(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110458561 A
(43)申请公布日 2019.11.15

(21)申请号 201910704690.1

(22)申请日 2019.07.31

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 马环宇 马宝利

(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 李威

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
G06Q 40/04(2012.01)
H04L 9/00(2006.01)

权利要求书4页 说明书24页 附图12页

(54)发明名称

区块链网络中实现机密交易的方法及装置

(57)摘要

本说明书一个或多个实施例提供一种区块链网络中实现机密交易的方法及装置，该方法可以包括：确定汇款方与收款方之间的汇款额；根据汇款方账户中被选取的资产额承诺和每一被选取的资产额承诺对应的指定数量创建汇款交易，汇款交易包含汇款额对应的汇款额承诺、每一被选取的资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明；向区块链提交汇款交易，使得每一被选取的资产额承诺对应的统计数量在交易完成后减去相应的指定数量、汇款方账户的收入余额在交易完成后增加找零额承诺、收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加汇款额承诺。

CN 110458561 A

1.一种区块链网络中实现机密交易的方法,应用于汇款方设备;所述方法包括:

确定汇款方与收款方之间的汇款额,所述汇款方在区块链账本上存在对应的汇款方账户,所述汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量,其中相同资产额的资产具有相同的资产额承诺;

根据所述汇款方账户中被选取的资产额承诺和每一被选取的资产额承诺对应的指定数量创建汇款交易,所述汇款交易包含所述汇款额对应的汇款额承诺、每一被选取的资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明,所述资产总额为每一被选取的资产额承诺对应的资产额与相应的指定数量的加权和;

向区块链提交所述汇款交易,使得每一被选取的资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

2.根据权利要求1所述的方法,

所述汇款方账户所含的所有资产对应于同一预设取值的资产额;或,

所述汇款方账户包含多个资产组,每一资产组的所有资产对应于同一预设取值的资产额,且不同资产组的资产对应于不同预设取值的资产额。

3.根据权利要求1所述的方法,所述汇款方账户还包括被记录为主余额承诺的主余额;所述方法还包括:

创建充值交易,所述充值交易包含指定的至少一个取值的资产额承诺和相应的充值数量、用于证明所述主余额不小于充值额的区间证明,所述充值额为所述指定的至少一个取值的资产额承诺对应的资产额与相应的充值数量的加权和;

向区块链提交所述充值交易,使得所述汇款方账户中对应于所述指定的至少一个取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、所述汇款方账户的主余额在交易完成后减少所述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。

4.根据权利要求3所述的方法,还包括:

创建合并交易,所述合并交易包含指定的至少一个取值的资产额承诺和相应的合并数量;

向区块链提交所述合并交易,使得所述汇款方账户中对应于所述指定的至少一个取值的资产额承诺的统计数量在交易完成后减少相应的合并数量、所述主余额在交易完成后增加合并额承诺,和/或所述汇款方账户的收入余额在交易完成后清零、所述汇款方账户的主余额在交易完成后增加相应的收入余额承诺;其中,所述合并额承诺为所述指定的至少一个取值的资产额承诺与相应的合并数量的加权和。

5.根据权利要求3所述的方法,还包括:

根据所述汇款方与所述收款方之间的主余额交易额,生成主余额汇款交易,所述主余额汇款交易包含所述主余额交易额对应的主余额交易额承诺、用于证明所述主余额交易额非负且不大于所述主余额的区间证明;

向区块链提交所述主余额汇款交易,使得所述主余额在交易完成后扣除所述主余额交易额承诺、所述收款方账户的收入余额在交易完成后增加所述主余额交易额承诺。

6.根据权利要求1所述的方法，还包括：

创建充值交易，所述充值交易包含至少一个指定取值的资产额承诺和相应的充值数量、用于证明所述汇款方账户的收入余额不小于充值额的区间证明，所述充值额为所述指定取值的资产额承诺对应的资产额与充值数量的加权和；

向区块链提交所述充值交易，使得所述汇款方账户中对应于所述指定取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、所述汇款方账户的收入余额在交易完成后减少所述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。

7.一种区块链网络中实现机密交易的方法，应用于区块链节点；所述方法包括：

接收汇款交易，所述汇款交易包含汇款方与收款方之间的汇款额对应的汇款额承诺、至少一个资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为所述至少一个资产额承诺对应的资产额与相应的指定数量的加权和；其中，所述汇款方在区块链账本上对应的汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺；

执行所述汇款交易，使得所述汇款交易所含每一资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

8.根据权利要求7所述的方法，

所述汇款方账户所含的所有资产对应于同一预设取值的资产额；或，

所述汇款方账户包含多个资产组，每一资产组的所有资产对应于同一预设取值的资产额，且不同资产组的资产对应于不同预设取值的资产额。

9.根据权利要求7所述的方法，所述汇款方账户还包括被记录为主余额承诺的主余额；所述方法还包括：

接收充值交易，所述充值交易包含指定的至少一个取值的资产额承诺和相应的充值数量、用于证明所述主余额不小于充值额的区间证明，所述充值额为所述指定的至少一个取值的资产额承诺对应的资产额与相应的充值数量的加权和；

执行所述充值交易，使得所述汇款方账户中对应于所述指定的至少一个取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、所述汇款方账户的主余额在交易完成后减少所述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。

10.根据权利要求9所述的方法，还包括：

接收合并交易，所述合并交易包含指定的至少一个取值的资产额承诺和相应的合并数量；

执行所述合并交易，使得所述汇款方账户中对应于所述指定的至少一个取值的资产额承诺的统计数量在交易完成后减少相应的合并数量、所述主余额在交易完成后增加合并额承诺，和/或所述汇款方账户的收入余额在交易完成后清零、所述汇款方账户的主余额在交易完成后增加相应的收入余额承诺；其中，所述合并额承诺为所述指定的至少一个取值的资产额承诺与相应的合并数量的加权和。

11.根据权利要求9所述的方法，还包括：

接收主余额汇款交易，所述主余额汇款交易包含所述汇款方与所述收款方之间的主余额交易额对应的主余额交易额承诺、用于证明所述主余额交易额非负且不大于所述主余额的区间证明；

执行所述主余额汇款交易，使得所述主余额在交易完成后扣除所述主余额交易额承诺、所述收款方账户的收入余额在交易完成后增加所述主余额交易额承诺。

12.根据权利要求7所述的方法，还包括：

接收充值交易，所述充值交易包含至少一个指定取值的资产额承诺和相应的充值数量、用于证明所述汇款方账户的收入余额不小于充值额的区间证明，所述充值额为所述指定取值的资产额承诺对应的资产额与充值数量的加权和；

执行所述充值交易，使得所述汇款方账户中对应于所述指定取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、所述汇款方账户的收入余额在交易完成后减少所述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。

13.一种区块链网络中实现机密交易的装置，应用于汇款方设备；所述装置包括：

确定单元，确定汇款方与收款方之间的汇款额，所述汇款方在区块链账本上存在对应的汇款方账户，所述汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺；

创建单元，根据所述汇款方账户中被选取的资产额承诺和每一被选取的资产额承诺对应的指定数量创建汇款交易，所述汇款交易包含所述汇款额对应的汇款额承诺、每一被选取的资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为每一被选取的资产额承诺对应的资产额与相应的指定数量的加权和；

提交单元，向区块链提交所述汇款交易，使得每一被选取的资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

14.一种区块链网络中实现机密交易的装置，应用于区块链节点；所述装置包括：

接收单元，接收汇款交易，所述汇款交易包含汇款方与收款方之间的汇款额对应的汇款额承诺、至少一个资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为所述至少一个资产额承诺对应的资产额与相应的指定数量的加权和；其中，所述汇款方在区块链账本上对应的汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺；

执行单元，执行所述汇款交易，使得所述汇款交易所含每一资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

15.一种电子设备，其特征在于，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1-6中任一项所述的方法。

16.一种计算机可读存储介质，其上存储有计算机指令，其特征在于，该指令被处理器执行时实现如权利要求1-6中任一项所述方法的步骤。

17.一种电子设备，其特征在于，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7-12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，其特征在于，该指令被处理器执行时实现如权利要求7-12中任一项所述方法的步骤。

区块链网络中实现机密交易的方法及装置

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网络中实现机密交易的方法及装置。

背景技术

[0002] 区块链技术(也被称之为，分布式账本技术)是一种去中性化的分布式数据库技术，具有去中心化、公开透明、不可篡改、可信任等多种特点，适用于诸多对数据可靠性具有高需求的应用场景中。

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网络中实现机密交易的方法及装置。

[0004] 为实现上述目的，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，提出了一种区块链网络中实现机密交易的方法，应用于汇款方设备；所述方法包括：

[0006] 确定汇款方与收款方之间的汇款额，所述汇款方在区块链账本上存在对应的汇款方账户，所述汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺；

[0007] 根据所述汇款方账户中被选取的资产额承诺和每一被选取的资产额承诺对应的指定数量创建汇款交易，所述汇款交易包含所述汇款额对应的汇款额承诺、每一被选取的资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为每一被选取的资产额承诺对应的资产额与相应的指定数量的加权和；

[0008] 向区块链提交所述汇款交易，使得每一被选取的资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

[0009] 根据本说明书一个或多个实施例的第二方面，提出了一种区块链网络中实现机密交易的方法，应用于区块链节点；所述方法包括：

[0010] 接收汇款交易，所述汇款交易包含汇款方与收款方之间的汇款额对应的汇款额承诺、至少一个资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为所述至少一个资产额承诺对应的资产额与相应的指定数量的加权和；其中，所述汇款方在区块链账本上对应的汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺；

[0011] 执行所述汇款交易，使得所述汇款交易所含每一资产额承诺对应的统计数量在交

易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

[0012] 根据本说明书一个或多个实施例的第三方面，提出了一种区块链网络中实现机密交易的装置，应用于汇款方设备；所述装置包括：

[0013] 确定单元，确定汇款方与收款方之间的汇款额，所述汇款方在区块链账本上存在对应的汇款方账户，所述汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺；

[0014] 创建单元，根据所述汇款方账户中被选取的资产额承诺和每一被选取的资产额承诺对应的指定数量创建汇款交易，所述汇款交易包含所述汇款额对应的汇款额承诺、每一被选取的资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为每一被选取的资产额承诺对应的资产额与相应的指定数量的加权和；

[0015] 提交单元，向区块链提交所述汇款交易，使得每一被选取的资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

[0016] 根据本说明书一个或多个实施例的第四方面，提出了一种区块链网络中实现机密交易的装置，应用于区块链节点；所述装置包括：

[0017] 接收单元，接收汇款交易，所述汇款交易包含汇款方与收款方之间的汇款额对应的汇款额承诺、至少一个资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为所述至少一个资产额承诺对应的资产额与相应的指定数量的加权和；其中，所述汇款方在区块链账本上对应的汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺；

[0018] 执行单元，执行所述汇款交易，使得所述汇款交易所含每一资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

[0019] 根据本说明书一个或多个实施例的第五方面，提出了一种电子设备，包括：

[0020] 处理器；

[0021] 用于存储处理器可执行指令的存储器；

[0022] 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。

[0023] 根据本说明书一个或多个实施例的第六方面，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。

[0024] 根据本说明书一个或多个实施例的第七方面，提出了一种电子设备，包括：

[0025] 处理器；

[0026] 用于存储处理器可执行指令的存储器；

[0027] 其中，所述处理器通过运行所述可执行指令以实现如第二方面所述的方法。

[0028] 根据本说明书一个或多个实施例的第八方面，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二方面所述方法的步骤。

附图说明

[0029] 图1是一示例性实施例提供的一种示例环境的示意图。

[0030] 图2是一示例性实施例提供的一种概念架构的示意图。

[0031] 图3是一示例性实施例提供的一种区块链网络中实现机密交易的方法的流程图。

[0032] 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。

[0033] 图5是一示例性实施例提供的一种隐私保护的汇款交易的流程图。

[0034] 图6是一示例性实施例提供的一种汇款前后的账户变化情况的示意图。

[0035] 图7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。

[0036] 图8是一示例性实施例提供的一种通过主余额进行资产充值的交互示意图。

[0037] 图9是一示例性实施例提供的一种充值前后的账户变化情况的示意图。

[0038] 图10是一示例性实施例提供的一种合并操作的交互示意图。

[0039] 图11是一示例性实施例提供的一种合并前后的账户变化情况的示意图。

[0040] 图12是一示例性实施例提供的一种主余额转账交易的流程图。

[0041] 图13是一示例性实施例提供的一种主余额汇款前后的账户变化情况的示意图。

[0042] 图14是一示例性实施例提供的另一种区块链网络中实现机密交易的方法的流程图。

[0043] 图15是一示例性实施例提供的一种设备的结构示意图。

[0044] 图16是一示例性实施例提供的一种区块链网络中实现机密交易的装置的框图。

[0045] 图17是一示例性实施例提供的另一种设备的结构示意图。

[0046] 图18是一示例性实施例提供的另一种区块链网络中实现机密交易的装置的框图。

具体实施方式

[0047] 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。

[0048] 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。

[0049] 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。

[0050] 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。

[0051] 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。

[0052] 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。

[0053] 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。

[0054] 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。

[0055] 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。

[0056] 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。

[0057] 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。

[0058] 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。

[0059] 区块链一般被划分为三种类型:公有链(Public Blockchain),私有链(Private Blockchain)和联盟链(Consortium Blockchain)。此外,还有多种类型的结合,比如私有链+联盟链、联盟链+公有链等不同组合形式。其中去中心化程度最高的是公有链。公有链以比特币、以太坊为代表,加入公有链的参与者可以读取链上的数据记录、参与交易以及竞争新区块的记账权等。而且,各参与者(即节点)可自由加入以及退出网络,并进行相关操作。私有链则相反,该网络的写入权限由某个组织或者机构控制,数据读取权限受组织规定。简单来说,私有链可以为一个弱中心化系统,参与节点具有严格限制且少。这种类型的区块链更适合于特定机构内部使用。联盟链则是介于公有链以及私有链之间的区块链,可实现“部分去中心化”。联盟链中各个节点通常有与之相对应的实体机构或者组织;参与者通过授权加入网络并组成利益相关联盟,共同维护区块链运行。

