(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 110033363 A
(43)申请公布日 2019.07.19

(21)申请号 201811530105.2

(22)申请日 2018.12.14

(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 黄章杰

(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 林祥

(51)Int.Cl.
G06Q 40/02(2012.01)
G06Q 40/04(2012.01)

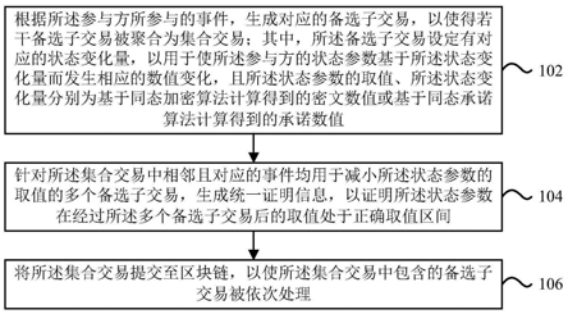
权利要求书4页 说明书22页 附图6页

(54)发明名称

基于区块链的事件处理方法及装置、电子设备

(57)摘要

本说明书一个或多个实施例提供一种基于区块链的事件处理方法及装置、电子设备，当应用于参与方时，该方法包括：根据该参与方所参与的事件，生成对应的备选子交易，以使得若干备选子交易被聚合为集合交易；其中，该备选子交易设定有对应的状态变化量，以用于使该参与方的状态参数基于该状态变化量而发生相应的数值变化，且该状态参数的取值、该状态变化量分别为基于同态加密算法或同态承诺算法计算得到；针对该集合交易中相邻且对应的事件均用于减小该状态参数的取值的多个备选子交易，生成统一证明信息；将该集合交易提交至区块链，以使该集合交易中包含的备选子交易被依次处理。



CN 110033363 A

1.一种基于区块链的事件处理方法,应用于参与方,所述方法包括:

根据所述参与方所参与的事件,生成对应的备选子交易,以使得若干备选子交易被聚合为集合交易;其中,所述备选子交易设定有对应的状态变化量,以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化,且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值;

针对所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易,生成统一证明信息,以证明所述状态参数在经过所述多个备选子交易后的取值处于正确取值区间;

将所述集合交易提交至区块链,以使所述集合交易中包含的备选子交易被依次处理。

2.根据权利要求1所述的方法,还包括:

当若干备选子交易被选取以用于聚合为所述集合交易时,识别每一被选取的备选子交易对应的事件对所述状态参数的取值的调整方式;

当至少两个备选子交易对应的事件均用于减小所述状态参数的取值时,将所述至少两个备选子交易相邻地排列于所述集合交易中。

3.根据权利要求1所述的方法,所述集合交易中包含分别对应于每一备选子交易的变化前状态值、变化后状态值,以配合于每一备选子交易中设定的状态变化量,使得每一备选子交易被处理后,所述参与方的状态参数由所述变化前状态值经由所述状态变化量而变化至所述变化后状态值;其中,所述变化前状态值和所述变化后状态值分别为基于所述同态加密算法计算得到的密文数值或基于所述同态承诺算法计算得到的承诺数值。

4.根据权利要求1所述的方法,还包括:

分别为所述集合交易中的每一备选子交易生成相应的独立证明信息,所述独立证明信息用于证明相应的备选子交易中设定的状态变化量处于所述正确数值区间。

5.根据权利要求1所述的方法,在所述事件对应的备选子交易中,包含所述参与方对所述事件的单方触发信息;其中,当所述事件的所有参与方分别向区块链提交的针对所述事件的单方触发信息均通过验证时,所述事件对应的备选子交易在区块链中被触发执行。

6.根据权利要求1所述的方法,还包括:

按照生成顺序为各个集合交易添加相应的编号,以使各个集合交易在区块链中被按照对应的编号大小进行依次处理。

7.一种基于区块链的事件处理方法,应用于区块链节点,所述方法包括:

接收参与方提交至区块链的集合交易,所述集合交易中包含若干备选子交易,所述备选子交易对应于所述参与方所参与的事件;其中,所述备选子交易设定有对应的状态变化量,以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化,且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值;

获取所述集合交易中的统一证明信息,所述统一证明信息对应于所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易,以验证所述状态参数在经过所述多个备选子交易后的取值是否处于正确取值区间;

根据验证结果确定对所述多个备选子交易的处理方式。

8.根据权利要求7所述的方法，

还包括：获取所述集合交易中对应于每一备选子交易的独立证明信息，以验证相应的备选子交易中设定的状态变化量是否处于所述正确数值区间；

所述根据验证结果确定对所述多个备选子交易的处理方式，包括：当所述验证结果为通过验证，且所述多个备选子交易中的任一备选子交易对应的独立证明信息通过验证时，触发执行所述任一备选子交易。

9.根据权利要求7所述的方法，还包括：

当所述集合交易中的任一备选子交易对应的事件用于增大所述状态参数的取值时，获取所述集合交易中对应于所述任一备选子交易的独立证明信息；

当对应于所述任一备选子交易的独立证明信息通过验证时，触发执行所述任一备选子交易。

10.根据权利要求7所述的方法，在所述事件对应的备选子交易中，包含所述参与方对所述事件的单方触发信息；所述方法还包括：

当所述事件的所有参与方分别向区块链提交的针对所述事件的单方触发信息均通过验证时，触发执行所述事件对应的备选子交易。

11.根据权利要求7所述的方法，还包括：

识别所述集合交易对应的编号，所述编号被按照各个集合交易的生成顺序而添加，以按照对应的编号大小对所述参与方提交的各个集合交易进行依次处理。

12.一种基于区块链的事件处理装置，应用于参与方，所述装置包括：

第一生成单元，根据所述参与方所参与的事件，生成对应的备选子交易，以使得若干备选子交易被聚合为集合交易；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值；

第二生成单元，针对所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，生成统一证明信息，以证明所述状态参数在经过所述多个备选子交易后的取值处于正确取值区间；

提交单元，将所述集合交易提交至区块链，以使所述集合交易中包含的备选子交易被依次处理。

13.根据权利要求12所述的装置，还包括：

识别单元，当若干备选子交易被选取以用于聚合为所述集合交易时，识别每一被选取的备选子交易对应的事件对所述状态参数的取值的调整方式；

排列单元，当至少两个备选子交易对应的事件均用于减小所述状态参数的取值时，将所述至少两个备选子交易相邻地排列于所述集合交易中。

14.根据权利要求12所述的装置，所述集合交易中包含分别对应于每一备选子交易的变化前状态值、变化后状态值，以配合于每一备选子交易中设定的状态变化量，使得每一备选子交易被处理后，所述参与方的状态参数由所述变化前状态值经由所述状态变化量而变化至所述变化后状态值；其中，所述变化前状态值和所述变化后状态值分别为基于所述同态加密算法计算得到的密文数值或基于所述同态承诺算法计算得到的承诺数值。

15.根据权利要求12所述的装置，还包括：

第三生成单元，分别为所述集合交易中的每一备选子交易生成相应的独立证明信息，所述独立证明信息用于证明相应的备选子交易中设定的状态变化量处于所述正确数值区间。

16.根据权利要求12所述的装置，在所述事件对应的备选子交易中，包含所述参与方对所述事件的单方触发信息；其中，当所述事件的所有参与方分别向区块链提交的针对所述事件的单方触发信息均通过验证时，所述事件对应的备选子交易在区块链中被触发执行。

17.根据权利要求12所述的装置，还包括：

添加单元，按照生成顺序为各个集合交易添加相应的编号，以使各个集合交易在区块链中被按照对应的编号大小进行依次处理。

18.一种基于区块链的事件处理装置，应用于区块链节点，所述装置包括：

接收单元，接收参与方提交至区块链的集合交易，所述集合交易中包含若干备选子交易，所述备选子交易对应于所述参与方所参与的事件；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值；

第一获取单元，获取所述集合交易中的统一证明信息，所述统一证明信息对应于所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，以验证所述状态参数在经过所述多个备选子交易后的取值是否处于正确取值区间；

确定单元，根据验证结果确定对所述多个备选子交易的处理方式。

19.根据权利要求18所述的装置，

还包括：第二获取单元，获取所述集合交易中对应于每一备选子交易的独立证明信息，以验证相应的备选子交易中设定的状态变化量是否处于所述正确数值区间；

所述确定单元具体用于：当所述验证结果为通过验证，且所述多个备选子交易中的任一备选子交易对应的独立证明信息通过验证时，触发执行所述任一备选子交易。

20.根据权利要求18所述的装置，还包括：

第三获取单元，当所述集合交易中的任一备选子交易对应的事件用于增大所述状态参数的取值时，获取所述集合交易中对应于所述任一备选子交易的独立证明信息；

第一触发单元，当对应于所述任一备选子交易的独立证明信息通过验证时，触发执行所述任一备选子交易。

21.根据权利要求18所述的装置，在所述事件对应的备选子交易中，包含所述参与方对所述事件的单方触发信息；所述装置还包括：

第二触发单元，当所述事件的所有参与方分别向区块链提交的针对所述事件的单方触发信息均通过验证时，触发执行所述事件对应的备选子交易。

22.根据权利要求18所述的装置，还包括：

识别单元，识别所述集合交易对应的编号，所述编号被按照各个集合交易的生成顺序而添加，以按照对应的编号大小对所述参与方提交的各个集合交易进行依次处理。

23.一种电子设备，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1-6中任一项所述的方法。

24.一种电子设备，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7-11中任一项所述的方法。

基于区块链的事件处理方法及装置、电子设备

技术领域

[0001] 本说明书一个或多个实施例涉及终端技术领域，尤其涉及一种基于区块链的事件处理方法及装置、电子设备。

背景技术

[0002] 在相关技术中，事件的参与方可以针对该事件生成相应的区块链交易，并通过向区块链中提交该区块链交易，使得该区块链交易可以被区块链节点所执行，从而完成该事件的实施。

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基于区块链的事件处理方法及装置、电子设备。

[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，提出了一种基于区块链的事件处理方法，应用于参与方，所述方法包括：

[0006] 根据所述参与方所参与的事件，生成对应的备选子交易，以使得若干备选子交易被聚合为集合交易；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于所述同态承诺算法计算得到的承诺数值；

[0007] 针对所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，生成统一证明信息，以证明所述状态参数在经过所述多个备选子交易后的取值处于正确取值区间；

[0008] 将所述集合交易提交至区块链，以使所述集合交易中包含的备选子交易被依次处理。

[0009] 根据本说明书一个或多个实施例的第二方面，提出了一种基于区块链的事件处理方法，应用于区块链节点，所述方法包括：

[0010] 接收参与方提交至区块链的集合交易，所述集合交易中包含若干备选子交易，所述备选子交易对应于所述参与方所参与的事件；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值；

[0011] 获取所述集合交易中的统一证明信息，所述统一证明信息对应于所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，以验证所述状态参数在经过所述多个备选子交易后的取值是否处于正确取值区间；

[0012] 根据验证结果确定对所述多个备选子交易的处理方式。

[0013] 根据本说明书一个或多个实施例的第三方面，提出了一种基于区块链的事件处理装置，应用于参与方，所述装置包括：

[0014] 第一生成单元，根据所述参与方所参与的事件，生成对应的备选子交易，以使得若干备选子交易被聚合为集合交易；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值；

[0015] 第二生成单元，针对所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，生成统一证明信息，以证明所述状态参数在经过所述多个备选子交易后的取值处于正确取值区间；

[0016] 提交单元，将所述集合交易提交至区块链，以使所述集合交易中包含的备选子交易被依次处理。

[0017] 根据本说明书一个或多个实施例的第四方面，提出了一种基于区块链的事件处理装置，应用于区块链节点，所述装置包括：

[0018] 接收单元，接收参与方提交至区块链的集合交易，所述集合交易中包含若干备选子交易，所述备选子交易对应于所述参与方所参与的事件；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值；

[0019] 第一获取单元，获取所述集合交易中的统一证明信息，所述统一证明信息对应于所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，以验证所述状态参数在经过所述多个备选子交易后的取值是否处于正确取值区间；

[0020] 确定单元，根据验证结果确定对所述多个备选子交易的处理方式。

[0021] 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：

[0022] 处理器；

[0023] 用于存储处理器可执行指令的存储器；

[0024] 其中，所述处理器通过运行所述可执行指令以实现如上述第一方面所述的方法。

[0025] 根据本说明书一个或多个实施例的第六方面，提出了一种电子设备，包括：

[0026] 处理器；

[0027] 用于存储处理器可执行指令的存储器；

[0028] 其中，所述处理器通过运行所述可执行指令以实现如上述第二方面所述的方法。

附图说明

[0029] 图1是一示例性实施例提供的一种基于区块链的事件处理方法的流程图。

[0030] 图2是一示例性实施例提供的另一种基于区块链的事件处理方法的流程图。

[0031] 图3是一示例性实施例提供的一种跨境汇款的场景示意图。

[0032] 图4是一示例性实施例的一种跨境汇款过程中的交互示意图。

[0033] 图5是一示例性实施例提供的一种区块链交易的内容示意图。

[0034] 图6是一示例性实施例提供的一种统计触发情况的示意图。

[0035] 图7是一示例性实施例提供的一种设备的结构示意图。

[0036] 图8是一示例性实施例提供的一种基于区块链的事件处理装置的框图。

[0037] 图9是一示例性实施例提供的另一种设备的结构示意图。

[0038] 图10是一示例性实施例提供的另一种基于区块链的事件处理装置的框图。

具体实施方式

[0039] 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。

[0040] 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。

[0041] 图1是一示例性实施例提供的一种基于区块链的事件处理方法的流程图。如图1所示，该方法应用于参与方，可以包括以下步骤：

[0042] 步骤102，根据所述参与方所参与的事件，生成对应的备选子交易，以使得若干备选子交易被聚合为集合交易；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值。

