(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112651740 B
(45)授权公告日 2024.10.29

(21)申请号 202011554075.6

(22)申请日 2018.08.30

(65)同一申请的已公布的文献号
申请公布号 CN 112651740 A

(43)申请公布日 2021.04.13

(62)分案原申请数据
201811003743.9 2018.08.30

(73)专利权人 蚂蚁链技术有限公司
地址 新加坡美芝路128号国浩时代城#20-01

(72)发明人 马宝利 刘正 殷山 张文彬 李漓春

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
专利代理师 周嗣勇

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 40/04(2012.01)

(56)对比文件
CN 109359974 B,2020.10.30

审查员 宋秋轶

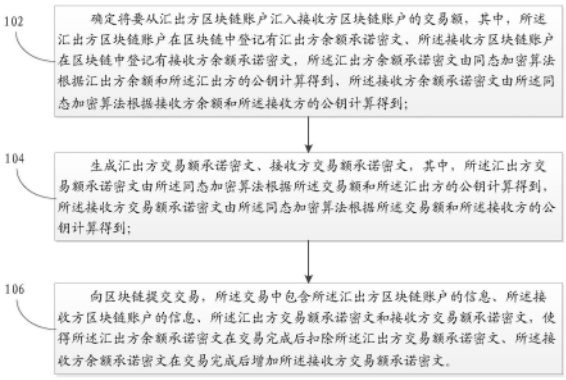
权利要求书3页 说明书12页 附图3页

(54)发明名称

区块链交易方法及装置、电子设备

(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，应用于汇出方设备，所述方法包括：确定交易额，其中，所述区块链中登记有汇出方余额承诺密文、接收方余额承诺密文；生成汇出方交易额承诺密文、接收方交易额承诺密文；向区块链提交交易，所述交易中包含所述汇出方区块链账户的信息、所述接收方区块链账户的信息、所述汇出方交易额承诺密文和接收方交易额承诺密文，使得所述汇出方余额承诺密文在交易完成后扣除所述汇出方交易额承诺密文、所述接收方余额承诺密文在交易完成后增加所述接收方交易额承诺密文。



CN 112651740 B

1.一种区块链交易方法,应用于汇出方设备,所述方法包括:

确定将要从汇出方区块链账户汇入接收方区块链账户的交易额;其中,所述汇出方区块链账户在区块链中登记有汇出方余额承诺密文,所述汇出方余额承诺密文由同态加密算法根据汇出方余额和所述汇出方的公钥计算得到;所述接收方区块链账户在区块链中登记有接收方余额承诺密文,所述接收方余额承诺密文由所述同态加密算法根据接收方余额和所述接收方的公钥计算得到;

由所述同态加密算法根据汇出方交易额随机数、所述交易额和所述汇出方的公钥进行计算,生成汇出方交易额承诺密文,并由所述同态加密算法根据接收方交易额随机数、所述交易额和所述接收方的公钥进行计算,生成接收方交易额承诺密文;以及,生成所述汇出方交易额随机数与接收方交易额随机数的差值;

向区块链提交交易,所述交易中包含所述汇出方区块链账户的信息、所述接收方区块链账户的信息、所述汇出方交易额承诺密文、所述接收方交易额承诺密文和所述汇出方交易额随机数与接收方交易额随机数的差值,使得所述区块链中的区块链节点验证所述汇出方交易额承诺密文所加密的交易额与所述接收方交易额承诺密文所加密的交易额相等,并使得所述汇出方余额承诺密文在交易完成后扣除所述汇出方交易额承诺密文,所述接收方余额承诺密文在交易完成后增加所述接收方交易额承诺密文。

2.根据权利要求1所述的方法,还包括:

生成接收方公钥证明,所述接收方公钥证明是由所述同态加密算法基于所述接收方交易额承诺密文生成的;

将所述接收方公钥证明添加到所述交易中,以供所述区块链中的区块链节点验证所述接收方交易额承诺密文与所述接收方余额承诺密文是由所述同态加密算法基于相同的公钥计算得到的;

所述生成接收方公钥证明包括:

生成第一验证随机数和第二验证随机数;

由所述同态加密算法基于所述第一验证随机数、第二验证随机数和所述接收方的公钥生成随机数承诺密文;

对所述接收方的交易额承诺密文和所述随机数承诺密文作哈希运算得到哈希摘要;

根据所述哈希摘要计算生成与第一验证随机数对应的第一验证元素,和与第二验证随机数对应的第二验证元素;

上述接收方公钥证明包括所述随机数承诺密文、所述第一验证元素和所述第二验证元素。

3.根据权利要求2所述的方法,所述汇出方余额承诺密文由所述同态加密算法根据汇出方余额、所述汇出方的公钥和汇出方随机数计算得到;

所述方法还包括:

根据所述汇出方随机数、所述汇出方交易额随机数、所述汇出方余额、所述汇出方余额承诺密文、所述交易额、所述汇出方交易额承诺密文生成区间证明;

将所述区间证明添加至所述交易中,以供所述区块链中的区块链节点验证所述交易额是否满足:所述交易额不小于0且所述交易额不大于所述汇出方余额。

4.根据权利要求1至3任一权利要求所述的方法,还包括:

通过汇出方私钥生成与所述汇出方交易额承诺密文和接收方交易额承诺密文相关的汇出方电子签名;

将所述电子签名添加到所述交易中,以供所述区块链中的区块链节点进行电子签名验证。

5.根据权利要求1所述的方法,还包括:

将所述接收方交易额随机数通过链外通道发送给所述接收方。

6.一种区块链交易装置,应用于汇出方设备,所述装置包括:

确定单元,确定将要从汇出方区块链账户汇入接收方区块链账户的交易额;其中,所述汇出方区块链账户在区块链中登记有汇出方余额承诺密文,所述汇出方余额承诺密文由同态加密算法根据汇出方余额和所述汇出方的公钥计算得到;所述接收方区块链账户在区块链中登记有接收方余额承诺密文,所述接收方余额承诺密文由所述同态加密算法根据接收方余额和所述接收方的公钥计算得到;

生成单元,由所述同态加密算法根据汇出方交易额随机数、所述交易额和所述汇出方的公钥进行计算,生成汇出方交易额承诺密文,并由所述同态加密算法根据接收方交易额随机数、所述交易额和所述接收方的公钥进行计算,生成接收方交易额承诺密文;以及,生成所述汇出方交易额随机数与接收方交易额随机数的差值;

提交单元,向区块链提交交易,所述交易中包含所述汇出方区块链账户的信息、所述接收方区块链账户的信息、所述汇出方交易额承诺密文、所述接收方交易额承诺密文和所述汇出方交易额随机数与接收方交易额随机数的差值,使得所述区块链中的区块链节点验证所述汇出方交易额承诺密文所加密的交易额与所述接收方交易额承诺密文所加密的交易额相等,并使得所述汇出方余额承诺密文在交易完成后扣除所述汇出方交易额承诺密文,所述接收方余额承诺密文在交易完成后增加所述接收方交易额承诺密文。

7.根据权利要求6所述的装置,所述生成单元:

生成接收方公钥证明,所述接收方公钥证明是由所述同态加密算法基于所述接收方交易额承诺密文生成的;

