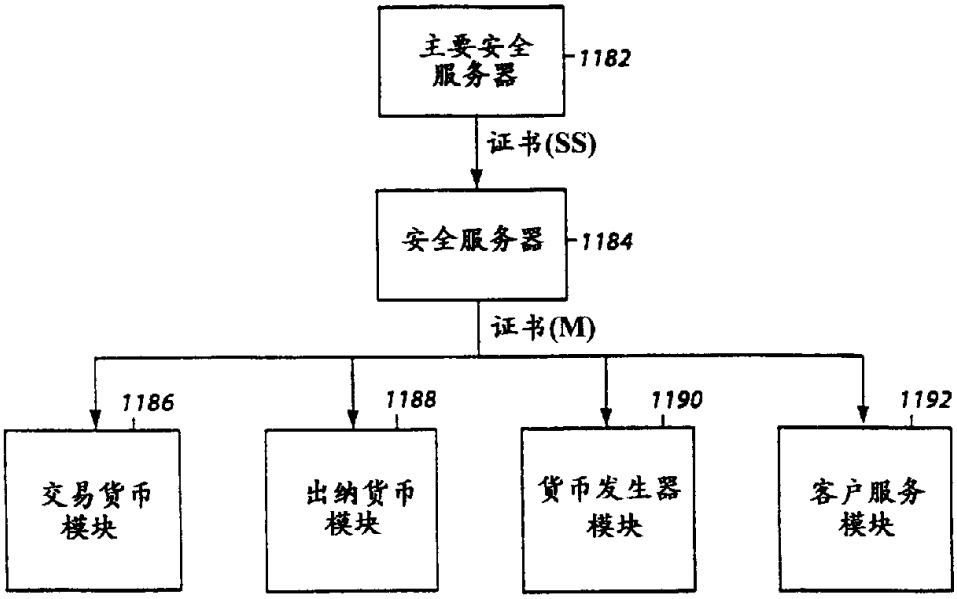


图 1A

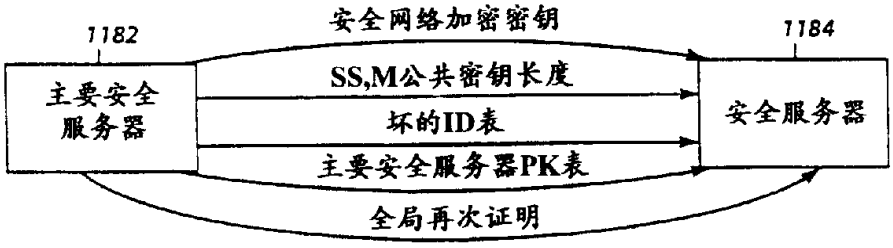


图 1B

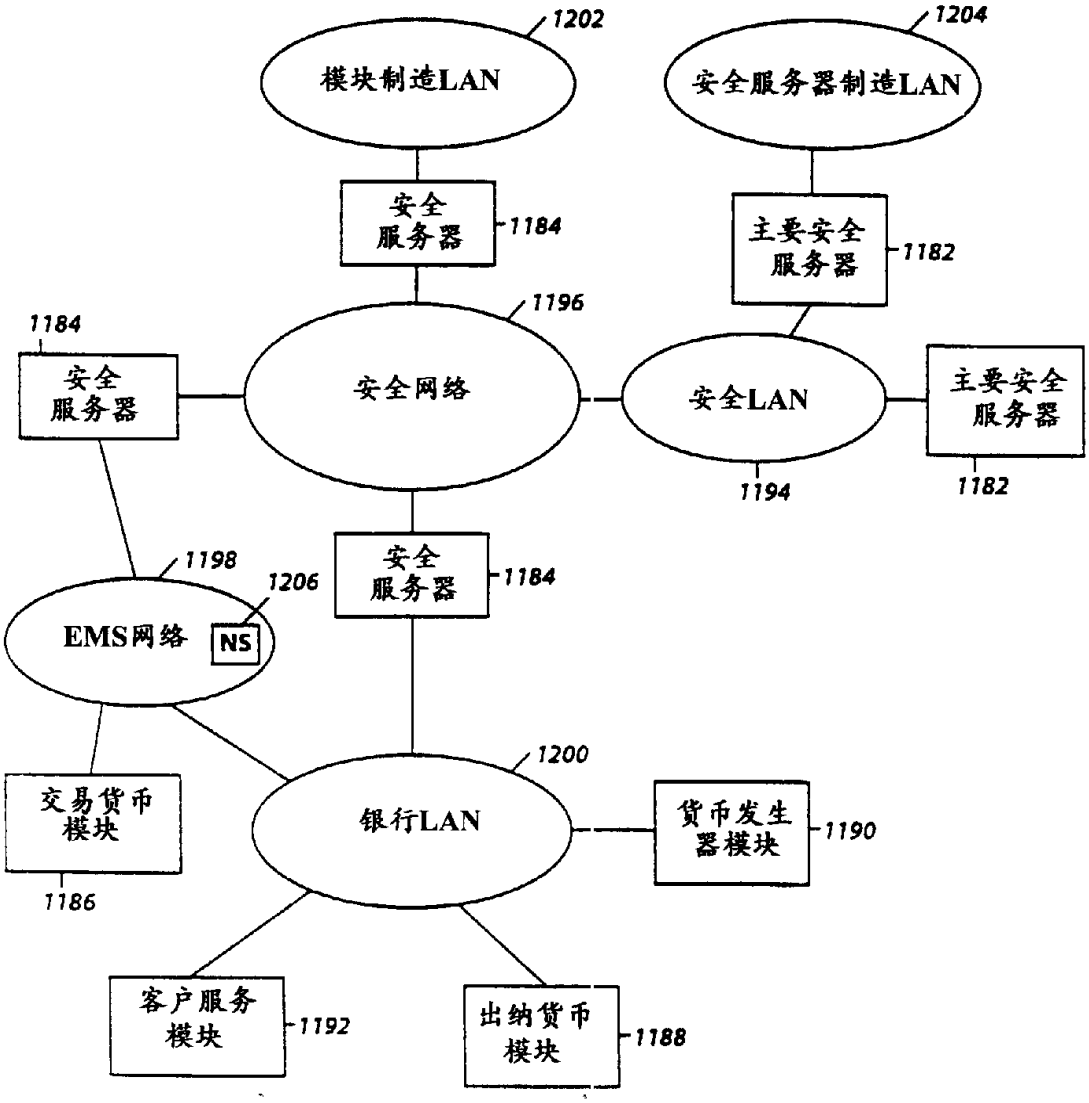

1202
模块制造LAN
1204
安全服务器制造LAN
安全
服务器
1184
主要安全
服务器
1182
1196
1184
安全
服务器
安全网络
安全LAN
主要安全
服务器
1194
1182
1198
1206
1184
安全
服务器
EMS网络
NS
1200
交易货币
模块
银行LAN
货币发生
器模块
1190
1186
客户服务
模块
1192
出纳货币
模块
1188

图 2

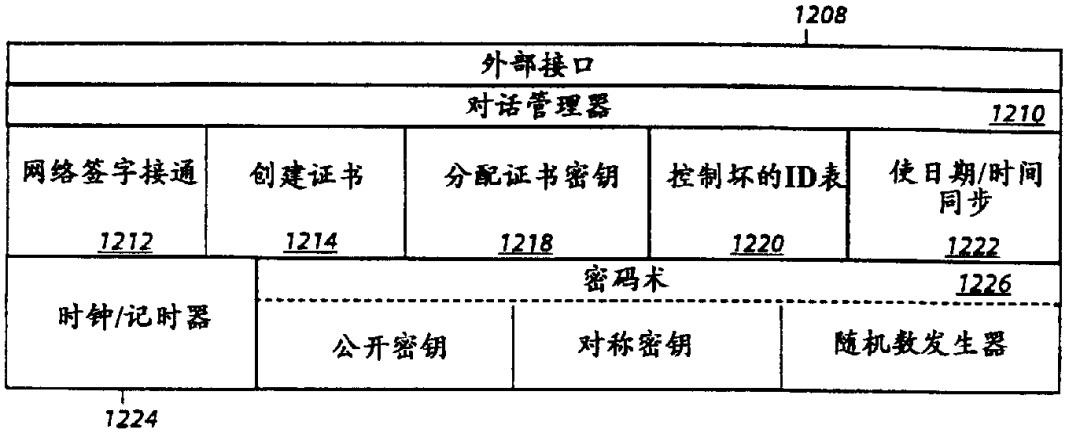

1208
外部接口
对话管理器
1210
网络签字接通
1212
创建证书
1214
分配证书密钥
1218
控制坏的ID表
1220
使日期/时间同步
1222
时钟/记时器
密码术
1226
公开密钥
对称密钥
随机数发生器
1224

图 3A

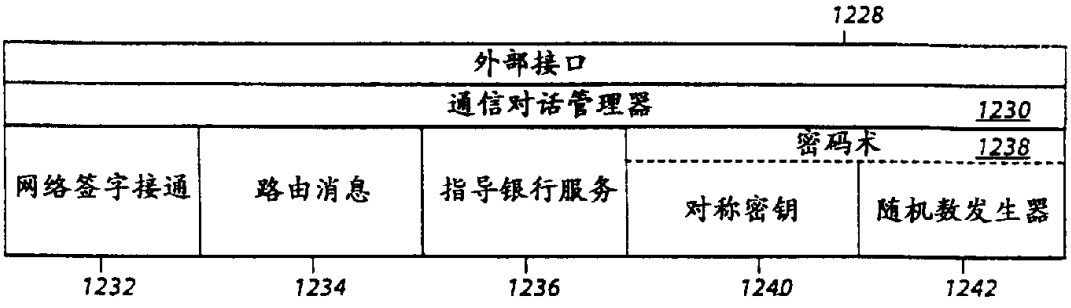

1228
外部接口
通信对话管理器
1230
密码术
1238
网络签字接通
路由消息
指导银行服务
对称密钥
随机数发生器
1232
1234
1236
1240
1242

图 3B

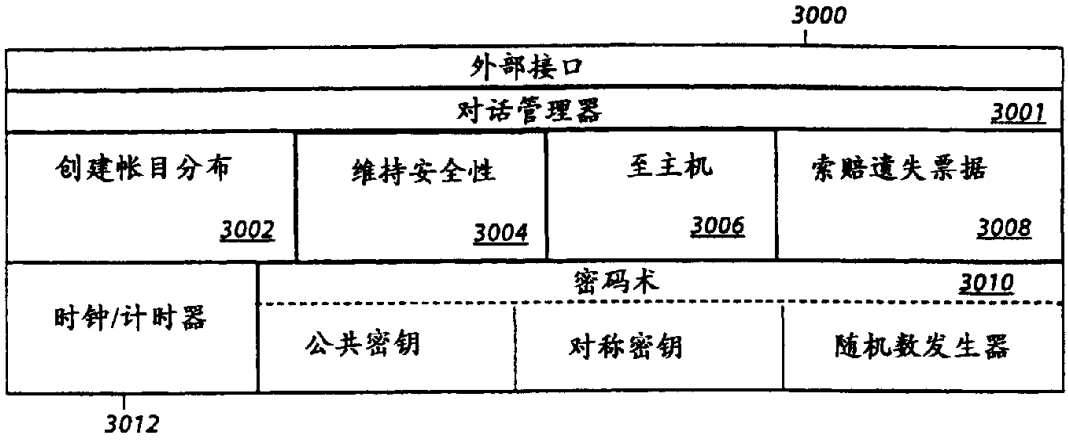

3000
外部接口
对话管理器
3001
创建帐目分布
3002
维持安全性
3004
至主机
3006
索赔遗失票据
3008
时钟/计时器
密码术
3010
公共密钥
对称密钥
随机数发生器
3012

图 4A

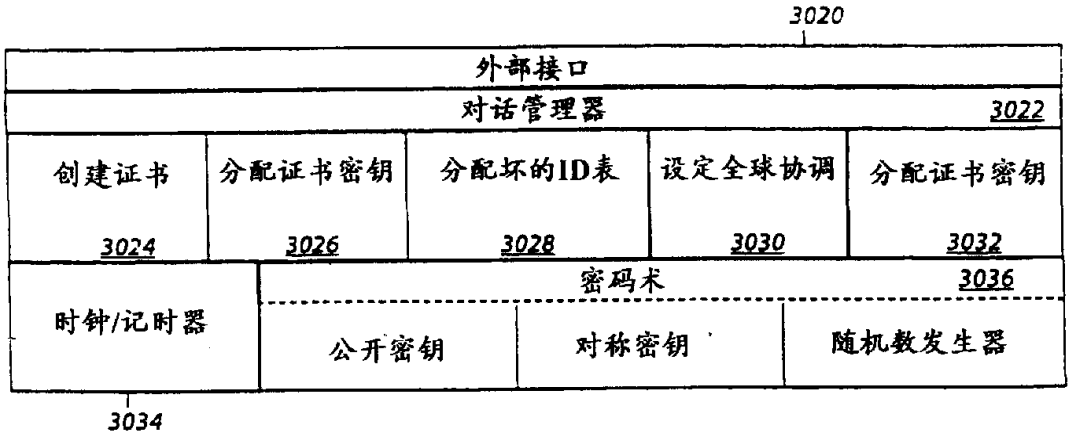

3020
外部接口
对话管理器
3022
创建证书
3024
分配证书密钥
3026
分配坏的ID表
3028
设定全球协调
3030
分配证书密钥
3032
时钟/记时器
密码术
3036
公开密钥
对称密钥
随机数发生器
3034

图 4B

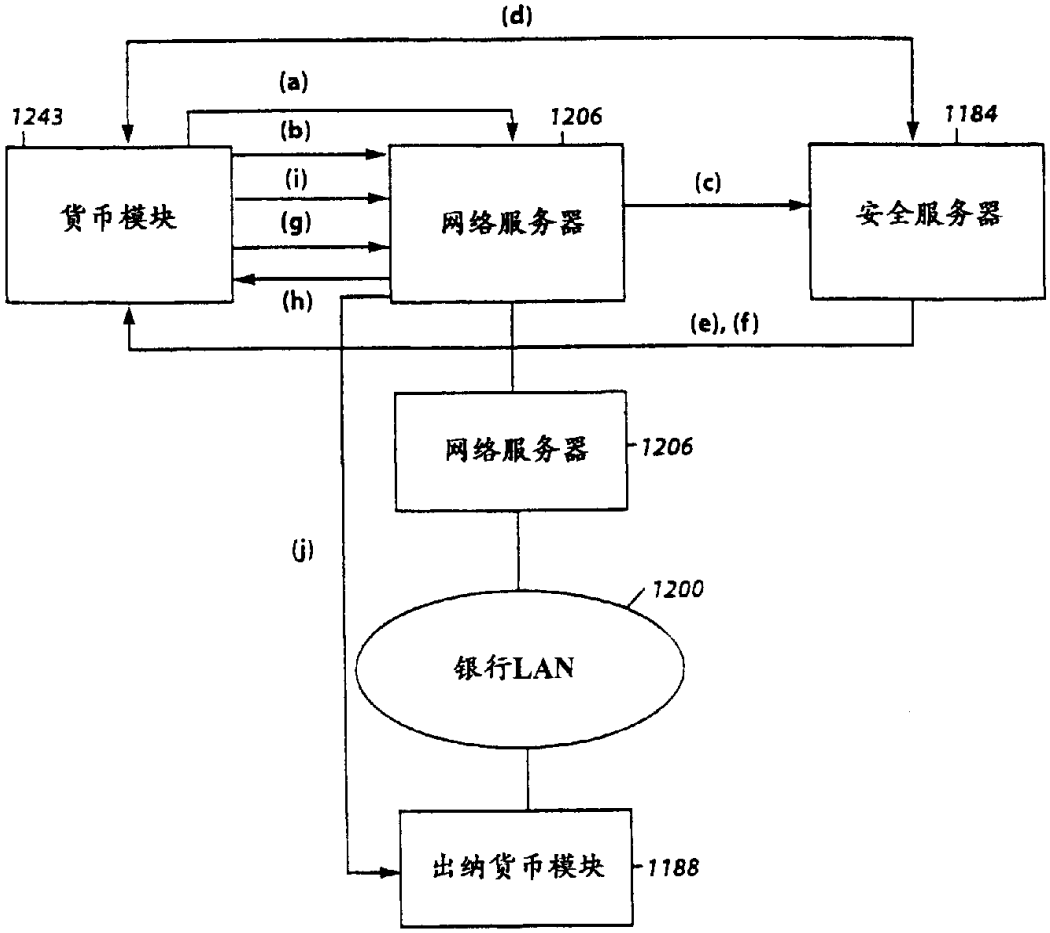

(d)
(a)
1243
(b)
1206
1184
(i)
(c)
货币模块
(g)
网络服务器
安全服务器
(h)
(e), (f)
网络服务器
1206
(j)
1200
银行LAN
出纳货币模块
1188

图 5

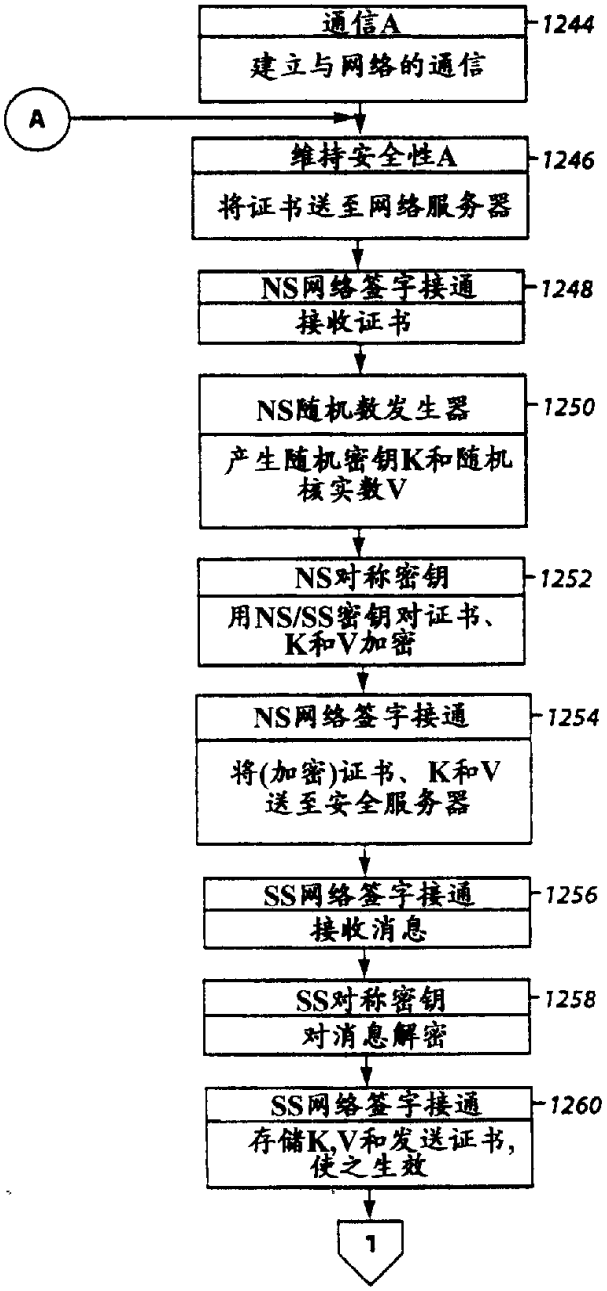

通信A
1244
建立与网络的通信
A
维持安全性A
1246
将证书送至网络服务器
NS网络签字接通
1248
接收证书
NS随机数发生器
1250
产生随机密钥K和随机核实数V
NS对称密钥
1252
用NS/SS密钥对证书、K和V加密
NS网络签字接通
1254
将(加密)证书、K和V送至安全服务器
SS网络签字接通
1256
接收消息
SS对称密钥
1258
对消息解密
SS网络签字接通
1260
存储K,V和发送证书，使之生效
1

图 6A

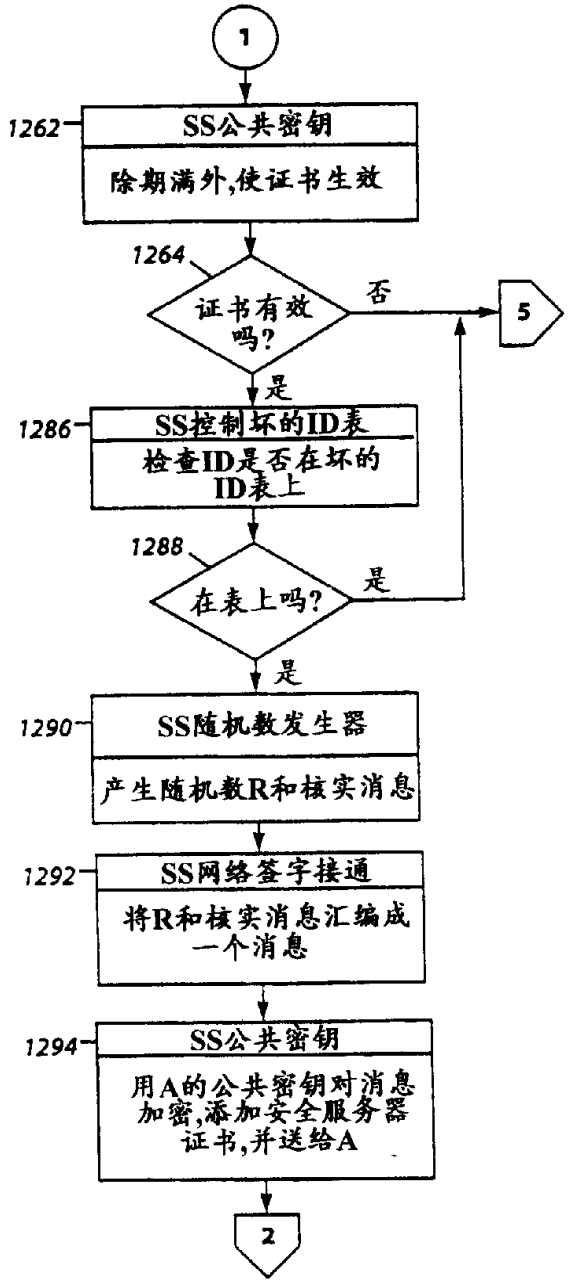

1
1262
SS公共密钥
除期满外,使证书生效
1264
证书有效吗?
否
5
是
1286
SS控制坏的ID表
检查ID是否在坏的ID表上
1288
在表上吗?
是
是
1290
SS随机数发生器
产生随机数R和核实消息
1292
SS网络签字接通
将R和核实消息汇编成一个消息
1294
SS公共密钥
用A的公共密钥对消息加密,添加安全服务器证书,并送给A
2