[0060] 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。

[0061] 通过区块链网络所采用的分布式架构,以及区块所采用的链式结构,使得信息可以永久、无篡改地记录在各个区块链节点统一维护的区块链账本中。但是,由于区块链账本完全公开,导致信息隐私性无法得到保障。例如,任意用户可以在任意区块链节点上查询区块链账本,以获知某一用户持有的资产、某一交易的转账额等信息,而这些可能都是敏感的、需要隐藏的信息。因此,相关技术中提出了基于承诺的机密交易(Confidential Transaction)方案,可以将区块链账本中记录的账户余额、资产额、交易的汇款额等敏感数据均转换为相应的承诺数额,而避免在区块链账本中直接记载这些敏感数据的明文数额。例如,当采用Pedersen承诺机制时,假定原始数额为t,相应的承诺数额可以为PC(r,t)=r×G+t×H,其中G、H为椭圆曲线的生成元,r为随机数,并且r的取值仅由私人(如账户拥有者、资产持有者、交易参与者等)掌握,使得无关人员仅根据PC(r,t)的取值将无法反推出原始数额t。同时,承诺数额还具有同态特性,譬如PC(r1,t1)-PC(r2,t2)=PC(r1-r2,t1-t2),使得承诺数额之间可以直接参与交易过程中的计算。

[0062] 具体的,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。

[0063] 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。但是，UTXO模型会导致区块链网络中的资产数量远大于用户数量，可能对区块链存储造成极大的挑战；同时，如前所述，UTXO模型对智能合约的支持很弱，限制了UTXO模型能够使用的场景。

[0064] 虽然账户模型可以解决UTXO模型对区块链存储造成的挑战，以及通过对智能合约的支持而扩展更多的应用场景，但是：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，否则交易会因为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。

[0065] 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提出了改进，以使其能够适应于高吞吐量的并发交易。下面结合实施例对本说明书的相关方案进行介绍。

[0066] 图3是一示例性实施例提供的一种区块链网络中实现机密交易的方法的流程图。如图3所示，该方法应用于汇款方设备，可以包括以下步骤：

[0067] 步骤302，确定汇款方与收款方之间的汇款额，所述汇款方在区块链账本上存在对应的汇款方账户，所述汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺。

[0068] 汇款额可以由汇款方与收款方之间协商确定，也可以由汇款方自行确定。基于已确定的汇款额，可以从汇款方账户中选取恰当的资产，以用于支付该汇款额。

[0069] 汇款方对应于汇款方账户、收款方对应于收款方账户，汇款方账户与收款方账户均记录于区块链账本中。区块链网络中的每一区块链节点分别维护有一份区块链账本，而基于共识机制可以确保所有区块链节点维护的区块链账本的内容一致，因而可以认为所有区块链节点共同维护了一份区块链账本。

[0070] 如前所述，本说明书针对相关技术中的账户模型进行了改进。例如，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。假定汇款方账户为如图4所示的账户A，该账户A包括收入余额和资产信息。其中，收入余额的明文数额为Au，而出于保密的目的，在区块链账本上具体记录为相应的收入余额承诺PC(Au,r_Au)，其中r_Au为随机数。

[0071] 资产信息用于记录汇款方所持有的资产，该资产是基于汇款方所持有的余额而生成，区别于UTXO模型中的交易输出。比如，基于汇款方持有的明文数额为t_a_1的余额，可以结合随机数r_a_1生成相应的承诺数额PC(t_a_1,r_a_1)，相当于汇款方持有一份资产额为t_a_1、资产额承诺为PC(t_a_1,r_a_1)的资产；类似地，可以基于汇款方持有的明文数额为

t_a_2的余额和随机数r_a_2生成相应的承诺数额PC(t_a_2,r_a_2)，相当于汇款方持有一份资产额为t_a_2、资产额承诺为PC(t_a_2,r_a_2)的资产；以此类推，可以生成其他的具有相同或不同资产额的资产。

[0072] 对于具有相同资产额的不同资产而言，本说明书中可以限定同一取值的资产额必然选取相同的随机数，譬如上述资产额t_a_1必然对应于随机数r_a_1、资产额t_a_2必然对应于随机数r_a_2，使得同一取值的资产额必然对应于相同取值的资产额承诺，比如资产额t_a_1必然对应于资产额承诺PC(t_a_1,r_a_1)、资产额t_a_2必然对应于资产额承诺PC(t_a_2,r_a_2)。因此，汇款方账户所含的资产信息可以具体包含各个取值的资产额承诺和每一取值的资产额承诺的统计数量，比如图4所示的账户A中，资产额承诺PC(t_a_1,r_a_1)对应的统计数量为n1、资产额承诺PC(t_a_2,r_a_2)对应的统计数量为n2，即汇款方持有n1个取值为PC(t_a_1,r_a_1)的资产额承诺、n2个取值为PC(t_a_2,r_a_2)的资产额承诺。这样，相当于将汇款方账户所含的资产进行了组别划分，每一资产组的所有资产对应于同一预设取值的资产额(或资产额承诺)，且不同资产组的资产对应于不同预设取值的资产额(或资产额承诺)；当然，所有资产可以对应于同一预设取值的资产额(或资产额承诺)，相当于仅存在一个资产组。

[0073] 基于上述方式记录汇款方账户所含的资产，只需要记录各个资产组对应的资产额承诺和每一资产组对应的统计数量，譬如图4中的一个资产组对应的资产额承诺为PC(t_a_1,r_a_1)、统计数量为n1，另一个资产组对应的资产额承诺为PC(t_a_2,r_a_2)、统计数量为n2，而无需分别记录每一资产的详细信息，使得资产发生增减变化时仅需调整对应的统计数量的取值，可以极大地降低资产信息的维护成本，有助于缓解存储压力。

[0074] 与汇款方账户相类似的，收款方账户同样包含收入余额和资产信息，收入余额被记录为收入余额承诺，资产信息包括资产额承诺的各个取值及其统计数量，其中相同资产额的资产具有相同的资产额承诺，此处不再赘述。

[0075] 步骤304，根据所述汇款方账户中被选取的资产额承诺和每一被选取的资产额承诺对应的指定数量创建汇款交易，所述汇款交易包含所述汇款额对应的汇款额承诺、每一被选取的资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为每一被选取的资产额承诺对应的资产额与相应的指定数量的加权和。

[0076] 根据汇款方与收款方之间的汇款额，可以选取汇款方账户所含的一个或多个资产额承诺，以及每一被选取的资产额承诺对应的指定数量。比如，当汇款额为t时，如果选取的资产额承诺分别为PC(t_a_1,r_a_1)和PC(t_a_2,r_a_2)，且对应的指定数量分别为x1和x2，那么可以确定资产总额为(t_a_1*x1+t_a_2*x2)，并且应当确保0≤t≤(t_a_1*x1+t_a_2*x2)；具体的，可以生成用于证明汇款额非负且不大于资产总额的区间证明，从而在不暴露汇款额和资产总额的明文数值的情况下，即可基于该区间证明来验证是否满足0≤t≤(t_a_1*x1+t_a_2*x2)。

[0077] 步骤306，向区块链提交所述汇款交易，使得每一被选取的资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

[0078] 汇款交易被提交至区块链后，可由某一区块链节点将该汇款交易打包至区块中，该区块在经过共识后被添加至区块链中，使得该区块所含的上述汇款交易在所有区块链节点上被执行。当然，区块链节点可以针对汇款交易进行验证，比如验证汇款方、收款方的签名、验证上述的区间证明等，从而在通过验证后允许执行该汇款交易，否则可以解决执行。

[0079] 汇款交易的输入来自汇款方账户中的资产，而输出包括两个部分：一部分的输出目标为收款方账户、输出额为汇款额(实际记录为汇款额承诺)，另一部分的输出目标为收款方账户、输出额为找零额(实际记录为找零额承诺)。其中，找零额为上述的资产总额与汇款额之差；比如，当资产总额为(t_a_1*x1+t_a_2*x2)、汇款额为t时，可以确定找零额t’＝t_a_1*x1+t_a_2*x2-t，找零额承诺为PC(t’,r’)，r’为随机数。

[0080] 可见，基于本说明书改进后的账户模型，收入余额专用于实现收款(作为汇款方时用于汇入找零额，作为收款方时用于汇入汇款额)、资产专用于实现汇款，可以实现同一账户的收款与汇款之间的解耦，因而可使一个用户作为汇款交易TX1的汇款方、作为汇款交易TX2的收款方而同时参与至汇款交易TX1和TX2中，实现了账户模型下的交易并发，可以提升区块链网络中的交易执行效率。

[0081] 同时，由于在生成上述汇款额与资产总额之间的区间证明时，资产总额的取值仅与被选取的资产额承诺及其指定数量相关，并不涉及区块链账本上记录的各个资产额承诺的统计数量，使得不同汇款交易可以分别生成相应的区间证明且互不影响。进一步的，由于在区块链账本上对各个取值的资产额承诺的统计数量采用明文形式进行记录，使得区块链节点可以对汇款交易中包含的指定数量与区块链账本上记录的统计数量进行直接比较：若指定数量不大于统计数量，则允许执行相应的汇款交易，否则不允许执行。因此，同一用户可以同时作为多个汇款交易的汇款方，以实现账户模型下的交易并发，可以提升区块链网络中的交易执行效率；以及，当在后生成的汇款交易优先到达区块链节点时，区块链节点可以优先处理该在后生成的汇款交易，而无需等待在先生成的汇款交易执行完成，避免了区块链节点处的交易阻塞。

[0082] 下面以作为汇款方的用户A、作为收款方的用户B为例，对本说明书的汇款交易的实施过程进行描述。图5是一示例性实施例提供的一种隐私保护的汇款交易的流程图；如图5所示，汇款方、收款方和区块链节点之间的交互过程可以包括以下步骤：

[0083] 步骤501，汇款方确定汇款额t。

[0084] 在起草汇款交易时，汇款额t可由汇款方与收款方之间进行协商。当然，汇款方也可以自行确定汇款额t，由收款方在后续步骤中予以确认。其中，汇款方是指汇款交易中对款项、资产等资源进行汇出的角色，相应地收款方是指汇款交易中对款项、资产等资源进行接收的角色。例如，用户A向用户B进行汇款时，用户A为汇款方、用户B为收款方；同时，当用户B向用户A进行汇款时，用户B为汇款方、用户A为收款方。因此，汇款方、收款方的角色与用户之间并不存在绑定关系，需要根据实际的汇款关系来确定。

[0085] 假定用户A作为汇款方、用户B作为收款方，由用户A向用户B进行汇款。图6是一示例性实施例提供的一种汇款前后的账户变化的示意图。如图6所示，假定用户A在区块链账本上存在相应的账户A、用户B在区块链账本上存在相应的账户B。如前所述，账户A可以包括收入余额和资产信息，其中收入余额被记录为PC(Au,r_Au)、资产信息被记录为[n1,PC(t_a_1,r_a_1)]和[n2,PC(t_a_2,r_a_2)]等，表明账户A中对应于资产额承诺PC(t_a_1,r_a_

1)的资产的统计数量为n1、对应于资产额承诺PC(t_a_2,r_a_2)的资产的统计数量为n2等。类似地,账户B可以包括收入余额和资产信息,其中收入余额被记录为PC(Bu,r_Bu)、资产信息被记录为[m1,PC(t_b_1,r_b_1)]和[m2,PC(t_b_2,r_b_2)]等,表明账户B中对应于资产额承诺PC(t_b_1,r_b_1)的资产的统计数量为m1、对应于资产额承诺PC(t_b_2,r_b_2)的资产的统计数量为m2等。

[0086] 步骤502,汇款方确定汇款额t对应的随机数r。

[0087] 汇款方为汇款额t产生随机数r后,可以根据随机数r对汇款额t进行处理得到相应的汇款额承诺T=PC(t,r)。例如,当采用Pedersen承诺机制时,T=PC(t,r)=r*G+t*H。

[0088] 步骤503,汇款方通过链下通道将(r,t,T)发送至收款方。

[0089] 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除汇款方和收款方之外不可知。

[0090] 步骤504,收款方对收到的(r,t,T)进行验证。

[0091] 收款方可以对汇款额t进行验证,以确定为希望收取的汇款数额。例如,当汇款额承诺T是基于Perdersen承诺机制而生成时,收款方可以对汇款额承诺T进行验证的过程,即收款方可以通过Perdersen承诺机制对随机数r和汇款额t进行计算,以验证汇款额承诺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。

[0092] 步骤505,收款方在验证通过后,生成签名并返回至汇款方。

[0093] 在验证通过后,收款方可以利用收款方私钥对(A,B:T)进行签名,生成签名SigB并返回至汇款方。该签名SigB表明收款方同意由汇款方对应的账户A向收款方对应的账户B实施汇款额承诺为T的汇款交易。

[0094] 步骤506,在收到签名SigB后,汇款方根据选取的资产额承诺和指定数量生成区间证明PR。

[0095] 如前所述,诸如图6所示的账户A中包含若干资产额承诺及其对应的统计数量,比如资产额承诺PC(t_a_1,r_a_1)对应的统计数量为n1、资产额承诺PC(t_a_2,r_a_2)对应的统计数量为n2。与汇款额t相类似的,资产额承诺PC(t_a_1,r_a_1)是根据资产额t_a_1和随机数r_a_1进行计算得到、资产额承诺PC(t_a_2,r_a_2)是根据资产额t_a_2和随机数r_a_2进行计算得到。同时,本说明书中在计算资产额对应的资产额承诺时,限定为:当不同资产的资产额相同时,相应选取的随机数也相同,以确保这些资产额相同的多份资产可以对应产生相同的资产额承诺,因而使得同一账户内存在多份对应于同一资产额承诺的资产,并且不需要具体关注、记录和区分这些资产,只需要记录资产额承诺的取值和资产数量(即统计数量)即可。而花费这些资产时,只需要确定被花费的资产对应的资产额承诺,并基于花费情况对相应的统计数量进行调整即可,下文将对此进行详述。

[0096] 根据汇款额t的取值,可以选取恰当的资产组合,以满足汇款需求。假定汇款额t=215,t_a_1=20、t_a_2=100,那么可以选取1份资产额为t_a_1的资产、2份资产额为t_a_2的资产,组合得到t_a_1+t_a_2*2=220>t=215,可以满足汇款需求。因此,汇款方可以选取资产额承诺PC(t_a_1,r_a_1)和资产额承诺PC(t_a_2,r_a_2),并设置资产额承诺PC(t_a_1,r_a_1)对应的指定数量为x1=1、资产额承诺PC(t_a_2,r_a_2)对应的指定数量为x2=2。

[0097] 而相应地,汇款方可以根据被选取的资产额承诺PC(t_a_1,r_a_1)和资产额承诺

PC(t_a_2,r_a_2)、对应的指定数量x1和x2，以及汇款额t，生成区间证明PR，该区间证明PR用于证明：0≤t≤(t_a_1*x1+t_a_2*x2)。本说明书中可以采用相关技术中的Bulletproofs方案、Borromean环签名方案等生成上述的区间证明，本说明书并不对此进行限制；而区块链节点可以在密文状态下验证上述的“0≤t≤(t_a_1*x1+t_a_2*x2)”是否成立，既可以确保汇款交易符合条件，又可以避免暴露汇款额t、资产额t_a_1、资产额t_a_2等的明文取值。

