



(12) 发明专利申请

(10) 申请公布号 CN 113128989 A

(43) 申请公布日 2021.07.16

(21) 申请号 202110391044.1

G06Q 40/04 (2012.01)

(22) 申请日 2019.02.01

(62) 分案原申请数据

201910104654.1 2019.02.01

(71) 申请人 创新先进技术有限公司

地址 开曼群岛大开曼岛乔治镇医院路27号
开曼企业中心

(72) 发明人 张文彬 陈盛龙 胡丹青 蒋国飞
马宝利 马环宇 闫雪冰 陈春伟

(74) 专利代理机构 北京博思佳知识产权代理有
限公司 11415

代理人 周嗣勇

(51) Int. Cl.

G06Q 20/10 (2012.01)

G06Q 20/38 (2012.01)

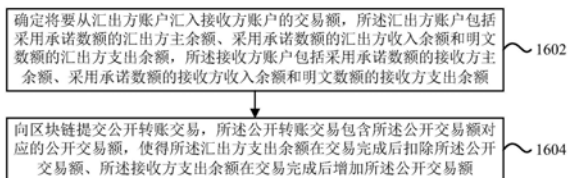
权利要求书3页 说明书16页 附图11页

(54) 发明名称

区块链交易方法及装置、电子设备、存储介
质

(57) 摘要

本说明书一个或多个实施例提供一种区块链交易方法及装置、电子设备、存储介质,应用于汇出方设备,所述方法包括:确定将从汇出方账户汇入接收方账户的交易额,所述汇出方账户包括采用承诺数额的汇出方主余额、采用承诺数额的汇出方收入余额和明文数额的汇出方支出余额,所述接收方账户包括采用承诺数额的接收方主余额、采用承诺数额的接收方收入余额和明文数额的接收方支出余额;向区块链提交公开转账交易,所述公开转账交易包含所述公开交易额对应的公开交易额,使得所述汇出方支出余额在交易完成后扣除所述公开交易额、所述接收方支出余额在交易完成后增加所述公开交易额。



1. 一种区块链交易方法,应用于汇出方设备,所述方法包括:

确定将要从汇出方账户汇入接收方账户的交易额,所述汇出方账户包括采用承诺数额的汇出方收入余额和明文数额的汇出方支出余额,所述接收方账户包括采用承诺数额的接收方收入余额和明文数额的接收方支出余额;

获取隐私类型设定信息;

当有限公开转账交易的发起条件被满足时,向区块链提交所述有限公开转账交易,所述有限公开转账交易包含所述交易额对应的交易额承诺、扣款额、用于证明所述交易额非负且所述扣款额不小于所述交易额的区间证明,使得所述汇出方支出余额在交易完成后扣除所述扣款额、所述汇出方收入余额在交易完成后增加所述扣款额和所述交易额之间的差值、所述接收方收入余额在交易完成后增加所述交易额,所述有限公开转账交易的发起条件包括所述隐私类型设定信息为私密类型。

2. 根据权利要求1所述的方法,所述有限公开转账交易的发起条件还包括下述至少之一:

用户设定选用有限公开转账交易、所述有限公开转账交易被设定为优先选用且所述汇出方支出余额不小于所述交易额、所述汇出方账户对应的备选扣款额集合内的任一预定数值的备选扣款额不小于所述交易额。

3. 根据权利要求2所述的方法,所述汇出方账户包括采用承诺数额的汇出方主余额,所述接收方账户包括采用承诺数额的接收方主余额;所述方法还包括:

当所述隐私类型设定信息为私密类型且主余额转账交易的发起条件被满足时,向区块链提交所述主余额转账交易,所述主余额转账交易包含所述交易额对应的交易额承诺和用于证明所述交易额非负且所述汇出方主余额不小于所述交易额的区间证明,使得所述汇出方主余额在交易完成后扣除所述交易额、所述接收方收入余额在交易完成后增加所述交易额,所述主余额转账交易的发起条件包括下述至少之一:用户设定选用主余额转账交易、所述主余额转账交易被设定为优先选用且所述汇出方支出余额小于所述交易额、所述汇出方账户对应的备选扣款额集合内的若干预定数值的备选扣款额均小于所述交易额。

4. 根据权利要求1所述的方法,还包括:

当所述隐私类型设定信息为非私密类型时,向区块链提交公开转账交易,所述公开转账交易包含所述交易额对应的公开交易额,使得所述汇出方支出余额在交易完成后扣除所述公开交易额、所述接收方支出余额在交易完成后增加所述公开交易额。

5. 根据权利要求1所述的方法,还包括:

获取所述汇出方账户对应的备选扣款额集合,所述备选扣款额集合包含若干预定数值的备选扣款额;

选取不小于所述交易额的任一备选扣款额,以作为所述扣款额。

6. 根据权利要求1或3所述的方法,所述交易额承诺由预设加密算法根据所述交易额和交易随机数计算得到;所述方法还包括:

在提交所述主余额转账交易或所述有限公开转账交易之前,将所述交易额、所述交易额承诺和所述交易随机数通过链外通道发送至接收方设备,以由所述接收方设备验证所述交易额承诺、所述交易随机数和所述交易额之间的对应关系;

接收所述接收方设备返回的接收方签名,以添加至所述主余额转账交易或所述有限公

开转账交易中;其中,所述接收方签名由所述接收方设备在所述对应关系通过验证后生成。

7. 根据权利要求1所述的方法,当所述汇出方账户的汇出方余额增大时,相应的金额被增加至所述汇出方收入余额。

8. 根据权利要求1所述的方法,所述汇出方账户包括采用承诺数额的汇出方主余额,所述接收方账户包括采用承诺数额的接收方主余额;所述方法还包括:

向区块链提交充值交易,所述充值交易包含充值额和用于证明所述汇出方主余额不小于所述充值额的区间证明,使得所述汇出方主余额在交易完成后扣除所述充值额、所述汇出方支出余额在交易完成后增加所述充值额。

9. 根据权利要求8所述的方法,还包括:

向区块链提交合并交易,所述合并交易包含合并额;

其中,所述汇出方支出余额在交易完成后扣除所述合并额、所述汇出方主余额在交易完成后增加所述合并额,和/或所述汇出方收入余额在交易完成后清零、所述汇出方主余额在交易完成后增加所述收入余额。

10. 一种区块链交易方法,应用于区块链节点,所述方法包括:

接收有限公开转账交易,所述有限公开转账交易在所述有限公开转账交易的发起条件被满足时由汇出方设备提交,所述有限公开转账交易的发起条件包括:隐私类型设定信息为私密类型;以及,所述汇出方设备被用于确定将从汇出方账户汇入接收方账户的交易额,所述汇出方账户包括采用承诺数额的汇出方收入余额和明文数额的汇出方支出余额,所述接收方账户包括采用承诺数额的接收方收入余额和明文数额的接收方支出余额;

执行所述有限公开转账交易,所述有限公开转账交易包含所述交易额对应的交易额承诺、扣款额、用于证明所述交易额非负且所述扣款额不小于所述交易额的区间证明,使得所述汇出方支出余额在交易完成后扣除所述扣款额、所述汇出方收入余额在交易完成后增加所述扣款额和所述交易额之间的差值、所述接收方收入余额在交易完成后增加所述交易额。

11. 根据权利要求10所述的方法,所述有限公开转账交易的发起条件还包括下述至少之一:

用户设定选用有限公开转账交易、所述有限公开转账交易被设定为优先选用且所述汇出方支出余额不小于所述交易额、所述汇出方账户对应的备选扣款额集合内的任一预定数值的备选扣款额不小于所述交易额。

12. 根据权利要求11所述的方法,所述汇出方账户包括采用承诺数额的汇出方主余额,所述接收方账户包括采用承诺数额的接收方主余额;所述方法还包括:

接收主余额转账交易,所述主余额转账交易在所述隐私类型设定信息为私密类型且所述主余额转账交易的发起条件被满足时由所述汇出方设备提交,所述主余额转账交易的发起条件包括下述至少之一:用户设定选用主余额转账交易、所述主余额转账交易被设定为优先选用且所述汇出方支出余额小于所述交易额、所述汇出方账户对应的备选扣款额集合内的若干预定数值的备选扣款额均小于所述交易额;

执行所述主余额转账交易,所述主余额转账交易包含所述交易额对应的交易额承诺和用于证明所述交易额非负且所述汇出方主余额不小于所述交易额的区间证明,使得所述汇出方主余额在交易完成后扣除所述交易额、所述接收方收入余额在交易完成后增加所述交

易额。

13. 根据权利要求10所述的方法,所述方法还包括:

接收公开转账交易,所述公开转账交易在所述隐私类型设定信息为非私密类型时由所述汇出方设备提交;

执行所述公开转账交易,所述公开转账交易包含所述交易额对应的公开交易额,使得所述汇出方支出余额在交易完成后扣除所述公开交易额、所述接收方支出余额在交易完成后增加所述公开交易额。

14. 根据权利要求10所述的方法,所述汇出方账户包括采用承诺数额的汇出方主余额,所述接收方账户包括采用承诺数额的接收方主余额;所述方法还包括:

接收由所述汇出方设备提交的充值交易,所述充值交易包含充值额和用于证明所述汇出方主余额不小于所述充值额的区间证明;

执行所述充值交易,以使得所述汇出方主余额在交易完成后扣除所述充值额、所述汇出方支出余额在交易完成后增加所述充值额。

15. 根据权利要求14所述的方法,还包括:

接收由所述汇出方设备提交的合并交易,所述合并交易包含合并额;

执行所述合并交易,以使得所述汇出方支出余额在交易完成后扣除所述合并额、所述汇出方主余额在交易完成后增加所述合并额,和/或所述汇出方收入余额在交易完成后清零、所述汇出方主余额在交易完成后增加所述收入余额。

16. 一种区块链交易装置,应用于汇出方设备,所述装置包括:

确定单元,确定将要从汇出方账户汇入接收方账户的交易额,所述汇出方账户包括采用承诺数额的汇出方收入余额和明文数额的汇出方支出余额,所述接收方账户包括采用承诺数额的接收方收入余额和明文数额的接收方支出余额;

提交单元,获取隐私类型设定信息;当有限公开转账交易的发起条件被满足时,向区块链提交所述有限公开转账交易,所述有限公开转账交易包含所述交易额对应的交易额承诺、扣款额、用于证明所述交易额非负且所述扣款额不小于所述交易额的区间证明,使得所述汇出方支出余额在交易完成后扣除所述扣款额、所述汇出方收入余额在交易完成后增加所述扣款额和所述交易额之间的差值、所述接收方收入余额在交易完成后增加所述交易额,所述有限公开转账交易的发起条件包括所述隐私类型设定信息为私密类型。

17. 一种电子设备,包括:

处理器;

用于存储处理器可执行指令的存储器;

其中,所述处理器通过运行所述可执行指令以实现如权利要求1-15中任一项所述的方法。

18. 一种计算机可读存储介质,其上存储有计算机指令,该指令被处理器执行时实现如权利要求1-15中任一项所述方法的步骤。

区块链交易方法及装置、电子设备、存储介质

技术领域

[0001] 本说明书一个或多个实施例涉及区块链技术领域,尤其涉及一种区块链交易方法及装置、电子设备、存储介质。

背景技术

[0002] 区块链可以通过在各个区块链节点之间达成共识,从而在各个区块链节点之间共同维护统一的区块链账本,以永久记载区块链网络中发生的交易信息。区块链账本是完全公开的,以便于随时查看和验证已发生交易的历史数据。

发明内容

[0003] 有鉴于此,本说明书一个或多个实施例提供一种区块链交易方法及装置、电子设备、存储介质。

[0004] 本说明书一个或多个实施例提供技术方案如下:

[0005] 根据本说明书一个或多个实施例的第一方面,提出了一种区块链交易方法,应用于汇出方设备,所述方法包括:

[0006] 确定将要从汇出方账户汇入接收方账户的交易额,所述汇出方账户包括采用承诺数额的汇出方主余额、采用承诺数额的汇出方收入余额和明文数额的汇出方支出余额,所述接收方账户包括采用承诺数额的接收方主余额、采用承诺数额的接收方收入余额和明文数额的接收方支出余额;

[0007] 向区块链提交公开转账交易,所述公开转账交易包含所述公开交易额对应的公开交易额,使得所述汇出方支出余额在交易完成后扣除所述公开交易额、所述接收方支出余额在交易完成后增加所述公开交易额。

[0008] 根据本说明书一个或多个实施例的第二方面,提出了一种区块链交易装置,应用于汇出方设备,所述装置包括:

[0009] 确定单元,确定将要从汇出方账户汇入接收方账户的交易额,所述汇出方账户包括采用承诺数额的汇出方主余额、采用承诺数额的汇出方收入余额和明文数额的汇出方支出余额,所述接收方账户包括采用承诺数额的接收方主余额、采用承诺数额的接收方收入余额和明文数额的接收方支出余额;

[0010] 提交单元,向区块链提交公开转账交易,所述公开转账交易包含所述公开交易额对应的公开交易额,使得所述汇出方支出余额在交易完成后扣除所述公开交易额、所述接收方支出余额在交易完成后增加所述公开交易额。

[0011] 根据本说明书一个或多个实施例的第三方面,提出了一种电子设备,包括:

[0012] 处理器;

[0013] 用于存储处理器可执行指令的存储器;

[0014] 其中,所述处理器通过运行所述可执行指令以实现如第一方面所述的方法。

[0015] 根据本说明书一个或多个实施例的第四方面,提出了一种计算机可读存储介质,

其上存储有计算机指令,该指令被处理器执行时实现如第一方面所述方法的步骤。

附图说明

- [0016] 图1是一示例性实施例提供的一种示例环境的示意图。
- [0017] 图2是一示例性实施例提供的一种概念架构的示意图。
- [0018] 图3是一示例性实施例提供的一种账户创建方法的流程图。
- [0019] 图4是一示例性实施例提供的一种区块链账户结构的示意图。
- [0020] 图5是一示例性实施例提供的一种区块链交易方法的流程图。
- [0021] 图6是一示例性实施例提供的一种基于支出余额实施的有限公开的汇款交易的流程图。
- [0022] 图7是一示例性实施例提供的一种汇款前后的账户余额变化情况的示意图。
- [0023] 图8是一示例性实施例提供的另一种区块链账户结构的示意图。
- [0024] 图9是一示例性实施例提供的一种主余额对支出余额进行充值的交互示意图。
- [0025] 图10是一示例性实施例提供的一种充值前后的账户余额变化情况的示意图。
- [0026] 图11是一示例性实施例提供的一种合并操作的交互示意图。
- [0027] 图12是一示例性实施例提供的一种合并前后的账户余额变化情况的示意图。
- [0028] 图13是一示例性实施例提供的另一种区块链交易方法的流程图。
- [0029] 图14是一示例性实施例提供的一种基于主余额实施的完全隐私的汇款交易的流程图。
- [0030] 图15是一示例性实施例提供的另一种汇款前后的账户余额变化情况的示意图。
- [0031] 图16是一示例性实施例提供的又一种区块链交易方法的流程图。
- [0032] 图17是一示例性实施例提供的一种基于支出余额实施的公开汇款交易的流程图。
- [0033] 图18是一示例性实施例提供的又一种汇款前后的账户余额变化情况的示意图。
- [0034] 图19是一示例性实施例提供的一种设备的结构示意图。
- [0035] 图20是一示例性实施例提供的一种区块链交易装置的框图。

具体实施方式

[0036] 这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[0037] 需要说明的是:在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中,其方法所包括的步骤可以比本说明书所描述的更多或更少。此外,本说明书中所描述的单个步骤,在其他实施例中可能被分解为多个步骤进行描述;而本说明书中所描述的多个步骤,在其他实施例中也可能被合并为单个步骤进行描述。

[0038] 图1是一示例性实施例提供的一种示例环境的示意图。如图1所示,示例环境100允许实体参与区块链网络102。区块链网络102可以为公有类型、私有类型或联盟类型的区块

链网络。示例环境100可以包括计算设备104、106、108、110、112和网络114；在一实施例中，网络114可以包括局域网(Local Area Network, LAN)、广域网(Wide Area Network, WAN)、因特网或其组合，并连接至网站、用户设备(例如计算设备)和后端系统。在一实施例中，可以通过有线和/或无线通信方式访问网络114。

[0039] 在某些情况下，计算设备106、108可以是云计算系统的节点(未显示)，或者每个计算设备106、108可以是单独的云计算系统，包括由网络互连并作为分布式处理系统工作的多台计算机。

[0040] 在一实施例中，计算设备104~108可以运行任何适当的计算系统，使其能够作为区块链网络102中的节点；例如，计算设备104~108可以包括但不限于服务器、台式计算机、笔记本电脑、平板电脑计算设备和智能手机。在一实施例中，计算设备104~108可以归属于相关实体并用于实现相应的服务，例如该服务可以用于对某一实体或多个实体之间的交易进行管理。

[0041] 在一实施例中，计算设备104~108分别存储有区块链网络102对应的区块链账本。计算设备104可以是(或包含)用于提供浏览器功能的网络服务器，该网络服务器可基于网络114提供与区块链网络102相关的可视化信息。在一些情况下，计算设备104可以不参与区块验证，而是监控区块链网络102以确定其他节点(譬如可以包括计算设备106-108)何时达成共识，并据此生成相应的区块链可视化用户界面。

[0042] 在一实施例中，计算设备104可接收客户端设备(例如计算设备110或计算设备112)针对区块链可视化用户界面发起的请求。在一些情况下，区块链网络102的节点也可以作为客户端设备，比如计算设备108的用户可以使用运行在计算设备108上的浏览器向计算设备104发送上述请求。

[0043] 响应于上述请求，计算设备104可以基于存储的区块链账本生成区块链可视化用户界面(如网页)，并将生成的区块链可视化用户界面发送给请求的客户端设备。如果区块链网络102是私有类型或联盟类型的区块链网络，对区块链可视化用户界面的请求可以包括用户授权信息，在生成区块链可视化用户界面并发送给请求的客户端设备之前，可以由计算设备104对该用户授权信息进行验证，并在验证通过后返回相应的区块链可视化用户界面。

[0044] 区块链可视化用户界面可以显示在客户端设备上(例如可显示在图1所示的用户界面116中)。当区块链账本发生更新时，用户界面116的显示内容也可以随之发生更新。此外，用户与用户界面116的交互可能导致对其他用户界面的请求，例如显示区块列表、区块详情、交易列表、交易详情、账户列表、账户详情、合约列表、合约详情或者用户对区块链网络实施搜索而产生的搜索结果页面等。

[0045] 图2是一示例性实施例提供的一种概念架构的示意图。如图2所示，该概念架构200包括实体层202、托管服务层204和区块链网络层206。例如，实体层202可以包括三个实体：实体1、实体2和实体3，每个实体都有各自的交易管理系统208。

[0046] 在一实施例中，托管服务层204可以包括每个事务管理系统208对应的接口210。例如，各个事务管理系统208使用协议(例如超文本传输协议安全(HTTPS)等)通过网络(例如图1中的网络114)与各自的接口210通信。在一些例子中，每个接口210可以提供各自对应的交易管理系统208与区块链网络层206之间的通信连接；更具体地，接口210可与区块链网络

层206的区块链网络212通信。在一些例子中,接口210和区块链网络层206之间的通信可以使用远程过程调用(Remote Procedure Calls,RPCs)而实现。在一些例子中,接口210可以向交易管理系统208提供用于访问区块链网络212的API接口。

[0047] 如本文所述,区块链网络212以对等网络的形式提供,该对等网络包括多个节点214,这些节点214分别用于对区块链数据所形成的区块链账本216进行持久化;其中,图2中仅示出了一份区块链账本216,但区块链网络212中可以存在多份区块链账本216或其副本,比如每一节点214可以分别维护一份区块链账本216或其副本。

[0048] 需要指出的是:在本说明书中所描述的交易(transaction),是指用户通过区块链的客户端创建,并需要最终发布至区块链的分布式数据库中的一笔数据。其中,区块链中的交易,存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移;例如,在传统的比特币区块链网络中,交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔具有业务意图的业务数据;例如,运营方可以基于实际的业务需求搭建一个联盟链,依托于联盟链部署一些与价值转移无关的其它类型的在线业务(比如,租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等),而在这类联盟链中,交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求。

[0049] 在本说明书的技术方案中,通过对区块链中的账户结构进行改进,可以实现新的账户交易形式,从而在保障交易隐私的前提下,实现账户模型下的并发交易,从而提升交易吞吐量。

[0050] 图3是一示例性实施例提供的一种账户创建方法的流程图。如图3所示,该方法应用于区块链节点,所述方法包括:

[0051] 步骤302,接收区块链交易,所述区块链交易的类型为账户创建类型。

[0052] 在一实施例中,用户可以在客户端生成区块链交易,并通过该客户端将区块链交易提交至区块链节点,以由区块链节点进行处理。

[0053] 在一实施例中,区块链交易包含若干字段。比如在以太坊区块链中,区块链交易通常可以包括from字段、to字段、data字段等,以分别表示交易发起方的账户地址、需调用的智能合约的合约地址、交易相关内容等。而在本说明书的技术方案,可以在区块链交易中设置一类型字段,该类型字段所含的内容用于表明相关区块链交易的类型,使得区块链节点可以据此实施对应的处理。例如,可以将区块链交易标注为账户创建类型,使得区块链节点可以据此创建新的账户。

[0054] 步骤304,执行所述区块链交易以创建第一账户,所述第一账户包括采用密文数额的收入余额和明文数额的支出余额。

[0055] 区块链网络中通常采用两种交易模型,即UTXO(Unspent Transaction Output,未花费的交易输出)模型和账户模型。UTXO模型的典型应用场景为比特币区块链,该模型下的链上资产以交易输出的形式存在,当一笔交易存在未花费的交易输出时,该未花费的交易输出归私钥持有者所有;在使用时,可以将一个或多个未花费的交易输出作为输入,并指定一个或多个输出,从而形成新的一笔或多笔未花费的交易输出。虽然UTXO模型被多种区块链网络所采用,但对智能合约的支持很弱,从而对应用场景造成了较大限制。而账户模型的典型应用场景为以太坊区块链,该模型下通过创建账户,将账户持有的链上资产表现为账

户地址对应的余额,每笔转账交易可以将资产从一个账户地址转移至另一个账户地址,且交易的金额直接更新至账户地址对应的余额。相比于UTXO模型而言,账户模型能够支持完备的智能合约功能,具有较好的场景扩展性。

[0056] 出于交易隐私保护的目,相关技术中提出了对区块链交易的改进。在UTXO模型下,可以通过同态加密或同态承诺技术对交易金额进行保护,以及利用区间证明技术保证交易的输出非负等。而在账户模型下,可以通过同态加密或同态承诺技术对交易金额进行保护,以及利用区间证明技术保证交易额非负且账户余额足够支付。

[0057] 在UTXO模型下,将一个或多个交易输出作为一笔转账交易的输入,并在转账完成后形成一个或多个新的交易输出。可见,一个交易输出只会在一笔转账交易中被花费,无法被多笔转账交易所花费,使得针对一笔转账交易生成的区间证明仅与该转账交易输入相关,与其他转账交易的输入无关,因而UTXO模型天然地具有高的交易并发性。而在账户模型下,每笔交易的输入均为账户的余额,每笔交易的区间证明都与账户的余额相关,而账户的余额在每笔交易后都会发生更新,使得同一账户下的所有交易需要按顺序串行执行,即一笔交易结束并导致账户的余额发生更新后,才能够针对下一笔交易生成区间证明、触发实施下一笔交易,否则交易会因区间证明不合法而被共识节点拒绝执行。因此,在账户模型下使用带有区间证明的隐私保护技术时,会严重地阻碍交易的吞吐量。

[0058] 为了解决账户模型下的并发性问题,确保对智能合约功能的充分支持,本说明书针对相关技术中的账户模型下的账户结构提出了改进,以使其能够适应于高吞吐量的并发交易。

[0059] 区块链网络中的账户可以包括外部账户和合约账户等。外部账户通常为用户(个人或机构)所有,而合约账户则对应于区块链中的智能合约。各类账户的结构都类似,例如如图4所示,可以包含Nonce字段、Balance字段、Code字段和Storage字段等。每个账户的Nonce字段的取值从0开始,且Nonce字段的取值随相应账户所发起的交易而依次递增,使得该账户发起的每一交易所含Nonce取值均不相同,从而避免重放攻击。Balance字段用于存放余额。Code字段用于存放智能合约的代码,因而外部账户的Code字段通常为空白。Storage字段用于存放账户在状态树中对应节点处的取值。

[0060] 在不考虑隐私保护的情况下,Balance字段的取值为账户持有的明文余额。在考虑隐私保护的情况下,可以通过诸如Pedersen承诺机制将明文余额生成为相应的密文承诺,使得区块链账本上仅记录该密文承诺、只有持有者能够对该密文承诺进行解密;但是,这种情况下由于区间证明的限制,使其存在上文所述的并发性不足的问题。而本说明书中针对Balance字段进行了结构改进,对Balance字段做了进一步划分,比如使得该Balance字段包含收入余额和支出余额,其中收入余额在区块链账本中记录为密文数额、支付余额在区块链账本中记录为明文数额。