图 6B

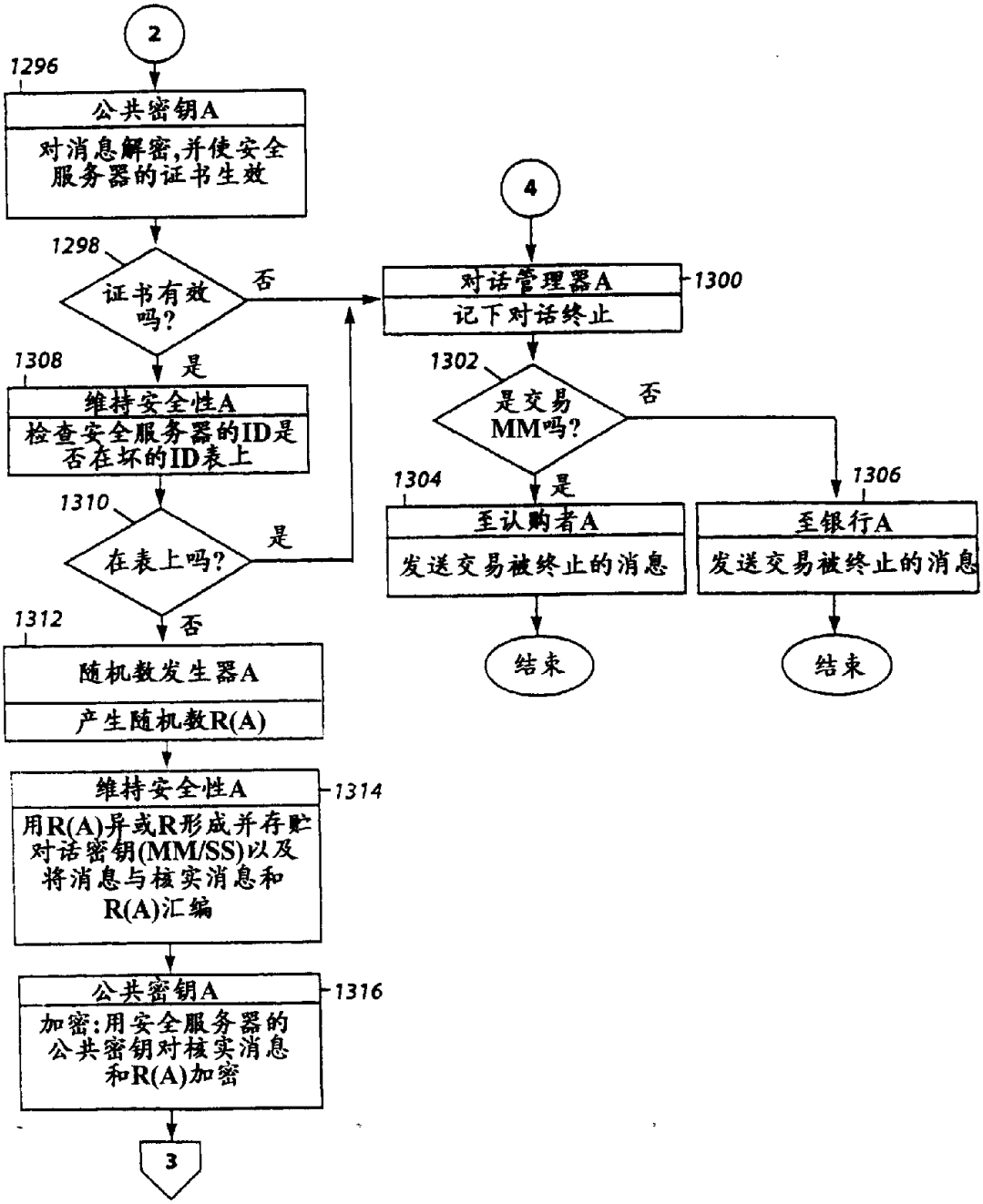

2
1296
公共密钥A
对消息解密,并使安全服务器的证书生效
1298
证书有效吗?
否
是
1308
维持安全性A
检查安全服务器的ID是否在坏的ID表上
1310
在表上吗?
是
否
1312
随机数发生器A
产生随机数R(A)
维持安全性A
1314
用R(A)异或R形成并存贮对话密钥(MM/SS)以及将消息与核实消息和R(A)汇编
公共密钥A
1316
加密:用安全服务器的公共密钥对核实消息和R(A)加密
3
4
对话管理器A
1300
记下对话终止
1302
是交易MM吗?
否
是
1304
至认购者A
发送交易被终止的消息
结束
1306
至银行A
发送交易被终止的消息
结束

图 6C

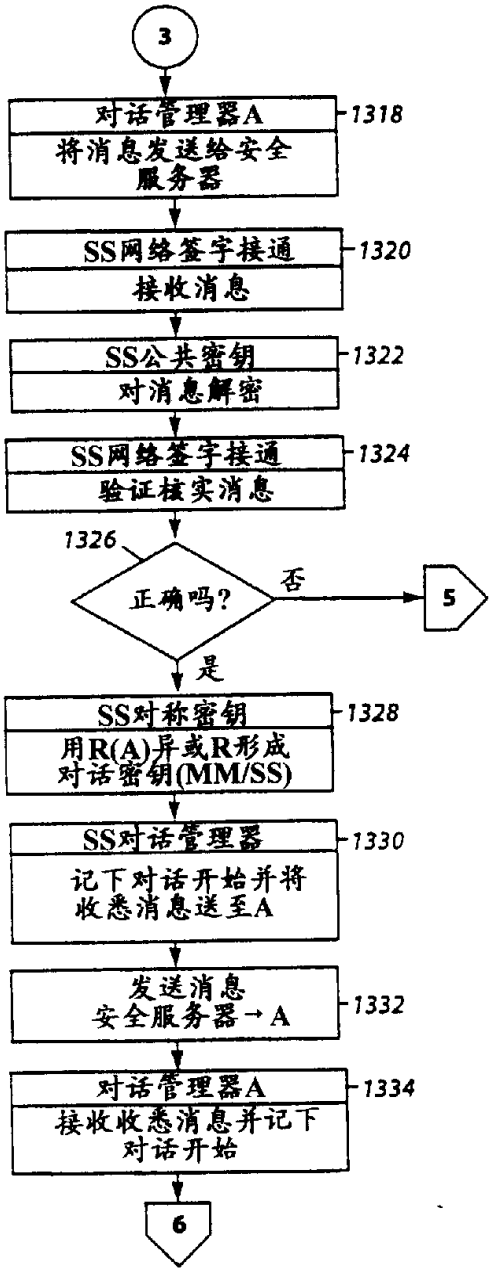

3
对话管理器A
将消息发送给安全服务器
1318
SS网络签字接通
接收消息
1320
SS公共密钥
对消息解密
1322
SS网络签字接通
验证核实消息
1324
1326
正确吗?
否
5
是
SS对称密钥
用R(A)异或R形成对话密钥(MM/SS)
1328
SS对话管理器
记下对话开始并将收悉消息送至A
1330
发送消息
安全服务器→A
1332
对话管理器A
接收收悉消息并记下对话开始
1334
6

图 6D

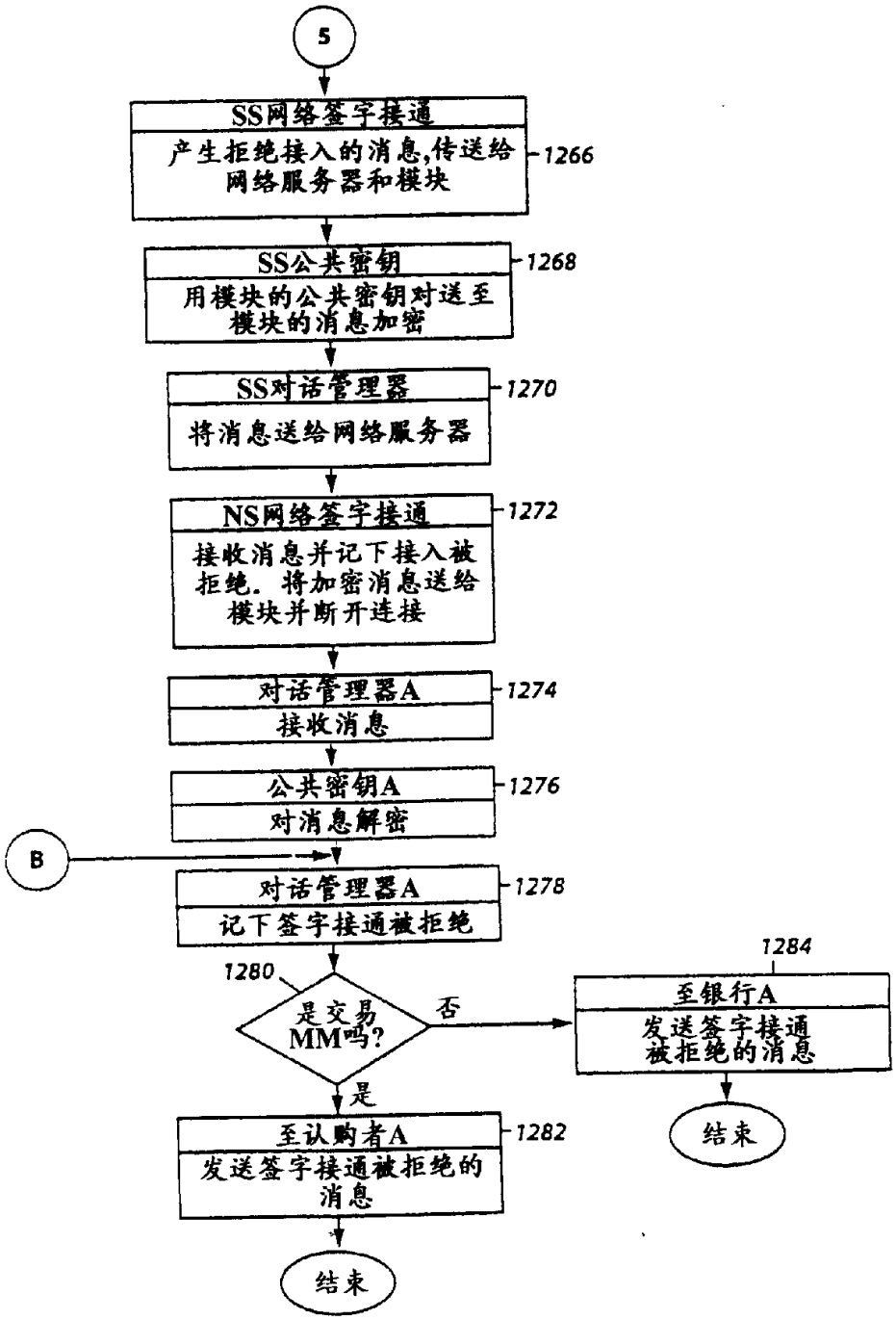

5
SS网络签字接通
产生拒绝接入的消息,传送给网络服务器和模块
1266
SS公共密钥
用模块的公共密钥对送至模块的消息加密
1268
SS对话管理器
将消息送给网络服务器
1270
NS网络签字接通
接收消息并记下接入被拒绝. 将加密消息送给模块并断开连接
1272
对话管理器A
接收消息
1274
公共密钥A
对消息解密
1276
B
对话管理器A
记下签字接通被拒绝
1278
1280
是交易MM吗?
否
是
1284
至银行A
发送签字接通被拒绝的消息
结束
至认购者A
发送签字接通被拒绝的消息
1282
结束

图 6E

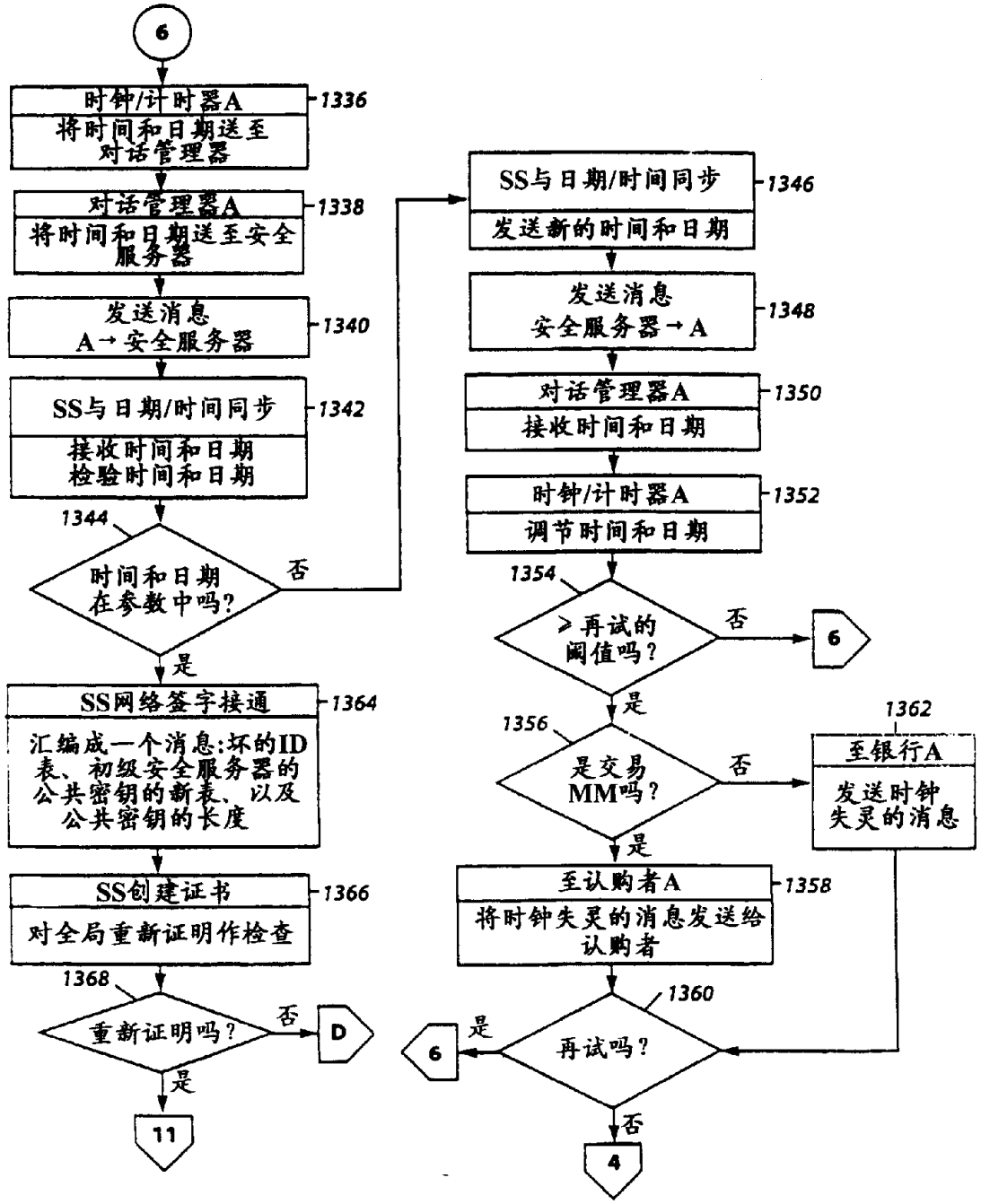

6
时钟/计时器A
将时间和日期送至对话管理器
1336
对话管理器A
将时间和日期送至安全服务器
1338
发送消息
A→安全服务器
1340
SS与日期/时间同步
接收时间和日期
检验时间和日期
1342
1344
时间和日期在参数中吗?
否
是
SS网络签字接通
汇编成一个消息:坏的ID表、初级安全服务器的公共密钥的新表、以及公共密钥的长度
1364
SS创建证书
对全局重新证明作检查
1366
1368
重新证明吗?
否
D
是
11
SS与日期/时间同步
发送新的时间和日期
1346
发送消息
安全服务器→A
1348
对话管理器A
接收时间和日期
1350
时钟/计时器A
调节时间和日期
1352
1354
≥再试的阈值吗?
否
6
是
1356
是交易MM吗?
否
1362
至银行A
发送时钟失灵的消息
是
至认购者A
将时钟失灵的消息发送给认购者
1358
1360
再试吗?
是
6
否
4

图 6F

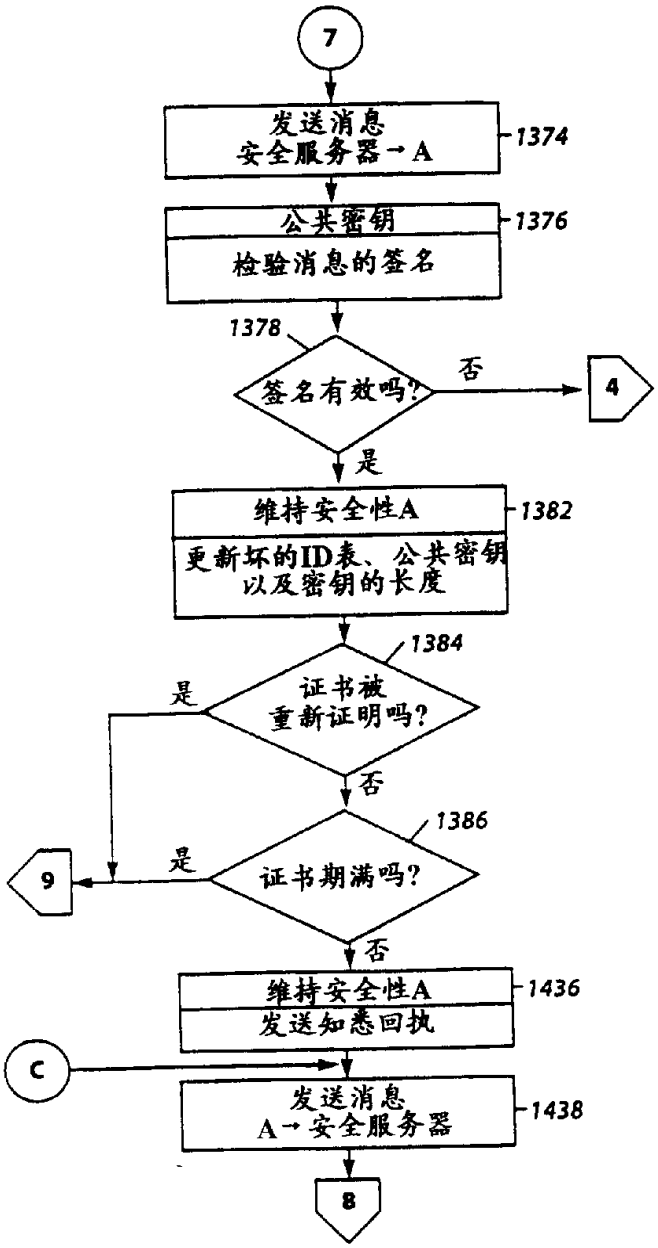

7
发送消息
安全服务器→A
1374
公共密钥
检验消息的签名
1376
1378
签名有效吗?
否
4
是
维持安全性A
更新坏的ID表、公共密钥
以及密钥的长度
1382
1384
证书被
重新证明吗?
是
否
1386
证书期满吗?
是
9
否
维持安全性A
发送知悉回执
1436
C
发送消息
A→安全服务器
1438
8

图 6G

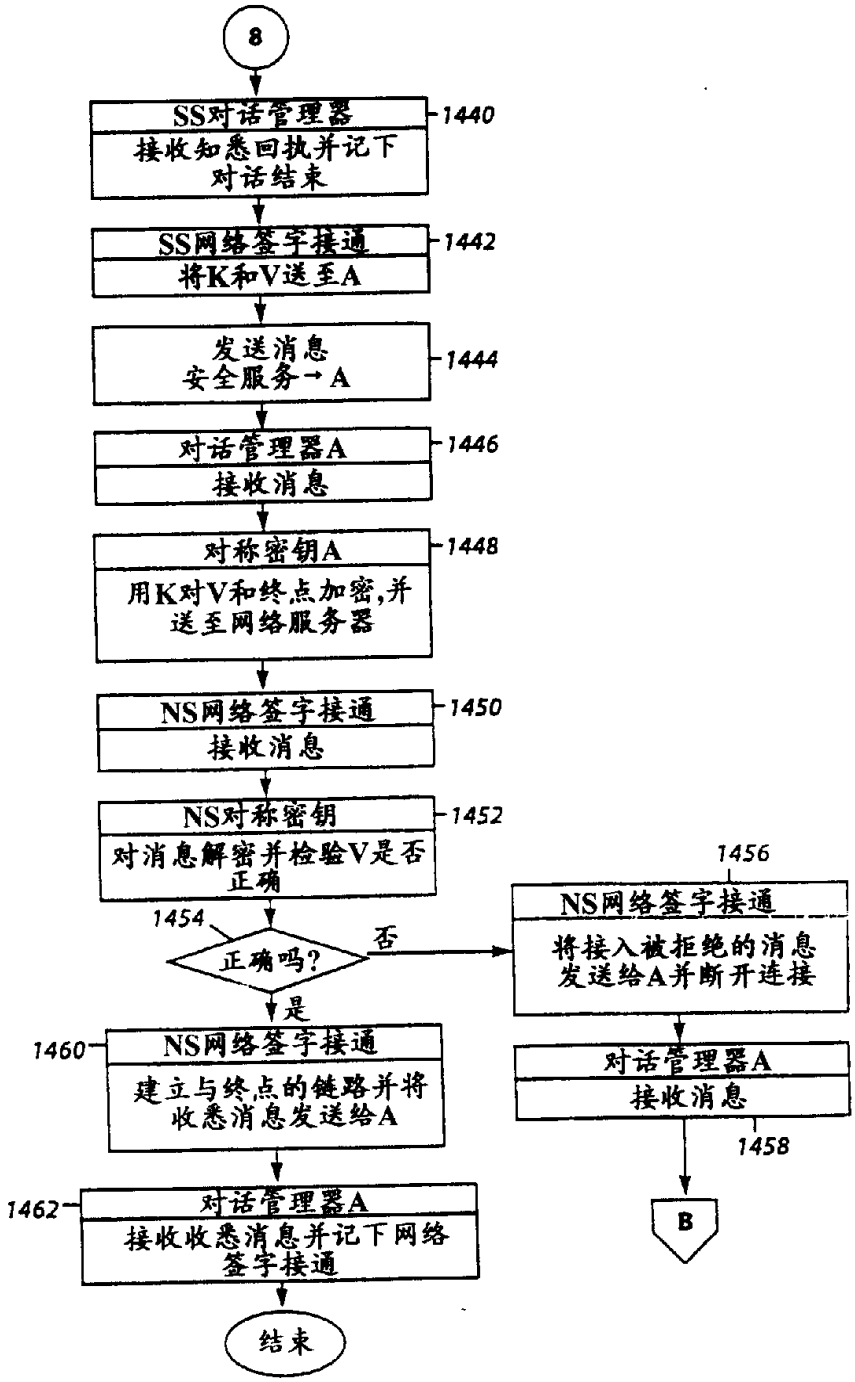

8
SS对话管理器
接收知悉回执并记下对话结束
1440
SS网络签字接通
将K和V送至A
1442
发送消息
安全服务→A
1444
对话管理器A
接收消息
1446
对称密钥A
用K对V和终点加密,并送至网络服务器
1448
NS网络签字接通
接收消息
1450
NS对称密钥
对消息解密并检验V是否正确
1452
1454
正确吗?
否
是
1456
NS网络签字接通
将接入被拒绝的消息发送给A并断开连接
对话管理器A
接收消息
1458
B
1460
NS网络签字接通
建立与终点的链路并将收悉消息发送给A
1462
对话管理器A
接收收悉消息并记下网络签字接通
结束