[0098] 同时，根据上述区间证明PR的生成过程，可以确定：区间证明PR与账户A中各个资产额承诺的统计数量无关，因而除了上述的汇款交易之外，账户A还可以同时参与其他汇款交易，并且均能够顺利生成区间证明而不会相互影响，从而实现并发交易。

[0099] 步骤507，汇款方对交易内容{A,B:T,[PC(t_a_1,r_a_1),x1;PC(t_a_2,r_a_2),x2],PR;SigB}进行签名，生成签名SigA。

[0100] 汇款方可以利用汇款方私钥对交易内容{A,B:T,[PC(t_a_1,r_a_1),x1;PC(t_a_2,r_a_2),x2],PR;SigB}进行签名，生成签名SigA。

[0101] 步骤508，汇款方向区块链提交交易。

[0102] 汇款方可以将汇款交易提交至区块链网络中的某一区块链节点，该汇款交易还可以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。

[0103] 步骤509，区块链节点检查交易是否执行过。

[0104] 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509～512等实施验证等操作。

[0105] 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510。

[0106] 步骤510，区块链节点检查签名。

[0107] 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511。

[0108] 步骤511，区块链节点检查区间证明PR。

[0109] 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≤t≤(t_a_1*x1+t_a_2*x2)。如果不满足，可以拒绝执行该汇款交易，否则转入步骤512。

[0110] 步骤512，区块链节点检查统计数量是否不小于指定数量。

[0111] 由于账户A中各个资产额承诺对应的统计数量以明文形式记录于区块链账本上，且指定数量也以明文形式记录于汇款交易中，使得区块链节点可以直接将统计数量与指定数量进行比较，以确定账户A是否足够支付。以图6所示，由于资产额承诺PC(t_a_1,r_a_1)的统计数量为n1、资产额承诺PC(t_a_2,r_a_2)的统计数量为n2，而汇款交易中资产额承诺PC(t_a_1,r_a_1)对应的指定数量为x1、资产额承诺PC(t_a_2,r_a_2)对应的指定数量为x2，因而只要确定n1≥x1、n2≥x2，即表明账户A足够支付，可以完成汇款交易。

[0112] 同时，由于采用明文比较，因而不需要在汇款交易中添加账户A足够支付的区间证明，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。

[0113] 步骤513,区块链节点在维护的区块链账本中更新用户A、用户B分别对应的账户。

[0114] 在通过步骤509～512的验证后,区块链节点可以分别对区块链账本中记载的账户A、账户B进行更新,如图6所示:

[0115] 在账户A中,交易前的收入余额为Au、在区块链账本中被记录为相应的收入余额承诺PC(Au,r_Au),交易前资产额承诺PC(t_a_1,r_a_1)对应的统计数量为n1、资产额承诺PC(t_a_2,r_a_2)对应的统计数量为n2。在交易完成后,资产额承诺PC(t_a_1,r_a_1)对应的统计数量减小x1、更新为n1-x1,而资产额承诺PC(t_a_2,r_a_2)对应的统计数量减小x2、更新为n2-x2;同时,收入余额增加了找零额t'、对应于找零额承诺PC(t',r'),因而在区块链账本中记录的收入余额承诺更新为PC(Au,r_Au)+PC(t',r')。需要指出的是:虽然上文中并未具体描述,但找零额承诺PC(t',r')也被包含于上述的汇款交易中,使得区块链节点在执行该汇款交易时,可以根据找零额承诺PC(t',r')对账户A的收入余额进行更新。

[0116] 在账户B中,交易前的收入余额为Bu、在区块链账本中被记录为相应的收入余额承诺PC(Bu,r_Bu),交易前资产额承诺PC(t_b_1,r_b_1)对应的统计数量为m1、资产额承诺PC(t_b_2,r_b_2)对应的统计数量为m2。在交易完成后,统计数量m1和m2不变,而收入余额Bu则增加了汇款额t,因而在区块链账本中被记录为相应的收入余额承诺PC(Bu,r_Bu)+PC(t,r)。

[0117] 如上文所述,当账户包含上述的收入余额和资产信息时,可以在保障交易隐私的情况下,实现账户的输入与输出解耦,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、而汇出的资金都从资产信息中扣除(减小统计数量的取值),因而统计数量的取值(即账户内的资产)在不断下降,可能小于汇款交易中的指定数量而影响到汇款交易的执行。为了确保统计数量的数额总是能够处于充足状态、足够完成交易,可以定期或随时通过充值调整统计数量的数额。

[0118] 以汇款方账户的充值过程为例。可以创建充值交易,该充值交易包含至少一个指定取值的资产额承诺和相应的充值数量、用于证明汇款方账户的收入余额不小于充值额的区间证明,该充值额为指定取值的资产额承诺对应的资产额与充值数量的加权和(如果仅涉及到一个指定取值的资产额承诺,则充值额为该资产额承诺对应的资产额与充值数量的乘积);向区块链提交充值交易,使得汇款方账户中对应于上述指定取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、汇款方账户的收入余额在交易完成后减少上述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。换言之,可以将汇款方账户中的收入余额划分出至少一部分,将这部分余额转换为相应的资产,这些资产可使对应的资产额承诺的统计数量实现取值增大。当然,收款方账户也可以采用上述方式进行充值。

[0119] 虽然可以按照上述方式实现基于收入余额的资产充值操作,但是当账户参与的汇款交易较为频繁、汇款额较大时,可能导致频繁充值,造成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(其他账户向该账户进行汇款的交易)与充值交易之间相应影响,反而造成效率下降。

[0120] 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7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。仍以账户A为例,在图4所示账户结构的基础上,除了包含收入余额和资产信息之外,图7所示的账户A可以进一步包含主余额,即账户A总共包含三部分:主余额、收入余额和资产信息。其中,收入余额专用于收取汇入交易的交

易额、资产信息专用于参与汇出交易，而主余额用于对资产信息进行充值，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。

[0121] 以汇款方为例。汇款方可以创建充值交易，该充值交易包含指定的至少一个取值的资产额承诺和相应的充值数量、用于证明主余额不小于充值额的区间证明，充值额为上述指定的至少一个取值的资产额承诺对应的资产额与相应的充值数量的加权和；向区块链提交充值交易，使得汇款方账户中对应于上述指定的至少一个取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、汇款方账户的主余额在交易完成后减少上述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。例如，图8是一示例性实施例提供的一种通过主余额进行资产充值的交互示意图。如图8所示，该交互过程可以包括以下步骤：

[0122] 步骤801，汇款方确定指定取值的资产额和充值数量。

[0123] 汇款方可以设置指定取值的资产额和充值数量，比如取值为100的资产额对应的充值数量为3、取值为20的资产额对应的充值数量为5，那么可以确定本次总共的充值额h＝100*3+20*5＝400。

[0124] 汇款方可以确定账户中已存在的资产额承诺对应的资产额，并将其中的一个或多个资产额作为上述的指定取值的资产额，使得这些已存在的资产额承诺对应的统计数量在完成充值后可以相应增加。或者，汇款方可以设置与已有资产额承诺所对应的资产额不同的其他资产额，比如当账户中已存在取值为100的资产对应的资产额承诺、取值为20的资产对应的资产额承诺时，可以设定上述的指定取值为50，从而充值得到取值为50的资产对应的资产额承诺，而账户所含的资产信息中可以新增该取值为50的资产对应的资产额承诺的统计数量。

[0125] 虽然汇款方可以手动发起充值交易，但是在一实施例中可以实现自动化的充值操作。例如，可以为账户中各个取值的资产额承诺的统计数量设定水位值，当某一取值的资产额承诺对应的统计数量低于相应的水位值时，可以自动发起充值交易，对该取值的资产额承诺进行充值，以使得相应的统计数量上升至不低于水位值。

[0126] 步骤802，汇款方生成区间证明PR。

[0127] 在一实施例中，由于主余额的取值Az在区块链账本中记录为相应的承诺数额PC(Az,r_Az)，其中r_Az为随机数，因而需要通过生成区间证明PR，以用于验证主余额的取值Az≥充值额h≥0。

[0128] 步骤803，汇款方对交易签名后，提交至区块链。

[0129] 基于上述步骤，汇款方生成的充值交易的交易内容可以为Topup{A:[PC(t_a_1,r_a_1),y1;PC(t_a_2,r_a_2),y2],PR}，“A”代表该账户A的账户地址，[PC(t_a_1,r_a_1),y1;PC(t_a_2,r_a_2),y2]表明充值目标为账户A所含的资产额承诺PC(t_a_1,r_a_1)的充值数量为y1、资产额承诺PC(t_a_2,r_a_2)的充值数量为y2。

[0130] 同时，交易中可以增加一类型字段，而汇款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汇款交易、充值交易以及下文所述的合并交易、主余额汇款交易等进行区分。例如，可以通过取值“Transfer”来标注汇款交易，并可以通过取值“Topup”来标注充值交易。

[0131] 汇款方采用持有的汇款方私钥对上述的交易内容Topup{A:[PC(t_a_1,r_a_1),

y1;PC(t_a_2,r_a_2),y2],PR}进行签名,并将签名后创建的充值交易提交至区块链网络,以由所有区块链节点进行验证和执行。

[0132] 步骤804,区块链节点验证交易。

[0133] 区块链节点可以验证上述充值交易的签名是否正确;如果不正确,可以拒绝执行该交易。

[0134] 区块链节点可以验证上述充值交易所含的区间证明PR,以确定是否满足0≤(t_a_1*y1+t_a_2*y2)≤Az;如果不正确,可以拒绝执行该交易。

[0135] 当所有验证均通过后,可以转入步骤805。

[0136] 步骤805,区块链节点更新账户。

[0137] 在通过步骤804的验证后,区块链节点可以对区块链账本中记载的账户A进行更新。例如,图9是一示例性实施例提供的一种充值前后的账户变化情况的示意图。如图9所示:

[0138] 交易前的主余额为Az、在区块链账本中被记录为相应的承诺数额PC(Az,r_Az),交易前的收入余额为Au、在区块链账本中被记录为相应的承诺数额PC(Au,r_Au),交易前的资产额承诺PC(t_a_1,r_a_1)对应于统计数量n1、资产额承诺PC(t_a_2,r_a_2)对应于统计数量n2。

[0139] 在交易完成后,主余额被扣除了(t_a_1*y1+t_a_2*y2),即前述各个取值的资产额与充值数量的加权和,因而在区块链账本中被记录为PC(Az,r_Az)-PC(t_a_1,r_a_1)*y1-PC(t_a_2,r_a_2)*y2,而资产信息中的统计数量n1增加了充值数量y1、统计数量n2增加了充值数量y2,因而在区块链账本中以明文形式记录为[n1+y1,PC(t_a_1,r_a_1)]和[n2+y2,PC(t_a_2,r_a_2)];同时,收入余额的取值不变。

[0140] 随着账户中的资产信息不断参与汇出交易,而主余额不断向资产信息进行充值,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,将无法继续充值,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。

[0141] 以汇款方为例。汇款方可以创建合并交易,该合并交易包含指定的至少一个取值的资产额承诺和相应的合并数量;然后,向区块链提交该合并交易,使得汇款方账户中对应于上述指定的至少一个取值的资产额承诺的统计数量在交易完成后减少相应的合并数量、主余额在交易完成后增加合并额承诺,和/或汇款方账户的收入余额在交易完成后清零、汇款方账户的主余额在交易完成后增加相应的收入余额承诺;其中,合并额承诺为上述指定的至少一个取值的资产额承诺与相应的合并数量的加权和。换言之,合并交易可以将收入余额所含的资金全部并入主余额,或者在一些情况下可以将至少一部分资产以资金形式并入主余额,或者还可以同时将收入余额所含的资金并入主余额、将至少一部分资产以资金形式并入主余额。例如,图10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10所示,该交互过程可以同时将收入余额中的全部资金和指定数额的资产并入主余额,具体包括以下步骤:

[0142] 步骤1001,汇款方确定资产额承诺和合并数量。

[0143] 通过选取一种或多种取值的资产额承诺以及每种资产额承诺对应的合并数量,可以确定汇款方希望合并至主余额的资产额。例如,当被选取的资产额承诺分别为PC(t_a_1,r_a_1)和PC(t_a_2,r_a_2)时,如果资产额承诺PC(t_a_1,r_a_1)对应的合并数量为z1、资

产额承诺PC(t_a_2,r_a_2)对应的合并数量为z2,那么可以确定相应的合并额为k＝t_a_1*z1+t_a_2*z2。

[0144] 步骤1002,汇款方对交易签名后,提交至区块链。

[0145] 基于上述步骤,汇款方生成的合并交易的交易内容可以为Merge{A:[PC(t_a_1,r_a_1),z1;PC(t_a_2,r_a_2),z2]},“A”代表该账户A的账户地址,表明需要对该账户A实施合并操作,[PC(t_a_1,r_a_1),z1;PC(t_a_2,r_a_2),z2]表明需要将z1数量且相应承诺为PC(t_a_1,r_a_1)的资产、z2数量且相应承诺为PC(t_a_2,r_a_2)的资产合并至主余额。而Merge表明当前的交易类型为合并交易,以用于针对账户A实施合并操作。

[0146] 由于收入余额的全部资金都将转入主余额,因而不需要针对收入余额的资金转移生成区间证明;同时,由于资产信息中采用明文形式记录各个统计数量,合并交易中同样以明文形式记录合并数量,因而区块链节点可以直接将统计数量与合并数量进行比较,从而在统计数量不小于合并数量时促成交易完成、否则不允许交易执行,同样不需要生成区间证明。

[0147] 汇款方采用持有的汇款方私钥对上述的交易内容Merge{A:[PC(t_a_1,r_a_1),z1;PC(t_a_2,r_a_2),z2]}进行签名,并将签名后创建的充值交易提交至区块链网络,以由所有区块链节点进行验证和执行。

[0148] 步骤1003,区块链节点验证交易。

[0149] 区块链节点可以验证上述合并交易的签名是否正确;如果不正确,可以拒绝执行该交易。

[0150] 区块链节点可以验证上述合并交易中对应于各个资产额承诺的合并数量是否不大于相应的统计数量。比如,以资产额承诺PC(t_a_1,r_a_1)为例,假定合并交易中记录的合并数量为z1＝2,而区块链账本上记录的统计数量为n1＝5,那么由于z1＜n1,允许执行该合并交易;而如果合并数量为z1＝4、统计数量为n1＝3,那么由于z1＞n1,不允许执行该合并交易。

[0151] 当所有验证均通过后,可以转入步骤1004。

[0152] 步骤1004,区块链节点更新账户。

[0153] 在通过步骤1003的验证后,区块链节点可以对区块链账本中记载的账户A进行更新。例如,图11是一示例性实施例提供的一种合并前后的账户变化情况的示意图。如图11所示:

[0154] 交易前的主余额为Az、在区块链账本中被记录为相应的承诺数额PC(Az,r_Az),交易前的收入余额为Au、在区块链账本中被记录为相应的承诺数额PC(Au,r_Au),交易前的资产额承诺PC(t_a_1,r_a_1)对应于统计数量n1、资产额承诺PC(t_a_2,r_a_2)对应于统计数量n2。

[0155] 在交易完成后,收入余额变为0;资产额承诺PC(t_a_1,r_a_1)对应的统计数量n1减少了合并数量z1、更新为n1-z1,而资产额承诺PC(t_a_2,r_a_2)对应的统计数量n2减少了合并数量z2、更新为n2-z2;主余额增加了收入余额的全部资金、z1数量的资产额承诺PC(t_a_1,r_a_1)、z2数量的资产额承诺PC(t_a_2,r_a_2),因而在区块链账本中记录的主余额承诺更新为PC(Az,r_Az)+PC(Au,r_Au)+PC(t_a_1,r_a_1)*z1+PC(t_a_2,r_a_2)*z2。

[0156] 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、资产信息,

可以通过由资产信息参与汇出交易、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等,下文分别予以介绍。

[0157] 对于主余额转账交易而言,可以根据汇款方与收款方之间的主余额交易额,生成主余额汇款交易,该主余额汇款交易包含主余额交易额对应的主余额交易额承诺、用于证明主余额交易额非负且不大于主余额的区间证明;然后,汇款方可以向区块链提交主余额汇款交易,使得主余额在交易完成后扣除主余额交易额承诺、收款方账户的收入余额在交易完成后增加主余额交易额承诺。图12是一示例性实施例提供的一种主余额转账交易的流程图。如图12所示,汇款方、收款方和区块链节点之间的交互过程可以包括以下步骤:

[0158] 步骤1201,汇款方确定汇款额t_z。

[0159] 在起草汇款交易时,汇款额t_z可由汇款方与收款方之间进行协商。当然,汇款方也可以自行确定汇款额t_z,由收款方在后续步骤中予以确认。

[0160] 步骤1202,汇款方确定汇款额t_z对应的随机数r_z。

[0161] 汇款方可以为该汇款额t_z产生随机数r_z,则譬如基于Pedersen承诺机制可以计算出汇款额t_z对应的汇款承诺T=PC(t_z,r_z)。

[0162] 步骤1203,汇款方通过链下通道将(r_z,t_z,T)发送至收款方。

[0163] 通过将(r_z,t_z,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_z和汇款额t_z被记录至区块链账本中,确保汇款额t_z除汇款方和收款方之外不可知。

[0164] 步骤1204,收款方对收到的(r_z,t_z,T)进行验证。

[0165] 收款方可以对汇款额t_z进行验证,以确定为希望收取的汇款数额。以及,收款方可以对汇款承诺T进行验证,即收款方可以通过Perdersen承诺机制对随机数r_z和汇款额t_z进行计算,以验证汇款承诺T=PC(t_z,r_z)是否正确,若正确则表明验证通过,否则验证不通过。

[0166] 步骤1205,收款方在验证通过后,生成签名并返回至汇款方。

[0167] 在一实施例中,在验证通过后,收款方可以利用收款方私钥对(A,B:T)进行签名,生成签名SigB并返回至汇款方。该签名SigB表明收款方同意由汇款方对应的账户A向收款方对应的账户B实施承诺为T的汇款交易。

[0168] 步骤1206,在收到签名SigB后,汇款方根据主余额Az生成区间证明RP。

[0169] 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_z、主余额Az满足下述条件:0≤t_z≤Az,因而汇款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,使得区块链节点在密文状态下即可验证交易是否符合上述条件。

[0170] 步骤1207,汇款方对交易内容PrimaryTransfer(A,B:T,RP;SigB)进行签名,生成签名SigA。

[0171] 汇款方可以利用汇款方私钥对交易内容PrimaryTransfer(A,B:T,RP;SigB)进行签名,生成签名SigA。其中,PrimaryTransfer用于表明交易类型为主余额转账交易,使得汇款额t_z从账户A的主余额中扣除。

[0172] 步骤1208,汇款方向区块链提交交易。

[0173] 汇款方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。

[0174] 步骤1209，区块链节点检查交易是否执行过。

[0175] 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1209～1211等实施验证等操作。

[0176] 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1210。

[0177] 步骤1210，区块链节点检查签名。

[0178] 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1211。

[0179] 步骤1211，区块链节点检查区间证明RP。

[0180] 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≤t_z≤Az。如果不满足，可以拒绝执行该汇款交易，否则转入步骤1212。

[0181] 步骤1212，区块链节点在维护的区块链账本中更新汇款方、收款方分别对应的账户A、账户B。

[0182] 在一实施例中，在通过步骤1209～1211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。图13是一示例性实施例提供的一种主余额汇款前后的账户变化情况的示意图。如图13所示：

[0183] 在账户A中，交易前的主余额为Az、在区块链账本中被记录为相应的承诺数额PC(Az,r_Az)，交易前的收入余额为Au、在区块链账本中被记录为相应的承诺数额PC(Au,r_Au)，交易前的资产额承诺PC(t_a_1,r_a_1)对应于统计数量n1、资产额承诺PC(t_a_2,r_a_2)对应于统计数量n2。在交易完成后，主余额被扣除了上述的交易额t_z，因而在区块链账本中被记录为相应的承诺数额PC(Az,r_Az)-PC(t_z,r_z)，而收入余额Au、统计数量n1-n2不变。

[0184] 在账户B中，交易前的主余额为Bz、在区块链账本中被记录为相应的承诺数额PC(Bz,r_Bz)，交易前的收入余额为Bu、在区块链账本中被记录为相应的承诺数额PC(Bu,r_Bu)，交易前的资产额承诺PC(t_b_1,r_b_1)对应于统计数量m1、资产额承诺PC(t_b_2,r_b_2)对应于统计数量m2。在交易完成后，主余额为Bz、统计数量n1-n2不变，而收入余额则增加了汇款额t_z，因而在区块链账本中被记录为相应的承诺数额PC(Bu,r_Bu)+PC(t_z,r_z)。

[0185] 图14是一示例性实施例提供的另一种区块链网络中实现机密交易的方法的流程图。如图14所示，该方法应用于区块链节点，可以包括以下步骤：

[0186] 步骤1402，接收汇款交易，所述汇款交易包含汇款方与收款方之间的汇款额对应的汇款额承诺、至少一个资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为所述至少一个资产额承诺对应的资产额与相应的指定数量的加权和；其中，所述汇款方在区块链账本上对应的汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺。

[0187] 汇款额可以由汇款方与收款方之间协商确定，也可以由汇款方自行确定。基于已确定的汇款额，可以从汇款方账户中选取恰当的资产，以用于支付该汇款额。

[0188] 汇款方对应于汇款方账户、收款方对应于收款方账户，汇款方账户与收款方账户均记录于区块链账本中。区块链网络中的每一区块链节点分别维护有一份区块链账本，而基于共识机制可以确保所有区块链节点维护的区块链账本的内容一致，因而可以认为所有区块链节点共同维护了一份区块链账本。

[0189] 如前所述，本说明书针对相关技术中的账户模型进行了改进。譬如图4所示，账户A包括收入余额和资产信息。其中，收入余额的明文数额为Au，而出于保密的目的，在区块链账本上具体记录为相应的收入余额承诺PC(Au,r_Au)，其中r_Au为随机数。资产信息用于记录汇款方所持有的资产，该资产是基于汇款方所持有的余额而生成，区别于UTXO模型中的交易输出。比如，基于汇款方持有的明文数额为t_a_1的余额，可以结合随机数r_a_1生成相应的承诺数额PC(t_a_1,r_a_1)，相当于汇款方持有一份资产额为t_a_1、资产额承诺为PC(t_a_1,r_a_1)的资产；类似地，可以基于汇款方持有的明文数额为t_a_2的余额和随机数r_a_2生成相应的承诺数额PC(t_a_2,r_a_2)，相当于汇款方持有一份资产额为t_a_2、资产额承诺为PC(t_a_2,r_a_2)的资产；以此类推，可以生成其他的具有相同或不同资产额的资产。

[0190] 对于具有相同资产额的不同资产而言，本说明书中可以限定同一取值的资产额必然选取相同的随机数，譬如上述资产额t_a_1必然对应于随机数r_a_1、资产额t_a_2必然对应于随机数r_a_2，使得同一取值的资产额必然对应于相同取值的资产额承诺，比如资产额t_a_1必然对应于资产额承诺PC(t_a_1,r_a_1)、资产额t_a_2必然对应于资产额承诺PC(t_a_2,r_a_2)。因此，汇款方账户所含的资产信息可以具体包含各个取值的资产额承诺和每一取值的资产额承诺的统计数量，比如图4所示的账户A中，资产额承诺PC(t_a_1,r_a_1)对应的统计数量为n1、资产额承诺PC(t_a_2,r_a_2)对应的统计数量为n2，即汇款方持有n1个取值为PC(t_a_1,r_a_1)的资产额承诺、n2个取值为PC(t_a_2,r_a_2)的资产额承诺。这样，相当于将汇款方账户所含的资产进行了组别划分，每一资产组的所有资产对应于同一预设取值的资产额(或资产额承诺)，且不同资产组的资产对应于不同预设取值的资产额(或资产额承诺)；当然，所有资产可以对应于同一预设取值的资产额(或资产额承诺)，相当于仅存在一个资产组。

[0191] 基于上述方式记录汇款方账户所含的资产，只需要记录各个资产组对应的资产额承诺和每一资产组对应的统计数量，譬如图4中的一个资产组对应的资产额承诺为PC(t_a_1,r_a_1)、统计数量为n1，另一个资产组对应的资产额承诺为PC(t_a_2,r_a_2)、统计数量为n2，而无需分别记录每一资产的详细信息，使得资产发生增减变化时仅需调整对应的统计数量的取值，可以极大地降低资产信息的维护成本，有助于缓解存储压力。

[0192] 与汇款方账户相类似的，收款方账户同样包含收入余额和资产信息，收入余额被记录为收入余额承诺，资产信息包括资产额承诺的各个取值及其统计数量，其中相同资产额的资产具有相同的资产额承诺，此处不再赘述。

[0193] 如前所述，汇款交易添加了汇款方账户中被选取的一个或多个资产额承诺，以及每一被选取的资产额承诺对应的指定数量。比如，当汇款额为t时，如果选取的资产额承诺分别为PC(t_a_1,r_a_1)和PC(t_a_2,r_a_2)，且对应的指定数量分别为x1和x2，那么可以

确定资产总额为(t_a_1*x1+t_a_2*x2)，并且应当确保0≤t≤(t_a_1*x1+t_a_2*x2)；具体的，可以生成用于证明汇款额非负且不大于资产总额的区间证明，从而在不暴露汇款额和资产总额的明文数值的情况下，即可基于该区间证明来验证是否满足0≤t≤(t_a_1*x1+t_a_2*x2)。

[0194] 步骤1404，执行所述汇款交易，使得所述汇款交易所含每一资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

[0195] 汇款交易被提交至区块链后，可由某一区块链节点将该汇款交易打包至区块中，该区块在经过共识后被添加至区块链中，使得该区块所含的上述汇款交易在所有区块链节点上被执行。当然，区块链节点可以针对汇款交易进行验证，比如验证汇款方、收款方的签名、验证上述的区间证明等，从而在通过验证后允许执行该汇款交易，否则可以解决执行。

[0196] 汇款交易的输入来自汇款方账户中的资产，而输出包括两个部分：一部分的输出目标为收款方账户、输出额为汇款额(实际记录为汇款额承诺)，另一部分的输出目标为收款方账户、输出额为找零额(实际记录为找零额承诺)。其中，找零额为上述的资产总额与汇款额之差；比如，当资产总额为(t_a_1*x1+t_a_2*x2)、汇款额为t时，可以确定找零额t’＝t_a_1*x1+t_a_2*x2-t，找零额承诺为PC(t’,r’)，r’为随机数。

[0197] 可见，基于本说明书改进后的账户模型，收入余额专用于实现收款(作为汇款方时用于汇入找零额，作为收款方时用于汇入汇款额)、资产专用于实现汇款，可以实现同一账户的收款与汇款之间的解耦，因而可使一个用户作为汇款交易TX1的汇款方、作为汇款交易TX2的收款方而同时参与至汇款交易TX1和TX2中，实现了账户模型下的交易并发，可以提升区块链网络中的交易执行效率。

[0198] 同时，由于在生成上述汇款额与资产总额之间的区间证明时，资产总额的取值仅与被选取的资产额承诺及其指定数量相关，并不涉及区块链账本上记录的各个资产额承诺的统计数量，使得不同汇款交易可以分别生成相应的区间证明且互不影响。进一步的，由于在区块链账本上对各个取值的资产额承诺的统计数量采用明文形式进行记录，使得区块链节点可以对汇款交易中包含的指定数量与区块链账本上记录的统计数量进行直接比较：若指定数量不大于统计数量，则允许执行相应的汇款交易，否则不允许执行。因此，同一用户可以同时作为多个汇款交易的汇款方，以实现账户模型下的交易并发，可以提升区块链网络中的交易执行效率；以及，当在后生成的汇款交易优先到达区块链节点时，区块链节点可以优先处理该在后生成的汇款交易，而无需等待在先生成的汇款交易执行完成，避免了区块链节点处的交易阻塞。

[0199] 如上文所述，当账户包含上述的收入余额和资产信息时，可以在保障交易隐私的情况下，实现账户的输入与输出解耦，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、而汇出的资金都从资产信息中扣除(减小统计数量的取值)，因而统计数量的取值(即账户内的资产)在不断下降，可能小于汇款交易中的指定数量而影响到汇款交易的执行。为了确保统计数量的数额总是能够处于充足状态、足够完成交易，可以定期或随时通过充值调整统计数量的数额。

[0200] 以汇款方账户的充值过程为例。区块链节点可以接收充值交易，该充值交易包含

至少一个指定取值的资产额承诺和相应的充值数量、用于证明汇款方账户的收入余额不小于充值额的区间证明，充值额为上述指定取值的资产额承诺对应的资产额与充值数量的加权和；区块链节点执行充值交易，使得汇款方账户中对应于上述指定取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、汇款方账户的收入余额在交易完成后减少上述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。换言之，可以将汇款方账户中的收入余额划分出至少一部分，将这部分余额转换为相应的资产，这些资产可使对应的资产额承诺的统计数量实现取值增大。当然，收款方账户也可以采用上述方式进行充值。