[0043] 在一实施例中，本说明书的事件可以包括任意类型、覆盖任意场景，比如投票、签订协议、流量分配、转账、跨境汇款等，本说明书并不对此进行限制。以投票为例，描述信息可以包括投票事由和投票选项等信息，而各个参与方向区块链中提交的触发信息可以包括对投票选项的选择结果，从而触发完成投票操作。

[0044] 在一实施例中，事件可以存在多个参与方，每一参与方对应于参与对象，该参与对象可以为个人、企业、组织等，本说明书并不对此进行限制。参与对象存在对应的数字身份，使得承载该数字身份的电子设备相当于被配置为该参与对象所对应的参与方。

[0045] 在一实施例中，备选子交易中包含事件的描述信息，该描述信息用于描述相关事件的情况，使得该备选子交易被处理时，可以根据该描述信息实施相应的事件。例如，描述信息可以表征相关事件的执行逻辑、所涉及的参与方、对参与方的状态参数的改变方式(如增大或减小状态参数的取值)、状态变化量等，本说明书并不对此进行限制。实际上，事件的相关内容可由各个参与方之间预先通过任意方式进行沟通，然后由所述任一参与方进行起草该事件的描述信息，使得事件的其他参与方可以根据预先的沟通结果对该描述信息的内容进行查看和确认；当然，所述任一参与方也可以在并未预先沟通的情况下，自行确定事件的其他参与方以及描述信息中的其他内容，本说明书并不对此进行限制。

[0046] 在一实施例中，事件的描述信息可由该事件的任一参与方生成，并添加为该任一

参与方维护的等待队列中的备选子交易。以及，该任一参与方还将生成的描述信息分享至其他参与方，使得其他参与方对描述信息进行确认。

[0047] 在一实施例中，任一参与方可以将描述信息通过链外通道发送至事件的其他参与方。通过链外通道将描述信息发送至事件的其他参与方，可以实现对描述信息的高效传输。其中，链外通道可以为事件的各个参与方之间建立的加密通道或其他形式的安全通道，以避免发生信息泄露。

[0048] 在一实施例中，任一参与方可以通过向区块链提交一笔交易，并将上述的描述信息包含于该交易中，使得该交易在经过共识后可以被发送至区块链中的所有区块链节点；而事件的每一参与方均可以被配置为区块链中的区块链节点，或者每一参与方可以在区块链中存在对应的区块链节点，使得每一参与方可以通过自身或对应的区块链节点所维护的区块链账本(区块链账本包含区块链的全量交易数据)，获得上述交易及其包含的描述信息，从而使得上述的描述信息被同步至事件的其他参与方。

[0049] 在一实施例中，任一参与方在生成描述信息时，该描述信息中的状态变化量可以为密文数值或承诺数值。比如当状态变化量的明文数值为t1时，若采用Pedersen承诺机制，可以根据该明文数值t1与随机数r1生成相应的密文承诺T1，而描述信息中可以包含该T1、t1和r1，使得事件的其他参与方可以验证密文承诺T1与明文数值t1、随机数r1之间的对应关系。其中，描述信息中可以对明文数值t1和随机数r1进行加密保护，比如当描述信息需要被发送至参与方X时，可以采用该参与方X的数字身份对应的身份公钥进行加密，分别得到加密后的Enc_X(t1)、Enc_X(r1)并添加至描述信息中，因而只有参与方X能够通过自身的身份私钥对Enc_X(t1)、Enc_X(r1)进行解密得到上述的明文数值t1和随机数r1，显著提升了数据安全性。当然，除了采用公钥加密方式之外，还可以采用相关技术中的其他任意加密方式，比如数字信封等，本说明书并不对此进行限制。

[0050] 在一实施例中，当存在多个其他参与方时，描述信息可以分别包含对应于各个其他参与方的加密后数据。例如，当其他参数方包括参与方X和参与方Y时，可以根据参与方X的身份公钥对明文数值t1、随机数r1分别加密得到Enc_X(t1)、Enc_X(r1)，以及根据参与方Y的身份公钥对明文数值t1、随机数r1分别加密得到Enc_Y(t1)、Enc_Y(r1)，并将Enc_X(t1)、Enc_X(r1)、Enc_Y(t1)和Enc_Y(r1)均添加至描述信息中，使得所述任一参与方只需要准备一份描述信息并分别发送至各个其他参与方，而无需针对每一其他参与方准备不同的描述信息。当然，所述任一参与方可以针对每一其他参与方准备不同的描述信息，比如在发送至参与方X的描述信息中包含Enc_X(t1)和Enc_X(r1)，而在发送至参与方Y的描述信息中包含Enc_Y(t1)和Enc_Y(r1)，本说明书并不对此进行限制。

[0051] 在一实施例中，参与方可以维护有等待队列，该等待队列中包含该参与方所参与的各个事件对应的备选子交易；而通过从所述等待队列中选取若干备选子交易，可以生成相应的集合交易。集合交易中可以包含多个备选子交易，每一备选子交易分别对应于上述参与方所参与的一个事件，使得该集合交易被提交至区块链后，所包含的多个备选子交易均可以在区块链中被处理，从而使得这些备选子交易对应的多个事件被实施。可见，通过在集合交易中包含多个备选子交易，使得这些备选子交易被批量提交至区块链，可以减少向区块链提交的交易数量，无需针对每一备选子交易均生成一笔区块链交易，有助于降低资源消耗、提升处理效率。

[0052] 在一实施例中，可以在所述等待队列中的备选子交易达到预设数量时，选取所述等待队列中已存在的备选子交易(即预设数量的备选子交易)，以生成相应的集合交易。在另一实施例中，可以按照预设时长周期性地选取所述等待队列中已存在的备选子交易，以生成相应的集合交易；当然，每一集合交易的容量可以存在最大限制，使得同一周期内选取的备选子交易的数量存在相应的最大值，超出的部分可以延期至下一周期进行选取。当然，还可以通过其他的预设规则来选取备选子交易，本说明书并不对此进行限制。

[0053] 在一实施例中，等待队列中的备选子交易可以按照添加时刻进行依次排列，而每次可以从前向后依次选取各个备选子交易，使得在先生成的备选子交易可以被优先选取。当然，参与方也可以根据实际需求，比如事件的紧急程度、事件的优先级等，对等待队列中的备选子交易实施与顺序无关的选取操作；或者，等待队列本身就可以按照上述的紧急程度、优先级等进行排列，这样依然可以视为依次选取。

[0054] 在一实施例中，事件的描述信息可以包括状态变化量，而所述事件可以用于使各个参与方在区块链上对应记录的状态参数按照所述状态变化量发生取值变化，比如增大取值、减小取值等。其中，根据事件的类型或场景差异，相应的状态参数也可能不同，比如转账或跨境汇款场景下的状态参数可以为参与方的账户余额，再比如流量分配场景下的状态参数可以为参与方持有的剩余流量的数额，本说明书并不对此进行限制。

[0055] 步骤104，针对所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，生成统一证明信息，以证明所述状态参数在经过所述多个备选子交易后的取值处于正确取值区间。

[0056] 在一实施例中，通过生成上述的统一证明信息，使得上述的多个备选子交易可以仅生成一个统一证明信息，而无需分别、单独生成对应的证明信息，有助于简化证明信息、提升处理效率。

[0057] 在一实施例中，“针对所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，生成统一证明信息”并不一定是指仅由该多个备选子交易来生成统一证明信息，如果集合交易中还存在排列于该多个备选子交易之前的其他备选子交易，那么该其他备选子交易同样会对状态参数的取值造成影响，因而统一证明信息还跟该其他备选子交易相关。换言之，如果集合交易中存在排列于该多个备选子交易之前的其他备选子交易，那么状态参数在经历该多个备选子交易之前，还需经历该其他备选子交易所带来的取值变化，而统一证明信息用于证明状态参数在该其他备选子交易和该多个备选子交易的共同作用后的取值处于正确取值区间。

[0058] 例如，当集合交易包含的备选子交易依次为“减减减加加”(“减”代表用于减小状态参数的取值的备选子交易，“加”代表用于增大状态参数的取值的备选子交易)时，可以针对前三个连续的备选子交易生成统一证明信息，此时由于这三个备选子交易之前并不存在其他备选子交易，因而状态参数仅受这三个备选子交易的作用而产生取值变化，统一证明信息用于证明该变化后的取值处于正确数值区间。

[0059] 再例如，当集合交易包含的备选子交易依次为“加加减加减减减加”时，可以针对第五、第六、第七共三个连续的备选子交易生成统一证明信息，此时由于这三个备选子交易之前存在第一、第二、第三、第四共四个其他备选子交易，因而状态参数不仅受到三个连续的“减”的备选子交易的作用，还受到四个其他备选子交易的作用，统一证明信息用于证明

状态参数在这七个备选子交易的作用下而产生取值变化后，该变化后的取值处于正确数值区间。

[0060] 在一实施例中，上述“对应的事件均用于减小所述状态参数的取值的多个备选子交易”可以是恰好处于相邻位置，而并未实施特别的排序处理，这使得一些情况下，多个符合条件的备选子交易可能并未相邻设置、导致无法采用本说明书来生成统一证明信息，还可能使得多个符合条件的备选子交易无法完全连续排列、被进一步分割为多组，那么每组仍然可以分别生成统一证明信息，只是无法为多个符合条件的备选子交易生成一份统一证明信息。

[0061] 在一实施例中，当若干备选子交易被选取以用于聚合为所述集合交易时，可以识别每一被选取的备选子交易对应的事件对所述状态参数的取值的调整方式；当至少两个备选子交易对应的事件均用于减小所述状态参数的取值时，可以将所述至少两个备选子交易相邻地排列于所述集合交易中。换言之，在聚合形成集合交易时，可以主动对各个备选子交易进行排序，并尽量将用于减小状态参数取值的备选子交易都进行相邻排列，从而使得这些备选子交易可以仅生成一份统一证明信息，可以尽量减少证明信息的数量。

[0062] 在一实施例中，当采用密文数值或承诺数值时，对于集合交易中单独存在的、对应的事件均用于减小所述状态参数的取值的多个备选子交易，参与方可以单独为其生成证明信息，以证明状态参数在经过该多个备选子交易后的取值处于正确取值区间。

[0063] 在一实施例中，各个参与方对应的状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值。对于同态加密算法而言，可以采用任意类型的同态加密算法，只要确保该同态加密算法能够满足加法同态，使得即便处于密文状态下，仍然能够使得状态参数的取值增加或减少该状态变化量；对于该同态加密算法为加法同态加密算法或全同态加密算法，本说明书并不对此进行限制。对于同态承诺算法而言，当采用相关技术中的Pedersen承诺机制时，可以为未加密数据确定一随机数，并基于该随机数与未加密数据进行计算得到相应的承诺数值。

[0064] 在一实施例中，当状态参数的取值、状态变化量为密文数值或承诺数值时，参与方需要提供相关的证明信息，以使得区块链节点在执行相关交易时，能够确定交易的合法有效性。例如，当事件用于使得某一参与方对应的状态参数按照该状态变化量发生取值减小时，即交易目的是使得该某一参与方的状态参数的取值减小该状态变化量，譬如上述的统一证明信息用于证明：该参与方的状态参数的取值足以实施上述集合交易中相邻的多个“减小”类型的备选子交易(即状态参数的取值不小于该相邻的多个“减小”类型的备选子交易所对应的状态变化量之和)。

[0065] 例如，所述集合交易中可以包含分别对应于每一备选子交易的变化前状态值、变化后状态值，以配合于每一备选子交易中设定的状态变化量，使得每一备选子交易被处理后，所述参与方的状态参数由所述变化前状态值经由所述状态变化量而变化至所述变化后状态值；其中，所述变化前状态值和所述变化后状态值分别为基于所述同态加密算法计算得到的密文数值或基于所述同态承诺算法计算得到的承诺数值。那么，统一证明信息可以用于证明：在上述相邻的多个“减小”类型的备选子交易中，最后一个备选子交易的变化后状态值不小于0。