图 6H

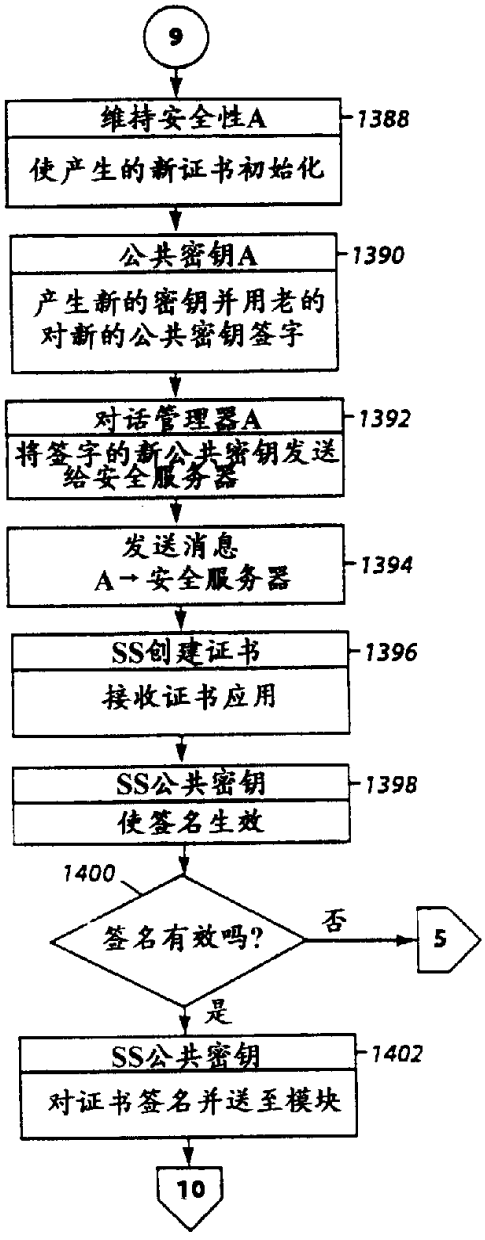

9
维持安全性A
使产生的新证书初始化
1388
公共密钥A
产生新的密钥并用老的对新的公共密钥签字
1390
对话管理器A
将签字的新公共密钥发送给安全服务器
1392
发送消息
A→安全服务器
1394
SS创建证书
接收证书应用
1396
SS公共密钥
使签名生效
1398
1400
签名有效吗?
否
5
是
SS公共密钥
对证书签名并送至模块
1402
10

图 6I

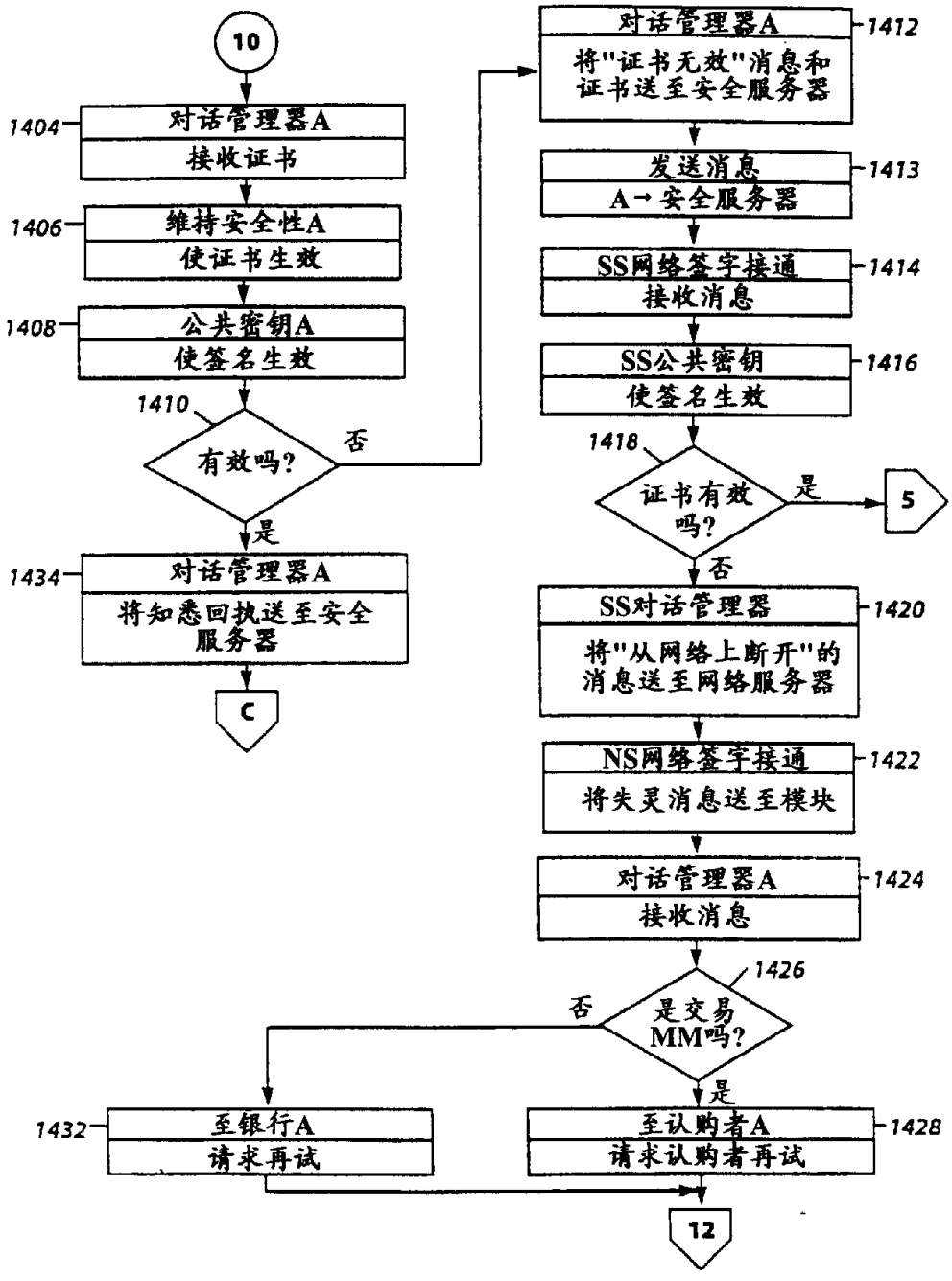

10
1404
对话管理器A
接收证书
1406
维持安全性A
使证书生效
1408
公共密钥A
使签名生效
1410
有效吗?
否
是
1434
对话管理器A
将知悉回执送至安全服务器
C
对话管理器A
1412
将"证书无效"消息和证书送至安全服务器
发送消息
1413
A→安全服务器
SS网络签字接通
1414
接收消息
SS公共密钥
1416
使签名生效
1418
证书有效吗?
是
5
否
SS对话管理器
1420
将"从网络上断开"的消息送至网络服务器
NS网络签字接通
1422
将失灵消息送至模块
对话管理器A
1424
接收消息
1426
是交易MM吗?
否
是
1432
至银行A
请求再试
至认购者A
1428
请求认购者再试
12

图 6J

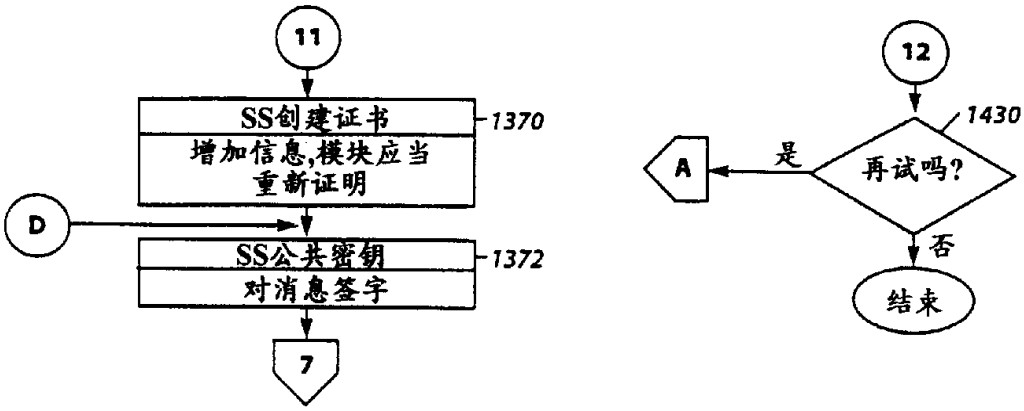

11
SS创建证书
增加信息,模块应当
重新证明
1370
D
SS公共密钥
对消息签字
1372
7
12
1430
A
是
再试吗?
否
结束

图 6K

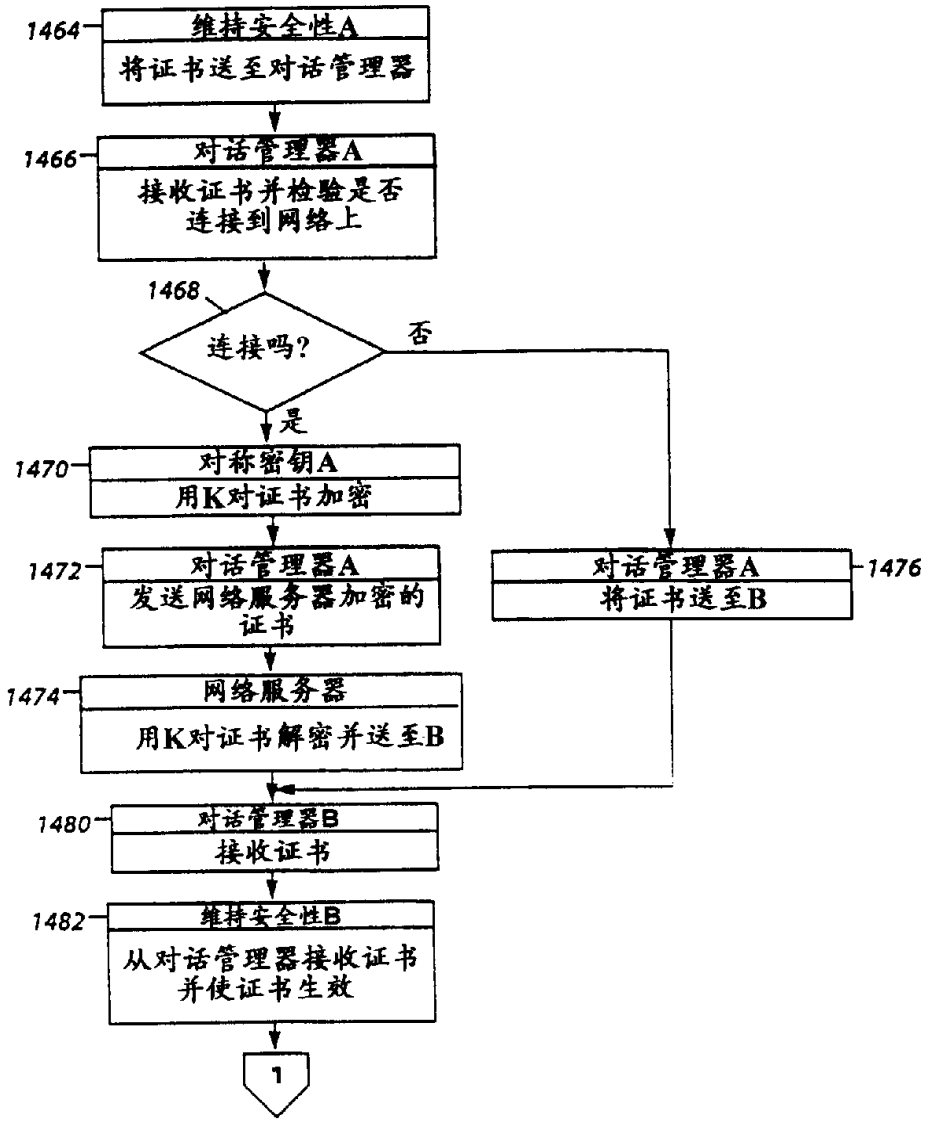

1464
维持安全性A
将证书送至对话管理器
1466
对话管理器A
接收证书并检验是否连接到网络上
1468
连接吗?
否
是
1470
对称密钥A
用K对证书加密
1472
对话管理器A
发送网络服务器加密的证书
1474
网络服务器
用K对证书解密并送至B
对话管理器A
将证书送至B
1476
1480
对话管理器B
接收证书
1482
维持安全性B
从对话管理器接收证书并使证书生效
1

图 7A

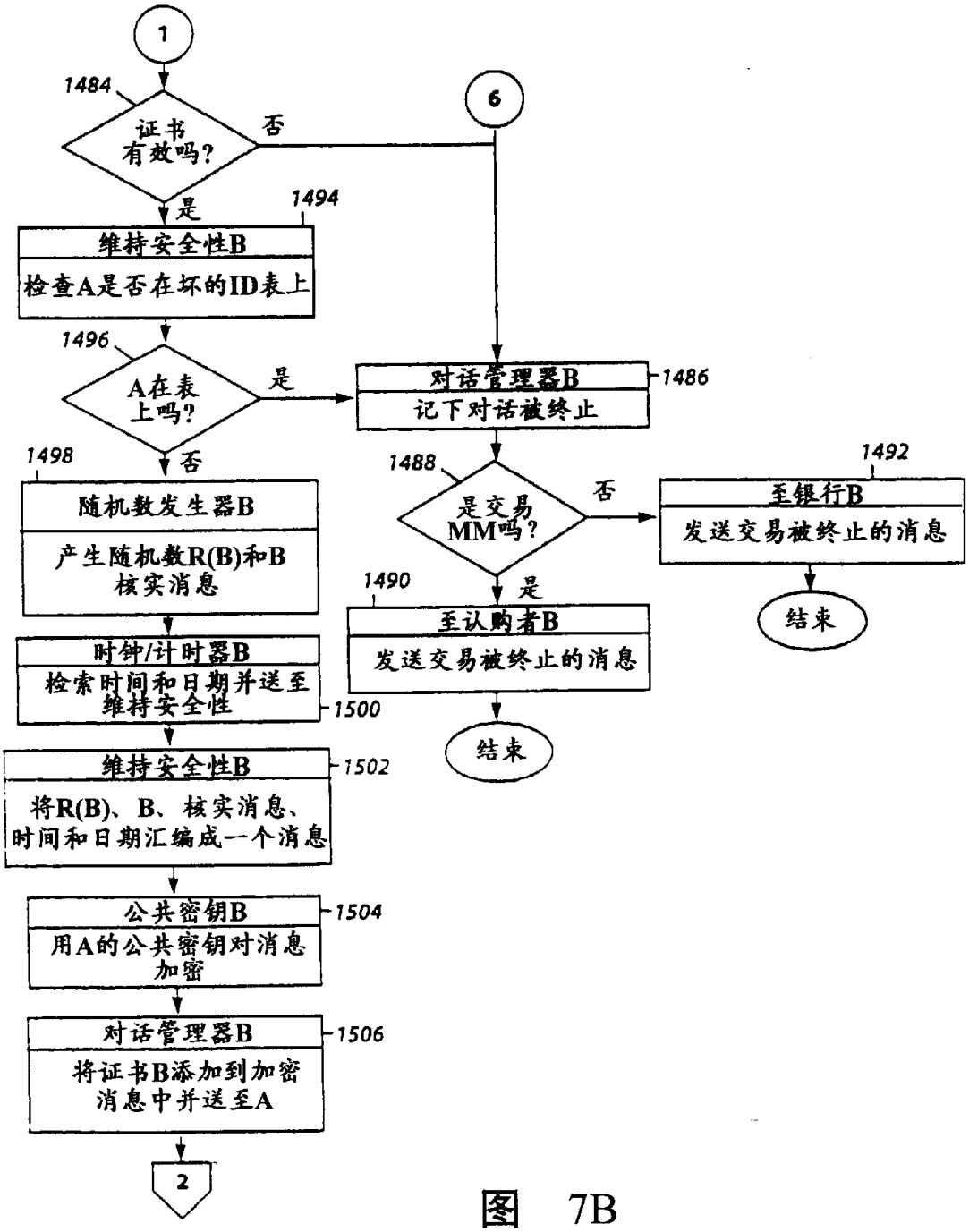

1
1484
证书有效吗?
否
是
6
1494
维持安全性B
检查A是否在坏的ID表上
1496
A在表上吗?
是
否
对话管理器B
记下对话被终止
1486
1488
是交易MM吗?
否
是
1492
至银行B
发送交易被终止的消息
结束
1490
至认购者B
发送交易被终止的消息
结束
1498
随机数发生器B
产生随机数R(B)和B核实消息
时钟/计时器B
检索时间和日期并送至维持安全性
1500
维持安全性B
1502
将R(B)、B、核实消息、时间和日期汇编成一个消息
公共密钥B
1504
用A的公共密钥对消息加密
对话管理器B
1506
将证书B添加到加密消息中并送至A
2

图 7B

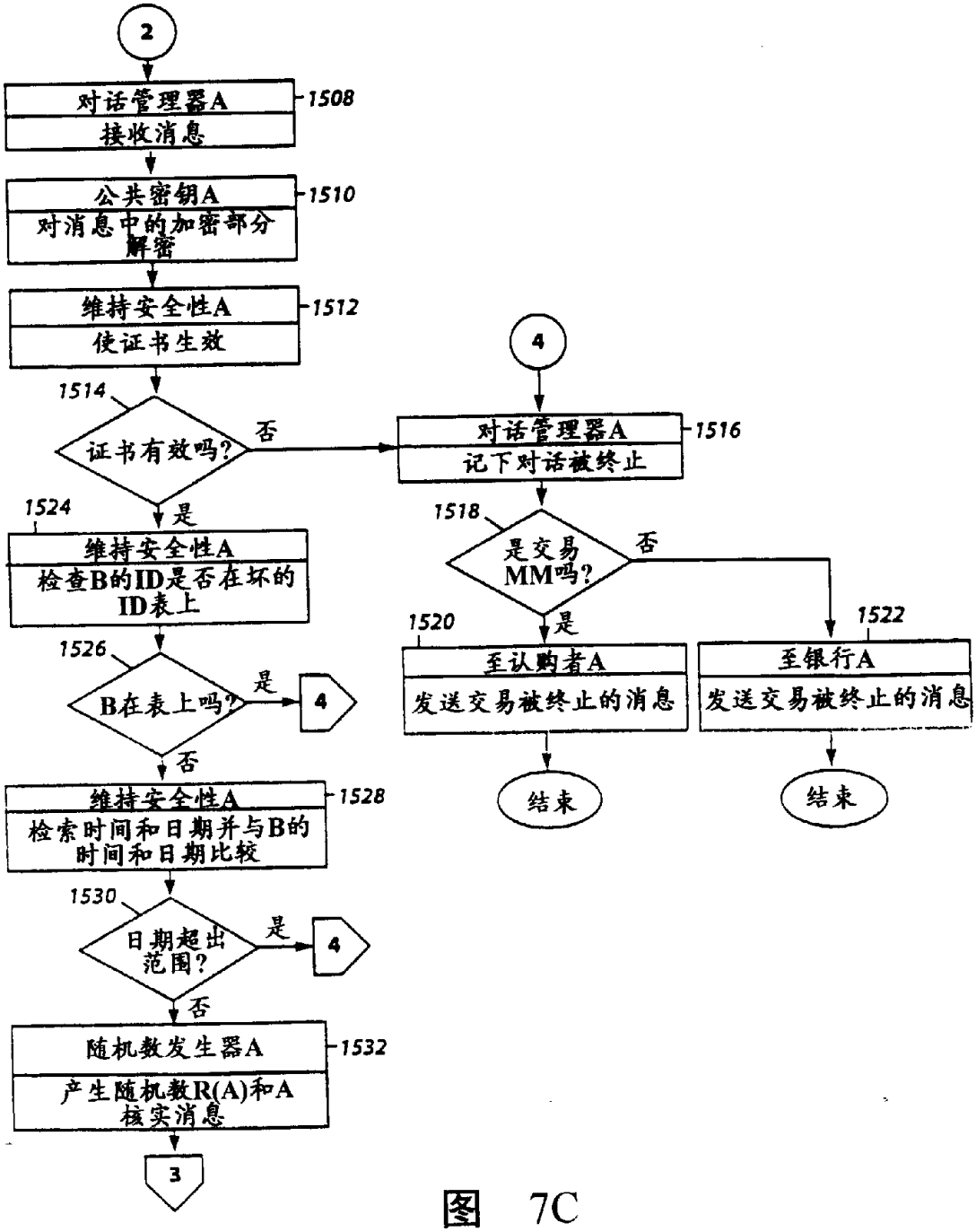

2
对话管理器A
接收消息
1508
公共密钥A
对消息中的加密部分解密
1510
维持安全性A
使证书生效
1512
1514
证书有效吗?
否
是
4
对话管理器A
记下对话被终止
1516
1518
是交易MM吗?
否
是
1520
至认购者A
发送交易被终止的消息
1522
至银行A
发送交易被终止的消息
结束
结束
1524
维持安全性A
检查B的ID是否在坏的ID表上
1526
B在表上吗?
是
4
否
维持安全性A
检索时间和日期并与B的时间和日期比较
1528
1530
日期超出范围?
是
4
否
随机数发生器A
产生随机数R(A)和A核实消息
1532
3

图 7C

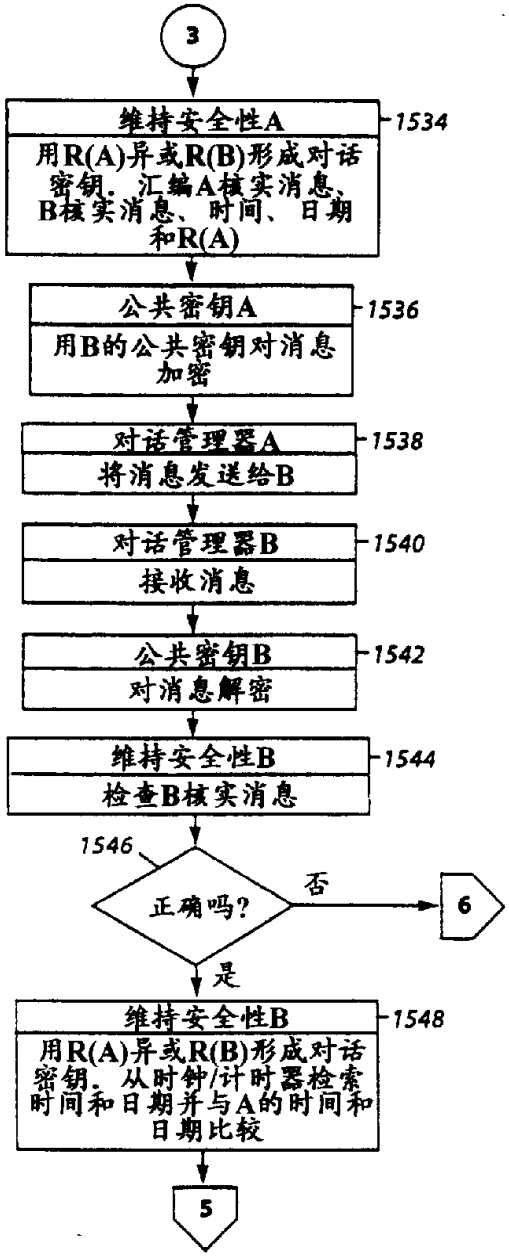

3
维持安全性A
用R(A)异或R(B)形成对话密钥，汇编A核实消息、B核实消息、时间、日期和R(A)
1534
公共密钥A
用B的公共密钥对消息加密
1536
对话管理器A
将消息发送给B
1538
对话管理器B
接收消息
1540
公共密钥B
对消息解密
1542
维持安全性B
检查B核实消息
1544
1546
正确吗?
否
6
是
维持安全性B
用R(A)异或R(B)形成对话密钥，从时钟/计时器检索时间和日期并与A的时间和日期比较
1548
5

