



(12) 发明专利

(10) 授权公告号 CN 112334933 B

(45) 授权公告日 2024. 03. 01

(21) 申请号 201980041477.5

(22) 申请日 2019.04.18

(65) 同一申请的已公布的文献号
申请公布号 CN 112334933 A

(43) 申请公布日 2021.02.05

(30) 优先权数据
62/659,917 2018.04.19 US
62/664,981 2018.05.01 US

(85) PCT国际申请进入国家阶段日
2020.12.18

(86) PCT国际申请的申请数据
PCT/SG2019/050223 2019.04.18

(87) PCT国际申请的公布数据
W02019/203736 EN 2019.10.24

(73) 专利权人 唯链基金会有限公司
地址 新加坡新加坡城

(72) 发明人 顾建良 钱斌 周子衡

(74) 专利代理机构 北京安信方达知识产权代理有限公司 11262

专利代理师 李琰 凌齐文

(51) Int.Cl.
G06Q 20/22 (2006.01)
G06Q 30/06 (2006.01)

(56) 对比文件
US 10055715 B1, 2018.08.21
US 2010223184 A1, 2010.09.02
US 2014370846 A1, 2014.12.18
US 2018075527 A1, 2018.03.15
CN 106845960 A, 2017.06.13
CN 107424073 A, 2017.12.01
CN 107851245 A, 2018.03.27
RU 2015157156 A, 2017.07.06
US 10299128 B1, 2019.05.21
US 2016203477 A1, 2016.07.14
US 2016371680 A1, 2016.12.22
US 2017154331 A1, 2017.06.01

(续)

审查员 李菲

权利要求书4页 说明书14页 附图7页

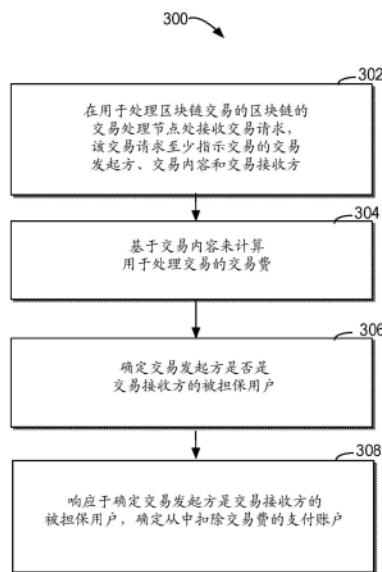
(54) 发明名称

区块链交易处理

(57) 摘要

本公开的实施例涉及用于处理或管理区块链交易的方法、设备、计算机可读存储介质和计算机程序产品。在用于处理区块链交易的方法中,用于处理区块链交易的区块链的区块链节点接收交易请求,该交易请求至少指示交易的发起方、交易内容和交易的交易接收方。区块链节点基于交易内容来计算用于处理交易的交易费。区块链节点确定交易的发起方是否是交易接收方的被担保用户,并且响应于确定交易的发起方是交易接收方的被担保用户而确定从中扣除交易费的支付账户。如在本公开中提供的交易处理和管理方案使普通用户能够方便地使用区块链服务。

CN 112334933 B



[接上页]

(56) 对比文件

US 2017230478 A1,2017.08.10

US 2017300978 A1,2017.10.19

US 2017323294 A1,2017.11.09

US 2017344987 A1,2017.11.30

WO 2017167437 A1,2017.10.05

周永林deng .区块链与金融市场基础设施.
区块链与金融市场基础设施.2016,全文.

Hoon, Lee Jung et al..A Study on the
Criminal Issues Related to Virtual
Currency.Korean Criminological

Review.2017,第28卷(第2期),全文.

Buterin et al..a next generation
smart contract and decentralized
application platform.Buterin.2014,全文.

袁勇等.区块链技术发展现状与展望.自动
化学报.2016,第42卷(第4期),全文.

祝烈煌;董慧;沈蒙.区块链交易数据隐私保
护机制.大数据.2018,(第01期),全文.

傅晓彤;陈思;张宁.基于代理的密码货币支
付系统.通信学报.2017,(第07期),全文.

1. 一种用于处理区块链交易的方法,包括:

在用于处理所述区块链交易的区块链的区块链节点处,接收交易请求,所述交易请求至少指示所述交易的交易发起方、交易内容和交易接收方;

基于所述交易内容来计算用于处理所述交易的交易费;

确定所述交易发起方是否是所述交易接收方的被担保用户;以及

响应于确定所述交易发起方是所述交易接收方的被担保用户:

确定是否存在与所述交易接收方相关联的担保账户:

响应于确定存在与所述交易接收方相关联的担保账户,确定所述担保账户的余额是否大于或等于所述交易费;以及响应于确定所述担保账户的余额大于或等于所述交易费,将所述担保账户确定为从中扣除所述交易费的支付账户。

2. 根据权利要求1所述的方法,其中,确定所述交易发起方是否是所述交易接收方的被担保用户包括:

响应于确定所述交易请求还指示所述交易接收方的签名信息,确定所述交易发起方是所述交易接收方的被担保用户。

3. 根据权利要求2所述的方法,其中,响应于基于在所述交易接收方的管理设备处存储的在所述交易发起方和所述交易接收方之间的担保关系而确定所述交易发起方是所述交易接收方的被担保用户,所述交易接收方的所述签名信息由所述管理设备利用所述交易接收方的私钥对所述交易内容进行签名来生成并被添加到所述交易请求。

4. 根据权利要求3所述的方法,其中,还响应于确定所述交易发起方的信用余额大于或等于所述交易费,所述交易接收方的所述签名信息由所述交易接收方的管理设备利用所述交易接收方的私钥对所述交易内容进行签名来生成并被添加到所述交易请求。

5. 根据权利要求1所述的方法,其中,确定所述交易发起方是否是所述交易接收方的所述被担保用户包括:

基于在所述区块链上记录的在所述交易发起方和所述交易接收方之间的担保关系来确定所述交易发起方是否是所述交易接收方的所述被担保用户。

6. 根据权利要求5所述的方法,还包括:

响应于确定所述交易发起方不是所述交易接收方的被担保用户,确定所述交易发起方的第一账户的余额是否大于或等于所述交易费;以及

响应于确定所述交易发起方的所述第一账户的余额大于或等于所述交易费,将所述交易发起方的所述第一账户确定为所述支付账户。

7. 根据权利要求1所述的方法,其中,确定从中扣除所述交易费的支付账户还包括:

响应于确定不存在与所述交易接收方相关联的担保账户或者响应于确定所述担保账户的余额小于所述交易费,确定所述交易接收方的第二账户的余额是否大于或等于所述交易费;以及

响应于确定所述交易接收方的所述第二账户的余额大于或等于所述交易费,将所述交易接收方的所述第二账户确定为所述支付账户。

8. 根据权利要求7所述的方法,其中,确定从中扣除所述交易费的支付账户包括:

响应于确定所述交易接收方的所述第二账户的余额小于所述交易费,确定所述交易发起方的第一账户的余额是否大于或等于所述交易费;以及

响应于确定所述交易发起方的所述第一账户的余额大于或等于所述交易费,将所述交易发起方的所述第一账户确定为所述支付账户。

9. 根据权利要求8所述的方法,还包括:

响应于确定所述交易内容指示将转账金额的加密货币从所述交易发起方转移到所述交易接收方的转账交易,确定所述交易发起方的第三账户的余额是否大于或等于所述转账金额;以及

响应于确定所述交易发起方的所述第三账户的余额大于或等于所述转账金额,将所述转账金额的加密货币从所述交易发起方的所述第三账户转移到所述交易接收方的第四账户。

10. 根据权利要求9所述的方法,其中,所述第一账户和所述第二账户对应于第一类型的加密货币,所述第三账户和所述第四账户对应于第二类型的加密货币,以及所述第一类型不同于所述第二类型。

11. 根据权利要求8所述的方法,还包括:

响应于确定所述交易内容指示将转账金额的加密货币从所述交易发起方转移到所述交易接收方的转账交易,确定所述交易发起方的所述第一账户的余额是否大于或等于所述转账金额;以及

响应于确定所述交易发起方的所述第一账户的余额大于或等于所述转账金额,将所述转账金额的加密货币从所述交易发起方的所述第一账户转移到所述交易接收方的所述第二账户,其中所述第一账户、所述第二账户和所述转账金额的加密货币对应于第一类型的加密货币。

12. 根据权利要求1所述的方法,其中,确定从中扣除所述交易费的支付账户还包括:

基于在所述区块链上记录的所述交易发起方的信用信息来确定所述交易发起方的信用余额是否大于或等于所述交易费;以及

响应于确定所述交易发起方的所述信用余额大于或等于所述交易费,确定从中扣除所述交易费的所述支付账户。

13. 根据权利要求4或12所述的方法,其中,在所述区块链上记录的所述交易发起方的信用信息至少指示信用限额和已使用的信用,以及所述信用余额由下式确定:

信用余额 = 信用限额 - 已使用的信用。

14. 根据权利要求13所述的方法,其中,所述信用信息还包括信用恢复速率和区块的高度,所述信用恢复速率指示由经过的每个区块所恢复的信用量,所述区块的高度指示从上次所述交易接收方为所述交易发起方支付所述交易费起所经过的区块的数量,以及所述信用余额由下式确定:信用余额 = 信用限额 - 已使用的信用 + 区块的高度 * 信用恢复速率。

15. 根据权利要求4或12所述的方法,其中,在所述区块链上记录的所述交易发起方的信用信息至少指示信用支付次数限制和已使用的信用支付次数,以及所述信用余额由下式确定:

信用余额 = 信用支付次数限制 - 已使用的信用支付次数。

16. 一种用于管理区块链交易的方法,包括:

在用于管理所述区块链交易的管理设备处,从所述交易的交易发起方接收请求,所述请求至少指示所述交易的所述交易发起方、交易内容和交易接收方;

确定所述交易发起方是否是所述交易接收方的被担保用户;以及

响应于确定所述交易发起方是所述交易接收方的被担保用户:

通过生成所述交易接收方的签名信息并将所述签名信息添加到接收到的请求来形成交易请求,所述签名信息指示允许从与所述交易接收方相关联的支付账户扣除区块链的区块链节点处理所述区块链交易的交易费;以及

确定是否存在与所述交易接收方相关联的担保账户:

响应于确定存在与所述交易接收方相关联的担保账户,确定所述担保账户的余额是否大于或等于所述交易费;以及响应于确定所述担保账户的余额大于或等于所述交易费,将所述担保账户确定为所述支付账户。

17. 根据权利要求16所述的方法,其中,确定所述交易发起方是否是所述交易接收方的被担保用户包括:

基于在所述管理设备处存储的在所述交易发起方和所述交易接收方之间的担保关系来确定所述交易发起方是否是所述交易接收方的被担保用户。

18. 根据权利要求16所述的方法,其中,通过生成所述签名信息并将所述签名信息添加到接收到的请求来形成交易请求包括:

基于在所述管理设备处存储的所述交易发起方的信用信息来确定所述交易发起方的信用余额是否大于或等于所述交易费;以及

响应于确定所述交易发起方的所述信用余额大于或等于所述交易费,通过利用所述交易接收方的私钥对所述交易内容进行签名来生成所述签名信息并将所述签名信息添加到所述接收到的请求。

19. 根据权利要求18所述的方法,其中,所述信用信息至少指示信用限额和已使用的信用,以及所述信用余额由下式确定:

信用余额 = 信用限额 - 已使用的信用。

20. 根据权利要求19所述的方法,其中,所述信用信息还包括信用恢复速率和区块的高度,所述信用恢复速率指示由经过的每个区块所恢复的信用量,所述区块的高度指示从上次所述交易接收方为所述交易发起方支付所述交易费起所经过的区块的数量,以及所述信用余额由下式确定:信用余额 = 信用限额 - 已使用的信用 + 区块的高度 * 信用恢复速率。

21. 根据权利要求18所述的方法,其中,所述信用信息至少指示信用支付次数限制和已使用的信用支付次数,以及所述信用余额由下式确定:

信用余额 = 信用支付次数限制 - 已使用的信用支付次数。

22. 一种用于处理区块链交易的设备,所述设备包括:

存储器,其被配置为存储一个或更多个程序;以及

处理单元,其耦合到所述存储器并被配置为执行所述一个或更多个程序以使所述设备执行根据权利要求1-15中的任一项所述的方法。

23. 一种用于管理区块链交易的设备,所述设备包括:

存储器,其被配置为存储一个或更多个程序;以及

处理单元,其耦合到所述存储器并被配置为执行所述一个或更多个程序以使所述设备执行根据权利要求16-21中的任一项所述的方法。

24. 一种存储有机器可执行指令的非暂时性计算机可读存储介质,所述机器可执行指

令在被执行时使机器执行根据权利要求1-21中的任一项所述的方法。

区块链交易处理

[0001] 领域

[0002] 本公开的实施例总体上涉及在区块链上的交易处理的领域,且更特别地涉及处理或管理区块链交易。

[0003] 背景

[0004] 在传统的区块链交易处理方案中,每当个人或企业想要使用区块链服务来转移加密货币或调用和执行智能合约时,他们必须将交易发送到网络,并通过使用他们自己的账户余额来支付处理区块链交易所需的交易费。

[0005] 对于一些区块链应用,交易的发起方可以是普通用户。当用户从市场上获得加密货币时,他/她将不得不面对高价格波动。因此,传统的交易管理方案对普通用户支付用于处理区块链交易的交易费是不方便的。此外,对于转账交易,一定金额的加密货币需要从交易的发起方转移到交易接收方。区块链交易费和待转移的金额可以是不同类型的加密货币,这要求用户有至少两种类型的加密货币,并熟悉用于管理他们的加密货币的各种类型的工具,以便确保他们的账户余额足够用于交易费和待转移的金额。因此,传统的交易处理方案对使用区块链应用的普通用户造成许多负担。

[0006] 概述

[0007] 通常,本公开的示例实施例提供了用于处理或管理区块链交易的解决方案,区块链服务可以通过该解决方案由普通用户方便地使用。

[0008] 根据本公开的第一方面,提供了用于处理区块链交易的方法。该方法包括:在用于处理区块链交易的区块链的区块链节点处,接收交易请求,交易请求至少指示交易的交易发起方、交易内容和交易接收方;基于交易内容来计算用于处理交易的交易费;确定交易发起方是否是交易接收方的被担保用户(a sponsored user);以及响应于确定交易发起方是交易接收方的被担保用户,确定从中扣除交易费的支付账户。

[0009] 根据本公开的第二方面,提供了用于管理区块链交易的方法。该方法包括:在用于管理区块链交易的管理设备处,从交易的交易发起方接收请求,该请求至少指示交易的交易发起方、交易内容和交易接收方;确定交易发起方是否是交易接收方的被担保用户;以及响应于确定交易的发起方是交易接收方的被担保用户,通过生成交易接收方的签名信息并将该签名信息添加到接收到的请求来形成交易请求,该签名信息指示允许从与交易接收方相关联的支付账户中扣除对于区块链的区块链节点处理区块链交易的交易费。

[0010] 根据本公开的第三方面,提供了用于处理区块链交易的设备。该设备包括:存储器,其被配置为存储一个或多个程序;以及处理单元,其耦合到存储器并被配置为执行所述一个或多个程序以使设备执行在本公开的第一方面中的方法的步骤。

[0011] 根据本公开的第四方面,提供了用于管理区块链交易的设备。该设备包括:存储器,其被配置为存储一个或多个程序;以及处理单元,其耦合到存储器并被配置为执行所述一个或多个程序以使设备执行在本公开的第二方面中的方法的步骤。

[0012] 根据本公开的第五方面,提供了其上存储有机器可执行指令的非暂时性计算机可读存储介质,机器可执行指令在被执行时使机器执行本公开的第一方面和第二方面中的任

一方面中的方法的步骤。

[0013] 根据本公开的第六方面,提供了计算机程序产品。计算机程序产品有形地存储在非暂时性计算机可读介质上并且包括机器可执行指令,机器可执行指令当被执行时使机器执行本公开的第一方面和第二方面中的任一方面中的方法的步骤。

[0014] 应理解,本概述既不意欲确定本公开的实施例的关键或必要特征,也不意欲用于限制本公开的范围。本公开的其他特征通过下面的描述将变得易于理解。

[0015] 附图简述

[0016] 通过参考附图更详细地描述本公开的示例性实施例,本公开的上述和其他目的、特征和优点将变得更明显,其中在本公开的示例性实施例中相同的参考符号表示相同的部件。

[0017] 图1示出了在现有技术中的交易处理方法的流程图;

[0018] 图2示出了根据本公开的实施例的交易处理系统的架构图;

[0019] 图3示出了根据本公开的实施例的用于处理区块链交易的方法的流程图;

[0020] 图4示出了根据本公开的实施例的用于管理区块链交易的方法的流程图;

[0021] 图5示出了根据本公开的实施例的由管理设备接收的请求;

[0022] 图6示出了根据本公开的实施例的具有交易接收方的签名信息的交易请求;

[0023] 图7示出了根据本公开的实施例的用于处理区块链交易的方法的流程图;以及

[0024] 图8示意性示出了适合于实现本公开的实施例的示例设备的框图。

[0025] 在每个图中,相同或相应的符号指示相同或相应的部件。

[0026] 详细描述

[0027] 现在将参考一些示例实施例描述本公开的原理。应当理解,这些实施例仅仅为了说明的目的而被描述,并且帮助本领域中的技术人员理解和实现本公开而不暗示关于本公开的范围的任何限制。本文所述的本公开可以以除了下面描述的方式之外的各种方式被实现。

[0028] 在下面的描述和权利要求中,除非另有规定,否则本文所使用的所有技术和科学术语具有与由在本公开所属的领域中的普通技术人员之一通常理解的相同的含义。

[0029] 在本公开中对“一个实施例”、“实施例”、“示例实施例”和诸如此类的提及指示所描述的实施例可包括特定特征、结构或特性,但是不一定每个实施例都包括该特定特征、结构或特性。此外,这样的短语不一定指同一实施例。此外,当关于实施例描述特定特征、结构或特性时,认为关于其他实施例(无论是否被明确地描述)实现这种特征、结构或特性是在本领域中的技术人员的知识范围内的。

[0030] 应理解,尽管术语“第一”、“第二”、“第三”和“第四”等在本文可用于描述各种元件,但这些元件不应被这些术语限制。这些术语仅用来将一个元件与另一元件区分开。例如,第一元件可以被称为第二元件,且类似地,第二元件可以被称为第一元件,而不偏离示例实施例的范围。例如,在下面的描述中,第一、第二、第三和第四账户仅意欲区分不同实体的不同账户,而不是账户的数量或顺序的限制的任何意图。如本文所使用的,术语“和/或”包括所列出的项目中的一个或更多的任何和所有组合。

[0031] 本文使用的术语仅为了描述特定实施例的目的,且并没有被规定为示例实施例的限制。如本文所使用的,单数形式“一(a)”、“一(an)”和“该(the)”意欲也包括复数形式,除