[0066] 在一实施例中，当采用密文数值或承诺数值时，对于集合交易中的每一备选子交

易，不论其用于增大或减小状态参数的取值，均生成相应的独立证明信息，所述独立证明信息用于证明相应的备选子交易中设定的状态变化量处于所述正确数值区间。例如，独立证明信息可以用于表明相应的状态变化量处于正确数值区间，譬如$[0,2^{64})$。

[0067] 在一实施例中，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，生成上述的证明信息，本说明书并不对此进行限制。

[0068] 步骤106，将所述集合交易提交至区块链，以使所述集合交易中包含的备选子交易被依次处理。

[0069] 在一实施例中，参与方可以按照生成顺序为各个合并交易添加编号，使各个合并交易在区块链中被按照对应编号的大小进行依次处理。换言之，区块链交易在收到参与方提交的合并交易后，需要读取合并交易所包含的编号；如果编号与先前处理的合并交易的编号连续，比如最新处理的合并交易的编号为99、当前收到的合并交易的编号为100，则可以对该编号为100的合并交易进行处理；如果编号之间并不连续，比如最新处理的合并交易的编号为99、当前收到的合并交易的编号为101，则区块链节点需要等待并优先处理编号为100的合并交易，然后才能处理编号为101的合并交易。由于每条交易被执行后都可能导致该参与方的状态参数发生变化，而在后交易的执行需要依赖于先前交易执行后的状态参数的取值，因而需要确保各个合并交易被按照对应编号的大小进行依次处理，以使得各个合并交易均能够正确执行。

[0070] 在一实施例中，在事件对应的备选子交易中，包含所述参与方对所述事件的单方触发信息；其中，当所述事件的所有参与方分别向区块链提交的针对所述事件的单方触发信息均通过验证时，所述事件对应的备选子交易在区块链中被触发执行。单方触发信息表明相应的参与方对事件的描述信息予以确认，希望触发事件的执行；而事件的每一参与方都需要分别向区块链提交单方触发信息，使得区块链节点基于所有参与方分别提交的单方触发信息，确定是否应当执行相应的备选子交易所指示的事件。例如，事件的任一参与方生成描述信息并提供至其他参与方后，不仅该任一参与方需要向自身维护的等待队列中添加相应的备选子交易，每一其他参与方在对描述信息予以确认后，也分别向自身维护的等待队列中添加相应的备选子交易；以及，每一参与方分别基于自身维护的等待队列生成集合交易，从而通过将集合交易提交至区块链，使得上述的单方触发信息被提交至区块链，以供区块链节点进行验证。单方触发信息中可以包含描述信息和相应参与方对描述信息生成的签名；签名属于相应参与方提供的确认信息，而如果采用密文数值或承诺数值，确认信息还包含证明信息，这在上文中已经详细描述。通过由各个参与方分别向区块链提交单方触发信息，而非某一参与方提交多方触发信息，不仅可以对处理压力进行分担、防止单个参与方的处理压力过大，还可使各个参与方根据自身的实际情况(如处理压力、优先级管理等)对所参与的各个事件进行选择性地处理甚至批量处理。

[0071] 与图1所示实施例相对应地，图2是一示例性实施例提供的另一种基于区块链的事件处理方法的流程图。如图2所示，该方法应用于区块链节点，可以包括以下步骤：

[0072] 步骤202，接收参与方提交至区块链的集合交易，所述集合交易中包含若干备选子交易，所述备选子交易对应于所述参与方所参与的事件；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变

化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值。

[0073] 在一实施例中，本说明书的事件可以包括任意类型、覆盖任意场景，比如投票、签订协议、流量分配、转账、跨境汇款等，本说明书并不对此进行限制。以投票为例，描述信息可以包括投票事由和投票选项等信息，而各个参与方向区块链中提交的触发信息可以包括对投票选项的选择结果，从而触发完成投票操作。

[0074] 在一实施例中，事件可以存在多个参与方，每一参与方对应于参与对象，该参与对象可以为个人、企业、组织等，本说明书并不对此进行限制。参与对象存在对应的数字身份，使得承载该数字身份的电子设备相当于被配置为该参与对象所对应的参与方。

[0075] 在一实施例中，备选子交易中包含事件的描述信息，该描述信息用于描述相关事件的情况，使得该备选子交易被处理时，可以根据该描述信息实施相应的事件。例如，描述信息可以表征相关事件的执行逻辑、所涉及的参与方、对参与方的状态参数的改变方式(如增大或减小状态参数的取值)、状态变化量等，本说明书并不对此进行限制。实际上，事件的相关内容可由各个参与方之间预先通过任意方式进行沟通，然后由所述任一参与方进行起草该事件的描述信息，使得事件的其他参与方可以根据预先的沟通结果对该描述信息的内容进行查看和确认；当然，所述任一参与方也可以在并未预先沟通的情况下，自行确定事件的其他参与方以及描述信息中的其他内容，本说明书并不对此进行限制。

[0076] 在一实施例中，事件的描述信息可由该事件的任一参与方生成，并添加为该任一参与方维护的等待队列中的备选子交易。以及，该任一参与方还将生成的描述信息分享至其他参与方，使得其他参与方对描述信息进行确认。

[0077] 在一实施例中，任一参与方可以将描述信息通过链外通道发送至事件的其他参与方。通过链外通道将描述信息发送至事件的其他参与方，可以实现对描述信息的高效传输。其中，链外通道可以为事件的各个参与方之间建立的加密通道或其他形式的安全通道，以避免发生信息泄露。

[0078] 在一实施例中，任一参与方可以通过向区块链提交一笔交易，并将上述的描述信息包含于该交易中，使得该交易在经过共识后可以被发送至区块链中的所有区块链节点；而事件的每一参与方均可以被配置为区块链中的区块链节点，或者每一参与方可以在区块链中存在对应的区块链节点，使得每一参与方可以通过自身或对应的区块链节点所维护的区块链账本(区块链账本包含区块链的全量交易数据)，获得上述交易及其包含的描述信息，从而使得上述的描述信息被同步至事件的其他参与方。

[0079] 在一实施例中，任一参与方在生成描述信息时，该描述信息中的状态变化量可以为密文数值或承诺数值。比如当状态变化量的明文数值为t1时，若采用Pedersen承诺机制，可以根据该明文数值t1与随机数r1生成相应的密文承诺T1，而描述信息中可以包含该T1、t1和r1，使得事件的其他参与方可以验证密文承诺T1与明文数值t1、随机数r1之间的对应关系。其中，描述信息中可以对明文数值t1和随机数r1进行加密保护，比如当描述信息需要被发送至参与方X时，可以采用该参与方X的数字身份对应的身份公钥进行加密，分别得到加密后的Enc_X(t1)、Enc_X(r1)并添加至描述信息中，因而只有参与方X能够通过自身的身份私钥对Enc_X(t1)、Enc_X(r1)进行解密得到上述的明文数值t1和随机数r1，显著提升了数据安全性。当然，除了采用公钥加密方式之外，还可以采用相关技术中的其他任意加密方

式,比如数字信封等,本说明书并不对此进行限制。

[0080] 在一实施例中,当存在多个其他参与方时,描述信息可以分别包含对应于各个其他参与方的加密后数据。例如,当其他参数方包括参与方X和参与方Y时,可以根据参与方X的身份公钥对明文数值t1、随机数r1分别加密得到Enc_X(t1)、Enc_X(r1),以及根据参与方Y的身份公钥对明文数值t1、随机数r1分别加密得到Enc_Y(t1)、Enc_Y(r1),并将Enc_X(t1)、Enc_X(r1)、Enc_Y(t1)和Enc_Y(r1)均添加至描述信息中,使得所述任一参与方只需要准备一份描述信息并分别发送至各个其他参与方,而无需针对每一其他参与方准备不同的描述信息。当然,所述任一参与方可以针对每一其他参与方准备不同的描述信息,比如在发送至参与方X的描述信息中包含Enc_X(t1)和Enc_X(r1),而在发送至参与方Y的描述信息中包含Enc_Y(t1)和Enc_Y(r1),本说明书并不对此进行限制。

[0081] 在一实施例中,参与方可以维护有等待队列,该等待队列中包含该参与方所参与的各个事件对应的备选子交易;而通过从所述等待队列中选取若干备选子交易,可以生成相应的集合交易。集合交易中可以包含多个备选子交易,每一备选子交易分别对应于上述参与方所参与的一个事件,使得该集合交易被提交至区块链后,所包含的多个备选子交易均可以在区块链中被处理,从而使得这些备选子交易对应的多个事件被实施。可见,通过在集合交易中包含多个备选子交易,使得这些备选子交易被批量提交至区块链,可以减少向区块链提交的交易数量,无需针对每一备选子交易均生成一笔区块链交易,有助于降低资源消耗、提升处理效率。

[0082] 在一实施例中,可以在所述等待队列中的备选子交易达到预设数量时,选取所述等待队列中已存在的备选子交易(即预设数量的备选子交易),以生成相应的集合交易。在另一实施例中,可以按照预设时长周期性地选取所述等待队列中已存在的备选子交易,以生成相应的集合交易;当然,每一集合交易的容量可以存在最大限制,使得同一周期内选取的备选子交易的数量存在相应的最大值,超出的部分可以延期至下一周期进行选取。当然,还可以通过其他的预设规则来选取备选子交易,本说明书并不对此进行限制。

[0083] 在一实施例中,等待队列中的备选子交易可以按照添加时刻进行依次排列,而每次可以从前向后依次选取各个备选子交易,使得在先生成的备选子交易可以被优先选取。当然,参与方也可以根据实际需求,比如事件的紧急程度、事件的优先级等,对等待队列中的备选子交易实施与顺序无关的选取操作;或者,等待队列本身就可以按照上述的紧急程度、优先级等进行排列,这样依然可以视为依次选取。

[0084] 在一实施例中,事件的描述信息可以包括状态变化量,而所述事件可以用于使各个参与方在区块链上对应记录的状态参数按照所述状态变化量发生取值变化,比如增大取值、减小取值等。其中,根据事件的类型或场景差异,相应的状态参数也可能不同,比如转账或跨境汇款场景下的状态参数可以为参与方的账户余额,再比如流量分配场景下的状态参数可以为参与方持有的剩余流量的数额,本说明书并不对此进行限制。

[0085] 步骤204,获取所述集合交易中的统一证明信息,所述统一证明信息对应于所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易,以验证所述状态参数在经过所述多个备选子交易后的取值是否处于正确取值区间。

[0086] 在一实施例中,通过生成上述的统一证明信息,使得上述的多个备选子交易可以仅生成一个统一证明信息,而无需分别、单独生成对应的证明信息,有助于简化证明信息、

提升处理效率。

[0087] 在一实施例中，“针对所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，生成统一证明信息”并不一定是指仅由该多个备选子交易来生成统一证明信息，如果集合交易中还存在排列于该多个备选子交易之前的其他备选子交易，那么该其他备选子交易同样会对状态参数的取值造成影响，因而统一证明信息还跟该其他备选子交易相关。换言之，如果集合交易中存在排列于该多个备选子交易之前的其他备选子交易，那么状态参数在经历该多个备选子交易之前，还需经历该其他备选子交易所带来的取值变化，而统一证明信息用于证明状态参数在该其他备选子交易和该多个备选子交易的共同作用后的取值处于正确取值区间。

[0088] 例如，当集合交易包含的备选子交易依次为“减减减加加”(“减”代表用于减小状态参数的取值的备选子交易，“加”代表用于增大状态参数的取值的备选子交易)时，可以针对前三个连续的备选子交易生成统一证明信息，此时由于这三个备选子交易之前并不存在其他备选子交易，因而状态参数仅受这三个备选子交易的作用而产生取值变化，统一证明信息用于证明该变化后的取值处于正确数值区间。

[0089] 再例如，当集合交易包含的备选子交易依次为“加加减加减减减加”时，可以针对第五、第六、第七共三个连续的备选子交易生成统一证明信息，此时由于这三个备选子交易之前存在第一、第二、第三、第四共四个其他备选子交易，因而状态参数不仅受到三个连续的“减”的备选子交易的作用，还受到四个其他备选子交易的作用，统一证明信息用于证明状态参数在这七个备选子交易的作用下而产生取值变化后，该变化后的取值处于正确数值区间。

[0090] 在一实施例中，上述“对应的事件均用于减小所述状态参数的取值的多个备选子交易”可以是恰好处于相邻位置，而并未实施特别的排序处理，这使得一些情况下，多个符合条件的备选子交易可能并未相邻设置、导致无法采用本说明书来生成统一证明信息，还可能使得多个符合条件的备选子交易无法完全连续排列、被进一步分割为多组，那么每组仍然可以分别生成统一证明信息，只是无法为多个符合条件的备选子交易生成一份统一证明信息。

[0091] 在一实施例中，当若干备选子交易被选取以用于聚合为所述集合交易时，可以识别每一被选取的备选子交易对应的事件对所述状态参数的取值的调整方式；当至少两个备选子交易对应的事件均用于减小所述状态参数的取值时，可以将所述至少两个备选子交易相邻地排列于所述集合交易中。换言之，在聚合形成集合交易时，可以主动对各个备选子交易进行排序，并尽量将用于减小状态参数取值的备选子交易都进行相邻排列，从而使得这些备选子交易可以仅生成一份统一证明信息，可以尽量减少证明信息的数量。