图 7D

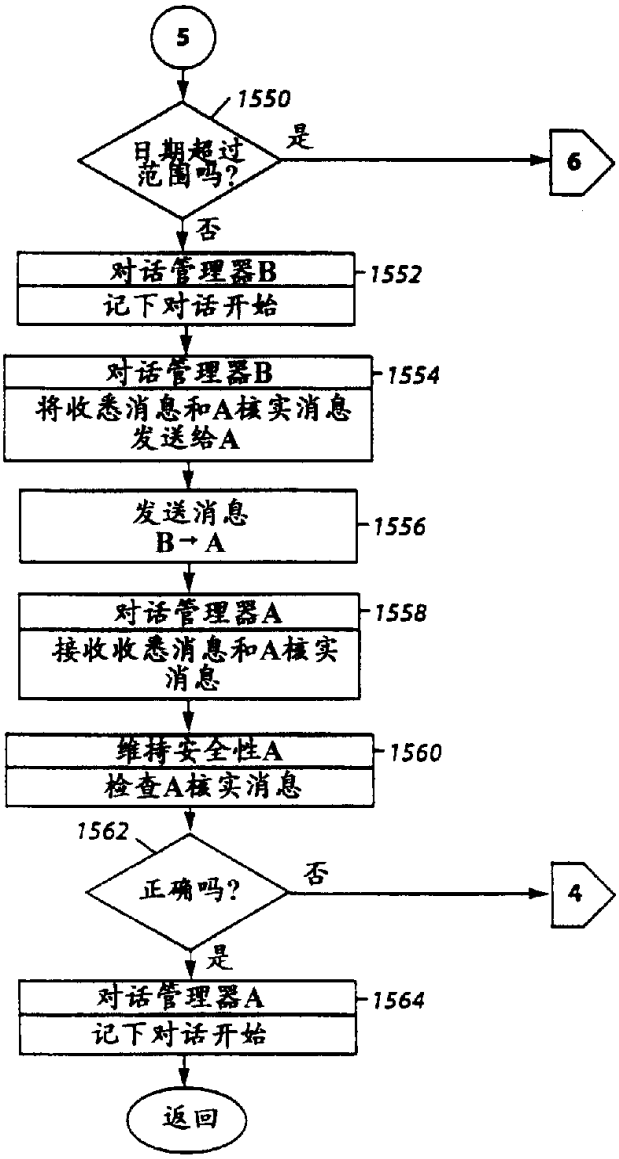

5
1550
日期超过范围吗?
是
6
否
对话管理器B
记下对话开始
1552
对话管理器B
将收悉消息和A核实消息发送给A
1554
发送消息
B→A
1556
对话管理器A
接收收悉消息和A核实消息
1558
维持安全性A
检查A核实消息
1560
1562
正确吗?
否
4
是
对话管理器A
记下对话开始
1564
返回

图 7E

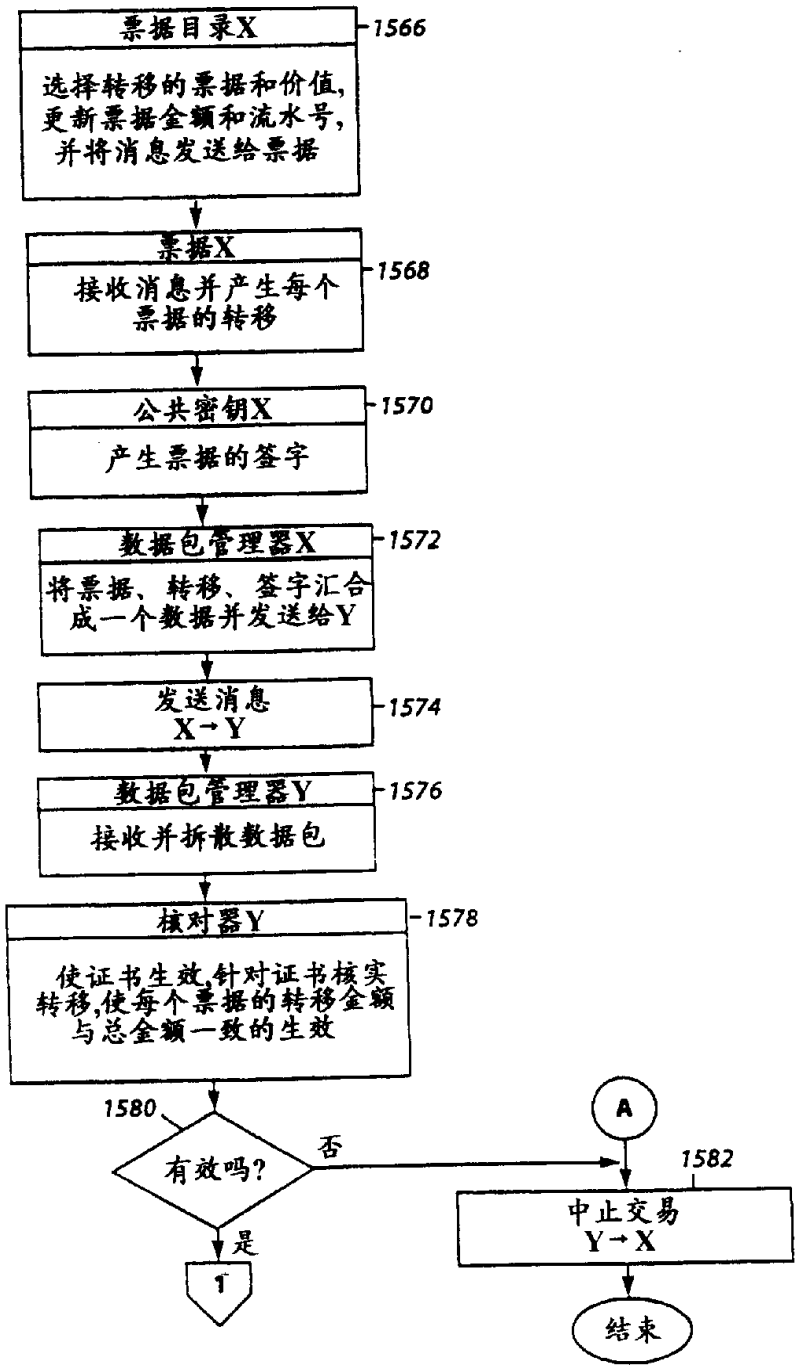

票据目录X
1566
选择转移的票据和价值，更新票据金额和流水号，并将消息发送给票据
票据X
1568
接收消息并产生每个票据的转移
公共密钥X
1570
产生票据的签字
数据包管理器X
1572
将票据、转移、签字汇合成一个数据并发送给Y
发送消息
X→Y
1574
数据包管理器Y
1576
接收并拆散数据包
核对器Y
1578
使证书生效，针对证书核实转移，使每个票据的转移金额与总金额一致的生效
1580
有效吗？
否
是
1
A
1582
中止交易
Y→X
结束

图 8A

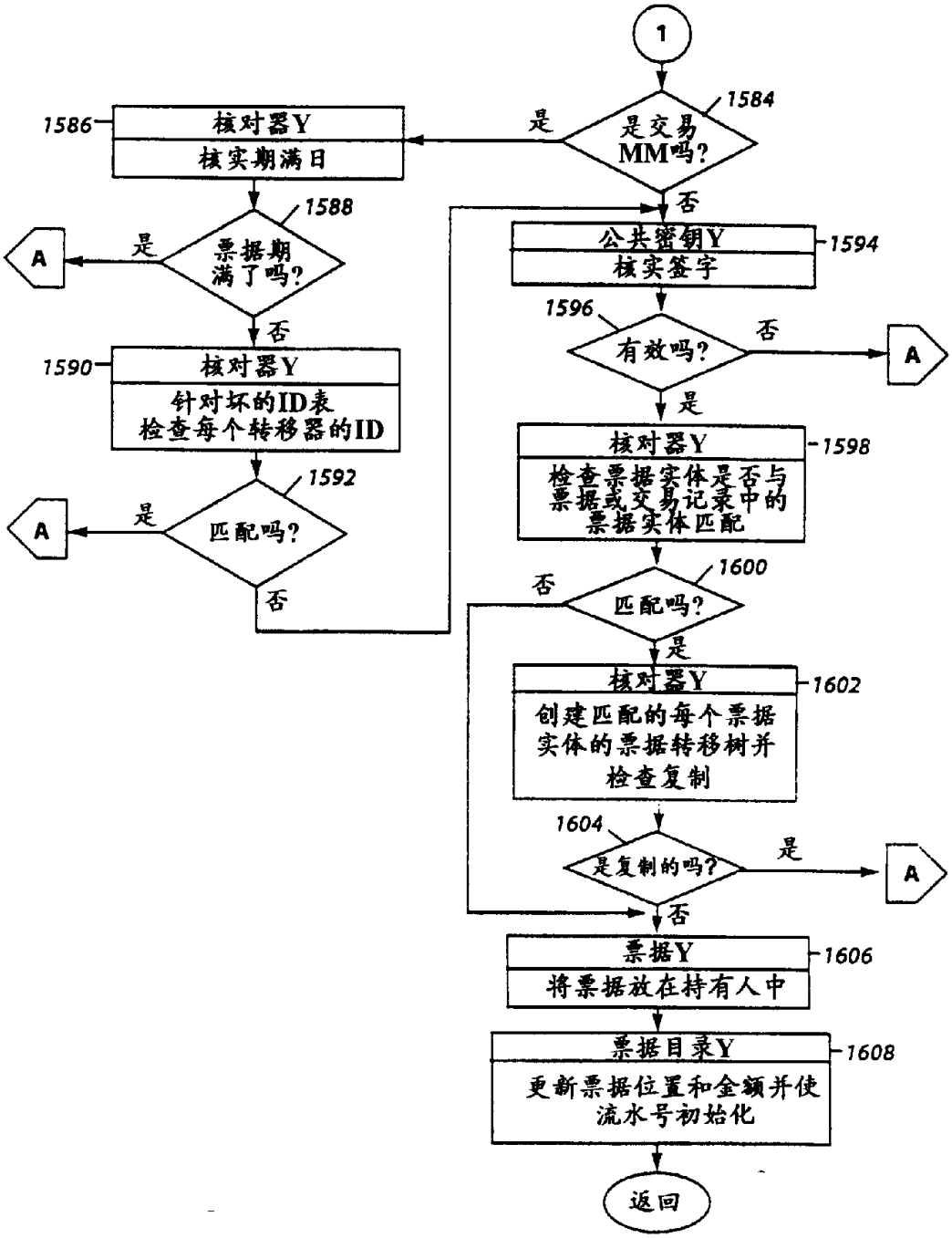

1
1584
是交易MM吗?
是
否
1586
核对器Y
核实期满日
1588
票据期满了吗?
是
A
否
1590
核对器Y
针对坏的ID表检查每个转移器的ID
1592
匹配吗?
是
A
否
公共密钥Y
核实签字
1594
1596
有效吗?
否
A
是
核对器Y
检查票据实体是否与票据或交易记录中的票据实体匹配
1598
1600
匹配吗?
否
是
核对器Y
创建匹配的每个票据实体的票据转移树并检查复制
1602
1604
是复制的吗?
是
A
否
票据Y
将票据放在持有人中
1606
票据目录Y
更新票据位置和金额并使流水号初始化
1608
返回

图 8B

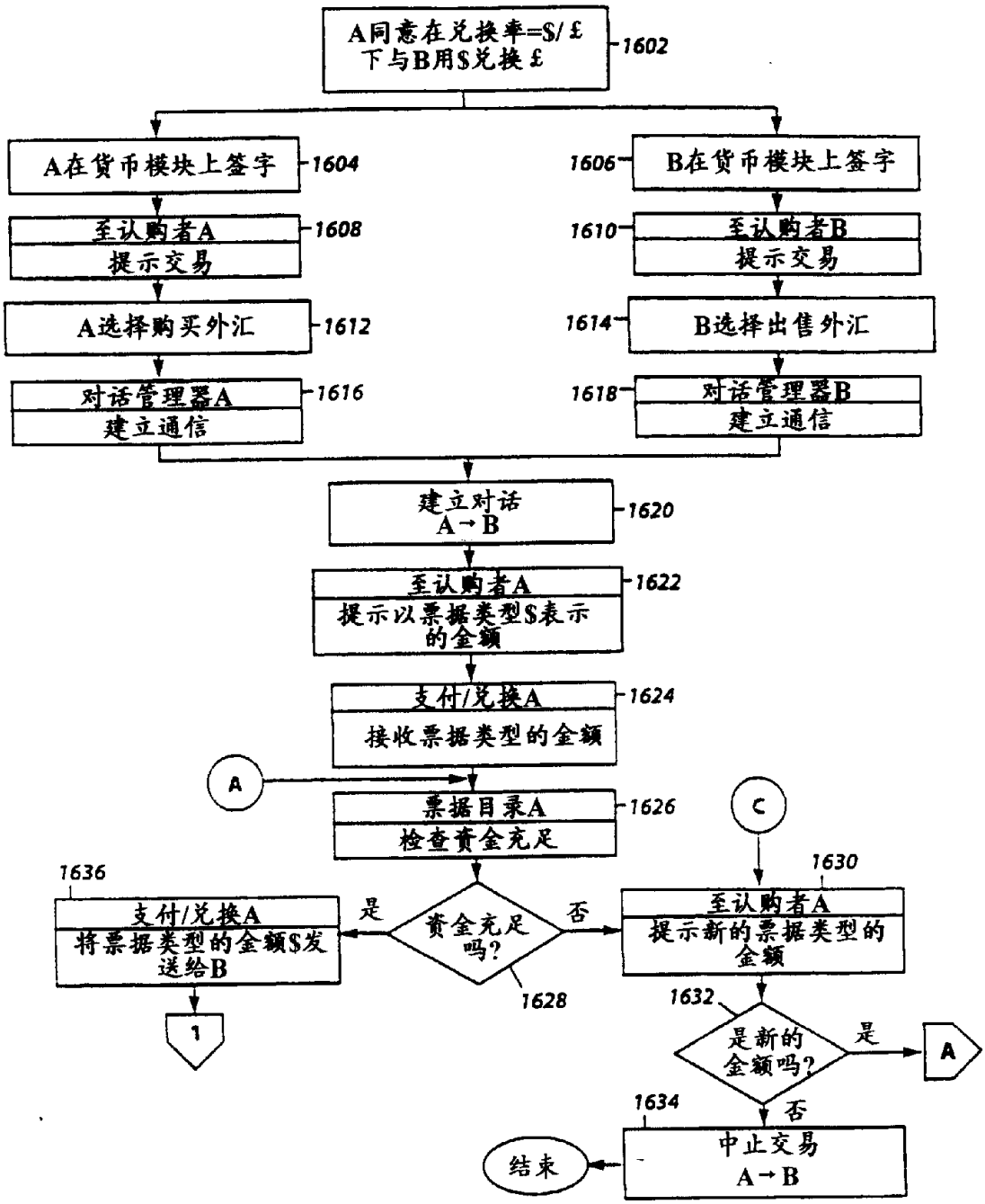

A同意在兑换率=$/£
下与B用$兑换£
1602
A在货币模块上签字
1604
B在货币模块上签字
1606
至认购者A
提示交易
1608
至认购者B
提示交易
1610
A选择购买外汇
1612
B选择出售外汇
1614
对话管理器A
建立通信
1616
对话管理器B
建立通信
1618
建立对话
A→B
1620
至认购者A
提示以票据类型$表示的金额
1622
支付/兑换A
接收票据类型的金额
1624
A
票据目录A
检查资金充足
1626
C
1630
1636
支付/兑换A
将票据类型的金额$发送给B
是
资金充足吗?
否
1628
至认购者A
提示新的票据类型的金额
1632
1
是新的金额吗?
是
A
否
1634
结束
中止交易
A→B

图 9A

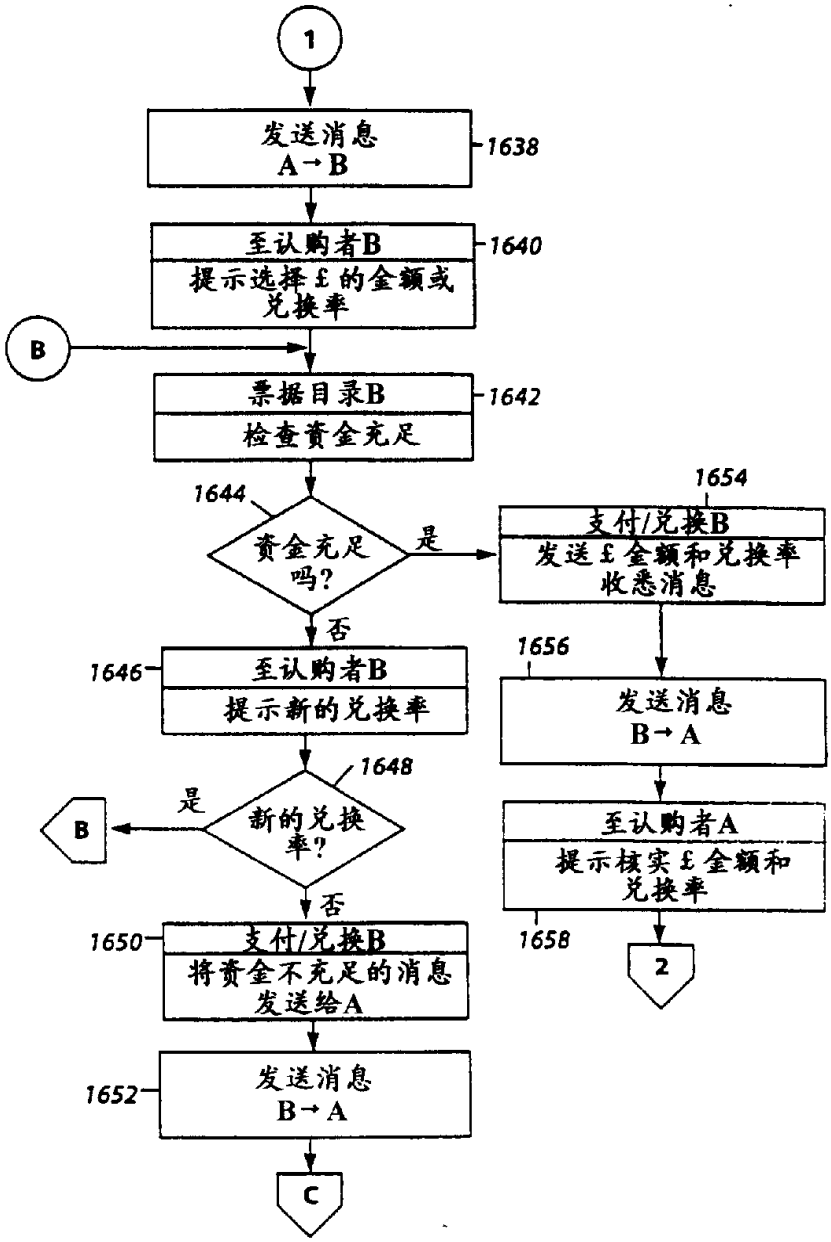

1
发送消息
A→B
1638
至认购者B
提示选择£的金额或
兑换率
1640
B
票据目录B
检查资金充足
1642
1644
资金充足
吗?
是
1654
支付/兑换B
发送£金额和兑换率
收悉消息
否
1646
至认购者B
提示新的兑换率
1656
发送消息
B→A
1648
是
B
新的兑换
率?
至认购者A
提示核实£金额和
兑换率
否
1650
支付/兑换B
将资金不充足的消息
发送给A
1658
2
发送消息
B→A
1652
C

图 9B

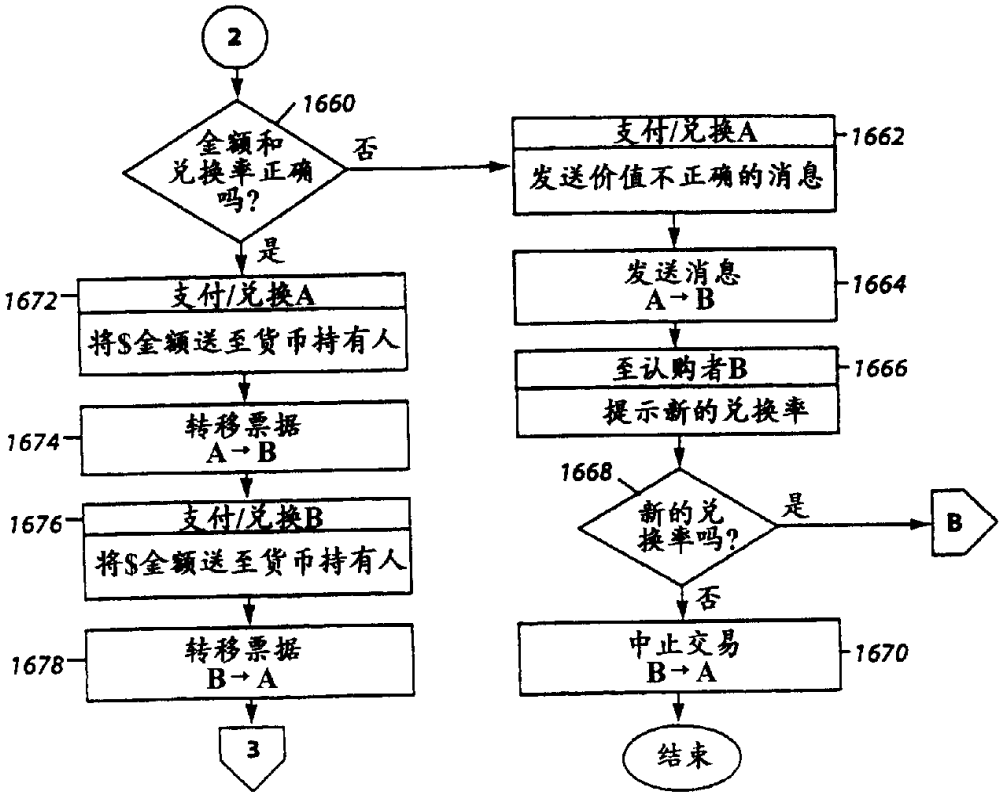

2
1660
金额和
兑换率正确
吗?
否
是
支付/兑换A
发送价值不正确的消息
1662
发送消息
A→B
1664
至认购者B
提示新的兑换率
1666
1668
新的兑
换率吗?
是
B
否
中止交易
B→A
1670
结束
1672
支付/兑换A
将$金额送至货币持有人
1674
转移票据
A→B
1676
支付/兑换B
将$金额送至货币持有人
1678
转移票据
B→A
3