非上下文另外清楚地指示。将进一步理解,术语“包括(comprises)”、“包括(comprising)”、“具有(has)”、“具有(having)”、“包括(includes)”和/或“包括(including)”当在本文中被使用时规定所陈述的特征、元件和/或部件等的存在,但不排除一个或更多个其它特征、元件、部件和/或其组合的存在或添加。

[0032] 图1示出了在现有技术中的交易管理方法100的流程图。如图1所示,在块102处,区块链的交易处理节点接收交易请求。例如,交易请求指示将一定金额的加密货币从交易发起方转移到交易接收方的转账交易。在块104处,交易处理节点认证交易发起方的身份。在块106处,交易处理节点计算用于处理交易的交易费。在块108处,交易处理节点确定交易发起方的账户余额是否大于或等于所计算的交易费。如果在块108中的确定的结果为否,则方法100转到块116,其中确定交易的处理失败。如果在块108中的确定的结果为是,即,交易发起方的账户余额大于或等于所计算的交易费,则在块110处交易处理节点从交易发起方的账户中扣除交易费。然后,如果交易请求指示将一定金额的加密货币从交易发起方转移到交易接收方的转账交易,则在块112处交易处理节点确定交易发起方的已更新账户余额是否大于或等于待转移的金额。如果在块112中的确定的结果为是,则在块114处交易处理节点将该金额的加密货币从交易发起方的账户转移到交易接收方的账户。如果在块112中的确定的结果为否,即,交易发起方的已更新账户余额小于待转移的金额,则方法100转到块116,其中也确定交易的处理失败。

[0033] 如上面所陈述的,在传统的交易处理方案中,用于处理交易的交易费只可以由交易发起方支付。如果发起方的账户余额小于所需的交易费或小于待转移的金额,则交易的处理将失败。此外,在许多区块链系统中,区块链交易费和待转移的金额可以是不同类型的加密货币。在这种情况下,交易发起方需要具有至少两种类型的加密货币,并熟悉用于管理他们的加密货币的至少两种类型的工具,以便确保他们的账户余额足够用于交易费和待转移的金额。因此,传统的交易处理方案为普通用户造成很多负担。

[0034] 为了至少部分地解决上述问题以及其他潜在问题中的一个或更多个,本公开的示例实施例提出了交易处理解决方案。在该解决方案中,用于处理区块链交易的区块链的区块链节点接收至少指示交易的交易发起方、交易内容和交易接收方的交易请求。区块链节点基于交易内容来计算用于处理交易的交易费,并确定交易发起方是否是交易接收方的被担保用户。响应于确定交易发起方是交易接收方的被担保用户,区块链节点确定从中扣除交易费的支付账户。如在本公开中提供的交易处理解决方案使普通用户能够方便地使用区块链服务。

[0035] 与区块链交易费只可以由交易发起方支付的传统交易处理方案不同,在上述解决方案中,通过确定交易发起方是交易接收方的被担保用户,交易处理节点可以确定从中扣除交易费的支付账户。区块链交易费可以由所确定的支付账户(例如,担保账户(a sponsor account)、交易接收方的账户或交易发起方的账户中的任一个)支付。以这种方式,普通用户可以像当前的普通应用一样使用区块链服务,而无需特别注意使用/管理他们的加密货币来支付交易费。因此,本公开为普通用户使用区块链服务以及为具有多个不同区块链服务的企业管理这些服务提供了更大的便利,这将鼓励更多用户使用区块链服务。

[0036] 图2示出了根据本公开的实施例的交易处理系统200的架构图。如图2所示,系统200包括管理设备214、用于处理区块链交易的多个节点212-1、212-2至212-N(即,交易处理

节点212)以及多个终端设备(例如,移动电话242、计算机240和244)。管理设备214和交易处理节点212可以都是区块链平台210的区块链节点。管理设备214、交易处理节点212和终端设备可以经由网络230来执行数据的交互。

[0037] 应当理解,区块链节点的数量和终端设备的数量仅仅是为了说明的目的,而不暗示任何限制。系统200可以包括适合于实现本公开的实施例的任何合适数量的区块链节点和终端设备。

[0038] 终端设备可以是任何终端设备,其可以包括但不限于移动电话、蜂窝电话、智能电话、IP语音(VoIP)电话、无线本地环路电话、平板计算机、个人数字助理(PDA)、便携式计算机、台式计算机等。用户250或252可以通过相应的终端设备240或242发起交易,并且终端设备可以向管理设备214传输对与管理设备214的接收方地址相关联的服务的相应交易请求。在一些实施例中,钱包应用可以在终端设备上运行。用户250或252可以通过钱包应用向管理设备214注册以获得在管理设备214处唯一地标识用户的关联账户ID。关联账户ID可以是例如但不限于用户的标识(例如邮箱或移动电话号码)和管理设备214或管理设备214的运营商的标识的组合。此外,用户250或252可以通过钱包应用生成他们自己的地址以充当用于他们的区块链交易的发起方地址或接收方地址。在一些实施例中,终端设备可以通过使用用户的私钥对交易请求进行签名来生成关于交易请求的签名信息。用户可以通过向交易接收方的智能合约注册来成为交易接收方的被担保用户,该智能合约专用于担保交易费的支付。

[0039] 管理设备214可以是用于充当区块链平台210的节点的网络设备。管理设备214可以包括但不限于一个或更多个计算机或服务器。管理设备214可以经由相应的终端设备从用户250和252接收交易请求。管理设备214可以经由用户250和252的地址为他们提供区块链服务。例如,假设用户252是交易接收方的被担保用户,其已经向交易接收方的接收方地址注册并与交易接收方一起签署了担保支付的智能合约。换句话说,交易接收方的被担保用户不仅向交易接收方(例如管理设备214)注册为交易接收方的注册用户,而且还特别向交易接收方的智能合约注册,该智能合约专用于担保由用户向交易接收方发起的交易的交易费的支付。还假设用户250仅仅是交易接收方的普通注册用户,但不是接收方的被担保用户。管理设备214可以在管理设备214的初始化过程期间使担保账户与交易接收方相关联。此外,在一些实施例中,管理设备214还可以确定对于每个被担保用户的信用信息。在一些实施例中,管理设备214可以确定接收到的请求的交易发起方是交易接收方的被担保用户,并且其后它可以通过使用交易接收方的私钥对交易请求签名来生成签名信息并将该签名信息添加到接收到的请求,以形成交易请求。管理设备214可以进一步在区块链平台210上分发具有签名信息的交易请求,或者将具有签名信息的交易请求传输到交易处理节点212中的任一个或全部。在这种情况下,利用交易接收方的签名信息,管理设备214可以向用于处理交易的交易处理节点212指示针对该交易的交易费可以由交易接收方支付。

[0040] 在本文中,管理设备214、交易接收方、接收方地址和交易接收方的账户可以在一些实施例中可互换地被使用,以指示当前交易指向的区块链实体。

[0041] 关于区块链平台210,它用于处理区块链交易和存放交易结果数据。在架构上,区块链平台210自上而下包括例如基本服务层、智能合约层和区块链底层(未示出)。区块链平台210可以包括管理设备214和交易处理节点212。此外,如果终端设备240、242和244可以充

当区块链节点,则区块链平台210还可以包括它们中的任一个或全部。在一些实施例中,区块链平台210可以基于私有区块链、公共区块链或联合区块链(federated blockchain)。

[0042] 交易处理节点212可以是充当区块链平台210的节点的网络设备。用于交易处理的交易处理节点212(即,交易处理节点212)可以包括但不限于一个或多个计算机或服务。交易处理节点212能够从管理设备214接收交易请求,并基于接收到的交易请求来计算用于处理交易的交易费。当交易处理节点212确定交易的发起方是交易接收方的被担保用户时,它可以确定支付账户并从该支付账户中扣除所计算的交易费。在一些实施例中,交易处理节点212可以基于在接收到的交易请求中指示的交易接收方的签名信息或者基于在交易发起方和交易接收方之间的担保关系来确定交易发起方是否是交易接收方的被担保用户。在后一种情况下,担保关系可以存储在区块链平台210上或交易处理节点212处。在前一种情况下,类似的担保关系可以存储在管理设备214处,用于使管理设备214确定交易发起方是否是交易接收方的被担保用户。

[0043] 在一些实施例中,如果交易处理节点212确定交易发起方是交易接收方的被担保用户,则本公开的三层支付模型将用于确定从中扣除交易费的支付账户。将在下面参考图3到图7详细描述三层支付模型。

[0044] 另一方面,如果交易处理节点212确定交易发起方不是交易接收方的被担保用户,则它可以确定交易发起方的第一账户的余额是否大于或等于交易费。如果发起方的第一账户的余额大于或等于交易费,则交易处理节点212可以将交易发起方的第一账户确定为支付账户,并从交易发起方的第一账户中扣除交易费。

[0045] 图3示出根据本公开的实施例的用于处理区块链交易的方法300的流程图。在图3中,各种行动例如由如图2所示的交易处理节点212的处理器执行。方法300还可以包括未示出的附加行动和/或可以省略所示出的行动,本公开的范围并不被限制在这个方面中。

[0046] 在块302处,交易处理节点212接收交易请求。交易请求至少指示交易的交易发起方、交易内容和交易接收方。交易请求可以由交易处理节点212从图2所示的管理设备214接收。在一些实施例中,交易请求进一步指示交易发起方的签名信息和/或交易接收方的签名信息。在一些实施例中,交易接收方是用于基于特定智能合约来为接收方的被担保用户或普通注册用户提供一个或多个服务的商业操作系统。