[0092] 在一实施例中，当采用密文数值或承诺数值时，对于集合交易中单独存在的、对应的事件均用于减小所述状态参数的取值的多个备选子交易，参与方可以单独为其生成证明信息，以证明状态参数在经过该多个备选子交易后的取值处于正确取值区间。

[0093] 在一实施例中，各个参与方对应的状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值。对于同态加密算法而言，可以采用任意类型的同态加密算法，只要确保该同态加密算法能够满足加法同态，使得即便处于密文状态下，仍然能够使得状态参数的取值增加或减少该状态变化量；

对于该同态加密算法为加法同态加密算法或全同态加密算法，本说明书并不对此进行限制。对于同态承诺算法而言，当采用相关技术中的Pedersen承诺机制时，可以为未加密数据确定一随机数，并基于该随机数与未加密数据进行计算得到相应的承诺数值。

[0094] 在一实施例中，当状态参数的取值、状态变化量为密文数值或承诺数值时，参与方需要提供相关的证明信息，以使得区块链节点在执行相关交易时，能够确定交易的合法有效性。例如，当事件用于使得某一参与方对应的状态参数按照该状态变化量发生取值减小时，即交易目的是使得该某一参与方的状态参数的取值减小该状态变化量，譬如上述的统一证明信息用于证明：该参与方的状态参数的取值足以实施上述集合交易中相邻的多个“减小”类型的备选子交易(即状态参数的取值不小于该相邻的多个“减小”类型的备选子交易所对应的状态变化量之和)。

[0095] 例如，所述集合交易中可以包含分别对应于每一备选子交易的变化前状态值、变化后状态值，以配合于每一备选子交易中设定的状态变化量，使得每一备选子交易被处理后，所述参与方的状态参数由所述变化前状态值经由所述状态变化量而变化至所述变化后状态值；其中，所述变化前状态值和所述变化后状态值分别为基于所述同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值。那么，统一证明信息可以用于证明：在上述相邻的多个“减小”类型的备选子交易中，最后一个备选子交易的变化后状态值不小于0。

[0096] 在一实施例中，当采用密文数值或承诺数值时，对于集合交易中的每一备选子交易，不论其用于增大或减小状态参数的取值，均生成相应的独立证明信息，所述独立证明信息用于证明相应的备选子交易中设定的状态变化量处于所述正确数值区间。例如，独立证明信息可以用于表明相应的状态变化量处于正确数值区间，譬如$[0,2^{64})$。

[0097] 在一实施例中，区块链节点可以获取所述集合交易中对应于每一备选子交易的独立证明信息，以验证相应的备选子交易中设定的状态变化量是否处于所述正确数值区间；其中，当区块链节点针对统一证明信息的验证结果为通过验证，且所述多个备选子交易中的任一备选子交易对应的独立证明信息通过验证时，区块链节点可以触发执行所述任一备选子交易。

[0098] 在一实施例中，区块链节点可以在所述集合交易中的任一备选子交易对应的事件用于增大所述状态参数的取值时，获取所述集合交易中对应于所述任一备选子交易的独立证明信息；其中，当对应于所述任一备选子交易的独立证明信息通过验证时，区块链节点可以触发执行所述任一备选子交易。

[0099] 在一实施例中，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，生成上述的证明信息，本说明书并不对此进行限制。

[0100] 步骤206，根据验证结果确定对所述多个备选子交易的处理方式。

[0101] 在一实施例中，参与方可以按照生成顺序为各个合并交易添加编号，使各个合并交易在区块链中被按照对应编号的大小进行依次处理。换言之，区块链交易在收到参与方提交的合并交易后，需要读取合并交易所包含的编号；如果编号与先前处理的合并交易的编号连续，比如最新处理的合并交易的编号为99、当前收到的合并交易的编号为100，则可以对该编号为100的合并交易进行处理；如果编号之间并不连续，比如最新处理的合并交易

的编号为99、当前收到的合并交易的编号为101，则区块链节点需要等待并优先处理编号为100的合并交易，然后才能处理编号为101的合并交易。由于每条交易被执行后都可能导致该参与方的状态参数发生变化，而在后交易的执行需要依赖于先前交易执行后的状态参数的取值，因而需要确保各个合并交易被按照对应编号的大小进行依次处理，以使得各个合并交易均能够正确执行。

[0102] 在一实施例中，在事件对应的备选子交易中，包含所述参与方对所述事件的单方触发信息；其中，当所述事件的所有参与方分别向区块链提交的针对所述事件的单方触发信息均通过验证时，所述事件对应的备选子交易在区块链中被触发执行。单方触发信息表明相应的参与方对事件的描述信息予以确认，希望触发事件的执行；而事件的每一参与方都需要分别向区块链提交单方触发信息，使得区块链节点基于所有参与方分别提交的单方触发信息，确定是否应当执行相应的备选子交易所指示的事件。例如，事件的任一参与方生成描述信息并提供至其他参与方后，不仅该任一参与方需要向自身维护的等待队列中添加相应的备选子交易，每一其他参与方在对描述信息予以确认后，也分别向自身维护的等待队列中添加相应的备选子交易；以及，每一参与方分别基于自身维护的等待队列生成集合交易，从而通过将集合交易提交至区块链，使得上述的单方触发信息被提交至区块链，以供区块链节点进行验证。单方触发信息中可以包含描述信息和相应参与方对描述信息生成的签名；签名属于相应参与方提供的确认信息，而如果采用密文数值或承诺数值，确认信息还包含证明信息，这在上文中已经详细描述。通过由各个参与方分别向区块链提交单方触发信息，而非某一参与方提交多方触发信息，不仅可以对处理压力进行分担、防止单个参与方的处理压力过大，还可使各个参与方根据自身的实际情况(如处理压力、优先级管理等)对所参与的各个事件进行选择性地处理甚至批量处理。

[0103] 为了便于理解，下面以跨境汇款场景为例，对本说明书一个或多个实施例的技术方案进行说明。基于本说明书的技术方案，每一机构可以分别对自身所参与的若干汇款交易(相当于上述的备选子交易)合并为一笔区块链交易(相当于上述的集合交易)，并通过向区块链提交该区块链交易，实现对若干汇款交易的批量提交和处理。下面将首先对单笔汇款交易的生成与处理过程进行描述，然后扩展至多笔汇款交易的批量处理。

[0104] 图3是一示例性实施例提供的一种跨境汇款的场景示意图。如图3所示，假定由用户1向用户2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。假定用户1在国家A的机构1处开设有客户资金账户1、用户2在国家B的机构4处开设有客户资金账户2，本说明书可以在机构1与机构4之间无法直接实施跨境汇款的情况下，通过机构2与机构3的协助而在区块链上实现该跨境汇款的操作。

[0105] 机构1、机构2、机构3和机构4分别存在对应的设备1、设备2、设备3和设备4，并通过在设备1～4上运行区块链的客户端程序，使得设备1～4被配置为相应的区块链节点；相应地，机构1～4可以通过设备1～4实现与区块链相关的操作。例如，机构1～4可以分别通过设备1～4向区块链提交相应的区块链交易；再例如，设备1～4分别维护有区块链上的全量交易数据，即区块链账本，使得机构1～4可以分别据此查询和维护各个区块链账户的余额数据，比如机构1对应的区块链账户Y1持有1000港币，机构2对应的区块链账户Y2持有2500港币和4200欧元，机构3对应的区块链账户Y3持有3000欧元和2000美元，机构4对应的区块链

账户Y4持有1500美元等。

[0106] 出于隐私保护等方面的考虑，区块链账户Y1～Y4的余额数据往往并非以明文形式进行维护，而是采用对应的密文数据。以区块链账户Y1为例，在区块链账本中可以被记录为(currency_1,PC(a,r_a),Enc_A(a),Enc_A(r_a))，其中：currency_1表示货币类型为港币，a表示港币数额为1000，r_a为a对应的随机数，PC(a,r_a)是通过Pedersen承诺机制对a和r_a进行计算得到的密文形式的承诺值，Enc_A(a)、Enc_A(r_a)分别为a和r_a的密文取值(比如可以采用机构1的身份公钥进行加密，或者可以采用其他任意形式的加密算法)。区块链账户Y2可以被记录为(currency_1,PC(b1,r_b1),Enc_B(b1),Enc_B(r_b1))、(currency_2,PC(b2,r_b2),Enc_B(b2),Enc_B(r_b2))，其中：b1表示港币数额为2500、r_b1为b1对应的随机数，currency_2表示货币类型为欧元，b2表示欧元数额为4200、r_b2为b2对应的随机数。区块链账户Y3可以被记录为(currency_2,PC(c1,r_c1),Enc_C(c1),Enc_C(r_c1))、(currency_3,PC(c2,r_c2),Enc_C(c2),Enc_C(r_c2))，其中：c1表示港币欧元为3000、r_c1为c1对应的随机数，currency_3表示货币类型为美元，c2表示美元数额为2000、r_c2为c2对应的随机数。区块链账户Y4可以被记录为(currency_3,PC(d,r_d),Enc_D(d),Enc_D(r_d))，其中d表示美元数额为1500、r_d为d对应的随机数。

[0107] 基于图3所示的汇款场景，图4是一示例性实施例的一种跨境汇款过程中的交互示意图。如图4所示，跨境汇款的交互过程可以包括以下步骤：

[0108] 步骤401，设备1起草汇款交易tx_i。

[0109] 在一实施例中，假定用户1希望向用户2汇款500港币，该用户1可以通过在机构1处的客户资金账户1提供该500港币，而用户2可以通过在机构4处的客户资金账户2收取按一定汇率计算后的美元。

[0110] 在一实施例中，机构1可以从用户1对应的客户资金账户1中扣取500港币；以及，机构1需要在自身与机构4之间确定出汇款路由，比如图4中的汇款路由为“机构1→机构2→机构3→机构4”，使得机构1可以向机构2转入500港币、机构2可以向机构3转入56欧元(相当于500港币)、机构3可以向机构4转入64美元(相当于56欧元、500港币)，并最终由机构4向用户2对应的客户资金账户2转入64美元，从而完成汇款操作。其中，机构1从客户资金账户1扣取500港币、机构4向客户资金账户2转入64美元属于链外操作，而机构1～机构4之间则通过区块链实现链上资金转移。

[0111] 在一实施例中，在上述的汇款路由“机构1→机构2→机构3→机构4”中，机构1与机构4之间存在2个中继方为机构3和机构4；而在其他实施例中，中继方的数量可以为1个、3个或3个以上，本说明书并不对此进行限制。

[0112] 针对已经确定的上述汇款路由，以及各个机构之间的汇款金额，设备1起草的汇款交易tx_i可以包括以下汇款交易详情：交易id为tx_i，区块链账户Y1的地址Z1、区块链账户Y2的地址Z2、区块链账户Y3的地址Z3、区块链账户Y4的地址Z4，与交易金额相关的密文信息{(currency_1,PC(t1,r_t1),Enc_B(t1),Enc_B(r_t1),Enc_C(t1),Enc_C(r_t1),Enc_D(t1),Enc_D(r_t1)),(currency_2,PC(t2,r_t2),Enc_B(t2),Enc_B(r_t2),Enc_C(t2),Enc_C(r_t2),Enc_D(t2),Enc_D(r_t2)),(currency_3,PC(t3,r_t3),Enc_B(t3),Enc_B(r_t3),Enc_C(t3),Enc_C(r_t3),Enc_D(t3),Enc_D(r_t3)),rate1,rate2,time,…}，针对交易金额t1、t2、t3的区间证明RP_t1、RP_t2、RP_t3等。

[0113] 其中，地址Z1～Z4用于表明本次汇款事件的参与方，以使得后续从该地址Z1～Z4对应的区块链账户Y1～Y4实施转账汇款。

[0114] 在(currency_1,PC(t1,r_t1),Enc_B(t1),Enc_B(r_t1),Enc_C(t1),Enc_C(r_t1),Enc_D(t1),Enc_D(r_t1))中，t1表示从地址Z1向地址Z2的转账金额(如上述的500港币)，r_t1为该金额t1对应的随机数，PC(t1,r_t1)为基于金额t1和随机数r_t1计算得到的承诺值，Enc_B(t1)表示用机构2的身份公钥对金额t1进行加密后的密文数值、Enc_C(t1)表示用机构3的身份公钥对金额t1进行加密后的密文数值、Enc_D(t1)表示用机构4的身份公钥对金额t1进行加密后的密文数值；类似地，Enc_B(r_t1)、Enc_C(r_t1)、Enc_D(r_t1)分别为通过机构2、机构3、机构4的身份公钥对金额t1进行加密后的密文数值。(currency_2,PC(t2,r_t2),Enc_B(t2),Enc_B(r_t2),Enc_C(t2),Enc_C(r_t2),Enc_D(t2),Enc_D(r_t2))和(currency_3,PC(t3,r_t3),Enc_B(t3),Enc_B(r_t3),Enc_C(t3),Enc_C(r_t3),Enc_D(t3),Enc_D(r_t3))的情况类似，此处不再赘述。rate1、rate2分别为currency_1与currency_2的汇率、currency_2与currency_3的汇率。time为交易时刻。以及，还可能存在一些其他的交易所需数据，这可以参考相关技术中的方案，此处不再一一列举。