[0201] 虽然可以按照上述方式实现基于收入余额的资产充值操作，但是当账户参与的汇款交易较为频繁、汇款额较大时，可能导致频繁充值，造成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(其他账户向该账户进行汇款的交易)与充值交易之间相应影响，反而造成效率下降。因此，本说明书中可以针对图4所示的账户结构实施进一步改进，得到如图7所示的账户结构，其在图4所示账户结构的基础上，除了包含收入余额和资产信息之外，进一步包含主余额，即账户A总共包含三部分：主余额、收入余额和资产信息。其中，收入余额专用于收取汇入交易的交易额、资产信息专用于参与汇出交易，而主余额用于对资产信息进行充值，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。

[0202] 以汇款方为例。区块链节点可以接收充值交易，该充值交易包含指定的至少一个取值的资产额承诺和相应的充值数量、用于证明主余额不小于充值额的区间证明，充值额为上述指定的至少一个取值的资产额承诺对应的资产额与相应的充值数量的加权和；区块链节点执行充值交易，使得汇款方账户中对应于上述指定的至少一个取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、汇款方账户的主余额在交易完成后减少上述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。具体的交互过程可以参考图8所示的实施例，以及图9还示出了账户充值前后的变化情况，此处不再赘述。

[0203] 随着账户中的资产信息不断参与汇出交易，而主余额不断向资产信息进行充值，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，将无法继续充值，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。

[0204] 以汇款方为例。区块链节点可以接收合并交易，该合并交易包含指定的至少一个取值的资产额承诺和相应的合并数量；区块链节点执行合并交易，使得汇款方账户中对应于上述指定的至少一个取值的资产额承诺的统计数量在交易完成后减少相应的合并数量、主余额在交易完成后增加合并额承诺，和/或汇款方账户的收入余额在交易完成后清零、汇款方账户的主余额在交易完成后增加相应的收入余额承诺；其中，合并额承诺为上述指定的至少一个取值的资产额承诺与相应的合并数量的加权和。换言之，合并交易可以将收入余额所含的资金全部并入主余额，或者在一些情况下可以将至少一部分资产以资金形式并入主余额，或者还可以同时将收入余额所含的资金并入主余额、将至少一部分资产以资金形式并入主余额。具体的交互过程可以参考图10所示的实施例，以及图11还示出了账户在合并前后的变化情况，此处不再赘述。

[0205] 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、资产信息，可以通过由资产信息参与汇出交易、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等。

[0206] 例如，区块链节点可以接收主余额汇款交易，该主余额汇款交易包含汇款方与收款方之间的主余额交易额对应的主余额交易额承诺、用于证明主余额交易额非负且不大于主余额的区间证明；区块链节点执行主余额汇款交易，使得主余额在交易完成后扣除主余额交易额承诺、收款方账户的收入余额在交易完成后增加主余额交易额承诺。具体的交互过程可以参考图12所示的实施例，以及图13还示出了账户在交易前后的变化情况，此处不再赘述。

[0207] 图15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15，在硬件层面，该设备包括处理器1502、内部总线1504、网络接口1506、内存1508以及非易失性存储器1510，当然还可能包括其他业务所需要的硬件。处理器1502从非易失性存储器1510中读取对应的计算机程序到内存1508中然后运行，在逻辑层面上形成区块链网络中实现机密交易的装置。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。

[0208] 请参考图16，在软件实施方式中，该区块链网络中实现机密交易的装置应用于汇款方设备(汇款方设备的硬件结构如图15所示)，可以包括：

[0209] 确定单元1601，确定汇款方与收款方之间的汇款额，所述汇款方在区块链账本上存在对应的汇款方账户，所述汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺；

[0210] 汇款交易创建单元1602，根据所述汇款方账户中被选取的资产额承诺和每一被选取的资产额承诺对应的指定数量创建汇款交易，所述汇款交易包含所述汇款额对应的汇款额承诺、每一被选取的资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为每一被选取的资产额承诺对应的资产额与相应的指定数量的加权和；

[0211] 汇款交易提交单元1603，向区块链提交所述汇款交易，使得每一被选取的资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

[0212] 可选的，

[0213] 所述汇款方账户所含的所有资产对应于同一预设取值的资产额；或，

[0214] 所述汇款方账户包含多个资产组，每一资产组的所有资产对应于同一预设取值的资产额，且不同资产组的资产对应于不同预设取值的资产额。

[0215] 可选的，所述汇款方账户还包括被记录为主余额承诺的主余额；所述装置还包括：

[0216] 第一充值交易创建单元，创建充值交易，所述充值交易包含指定的至少一个取值的资产额承诺和相应的充值数量、用于证明所述主余额不小于充值额的区间证明，所述充值额为所述指定的至少一个取值的资产额承诺对应的资产额与相应的充值数量的加权和；

[0217] 第一充值交易提交单元，向区块链提交所述充值交易，使得所述汇款方账户中对

应于所述指定的至少一个取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、所述汇款方账户的主余额在交易完成后减少所述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。

[0218] 可选的，还包括：

[0219] 合并交易创建单元，创建合并交易，所述合并交易包含指定的至少一个取值的资产额承诺和相应的合并数量；

[0220] 合并交易提交单元，向区块链提交所述合并交易，使得所述汇款方账户中对应于所述指定的至少一个取值的资产额承诺的统计数量在交易完成后减少相应的合并数量、所述主余额在交易完成后增加合并额承诺，和/或所述汇款方账户的收入余额在交易完成后清零、所述汇款方账户的主余额在交易完成后增加相应的收入余额承诺；其中，所述合并额承诺为所述指定的至少一个取值的资产额承诺与相应的合并数量的加权和。

[0221] 可选的，还包括：

[0222] 主余额汇款交易创建单元，根据所述汇款方与所述收款方之间的主余额交易额，生成主余额汇款交易，所述主余额汇款交易包含所述主余额交易额对应的主余额交易额承诺、用于证明所述主余额交易额非负且不大于所述主余额的区间证明；

[0223] 主余额汇款交易提交单元，向区块链提交所述主余额汇款交易，使得所述主余额在交易完成后扣除所述主余额交易额承诺、所述收款方账户的收入余额在交易完成后增加所述主余额交易额承诺。

[0224] 可选的，还包括：

[0225] 第二充值交易创建单元，创建充值交易，所述充值交易包含至少一个指定取值的资产额承诺和相应的充值数量、用于证明所述汇款方账户的收入余额不小于充值额的区间证明，所述充值额为所述指定取值的资产额承诺对应的资产额与充值数量的加权和；

[0226] 第二充值交易提交单元，向区块链提交所述充值交易，使得所述汇款方账户中对应于所述指定取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、所述汇款方账户的收入余额在交易完成后减少所述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。

[0227] 图17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17，在硬件层面，该设备包括处理器1702、内部总线1704、网络接口1706、内存1708以及非易失性存储器1710，当然还可能包括其他业务所需要的硬件。处理器1702从非易失性存储器1710中读取对应的计算机程序到内存1708中然后运行，在逻辑层面上形成区块链网络中实现机密交易的装置。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。

[0228] 请参考图18，在软件实施方式中，该区块链网络中实现机密交易的装置应用于区块链节点(该区块链节点的硬件结构如图17所示)，可以包括：

[0229] 汇款交易接收单元1801，接收汇款交易，所述汇款交易包含汇款方与收款方之间的汇款额对应的汇款额承诺、至少一个资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为所述至少一个资产额承诺对应的资产额与相应的指定数量的加权和；其中，所述汇款方在区块链账本上对应的汇款方账户包

括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺；

[0230] 汇款交易执行单元1802，执行所述汇款交易，使得所述汇款交易所含每一资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺。

[0231] 可选的，

[0232] 所述汇款方账户所含的所有资产对应于同一预设取值的资产额；或，

[0233] 所述汇款方账户包含多个资产组，每一资产组的所有资产对应于同一预设取值的资产额，且不同资产组的资产对应于不同预设取值的资产额。

[0234] 可选的，所述汇款方账户还包括被记录为主余额承诺的主余额；所述装置还包括：

[0235] 第一充值交易接收单元，接收充值交易，所述充值交易包含指定的至少一个取值的资产额承诺和相应的充值数量、用于证明所述主余额不小于充值额的区间证明，所述充值额为所述指定的至少一个取值的资产额承诺对应的资产额与相应的充值数量的加权和；

[0236] 第一充值交易执行单元，执行所述充值交易，使得所述汇款方账户中对应于所述指定的至少一个取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、所述汇款方账户的主余额在交易完成后减少所述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。

[0237] 可选的，还包括：

[0238] 合并交易接收单元，接收合并交易，所述合并交易包含指定的至少一个取值的资产额承诺和相应的合并数量；

[0239] 合并交易执行单元，执行所述合并交易，使得所述汇款方账户中对应于所述指定的至少一个取值的资产额承诺的统计数量在交易完成后减少相应的合并数量、所述主余额在交易完成后增加合并额承诺，和/或所述汇款方账户的收入余额在交易完成后清零、所述汇款方账户的主余额在交易完成后增加相应的收入余额承诺；其中，所述合并额承诺为所述指定的至少一个取值的资产额承诺与相应的合并数量的加权和。

[0240] 可选的，还包括：

[0241] 主余额汇款交易接收单元，接收主余额汇款交易，所述主余额汇款交易包含所述汇款方与所述收款方之间的主余额交易额对应的主余额交易额承诺、用于证明所述主余额交易额非负且不大于所述主余额的区间证明；

[0242] 主余额汇款交易执行单元，执行所述主余额汇款交易，使得所述主余额在交易完成后扣除所述主余额交易额承诺、所述收款方账户的收入余额在交易完成后增加所述主余额交易额承诺。

[0243] 可选的，还包括：

[0244] 第二充值交易接收单元，接收充值交易，所述充值交易包含至少一个指定取值的资产额承诺和相应的充值数量、用于证明所述汇款方账户的收入余额不小于充值额的区间证明，所述充值额为所述指定取值的资产额承诺对应的资产额与充值数量的加权和；

[0245] 第二充值交易执行单元，执行所述充值交易，使得所述汇款方账户中对应于所述指定取值的资产额承诺的统计数量在交易完成后增加相应的充值数量、所述汇款方账户的

收入余额在交易完成后减少所述指定的至少一个取值的资产额承诺与相应的充值数量的加权和。

[0246] 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。

[0247] 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。

[0248] 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。

[0249] 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。

[0250] 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。

[0251] 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。

[0252] 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。

[0253] 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”。

[0254] 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。

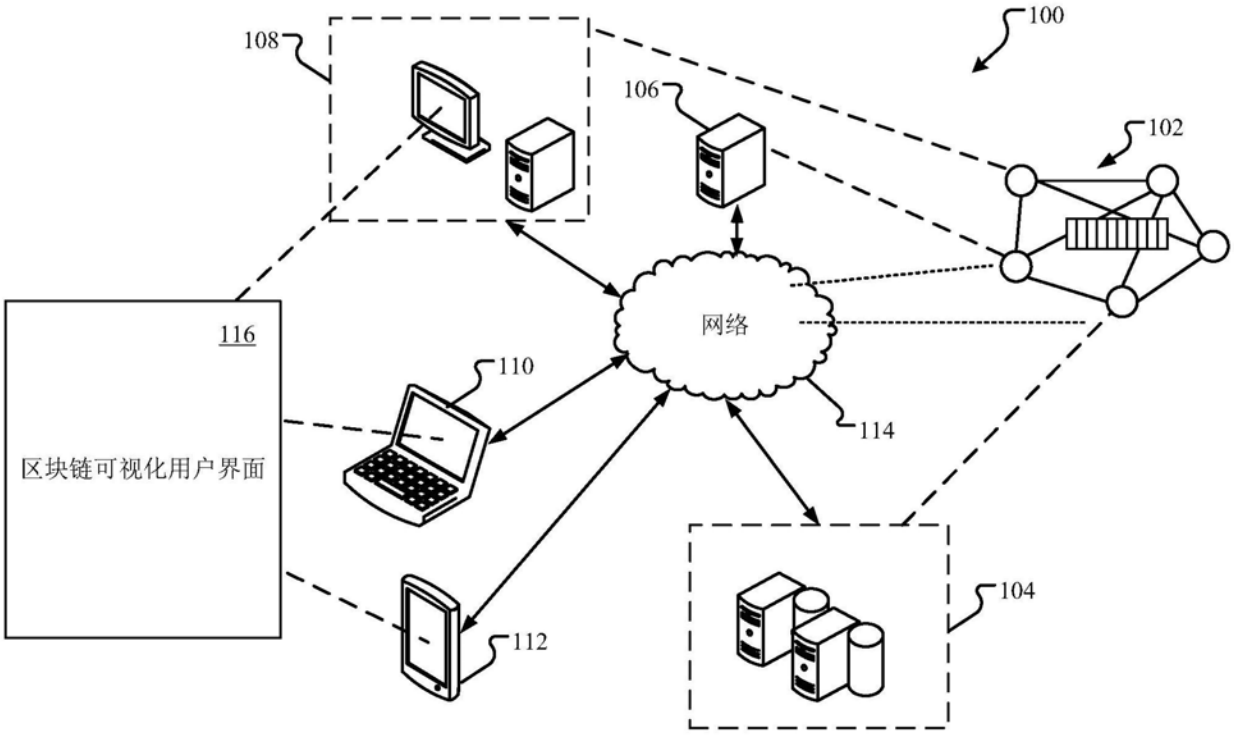

图1

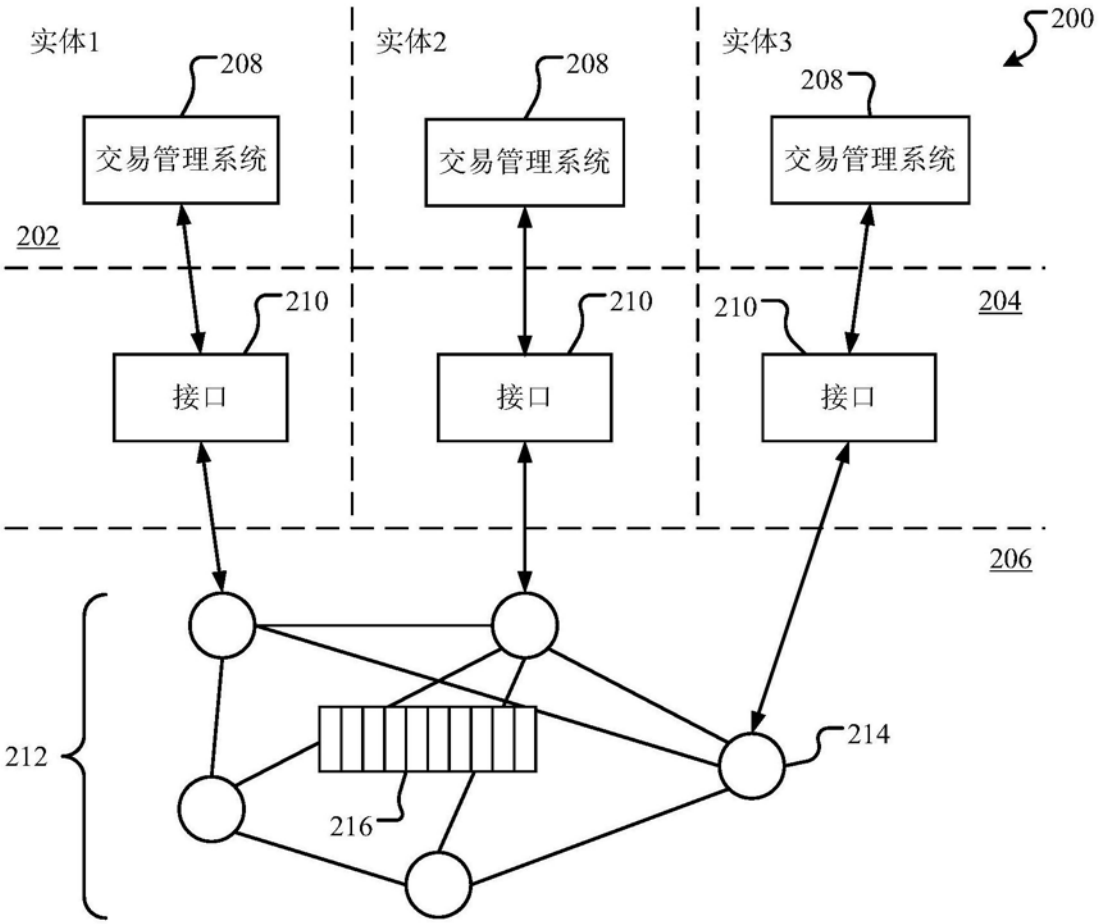
实体1
实体2
实体3
200
208
208
208
交易管理系统
交易管理系统
交易管理系统
202
204
210
210
210
接口
接口
接口
206
212
214
216