[0061] 基于上述改进后的账户结构,当第一账户作为汇出方账户、用于向作为接收方账户的第二账户进行转账时,相关转账过程将结合图5进行介绍。图5是一示例性实施例提供的一种区块链交易方法的流程图。如图5所示,该方法应用于汇出方设备,所述方法包括:

[0062] 步骤502,根据将要从汇出方账户汇入接收方账户的有限公开交易额,确定对应的扣款额;其中,所述汇出方账户包括采用承诺数额的收入余额和明文数额的支出余额。

[0063] 在一实施例中,本说明书提供了有限公开类型的转账交易模式,该模式下可以通

过采用承诺数额的收入余额、明文数额的支出余额实施具有隐私保护的转账交易。

[0064] 在一实施例中,扣款额可以为任意不小于有限公开交易额的数值。例如,汇出方账户可以根据预先定义的每种类型的转账场景下的转账数额上限,分别设定针对各类转账场景的备选扣款额,形成备选扣款额集合。或者,也可以根据其他方式确定各个备选扣款额的取值,本说明书并不对此进行限制。然后,只需要选取一不小于有限公开交易额的扣款额即可。当然,也可以根据有限公开交易额的数值,临时生成一扣款额。扣款额的取值最好与有限公开交易额本身无关,否则当生成扣款额的算法被泄露后,可能导致不法分子根据扣款额的数值逆推出有限公开交易额的取值。

[0065] 步骤504,向区块链提交有限公开转账交易,所述有限公开转账交易包含所述有限公开交易额对应的有限公开交易额承诺、所述扣款额、用于证明所述交易额非负且所述扣款额不小于所述有限公开交易额的区间证明。

[0066] 在一实施例中,当所述有限公开转账交易完成后,可使所述支出余额在交易完成后扣除所述扣款额、所述收入余额在交易完成后增加所述扣款额并扣除所述有限公开交易额(即增加了找零额,该找零额的取值即扣款额与有限公开交易额之差)、所述接收方账户在交易完成后增加所述有限公开交易额。那么,在从支出余额扣除所述扣款额时,由于支出余额、扣款额均采用明文形式,使得不需要生成余额充足的区间证明(可以直接比对明文数额),从而在转账交易与汇出方账户的余额之间实现了解绑,使得账户模型下能够实现并发交易。同时,由于收入余额采用承诺数额的形式,因而向收入余额中增加的找零额也采用承诺数额进行记录,又由于有限公开交易额也表现为相应的承诺数额,因而整个交易过程中仅暴露了明文的扣款额、其余数额均表现为密文形式的承诺数额,所以能够在实现并发交易的同时,确保足够的隐私保护。

[0067] 在一实施例中,当接收方账户在交易完成后增加所述有限公开交易额时,如果接收方账户采用本说明书的账户结构,那么该有限公开交易额可以增加至接收方账户的收入余额中。具体的,由于接收方账户的收入余额采用承诺数额的形式,因此有限公开交易额同样会以相应的承诺数额的形式被增加至接收方账户的收入余额中。类似地,当所述汇出方账户的汇出方余额增大时,譬如某一账户向该汇出方账户进行转账时,相应的金额被增加至该汇出方账户的收入余额。

[0068] 可见,通过在账户结构中分别设置承诺数额的收入余额和明文数额的支出余额,不仅可以在保证交易隐私性的同时,实现账户模型下的并发交易,而且可以将同一账户所参与的汇出交易与汇入交易之间的解耦,确保汇出方账户能够同时参与汇出交易和汇入交易,能够提升交易吞吐量。

[0069] 下面以作为汇出方的用户A、作为接收方的用户B为例,对有限公开交易的实施过程进行描述。图6是一示例性实施例提供的一种基于支出余额实施的有限公开的汇款交易的流程图;如图6所示,汇出方、接收方和区块链节点之间的交互过程可以包括以下步骤:

[0070] 步骤601,汇出方确定转账金额 t 。

[0071] 在一实施例中,汇出方是指汇款交易中对款项等资源进行汇出的角色,相应地接收方是指汇款交易中对款项等资源进行接收的角色。例如,用户A使用的用户设备可以被配置为汇出方,而用户B使用的用户设备可以被配置为接收方。

[0072] 在一实施例中,在起草汇款交易时,汇款额 t 可由汇出方与接收方之间进行协商。

当然,汇出方也可以自行确定汇款额 t ,由接收方在后续步骤中予以确认。

[0073] 步骤602,汇出方确定汇款额 t 对应的随机数 r 。

[0074] 在一实施例中,汇出方可以基于Pedersen承诺机制为该汇款额 t 产生随机数 r ,则汇款额 t 对应的汇款承诺 $T=PC(t,r)$,其中 $PC()$ 为预设算法。

[0075] 步骤603,汇出方通过链下通道将 (r,t,T) 发送至接收方。

[0076] 在一实施例中,通过将 (r,t,T) 由链下通道而非区块链网络进行发送,可以避免汇款随机数 r 和汇款额 t 被记录至区块链账本中,确保汇款额 t 除汇出方和接收方之外不可知。

[0077] 步骤604,接收方对收到的 (r,t,T) 进行验证。

[0078] 在一实施例中,接收方可以对汇款额 t 进行验证,以确定为希望收取的汇款数额。

[0079] 在一实施例中,接收方可以对汇款承诺 T 进行验证,即接收方可以通过Pedersen承诺机制对随机数 r 和汇款额 t 进行计算,以验证汇款承诺 $T=PC(t,r)$ 是否正确,若正确则表明验证通过,否则验证不通过。

[0080] 步骤605,接收方在验证通过后,生成签名并返回至汇出方。

[0081] 在一实施例中,在验证通过后,接收方可以利用接收方私钥对 $(A,B:T)$ 进行签名,生成签名 $SigB$ 并返回至汇出方。该签名 $SigB$ 表明接收方同意由用户A的区块链账户1向用户B的区块链账户2实施承诺为 T 的汇款交易。

[0082] 步骤606,在收到签名 $SigB$ 后,汇出方根据扣款额 L 生成区间证明 PR 。

[0083] 在一实施例中,扣款额 L 由汇出方根据转账金额 t 确定得到。例如,汇出方可以预先维护有若干扣款额 $L_1\sim L_n$,而汇出方可以随意选取一扣款额 L ,只要确保 $t\leq L\leq w$ 即可,其中 w 为用户A的区块链账户1中的支出余额的取值。

[0084] 在一实施例中,汇出方可以在生成区间证明 PR 之前的任意时刻确定出扣款额 L ,本说明书并不对此进行限制。

[0085] 在一实施例中,为了确保汇款交易顺利完成,区块链节点需要确定汇款额 t 、扣款额 L 满足下述条件: $0\leq t\leq L$;而区间证明技术可以使得区块链节点在密文状态下验证交易是否符合预设条件,譬如本说明书中可以采用相关技术中的Bulletproofs方案、Borromean环签名方案等实现,本说明书并不对此进行限制。汇出方可以利用区间证明技术生成区间证明 PR ,以供后续过程中由区块链节点进行验证是否满足 $0\leq t\leq L$ 。

[0086] 步骤607,汇出方对交易内容 $(A,B:T,L,PR;SigB)$ 进行签名,生成签名 $SigA$ 。

[0087] 在一实施例中,该汇出方可以利用汇出方私钥对交易内容 $(A,B:T,L,PR;SigB)$ 进行签名,生成签名 $SigA$ 。

[0088] 步骤608,汇出方向区块链提交交易。

[0089] 在一实施例中,汇出方被配置为区块链的客户端,可以将汇款交易提交至区块链网络中的某一区块链节点,并进而被传输至区块链网络中的所有区块链节点,并由各个区块链节点分别对该汇款交易进行验证,以在验证通过时执行汇款操作、在验证未通过时拒绝汇款。

[0090] 步骤609,区块链节点检查交易是否执行过。

[0091] 在一实施例中,此处的区块链节点可以表示区块链网络中的任意一个区块链节点,即区块链网络中的每一区块链节点均会收到上述汇款交易,并通过步骤609~612等实施验证等操作。

[0092] 在一实施例中,区块链节点在收到上述汇款交易后,可以利用相关技术中的防双花或防重放机制,验证该汇款交易是否已经执行过;如果已经执行过,可以拒绝执行该汇款交易,否则转入步骤610。

[0093] 步骤610,区块链节点检查签名。

[0094] 在一实施例中,区块链节点可以检查该汇款交易中包含的签名SigA、SigB是否正确;如果不正确,可以拒绝执行该汇款交易,否则转入步骤611。

[0095] 步骤611,区块链节点检查区间证明PR。

[0096] 在一实施例中,区块链节点可以基于区间证明技术对该汇款交易包含的区间证明PR进行检查,以确定是否满足 $0 \leq t \leq L$ 。如果不满足,可以拒绝执行该汇款交易,否则转入步骤612。

[0097] 步骤612,区块链节点检查支出余额是否充足。

[0098] 在一实施例中,由于区块链账户1的支出余额 w 以明文形式被记录于区块链账本中,使得区块链节点可以直接读取区块链账户1的支出余额 w ,并将该支出余额 w 与扣款额 L 进行比较,从而在 $w \geq L$ 时确定支出余额充足。

[0099] 因此,汇出方在步骤606中只需要针对交易额 t 和扣款额 L 生成上述的区间证明PR,而不需要针对扣款额 L 和支出余额 w 生成相应的区间证明,这样既可以省去区间证明的生成过程、提升交易的生成效率,又可以省去区间证明的验证过程、提升交易的执行效率。

[0100] 步骤613,区块链节点在维护的区块链账本中更新用户A、用户B分别对应的区块链账户。

[0101] 在一实施例中,在通过步骤609~612的验证后,区块链节点可以分别对区块链账本中记载的区块链账户1、区块链账户2进行更新,如图7所示:

[0102] 在用户A的区块链账户1中,交易前的收入余额为 v 、在区块链账本中被记录为相应的承诺数额 $PC(v, y)$,交易前的支出余额为 w 、在区块链账本中被记录为明文数额 w 。在交易完成后,支出余额被扣除了上述的扣款额 L ,因而在区块链账本中被记录为明文数额 $w-L$,而收入余额则增加了找零额、即扣款额 L 与汇款额 t 之差,因而在区块链账本中被记录为相应的承诺数额 $PC(v, y) + PC(L, 0) - PC(t, r)$,其中 $PC(L, 0)$ 为扣款额 L 对应的承诺值(预先约定采用的随机数为0;当然,也可以采用约定的其他数值)。

[0103] 在用户B的区块链账户2中,交易前的收入余额为 v' 、在区块链账本中被记录为相应的承诺数额 $PC(v', y')$,交易前的支出余额为 w' 、在区块链账本中被记录为明文数额 w' 。在交易完成后,支出余额 w' 不变,而收入余额则增加了汇款额 t ,因而在区块链账本中被记录为相应的承诺数额 $PC(v', y') + PC(t, r)$ 。

[0104] 如上文所述,当账户包含上述的收入余额和支出余额时,可以在保障交易隐私的情况下,实现账户模型下的高并发转账。但是,由于汇入账户的资金都记入收入余额、而汇出的资金都从支出余额中扣除,因而支出余额的数额在不断下降。为了确保支出余额的数额总是能够处于充足状态、足够完成交易,可以定期或随时向支出余额中进行充值。

[0105] 虽然可以从收入余额向支出余额进行充值,但是:由于支出余额本身是以明文形式而存在,实际上是在有限程度上暴露了部分隐私(表明相关账户中的余额不少于支出余额的数值),因而用户往往不希望使支出余额的数额过高,以控制和限制对隐私的暴露范围。那么,当账户向外汇出的交易较为频繁、交易额较大时,需要向支出余额频繁充值,导致

收入余额频繁参与资金的汇入与汇出(充值),甚至使得汇入交易与充值交易之间相应影响,反而造成效率下降。

[0106] 因此,本说明书针对图4所示的账户结构提出了进一步改进。例如图8所示,可以在Balance字段中进一步增加一主余额,使得Balance字段总共包含三个余额:主余额、收入余额和支出余额。其中,收入余额专用于收取汇入交易的交易额、支出余额专用于参与汇出交易,而主余额用于对支出余额进行充值,从而避免由收入余额承担充值任务,防止产生上文所述的影响。

[0107] 图9是一示例性实施例提供的一种主余额对支出余额进行充值的交互示意图。如图9所示,该交互过程可以包括以下步骤:

[0108] 步骤901,汇出方确定充值金额 m 。

[0109] 在一实施例中,充值金额 m 可以为任意金额,只要汇出方的主余额的数额充足即可。例如,可以为支出余额设置一最高水位,而充值金额 m 可以为最高水位与支出余额的剩余数值之差。