[0115] RP_t1、RP_t2、RP_t3分别为对应于交易金额t1、t2、t3的区间证明，以分别用于证明交易金额t1、t2、t3处于正确数值区间，比如$0\leqslant t1<2^{64}$、$0\leqslant t2<2^{64}$、$0\leqslant t3<2^{64}$。其中，设备1可以通过相关技术中的零知识证明技术生成上述的区间证明，本说明书并不对此进行限制。

[0116] 步骤402a～402c，设备1将汇款交易详情分别同步至设备2、设备3和设备4。

[0117] 在一实施例中，设备1可以通过机构1的身份私钥对汇款交易详情进行签名后，通过链外(或称为，链下)通道分别发送至设备2～设备4，以实现数据同步。

[0118] 在一实施例中，设备1～设备4分别运行有区块链的客户端程序，使得设备1～设备4分别被配置为区块链中的区块链节点；或者，设备1～设备4在区块链中分别存在对应的区块链节点，本说明书并不对此进行限制。其中，区块链中的每一区块链节点分别维护有内容统一的区块链账本，区块链账本中记录有全量的区块链数据。因此，设备1可以生成一笔交易，该交易的内容包含上述汇款交易tx_i的汇款交易详情，并将该交易提交至区块链中；相应地，当该交易通过共识后，可以被发送至区块链中的各个区块链节点，以供各个区块链节点更新自身维护的区块链账本。因此，设备1、设备2、设备3和设备4可以分别通过自身对应的区块链节点所维护的区块链账本，获知设备1提交的上述交易，从而获取该交易中包含的上述汇款交易tx_i的汇款交易详情。

[0119] 当然，设备1还可能通过其他方式将汇款交易数据同步至设备2～设备4，本说明书并不对此进行限制。

[0120] 步骤403a，设备1将汇款交易详情对应的汇款交易tx_i添加至自身的本地队列1。

[0121] 在一实施例中，当设备1通过链外通道发送汇款交易详情时，设备1可以直接向本地队列1添加汇款交易tx_i；当然，设备1可以等待设备2～设备4对汇款交易详情确认完毕并返回相应的确认响应后，才向本地队列1添加汇款交易tx_i，以确保设备2～设备4均参与至该汇款交易tx_i。

[0122] 在一实施例中，当设备1通过区块链将汇款交易详情同步至设备2～设备4时，设备1同样会收到区块链上同步的该汇款交易详情，那么设备1既可以对该汇款交易详情进行验

证(验证过程可参考步骤403b),并在通过验证后将汇款交易tx_i添加至本地队列1,也可以在确定该汇款交易详情对应于汇款交易tx_i、该汇款交易tx_i由该设备1自身起草并提交至区块链时,略去对汇款交易详情的验证过程,而直接添加至本地队列1。

[0123] 步骤403b,设备2对收到的汇款交易详情进行验证后,将其添加至自身的本地队列2。

[0124] 在一实施例中,设备2在收到汇款交易详情后,需要实施验证操作,包括:设备2通过自身的身份私钥对汇款交易详情包含的Enc_B(t1)、Enc_B(r_t1)、Enc_B(t2)、Enc_B(r_t2)、Enc_B(t3)、Enc_B(r_t3)进行解密,得到相应的金额t1与随机数r_t1、金额t2与随机数r_t2、金额t3与随机数r_t3,并分别验证PC(t1,r_t1)=r_t1G+t1H、PC(t2,r_t2)=r_t2G+t2H、PC(t3,r_t3)=r_t3G+t3H是否成立(其中,G、H为预设系统参数);设备2验证currency_1与currency_2之间的汇率是否为rate1、currency_2与currency_3之间的汇率是否为rate2;设备2验证区间证明RP_t1、RP_t2、RP_t3是否正确等。在确定汇款交易详情通过验证后,设备2可以向自身维护的本地队列2添加相应的汇款交易tx_i,并且向设备1返回确认响应、以表明接受相应的汇款交易。

[0125] 步骤403c-403d,设备3-4分别对收到的汇款交易详情进行验证后,将其添加至自身的本地队列3-4。

[0126] 在一实施例中,设备3、设备4所实施的操作与设备2相类似,此处不再一一赘述。

[0127] 至此,汇款交易tx_i已经被设备1～设备4分别添加至各自维护的本地队列1～4中。类似地,当设备1～设备4分别参与到其他的汇款交易(并不一定为设备1～设备4同时参与的汇款交易)时,同样可以采用类似于对上述汇款交易tx_i的处理方式,向相应的本地队列中添加汇款交易,以用于下述步骤中的交易聚合与批量处理。

[0128] 步骤404a,设备1根据本地队列1中的汇款交易,聚合生成交易TX_a,并在签名后提交至区块链。

[0129] 如上文所述,与汇款交易tx_i相类似的,机构1还可以参与其他的汇款交易,比如当某一用户需要通过机构1向另一用户进行汇款时,设备1可以通过类似于上述步骤的方式,起草相应的汇款交易、将汇款交易详情发送至其他各个机构进行验证、向本地队列1中添加相应的汇款交易tx_i。同时,机构1还可以作为一些汇款交易的中继方(类似于机构2-3在上述实施例中的角色)或收款方(类似于机构4在上述实施例中的角色),使得该机构1可以通过设备1接收这些汇款交易的汇款方(类似于机构1在上述实施例中的角色)发送的汇款交易详情,并在验证通过后向本地队列1中添加相应的汇款交易。

[0130] 因此,设备1维护的本地队列1中包含机构1所参与的诸多汇款交易。而设备1可以按照预定义的交易选择规则,每次从本地队列1中选取一个或多个汇款交易,并对被选取的汇款交易进行聚合,生成一笔区块链交易。

[0131] 例如,图5是一示例性实施例提供的一种区块链交易的内容示意图。如图5所示,假定设备1选取6个汇款交易并聚合为一笔区块链交易,比如汇款交易tx_i-3、tx_i-2、tx_i-1、tx_i、tx_i+1、tx_i+2被聚合为区块链交易TX_a,该设备1需要为各个汇款交易生成相应的证明信息。

[0132] 首先,对于区块链交易TX_a中的每一汇款交易,该区块链交易TX_a中需要包含针对每一汇款交易的交易额的证明信息,比如汇款交易tx_i-3对应的证明信息为RP_i-3、汇

款交易tx_i-2对应的证明信息为RP_i-2、汇款交易tx_i-1对应的证明信息为RP_i-1、汇款交易tx_i对应的证明信息为RP_i、汇款交易tx_i+1对应的证明信息为RP_i+1、汇款交易tx_i+2对应的证明信息为RP_i+2。

[0133] 以汇款交易tx_i对应的证明信息RP_i为例，相当于上文所述的区间证明RP_t1、RP_t2、RP_t3，分别用于证明汇款交易tx_i的交易额t1、t2、t3处于正确数值区间。类似地，对于其他非设备1所起草的汇款交易而言，可以由汇款交易的起草方生成对交易额的证明信息、无需设备1生成；当然，即便并非设备1所起草的汇款交易，仍然可由该设备1为相应的交易额生成证明信息，本说明书并不对此进行限制。

[0134] 然后，对于机构1作为汇款方或中继方的汇款交易，即导致机构1的区块链账户Y1的余额减少的汇款交易，设备1还需要生成区块链账户Y1的余额充足、不小于交易额的证明信息。此时，设备1需要从上述的6个汇款交易中，挑选出所有会导致区块链账户Y1的余额减少的汇款交易，并使得挑选出的这些汇款交易在区块链交易TX_a中相邻排列；例如，当汇款交易tx_i-3、tx_i-2和tx_i-1会导致区块链账户Y1的余额增加，而汇款交易tx_i、tx_i+1、tx_i+2会导致区块链账户Y1的余额减少时，设备1可以将汇款交易tx_i-3、tx_i-2和tx_i-1相邻排列，并针对这3个汇款交易生成统一证明信息RP_(i～i+2)，以证明区块链账户Y1的余额(指经过汇款交易tx_i、tx_i+1、tx_i+2带来的取值变化后的余额)足以完成汇款交易tx_i、tx_i+1和tx_i+2，而无需为汇款交易tx_i、tx_i+1和tx_i+2分别生成单独的区间证明。

[0135] 在一实施例中，考虑到设备1提交的汇款交易并不一定全部顺利执行，而在先提交的汇款交易可能影响区块链账户Y1的余额，从而影响在后的汇款交易，因此，在生成统一证明信息RP_(i～i+2)时，应当考虑在先提交的区块链交易的影响。例如，当机构1在该区块链交易中包含的若干汇款交易中作为汇款方或中继方时，机构1会将自身对应的区块链账户Y1的账户余额减去对应的转账金额(汇款方仅转出资金；中继方既可接收转入资金又需要转出资金，这里是针对转出资金的操作而描述)，并基于更新后的汇款金额继续参与后续的汇款交易。当该区块链交易被提交至区块链后，如果机构1作为汇款方或中继方的某一汇款交易成功执行，机构1无需调整区块链账户Y1；如果机构1作为汇款方或中继方的某一汇款交易未成功执行，机构1需要对区块链账户Y1的账户余额进行回滚调节。而当上述的区块链交易中包含机构1作为收款方或中继方(收款方仅转入资金；中继方既可接收转入资金又需要转出资金，这里是针对转入资金的操作而描述)的汇款交易时，如果该汇款交易成功执行，机构1需要向区块链账户Y1中增加相应资金、实现收款，如果汇款交易未成功执行，机构1无需调整区块链账户Y1。相应地，区块链节点在收到并处理设备1提交的区块链交易时，可以针对区块链交易所包含的汇款交易是否能够成功执行，对各个汇款交易进行状态标记，比如交易为成功状态、失败状态、超时状态等。

[0136] 因此，设备1在聚合生成区块链交易TX_a时，并不直接通过区块链账户Y1的余额取值生成统一证明信息RP_(i～i+2)，而是需要先确定出设备1先前提交的区块链交易中可能造成金额变化的汇款交易，包括：机构1作为中继方或收款方的汇款交易被标记为成功状态时产生的金额增加(收款)、机构1作为汇款方或中继方的汇款交易被标记为失败状态或超时状态时产生的金额增加(对已扣除的转账金额进行回滚)等。以及，设备1进一步根据区块链账户Y1的余额取值(已扣除先前提交的汇款交易的转账金额、尚未收款)与上述可能造成

金额变化的汇款交易实际产生的金额变化值，对区块链账户Y1的余额取值进行更新，然后根据更新后的余额取值生成统一证明信息RP_(i～i+2)。

[0137] 此外，设备1在生成各个区块链交易时，还按照区块链交易的生成顺序，为每一区块链交易添加相应的顺序编号seq。比如当设备1分别生成了区块链交易TX_1、TX_2和TX_3时，区块链交易TX_1的seq取值为99、区块链交易TX_2的seq取值为100、区块链交易TX_3的seq取值为101，表明区块链交易TX_1早于区块链交易TX_2生成、区块链交易TX_2早于区块链交易TX_3生成。相应的，区块链节点在收到设备1提交的各个区块链交易后，会按照seq取值从小到大的顺序依次对各个区块链交易进行处理，比如先处理区块链交易TX_1、再处理区块链交易TX_2、然后处理区块链交易TX_3。

[0138] 步骤404b-d，设备2～4根据本地队列2～4中的汇款交易，分别聚合生成交易TX_b、TX_c、TX_d，并在签名后分别提交至区块链。

[0139] 在一实施例中，与设备1相类似的，设备2可以从本地队列2中选取一个或多个汇款交易，以聚合生成相应的区块链交易。假定设备2在某一次选取的汇款交易中包含上述的汇款交易tx_i，并据此生成了相应的区块链交易TX_b；其中，导致机构2的区块链账户Y2的余额减少的汇款交易在TX_b中相邻排列，以生成相应的统一证明信息。

[0140] 在一实施例中，与设备1相类似的，设备3可以从本地队列3中选取一个或多个汇款交易，以聚合生成相应的区块链交易。假定设备3在某一次选取的汇款交易中包含上述的汇款交易tx_i，并据此生成了相应的区块链交易TX_c；其中，导致机构3的区块链账户Y3的余额减少的汇款交易在TX_c中相邻排列，以生成相应的统一证明信息。

[0141] 在一实施例中，与设备1相类似的，设备4可以从本地队列4中选取一个或多个汇款交易，以聚合生成相应的区块链交易。假定设备4在某一次选取的汇款交易中包含上述的汇款交易tx_i，并据此生成了相应的区块链交易TX_d；其中，导致机构4的区块链账户Y4的余额减少的汇款交易在TX_d中相邻排列，以生成相应的统一证明信息。