图2

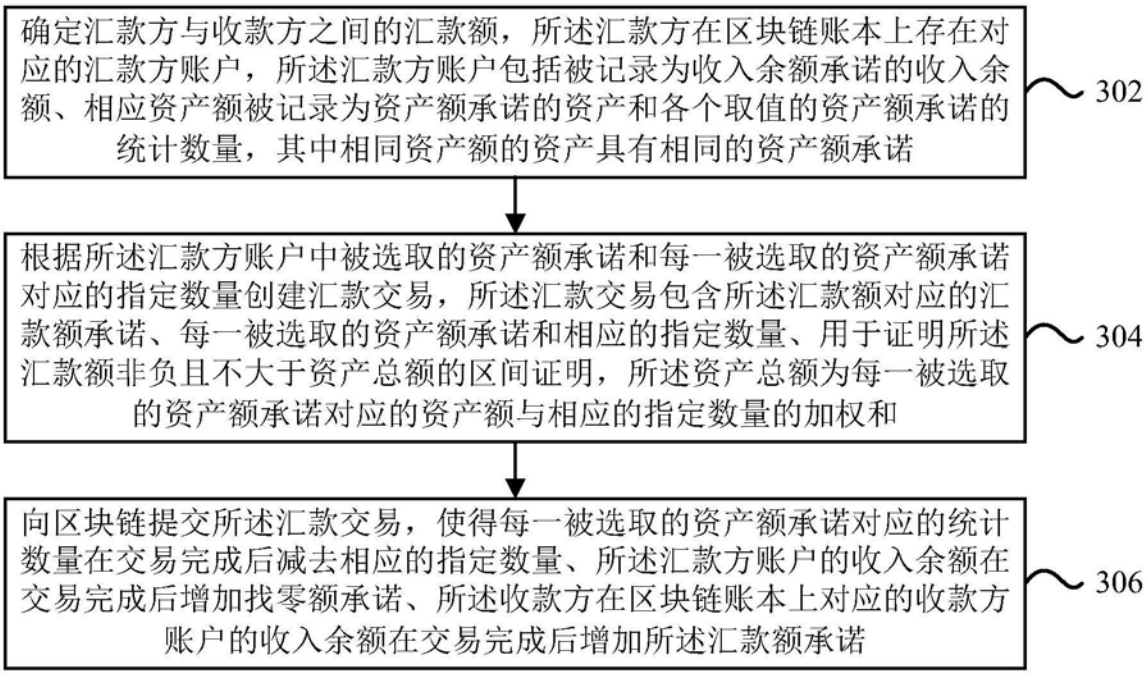
确定汇款方与收款方之间的汇款额，所述汇款方在区块链账本上存在对应的汇款方账户，所述汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺
302
根据所述汇款方账户中被选取的资产额承诺和每一被选取的资产额承诺对应的指定数量创建汇款交易，所述汇款交易包含所述汇款额对应的汇款额承诺、每一被选取的资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为每一被选取的资产额承诺对应的资产额与相应的指定数量的加权和
304
向区块链提交所述汇款交易，使得每一被选取的资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺
306

图3

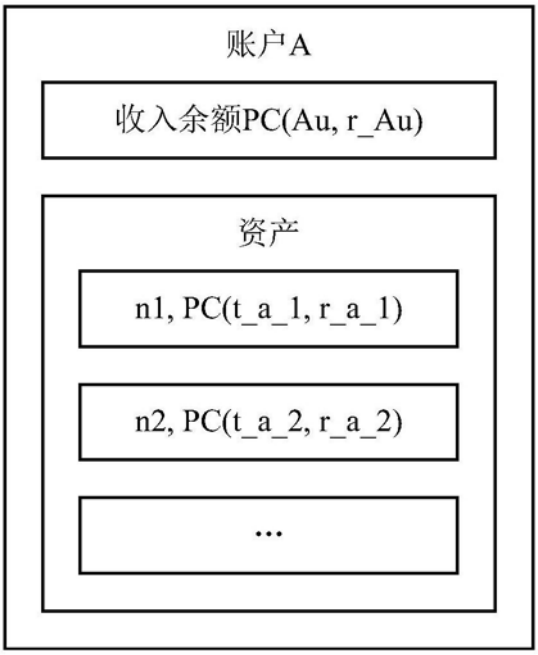
账户A
收入余额PC(Au, r_Au)
资产
n1, PC(t_a_1, r_a_1)
n2, PC(t_a_2, r_a_2)
...

图4

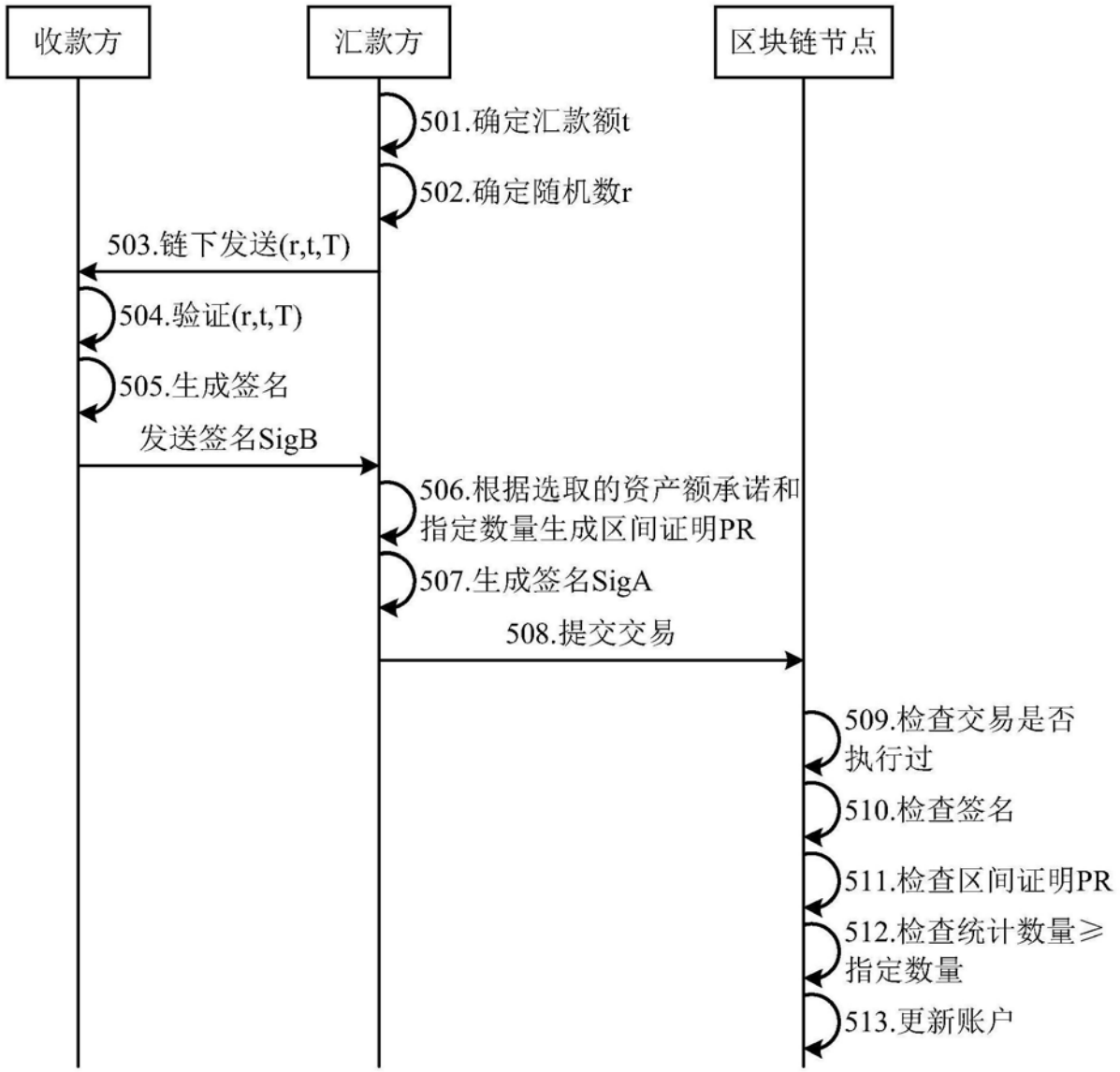
收款方
汇款方
区块链节点
501.确定汇款额t
502.确定随机数r
503.链下发送(r,t,T)
504.验证(r,t,T)
505.生成签名
发送签名SigB
506.根据选取的资产额承诺和指定数量生成区间证明PR
507.生成签名SigA
508.提交交易
509.检查交易是否执行过
510.检查签名
511.检查区间证明PR
512.检查统计数量≥指定数量
513.更新账户

图5

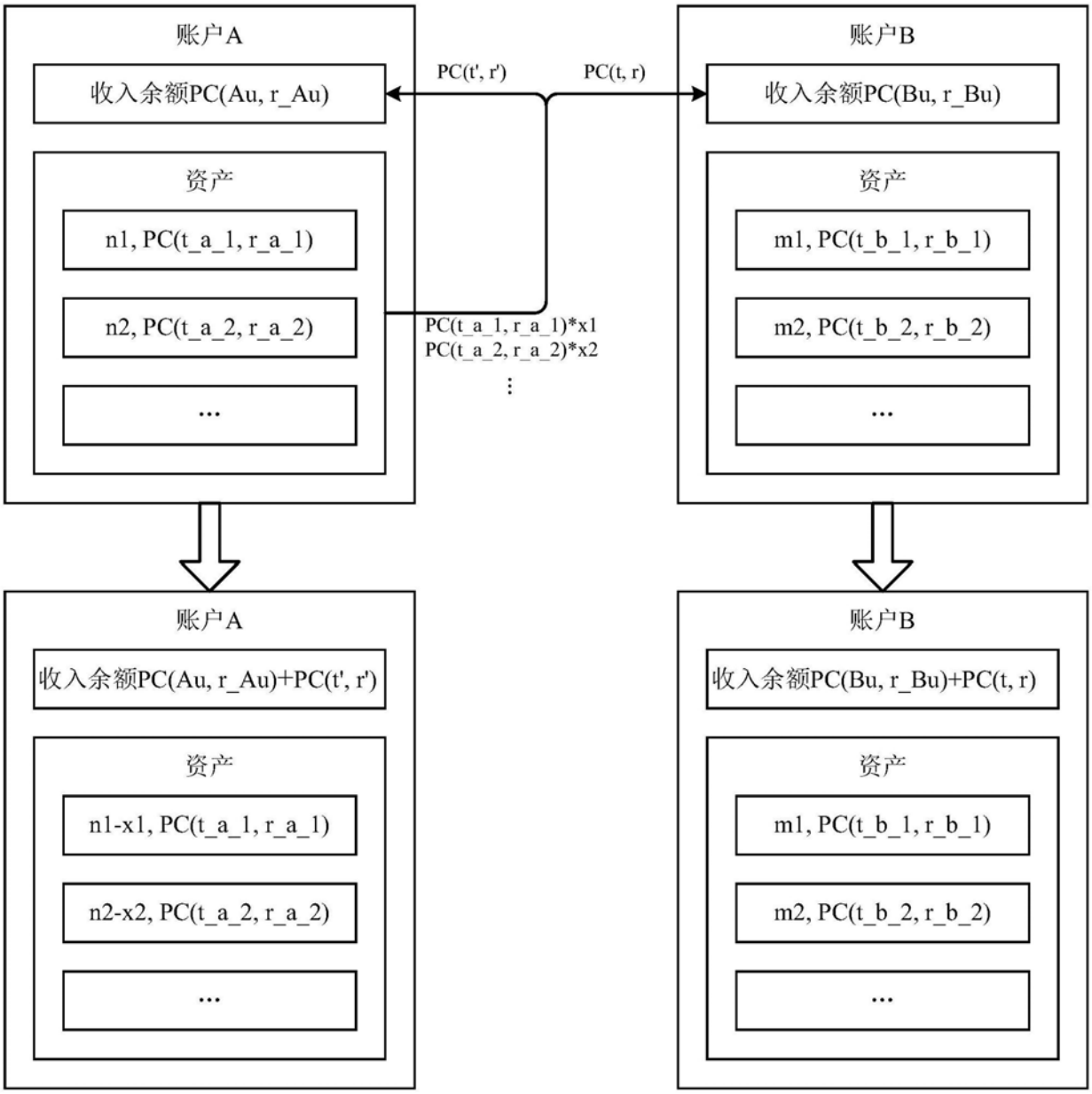
账户A
收入余额PC(Au, r_Au)
资产
n1, PC(t_a_1, r_a_1)
n2, PC(t_a_2, r_a_2)
...
PC(t', r')
PC(t, r)
PC(t_a_1, r_a_1)*x1
PC(t_a_2, r_a_2)*x2
账户B
收入余额PC(Bu, r_Bu)
资产
m1, PC(t_b_1, r_b_1)
m2, PC(t_b_2, r_b_2)
...
账户A
收入余额PC(Au, r_Au)+PC(t', r')
资产
n1-x1, PC(t_a_1, r_a_1)
n2-x2, PC(t_a_2, r_a_2)
...
账户B
收入余额PC(Bu, r_Bu)+PC(t, r)
资产
m1, PC(t_b_1, r_b_1)
m2, PC(t_b_2, r_b_2)
...