[0047] 在块304处,交易处理节点212基于交易内容来计算用于处理交易的交易费。例如,交易内容可以指示交易是要在区块链平台上部署新的智能合约、调用所部署的智能合约,或者将转账金额的加密货币从交易发起方转移到交易接收方。在一些实施例中,交易费和转账金额可以是不同类型的加密货币。在一些其他实施例中,交易费和转账金额都是相同类型的加密货币。

[0048] 在块306处,交易处理节点212可以确定交易发起方是否是交易接收方的被担保用户。

[0049] 在一些实施例中,交易处理节点212可以基于由接收到的交易请求指示的交易接收方的签名信息来确定交易发起方是否是交易接收方的被担保用户。在这种情况下,在向交易处理节点212传输交易请求之前,管理设备214可以基于例如存储在管理设备214处的交易发起方和交易接收方之间的担保关系来确定交易发起方是否是交易接收方(即,管理设备214)的被担保用户。响应于确定交易发起方是交易接收方的被担保用户,管理设备

214可以进一步在从交易发起方的相应终端设备接收的请求上添加签名。签名可以通过管理设备214利用管理设备214的私钥对交易内容进行签名来生成。以这种方式,交易处理节点212可以只检查接收到的交易请求是否包括管理设备214的签名来确定交易发起方是否是交易接收方的被担保用户。

[0050] 可选地或此外,交易处理节点212可以基于在区块链平台210的一些或所有节点上记录的在交易发起方和交易接收方之间的担保关系来确定交易发起方是否是交易接收方的被担保用户。在这种情况下,担保关系作为区块在区块链平台210上被预先发布,并且交易处理节点212可以基于在区块链平台210上记录的担保关系(例如下面在表1中所示的)来确定交易发起方是否是交易接收方的被担保用户。

[0051] 在一些另外的实施例中,在管理设备214确定交易发起方是交易接收方的被担保用户之后,管理设备214可以进一步确定交易发起方的信用余额是否大于或等于交易费。可以参考存储在管理设备214处的专用于被担保用户的信用信息(例如下面在表3中被示为信用计划的信用信息)来做出该确定。对于被担保用户的信用信息可以由管理设备214的操作者或管理设备214的其他监督者预先设置。只有当交易发起方的信用余额大于或等于交易费时,交易接收方的签名信息才被生成并被添加到交易请求中。以这种方式,交易处理节点212可以通过在交易请求中只检查管理设备214的签名信息的存在来确定交易发起方是交易接收方的被担保用户以及交易发起方的信用余额是足够的。

[0052] 返回到图3,在交易处理节点212基于在区块链平台210上记录的担保关系来确定交易发起方是否是交易接收方的被担保用户的实施例中,响应于确定交易发起方是交易接收方的被担保用户,方法300还可以包括交易处理节点212确定交易发起方的信用余额是否大于或等于交易费(未示出)。可以参考存储在区块链平台210的一些或所有节点上的专门用于被担保用户的信用信息(例如下面在表3中被示为信用计划的信用信息)来做出该确定。对于被担保用户的信用信息可以由管理设备214的操作者或管理设备214的其他监督者预先设置,并且可以作为区块在区块链平台210上被发布。

[0053] 关于上面提到的信用信息,它至少指示信用限额,该信用限额是交易接收方愿意为被担保用户支付交易费的金额的上限。在一些实施例中,存储在管理设备214或区块链平台210处的信用信息还可以包括已使用的信用,其指示交易接收方已经为被担保用户支付的交易费的金额。在这种情况下,可以基于信用限额和已使用的信用来确定信用余额。例如,信用余额可以由下面的公式(1)确定:

[0054] $\text{信用余额} = \text{信用限额} - \text{已使用的信用}$ (1)。

[0055] 在一些实施例中,除了信用限额和已使用的信用之外,信用信息还可以包括信用恢复速率和区块的高度(a height of blocks)。信用恢复速率指示由所经过的每个区块为被担保用户恢复的信用的量,以及区块的高度指示从上一次交易接收方为交易发起方(被担保用户)支付交易费起所经过的区块的数量。显然,由每个区块恢复的信用的量不能大于信用限额。在这种情况下,信用余额可以由下面的公式(2)确定:

[0056] $\text{信用余额} = \text{信用限额} - \text{已使用信用} + \text{区块的高度} * \text{信用恢复速率}$ (2)。

[0057] 可选地,信用计划可以是以由交易接收方为被担保用户进行担保支付的次数的形式。在这种情况下,信用信息可以至少指示信用支付次数限制和已使用的信用支付次数。信用支付次数限制可以是交易接收方愿意为被担保用户支付交易费的次数的上限,以及已使

用的信用支付次数可以指示交易接收方已经为被担保用户支付交易费的次数。在这种情况下,信用余额可由下面的公式(3)确定:

[0058] 信用余额=信用支付次数限制-已使用的信用支付次数(3)。

[0059] 在块308处,当交易处理节点212确定交易发起方是交易接收方的被担保用户(以及在一些另外的实施例中信用余额足够用于交易费)时,它进一步确定从中扣除交易费的支付账户。

[0060] 在一些实施例中,支付账户可以由三层模型确定,交易费可以利用该三层模型根据下面的顺序被扣除:担保账户、交易接收方和交易发起方。

[0061] 在一些实施例中,交易处理节点212可以确定是否存在与交易接收方相关联的担保账户。如果交易处理节点212确定存在与交易接收方相关联的担保账户,则交易处理节点212可以进一步确定担保账户的余额是否大于或等于交易费。如果确定担保账户的余额大于或等于交易费,则交易处理节点212可以将担保账户确定为支付账户,并从担保账户中扣除交易费。另一方面,如果交易处理节点212确定不存在与交易接收方相关联的担保账户或者确定担保账户的余额小于交易费,则交易处理节点212可以确定交易接收方的第二账户的余额是否大于或等于交易费。

[0062] 如果交易处理节点212确定交易接收方的第二账户的余额大于或等于交易费,则交易处理节点212可以将交易接收方的第二账户确定为支付账户,并从交易接收方的第二账户中扣除交易费。另一方面,如果交易处理节点212确定交易接收方的第二账户的余额小于交易费,则交易处理节点212可以确定交易发起方的第一账户的余额是否大于或等于交易费。如果交易处理节点212确定交易发起方的第一账户的余额大于或等于交易费,则交易处理节点212可以将交易发起方的第一账户确定为支付账户,并从交易发起方的第一账户中扣除交易费。

[0063] 在前述解决方案中,通过交易处理节点212基于交易发起方是交易接收方的被担保用户的确定来确定从中扣除交易费的支付账户,区块链交易费可以根据优选顺序从支付账户中被支付(例如,支付账户可以是担保账户、交易接收方的第二账户和交易发起方的第一账户中的任一个)。以这种方式,普通用户可以使用区块链服务,而无需特别注意使用/管理他们的加密货币来支付交易费。

[0064] 在一些实施例中,方法300还可以包括,在扣除交易费之后,如果交易处理节点212确定交易内容指示将转账金额的加密货币从交易发起方转移到交易接收方的转账交易,则交易处理节点212可以进一步确定交易发起方的第三账户的余额是否大于或等于转账金额。如果交易处理节点212确定交易发起方的第三账户的余额大于或等于转账金额,则它将转账金额的加密货币从交易发起方的第三账户转移到交易接收方的第四账户。

[0065] 在一些实施例中,交易费和转账金额可以对应于不同类型的加密货币。例如,交易发起方的第一账户和交易接收方的第二账户可以对应于交易费的第一类型的加密货币,交易发起方的第三账户和交易接收方的第四账户可以对应于转账金额的第二类型的加密货币,并且第一类型不同于第二类型。在这种情况下,交易处理节点212可以将转账金额的加密货币从交易发起方的第三账户转移到交易接收方的第四账户。换句话说,交易费以第一类型的加密货币被支付和接收,而待转移的加密货币以不同于第一类型的第二类型。

[0066] 在一些其他实施例中,交易费和转账金额可以对应于同一类型的加密货币。在这

种情况下,交易发起方的第一账户和第三账户可以是同一账户,以及交易接收方的第二账户和第四账户可以是同一账户。交易处理节点212可以将转账金额的加密货币从交易发起方的第一账户(即第三账户)转移到交易接收方的第二账户(即第四账户)。

[0067] 如上面所陈述的,描述了用于支付交易费的多层支付模型。例如,使用三层支付模型,交易费可以由担保账户、交易接收方的账户或交易发起方的账户中的任一个支付。以这种方式,普通用户可以像当前普通应用一样使用区块链服务,而不必特别注意区块链交易的交易费的支付。

[0068] 图4是根据本公开的实施例的用于管理区块链交易的方法400的流程图。在图4中,各种行动例如由图2所示的管理设备214的处理器执行。方法400还可以包括未示出的附加行动和/或可以省略所示出的行动,本公开的范围并不被限制在这个方面中。

[0069] 在块402处,管理设备214可以从交易发起方接收请求。该请求可以至少指示交易的交易发起方、交易内容和交易接收方。在一些实施例中,该请求从交易发起方经由终端设备(例如移动电话)242发送到管理设备214,即交易接收方。

[0070] 图5示出了根据本公开的实施例的由管理设备214接收的请求500。在图5中,请求500除了别的以外还至少包括交易内容。通常,请求500还包括如图5所示的交易发起方的签名信息。交易发起方的签名信息由交易发起方的终端设备用交易发起方的私钥对交易内容进行签名而生成。在请求500中的交易发起方的签名信息可以由管理设备214或交易处理节点212使用来认证交易发起方的身份。尽管没有特别示出,但是请求500可以进一步指示交易发起方和交易接收方。