图 9C

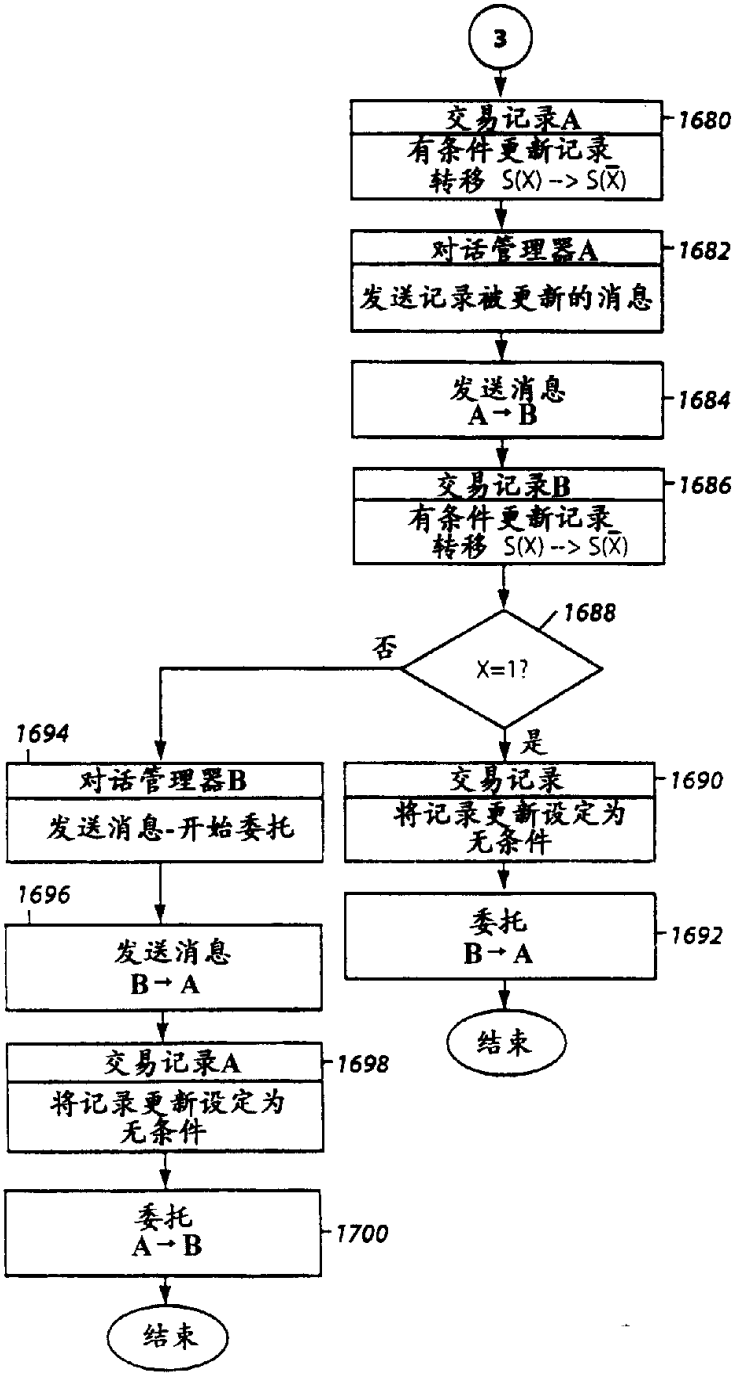

3
交易记录A
有条件更新记录
转移 S(X) --> S(X̄)
1680
对话管理器A
发送记录被更新的消息
1682
发送消息
A→B
1684
交易记录B
有条件更新记录
转移 S(X) --> S(X̄)
1686
1688
X=1?
否
是
1694
对话管理器B
发送消息-开始委托
交易记录
将记录更新设定为
无条件
1690
1696
发送消息
B→A
委托
B→A
1692
结束
交易记录A
将记录更新设定为
无条件
1698
委托
A→B
1700
结束

图 9D

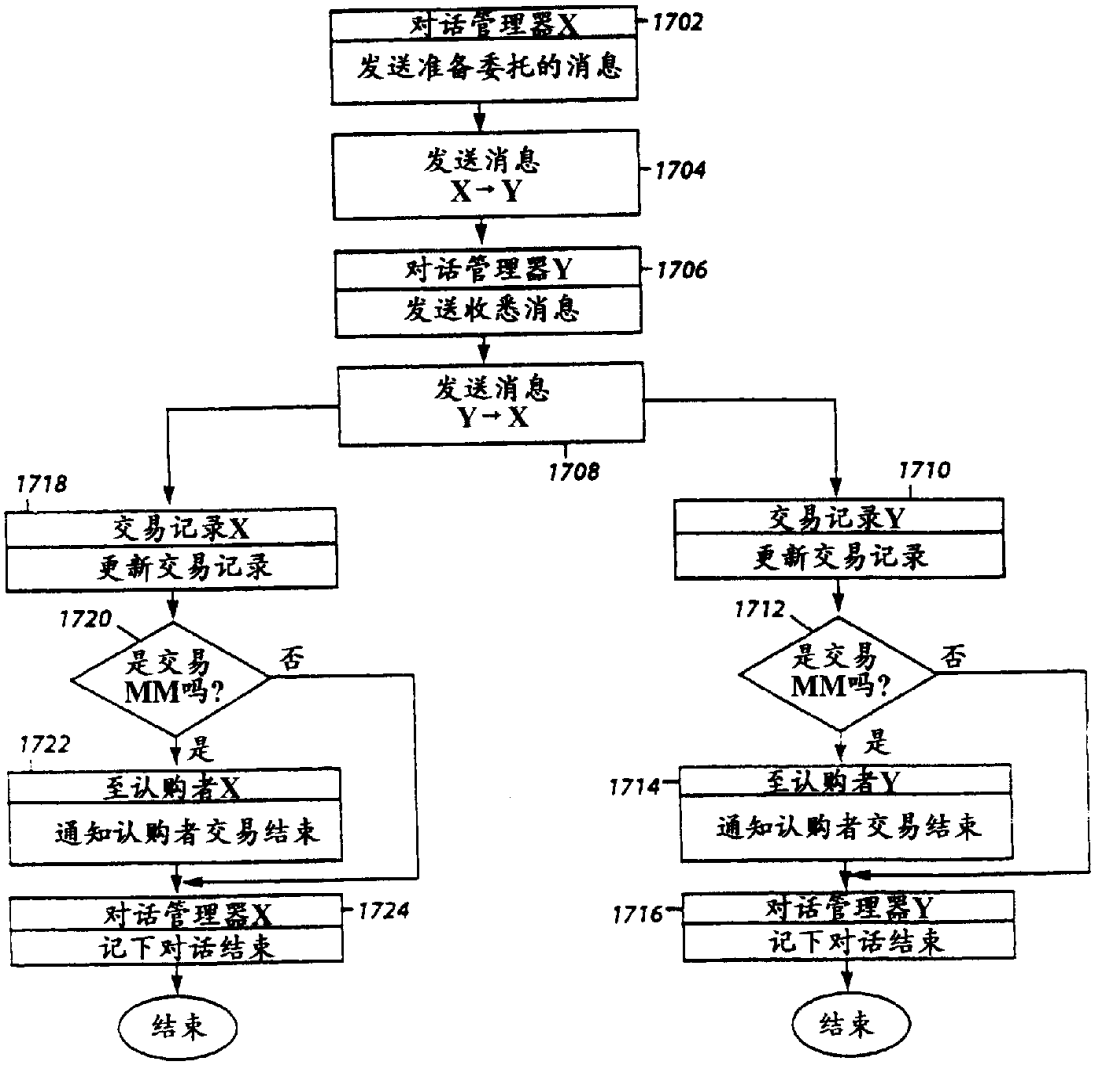

对话管理器X
发送准备委托的消息
1702
发送消息
X→Y
1704
对话管理器Y
发送收悉消息
1706
发送消息
Y→X
1708
1718
交易记录X
更新交易记录
1720
是交易
MM吗?
否
是
1722
至认购者X
通知认购者交易结束
对话管理器X
记下对话结束
1724
结束
1710
交易记录Y
更新交易记录
1712
是交易
MM吗?
否
是
1714
至认购者Y
通知认购者交易结束
1716
对话管理器Y
记下对话结束
结束

图 10

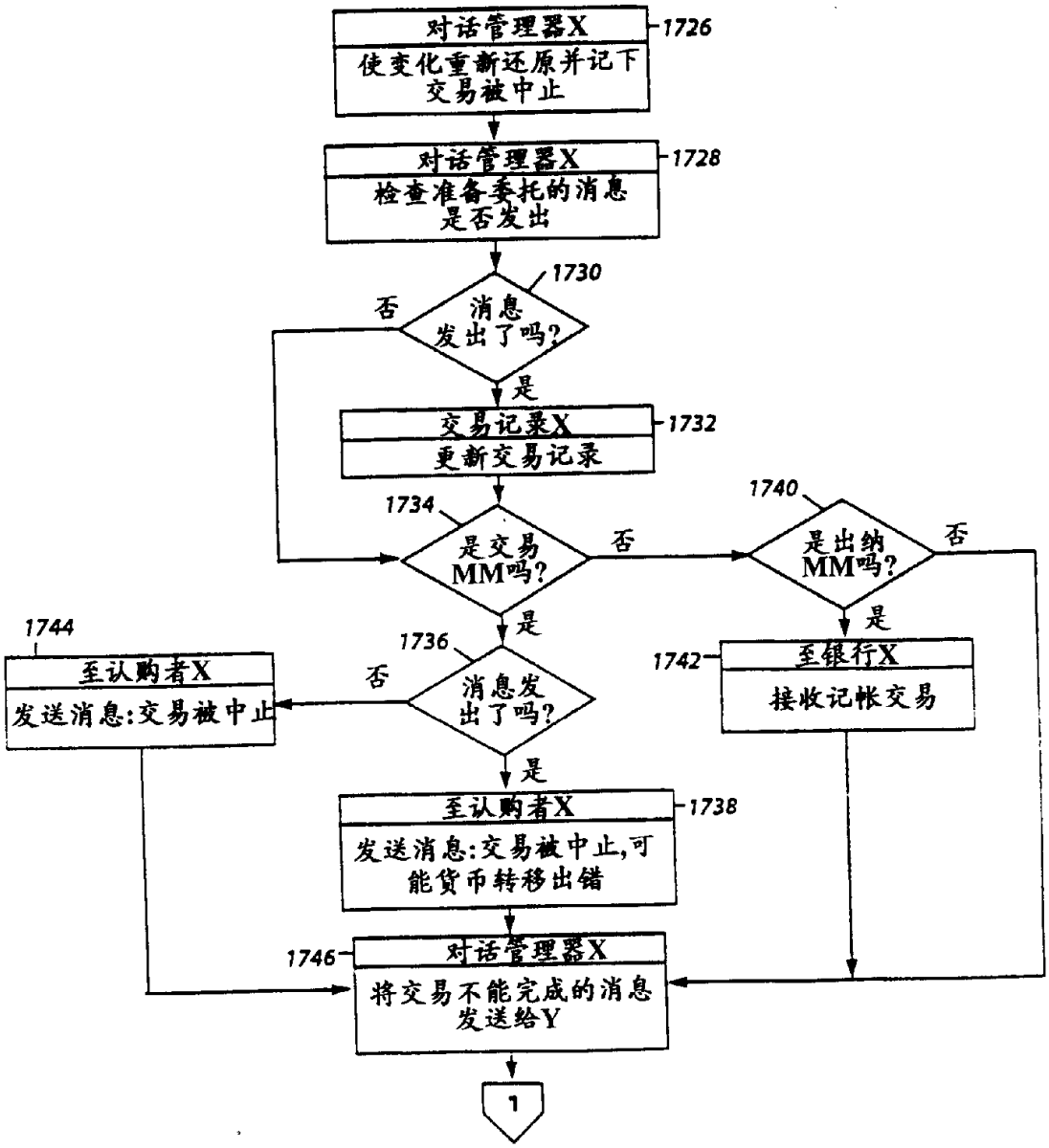

对话管理器X
使变化重新还原并记下交易被中止
1726
对话管理器X
检查准备委托的消息是否发出
1728
1730
消息发出了吗?
否
是
交易记录X
更新交易记录
1732
1734
是交易MM吗?
否
1740
是出纳MM吗?
否
是
是
1744
至认购者X
发送消息:交易被中止
1736
消息发出了吗?
否
1742
至银行X
接收记帐交易
是
至认购者X
发送消息:交易被中止,可能货币转移出错
1738
1746
对话管理器X
将交易不能完成的消息发送给Y
1

图 11A

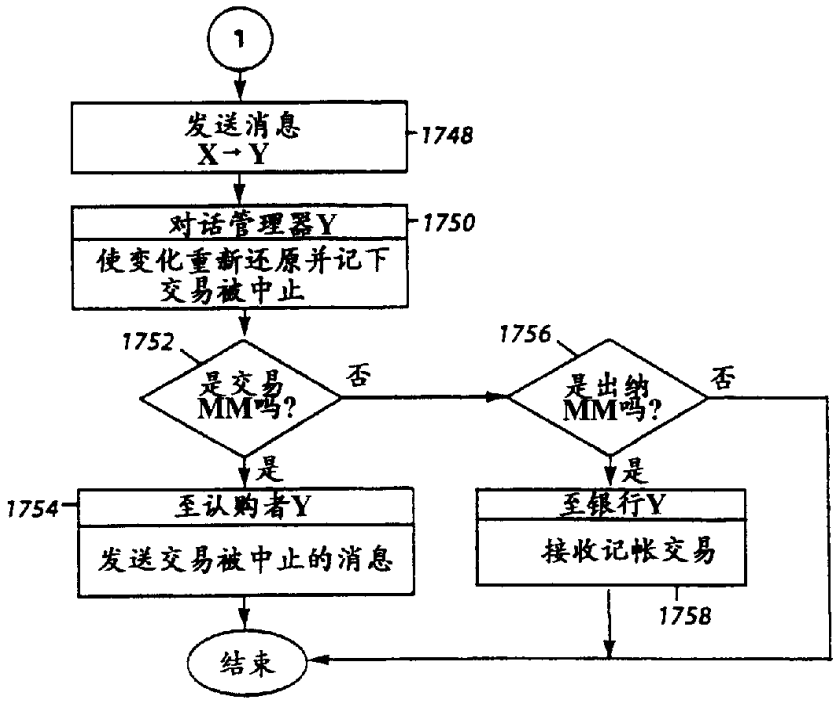

1
发送消息
X→Y
1748
对话管理器Y
使变化重新还原并记下
交易被中止
1750
1752
是交易
MM吗?
否
1756
是出纳
MM吗?
否
是
是
1754
至认购者Y
发送交易被中止的消息
至银行Y
接收记帐交易
1758
结束

图 11B

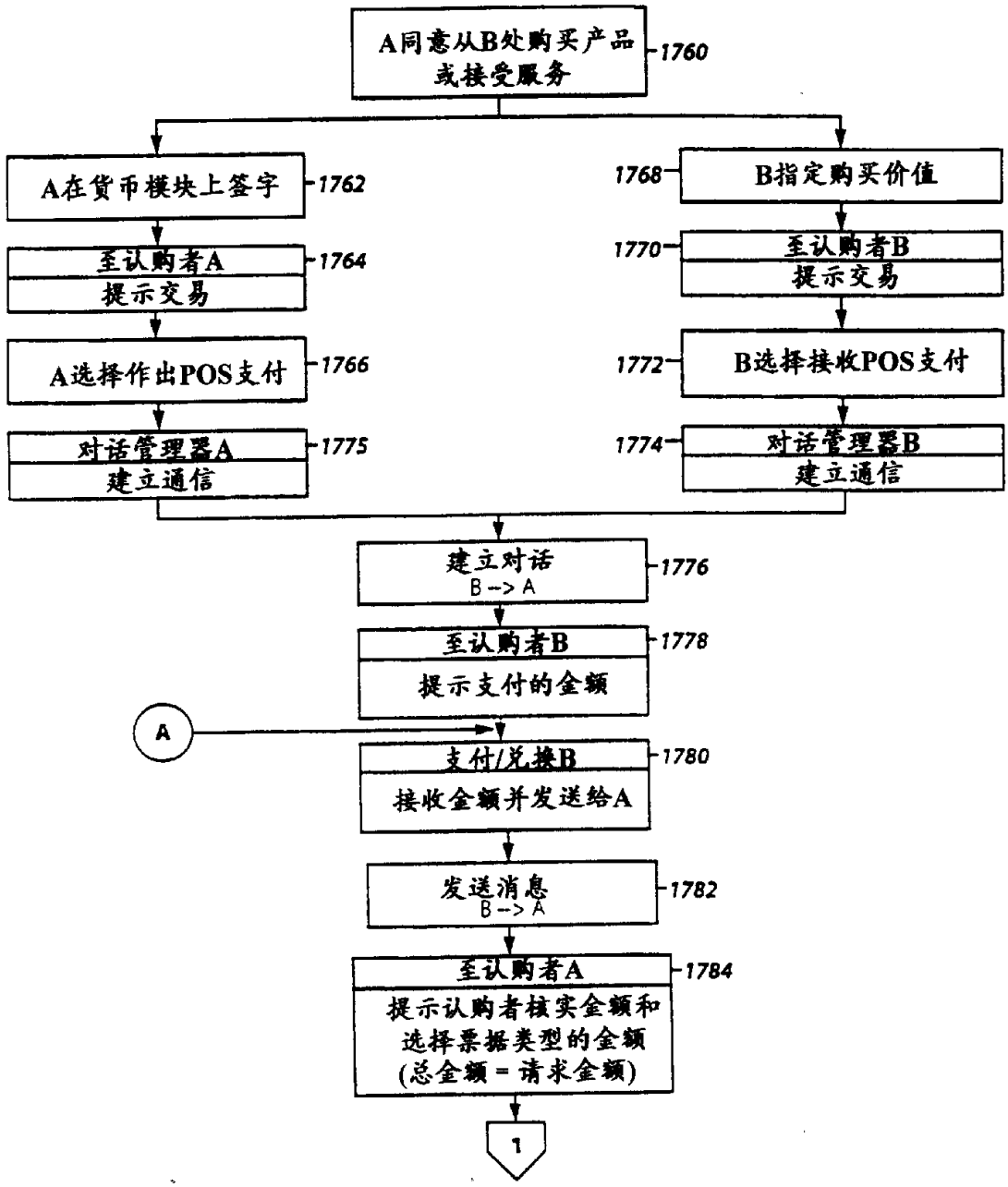

A同意从B处购买产品
或接受服务
1760
A在货币模块上签字
1762
至认购者A
提示交易
1764
A选择作出POS支付
1766
对话管理器A
建立通信
1775
1768
B指定购买价值
1770
至认购者B
提示交易
1772
B选择接收POS支付
1774
对话管理器B
建立通信
建立对话
B -> A
1776
至认购者B
提示支付的金额
1778
A
支付/兑换B
接收金额并发送给A
1780
发送消息
B -> A
1782
至认购者A
提示认购者核实金额和
选择票据类型的金额
(总金额 = 请求金额)
1784
1

图 12A

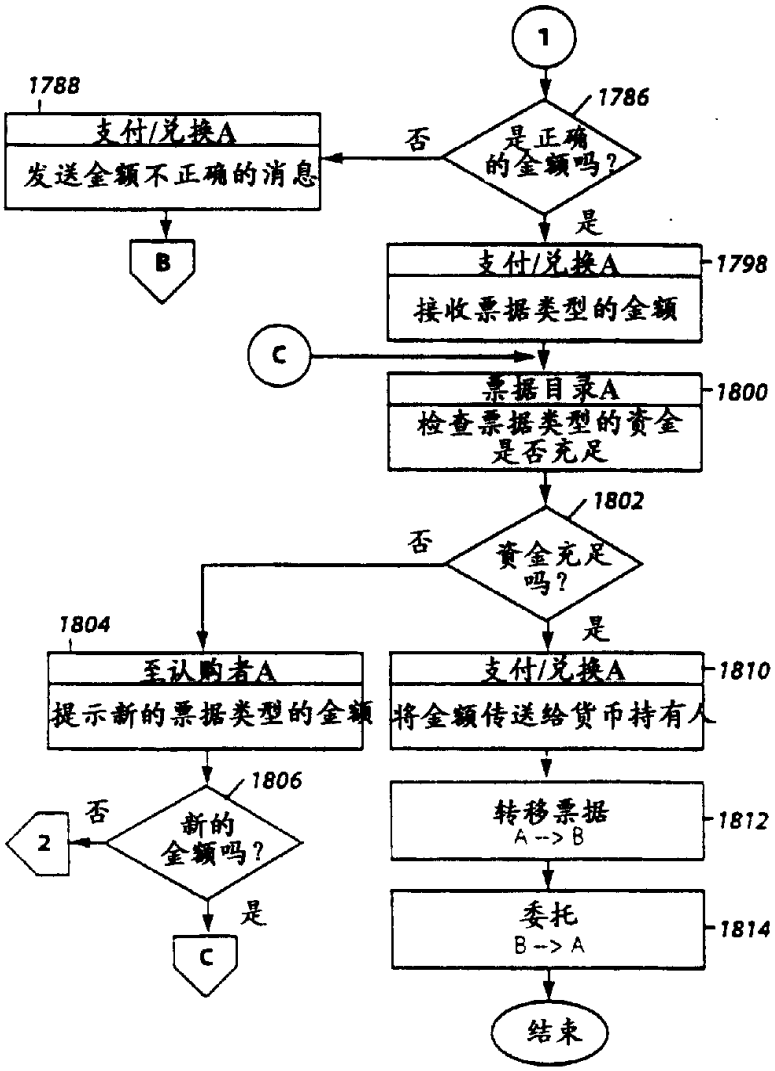

1
1786
是正确的金额吗?
否
1788
支付/兑换A
发送金额不正确的消息
B
是
支付/兑换A
接收票据类型的金额
1798
C
票据目录A
检查票据类型的资金是否充足
1800
1802
资金充足吗?
否
是
1804
至认购者A
提示新的票据类型的金额
支付/兑换A
将金额传送给货币持有人
1810
1806
新的金额吗?
否
2
是
C
转移票据
A --> B
1812
委托
B --> A
1814
结束