[0142] 需要指出的是：设备1～设备4可以根据实际情况选择生成相应的区块链交易，而并不一定立即对汇款交易tx_i进行处理；换言之，设备1～设备4实际上是异步地向区块链提交汇款交易tx_i(被包含于相应的区块链交易中)，使得该汇款交易tx_i的执行被分配至由设备1～设备4分别进行触发，促使设备1～设备4在参与大量汇款交易的情况下，可以对所参与的汇款交易进行批量生成区块链交易，从而减少区块链交易的生成和提交数量，有助于降低处理负担、提升处理效率。

[0143] 步骤405，区块链节点对收到的区块链交易进行处理，以验证区块链交易中包含的各笔汇款交易。

[0144] 步骤406，标记汇款交易tx_i。

[0145] 在一实施例中，由于每一机构会不断向区块链提交区块链交易，而在先提交的区块链交易所包含的汇款交易，会影响在后提交的区块链交易所包含的汇款交易，因而区块链节点在接收每一机构提交的区块链交易后，需要读取所接收到的区块链交易中包含的顺序编号seq，并按照顺序编号seq的大小，依次处理来自相应机构的区块链交易。例如，当区块链节点接收到设备1提交的区块链交易TX_a时，读取其中包含的顺序编号seq为100；而如果区块链节点已处理的最近一笔区块链交易的顺序编号seq为98，那么区块链节点需要等待设备1提交的顺序编号seq为99的区块链交易，并在该顺序编号为99的区块链交易被处理

后，才对上述顺序编号为100的区块链交易进行处理。

[0146] 在一实施例中，区块链节点在收到设备1～4分别提交的区块链交易后，可以分别提取每一区块链交易中包含的汇款交易并实施验证。以设备1提交的区块链交易TX_a为例，区块链节点可以分别验证如图5所示的证明信息RP_i-3、RP_i-2、RP_i-1、RP_i、RP_i+1、RP_i+2，以分别确定各个汇款交易的汇款额是否处于正确数值区间；以及，区块链节点通过验证统一证明信息RP_(i～i+2)，以确定区块链账户Y1的账户余额是否足额，以确定是否能够顺利执行区块链交易TX_a中的各个汇款交易。当然，区块链节点还可能实施其他的验证操作，可以参考相关技术中对于汇款交易的验证过程，比如验证汇出额与汇入额是否一致、与业务数额是否一致等，此处不再一一赘述，且本说明书并不对此进行限制。

[0147] 在一实施例中，如果汇款交易的执行由汇款方、中继方、收款方等参与方同时参与触发，因而区块链节点还需要验证汇款交易的各个参与方是否都实施了触发(即提交了包含该汇款交易的区块链交易)。例如，图6是一示例性实施例提供的一种统计触发情况的示意图。如图6所示，基于区块链的原生功能或智能合约所提供的扩展功能，区块链节点可以分别记录机构1～机构4所提交的区块链交易，比如机构1提交的区块链交易TX_a、TX_*，机构2提交的区块链交易TX_*、TX_b、TX_#，机构3提交的区块链交易TX_*、TX_c，机构4提交的区块链交易TX_d等；以及，区块链节点可以提取出各个区块链交易中包含的汇款交易，并分别针对各个汇款交易的参与方(汇款交易详情中包含汇款方、中继方、收款方的信息)进行统计：当收到相应参与方提交的区块链交易中包含该汇款交易，且该汇款交易通过了上述验证时，可以将该参与方标记为“OK”。

[0148] 比如，由于设备1提交的区块链交易TX_a中包含汇款交易tx_i，如果区块链交易TX_a中对应于汇款交易tx_i的内容通过验证，那么区块链节点可以标记为如图6所示的“Y1:OK”；类似地，如果区块链节点还分别针对机构2～机构4标记为“Y2:OK”、“Y3:OK”、“Y4:OK”等，那么区块链节点可以确定该汇款交易tx_i已经得到所有参与方的确认，可以将该汇款交易tx_i标记为成功状态。

[0149] 再比如，由于仅设备1、设备2和设备3提交的区块链交易中包含汇款交易tx_*的相关信息，因而即便这些信息都已经通过单独验证，区块链节点仍然仅能够为该汇款交易tx_*添加标记“Y1:OK”、“Y2:OK”、“Y3:OK”，而需要继续等待设备4提交的区块链交易。

[0150] 又比如，由于仅设备2提交的区块链交易中包含汇款交易tx_#的相关信息，因而即便相关信息已经通过单独验证，区块链节点仍然仅能够为该汇款交易tx_#添加标记“Y2:OK”，而需要继续等待设备1、设备3和设备4提交的区块链交易。

[0151] 仍以汇款交易tx_i为例，如果机构1～机构4中的任一参与方未能够在交易时刻到达之前提交包含该汇款交易tx_i的区块链交易，那么区块链节点会将该汇款交易tx_i标记为超时状态，使其无法被成功执行。如果机构1～机构4中的任一参与方虽然提及了包含该汇款交易tx_i的区块链交易，但由于金额累加详情出错或区间证明出错等原因而未通过单独验证，那么区块链节点会将该汇款交易tx_i标记为失败状态，使其无法被成功执行。

[0152] 当汇款交易tx_i或其他汇款交易被区块链节点添加了成功状态、失败状态或超时状态等标记时，机构1～机构4在后续生成区块链交易时，可以参考这些状态生成相应的金额累加详情、生成余额充足的区间证明等，这与上文中在步骤404a～404d中描述的过程相类似，此处不再赘述。

[0153] 在确认汇款交易tx_i被成功执行后，机构1在链外收取用户1的500港币、向机构2转出500港币，机构2收取机构1转入的500港币、向机构3转出56欧元，机构3收取机构2转入的56欧元、向机构4转出64美元，机构4收取机构3转入的64美元、在链外向用户1转入64美元，相当于机构1～4收支平衡、由用户1向用户2完成了500港币的汇款操作。

[0154] 而表现在区块链账本上的数据变化为：机构1对应的区块链账户Y1更新为(currency_1,PC(a-t1,r_a-r_t1),Enc_A(a-t1),Enc_A(r_a-r_t1))、减少了500港币；机构2对应的区块链账户Y2更新为：(currency_1,PC(b1+t1,r_b1+r_t1),Enc_B(b1+t1),Enc_B(r_b1+r_t1))、(currency_2,PC(b2-t2,r_b2-r_t2),Enc_B(b2-t2),Enc_B(r_b2-r_t2))，增加了500港币、减少了56欧元；机构3对应的区块链账户Y3更新为：(currency_2,PC(c1+t2,r_c1+r_t2),Enc_C(c1+t2),Enc_C(r_c1+r_t2))、(currency_3,PC(c2-t3,r_c2-r_t3),Enc_C(c2-t3),Enc_C(r_c2-r_t3))，增加了56欧元、减少了64美元；机构4对应的区块链账户Y4更新为：(currency_3,PC(d+t3,r_d+r_t3),Enc_D(d+t3),Enc_D(r_d+r_t3))、增加了64美元。

[0155] 需要指出的是：设备1～设备4所提交的区块链交易中，并不一定每条汇款交易都由所有参与方共同实施触发操作；譬如，至少一条汇款交易可以采用相关技术中的技术方案，即由某一参与方收集所有参与方对汇款交易的交易详情信息的确认信息、生成交易所需的区间证明等(即生成上述实施例中所述的多方触发信息)，并仅由该某一参与方提交包含该汇款交易的区块链交易。

[0156] 图7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7，在硬件层面，该设备包括处理器702、内部总线704、网络接口706、内存708以及非易失性存储器710，当然还可能包括其他业务所需要的硬件。处理器702从非易失性存储器710中读取对应的计算机程序到内存708中然后运行，在逻辑层面上形成基于区块链的事件处理终端交互装置。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。

[0157] 请参考图8，在软件实施方式中，该基于区块链的事件处理装置应用于参与方，可以包括：

[0158] 第一生成单元801，根据所述参与方所参与的事件，生成对应的备选子交易，以使得若干备选子交易被聚合为集合交易；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值；

[0159] 第二生成单元802，针对所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，生成统一证明信息，以证明所述状态参数在经过所述多个备选子交易后的取值处于正确取值区间；

[0160] 提交单元803，将所述集合交易提交至区块链，以使所述集合交易中包含的备选子交易被依次处理。

[0161] 可选的，还包括：

[0162] 识别单元804，当若干备选子交易被选取以用于聚合为所述集合交易时，识别每一

被选取的备选子交易对应的事件对所述状态参数的取值的调整方式；

[0163] 排列单元805，当至少两个备选子交易对应的事件均用于减小所述状态参数的取值时，将所述至少两个备选子交易相邻地排列于所述集合交易中。

[0164] 可选的，所述集合交易中包含分别对应于每一备选子交易的变化前状态值、变化后状态值，以配合于每一备选子交易中设定的状态变化量，使得每一备选子交易被处理后，所述参与方的状态参数由所述变化前状态值经由所述状态变化量而变化至所述变化后状态值；其中，所述变化前状态值和所述变化后状态值分别为基于所述同态加密算法计算得到的密文数值或基于所述同态承诺算法计算得到的承诺数值。

[0165] 可选的，还包括：

[0166] 第三生成单元806，分别为所述集合交易中的每一备选子交易生成相应的独立证明信息，所述独立证明信息用于证明相应的备选子交易中设定的状态变化量处于所述正确数值区间。

[0167] 可选的，在所述事件对应的备选子交易中，包含所述参与方对所述事件的单方触发信息；其中，当所述事件的所有参与方分别向区块链提交的针对所述事件的单方触发信息均通过验证时，所述事件对应的备选子交易在区块链中被触发执行。

[0168] 可选的，还包括：

[0169] 添加单元807，按照生成顺序为各个集合交易添加相应的编号，以使各个集合交易在区块链中被按照对应的编号大小进行依次处理。

[0170] 图9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9，在硬件层面，该设备包括处理器902、内部总线904、网络接口906、内存908以及非易失性存储器910，当然还可能包括其他业务所需要的硬件。处理器902从非易失性存储器910中读取对应的计算机程序到内存908中然后运行，在逻辑层面上形成基于区块链的事件处理终端交互装置。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。

[0171] 请参考图10，在软件实施方式中，该基于区块链的事件处理装置应用于区块链节点，可以包括：

[0172] 接收单元1001，接收参与方提交至区块链的集合交易，所述集合交易中包含若干备选子交易，所述备选子交易对应于所述参与方所参与的事件；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值；

[0173] 第一获取单元1002，获取所述集合交易中的统一证明信息，所述统一证明信息对应于所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，以验证所述状态参数在经过所述多个备选子交易后的取值是否处于正确取值区间；

[0174] 确定单元1003，根据验证结果确定对所述多个备选子交易的处理方式。

[0175] 可选的，

[0176] 还包括：第二获取单元1004，获取所述集合交易中对应于每一备选子交易的独立证明信息，以验证相应的备选子交易中设定的状态变化量是否处于所述正确数值区间；

[0177] 所述确定单元1003具体用于：当所述验证结果为通过验证，且所述多个备选子交易中的任一备选子交易对应的独立证明信息通过验证时，触发执行所述任一备选子交易。

[0178] 可选的，还包括：

[0179] 第三获取单元1005，当所述集合交易中的任一备选子交易对应的事件用于增大所述状态参数的取值时，获取所述集合交易中对应于所述任一备选子交易的独立证明信息；

[0180] 第一触发单元1006，当对应于所述任一备选子交易的独立证明信息通过验证时，触发执行所述任一备选子交易。

[0181] 可选的，在所述事件对应的备选子交易中，包含所述参与方对所述事件的单方触发信息；所述装置还包括：

[0182] 第二触发单元1007，当所述事件的所有参与方分别向区块链提交的针对所述事件的单方触发信息均通过验证时，触发执行所述事件对应的备选子交易。

[0183] 可选的，还包括：

[0184] 识别单元1008，识别所述集合交易对应的编号，所述编号被按照各个集合交易的生成顺序而添加，以按照对应的编号大小对所述参与方提交的各个集合交易进行依次处理。

