

基于以太坊的区块链系统和交易数据处理方法

本申请要求于 2017 年 10 月 26 日提交中国专利局、申请号为 2017110170233、发明名称为“基于以太坊的区块链系统和交易数据处理方法”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本申请涉及网络通信技术领域，特别是涉及一种基于以太坊的区块链系统和交易数据处理方法。

10 背景技术

联盟链通常是由一些商业联盟出于共同的利益采用以太坊技术搭建的区块链。联盟链不对外公开，只由商业联盟的各个成员进行管理。但是商业联盟的成员之间并没有完全相互信任，每一个联盟成员都需要去对区块链中其他成员进行监督，以维持联盟链准确运行。在一个新生成的区块被写入联盟链之前，需要联盟链中的各个节点达成一致意见，即达成共识。因此，联盟链的共识机制显得尤为重要。

利用联盟链进行交易时，在传统的方式中通常采用 PBFT (Practical Byzantine Fault Tolerance, 实用拜占庭容错算法) 机制使得各个节点进行共识。在 PBFT 机制中，节点不需要进行挖矿，虽然避免了通过算力竞争达到共识所需的大量运算，但是 PBFT 共识机制的网络资源消耗较高，网络开销较大。因此，如何在通过联盟链进行交易时有效减少网络资源消耗成为目前需要解决的一个技术问题。

发明内容

根据本申请公开的各种实施例，提供一种基于以太坊的区块链系统和交易数据处理方法。

一种基于以太坊的区块链系统，包括主节点和多个备份节点，其中：

所述主节点，用于接收客户终端发送的交易请求，根据所述交易请求调用联盟链中部署的智能合约进行交易处理，得到交易数据；利用交易数据生成区块，将所述区块向多个备份节点进行广播；所述区块具有对应的区块信息；

所述备份节点，用于接收所述区块，对所述区块的交易数据进行验证；

所述主节点还用于利用完整的区块信息生成第一阶段证书，将所述第一阶段证书发送至多个备份节点；所述备份节点还用于根据所述第一阶段证书中的区块哈希值分别生成第二阶段证书和第三阶段证书，分别利用所述第二阶段证书和第三阶段证书对所述区块进行协商，得到协商结果；

当所述区块验证通过且所述协商结果为协商成功时，所述主节点和多个备份节点分别将所述区块分别添加至本地联盟链的副本中。

一种基于以太坊区块链的交易数据处理方法，包括：

主节点接收客户终端发送的交易请求，根据所述交易请求调用本地联盟链副本中部署的智能合约进行交易处理，得到交易数据；

所述主节点利用交易数据生成区块，对所述区块的交易数据进行验证；所述区块具有对应的区块信息；

所述主节点利用完整的区块信息生成第一阶段证书，将所述第一阶段证书发送至多个备份节点，以使得所述备份节点根据所述第一阶段证书中的区块哈希值分别生成第二阶段证书和第三阶段证书，接收所述备份节点分别利用所述第二阶段证书和第三阶段证书对所述区块进行协商所得到的协商结果；及

当所述区块验证通过且所述协商结果为协商成功时，所述主节点将所述区块添加至本地联盟链的副本中。

一种基于以太坊区块链的交易数据处理方法，包括：

备份节点接收主节点广播的区块，所述区块是所述主节点在接收到客户终端发送的交易请求时调用联盟链中部署的智能合约进行交易得到交易数

据，并利用所述交易数据生成的；所述区块具有对应的区块信息；

所述备份节点接收所述区块，对所述区块的交易数据进行验证；所述备份节点接收所述主节点利用完整的区块信息生成的第一阶段证书，根据所述第一阶段证书中的区块哈希值分别生成第二阶段证书和第三阶段证书，分别
5 利用所述第二阶段证书和第三阶段证书对所述区块进行协商，得到协商结果；
及

当所述区块验证通过且所述协商结果为协商成功时，所述备份节点将所述区块添加至本地联盟链的副本中。

一种计算机设备，包括存储器和一个或多个处理器，所述存储器中储存
10 有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述一个或多个处理器执行上述任一项方法的步骤。计算机可读指令计算机可读指令

一个或多个存储有计算机可读指令的计算机可读非易失性存储介质，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行上述
15 任一项方法的步骤。计算机可读指令计算机可读指令