图 12B

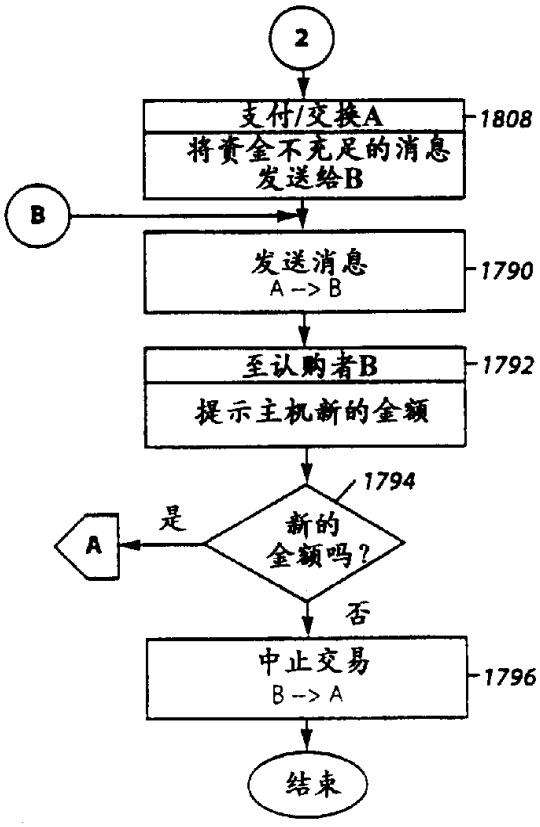

2
支付/交换A
将资金不充足的消息
发送给B
1808
B
发送消息
A -> B
1790
至认购者B
提示主机新的金额
1792
1794
新的
金额吗？
是
A
否
中止交易
B -> A
1796
结束

图 12C

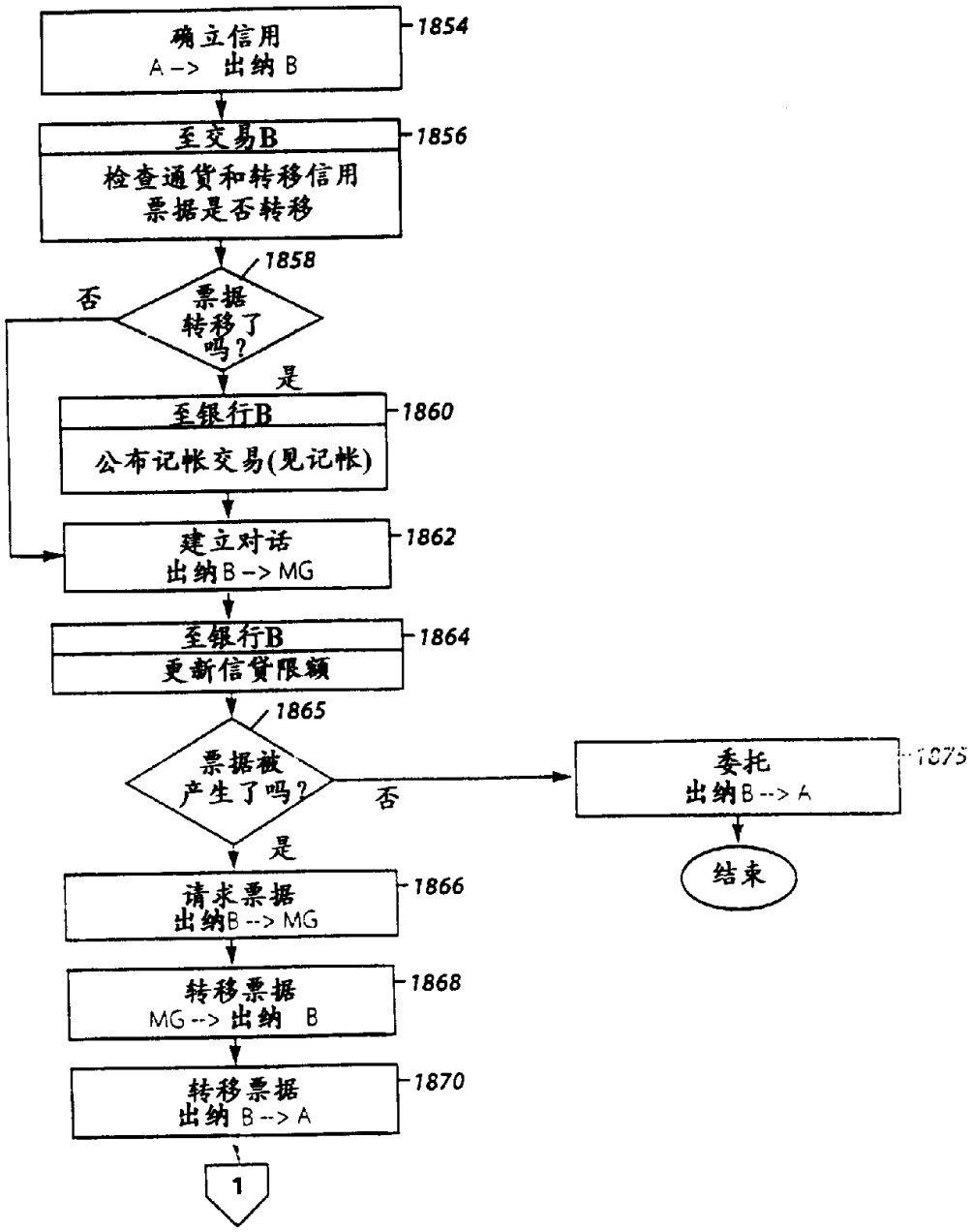

确立信用
A -> 出纳 B
1854
至交易B
检查通货和转移信用
票据是否转移
1856
1858
票据
转移了
吗?
否
是
至银行B
公布记帐交易(见记帐)
1860
建立对话
出纳B -> MG
1862
至银行B
更新信贷限额
1864
1865
票据被
产生了吗?
否
是
委托
出纳B --> A
1875
结束
请求票据
出纳B --> MG
1866
转移票据
MG --> 出纳 B
1868
转移票据
出纳 B --> A
1870
1

图 13A

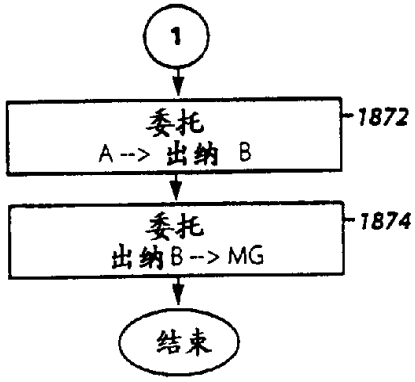


图 13B

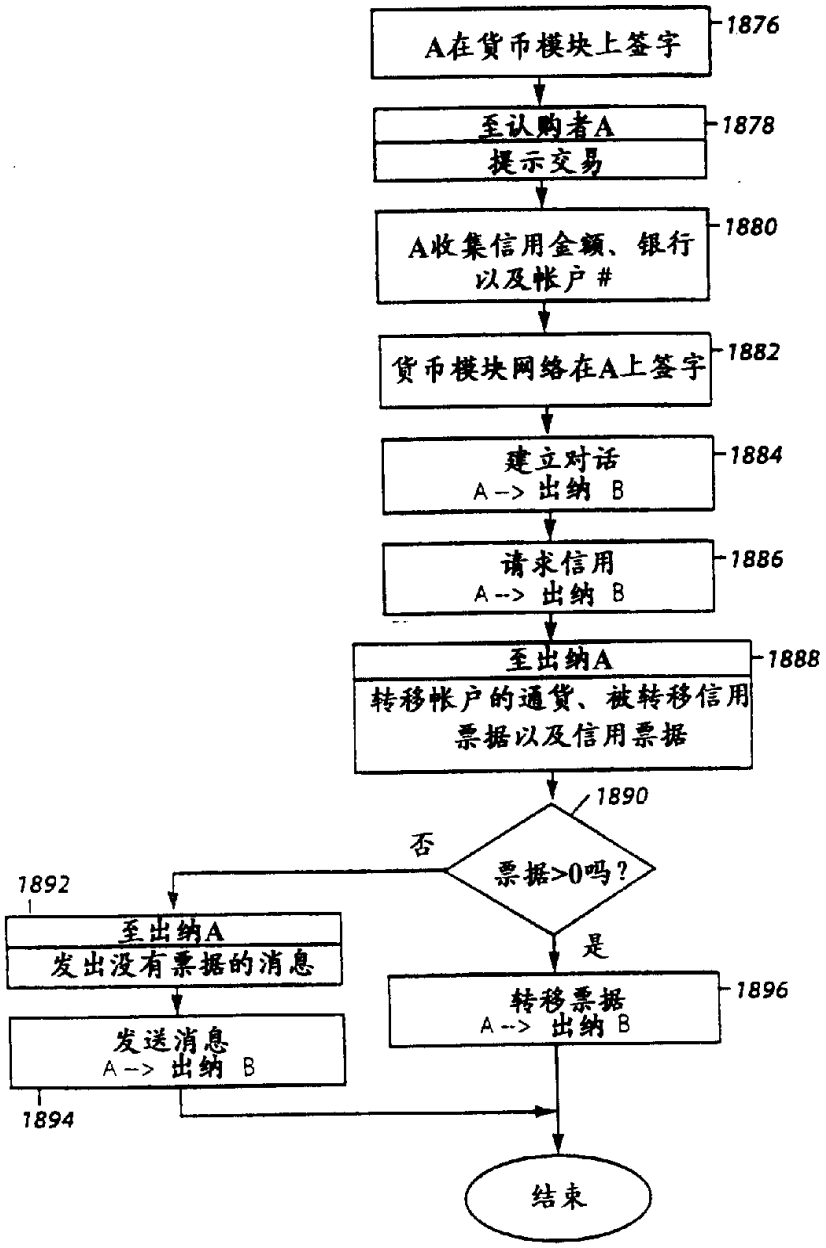

A在货币模块上签字
1876
至认购者A
提示交易
1878
A收集信用金额、银行以及帐户 #
1880
货币模块网络在A上签字
1882
建立对话
A -> 出纳 B
1884
请求信用
A --> 出纳 B
1886
至出纳A
转移帐户的通货、被转移信用票据以及信用票据
1888
1890
票据>0吗?
否
是
1892
至出纳A
发出没有票据的消息
发送消息
A -> 出纳 B
1894
转移票据
A --> 出纳 B
1896
结束

图 14

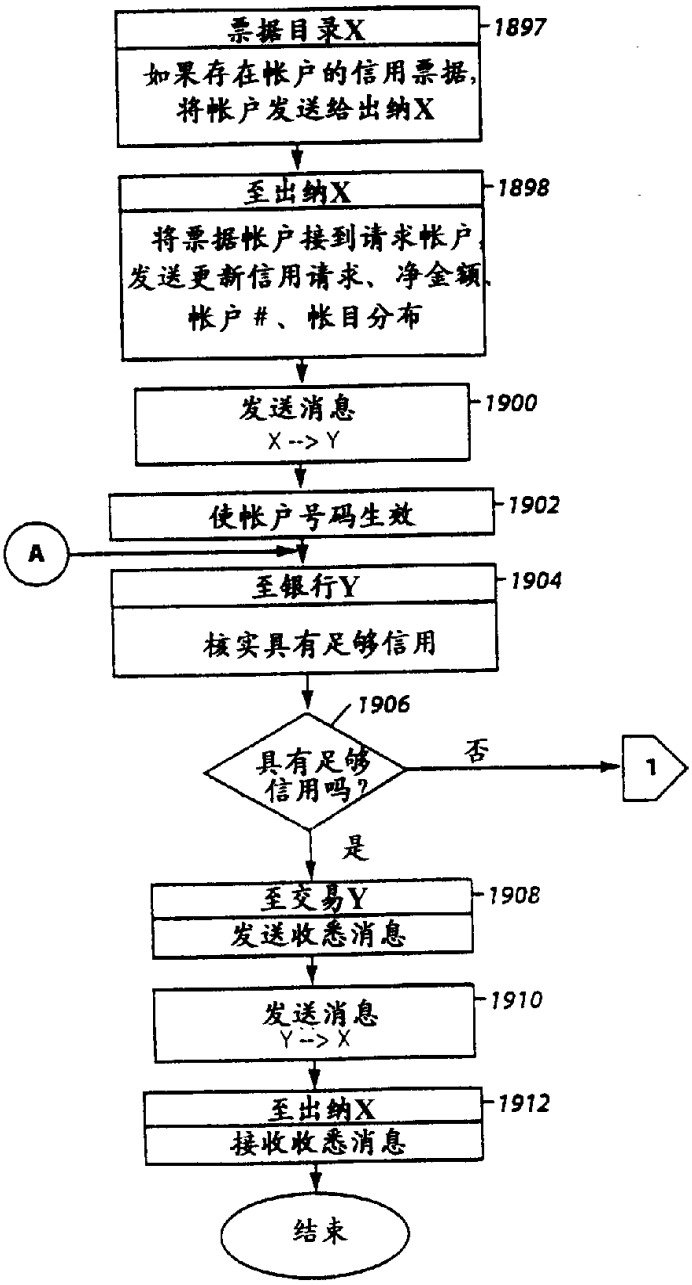

票据目录X
1897
如果存在帐户的信用票据，
将帐户发送给出纳X
至出纳X
1898
将票据帐户接到请求帐户，
发送更新信用请求、净金额、
帐户#、帐目分布
发送消息
X --> Y
1900
使帐户号码生效
1902
A
至银行Y
1904
核实具有足够信用
1906
具有足够
信用吗？
否
1
是
至交易Y
1908
发送收悉消息
发送消息
Y --> X
1910
至出纳X
1912
接收收悉消息
结束

图 15A

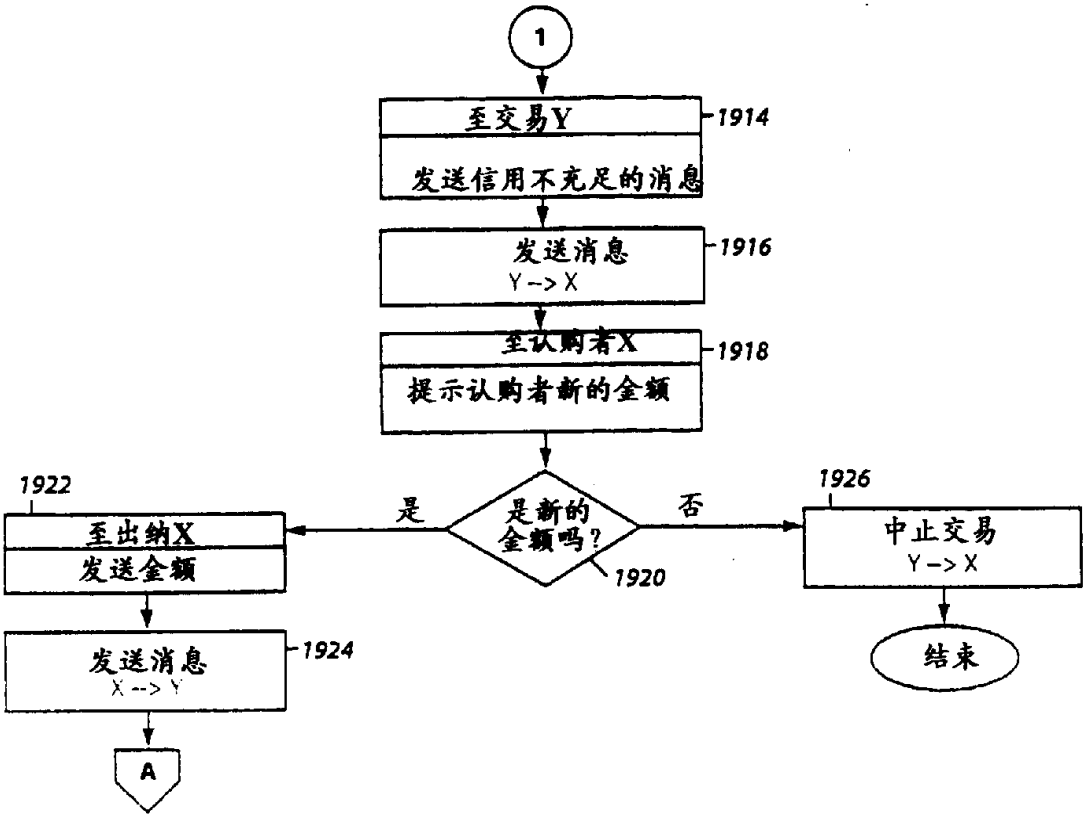

1
至交易Y
1914
发送信用不充足的消息
发送消息
Y -> X
1916
至认购者X
1918
提示认购者新的金额
是新的金额吗?
1920
是
否
1922
至出纳X
发送金额
1924
发送消息
X -> Y
A
1926
中止交易
Y -> X
结束

图 15B

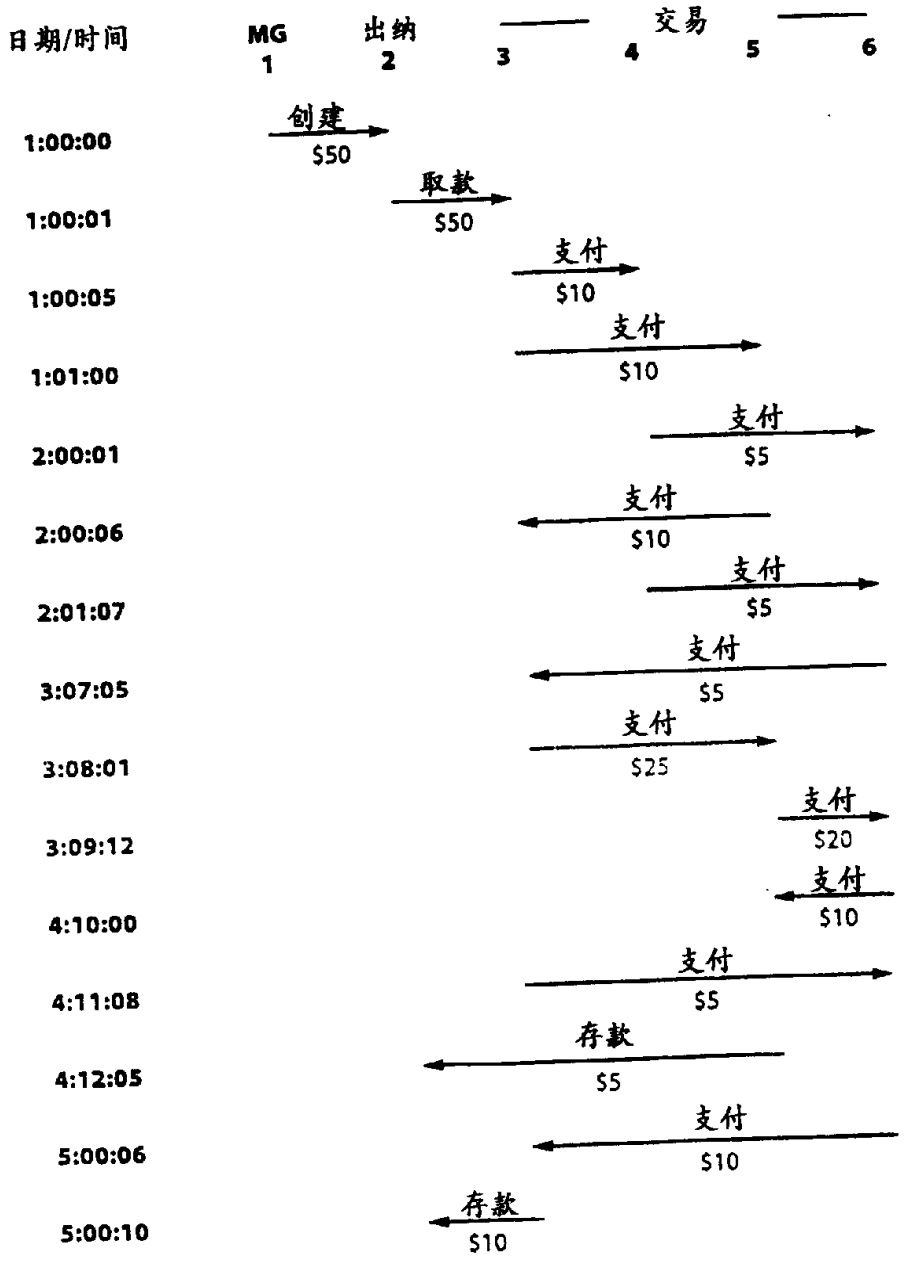
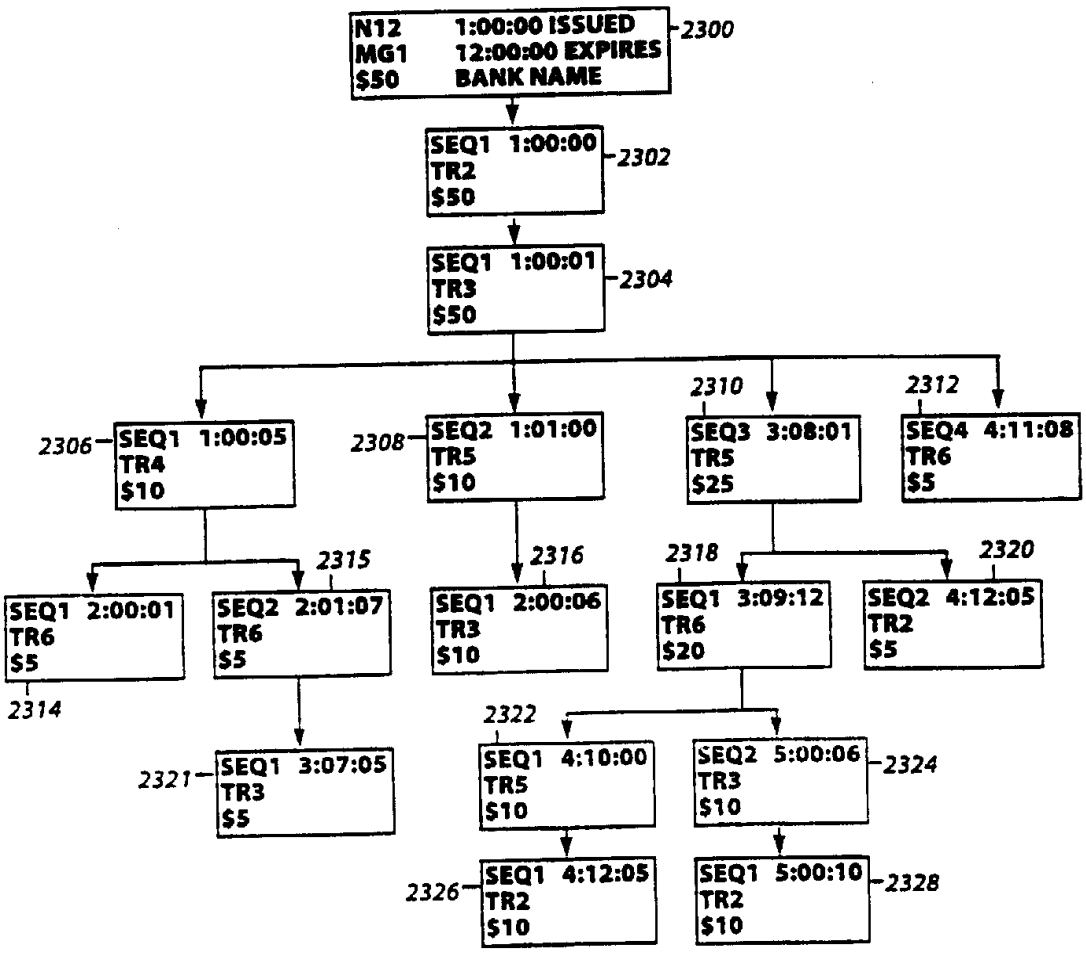