[0110] 步骤902,汇出方生成区间证明RF。

[0111] 在一实施例中,由于主余额的取值 u 在区块链账本中记录为相应的承诺数额 $PC(u, x)$,其中 x 为 u 对应的随机数,因而需要通过生成区间证明RF,以用于验证主余额的取值 $u \geq m$ 。

[0112] 步骤903,汇出方对交易 $Topup(A:m, RF)$ 签名后,提交至区块链。

[0113] 在一实施例中,以上述用户A的区块链账户1为例,上述交易中的“A”代表该区块链账户1的账户地址,表明需要对该区块链账户1的支出余额进行充值、充值金额为 m 。

[0114] 在一实施例中,交易中可以增加一类型字段,而汇出方在创建每一交易时,可以通过对类型字段进行赋值,以标注所提交的交易的类型,从而对本说明书中所涉及的有限公开转账交易、充值交易以及下文所述的合并交易、主余额转账交易、公开转账交易等进行区分。例如,在图6所示的实施例中,可以通过取值“Transfer”来标注有限公开转账交易,而此处可以通过取值“Topup”来标注充值交易。

[0115] 步骤904,区块链节点验证交易。

[0116] 在一实施例中,区块链节点可以验证该交易 $Topup(A:m, RF)$ 的签名是否正确;如果不正确,可以拒绝执行该交易。

[0117] 在一实施例中,区块链节点可以验证该交易 $Topup(A:m, RF)$ 的充值金额 m 是否满足 $m \geq 0$;如果不正确,可以拒绝执行该交易。

[0118] 在一实施例中,区块链节点可以验证该交易 $Topup(A:m, RF)$ 所含的区间证明RF,以确定是否满足 $0 \leq m \leq u$;如果不正确,可以拒绝执行该交易。

[0119] 当所有验证均通过后,可以转入步骤905。

[0120] 步骤905,区块链节点更新账户。

[0121] 在一实施例中,在通过步骤904的验证后,区块链节点可以对区块链账本中记载的区块链账户1进行更新,如图10所示:

[0122] 在用户A的区块链账户1中,交易前的主余额为 u 、在区块链账本中被记录为相应的承诺数额 $PC(u, x)$,交易前的收入余额为 v 、在区块链账本中被记录为相应的承诺数额 $PC(v, y)$,交易前的支出余额为 w 、在区块链账本中被记录为明文数额 w 。

[0123] 在交易完成后,主余额被扣除了上述的充值数额 m ,因而在区块链账本中被记录为相应的承诺数额 $PC(u, x) - PC(m, 0)$,而支出余额 w 增加了充值数额 m ,因而在区块链账本中被记录为明文数额 $w+m$;同时,收入余额的取值不变。

[0124] 随着账户中的支出余额不断参与汇出交易,而主余额不断向支出余额进行充值,会导致主余额逐步减少;当主余额减少至一定程度或减少至0时,将无法继续维持支出余额参与汇出交易,因而可以将收入余额中获得的资金转入主余额中,以便于维持账户不断地参与汇出交易。

[0125] 图11是一示例性实施例提供的一种合并操作的交互示意图。如图11所示,该交互过程可以包括以下步骤:

[0126] 步骤1101,汇出方确定提取金额 n 。

[0127] 在一实施例中,合并操作用于将账户中的收入余额的全部资金、支出余额的指定资金转入主余额,该指定资金的数额可由上述的提取金额 n 来指定。如果提取金额 n 为0,相当于仅将收入金额的资金转入主余额,或者可以将 n 设定为其他任意数值,本说明书并不对此进行限制。

[0128] 步骤1102,汇出方对交易Merge (A:n) 签名后,提交至区块链。

[0129] 在一实施例中,以上述用户A的区块链账户1为例,上述交易中的“A”代表该区块链账户1的账户地址,表明需要对该区块链账户1实施合并操作,具体将收入余额全部转入主余额、将支出余额中的资金 n 转入主余额。而Merge表明当前的交易类型为合并交易,以用于针对区块链账户1实施合并操作。

[0130] 在一实施例中,由于将收入余额全部转入主余额、而非部分转入,因而无需针对收入余额的部分生成区间证明;而提取金额 n 和支出余额均为明文,也不需要生成区间证明。

[0131] 步骤1103,区块链节点验证交易。

[0132] 在一实施例中,区块链节点可以验证该交易Merge (A:n) 的签名是否正确;如果不正确,可以拒绝执行该交易。

[0133] 在一实施例中,区块链节点可以验证该交易Merge (A:n) 的提取金额 n 是否满足 $1 \leq n \leq w$, w 为支出余额的取值;如果不正确,可以拒绝执行该交易。

[0134] 当所有验证均通过后,可以转入步骤1104。

[0135] 步骤1104,区块链节点更新账户。

[0136] 在一实施例中,在通过步骤1103的验证后,区块链节点可以对区块链账本中记载的区块链账户1进行更新,如图12所示:

[0137] 在用户A的区块链账户1中,交易前的主余额为 u 、在区块链账本中被记录为相应的承诺数额 $PC(u, x)$,交易前的收入余额为 v 、在区块链账本中被记录为相应的承诺数额 $PC(v, y)$,交易前的支出余额为 w 、在区块链账本中被记录为明文数额 w 。

[0138] 在交易完成后,收入余额变为0;主余额增加了收入余额的全部资金和上述的提取金额 n ,因而在区块链账本中被记录为相应的承诺数额 $PC(u, x) + PC(v, y) + PC(n, 0)$,而支出余额 w 减少了提取金额 n ,因而在区块链账本中被记录为明文数额 $w-n$ 。

[0139] 虽然在本说明书提供的实施例中,针对账户所含的主余额、收入余额、支出余额,可以通过由支出余额参与汇出交易、收入余额参与汇入交易(收入余额也在汇出交易中收取找零额)、主余额参与上述的充值交易和合并交易,但是并不意味着每一余额仅能够参与

上述类型的交易。例如,本说明书的账户结构,还可以兼容:由主余额参与汇出资金的主余额转账交易、由支出余额参与公开转账交易等,下文分别予以介绍。

[0140] 图13是一示例性实施例提供的另一种区块链交易方法的流程图。如图13所示,该方法应用于汇出方设备,所述方法包括:

[0141] 步骤1302,确定将从汇出方账户汇入接收方账户的交易额,所述汇出方账户包括采用承诺数额的汇出方主余额、采用承诺数额的汇出方收入余额和明文数额的汇出方支出余额,所述接收方账户包括采用承诺数额的接收方主余额、采用承诺数额的接收方收入余额和明文数额的接收方支出余额。

[0142] 在一实施例中,汇出方账户、接收方账户均采用如图8所示的账户结构,分别为汇出方账户中的汇出方主余额、汇出方收入余额和汇出方支出余额,接收方账户中的接收方主余额、接收方收入余额和接收方支出余额。

[0143] 步骤1304,向区块链提交主余额转账交易,所述主余额转账交易包含所述交易额对应的交易额承诺和用于证明所述交易额非负且所述汇出方主余额不小于所述交易额的区间证明,使得所述汇出方主余额在交易完成后扣除所述交易额、所述接收方收入余额在交易完成后增加所述交易额。

[0144] 在一实施例中,由于汇出方主余额、接收方收入余额均在区块链账本中以承诺数额的形式予以记录,因而通过上述的主余额转账交易,可以保证交易过程中不会发生数据泄露,从而确保数据的隐私安全。

[0145] 在一实施例中,汇出方可以将交易额与上文所述的备选扣款额集合包含的备选扣款额进行比较;如果所有备选扣款额均小于交易额,则汇出方创建并提交上述的主余额转账交易,如果存在不小于交易额的任一备选扣款项,则汇出方可以创建并提交有限公开转账交易,从而通过如图5所示的实施例,由汇出方支出余额和汇出方汇入余额参与实施有限公开类型的转账操作,有助于实现高并发性。

[0146] 在一实施例中,汇出方可以根据用户的设定操作,确定选用上述的主余额转账交易、有限公开转账交易或其他类型的转账交易。

[0147] 在一实施例中,由于汇出方主余额与汇出方支出余额属于相互独立的两部分,因而汇出方甚至可以同时通过汇出方主余额与汇出方支出余额分别发起不同的交易。例如,可以通过汇出方支出余额参与数额较小的有限公开转账交易,而通过汇出方主余额参与数额较大的主余额转账交易,以提升交易效率。

[0148] 下面以作为汇出方的用户A、作为接收方的用户B为例,对有限公开交易的实施过程进行描述。图14是一示例性实施例提供的一种基于主余额实施的完全隐私的汇款交易的流程图;如图14所示,汇出方、接收方和区块链节点之间的交互过程可以包括以下步骤:

[0149] 步骤1401,汇出方确定转账金额 t 。

[0150] 在一实施例中,汇出方是指汇款交易中对款项等资源进行汇出的角色,相应地接收方是指汇款交易中对款项等资源进行接收的角色。例如,用户A使用的用户设备可以被配置为汇出方,而用户B使用的用户设备可以被配置为接收方。

[0151] 在一实施例中,在起草汇款交易时,汇款额 t 可由汇出方与接收方之间进行协商。当然,汇出方也可以自行确定汇款额 t ,由接收方在后续步骤中予以确认。

[0152] 步骤1402,汇出方确定汇款额 t 对应的随机数 r 。

[0153] 在一实施例中,汇出方可以基于Pedersen承诺机制为该汇款额 t 产生随机数 r ,则汇款额 t 对应的汇款承诺 $T=PC(t,r)$,其中 $PC()$ 为预设算法。

[0154] 步骤1403,汇出方通过链下通道将 (r,t,T) 发送至接收方。

[0155] 在一实施例中,通过将 (r,t,T) 由链下通道而非区块链网络进行发送,可以避免汇款随机数 r 和汇款额 t 被记录至区块链账本中,确保汇款额 t 除汇出方和接收方之外不可知。

[0156] 步骤1404,接收方对收到的 (r,t,T) 进行验证。

[0157] 在一实施例中,接收方可以对汇款额 t 进行验证,以确定为希望收取的汇款数额。

[0158] 在一实施例中,接收方可以对汇款承诺 T 进行验证,即接收方可以通过Pedersen承诺机制对随机数 r 和汇款额 t 进行计算,以验证汇款承诺 $T=PC(t,r)$ 是否正确,若正确则表明验证通过,否则验证不通过。

[0159] 步骤1405,接收方在验证通过后,生成签名并返回至汇出方。

[0160] 在一实施例中,在验证通过后,接收方可以利用接收方私钥对 $(A,B:T)$ 进行签名,生成签名 $SigB$ 并返回至汇出方。该签名 $SigB$ 表明接收方同意由用户A的区块链账户1向用户B的区块链账户2实施承诺为 T 的汇款交易。

[0161] 步骤1406,在收到签名 $SigB$ 后,汇出方根据主余额 u 生成区间证明 RP 。

[0162] 在一实施例中,为了确保汇款交易顺利完成,区块链节点需要确定汇款额 t 、主余额 u 满足下述条件: $0 \leq t \leq u$;而区间证明技术可以使得区块链节点在密文状态下验证交易是否符合预设条件,譬如本说明书中可以采用相关技术中的Bulletproofs方案、Borromean环签名方案等实现,本说明书并不对此进行限制。汇出方可以利用区间证明技术生成区间证明 RP ,以供后续过程中由区块链节点进行验证是否满足 $0 \leq t \leq u$ 。

[0163] 步骤1407,汇出方对交易内容 $PrimaryTransfer(A,B:T,RP;SigB)$ 进行签名,生成签名 $SigA$ 。

[0164] 在一实施例中,该汇出方可以利用汇出方私钥对交易内容 $PrimaryTransfer(A,B:T,RP;SigB)$ 进行签名,生成签名 $SigA$ 。

[0165] 其中, $PrimaryTransfer$ 用于表明交易类型为主余额转账交易(或称为,主余额汇款交易)。

[0166] 步骤1408,汇出方向区块链提交交易。

[0167] 在一实施例中,汇出方被配置为区块链的客户端,可以将汇款交易提交至区块链网络中的某一区块链节点,并进而被传输至区块链网络中的所有区块链节点,并由各个区块链节点分别对该汇款交易进行验证,以在验证通过时执行汇款操作、在验证未通过时拒绝汇款。

[0168] 步骤1409,区块链节点检查交易是否执行过。

[0169] 在一实施例中,此处的区块链节点可以表示区块链网络中的任意一个区块链节点,即区块链网络中的每一区块链节点均会收到上述汇款交易,并通过步骤1409~1411等实施验证等操作。