图6

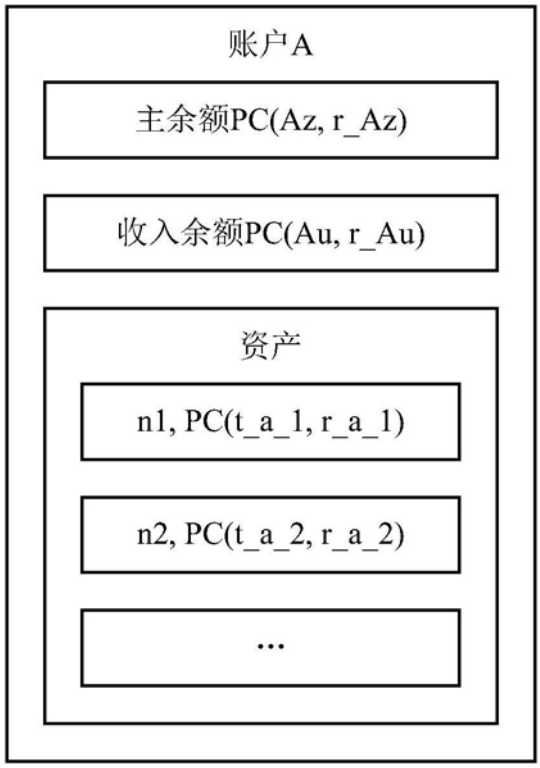
账户A
主余额PC(Az, r_Az)
收入余额PC(Au, r_Au)
资产
n1, PC(t_a_1, r_a_1)
n2, PC(t_a_2, r_a_2)
...

图7

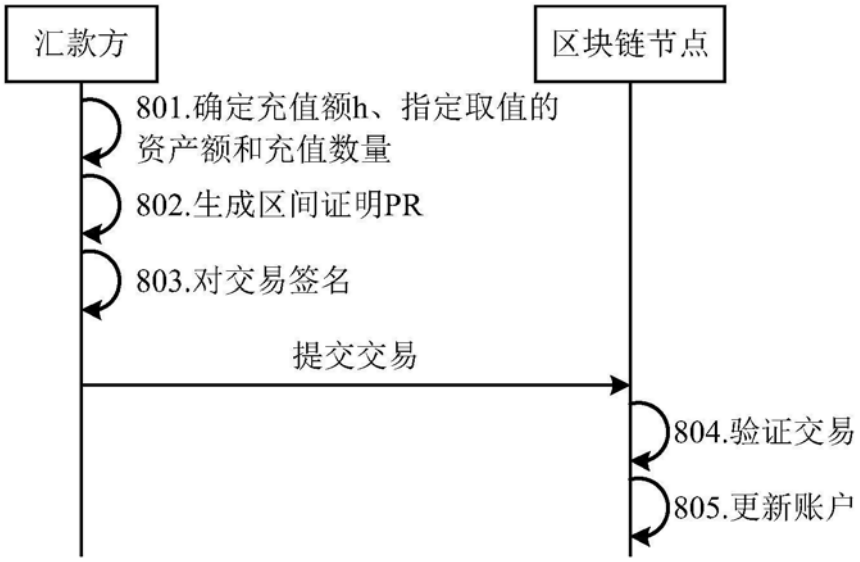
汇款方
区块链节点
801.确定充值额h、指定取值的资产额和充值数量
802.生成区间证明PR
803.对交易签名
提交交易
804.验证交易
805.更新账户

图8

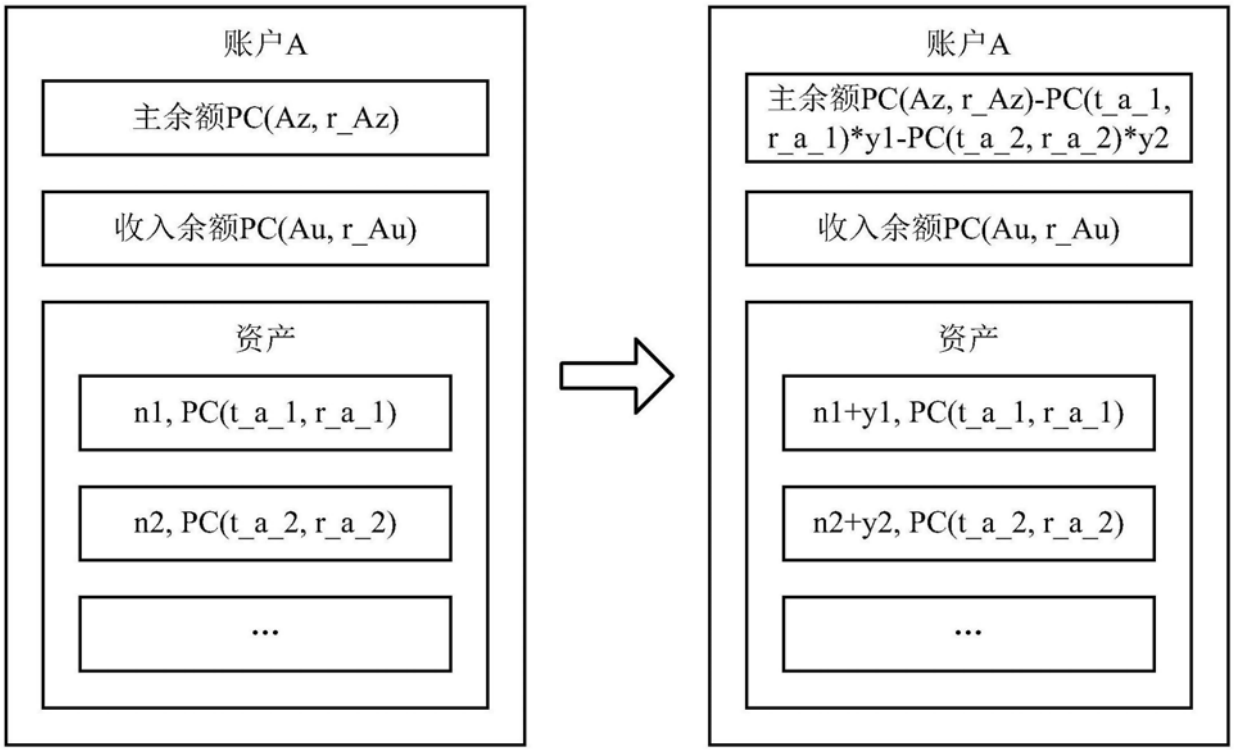
账户A
主余额PC(Az, r_Az)
收入余额PC(Au, r_Au)
资产
n1, PC(t_a_1, r_a_1)
n2, PC(t_a_2, r_a_2)
...
账户A
主余额PC(Az, r_Az)-PC(t_a_1, r_a_1)*y1-PC(t_a_2, r_a_2)*y2
收入余额PC(Au, r_Au)
资产
n1+y1, PC(t_a_1, r_a_1)
n2+y2, PC(t_a_2, r_a_2)
...

图9

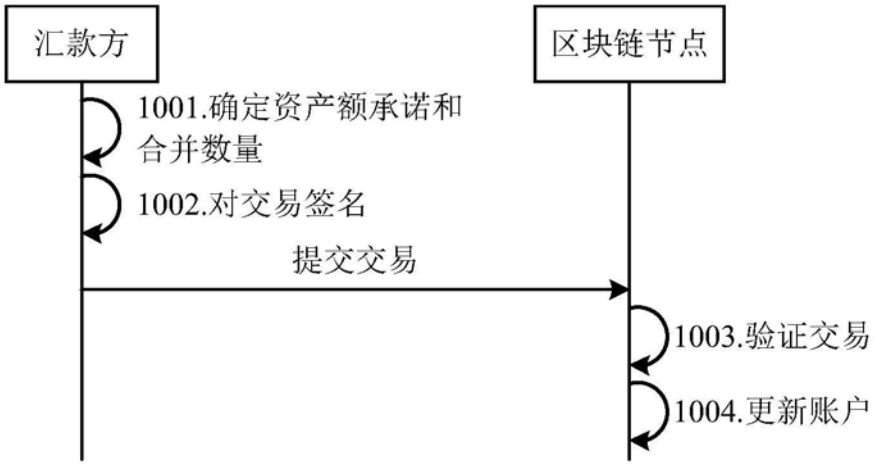
汇款方
区块链节点
1001.确定资产额承诺和合并数量
1002.对交易签名
提交交易
1003.验证交易
1004.更新账户

图10

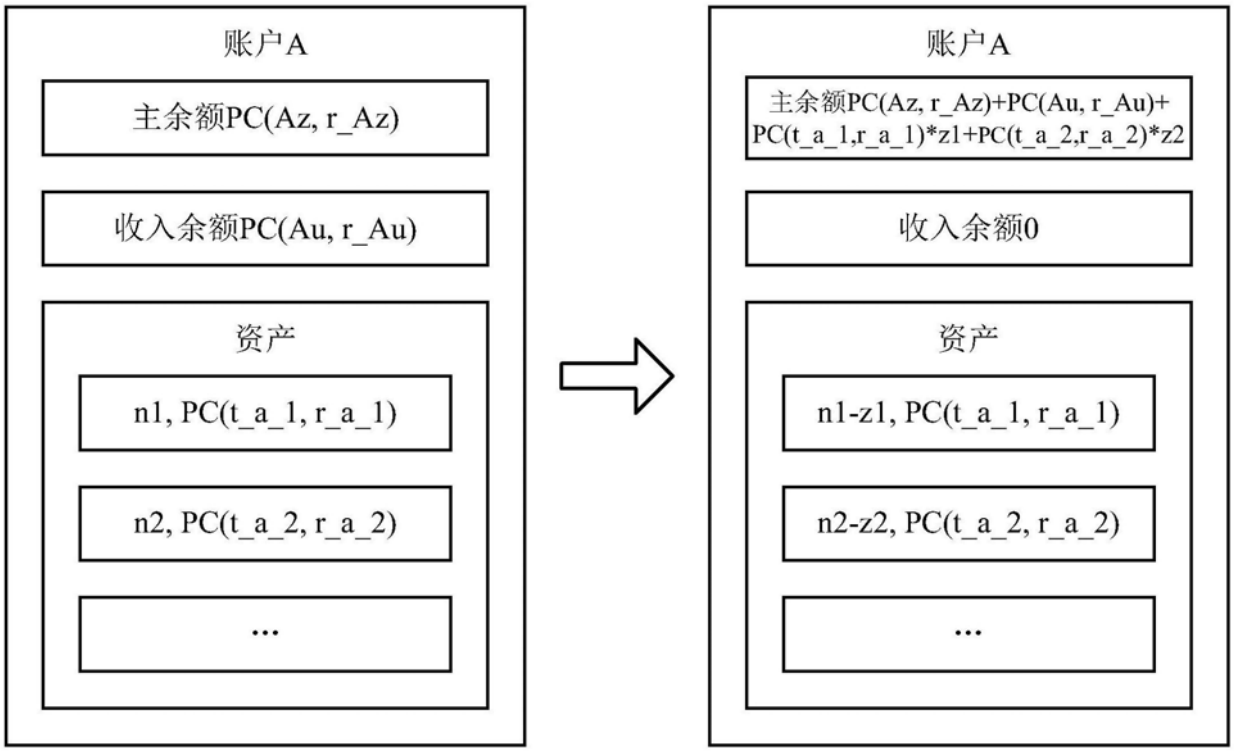
账户A
主余额PC(Az, r_Az)
收入余额PC(Au, r_Au)
资产
n1, PC(t_a_1, r_a_1)
n2, PC(t_a_2, r_a_2)
...
账户A
主余额PC(Az, r_Az)+PC(Au, r_Au)+
PC(t_a_1,r_a_1)*z1+PC(t_a_2,r_a_2)*z2
收入余额0
资产
n1-z1, PC(t_a_1, r_a_1)
n2-z2, PC(t_a_2, r_a_2)
...

图11

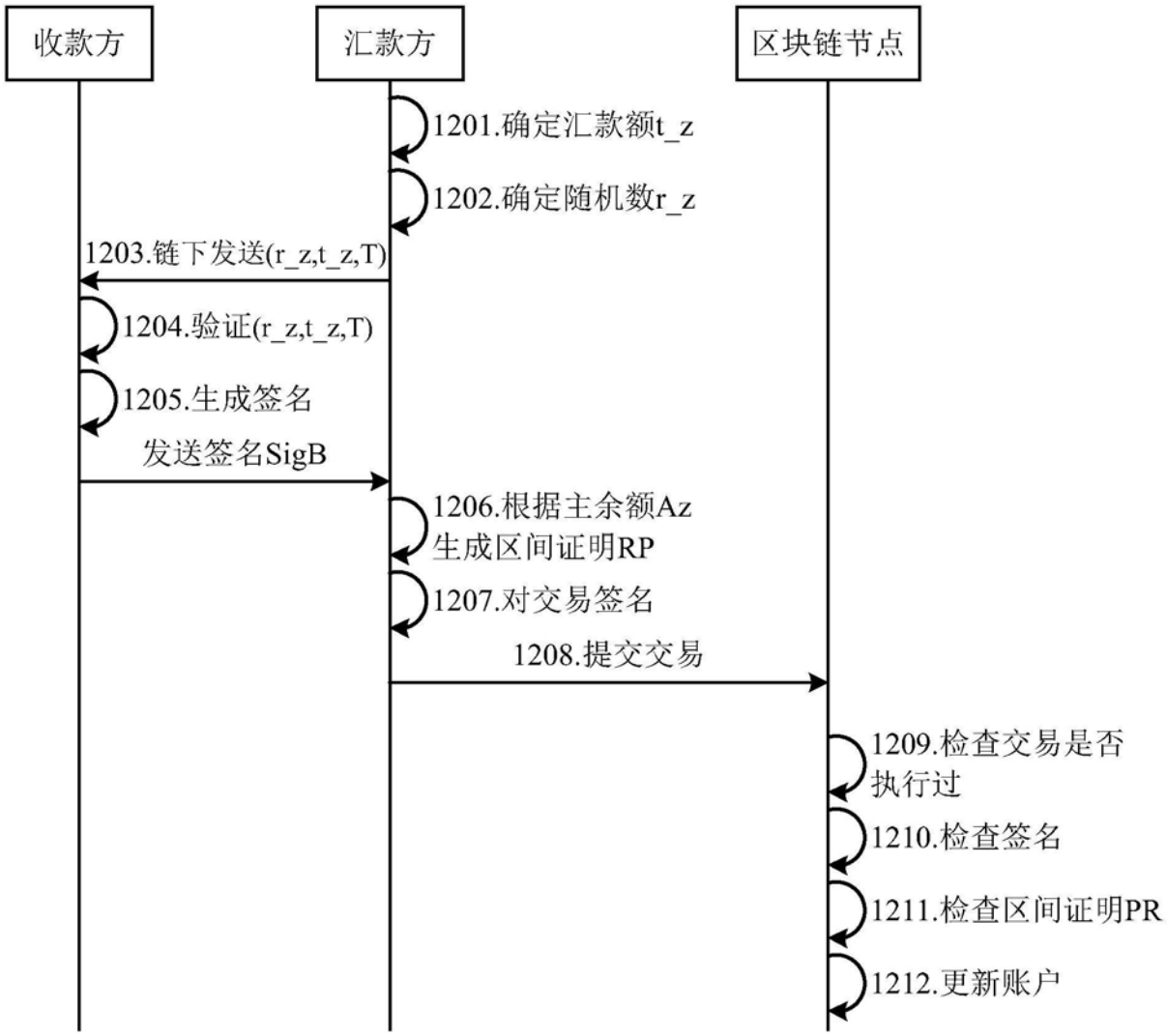
收款方
汇款方
区块链节点
1201.确定汇款额t_z
1202.确定随机数r_z
1203.链下发送(r_z,t_z,T)
1204.验证(r_z,t_z,T)
1205.生成签名
发送签名SigB
1206.根据主余额Az
生成区间证明RP
1207.对交易签名
1208.提交交易
1209.检查交易是否
执行过
1210.检查签名
1211.检查区间证明PR
1212.更新账户