日期/时间
MG
1
出纳
2
3
交易
4
5
6
1:00:00
创建
$50
1:00:01
取款
$50
1:00:05
支付
$10
1:01:00
支付
$10
2:00:01
支付
$5
2:00:06
支付
$10
2:01:07
支付
$5
3:07:05
支付
$5
3:08:01
支付
$25
3:09:12
支付
$20
4:10:00
支付
$10
4:11:08
支付
$5
4:12:05
存款
$5
5:00:06
支付
$10
5:00:10
存款
$10

图 16



SEQ = 流水号
TR = 受移者
D:TT:TT = 日期:时间

图 17

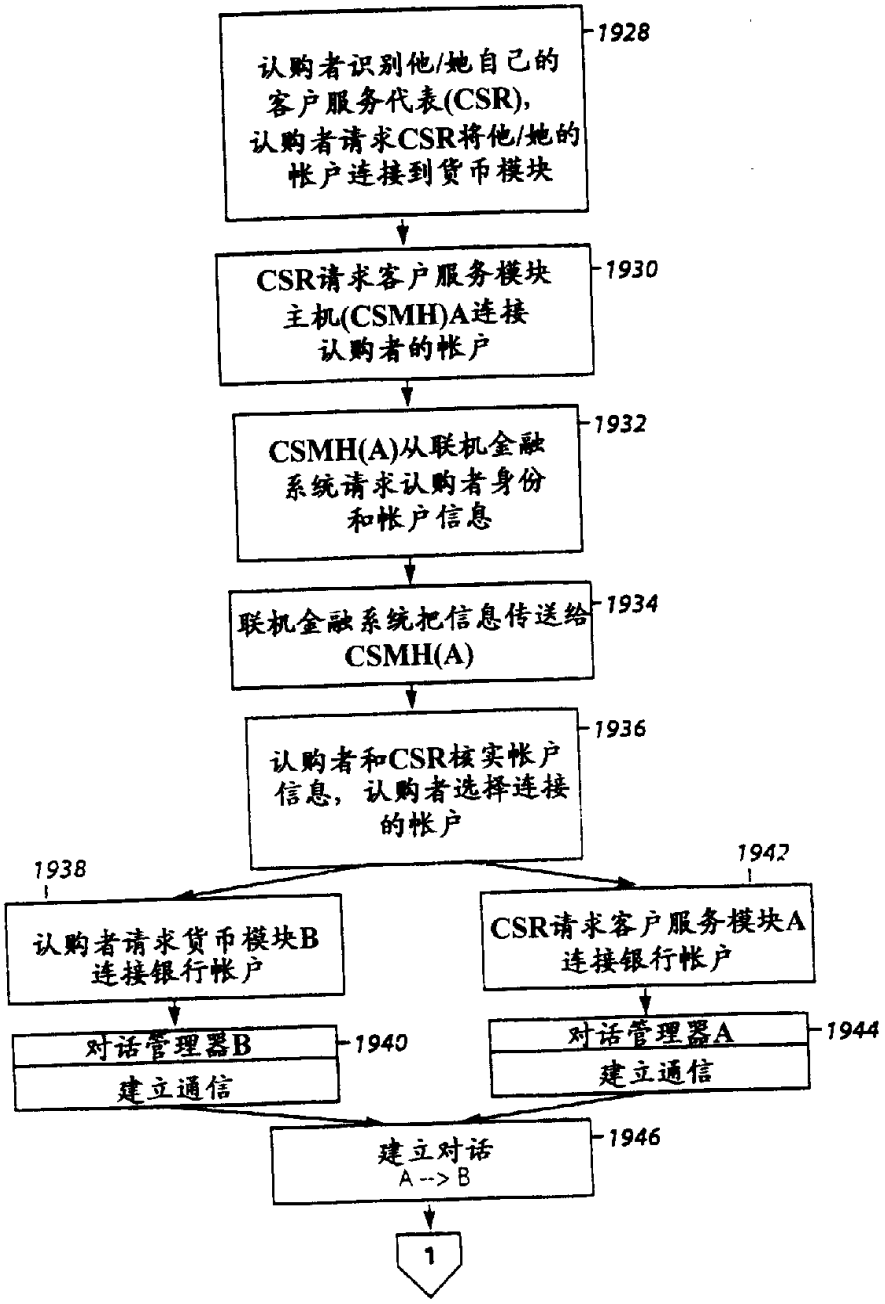

认购者识别他/她自己的客户服务代表(CSR),认购者请求CSR将他/她的帐户连接到货币模块
1928
CSR请求客户服务模块主机(CSMH)A连接认购者的帐户
1930
CSMH(A)从联机金融系统请求认购者身份和帐户信息
1932
联机金融系统把信息传送给CSMH(A)
1934
认购者和CSR核实帐户信息，认购者选择连接的帐户
1936
1938
认购者请求货币模块B连接银行帐户
1942
CSR请求客户服务模块A连接银行帐户
对话管理器B
建立通信
1940
对话管理器A
建立通信
1944
建立对话
A --> B
1946
1

图 18A

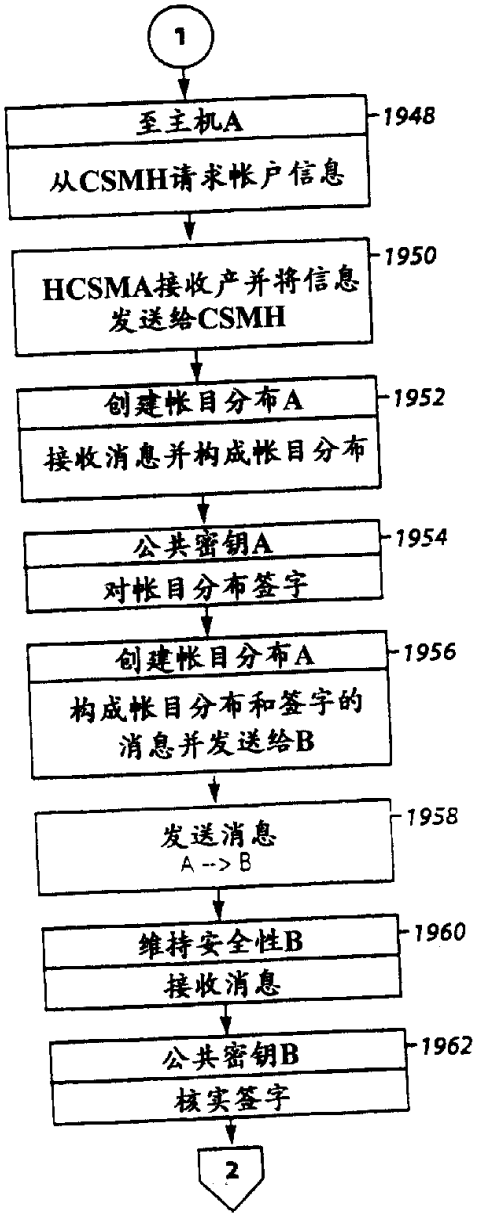

1
至主机A
从CSMH请求帐户信息
1948
HCSMA接收产并将信息发送给CSMH
1950
创建帐目分布A
接收消息并构成帐目分布
1952
公共密钥A
对帐目分布签字
1954
创建帐目分布A
构成帐目分布和签字的消息并发送给B
1956
发送消息
A --> B
1958
维持安全性B
接收消息
1960
公共密钥B
核实签字
1962
2

图 18B

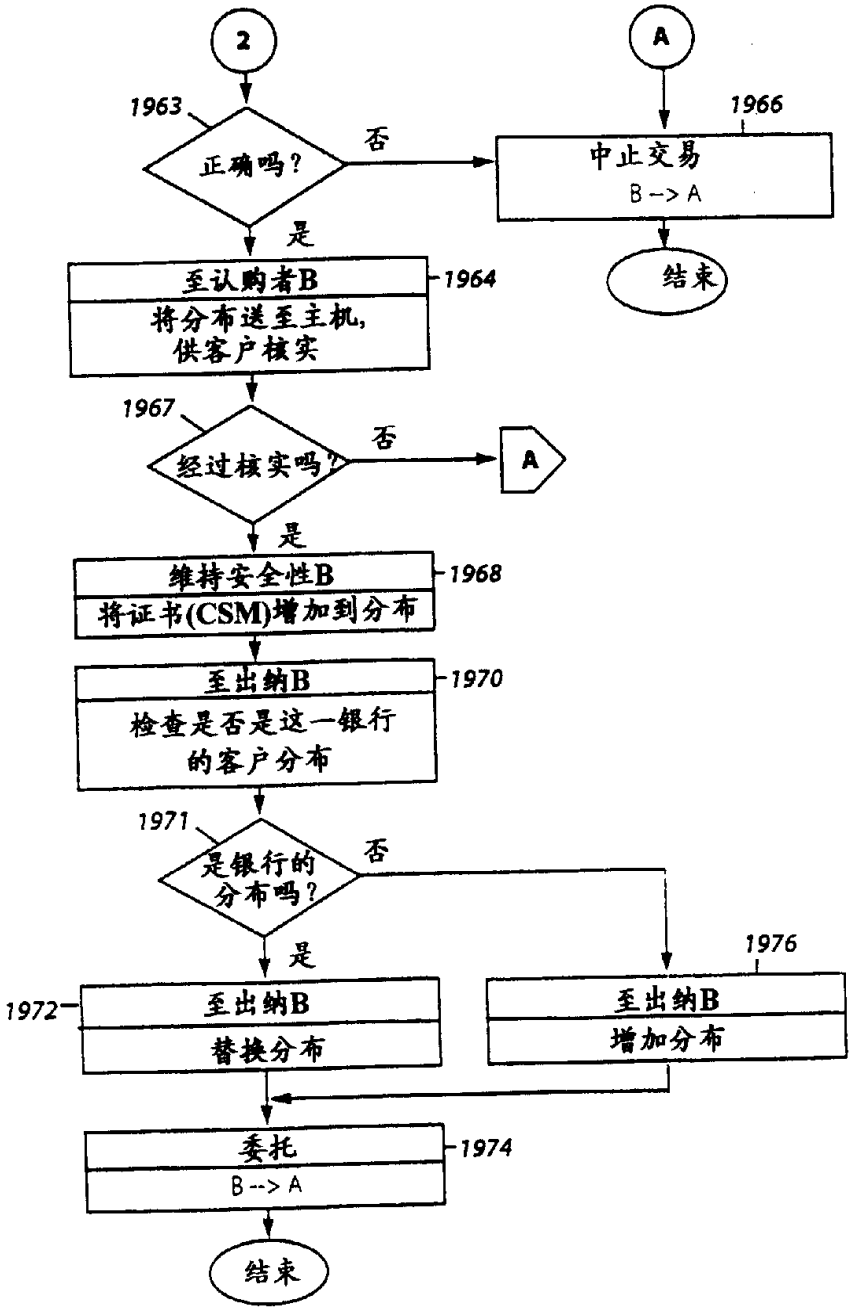

2
A
1963
正确吗?
否
1966
中止交易
B --> A
结束
是
至认购者B
将分布送至主机,
供客户核实
1964
1967
经过核实吗?
否
A
是
维持安全性B
将证书(CSM)增加到分布
1968
至出纳B
检查是否是这一银行
的客户分布
1970
1971
是银行的
分布吗?
否
是
1976
1972
至出纳B
替换分布
至出纳B
增加分布
委托
B --> A
1974
结束

图 18C

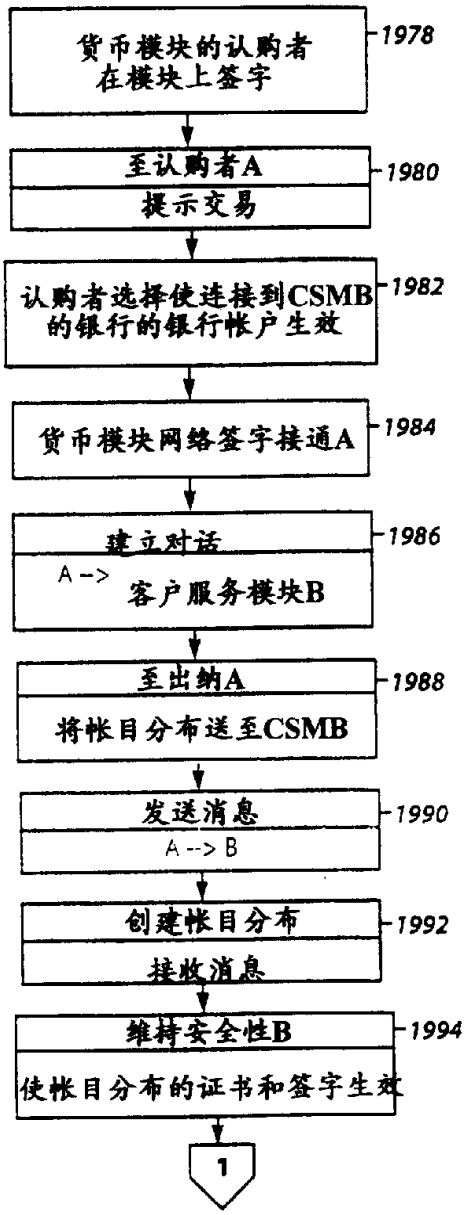

货币模块的认购者
在模块上签字
1978
至认购者A
提示交易
1980
认购者选择使连接到CSMB
的银行的银行帐户生效
1982
货币模块网络签字接通A
1984
建立对话
A ->
客户服务模块B
1986
至出纳A
将帐目分布送至CSMB
1988
发送消息
A --> B
1990
创建帐目分布
接收消息
1992
维持安全性B
使帐目分布的证书和签字生效
1994
1

图 19A

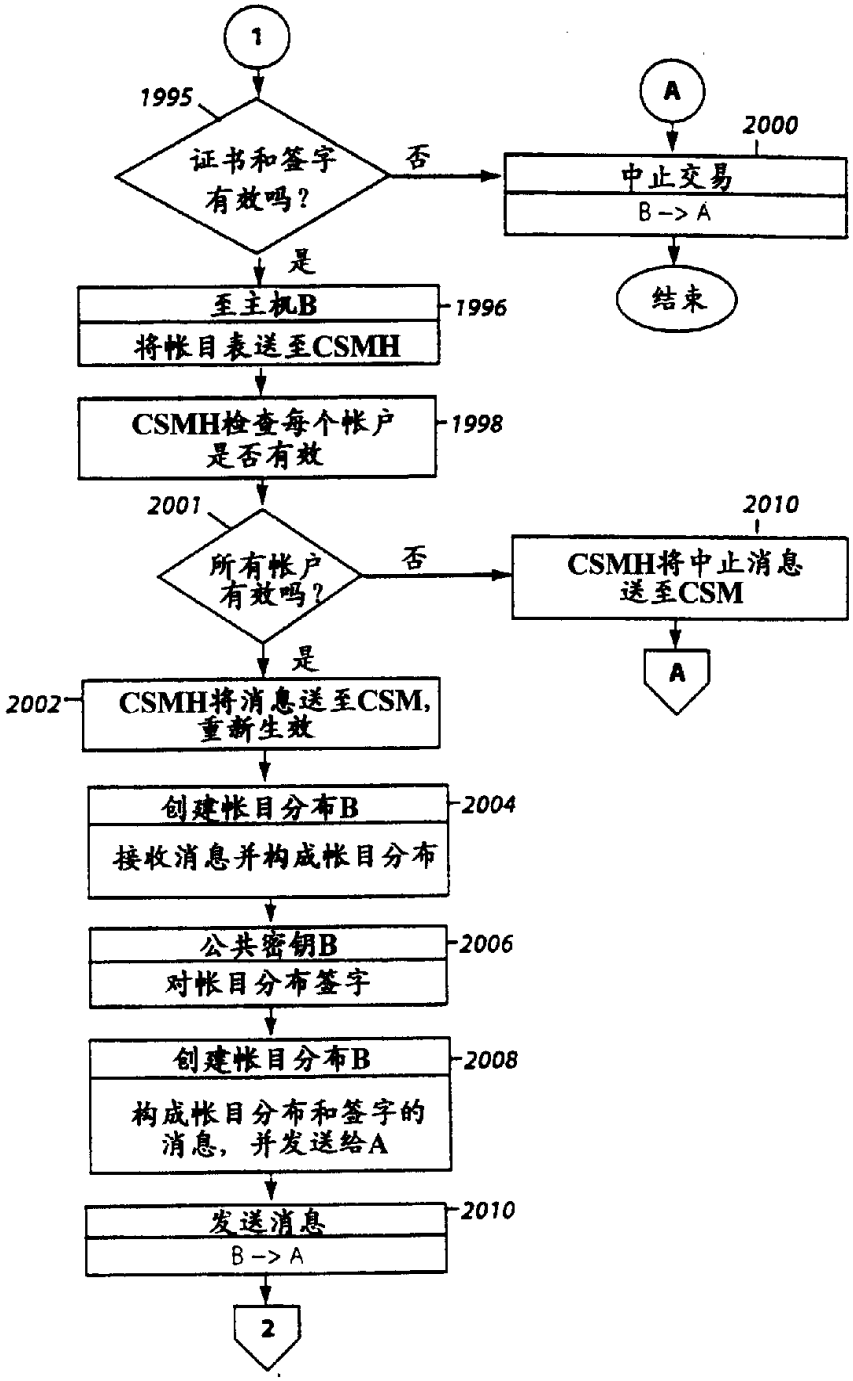

1
1995
证书和签字有效吗?
否
A
2000
中止交易
B -> A
结束
是
至主机B
将帐目表送至CSMH
1996
CSMH检查每个帐户是否有效
1998
2001
所有帐户有效吗?
否
2010
CSMH将中止消息送至CSM
A
是
2002
CSMH将消息送至CSM,重新生效
创建帐目分布B
接收消息并构成帐目分布
2004
公共密钥B
对帐目分布签字
2006
创建帐目分布B
构成帐目分布和签字的消息，并发送给A
2008
发送消息
B -> A
2010
2

图 19B

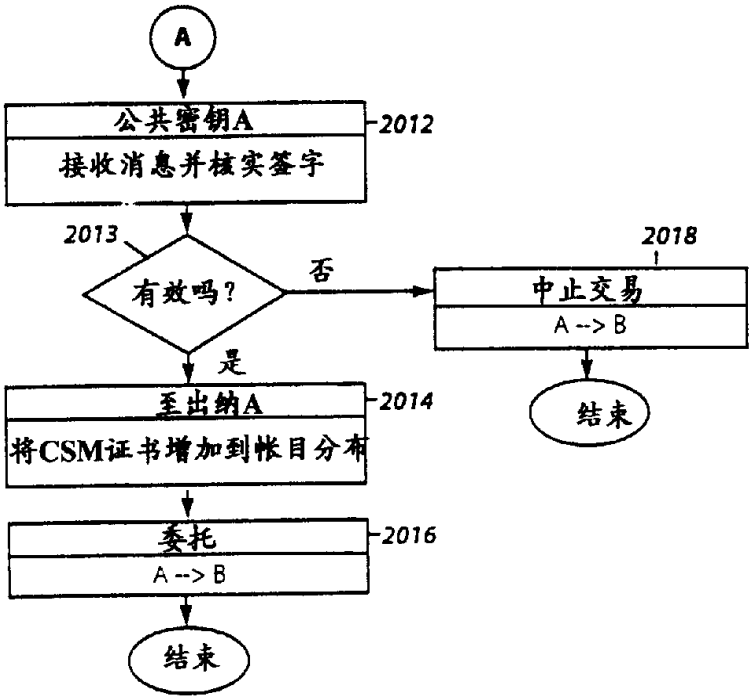

A
公共密钥A
接收消息并核实签字
2012
2013
有效吗?
否
是
2018
中止交易
A --> B
结束
至出纳A
将CSM证书增加到帐目分布
2014
委托
A --> B
2016
结束

图 19C

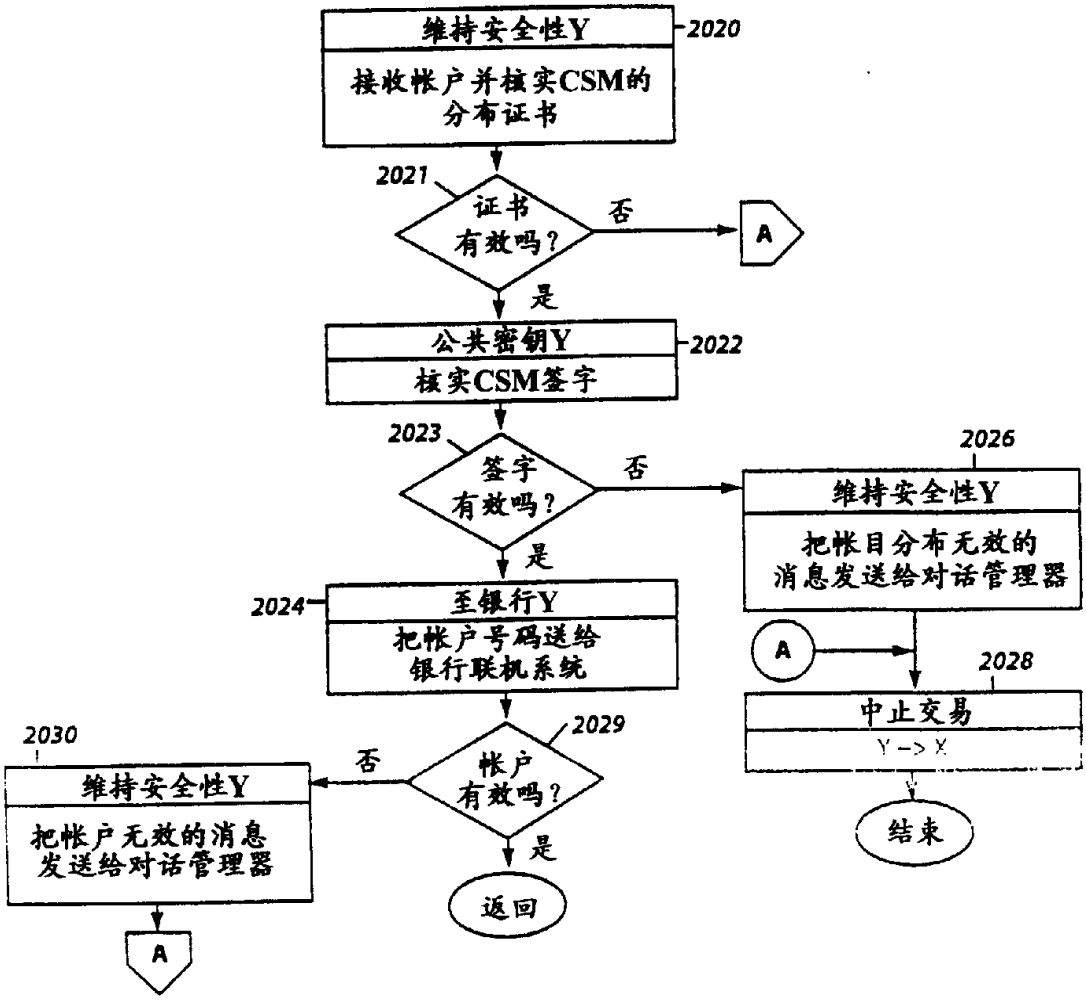

维持安全性Y
2020
接收帐户并核实CSM的分布证书
2021
证书有效吗?
否
A
是
公共密钥Y
2022
核实CSM签字
2023
签字有效吗?
否
2026
维持安全性Y
把帐目分布无效的消息发送给对话管理器
是
2024
至银行Y
把帐户号码送给银行联机系统
A
2028
中止交易
Y -> X
结束
2030
维持安全性Y
把帐户无效的消息发送给对话管理器
否
2029
帐户有效吗?
是
返回
A