本申请的一个或多个实施例的细节在下面的附图和描述中提出。本申请的其它特征、目的和优点将从说明书、附图以及权利要求书变得明显。

附图说明

20 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为一个实施例中基于以太坊的区块链系统的应用场景图；

25 图 2 为一个实施例中基于以太坊的区块链系统的框图；

图 3 为一个实施例中区块协商过程的示意图；

图 4 为一个实施例中基于以太坊的区块链方法的流程图；

图 5 为另一个实施例中基于以太坊的区块链方法的流程图；

图 6 为一个实施例中计算机设备的框图。

具体实施方式

5 为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

本申请提供的基于以太坊的区块链系统，可以应用于如图 1 所示的应用环境中。客户终端 102 通过网络与区块链系统中的第一终端 104 进行通信连接。区块链系统中还包括多个第二终端 106，其中第一终端 104 与多个第二终端 106 两两之间建立通信连接。第一终端 104 可以称为区块链系统中的主节点，第二终端 106 可以称为区块链系统中的备份节点。第一终端 104 和多个第二终端 106 中分别在本地存储了联盟链的副本。也就是联盟链的多个节点之间去中心化，对联盟链进行分布式存储。

15 客户终端 102 向第一终端 104 发送交易请求，第一终端 104 根据交易请求调用联盟链中部署的智能合约进行交易处理，得到交易数据。第一终端 104 利用交易数据生成区块。区块被写入联盟链之前，需要在区块链系统中达成共识，对区块达成共识需要对区块进行验证和协商。第一终端 104 将区块向多个第二终端 106 进行广播。第二终端 106 接收区块，对区块的交易数据进行验证。对区块协商可以包括三个阶段，第一终端 104 利用完整的区块信息生成第一阶段协商所需的第一阶段证书，将第一阶段证书发送至多个第二终端 106。第二终端 106 利用第一阶段证书中的区块哈希值生成第二阶段证书，将第二阶段证书发送至第一终端 104 和其他第二终端 106 进行第二阶段协商，以及利用区块哈希值生成第三阶段证书，将第三阶段证书发送至第一终端 104 和其他第二终端 106 进行第三阶段协商。当区块验证通过且协商成功时，表示该区块在区块链系统中达成共识。第一终端 104 和多个第二终端 106 分别将区块分别添加至本地联盟链的副本中。在协商过程中传输的第二阶段证书

和第三阶段证书并不是完整的区块信息，而是可以唯一标识一个区块的区块哈希值。因此能够在区块共识过程中有效减少网络资源消耗，节省通信开销。

在一个实施例中，如图 2 所示，提供了一种基于以太坊的区块链系统，包括主节点 202 和多个备份节点 204，其中：

- 5 主节点 202，用于接收客户终端发送的交易请求，根据交易请求调用联盟链中部署的智能合约进行交易处理，得到交易数据；利用交易数据生成区块，区块具有对应的区块信息，将区块向多个备份节点进行广播。

备份节点 204，用于接收区块，对区块的交易数据进行验证。

- 主节点 202 还用于利用完整的区块信息生成第一阶段证书，将第一阶段
10 证书发送至多个备份节点；备份节点 204 还用于根据第一阶段证书中的区块哈希值分别生成第二阶段证书和第三阶段证书，分别利用第二阶段证书和第三阶段证书对区块进行协商，得到协商结果。

当区块验证通过且协商结果为协商成功时，主节点 202 和多个备份节点 204 分别将区块分别添加至本地联盟链的副本中。

- 15 本实施例中，基于以太坊的区块链系统包括多个节点，节点包括主节点和备份节点。主节点可以只有一个，备份节点可以有多个。多个节点可以组成一个拜占庭系统。

- 节点具有相应的配置文件，配置文件中记录了 IP 地址。每个节点根据配置文件中 IP 地址建立与其他节点之间的通信连接，建立连接后向其他节点发
20 送对应的公钥，其他节点通过私钥签名完成验证，验证通过即表示节点间建立了有效连接。

- 联盟链可以视为联盟成员之间的一个去中心化的、分布式的数字账本。主节点和备份节点上都分别在本地存储了联盟链的副本。相当于联盟链对应的区块链系统中的每一个节点中都记录了该数字账本的复印件。联盟链中包
25 含多个区块，每个区块都分别记录了电子交易对应的交易数据，包括交易时间、交易对象、交易类型、交易金额以及交易数量等内容。