[0170] 在一实施例中,区块链节点在收到上述汇款交易后,可以利用相关技术中的防双花或防重放机制,验证该汇款交易是否已经执行过;如果已经执行过,可以拒绝执行该汇款交易,否则转入步骤1410。

[0171] 步骤1410,区块链节点检查签名。

[0172] 在一实施例中,区块链节点可以检查该汇款交易中包含的签名SigA、SigB是否正确;如果不正确,可以拒绝执行该汇款交易,否则转入步骤1411。

[0173] 步骤1411,区块链节点检查区间证明RP。

[0174] 在一实施例中,区块链节点可以基于区间证明技术对该汇款交易包含的区间证明RP进行检查,以确定是否满足 $0 \leq t \leq u$ 。如果不满足,可以拒绝执行该汇款交易,否则转入步骤1412。

[0175] 步骤1412,区块链节点在维护的区块链账本中更新用户A、用户B分别对应的区块链账户。

[0176] 在一实施例中,在通过步骤1409~1411的验证后,区块链节点可以分别对区块链账本中记载的区块链账户1、区块链账户2进行更新,如图15所示:

[0177] 在用户A的区块链账户1中,交易前的主余额为 u 、在区块链账本中被记录为相应的承诺数额 $PC(u, x)$,交易前的收入余额为 v 、在区块链账本中被记录为相应的承诺数额 $PC(v, y)$,交易前的支出余额为 w 、在区块链账本中被记录为明文数额 w 。在交易完成后,主余额被扣除了上述的交易额 t ,因而在区块链账本中被记录为相应的承诺数额 $PC(u, x) - PC(t, r)$,而收入余额 v 、支出余额 w 不变。

[0178] 在用户B的区块链账户2中,交易前的主余额为 u' 、在区块链账本中被记录为相应的承诺数额 $PC(u', x')$,交易前的收入余额为 v' 、在区块链账本中被记录为相应的承诺数额 $PC(v', y')$,交易前的支出余额为 w' 、在区块链账本中被记录为明文数额 w' 。在交易完成后,主余额为 u' 、支出余额 w' 不变,而收入余额则增加了汇款额 t ,因而在区块链账本中被记录为相应的承诺数额 $PC(v', y') + PC(t, r)$ 。

[0179] 图16是一示例性实施例提供的又一种区块链交易方法的流程图。如图16所示,该方法应用于汇出方设备,所述方法包括:

[0180] 步骤1602,确定将从汇出方账户汇入接收方账户的交易额,所述汇出方账户包括采用承诺数额的汇出方主余额、采用承诺数额的汇出方收入余额和明文数额的汇出方支出余额,所述接收方账户包括采用承诺数额的接收方主余额、采用承诺数额的接收方收入余额和明文数额的接收方支出余额。

[0181] 在一实施例中,汇出方账户、接收方账户均采用如图8所示的账户结构,分别为汇出方账户中的汇出方主余额、汇出方收入余额和汇出方支出余额,接收方账户中的接收方主余额、接收方收入余额和接收方支出余额。

[0182] 步骤1604,向区块链提交公开转账交易,所述公开转账交易包含所述公开交易额对应的公开交易额,使得所述汇出方支出余额在交易完成后扣除所述公开交易额、所述接收方支出余额在交易完成后增加所述公开交易额。

[0183] 在一实施例中,在将汇出方支出余额的取值记录为明文数值时,可以通过牺牲这一明文数值来换取转账交易的高并发性。当汇出方接收上述设定时,表明汇出方在隐私保护与交易效率之间,允许通过牺牲部分隐私来换取更高的交易效率,因而在一些场景中,比如对于部分独立的、金额较小的转账而言,可以通过提交上述的公开转账交易,直接在汇出方支出余额与接收方支出余额之间实施转账,这一过程类似于相关技术中未实施隐私保护场景下的转账操作,由于不需要实施加密、生成区间证明、验证区间证明等多种复杂的处理操作,能够极大地提升交易效率。

[0184] 在一实施例中,可以获取隐私类型设定信息,该隐私类型设定信息可由用户根据实际需求进行临时设定,或设定为长期生效。当所述隐私类型设定信息为非私密类型时,表明用户相对更加看重交易效率,因而可以基于上文向区块链提交所述公开转账交易。而当隐私类型设定信息为私密类型时,表明用户相对更加看重隐私,因而可以基于图5或图13所示的实施例,向区块链提交有限公开转账交易或主余额转账交易。

[0185] 其中,对于私密类型的场景下,用户可以进一步设定选用有限公开转账交易或主余额转账交易;或者如上文所述,可以优先选用有限公开转账交易,而在汇出方支出余额小于交易额时,选用主余额转账交易,这里可以参考图13所示的实施例,此次不再赘述。

[0186] 下面以作为汇出方的用户A、作为接收方的用户B为例,对有限公开交易的实施过程进行描述。图17是一示例性实施例提供的一种基于支出余额实施的公开汇款交易的流程图;如图17所示,汇出方、接收方和区块链节点之间的交互过程可以包括以下步骤:

[0187] 步骤1701,汇出方确定转账金额 t 。

[0188] 在一实施例中,汇出方是指汇款交易中对款项等资源进行汇出的角色,相应地接收方是指汇款交易中对款项等资源进行接收的角色。例如,用户A使用的用户设备可以被配置为汇出方,而用户B使用的用户设备可以被配置为接收方。

[0189] 在一实施例中,在起草汇款交易时,汇款额 t 可由汇出方与接收方之间进行协商。当然,汇出方也可以自行确定汇款额 t 。

[0190] 步骤1702,汇出方对交易内容OpenTransfer(A,B: t)进行签名,生成签名SigA,并提交交易。

[0191] 在一实施例中,该汇出方可以利用汇出方私钥对交易内容OpenTransfer(A,B: t)进行签名,生成签名SigA。

[0192] 其中,OpenTransfer用于表明交易类型为公开转账交易(或称为,公开汇款交易)。

[0193] 步骤1703,区块链节点验证交易。

[0194] 在一实施例中,区块链节点在收到上述汇款交易后,可以利用相关技术中的防双花或防重放机制,验证该汇款交易是否已经执行过;如果已经执行过,可以拒绝执行该汇款交易,否则转入步骤1704。

[0195] 在一实施例中,区块链节点可以检查该汇款交易中包含的签名SigA是否正确;如果不正确,可以拒绝执行该汇款交易,否则转入步骤1704。

[0196] 步骤1704,区块链节点在维护的区块链账本中更新用户A、用户B分别对应的区块链账户。

[0197] 在一实施例中,在通过步骤1703的验证后,区块链节点可以分别对区块链账本中记载的区块链账户1、区块链账户2进行更新,如图18所示:

[0198] 在用户A的区块链账户1中,交易前的主余额为 u 、在区块链账本中被记录为相应的承诺数额PC(u, x),交易前的收入余额为 v 、在区块链账本中被记录为相应的承诺数额PC(v, y),交易前的支出余额为 w 、在区块链账本中被记录为明文数额 w 。在交易完成后,支出余额 w 被扣除了上述的交易额 t ,因而在区块链账本中被记录为相应的明文数额 $w-t$,而收入余额 v 、主余额 u 不变。

[0199] 在用户B的区块链账户2中,交易前的主余额为 u' 、在区块链账本中被记录为相应的承诺数额PC(u', x'),交易前的收入余额为 v' 、在区块链账本中被记录为相应的承诺数额

PC (v' , y'), 交易前的支出余额为 w' 、在区块链账本中被记录为明文数额 w' 。在交易完成后, 主余额为 u' 、收入余额为 v' 不变, 而支出余额 w' 则增加了汇款额 t , 因而在区块链账本中被记录为相应的明文数额 $w' + t$ 。

[0200] 图19是一示例性实施例提供的一种设备的示意结构图。请参考图19, 在硬件层面, 该设备包括处理器1902、内部总线1904、网络接口1906、内存1908以及非易失性存储器1910, 当然还可能包括其他业务所需要的硬件。处理器1902从非易失性存储器1910中读取对应的计算机程序到内存1908中然后运行, 在逻辑层面上形成区块链交易装置。当然, 除了软件实现方式之外, 本说明书一个或多个实施例并不排除其他实现方式, 比如逻辑器件抑或软硬件结合的方式等等, 也就是说以下处理流程的执行主体并不限于各个逻辑单元, 也可以是硬件或逻辑器件。

[0201] 请参考图20, 在软件实施方式中, 该区块链交易装置可以包括:

[0202] 确定单元2001, 确定将要从汇出方账户汇入接收方账户的交易额, 所述汇出方账户包括采用承诺数额的汇出方主余额、采用承诺数额的汇出方收入余额和明文数额的汇出方支出余额, 所述接收方账户包括采用承诺数额的接收方主余额、采用承诺数额的接收方收入余额和明文数额的接收方支出余额;

[0203] 提交单元2002, 向区块链提交公开转账交易, 所述公开转账交易包含所述公开交易额对应的公开交易额, 使得所述汇出方支出余额在交易完成后扣除所述公开交易额、所述接收方支出余额在交易完成后增加所述公开交易额。

[0204] 上述实施例阐明的系统、装置、模块或单元, 具体可以由计算机芯片或实体实现, 或者由具有某种功能的产品来实现。一种典型的实现设备为计算机, 计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0205] 在一个典型的配置中, 计算机包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

[0206] 内存可能包括计算机可读介质中的非永久性存储器, 随机存取存储器 (RAM) 和/或非易失性内存等形式, 如只读存储器 (ROM) 或闪存 (flash RAM)。内存是计算机可读介质的示例。

[0207] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括, 但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带、磁盘存储、量子存储器、基于石墨烯的存储介质或其他磁性存储设备或任何其他非传输介质, 可用于存储可以被计算设备访问的信息。按照本文中的界定, 计算机可读介质不包括暂存电脑可读媒体 (transitory media), 如调制的数据信号和载波。

[0208] 还需要说明的是, 术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含, 从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素, 而且还包

括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0209] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下,在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外,在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中,多任务处理和并行处理也是可以的或者可能是有利的。

[0210] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0211] 应当理解,尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息,但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如,在不脱离本说明书一个或多个实施例范围的情况下,第一信息也可以被称为第二信息,类似地,第二信息也可以被称为第一信息。取决于语境,如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0212] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已,并不用以限制本说明书一个或多个实施例,凡在本说明书一个或多个实施例的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本说明书一个或多个实施例保护的范围之内。