图 20

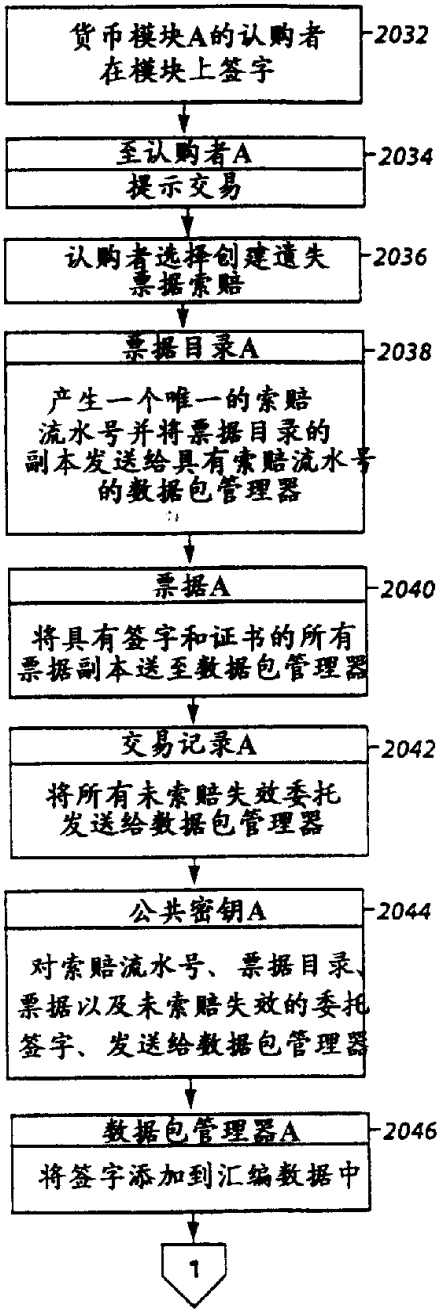

货币模块A的认购者
在模块上签字
2032
至认购者A
提示交易
2034
认购者选择创建遗失
票据索赔
2036
票据目录A
2038
产生一个唯一的索赔
流水号并将票据目录的
副本发送给具有索赔流水号
的数据包管理器
票据A
2040
将具有签字和证书的所有
票据副本送至数据包管理器
交易记录A
2042
将所有未索赔失效委托
发送给数据包管理器
公共密钥A
2044
对索赔流水号、票据目录、
票据以及未索赔失效的委托
签字、发送给数据包管理器
数据包管理器A
2046
将签字添加到汇编数据中
1

图 21A

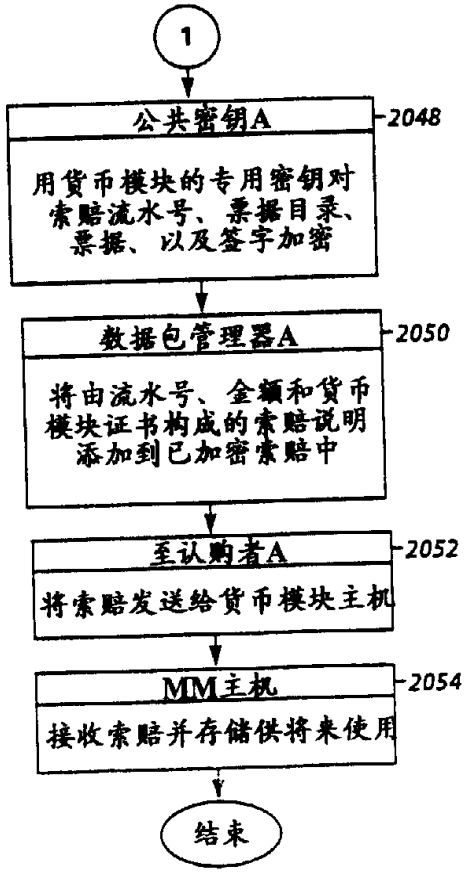

1
公共密钥A
2048
用货币模块的专用密钥对索赔流水号、票据目录、票据、以及签字加密
数据包管理器A
2050
将由流水号、金额和货币模块证书构成的索赔说明添加到已加密索赔中
至认购者A
2052
将索赔发送给货币模块主机
MM主机
2054
接收索赔并存储供将来使用
结束

图 21B

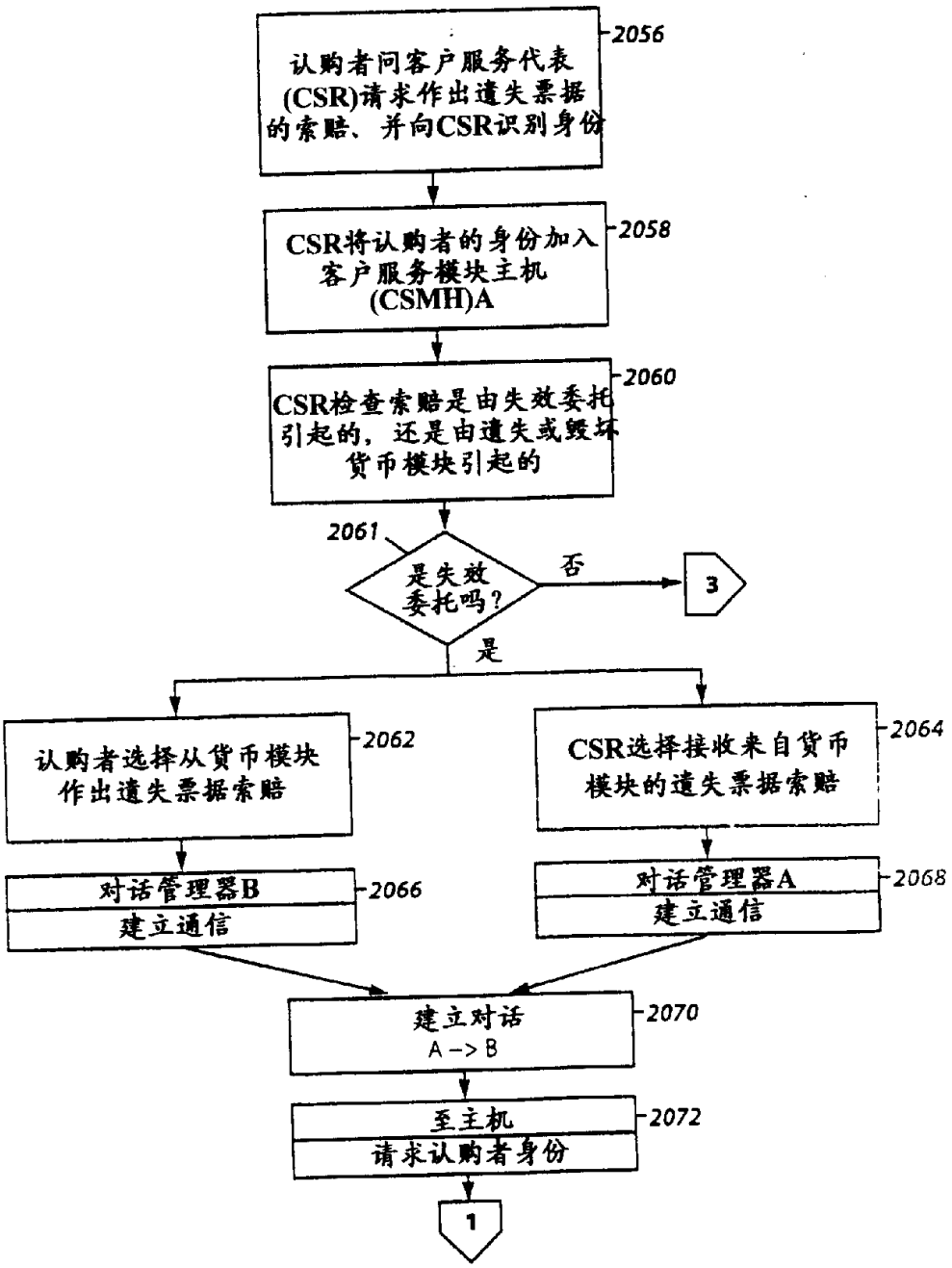

认购者问客户服务代表(CSR)请求作出遗失票据的索赔、并向CSR识别身份
2056
CSR将认购者的身份加入客户服务模块主机(CSMH)A
2058
CSR检查索赔是由失效委托引起的，还是由遗失或毁坏货币模块引起的
2060
2061
是失效委托吗？
否
3
是
认购者选择从货币模块作出遗失票据索赔
2062
CSR选择接收来自货币模块的遗失票据索赔
2064
对话管理器B
建立通信
2066
对话管理器A
建立通信
2068
建立对话
A -> B
2070
至主机
请求认购者身份
2072
1

图 22A

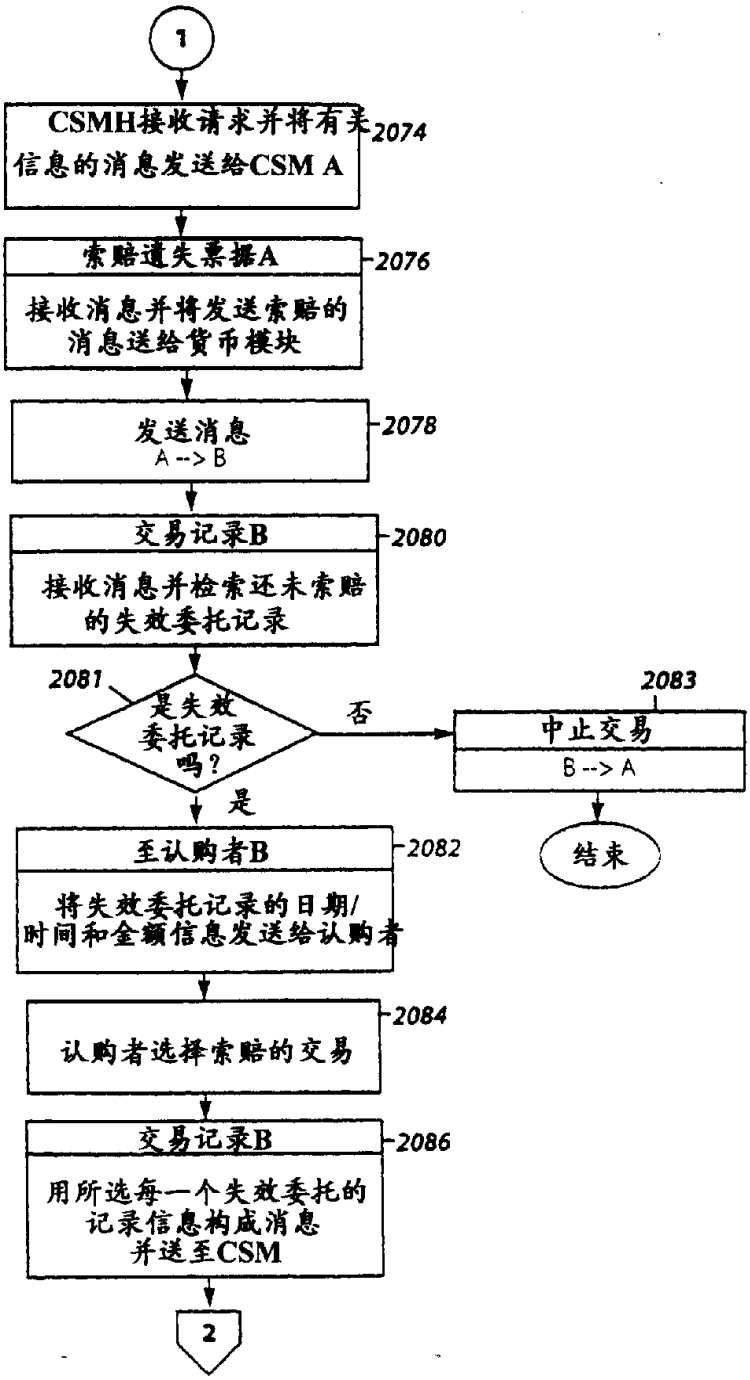

1
CSMH接收请求并将有关信息的消息发送给CSM A
2074
索赔遗失票据A
2076
接收消息并将发送索赔的消息送给货币模块
发送消息
A --> B
2078
交易记录B
2080
接收消息并检索还未索赔的失效委托记录
2081
是失效委托记录吗?
否
2083
中止交易
B --> A
结束
是
至认购者B
2082
将失效委托记录的日期/时间和金额信息发送给认购者
认购者选择索赔的交易
2084
交易记录B
2086
用所选每一个失效委托的记录信息构成消息并送至CSM
2

图 22B

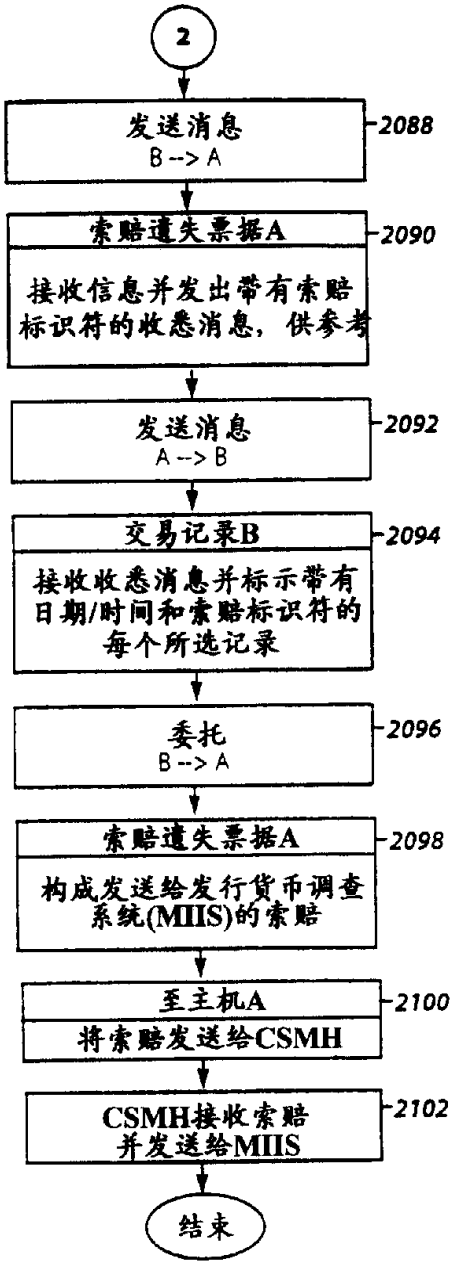

2
发送消息
B --> A
2088
索赔遗失票据A
2090
接收信息并发出带有索赔标识符的收悉消息，供参考
发送消息
A --> B
2092
交易记录B
2094
接收收悉消息并标示带有日期/时间和索赔标识符的每个所选记录
委托
B --> A
2096
索赔遗失票据A
2098
构成发送给发行货币调查系统(MIIS)的索赔
至主机A
2100
将索赔发送给CSMH
CSMH接收索赔并发送给MIIS
2102
结束

图 22C

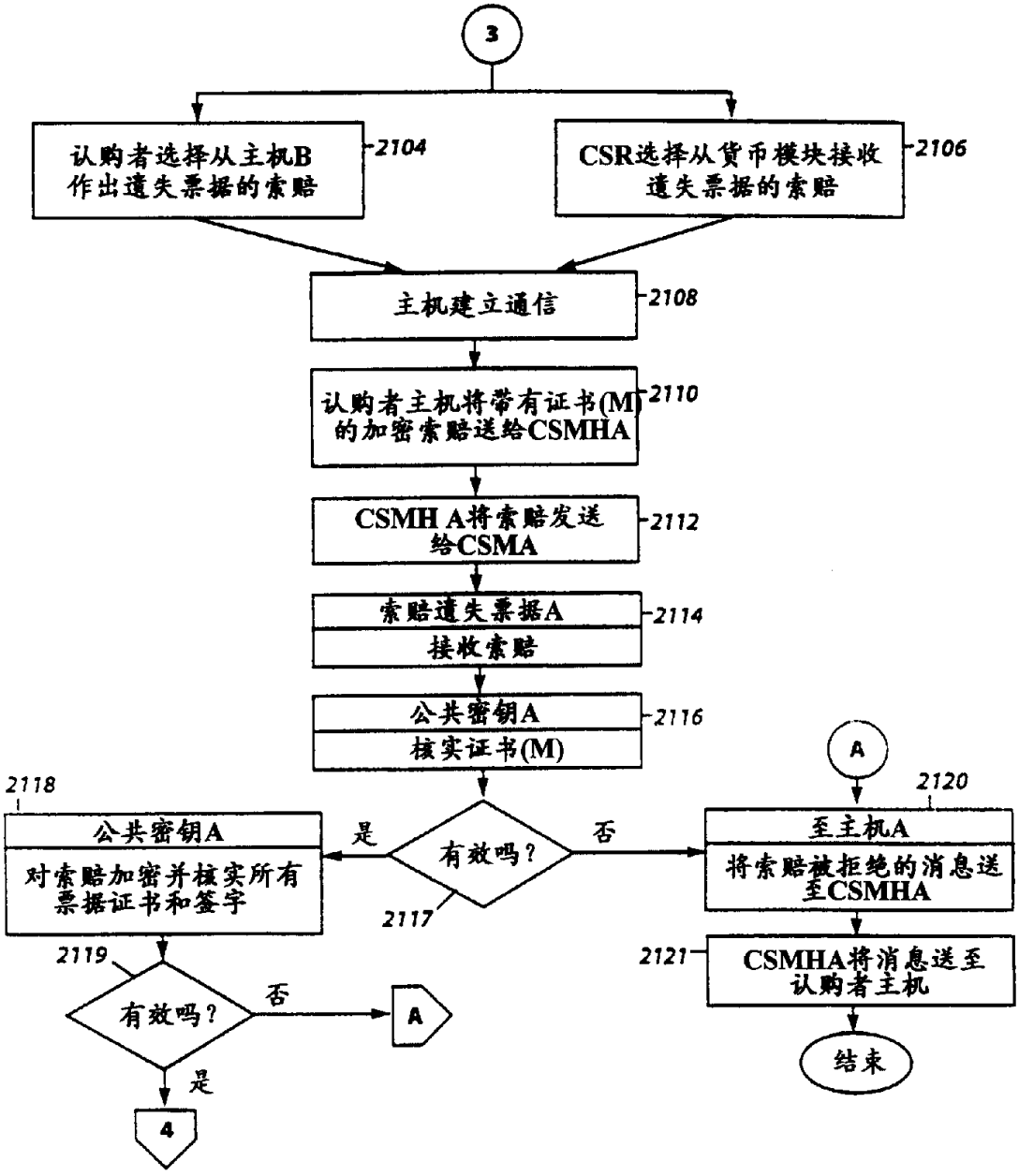

3
认购者选择从主机B
作出遗失票据的索赔
2104
CSR选择从货币模块接收
遗失票据的索赔
2106
主机建立通信
2108
认购者主机将带有证书(M)
的加密索赔送给CSMHA
2110
CSMH A将索赔发送
给CSMA
2112
索赔遗失票据A
接收索赔
2114
公共密钥A
核实证书(M)
2116
2118
公共密钥A
对索赔加密并核实所有
票据证书和签字
是
有效吗?
否
2117
A
2120
至主机A
将索赔被拒绝的消息送
至CSMHA
2121
CSMHA将消息送至
认购者主机
结束
2119
有效吗?
否
A
是
4

图 22D

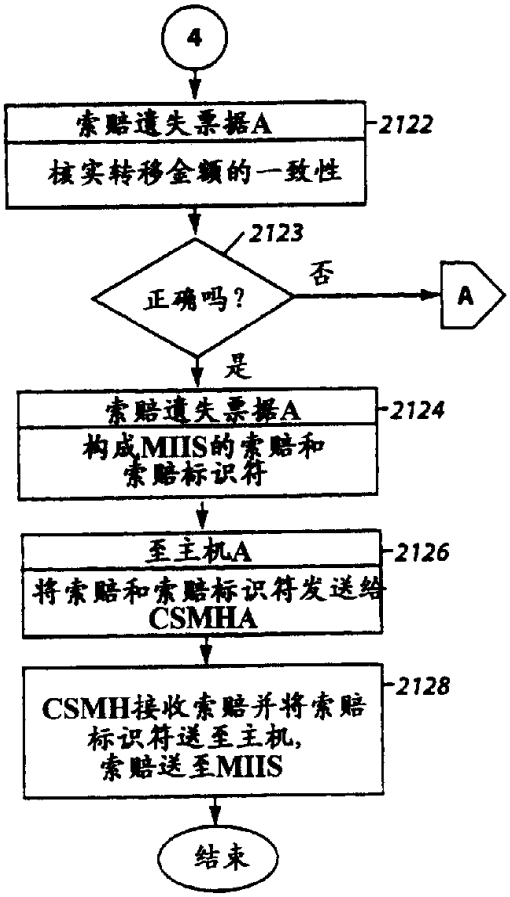

4
索赔遗失票据A
核实转移金额的一致性
2122
2123
正确吗?
否
A
是
索赔遗失票据A
构成MIIS的索赔和
索赔标识符
2124
至主机A
将索赔和索赔标识符发送给
CSMHA
2126
CSMH接收索赔并将索赔
标识符送至主机,
索赔送至MIIS
2128
结束

图 22E