[0071] 在块404处,管理设备214可以基于在管理设备214处存储的在交易发起方和交易接收方之间的担保关系来确定交易发起方是否是交易接收方的被担保用户。在一些实施例中,在管理设备214和/或用户的终端设备的初始化过程期间,管理设备214可以生成或以其他方式获得在被担保用户和交易接收方(即,管理设备214)之间的担保关系。此外,管理设备214可以为每个被担保用户设置信用计划。

[0072] 在一些实施例中,在交易发起方和交易接收方之间的担保关系指示在被担保用户和交易接收方之间的关联关系。在一些实施例中,担保关系进一步指示每个被担保用户的信用信息。例如,信用信息可以包括每个被担保用户的信用计划。

[0073] 下表1-3示出了根据本公开的实施例的担保关系。表1如下指示在接收方和被担保用户之间的关联关系。例如,用户1是接收方1的被担保用户,用户2是接收方2的被担保用户,以及用户3是接收方3的被担保用户。在一些实现方式中,表1中的接收方和被担保用户由他们的地址指示。其地址也可以被称为区块链地址、钱包地址,或者有时可以被称为账户或智能合约账户。例如,如果管理设备214(例如企业的服务器)为多于一个区块链应用托管多于一个智能合约,则每个智能合约地址可以充当指向相应智能合约的交易请求的交易接收方。在这种情况下,管理设备214可以维护包括如表1所示的关联关系的担保关系。在表1中,示出了一个接收方对应于一个被担保用户。然而,在大多数实际实现方式中,一个接收方可以对应于多于一个被担保用户。

[0074] 表1

[0075]	接收方1	被担保用户1
	接收方2	被担保用户2

接收方3	被担保用户3
------	--------

[0076] 表2如下指示在接收方和担保账户之间的关联关系,其指示接收方与用于为接收方支付交易费的对应的担保账户相关联。例如,担保账户1可以支持对接收方1的交易费的担保支付,担保账户2可以支持对接收方2的交易费的担保支付,以及担保账户3可以支持对接收方3的交易费的担保支付。这特别适用于企业开发和支持多个去中心化应用(DApp)的情况。在这种情况下,企业的管理设备214应该分别托管和管理DApp的多个智能合约,并且每个智能合约可以充当区块链交易的接收方。类似地,在实际实现方式中,表2中的接收方和担保账户由他们的地址指示。在表2中,示出了一个接收方对应于一个担保账户。然而,本公开不限于此,并且一个担保账户可以对应于多于一个接收方。例如,如果管理设备214(例如企业的服务器)为多个区块链应用托管多个智能合约,则它可以为所有或一些智能合约设置仅仅一个担保账户。

[0077] 表2

[0078]	接收方1	担保账户1
	接收方2	担保账户2
	接收方3	担保账户3

[0079] 表3如下指示在被担保用户和被担保用户的信用信息之间的关联关系。例如,如表3所示,用户1具有信用信息1,用户2具有信用信息2,以及用户3具有信用信息3。信用信息可以包括信用计划,并且信用计划可以针对所有被担保用户相同或不同地被配置。例如,信用信息可以至少包括信用限额和已使用的信用以用于根据上述公式(1)确定交易发起方的信用余额。在这种情况下,表3可以按区块动态地被更新。在一些另外的实施例中,信用信息还可以包括信用恢复速率和区块的高度,用于根据例如上述公式(2)确定交易发起方的信用余额。

[0080] 表3

[0081]	被担保用户1	信用信息1
	被担保用户2	信用信息2
	被担保用户3	信用信息3

[0082] 担保关系可以由管理设备214在区块链平台210上作为区块被发布,以便使用于处理交易的交易处理节点212能够得到担保关系。管理设备214还可以在本地存储担保关系。

[0083] 回来参考上面的表2,其说明了在多个接收方和多个担保账户之间的关系。在表中的每个接收方本质上由接收方的地址指示。根据接收方的性质,接收方的地址可以是智能合约地址或普通区块链地址(非智能合约地址)。在企业支持用于不同功能的多个DApp并且企业的管理设备214为DApp托管多个智能合约的情况下,可以为企业配置主账户(master account)以针对每个智能合约地址或非智能合约地址配置担保账户。例如,在管理设备或智能合约的初始化过程期间,主账户可以由管理设备214使用来确定每个接收方的担保账户或者确定在管理设备214中托管的所有或一些接收方的担保账户。以这种方式,通过使用主账户,企业可以使用甚至单个主账户来管理由它支持的所有智能合约。

[0084] 在一些实施例中,如果接收方是普通区块链地址(即,非智能合约地址),则接收方的主账户可以是接收方本身的账户或由企业指定的另一个账户。

[0085] 在一些其他实施例中,如果接收方是智能合约地址,则接收方的主账户可以缺省

地是智能合约的部署者的账户。此外,部署者可以将这个权利转移到另一个账户。

[0086] 在块406处,如果管理设备214确定发起方是交易接收方的被担保用户,则管理设备214将通过生成交易接收方的签名信息并将该签名信息添加到接收到的请求来形成交易请求。签名信息指示允许由接收方支付针对区块链节点处理区块链交易的交易费。在一些实施例中,签名信息通过管理设备214用交易接收方的私钥对交易内容进行签名来生成。在这种情况下,交易处理节点212将仅检查接收到的交易请求是否包括交易接收方的签名以确定交易发起方是否是交易接收方的被担保用户,而不是从区块链平台210取回担保12关系。

[0087] 图6示出了根据本公开的实施例的具有交易接收方的签名信息的交易请求600。在图6中,除了在请求500中包括的内容之外,交易请求600还包括交易接收方的签名信息。

[0088] 在一些实施例中,在管理设备214确定交易发起方是交易接收方的被担保用户之后,管理设备214可以基于在管理设备214处记录的交易发起方的信用信息来另外确定交易发起方的信用余额是否大于或等于交易费。在这种情况下,只有当管理设备214确定交易发起方的信用余额大于或等于交易费时,管理设备214才生成签名信息并将该签名信息添加到接收到的请求以形成交易请求。

[0089] 如上面所陈述的,在管理设备214在本地存储担保关系的实施例中,管理设备214可以确定是否为交易发起方支付交易费,并且如果它确定支付交易费则添加签名。在接收到交易请求(例如图6所示的交易请求)之后,交易处理节点212可以使用交易接收方的公钥来将接收到的交易请求解密,并获得接收方的签名信息。基于交易接收方的签名信息,交易处理节点212可以进一步确定接收到的交易已经被交易接收方确认为由接收方支付。在这种情况下,基于交易接收方的签名信息,交易处理节点212可以直接确定接收到的交易是具有担保支付的交易,并且不再需要做出关于交易发起方是否是交易接收方的被担保用户的进一步确定。

[0090] 图7是示出根据本公开的实施例的用于处理区块链交易的方法700的流程图。在图7中,行动可以由交易处理节点212-1、212-2到212-N中的任一个实现。应当认识到,方法700还可以包括未示出的附加行动和/或所示出的行动可以被省略,并且本公开的范围并不被限制在这个方面中。

[0091] 在块702处,交易处理节点212接收交易请求。交易请求可以至少指示交易的交易发起方、交易内容和交易接收方。在块704处,交易处理节点212可以认证交易发起方的身份。在块706处,如果交易发起方的身份在块704处被成功地认证,则交易处理节点212可以基于在交易请求中指示的交易内容来计算用于处理交易的交易费。

[0092] 在块708处,交易处理节点212可以确定交易请求是否指示交易接收方的签名信息。如果在块708处确定交易请求指示交易接收方的签名信息(是),这意味着交易发起方是交易接收方的被担保用户,则方法700继续进行到块712。另一方面,如果在块708处确定交易请求没有指示交易接收方的签名信息(否),则在块710处交易处理节点212可以基于在交易处理节点212处存储的或在区块链平台210上记录的在被担保用户和交易接收方之间的担保关系来进一步确定交易发起方是否是交易接收方的被担保用户。

[0093] 如果在块710处确定交易发起方不是交易接收方的被担保用户(否),则意味着交易不适用于本公开的担保支付模型并且方法700继续进行到块722以继续以传统方式处理

交易,即尝试由交易发起方支付交易费。另一方面,如果在块708或块710处确定交易发起方是交易接收方的被担保用户(是),则方法700继续进行以应用本公开的担保支付模型。在这种情况下,在块712处,交易处理节点212可以确定是否存在与交易接收方相关联的担保账户。

[0094] 如果在块712处确定存在与交易接收方相关联的担保账户(是),则方法700继续进行到块714,其中交易处理节点212可以确定担保账户的余额是否大于或等于交易费。如果在块714处确定担保账户的余额大于或等于交易费(是),则在块716处交易处理节点212可以从担保账户中扣除交易费。

[0095] 另一方面,如果在块712处确定不存在与交易接收方相关联的担保账户(否)或者在块714处确定担保账户的余额小于交易费,则该方法可以继续进行以尝试从接收方自己的账户支付交易费。在这种情况下,在块718处,交易处理节点212可以确定交易接收方的第二账户的余额是否大于或等于交易费。如果在块718处确定交易接收方的第二账户的余额大于或等于交易费(是),则在块720处,交易处理节点212可以从交易接收方的第二账户中扣除交易费。

[0096] 另一方面,如果在块718处确定交易接收方的第二账户的余额小于交易费(否),则方法700可以以传统方式继续进行,即,尝试由交易发起方支付交易费。在这种情况下,在块722处,交易处理节点212可以确定交易发起方的第一账户的余额是否大于或等于交易费。如果在块722处确定交易发起方的第一账户的余额大于或等于交易费(是),则在块724处交易处理节点212可以从交易发起方的第一账户中扣除交易费。