[0185] 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。

[0186] 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。

[0187] 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。

[0188] 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。

[0189] 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。

[0190] 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。

[0191] 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。

[0192] 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”。

[0193] 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。

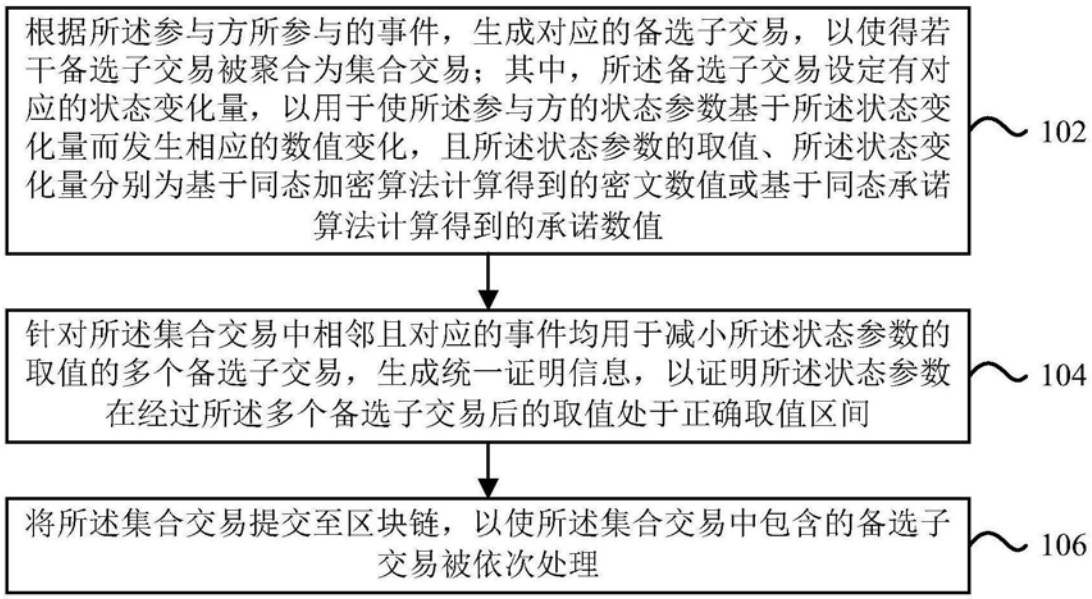

根据所述参与方所参与的事件，生成对应的备选子交易，以使得若干备选子交易被聚合为集合交易；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值
102
针对所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，生成统一证明信息，以证明所述状态参数在经过所述多个备选子交易后的取值处于正确取值区间
104
将所述集合交易提交至区块链，以使所述集合交易中包含的备选子交易被依次处理
106

图1

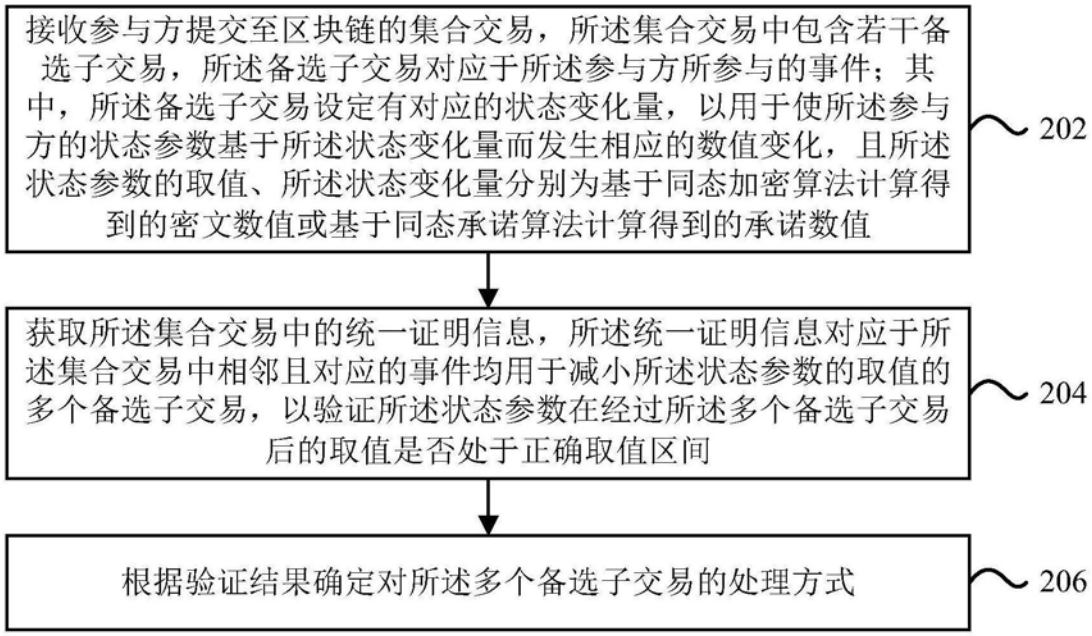

接收参与方提交至区块链的集合交易，所述集合交易中包含若干备选子交易，所述备选子交易对应于所述参与方所参与的事件；其中，所述备选子交易设定有对应的状态变化量，以用于使所述参与方的状态参数基于所述状态变化量而发生相应的数值变化，且所述状态参数的取值、所述状态变化量分别为基于同态加密算法计算得到的密文数值或基于同态承诺算法计算得到的承诺数值
202
获取所述集合交易中的统一证明信息，所述统一证明信息对应于所述集合交易中相邻且对应的事件均用于减小所述状态参数的取值的多个备选子交易，以验证所述状态参数在经过所述多个备选子交易后的取值是否处于正确取值区间
204
根据验证结果确定对所述多个备选子交易的处理方式
206

图2

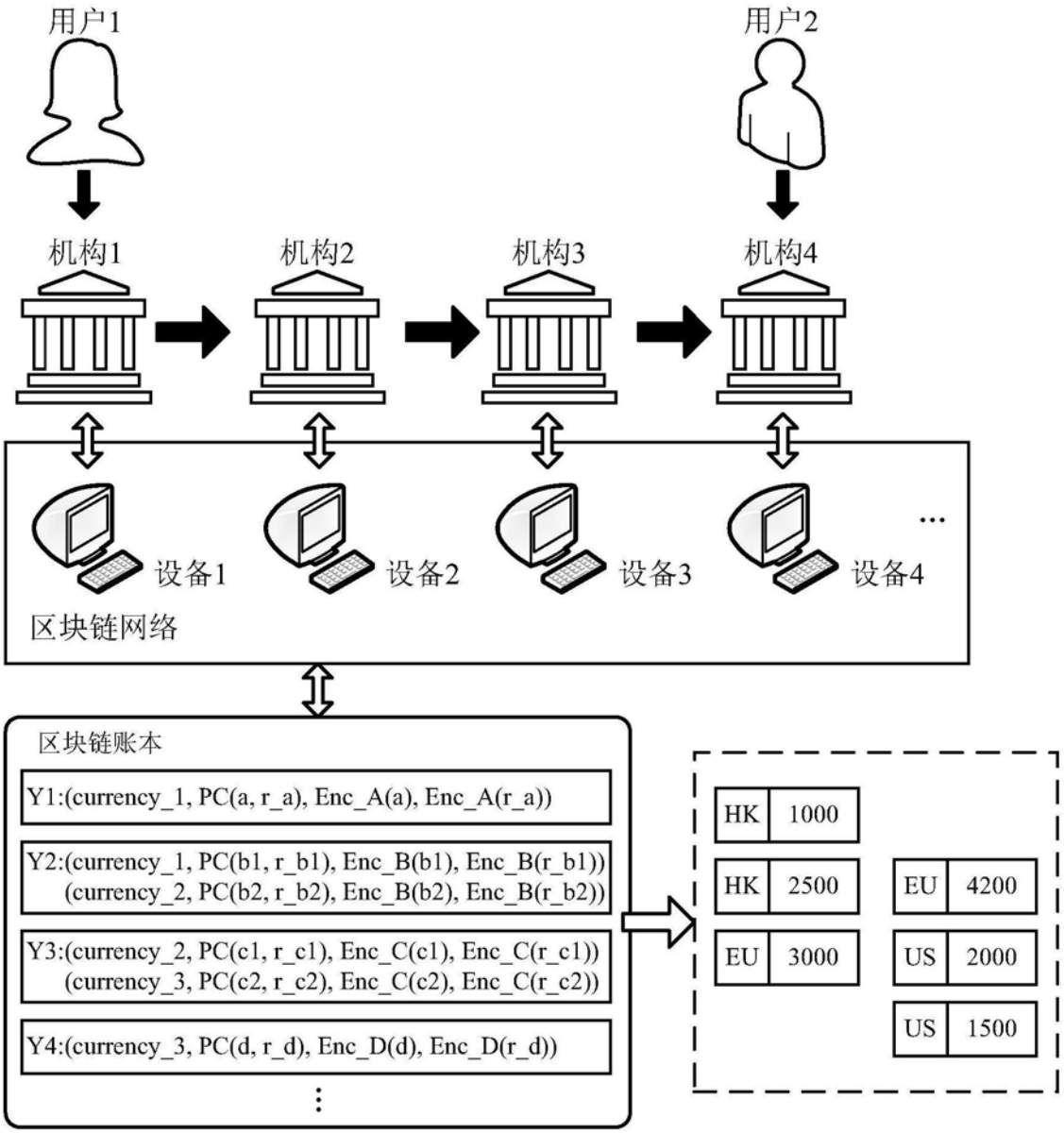

用户1
用户2
机构1
机构2
机构3
机构4
设备1
设备2
设备3
设备4
...
区块链网络
区块链账本
Y1:(currency_1, PC(a, r_a), Enc_A(a), Enc_A(r_a))
Y2:(currency_1, PC(b1, r_b1), Enc_B(b1), Enc_B(r_b1))
(currency_2, PC(b2, r_b2), Enc_B(b2), Enc_B(r_b2))
Y3:(currency_2, PC(c1, r_c1), Enc_C(c1), Enc_C(r_c1))
(currency_3, PC(c2, r_c2), Enc_C(c2), Enc_C(r_c2))
Y4:(currency_3, PC(d, r_d), Enc_D(d), Enc_D(r_d))
HK 1000
HK 2500
EU 3000
EU 4200
US 2000
US 1500

图3

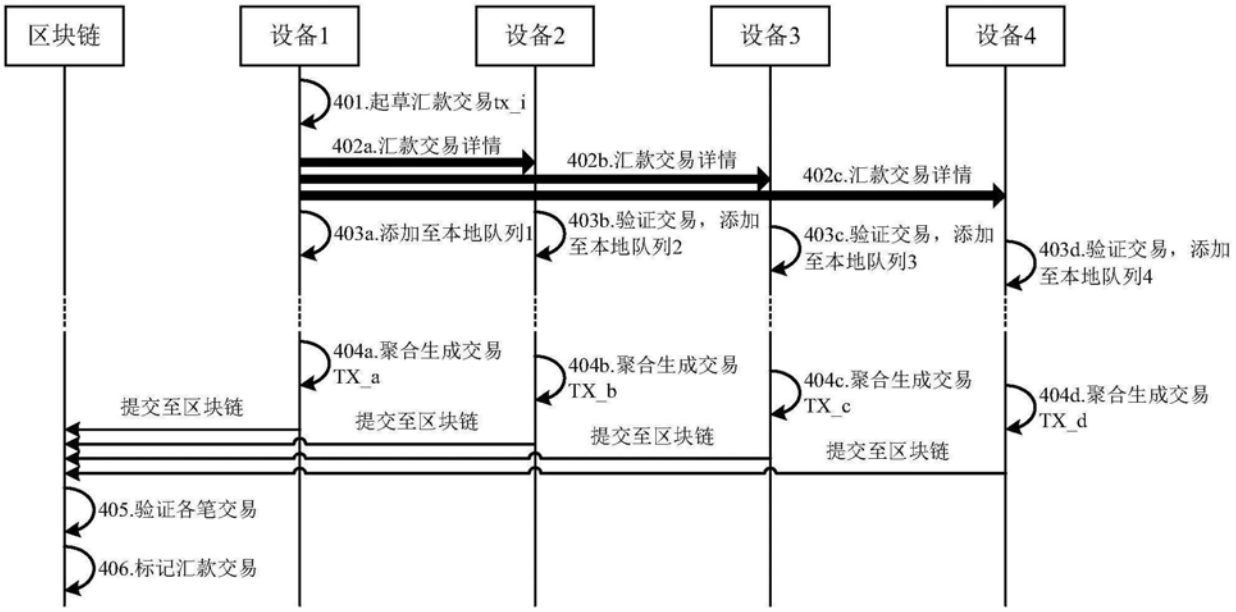

区块链
设备1
设备2
设备3
设备4
401.起草汇款交易tx_i
402a.汇款交易详情
402b.汇款交易详情
402c.汇款交易详情
403a.添加至本地队列1
403b.验证交易，添加至本地队列2
403c.验证交易，添加至本地队列3
403d.验证交易，添加至本地队列4
404a.聚合生成交易TX_a
404b.聚合生成交易TX_b
404c.聚合生成交易TX_c
404d.聚合生成交易TX_d
提交至区块链
提交至区块链
提交至区块链
提交至区块链
405.验证各笔交易
406.标记汇款交易