将所述接收方公钥证明添加到所述交易中,以供所述区块链中的区块链节点验证所述接收方交易额承诺密文与所述接收方余额承诺密文是由所述同态加密算法基于相同的公钥计算得到的;

所述生成接收方公钥证明包括:

生成第一验证随机数和第二验证随机数;

由所述同态加密算法基于所述第一验证随机数、第二验证随机数和所述接收方的公钥生成随机数承诺密文;

对所述接收方的交易额承诺密文和所述随机数承诺密文作哈希运算得到哈希摘要;

根据所述哈希摘要计算生成与第一验证随机数对应的第一验证元素,和与第二验证随机数对应的第二验证元素;

上述接收方公钥证明包括所述随机数承诺密文、所述第一验证元素和所述第二验证元素。

8.根据权利要求7所述的装置,所述汇出方余额承诺密文由所述同态加密算法根据汇出方余额、所述汇出方的公钥和汇出方随机数计算得到;

所述生成单元：

根据所述汇出方随机数、所述汇出方交易额随机数、所述汇出方余额、所述汇出方余额承诺密文、所述交易额、所述汇出方交易额承诺密文生成区间证明；

将所述区间证明添加至所述交易中，以供所述区块链中的区块链节点验证所述交易额是否满足：所述交易额不小于0且所述交易额不大于所述汇出方余额。

9.根据权利要求6至8任一权利要求所述的装置，所述生成单元：

通过汇出方私钥生成与所述汇出方交易额承诺密文和接收方交易额承诺密文相关的汇出方电子签名；

将所述电子签名添加到所述交易中，以供所述区块链中的区块链节点进行电子签名验证。

10.根据权利要求7所述的装置，还包括：

链外发送单元，将所述接收方交易额随机数通过链外通道发送给所述接收方。

11.一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求1到5任意一项所述的方法。

区块链交易方法及装置、电子设备

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。

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，因此区块链账本本身无隐私保护功能。

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，应用于汇出方设备，所述方法包括：

[0004] 确定将要从汇出方区块链账户汇入接收方区块链账户的交易额，其中，所述汇出方区块链账户在区块链中登记有汇出方余额承诺密文、所述接收方区块链账户在区块链中登记有接收方余额承诺密文，所述汇出方余额承诺密文由同态加密算法根据汇出方余额和所述汇出方的公钥计算得到、所述接收方余额承诺密文由所述同态加密算法根据接收方余额和所述接收方的公钥计算得到；

[0005] 生成汇出方交易额承诺密文、接收方交易额承诺密文，其中，所述汇出方交易额承诺密文由所述同态加密算法根据所述交易额和所述汇出方的公钥计算得到，所述接收方交易额承诺密文由所述同态加密算法根据所述交易额和所述接收方的公钥计算得到；

[0006] 向区块链提交交易，所述交易中包含所述汇出方区块链账户的信息、所述接收方区块链账户的信息、所述汇出方交易额承诺密文和接收方交易额承诺密文，使得所述汇出方余额承诺密文在交易完成后扣除所述汇出方交易额承诺密文、所述接收方余额承诺密文在交易完成后增加所述接收方交易额承诺密文。

[0007] 相应地，本说明书还提供了一种区块链交易装置，应用于汇出方设备，所述装置包括：

[0008] 确定单元，确定将要从汇出方区块链账户汇入接收方区块链账户的交易额，其中，所述汇出方区块链账户在区块链中登记有汇出方余额承诺密文、所述接收方区块链账户在区块链中登记有接收方余额承诺密文，所述汇出方余额承诺密文由同态加密算法根据汇出方余额和所述汇出方的公钥计算得到、所述接收方余额承诺密文由所述同态加密算法根据接收方余额和所述接收方的公钥计算得到；

[0009] 生成单元，生成汇出方交易额承诺密文、接收方交易额承诺密文，其中，所述汇出方交易额承诺密文由所述同态加密算法根据所述交易额和所述汇出方的公钥计算得到，所述接收方交易额承诺密文由所述同态加密算法根据所述交易额和所述接收方的公钥计算得到；

[0010] 提交单元,向区块链提交交易,所述交易中包含所述汇出方区块链账户的信息、所述接收方区块链账户的信息、所述汇出方交易额承诺密文和接收方交易额承诺密文,使得所述汇出方余额承诺密文在交易完成后扣除所述汇出方交易额承诺密文、所述接收方余额承诺密文在交易完成后增加所述接收方交易额承诺密文。

[0011] 相应的,本说明书还提供了一种计算机设备,包括:存储器和处理器;所述存储器上存储有可由处理器运行的计算机程序;所述处理器运行所述计算机程序时,执行如上述的区块链交易方法。

[0012] 本说明书提供的区块链交易方法、装置及计算机设备,提供了一种非交互式的转账方案,在区块链的账户模型下保护账户余额和交易金额隐私性,且无需接收方参与就可以完成转账。利用本说明书提供的技术方案,账户的余额只有该账户的所有人才能看到,交易的金额只有交易的转出方和转入方可以看到,而且区块链节点能够对加密的交易金额验证交易的合法性,并把合法的交易更新到转出方和转入方的账户余额上。这种非交互式的实施方案的优点是,交易的发起只需汇出方操作就行,不依赖于接收方以及和接收方的网络传输,从而避免了接收方不在线、回应延迟或网络故障、网络延迟等因素的干扰。

附图说明

[0013] 图1是一示例性实施例提供的一种区块链交易方法的流程图。

[0014] 图2是一示例性实施例提供的一种在区块链网络中实施汇款交易的示意图。

[0015] 图3是一示例性实施例提供的一种在区块链网络中实施汇款交易的流程图。

[0016] 图4是一示例性实施例提供的一种设备的结构示意图。

[0017] 图5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

[0018] 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。

[0019] 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。

[0020] 图1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1所示,该方法应用于汇出方设备,可以包括以下步骤:

[0021] 步骤102,确定将要从汇出方区块链账户汇入接收方区块链账户的交易额,其中,所述汇出方区块链账户在区块链中登记有汇出方余额承诺密文、所述接收方区块链账户在区块链中登记有接收方余额承诺密文,所述汇出方余额承诺密文由同态加密算法根据汇出方余额和所述汇出方的公钥计算得到、所述接收方余额承诺密文由所述同态加密算法根据

接收方余额和所述接收方的公钥计算得到。

[0022] 上述实施例所述的区块链,具体可指一个各节点通过共识机制达成的、具有分布式数据存储结构的P2P网络系统,该区块链内的数据分布在时间上相连的一个个“区块(block)”之内,后一区块包含前一区块的数据摘要,且根据具体的共识机制(如POW、POS、DPOS或PBFT等)的不同,达成全部或部分节点的数据全备份。本领域的技术人员熟知,由于区块链系统在相应共识机制下运行,已收录至区块链数据库内的数据很难被任意的节点篡改,例如采用Pow共识的区块链,至少需要全网51%算力的攻击才有可能篡改已有数据,因此区块链系统有着其他中心化数据库系统无法比拟的保证数据安全、防攻击篡改的特性。由此可知,在本说明书所提供的实施例中,被收录至区块链的分布式数据库中的数据不会被攻击或篡改,从而为发布至所述区块链的交易进行了存证。