[0097] 到现在为止,描述了交易费的支付。在下文中,交易处理节点212可以以传统方式根据交易内容来处理交易。交易内容可以指示交易将在区块链上部署新的智能合约、向接收方转移一定金额的加密货币、在区块链上调用所部署的智能合约或其任何组合。然而,本公开不限于此,并且交易内容可以指示被开发或将在未来被开发的任何其他类型的区块链交易。在下文中,以转账交易作为示例来描述方法700的附加行动。

[0098] 在块716、720或724处的交易费的支付之后,在交易处理节点212确定交易内容指示将转账金额的加密货币从交易发起方转移到交易接收方的转账交易的情况下,在块728处交易处理节点212可以确定交易发起方的第三账户的余额是否大于或等于转账金额。如果在块728处确定交易发起方的第三账户的余额大于或等于转账金额(是),则在块730处交易处理节点212可以将转账金额的加密货币从交易发起方的第三账户转移到交易接收方的第四账户。

[0099] 另一方面,如果在块722处确定交易发起方的第一账户的余额小于交易费(否)或者如果在块728处确定交易发起方的第三账户的余额小于转账金额(否),则在块726处确定交易的处理失败。也就是说,账户的余额不足以用于交易费,或者不足以用于转账金额,整个交易将失败。此外,尽管图7示出了指示交易失败的单个块,但是它可以包括指示失败的交易的不同原因的附加块。

[0100] 在上面的描述中,假设交易费和转账金额是不同类型的加密货币。在这种情况下,交易发起方具有两个账户(即,第一账户和第三账户),其分别具有用于交易费和转账账户的两种不同类型的加密货币。类似地,交易接收方也具有两个账户(即,第二账户和第四账户),其分别具有用于交易费和转账账户的两种不同类型的加密货币。

[0101] 从上面可以看到,与交易发起方需要对于交易费和转账金额都具有足够金额的加密货币的传统交易管理方案不同,在本文描述的实现方式中,交易费可以由接收方(例如与交易接收方相关联的担保账户或者交易接收方的第二账户)支付。以这种方式,普通用户可以方便地使用区块链服务,而无需特别注意管理不同的加密货币来支付交易费或转账金额。

[0102] 然而,本公开不限于此。该系统和方法可以应用于以下情形,其中只涉及一种类型的加密货币且因此交易费和转账金额都是同一类型的加密货币。在这种情况下,交易发起方和交易接收方可以各自只有具有同一类型的加密货币的一个账户。因此,在块728处,不是确定交易发起方的第三账户的余额是否大于或等于转账金额,而是确定交易发起方的第一账户的余额(在交易费在块716处由担保账户支付或在块720处由接收方的账户支付的情况下)或更新后的余额(在交易费由发起方的账户支付的情况下)大于或等于转账金额。因此,在块730处,转账金额从交易发起方的第一账户转移到交易接收方的第二账户。

[0103] 关于发起方是否是接收方的被担保用户的确定,方法700描述了两步骤确定,即块708和710。然而,本领域中的技术人员应该理解,该确定可以仅由块708或块710做出。也就是说,不管是只检查接收方的签名还是基于担保关系来做出独立确定或两者,它都可以是整个区块链配置的高级策略。

[0104] 在一些实施例中,支付模型不限于上面所述的第三层模型(例如块716、720和724),它可以是两层模型。例如,交易处理节点212可以根据下列顺序之一来确定支付账户以扣除交易费:与交易接收方相关联的担保账户和交易接收方的第二账户(块716和720)、交易接收方的第二账户和交易发起方的第一账户(块720和724)、或者担保账户和交易发起方的第一账户(块716和724)。可以相应地修改图7的流程。

[0105] 图8示出了适合于实现本文描述的主题的实现的电子设备800的框图。设备800可以用于实现图2所示的系统200的一个或多个主机(例如,图2所示的用于交易处理的管理设备214、节点212-1、212-2至212-N)。如图8所示,设备800包括中央处理单元(CPU)801,其能够根据存储在只读存储器(ROM)802中的计算机程序指令或从存储单元808加载到随机存取存储器(RAM)803的计算机程序指令来执行各种行动和过程。在RAM 803中存储如设备800的操作所需的各种程序和数据。CPU 801、ROM 802和RAM 803经由总线804彼此连接。输入输出(I/O)接口805也连接到总线804。

[0106] 设备800的下列部件连接到I/O接口805:输入单元806,其包括键盘、鼠标或诸如此类;输出单元807,其包括各种显示器、扬声器和诸如此类;存储单元808,例如磁盘、光盘或诸如此类;通信单元809,例如网卡、调制解调器、无线通信收发器或诸如此类。通信单元809允许设备800通过计算机网络(例如互连网和/或各种电信网络)与其他设备交换信息/数据。

[0107] 处理单元801执行上面所述的各种方法和处理,例如执行方法300、400和700。例如在一些实施例中,方法300、400和700可以被实现为计算机软件程序,其存储在机器可读介质(例如存储单元808)中。在一些实施例中,部分或全部计算机程序可以经由ROM 802和/或通信单元809加载到设备800中和/或安装在设备800上。当计算机程序被加载到RAM 803并由CPU 801执行时,上面所述的方法300、400和700的一个或多个操作可以被执行。可选地,在其他实施例中,CPU 801可以以任何其他适当的方式(例如,借助于固件)被配置成执

行方法300、400和700的一个或更多个行动。

[0108] 需要进一步认识到,本公开可以是方法、装置、系统和/或计算机程序产品。计算机程序产品可以包括计算机可读存储介质(或多个介质),其具有在其上的用于使处理器执行本公开的各方面的计算机可读程序指令。

[0109] 计算机可读存储介质可以是有形设备,其可以保留和存储指令用于由指令执行设备使用。计算机可读存储介质可以是例如但不限于电子存储设备、磁性存储设备、光学存储设备、电磁存储设备、半导体存储设备或上述设备的任何合适的组合。计算机可读存储介质的更特定的例子的非详尽列表包括下列项:便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或闪存)、静态随机存取存储器(SRAM)、便携式光盘只读存储器(CD-ROM)、数字通用盘(DVD)、记忆棒、软盘、记录有指令的机械编码设备(例如穿孔卡片或在凹槽中的凸起结构)以及上述项的任何适当组合。如本文使用的计算机可读存储介质不应被解释为暂时性信号本身,例如无线电波或其他自由传播的电磁波、通过波导或其他传输介质传播的电磁波(例如,通过光纤电缆传递的光脉冲)或通过电线传输的电信号。

[0110] 可以将本文描述的计算机可读程序指令从计算机可读存储介质下载到相应的计算/处理设备,或者经由网络(例如互联网、局域网、广域网和/或无线网络)下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光传输光纤、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。在每个计算/处理设备中的网络适配器卡或网络接口从网络接收计算机可读程序指令,并转发计算机可读程序指令用于存储在相应计算/处理设备内的计算机可读存储介质中。

[0111] 用于执行本公开的操作的计算机可读程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据或者用一种或更多种编程语言(包括面向对象编程语言(例如Java、Smalltalk、C++或诸如此类)以及传统过程编程语言(例如“C”编程语言或类似的编程语言))的任何组合编写的源代码或目标代码。计算机可读程序指令可以完全在用户的计算机上、部分地在用户的计算机上、作为独立的软件包、部分地在用户的计算机上和部分地在远程计算机上或者完全在远程计算机或服务器上执行。在后一情形中,远程计算机可通过任何类型的网络(包括局域网(LAN)或广域网(WAN))连接到用户的计算机,或者可以建立到外部计算机的连接(例如通过使用互联网服务提供商的互联网)。在一些实施例中,包括例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA)的电子电路可以通过利用计算机可读程序指令的状态信息使电子电路个性化来执行计算机可读程序指令,以便执行本公开的各方面。

[0112] 在本文中参考根据本公开的实施例的方法、装置(系统)和计算机程序产品的流程图图示和/或框图描述了本发明的各方面。将理解,流程图图示和/或框图的每个块和在流程图图示和/或框图中的块的组合可以由计算机可读程序指令实现。

[0113] 这些计算机可读程序指令可被提供到通用计算机的、专用计算机的或生产机器的其他可编程数据处理装置的处理器,使得经由计算机的或其他可编程数据处理装置的处理器执行的指令创建用于实现在流程图和/或框图的一个或更多个块中指定的功能/行动的模块。这些计算机可读程序指令还可存储在计算机可读存储介质中,该指令可引导计算机、可编程数据处理装置和/或其他设备以特定方式起作用,使得存储有指令的计算机可读存

储介质包括制造物品,其包括实现在流程图和/或框图的一个或更多个块中指定的功能/行动的方面的指令。

[0114] 计算机可读程序指令还可以被下载到计算机、其他可编程数据处理装置或其他设备上,以使将在计算机、其他可编程装置或其他设备上执行的一系列操作步骤产生计算机实现的过程,使得在计算机、其他可编程装置或其他设备上执行的指令实现在流程图和/或框图的一个或更多个块中指定的功能/行动。

[0115] 附图中的流程图和框图示出了根据本公开的各种实施例的系统、方法和计算机程序产品的可能实现的架构、功能和操作。在这点上,在流程图或框图中的每个块可代表代码的模块、段或部分,代码包括用于实现指定的逻辑功能的一个或更多个可执行指令。还应当注意,在一些可选的实现方式中,在块中提到的功能可以不以在图中提到的顺序出现。例如,连续地示出的两个块事实上可以实质上同时被执行,或者块有时可以以相反的顺序被执行,这取决于所涉及的功能。还将提到,框图和/或流程图图示的每个块以及在框图和/或流程图图示中的块的组合可以由执行指定功能或行动的基于专用硬件的系统或专用硬件和计算机指令的组合来实现。