图4

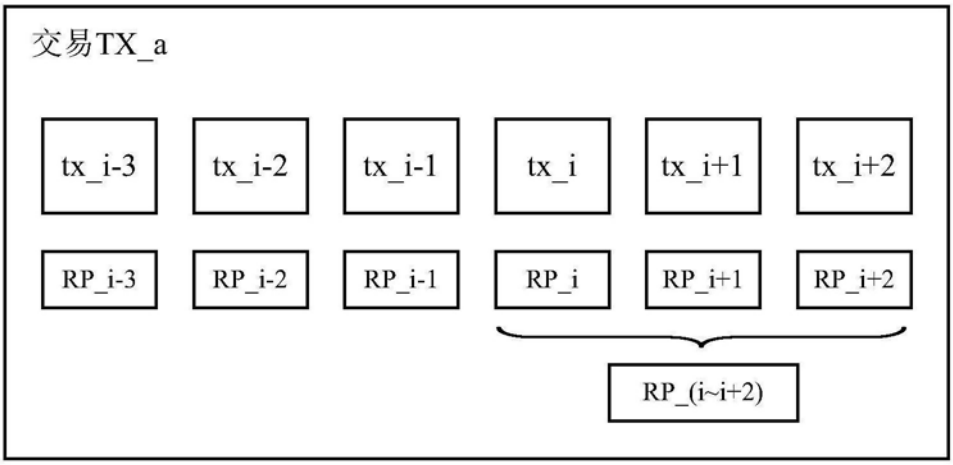

交易TX_a
tx_i-3
tx_i-2
tx_i-1
tx_i
tx_i+1
tx_i+2
RP_i-3
RP_i-2
RP_i-1
RP_i
RP_i+1
RP_i+2
RP_(i~i+2)

图5

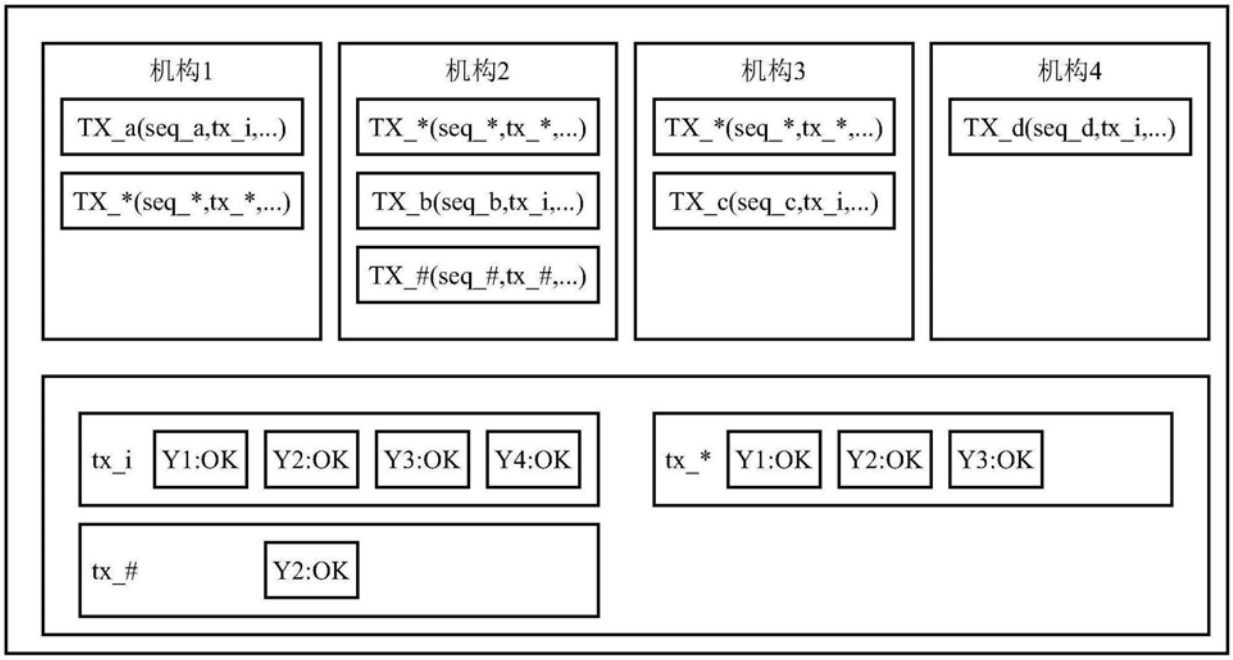

机构1
TX_a(seq_a,tx_i,...)
TX_*(seq_*,tx_*,...)
机构2
TX_*(seq_*,tx_*,...)
TX_b(seq_b,tx_i,...)
TX_#(seq_#,tx_#,...)
机构3
TX_*(seq_*,tx_*,...)
TX_c(seq_c,tx_i,...)
机构4
TX_d(seq_d,tx_i,...)
tx_i
Y1:OK
Y2:OK
Y3:OK
Y4:OK
tx_*
Y1:OK
Y2:OK
Y3:OK
tx_#
Y2:OK

图6

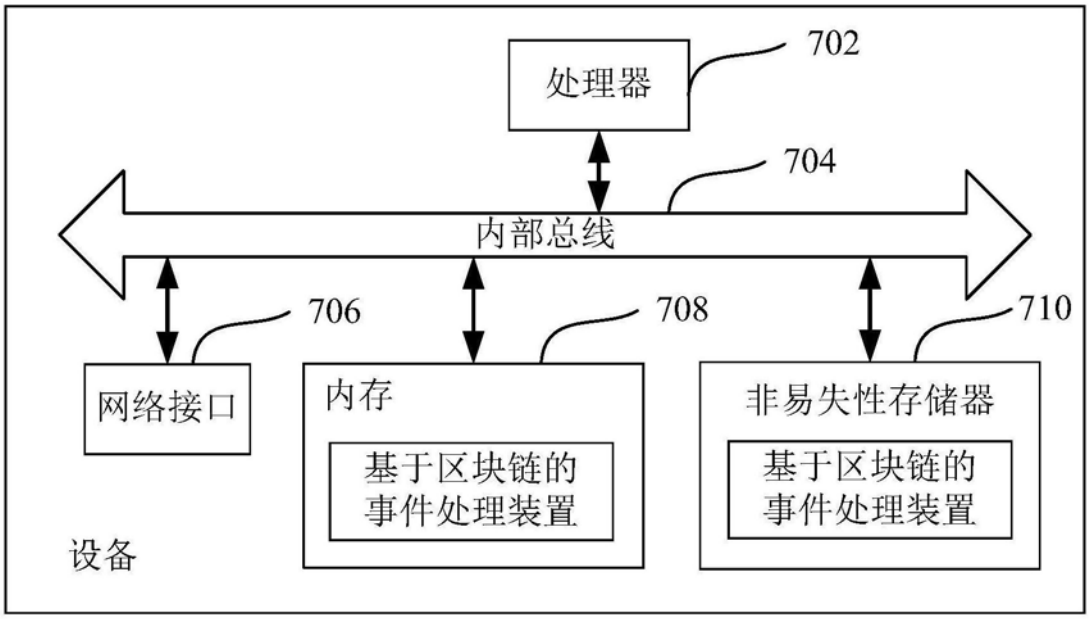

处理器
702
704
内部总线
706
708
710
网络接口
内存
基于区块链的
事件处理装置
非易失性存储器
基于区块链的
事件处理装置
设备

图7

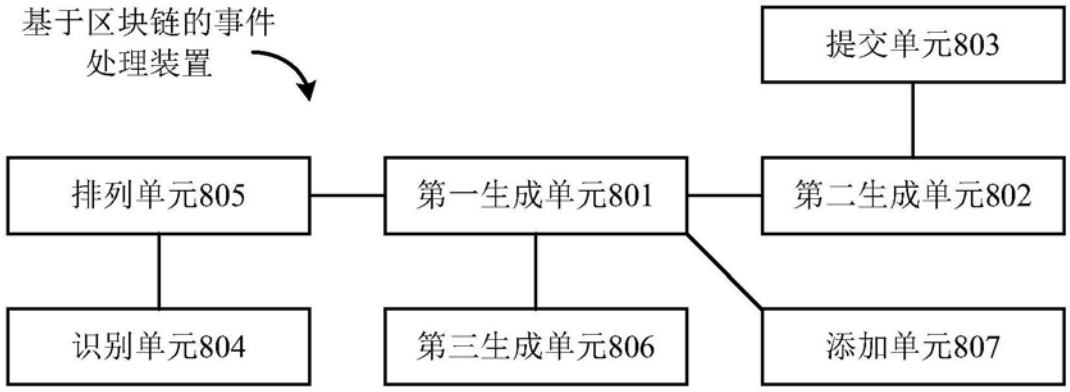

基于区块链的事件处理装置
提交单元803
排列单元805
第一生成单元801
第二生成单元802
识别单元804
第三生成单元806
添加单元807

图8

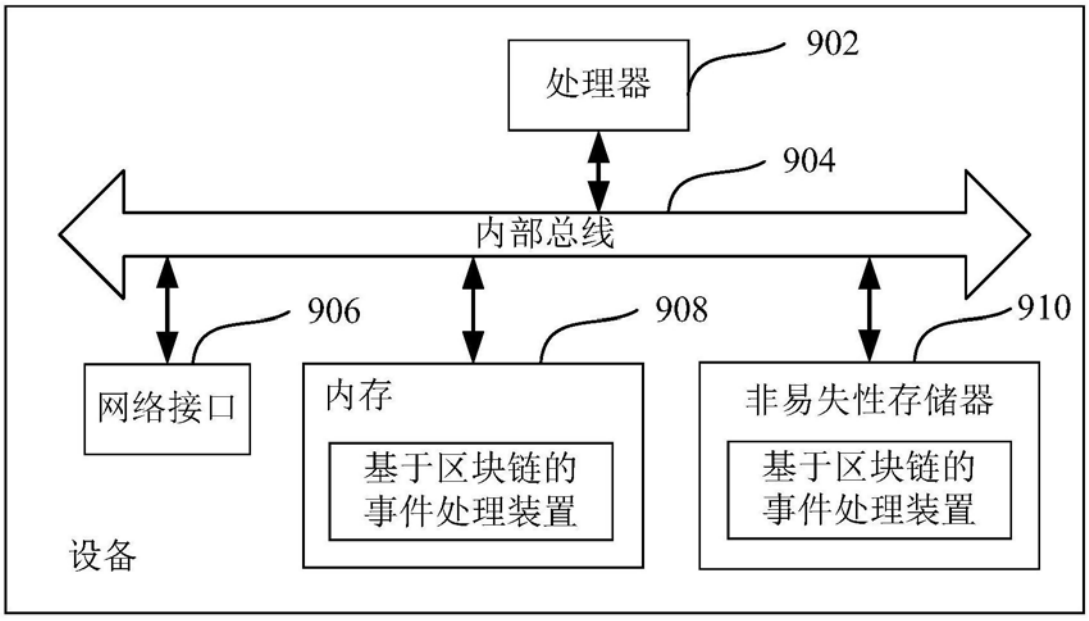

处理器
902
904
内部总线
906
908
910
网络接口
内存
基于区块链的事件处理装置
非易失性存储器
基于区块链的事件处理装置
设备

图9

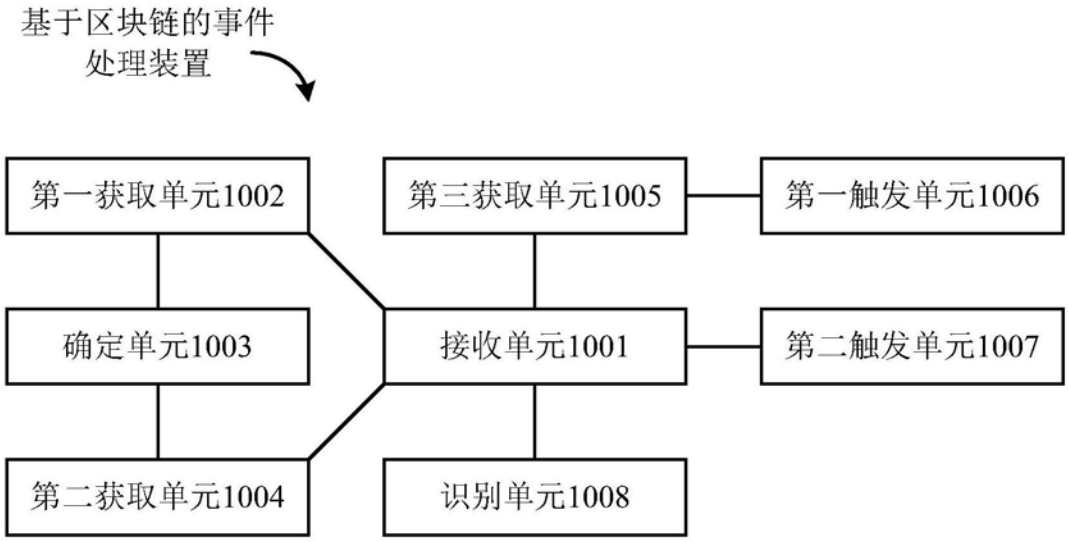

基于区块链的事件处理装置
第一获取单元1002
第三获取单元1005
第一触发单元1006
确定单元1003
接收单元1001
第二触发单元1007
第二获取单元1004
识别单元1008

图10