图12

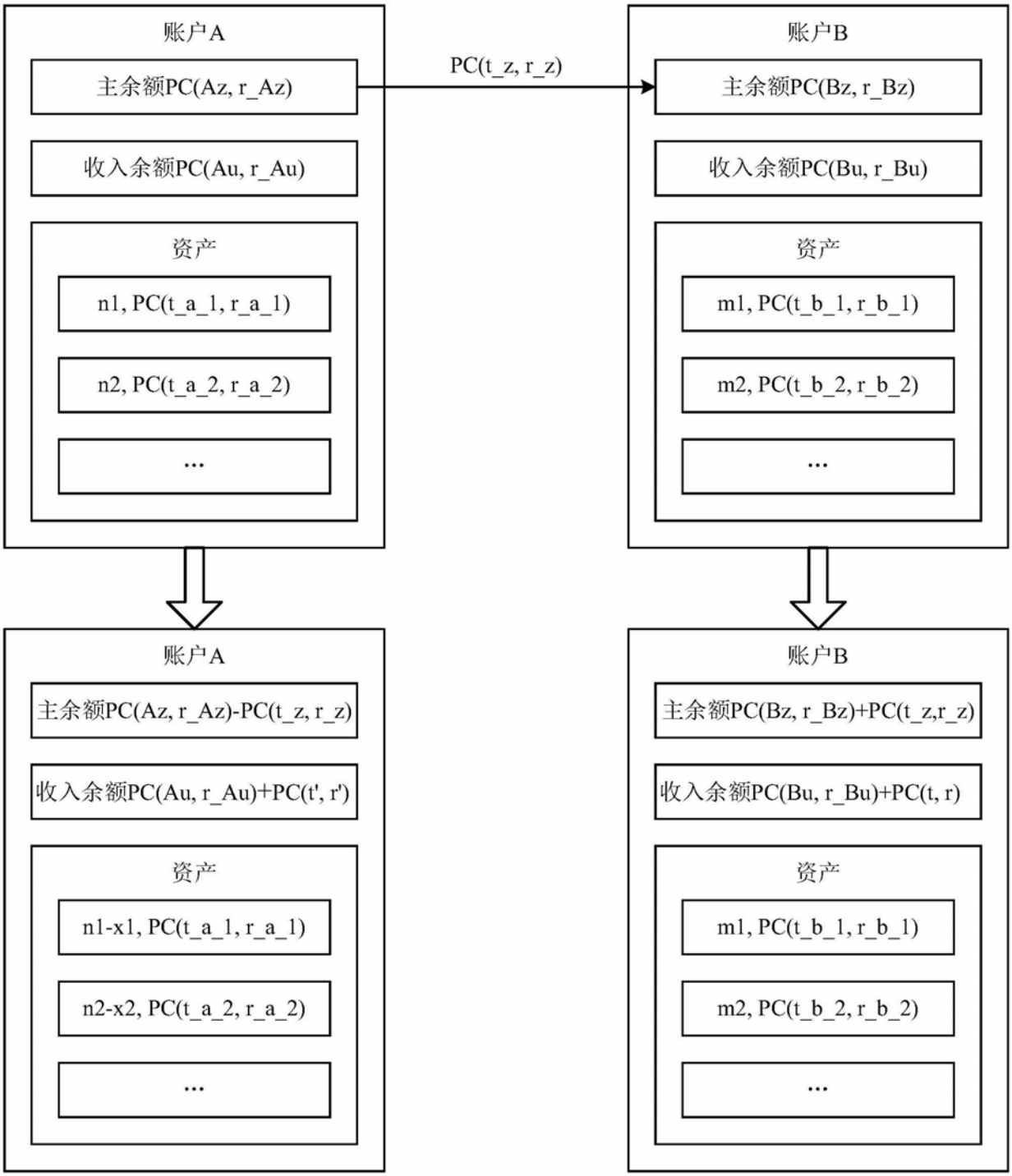
账户A
主余额PC(Az, r_Az)
收入余额PC(Au, r_Au)
资产
n1, PC(t_a_1, r_a_1)
n2, PC(t_a_2, r_a_2)
...
PC(t_z, r_z)
账户B
主余额PC(Bz, r_Bz)
收入余额PC(Bu, r_Bu)
资产
m1, PC(t_b_1, r_b_1)
m2, PC(t_b_2, r_b_2)
...
账户A
主余额PC(Az, r_Az)-PC(t_z, r_z)
收入余额PC(Au, r_Au)+PC(t', r')
资产
n1-x1, PC(t_a_1, r_a_1)
n2-x2, PC(t_a_2, r_a_2)
...
账户B
主余额PC(Bz, r_Bz)+PC(t_z,r_z)
收入余额PC(Bu, r_Bu)+PC(t, r)
资产
m1, PC(t_b_1, r_b_1)
m2, PC(t_b_2, r_b_2)
...

图13

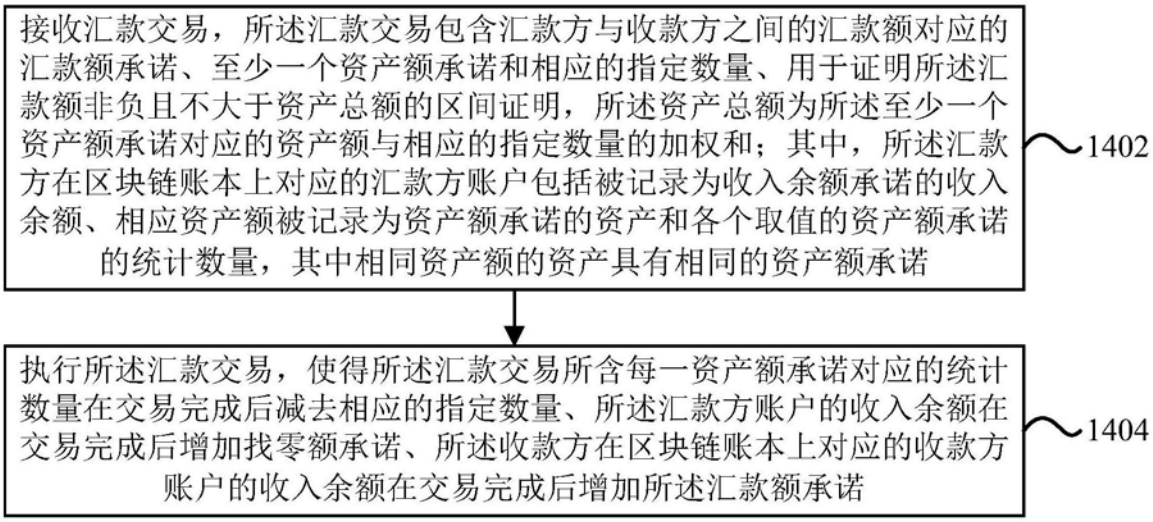
接收汇款交易，所述汇款交易包含汇款方与收款方之间的汇款额对应的汇款额承诺、至少一个资产额承诺和相应的指定数量、用于证明所述汇款额非负且不大于资产总额的区间证明，所述资产总额为所述至少一个资产额承诺对应的资产额与相应的指定数量的加权和；其中，所述汇款方在区块链账本上对应的汇款方账户包括被记录为收入余额承诺的收入余额、相应资产额被记录为资产额承诺的资产和各个取值的资产额承诺的统计数量，其中相同资产额的资产具有相同的资产额承诺
1402
执行所述汇款交易，使得所述汇款交易所含每一资产额承诺对应的统计数量在交易完成后减去相应的指定数量、所述汇款方账户的收入余额在交易完成后增加找零额承诺、所述收款方在区块链账本上对应的收款方账户的收入余额在交易完成后增加所述汇款额承诺
1404

图14

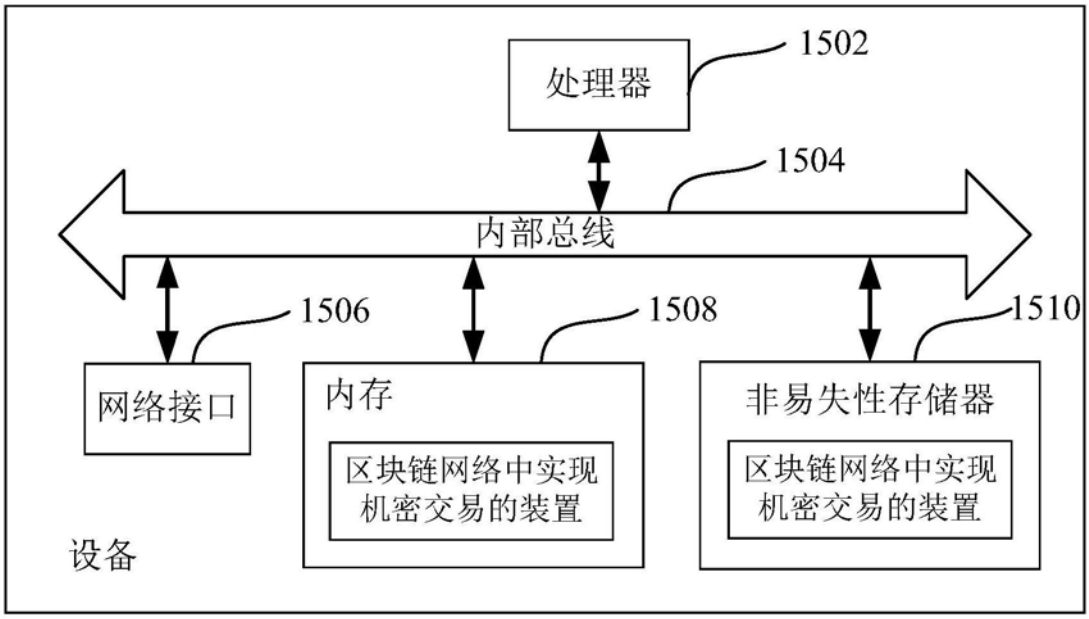
处理器
1502
1504
内部总线
1506
1508
1510
网络接口
内存
区块链网络中实现机密交易的装置
非易失性存储器
区块链网络中实现机密交易的装置
设备

图15


区块链网络中实现机密交易的装置
确定单元1601
汇款交易创建单元1602
汇款交易提交单元1603

图16

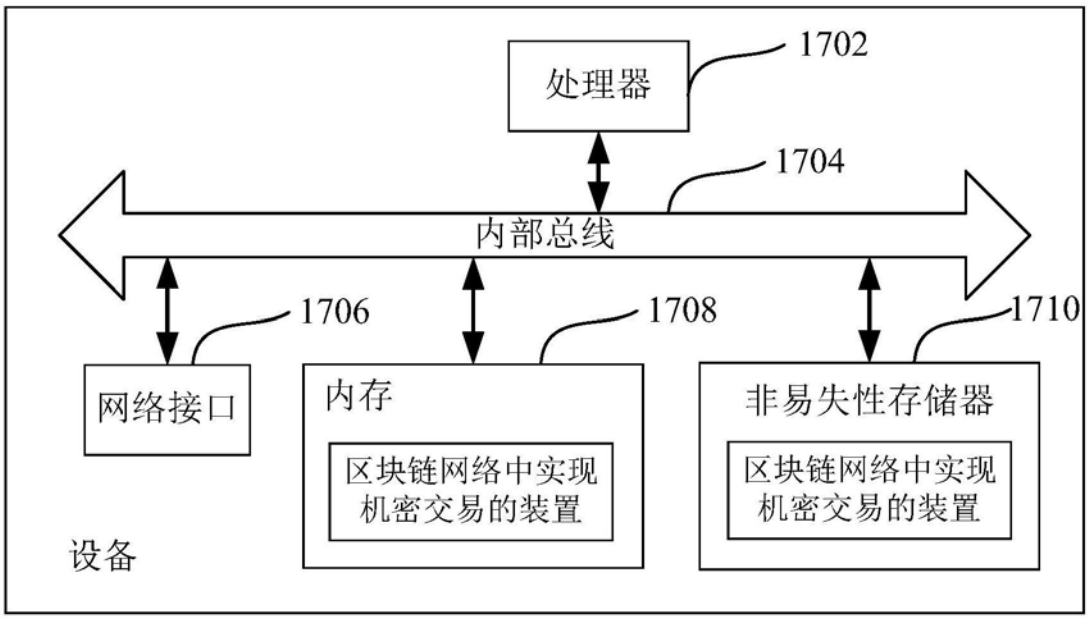
处理器
1702
1704
内部总线
1706
1708
1710
网络接口
内存
区块链网络中实现机密交易的装置
非易失性存储器
区块链网络中实现机密交易的装置
设备

图17

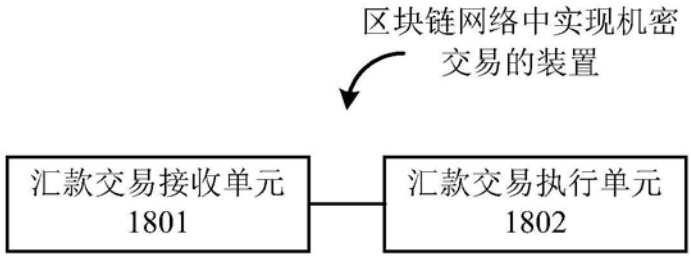
区块链网络中实现机密交易的装置
汇款交易接收单元
1801
汇款交易执行单元
1802

图18