[0116] 本公开的各种实施例的描绘为了说明的目的被呈现,但并没有被规定为穷尽的或被限制到所公开的实施例。许多修改和变化对于本领域中的普通技术人员将是明显的,而不偏离所述实施例的范围和精神。本文使用的术语被选择以最好地解释实施例的原理、实际应用或优于在市场上找到的技术的技术改进,或者使本领域中的普通技术人员能够理解本文公开的实施例。

[0117] 所描述的内容仅仅是本公开的优选实施例,且并不意欲限制本公开。本领域中的技术人员认识到,本公开可以具有各种修改和变化。在本公开的精神和原理内的任何修改、等同替换和改进都落在本公开的保护范围内。

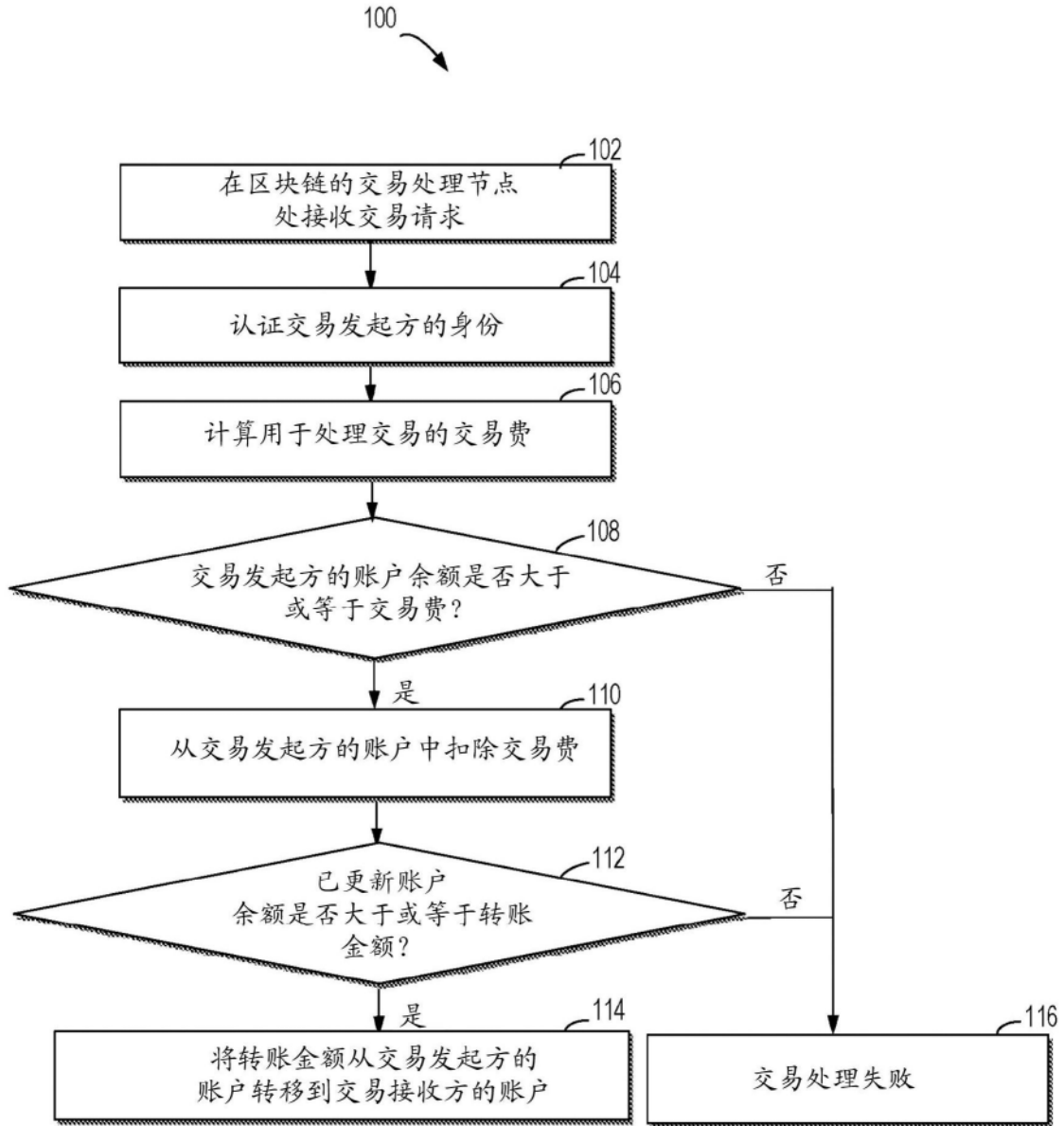