[0023] 在一实施例中,汇出方用户与接收方用户可以约定交易额的数值;其中,汇出方用户对应于汇出方设备、接收方用户对应于接收方设备,汇出方设备与接收方设备之间可以实现基于本说明书的区块链交易方案,从汇出方区块链账户向接收方区块链账户汇入(或称为转移)对应于该交易额的资产凭证。资产凭证可以对应于区块链内的代币(token)、数字资产等智能资产,资产凭证还可以对应于区块链外的现金、证券、优惠券、房产等链外资产,本说明书并不对此进行限制。

[0024] 上述实施例所述的汇出方余额承诺密文或接收方余额承诺密文是利用同态加密算法,根据所述汇出方或接收方的余额、及所述汇出方或接收方的公钥计算得到的。由于区块链中的各个区块链节点需要基于共识而分别维护有统一的区块链账本,因而通过在区块链内登记汇出方余额承诺密文、接收方余额承诺密文,使得区块链节点维护的区块链账本中仅会记录关于该汇出方余额承诺的密文、接收方余额承诺的密文,而不会直接记录汇出方余额、接收方余额,使得汇出方用户持有的区块链余额、接收方用户持有的区块链余额被作为私密数据而隐藏,既为上述汇出方及接收方的账户余额进行了区块链的存证,防止其余额数值被篡改,又维护了区块链账户的私密性。

[0025] 上述在区块链中登记汇出方余额承诺密文、或接收方余额承诺密文的方式不作限定,既可以交易的形式在区块链中发布上述汇出方余额承诺密文、或接收方余额承诺密文,也可以在汇出方或接收方的账户属性内登记上述汇出方余额承诺密文、或接收方余额承诺密文,或本领域的技术人员容易想到的其他方式。

[0026] 在一实施例中,同态加密算法可以通过生成一随机数,使得该随机数与未加密数据一并被计算为相应的承诺密文数据,从而可以通过获知随机数以对承诺密文数据进行解密得到相应的未加密数据,或者通过获知随机数以验证承诺密文数据是否对应于未加密数据。譬如,该同态加密算法可以基于相关技术中的Pedersen承诺机制,当然本说明书并不对此进行限制。

[0027] 例如,采用包含Pedersen Commitment(PC)的同态加密技术对汇出方账户余额t加密:公共参数(G,H)为椭圆曲线的两个生成元,基于上述椭圆曲线上述汇出方有一对公私钥(Pk,Sk),Pk=SkG;上述汇出方余额t的承诺密文为(rG+tH,rPk),其中rG+tH是Pedersen Commitment(Pedersen承诺),r为上述同特加密中所使用的随机数,由于在汇出方对自身的账户余额进行查验时,使用私钥Sk解密时可以消除含有随机数r部分,所以无需对r做记录。解密(T,T')=(rG+tH,rPk)时,先用密钥sk从T'=rPk=rSkG得到rG=T'Sk^{-1},从而可消除含

有随机数的部分得到tH＝T-rG。另外,为了解密金额的密文tH,有下面这个设定,即金额t有一个有效区间,比如[0,2^{32}]。有多种方法可以解密金额的密文tH,比如Pollard的Kangaroo方法,或者事先计算并保存这个区间相应的密文集,最后根据tH的值查表可确定t的值,当然本说明书并不对此进行限制。

[0028] 类似地,接收方余额承诺密文也应于汇出方余额承诺密文采用相同的同态加密算法生成,例如,采用基于相同的椭圆曲线生成元G、H,并基于上述接收方的公钥及账户余额生成,以使仅能通过接收方的私钥对上述接收方余额承诺密文解密来获知接收方账户的余额,保护区块链上用户账户的隐私性。

[0029] 步骤104,生成汇出方交易额承诺密文、接收方交易额承诺密文,其中,所述汇出方交易额承诺密文由所述同态加密算法根据所述交易额和所述汇出方的公钥计算得到,所述接收方交易额承诺密文由所述同态加密算法根据所述交易额和所述接收方的公钥计算得到。

[0030] 上述实施例所述的汇出方交易额承诺密文应与上述的汇出方余额承诺密文、接收方交易额承诺密文应与上述的接收方余额承诺密文采用相同的同态加密算法,以使得汇出方余额承诺密文可以直接扣除汇出方交易额承诺密文、接收方余额承诺密文可以直接增加接收方交易额承诺密文。

[0031] 在一实施例中,所述汇出方交易额承诺密文由所述同态加密算法根据汇出方交易额随机数r_A、所述交易额t_A和所述汇出方的公钥Pk_A计算得到,上述汇出方交易额承诺密文为(T_A,T'_A)＝(r_AG+t_AH,r_APk_A);类似地,所述接收方交易额承诺密文由所述同态加密算法根据接收方交易额随机数r_B、所述交易额t_B和所述接收方的公钥Pk_B计算得到,上述接收方交易额承诺密文为(T_B,T'_B)＝(r_BG+t_BH,r_BPk_B);其中,t_A＝t_B。另外值得注意的是,为了使接收方在接受到本次交易额后,可以依据更新后的账户余额对新交易生成相应的区间证明,接收方需要获知该r_B的具体值;为了防止区块链上其他节点获知r_B的值以解密该交易额,汇出方需要通过链外通道把这笔交易中的r_B发送给接收方,这个动作不影响进行中的这笔交易,可以是交易过后,汇出方通过email或其它与接收方事先商量好的途径来发送,本说明书并不对此进行限制。

[0032] 因为汇出方发出的汇出方交易承诺及接收方交易承诺均为密文,其他节点均不能获知汇出方汇出的金额t_A的值,更不知汇出方发出的t_A是否与接收方收到的t_B是否相同;接收方通过自身的私钥解密汇出方发出的接收方交易承诺,虽然能获知t_B的值,但仍不能获知接收到的t_B是否与汇出方发出的t_A是否相同,因此在本说明书的又一实施例中,上述汇出方还将上述随机数r_A与随机数r_B的差值r发布于所述区块链,以供区块链中的区块链节点通过验证rG与T_A-T_B的值是否相等,若相等,则证明t_A＝t_B。

[0033] 上述包含了一种特殊情况,即用同一个r＝r_A＝r_B和同一个t＝t_A＝t_B来计算汇出方交易额承诺密文(T_A,T'_A)＝(rG+tH,rPk_A)和接收方交易额承诺密文(T_B,T'_B)＝(rG+tH,rPk_B)。在这种特殊情况下,交易额可以不用区分为汇出方交易金额和接收方交易金额,并且其承诺密文可以聚合成为一个(rG+tH,rPk_A,rPk_B)。对这种特殊情况,以下的一些技术细节可以得到简化,由于简化的方式是明显的,本发明不另外对这种特殊情况在每个可简化的细节上予以详细说明。

[0034] 在一实施例中,当汇出方交易额承诺密文由所述同态加密算法根据所述交易额和

所述汇出方的公钥计算得到,所述接收方交易额承诺密文由所述同态加密算法根据所述交易额和所述接收方的公钥计算得到时,由于区块链中的其他节点无法从接收方交易额承诺密文中获知该接收方交易额承诺密文是否是基于上述接收方的公钥(是否是与接收方余额承诺密文中所用的公钥相同)生成的,更无法获知该接收方的交易额承诺密文是否可被上述接收方的私钥解密以得到所述交易额;完成其他节点对汇出方所发布的接收方交易额承诺密文的验证,防止汇出方的交易欺诈,汇出方还应向所述区块链中发布一个接收方公钥证明,以供所述区块链中的区块链节点验证所述接收方交易额承诺密文是与所述接收方余额承诺密文由所述同态加密算法基于相同的公钥计算得到的,其中,所述接收方公钥证明是由所述同态加密算法基于所述接收方交易额承诺密文生成的。