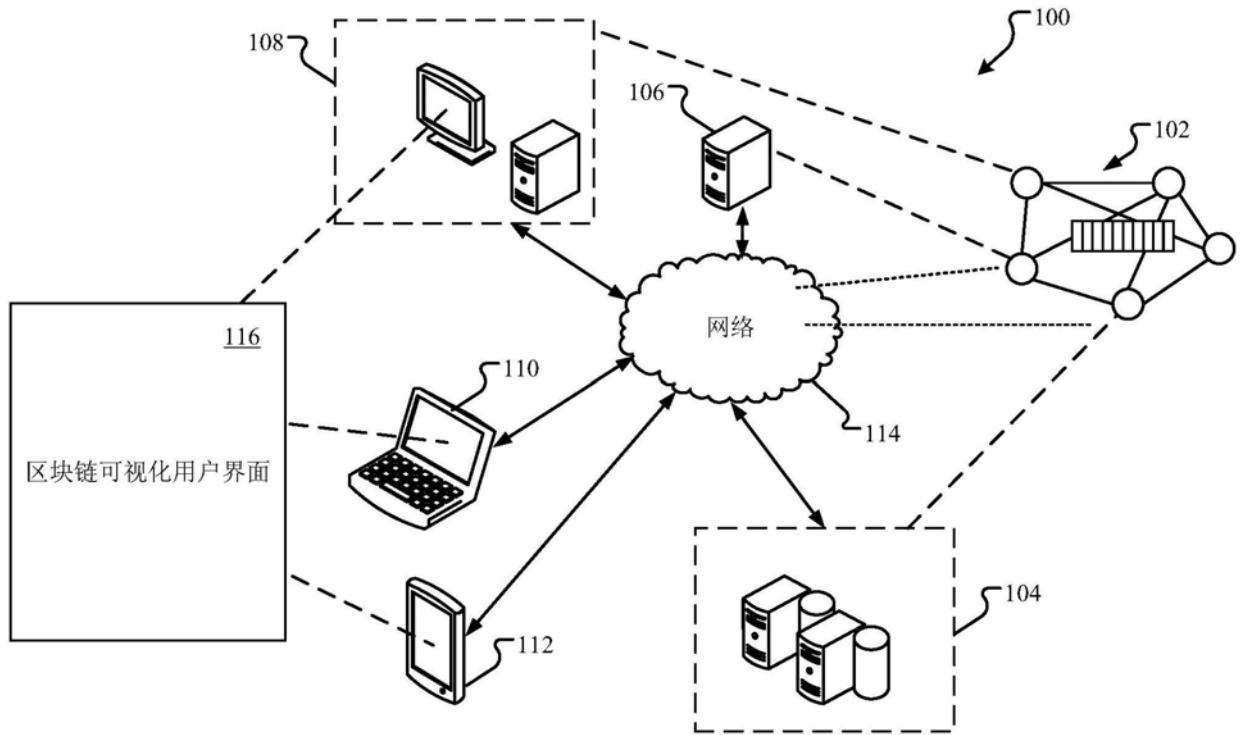


图1

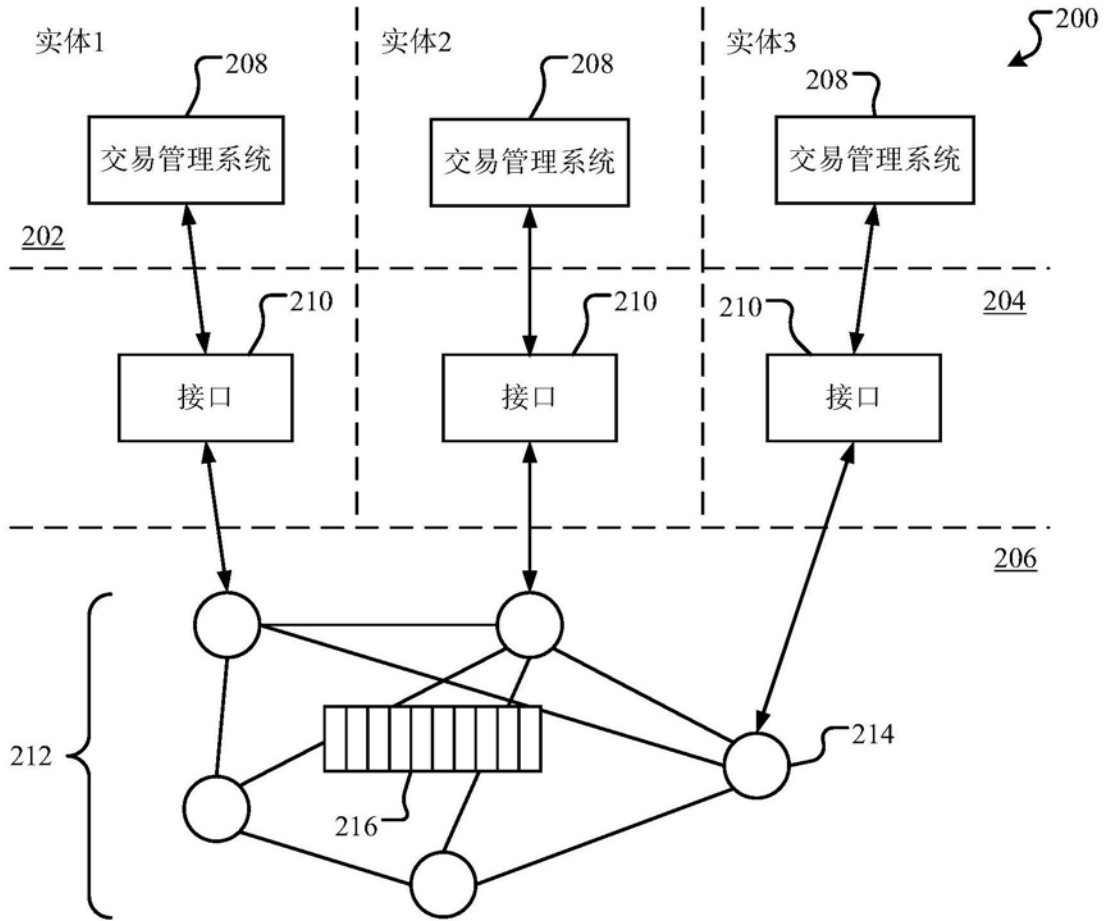


图2

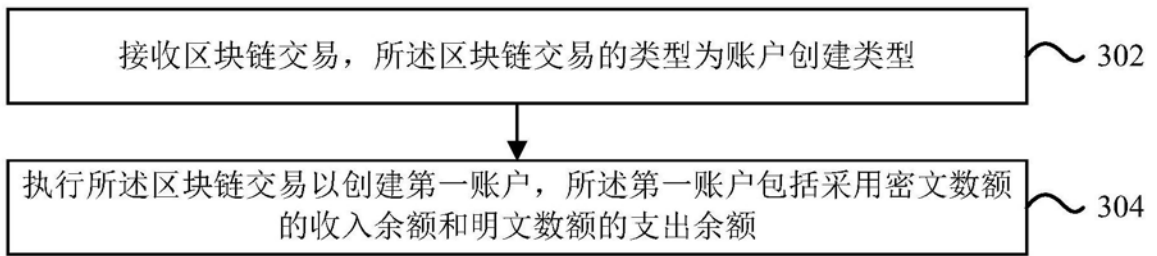


图3

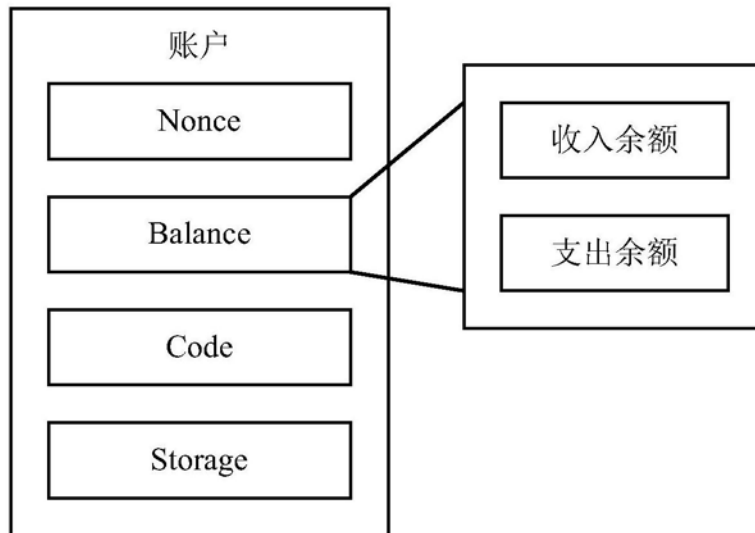


图4

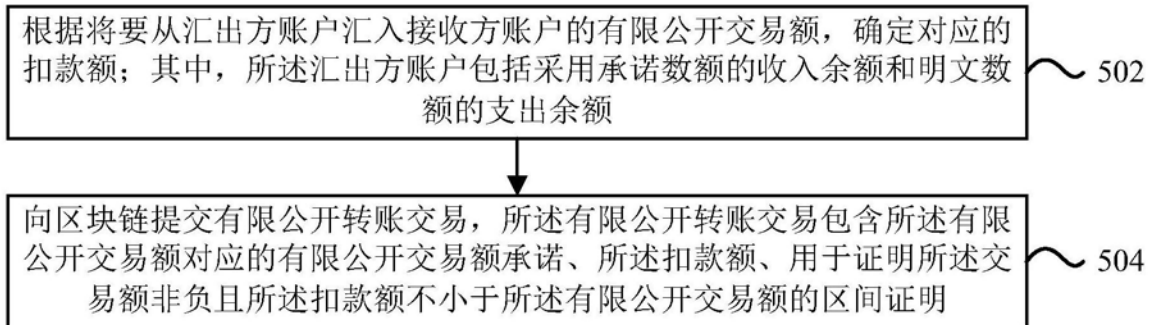


图5

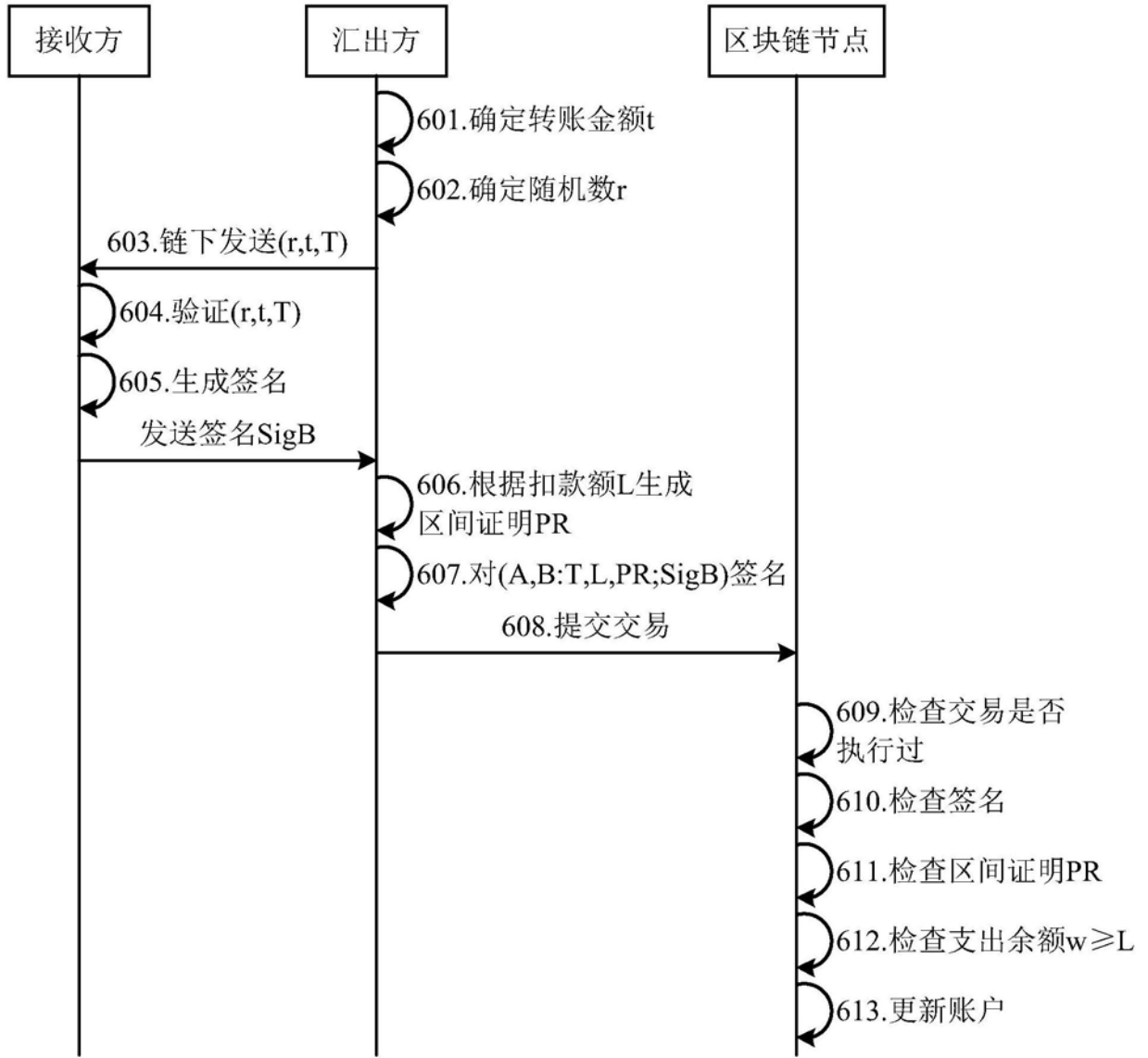


图6

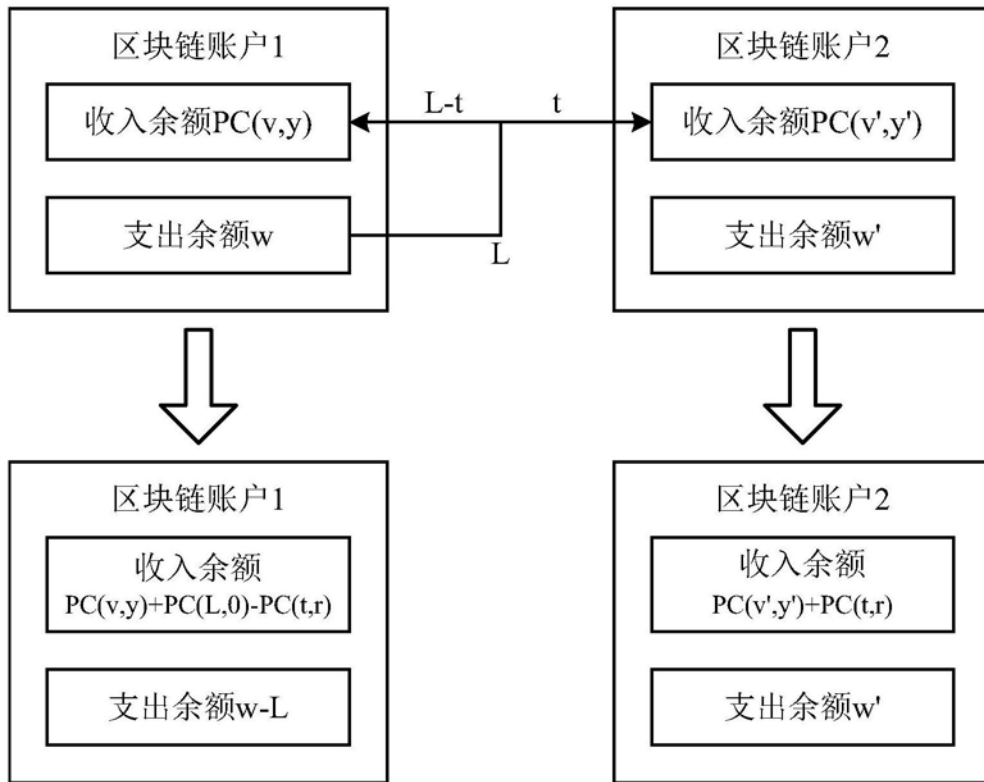