图1

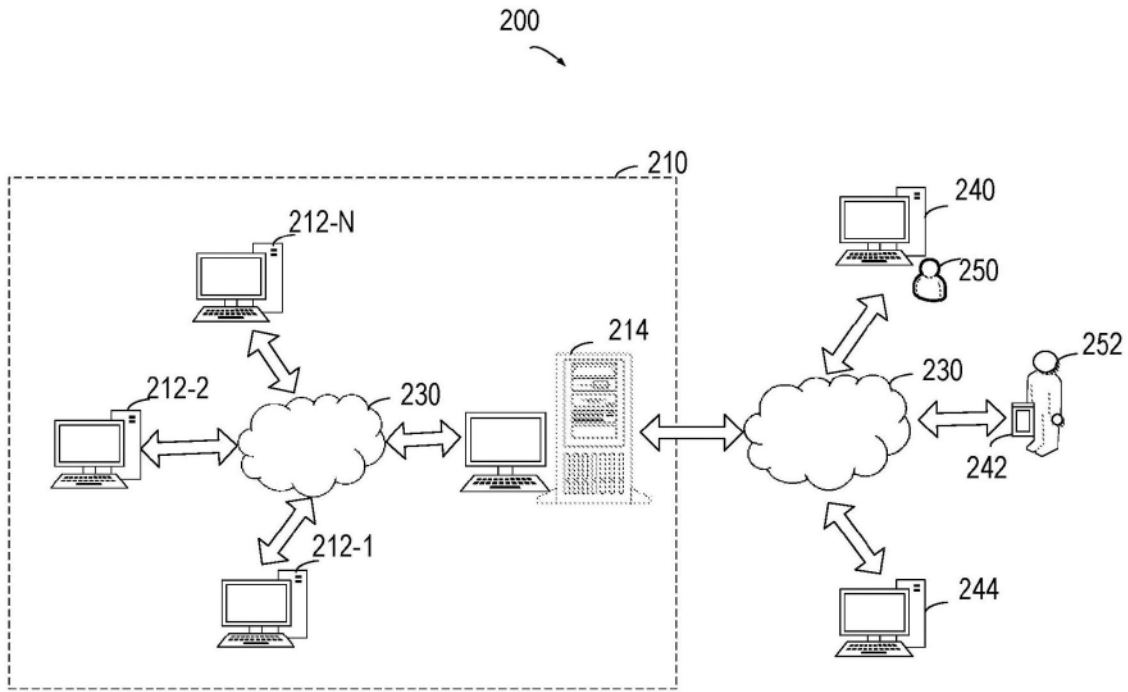


图2

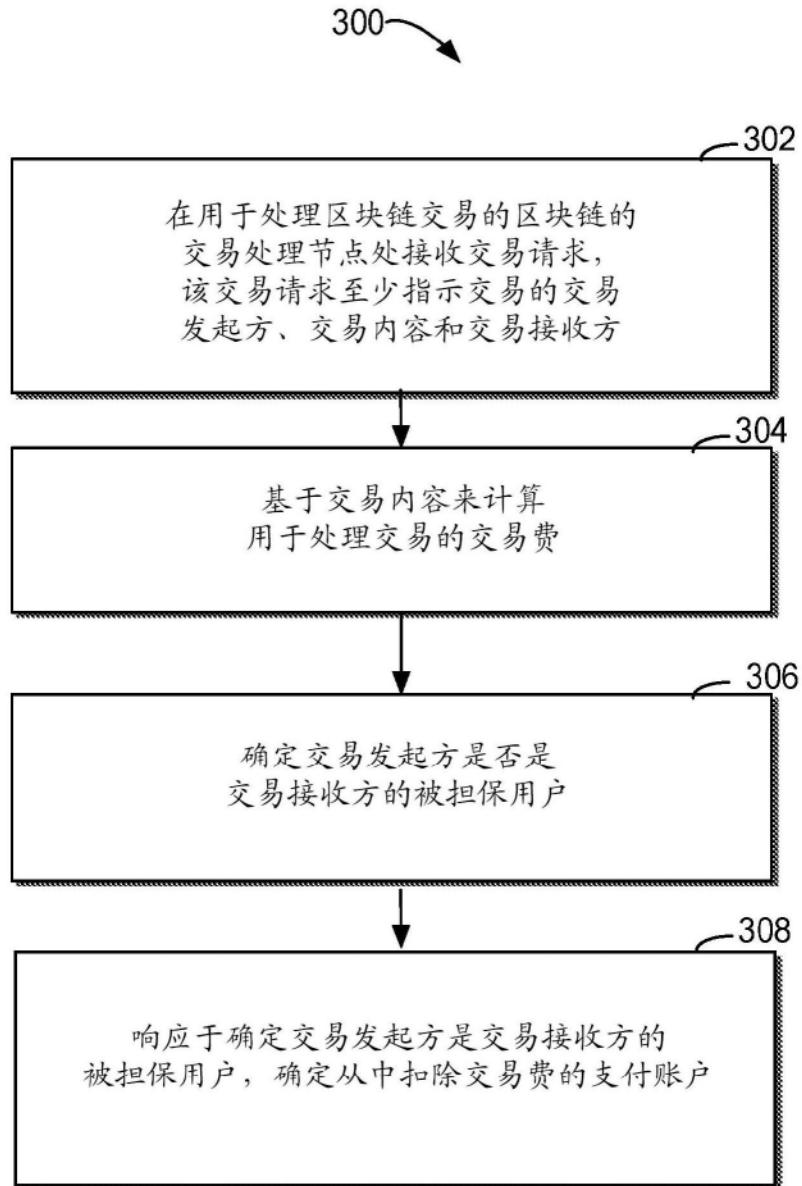


图3

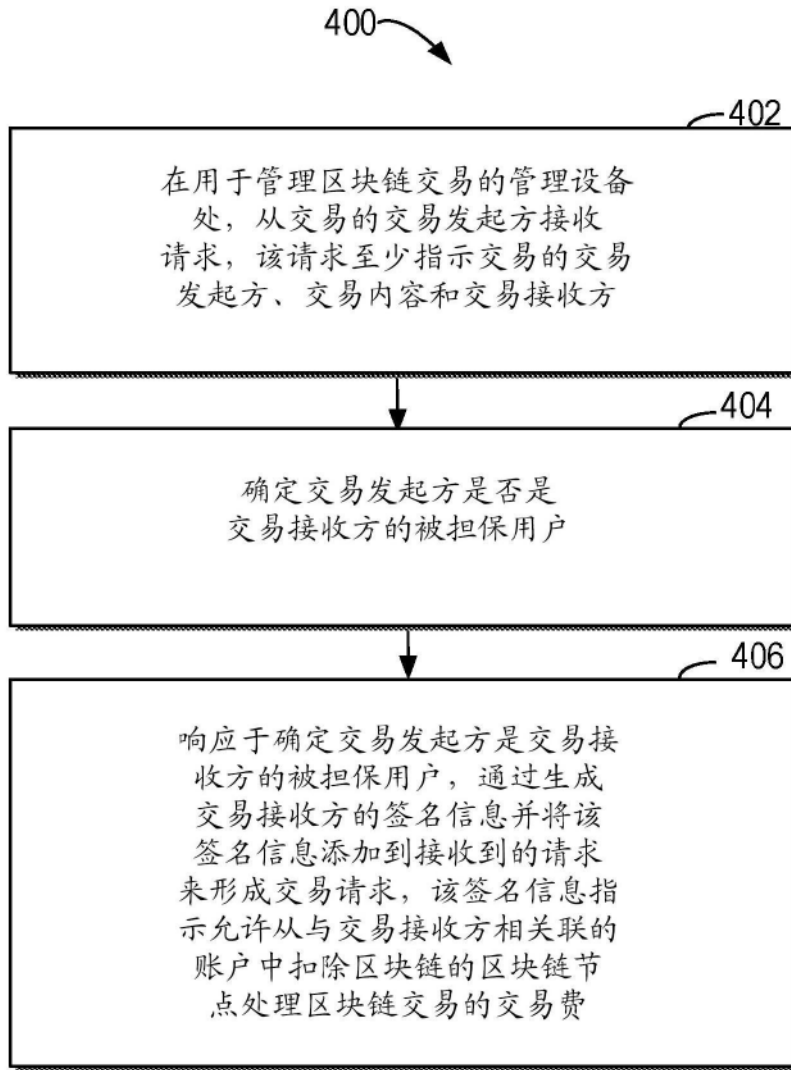


图4

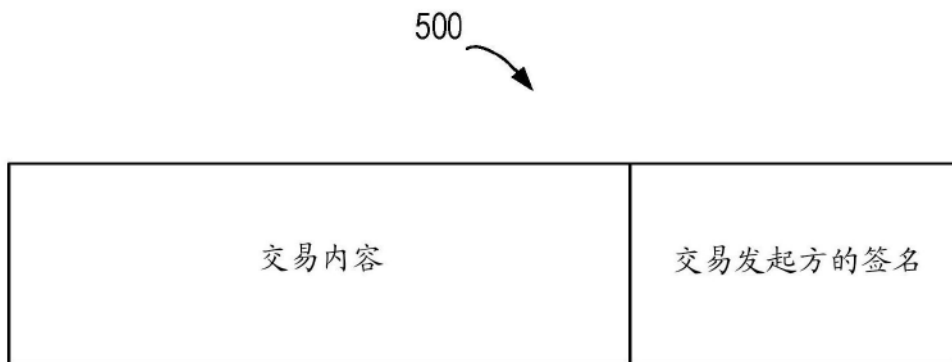


图5

600




图6

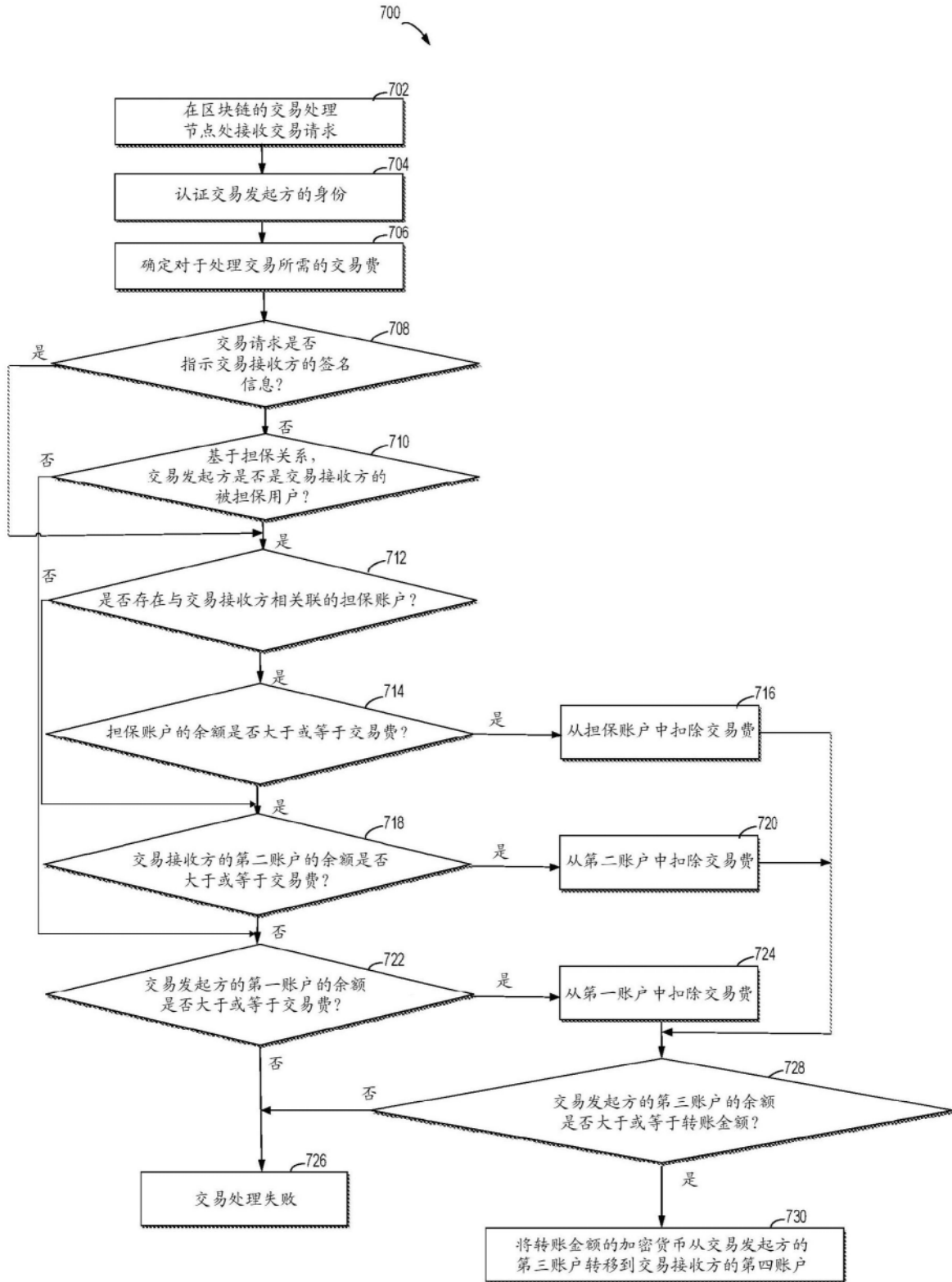


图7

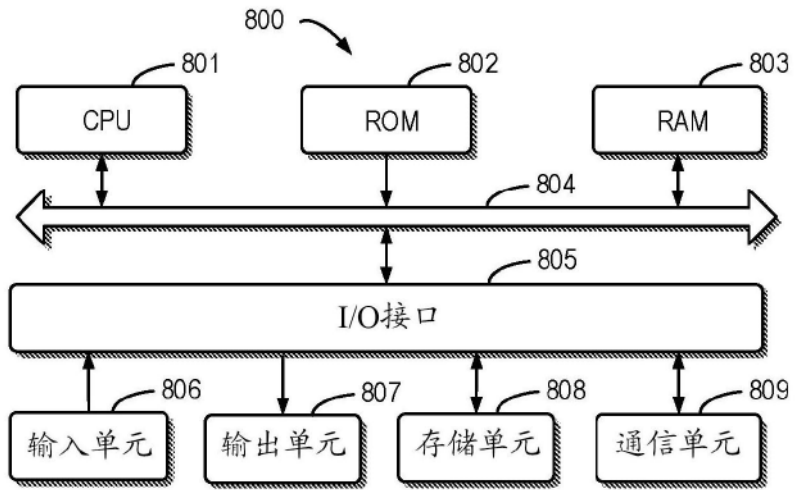


图8