[0035] 在一实施例中,汇出方以如下的方式生成公钥证明Pf,用来证明接收方交易额承诺密文(T_B,T'_B)=(r_BG+t_BH,r_BPk_B)是用B的公钥Pk_B加密的:

[0036] 产生一对随机数(r',t'),利用与生成上述接收方交易额承诺密文相同的同态加密算法计算随机数承诺密文(T,T')=(r'G+t'H,r'Pk_B),其中Pk_B是接收方的余额承诺密文中所使用的公钥;

[0037] 计算哈希u=Hash(T_B,T'_B,T,T')和v=u r_B+r',w=u t_B+t',其中,Hash表示哈希运算,v是与第一验证随机数r'对应的第一验证元素,w是与第二验证随机数t'对应的第二验证元素;

[0038] 生成Pf=(T,T';v,w)。

[0039] 区块链中其他节点在验证该汇出方发出的接收方交易额承诺密文是否是与接收方余额承诺密文中所用的公钥相同时,获取上述Pf=(T,T';v,w)验证(vG+wH,v Pk_B)=(uT_B+T,uT'_B+T')是否正确;

[0040] 如果正确,表示所述接收方交易额承诺密文与所述接收方余额承诺密文是由所述同态加密算法基于相同的公钥计算得到的,上述接收方交易额承诺密文可被上述公钥对应的私钥解密以得到交易额;

[0041] 如果不正确,应拒绝此交易,此时,汇出方以非接收方的公钥加密交易额以生成上述接收方交易额承诺密文,甚至以一个随便的数冒充上述接收方交易额承诺密文,那么该接收方交易额承诺密文更新到接收方余额承诺密文后,接收方将无法解密其余额承诺密文,也无法从其账户汇出资产,即接收方的账户被破坏了。

[0042] 本发明采用的上述接收方公钥证明的实施方案杜绝了上述账户被破坏的情况发生,并且不需要收款方的参与,是一种非交互式的方式。

[0043] 在又一实施例中,如上述实施例所述,所述汇出方余额承诺密文由所述同态加密算法根据汇出方随机数、汇出方余额、和所述汇出方的公钥计算得到,如上述实施例中所述的,汇出方余额承诺密文(S_A,S'_A)=(r'_AG+s_AH,r'_APk_A),其中,s_A为汇出方余额,所述汇出方交易额承诺密文由所述同态加密算法根据汇出方交易额随机数、所述交易额、和所述汇出方的公钥计算得到,即汇出方交易额承诺密文为(T_A,T'_A)=(r_AG+t_AH,r_APk_A),其中,t_A为交易额;汇出方设备可以根据所述汇出方随机数r'_A、所述汇出方余额s_A、所述汇出方余额承诺密文(S_A,S'_A)、所述汇出方交易额随机数r_A、所述交易额t_A和所述交易承诺密文(T_A,T'_A)生成区间证明,并将所述区间证明添加至所述交易中,以供所述区块链中的区块链节点验证所述交易额是否满足:所述交易额t_A不小于0且所述交

易额t_A不大于所述汇出方余额s_A。例如,可以采用相关技术中的区间证明(Range Proof)技术,譬如Bulletproofs方案或Borromean环签名方案等,本说明书并不对此进行限制。

[0044] 在一实施例中,汇出方设备可以通过汇出方私钥生成与所述汇出方交易额承诺密文和接收方交易额承诺密文相关的电子签名,并将所述电子签名添加至汇出方向所述区块链发布的交易中,以供所述区块链中的区块链节点进行电子签名验证。在又一实施例中,汇出方签名还可以与上述汇出方交易额随机数与接收方交易额随机数的差值、或上述接收方公钥证明、或上述区间证明相关,当交易中并未包含该汇出方签名时,区块链节点可以判定为共识失败,从而拒绝执行该交易。

[0045] 步骤106,向区块链提交交易,所述交易中包含所述汇出方区块链账户的信息、所述接收方区块链账户的信息、所述汇出方交易额承诺密文和接收方交易额承诺密文,使得所述汇出方余额承诺密文在交易完成后扣除所述汇出方交易额承诺密文、所述接收方余额承诺密文在交易完成后增加所述接收方交易额承诺密文,亦即:

[0046] (S_A,S'_A)-(T_A,T'_A)=(S_A-T_A,S'_A-T'_A),

[0047] (S_B,S'_B)+(T_B,T'_B)=(S_B+T_B,S'_B+T'_B)。

[0048] 在上述实施例中,通过在交易中采用所述汇出方交易额承诺密文和接收方交易额承诺密文,使得区块链账本中只会记录上述交易承诺密文,而无法获知相应的交易额,从而对交易额的取值进行隐藏和保密。同时,通过使用相同的同态加密算法生成汇出方余额对应的汇出方余额承诺密文、接收方余额对应的接收方余额承诺密文、交易额对应的汇出方交易额承诺密文和接收方交易额承诺密文,使得在区块链其他节点无需获知汇出方余额、接收方余额和交易额的情况下,即可在汇出方余额承诺密文与汇出方交易额承诺密文之间直接实现扣除运算、在接收方余额承诺密文与接收方交易承诺密文之间直接实现增加运算,确保在不透露隐私数据的情况下顺利完成交易。

[0049] 在一实施例中,区块链节点在接收到上述交易后,可以通过相关技术中的防双花或防重放机制,检查该交易是否已经执行过;如果已经执行过,则拒绝执行该交易。

[0050] 为了便于理解,下面以区块链网络中的汇款交易为例,对本说明书的技术方案进行详细说明。图2是一示例性实施例提供的一种在区块链网络中实施汇款交易的示意图。如图2所示,假定由用户A向用户B进行区块链汇款;其中,本说明书中的“用户”可以表现为所登录的用户账号,而该用户账号实际可以归属于个人或组织,本说明书并不对此进行限制。

[0051] 假定用户A使用的汇出方设备为用户设备1,譬如该用户设备1上登录有对应于用户A的用户账号;类似地,用户B使用的接收方设备为用户设备2。用户设备1上可以运行有区块链的客户端程序,使得该用户设备1在区块链网络中存在对应的区块链节点,比如图2所示的节点1。类似地,用户设备2上可以运行有区块链的客户端程序,使得该用户设备2在区块链网络中存在对应的区块链节点,比如图2所示的节点2。区块链网络中还存在其他区块链节点,比如图2所示的节点i等,此处不再一一列举。通过上述的节点1、节点2等,使得用户A与用户B之间的汇款交易可以经由区块链网络实施,相关交易信息可以被记录至各个区块链节点分别维护的区块链账本中,可以避免发生篡改,并有助于后续查验。

[0052] 针对图2所示的汇款交易场景,图3是一示例性实施例提供的一种在区块链网络中实施汇款交易的流程图;如图3所示,汇出方和区块链节点之间的交互过程可以包括以下步骤:

[0053] 步骤301,确定将要从汇出方区块链账户汇入接收方区块链账户的交易额t_A。

[0054] 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。例如在图2所示的实施例中,用户设备1可以被配置为汇出方,而用户设备2可以被配置为接收方。

[0055] 所述汇出方区块链账户在区块链中登记有汇出方余额承诺密文:

[0056] (S_A,S'_A)=(r'_AG+s_AH,r'_APk_A);

[0057] 所述接收方区块链账户在区块链中登记有接收方余额承诺密文:

[0058] (S_B,S'_B)=(r'_BG+s_BH,r'_BPk_B);

[0059] 所述汇出方余额承诺密文(S_A,S'_A)由同态加密算法根据汇出方余额s_A和所述汇出方的公钥Pk_A计算得到、所述接收方余额承诺密文(S_B,S'_B)由所述同态加密算法根据接收方余额s_B和所述接收方的公钥Pk_B计算得到;汇出方余额随机数r'_A和接收方余额随机数r'_B为上述同态加密算法所使用的随机数,G、H为椭圆曲线算法的两个元组。

[0060] 步骤302,生成汇出方交易额承诺密文(T_A,T'_A)=(r_AG+t_AH,r_APk_A)、和接收方交易额承诺密文(T_B,T'_B)=(r_BG+t_BH,r_BPk_B);

[0061] 其中,所述汇出方交易额承诺密文(T_A,T'_A)由所述同态加密算法根据所述交易额t_A和所述汇出方的公钥Pk_A计算得到,所述接收方交易额承诺密文(T_B,T'_B)由所述同态加密算法根据所述交易额t_B和所述接收方的公钥Pk_B计算得到,且t_B=t_A;汇出方交易额随机数r_A和接收方交易额随机数r_B为上述同态加密算法所使用的随机数,上述密文的生成过程中仍使用原椭圆曲线算法的两元组G、H。

[0062] 进一步地,为使区块链中的其他节点能够验证t_B=t_A,在接下来的步骤303中应生成r=r_A-r_B。

[0063] 在又一实施例中,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_A、账户余额s_A的取值满足下述条件:t_A≥0、s_A-t≥0;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与(r_A,s_A,S_A,r,t,T)相关的区间证明PR,以供后续过程中由区块链节点进行验证是否满足t_A≥0、s_A-t≥0。例如图3所示的:

[0064] 步骤304,生成一个区间证明RP1,用来证明t_A≥0。

[0065] 步骤305,生成一个区间证明RP2,用来证明s_A-t_A≥0。

[0066] 为使区块链中的节点验证上述的接收方交易额承诺密文(T_B,T'_B)是与接收方余额承诺密文(s_B,s'_B)采用相同的加密方式加密、且可被接收方的私钥解密,以正确地获得交易额并将其更新至账户余额,汇出方还应生成一接收方公钥证明,如图3所示:

[0067] 步骤306,生成证明Pf,用来证明(T_B,T'_B)是用B的公钥Pk_B加密的。

[0068] 在一实施例中,证明Pf的生成过程可包括:

[0069] 产生一对随机数(r',t');

[0070] 利用与生成上述接收方交易额承诺密文相同的同态加密算法计算随机数承诺密文(T,T')=(r'G+t'H,r'Pk_B),其中Pk_B是接收方的余额承诺密文中所使用的公钥;

[0071] 计算哈希u=Hash(T_B,T'_B,T,T'),v=ur_B+r',w=ut_B+t',其中,Hash表示哈希运算,v是与第一验证随机数r'对应的第一验证元素,w是与第二验证随机数t'对应的第

二验证元素;

[0072] 生成Pf＝(T,T';v,w)。

[0073] 步骤307,汇出方利用Pk_A对应的私钥对(A,T_A,T'_A;B,T_B,T'_B)电子签名Sign A,其中A、B分别为汇出方、接收方的账户或账户地址等识别信息,用以协助区块链的其他节点验证本次交易转移的汇出方和接收方;这里值得注意的是本实施例并不限定汇出方的电子签名所签署的内容对象,既可以包括A,T_A,T'_A,B,T_B,T'_B,还可进一步包括r,RP1,RP2,Pf中的一个或多个。

[0074] 步骤308,汇出方将上述生成的各密文(T_A,T'_A;T_B,T'_B)及汇出方、接收方的账户或账户地址等识别信以交易的格式提交到上述区块链的网络中等待区块链的节点对该交易进行共识验证,以最终将其收录至区块链的分布式账本中;更优地,为协助区块链的节点对本次交易进行共识验证,还可将上述生成的各证明参数(r,RP1,RP2,Pf)及电子签名Sign A加入到上述交易的内容中来。

[0075] 在一实施例中,汇出方可以通过节点1向区块链提交相应的上述交易,以执行汇款。该交易将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交易的内容和格式进行验证,以在验证通过时执行汇款操作、在验证未通过时拒绝汇款。

[0076] 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交易,如(A,T_A,T'_A;B,T_B,T'_B;r,RP1,RP2,Pf;Sign A),并通过步骤309～312等实施验证等操作。

[0077] 步骤309,区块链节点检查交易是否被执行过。

[0078] 在一实施例中,区块链节点在收到汇款交易(A,T_A,T'_A;B,T_B,T'_B;r,RP1,RP2,Pf;Sign A)后,可以利用区块链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310。

[0079] 步骤310,区块链节点检查签名Sign A。

[0080] 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Sign A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311。

[0081] 步骤311,区块链节点验证t_A是否与t_B相等。

[0082] 在一实施例中,通过验证rG＝T_A-T_B是否正确,即可验证t_A是否与t_B相等;如果不正确,可以拒绝执行该汇款交易,否则转入步骤312。

[0083] 步骤312,区块链节点验证t_A≥0;

[0084] 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PR1进行检查,以确定是否满足t_A≥0;如果不满足,可以拒绝执行该汇款交易,否则转入步骤313。

[0085] 步骤313,区块链节点验证s_A-t_A≥0;

[0086] 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PR2进行检查,以确定是否满足s_A-t_A≥0;如果不满足,可以拒绝执行该汇款交易,否则转入步骤314。

[0087] 步骤314,区块链节点验证金额密文(T_B,T'_B)是否与所述接收方余额承诺密文(s_B,s'_B)是由所述同态加密算法基于相同的公钥Pk_B计算得到。

[0088] 在一实施例中,区块链节点可以对该汇款交易包含的Pf中的各参数,验证(vG+wH,

v Pk_B)＝(uT_B+T,uT'_B+T')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315。

[0089] 步骤315,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的账户余额。

[0090] 在一实施例中,在通过步骤309～314的验证后,区块链节点可以将区块链账本中记载的汇出方账户余额s_A对应的余额承诺密文(S_A,S'_A)扣除汇出方交易额承诺密文(T_A,T'_A)、接收方账户余额s_B对应的余额承诺密文(S_B,S'_B)增加接收方交易额承诺密文(T_B,T'_B),使得用户A对应的区块链账户1的余额承诺更新为s_A-t_A、用户B对应的区块链账户2的余额承诺更新为s_B+t_B,其中t_A＝t_B。