图7

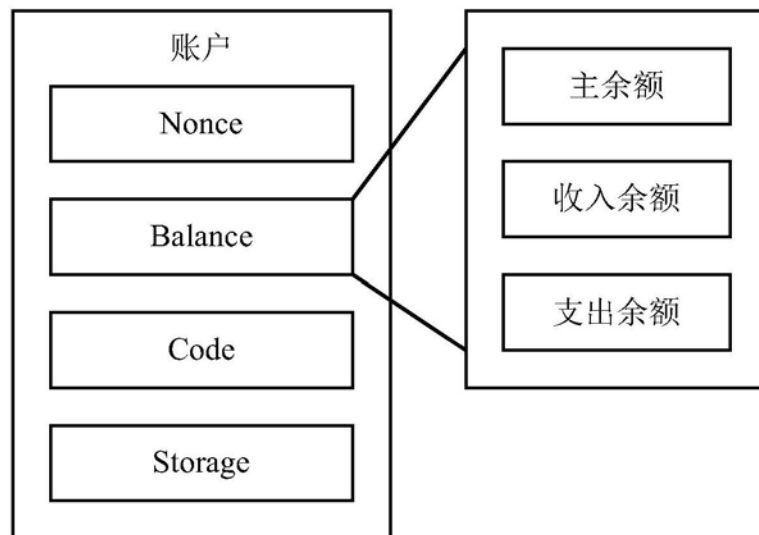


图8

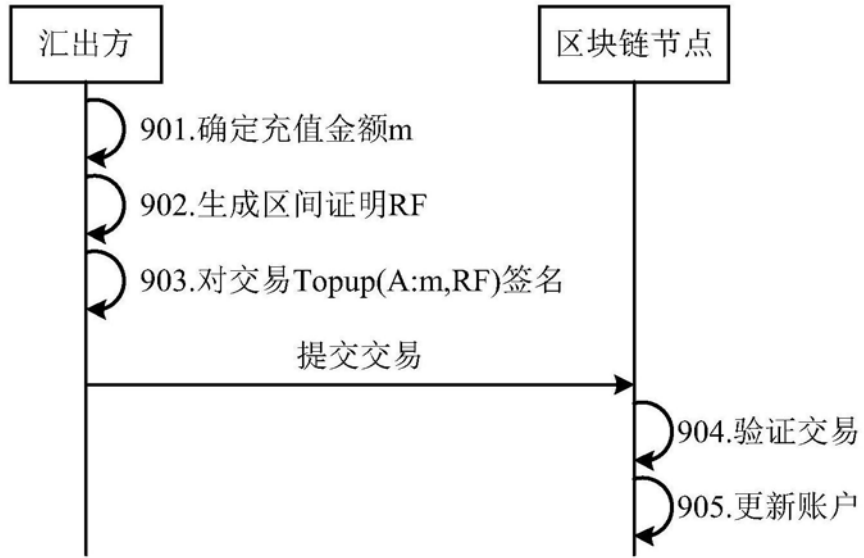


图9

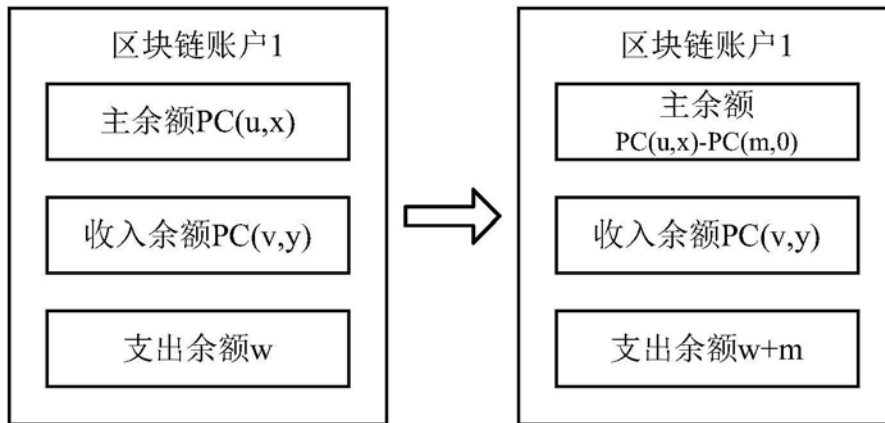


图10

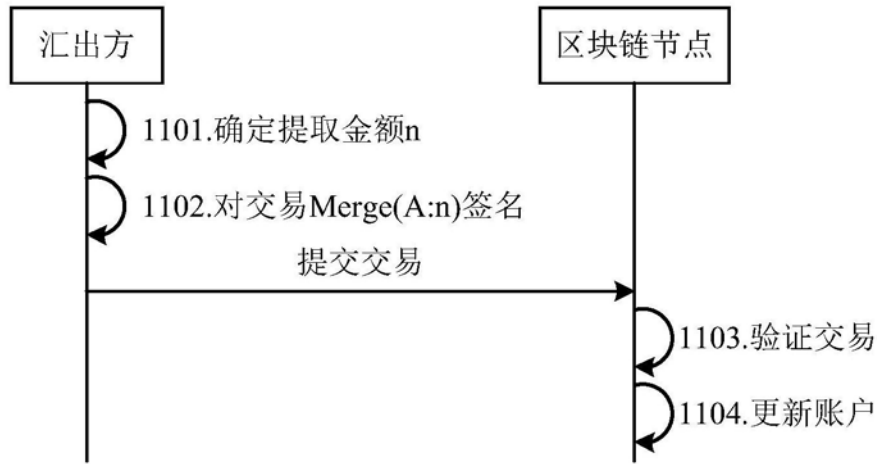


图11

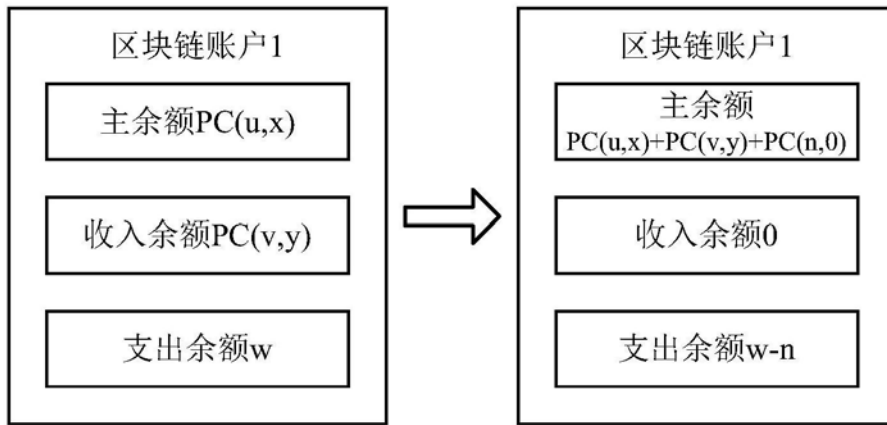


图12

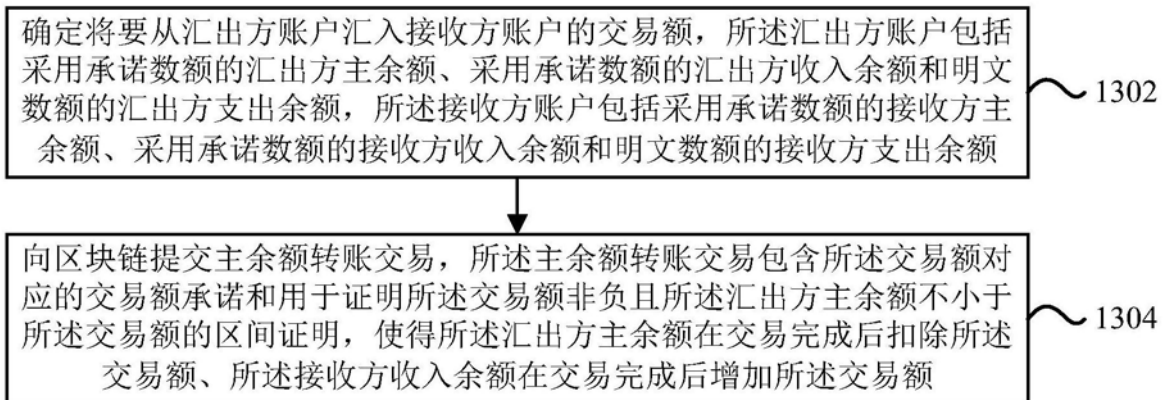


图13