[0091] 基于同态加密算法的性质,当余额承诺密文(S_A,S'_A)更新为[(S_A,S'_A)-(T_A,T'_A)]时,由于

[0092] (S_A,S'_A)-(T_A,T'_A)＝(S_A-T_A,S'_A-T'_A),

[0093] 且(S_A-T_A,S'_A-T'_A)＝(r'_A-r_A)G+(s_A-t_A)H,(r'_A-r_A)Pk_A),

[0094] 因此,区块链中的其他节点在不知晓汇出方的账户余额s_A的具体值、也不知晓汇出方汇出的交易额t_A的情况下,经区块链节点的共识验证,将汇出方的账户余额更新为(s_A-t_A)。

[0095] 同理,基于同态加密算法的性质,当余额承诺密文(S_B,S'_B)更新为[(S_B,S'_B)+(T_B,T'_B)]时,由于

[0096] (S_B,S'_B)+(T_B,T'_B)＝(S_B+T_B,S'_B+T'_B),

[0097] 且(S_B+T_B,S'_B+T'_B)＝(r'_B+r_B)G+(s_B+t_B)H,(r'_B+r_B)Pk_B),

[0098] 因此,区块链中的其他节点在不知晓接收方的账户余额s_B的具体值、也不知晓汇出方汇出的交易额t_B的情况下,经区块链节点的共识验证,将接收方的账户余额更新为(s_B+t_B)。

[0099] 可选地,为保证接收方能在接受本次交易后再基于其账户余额进行转账交易,上述实施例可包括步骤316:汇出方可通过链外通道将上述的接收方交易额随机数r_B发送给接收方。

[0100] 综上所述,通过采用同态加密机制,可以对区块链账户的账户余额进行加密、将加密后的余额承诺密文记载于区块链账本中,还可以在汇款交易过程中对汇款额加密、将加密后的汇款承诺密文用于实施汇款交易,可以在对账户余额、汇款额均保密的情况下,通过区块链网络顺利完成汇款交易,并且不影响区块链节点对交易条件的验证操作,使得区块链网络具备了隐私保护功能。而且本说明书提供的上述实施例中,仅通过汇出方生成汇款及验证参数、提交交易,在区块链其他节点对交易内容共识验证完成后即可完成上述汇款操作,全程无需接收方节点设备的参与,不依赖于接收方以及和接收方的网络传输,从而避免了接收方不在线、回应延迟或网络故障、网络延迟等因素的干扰。

[0101] 值得注意的是,本说明书并不限定生成各个证明或电子签名(如r、RP1、RP2、Pf、Sign A等)的先后顺序,也不限定区块链中的节点对汇出方提出的交易中各项内容及证明或电子签名的验证的先后顺序,图3仅仅是本说明书提供的交易生成及验证方法过程的一种实施例,本说明书不限于此。

[0102] 图4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4,在硬件层面,该

设备包括处理器402、内部总线404、网络接口406、内存408以及非易失性存储器410，当然还可能包括其他业务所需要的硬件。处理器402从非易失性存储器410中读取对应的计算机程序到内存408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定于各个逻辑单元，也可以是硬件或逻辑器件。

[0103] 请参考图5，在软件实施方式中，该区块链交易装置应用于汇出方设备50，可以包括：

[0104] 确定单元502，确定将要从汇出方区块链账户汇入接收方区块链账户的交易额，其中，所述汇出方区块链账户在区块链中登记有汇出方余额承诺密文、所述接收方区块链账户在区块链中登记有接收方余额承诺密文，所述汇出方余额承诺密文由同态加密算法根据汇出方余额和所述汇出方的公钥计算得到、所述接收方余额承诺密文由所述同态加密算法根据接收方余额和所述接收方的公钥计算得到；

[0105] 生成单元504，生成汇出方交易额承诺密文、接收方交易额承诺密文，其中，所述汇出方交易额承诺密文由所述同态加密算法根据所述交易额和所述汇出方的公钥计算得到，所述接收方交易额承诺密文由所述同态加密算法根据所述交易额和所述接收方的公钥计算得到；

[0106] 提交单元506，向区块链提交交易，所述交易中包含所述汇出方区块链账户的信息、所述接收方区块链账户的信息、所述汇出方交易额承诺密文和接收方交易额承诺密文，使得所述汇出方余额承诺密文在交易完成后扣除所述汇出方交易额承诺密文、所述接收方余额承诺密文在交易完成后增加所述接收方交易额承诺密文。

[0107] 更优的，所述汇出方交易额承诺密文由所述同态加密算法根据汇出方交易额随机数、所述交易额和所述汇出方的公钥计算得到，所述接收方交易额承诺密文由所述同态加密算法根据接收方交易额随机数、所述交易额和所述接收方的公钥计算得到；

[0108] 所述生成单元504：

[0109] 生成所述汇出方交易额随机数与接收方交易额随机数的差值；

[0110] 将所述汇出方交易额随机数与接收方交易额随机数的差值添加到所述交易中，以供区块链中的区块链节点验证所述汇出方交易额承诺密文所加密的交易额与所述接收方交易额承诺密文所加密的交易额相等。

[0111] 更优的，所述生成单元504：

[0112] 生成接收方公钥证明，所述接收方公钥证明是由所述同态加密算法基于所述接收方交易额承诺密文生成的；

[0113] 将所述接收方公钥证明添加到所述交易中，以供所述区块链中的区块链节点验证所述接收方交易额承诺密文与所述接收方余额承诺密文是由所述同态加密算法基于相同的公钥计算得到的。

[0114] 更优的，所述生成单元504：

[0115] 生成第一验证随机数和第二验证随机数；

[0116] 由所述同态加密算法基于所述第一验证随机数、第二验证随机数和所述接收方的公钥生成随机数承诺密文；

[0117] 对所述接收方的交易额承诺密文作哈希运算得到哈希摘要；

[0118] 根据所述哈希摘要计算生成与第一验证随机数对应的第一验证元素，和与第二验证随机数对应的第二验证元素；

[0119] 上述接收方公钥证明包括所述随机数承诺密文、所述第一验证元素和所述第二验证元素。

[0120] 更优的，所述汇出方余额承诺密文由所述同态加密算法根据汇出方余额、所述汇出方的公钥和汇出方随机数计算得到；

[0121] 所述生成单元504：

[0122] 根据所述汇出方随机数、所述汇出方交易额随机数、所述汇出方余额、所述汇出方余额承诺密文、所述交易额、所述汇出方交易额承诺密文生成区间证明；

[0123] 将所述区间证明添加至所述交易中，以供所述区块链中的区块链节点验证所述交易额是否满足：所述交易额不小于0且所述交易额不大于所述汇出方余额。

[0124] 更优的，所述生成单元504：

[0125] 通过汇出方私钥生成与所述汇出方交易额承诺密文和接收方交易额承诺密文相关的汇出方电子签名；

[0126] 将所述电子签名添加到所述交易中，以供所述区块链中的区块链节点进行电子签名验证。

[0127] 更优的，上述装置还包括：

[0128] 链外发送单元，将所述接收方交易额随机数通过链外通道发送给所述接收方。

[0129] 上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，相关之处参见方法实施例的部分说明即可，在此不再赘述。

[0130] 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。

[0131] 与上述方法实施例相对应，本说明书的实施例还提供了一种计算机设备，该计算机设备包括存储器和处理器。其中，存储器上存储有能够由处理器运行的计算机程序；处理器在运行存储的计算机程序时，执行本说明书实施例中区块链的交易方法的各个步骤。对区块链的交易方法的各个步骤的详细描述请参见之前的内容，不再重复。

[0132] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。

[0133] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0134] 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。

[0135] 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。

[0136] 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,磁带磁磁盘存储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。

[0137] 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。

[0138] 本领域技术人员应明白,本说明书的实施例可提供为方法、系统或计算机程序产品。因此,本说明书的实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且,本说明书的实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

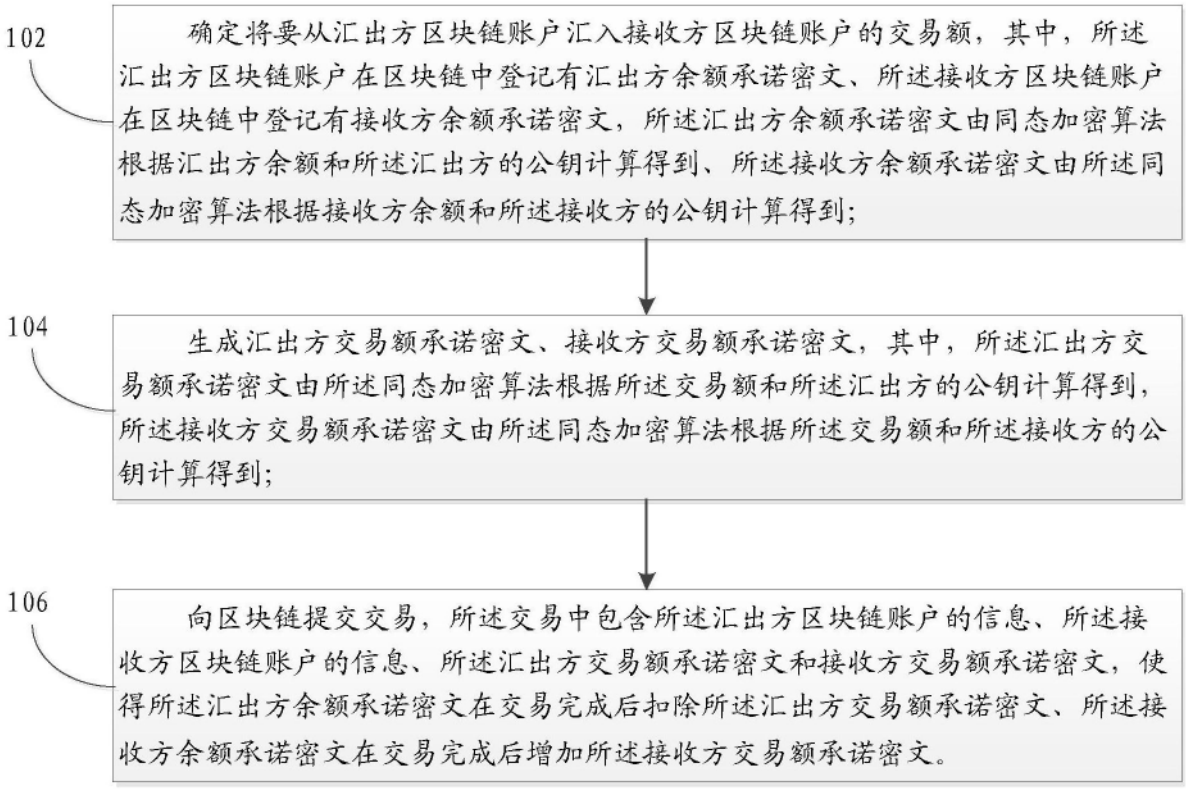

102
确定将要从汇出方区块链账户汇入接收方区块链账户的交易额，其中，所述汇出方区块链账户在区块链中登记有汇出方余额承诺密文、所述接收方区块链账户在区块链中登记有接收方余额承诺密文，所述汇出方余额承诺密文由同态加密算法根据汇出方余额和所述汇出方的公钥计算得到、所述接收方余额承诺密文由所述同态加密算法根据接收方余额和所述接收方的公钥计算得到；
104
生成汇出方交易额承诺密文、接收方交易额承诺密文，其中，所述汇出方交易额承诺密文由所述同态加密算法根据所述交易额和所述汇出方的公钥计算得到，所述接收方交易额承诺密文由所述同态加密算法根据所述交易额和所述接收方的公钥计算得到；
106
向区块链提交交易，所述交易中包含所述汇出方区块链账户的信息、所述接收方区块链账户的信息、所述汇出方交易额承诺密文和接收方交易额承诺密文，使得所述汇出方余额承诺密文在交易完成后扣除所述汇出方交易额承诺密文、所述接收方余额承诺密文在交易完成后增加所述接收方交易额承诺密文。