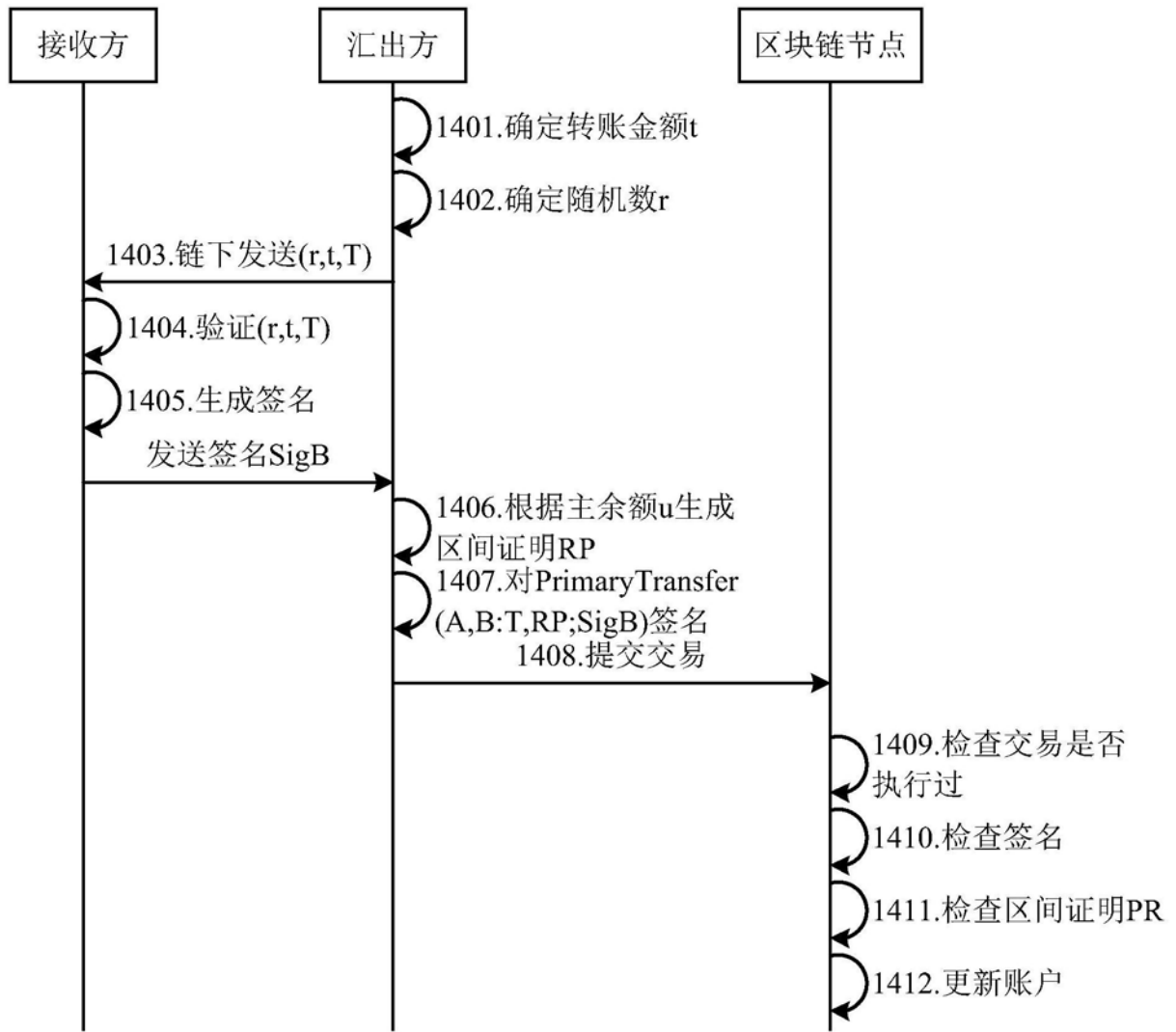


图14

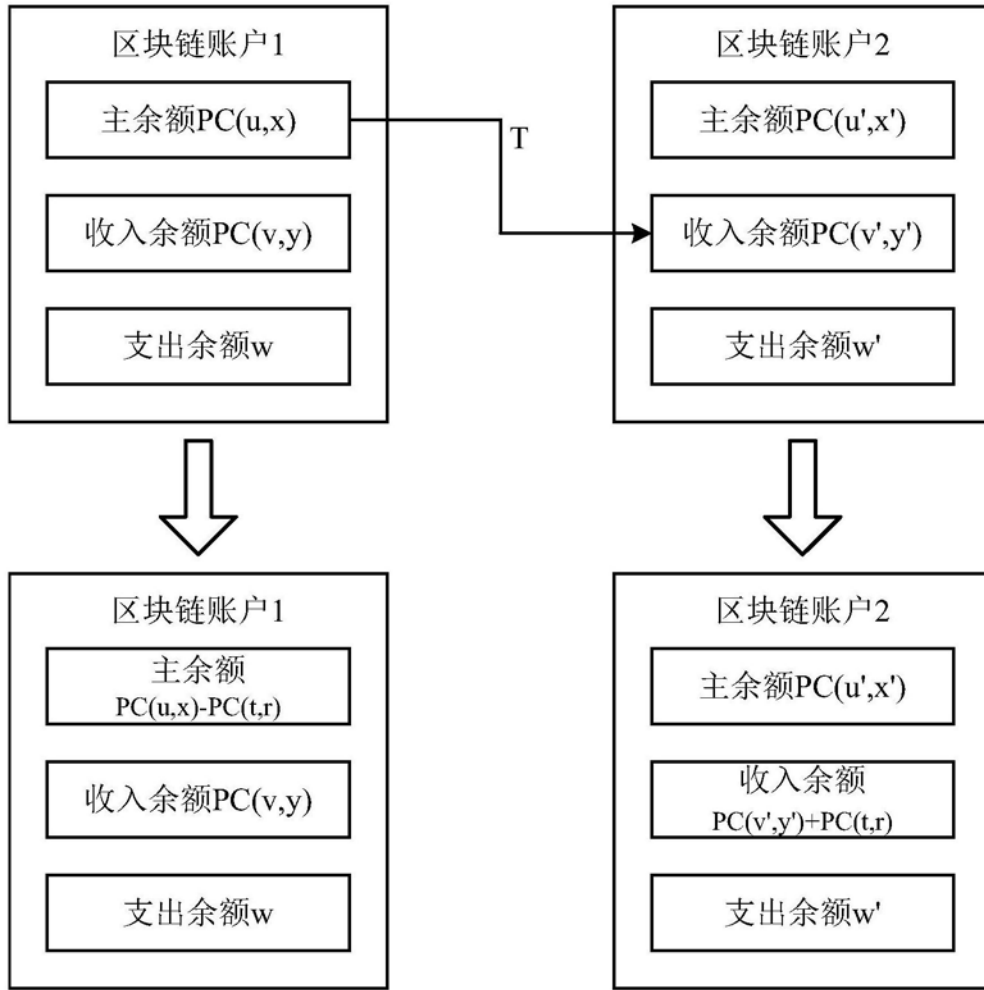


图15

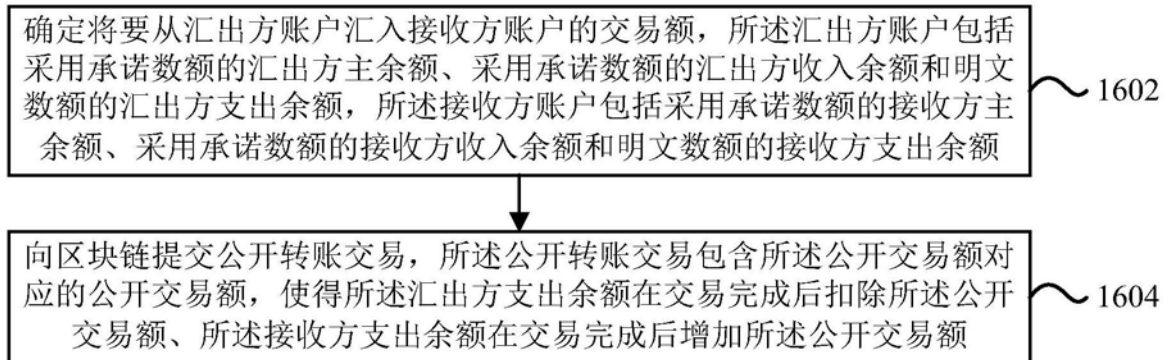


图16

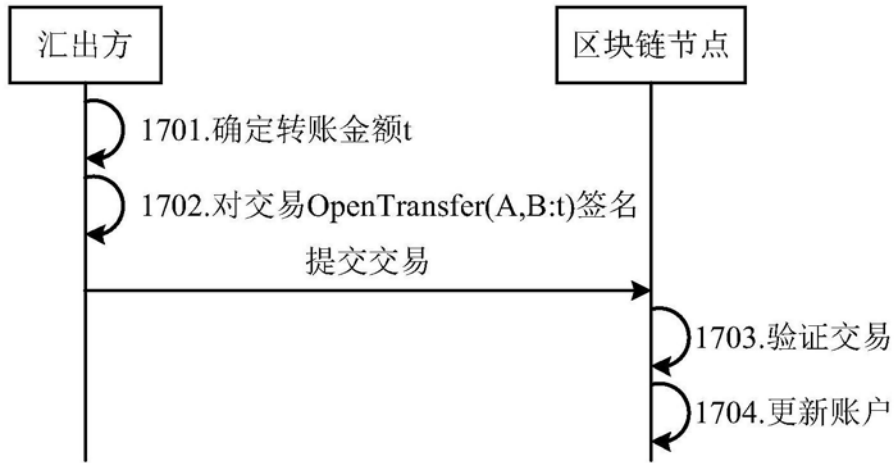


图17

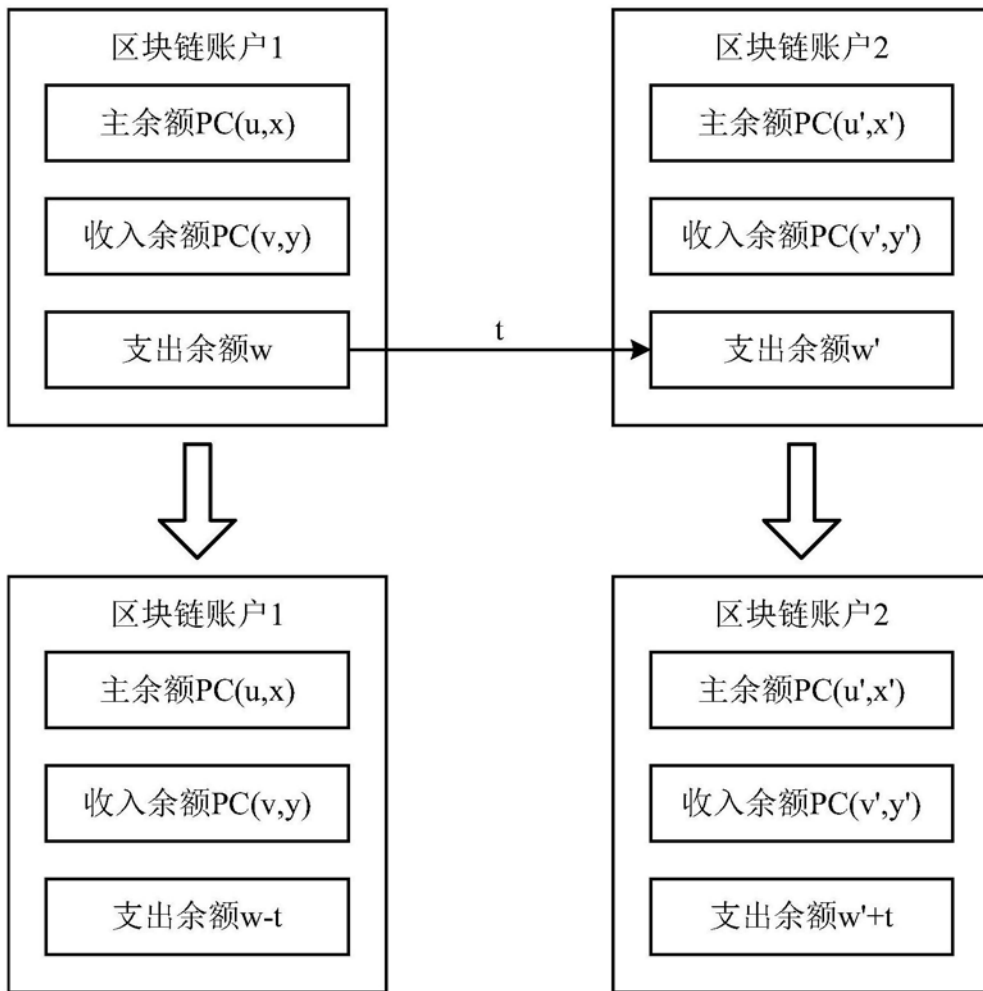


图18

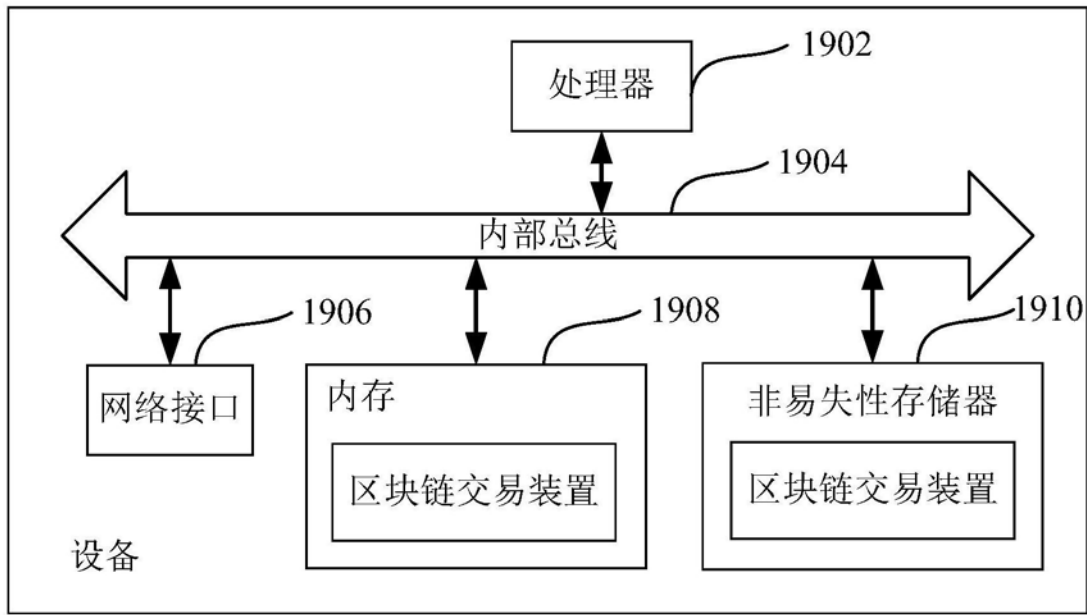


图19

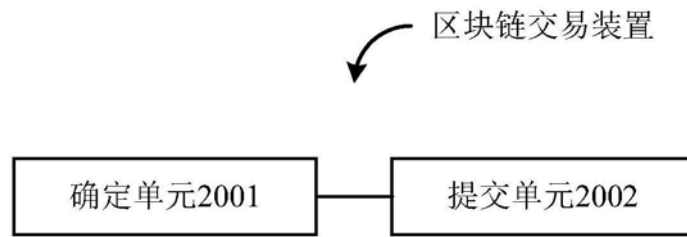


图20