图1

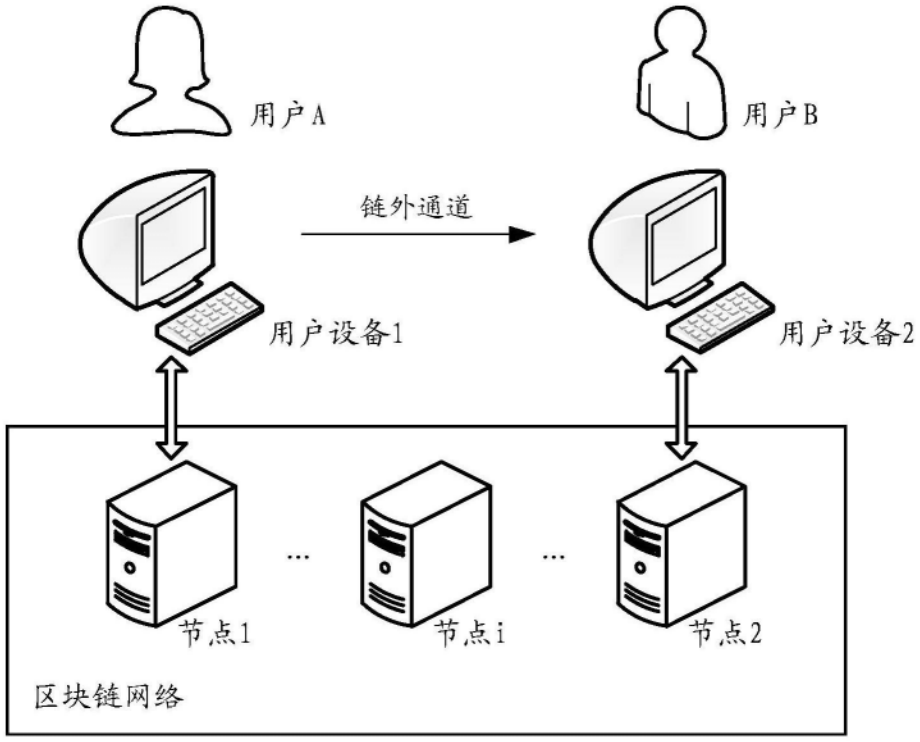

用户A
用户B
链外通道
用户设备1
用户设备2
节点1
节点i
节点2
区块链网络

图2

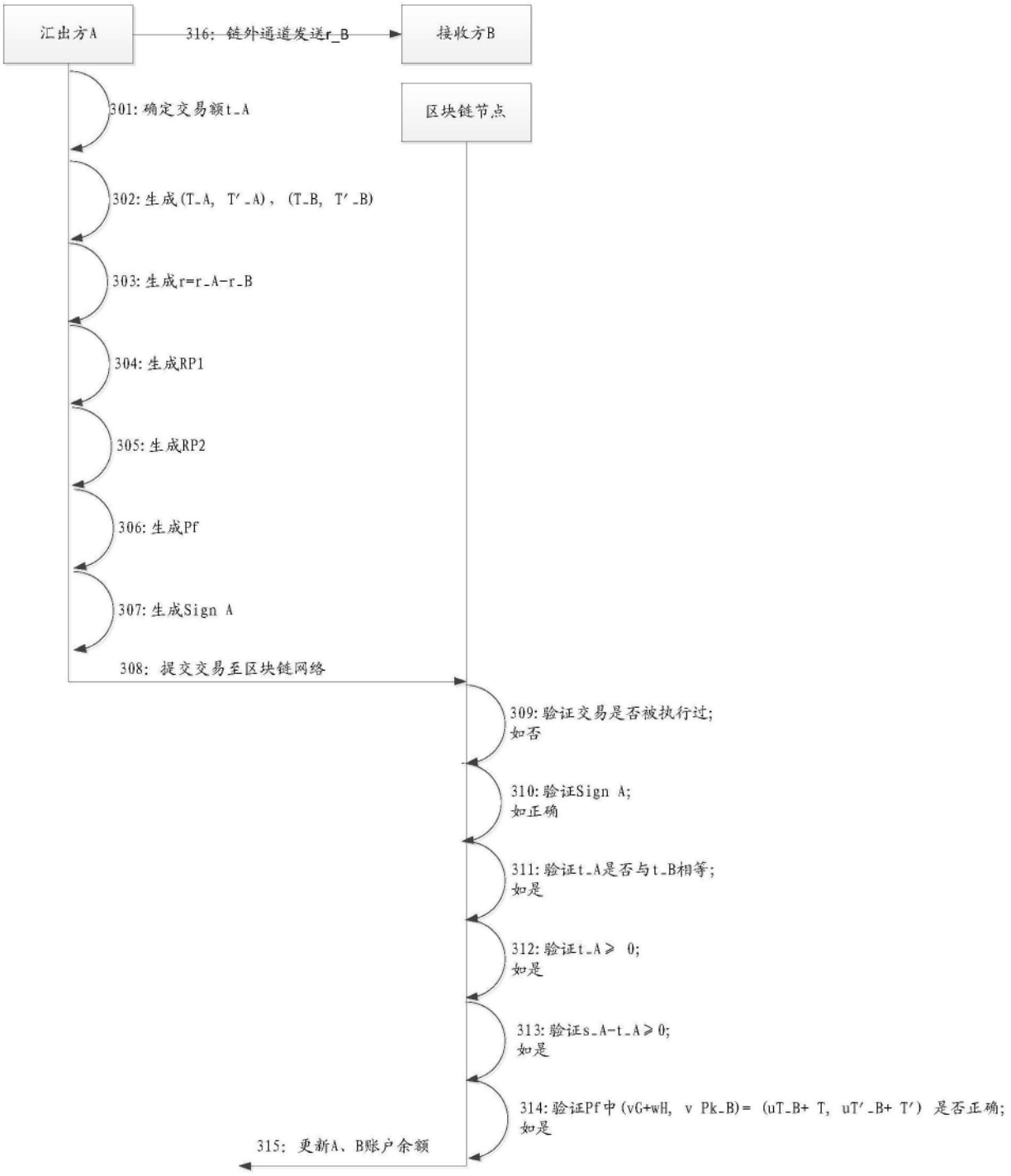

汇出方A
316：链外通道发送r_B
接收方B
区块链节点
301：确定交易额t_A
302：生成(T_A，T′_A)，(T_B，T′_B)
303：生成r=r_A-r_B
304：生成RP1
305：生成RP2
306：生成Pf
307：生成Sign A
308：提交交易至区块链网络
309：验证交易是否被执行过；
如否
310：验证Sign A；
如正确
311：验证t_A是否与t_B相等；
如是
312：验证t_A≥ 0；
如是
313：验证s_A-t_A≥0；
如是
314：验证Pf中(vG+wH，v Pk_B)=(uT_B+ T，uT′_B+ T′)是否正确；
如是
315：更新A、B账户余额

图3

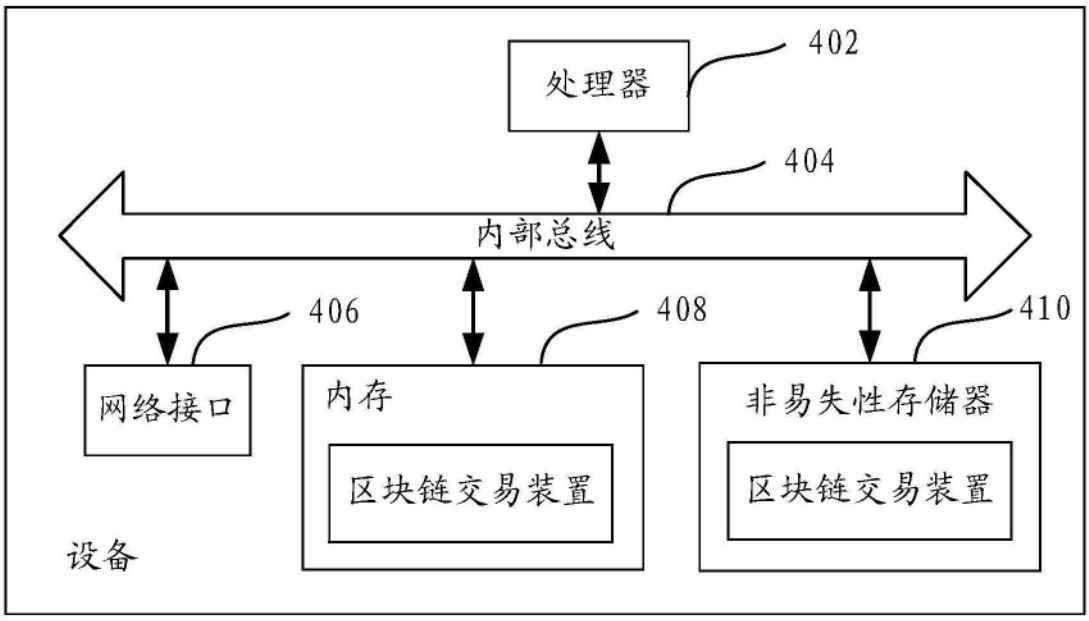

处理器
402
404
内部总线
406
408
410
网络接口
内存
区块链交易装置
非易失性存储器
区块链交易装置
设备

图4

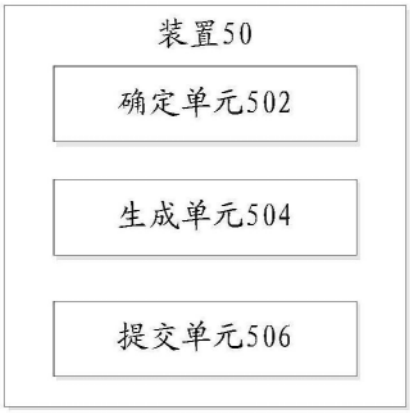

装置50
确定单元502
生成单元504
提交单元506

图5