联盟链上可以预先部署智能合约。智能合约可以理解为一可执行的

代码，并且定义了合约参与方的权利和义务。通过智能合约可以使得参与方按照合约进行电子交易。主节点可以接收客户终端发送的交易请求，通过调用智能合约进行交易，得到交易数据。主节点利用交易数据生成区块。具体的，主节点在利用交易数据生成区块之前，获取本地联盟链副本中的最优区块，判断当前时间距离最优区块的时间戳是否小于阈值。阈值可以是区块链系统中对区块达成一致所需的最长时间。若小于阈值，则利用交易数据生成区块。区块具有对应的区块信息，区块信息中除了记录交易数据之外，还记录了区块对应的哈希值等信息。其中，哈希值包含区块哈希值和父哈希值。区块哈希值是一个区块的唯一标识。父哈希值是指一个区块对应的上一个区块的区块哈希值。

主节点将新生成的区块向多个备份节点进行广播。备份节点接收该区块，对区块进行共识。共识包括验证和协商两部分。验证可以是多个节点（包括主节点和备份节点）分别在本地对区块的合法性进行验证。协商需要多个节点通过三个阶段的协商达成一致。

节点（包括主节点和备份节点）对新生成的区块进行校验之前，获取本地联盟链副本中的最优区块，获取新生成的区块的父哈希值，判断新生成的区块的父哈希值是否指向最优区块，若是，则对新生成的区块的交易数据进行校验；否则，将新生成的区块添加至本地交易列表中。节点对新生成的区块的交易数据进行校验时，利用区块中包含的交易数据生成 Merkle 树，计算 Merkle 树的根哈希值。节点获取新生成的区块对应的区块头交易树，计算交易树的哈希值。如果 Merkle 树的根哈希值与区块头交易树的哈希值相同，则在本地创建仓库类副本，并在该仓库类副本中执行交易。交易执行之后，节点修改交易对应的账户信息，利用修改后的账户信息生成该区块对应的状态树，计算状态树的根哈希值。节点根据该仓库类副本生成收据树，计算收据树的根哈希值。如果状态树的根哈希值与收据树的根哈希值相同，则新生成的区块的交易数据通过验证。

区块的共识还需要经过区块链系统的多个节点进行协商，达成一致。根

据拜占庭算法可知，一个拜占庭系统可以容忍发生拜占庭错误的节点数量不超过全部节点数量的三分之一。也就是说，在拜占庭系统中只要多余三分之二的节点对一个区块都反馈了同意加入联盟链中的信息，则协商成功，达成一致。为了可以容忍拜占庭错误，本实施例中的区块链系统中共有 $3f+1$ 个节点，其中 f 是该系统中允许出现的最大错误节点数量。例如，区块链系统中至少包括四个节点。根据 PBFT 机制，区块的协商需要经过三个阶段，包括：预准备阶段（也可以称为第一阶段）、准备阶段（也可以称为第二阶段）和确认阶段（也可以称为第三阶段）。每个阶段都具有相应的证书。证书也就是在区块共识过程中所传输的消息。

10 区块的协商过程如图 3 所示，其中，主节点利用完整的区块信息生成第一阶段证书，将第一阶段证书发送至多个备份节点。完整的区块信息也就是一个区块对应的全部的区块信息。主节点进入第二阶段状态（即准备状态）。备份节点收到第一阶段证书时，即接收到区块完整的区块信息，同时该备份节点进入第二阶段状态。当备份节点确定该第一阶段证书来自与主节点并且是第一次接收到该证书时，备份节点对第一阶段证书进行保存。由此使得每个备份节点中记录了新生成的区块对应的区块信息。备份节点根据完整的区块信息计算对应的区块哈希值，利用区块哈希值生成第二阶段证书。将第二阶段证书发送给其他节点（包括主节点和其他备份节点）。其他节点对第二阶段证书进行校验，校验通过之后，可以返回对第二阶段证书同意的信息。当
15 第二阶段信息经过 $2f$ 个节点的同意，即该备份节点接收到 $2f$ 个节点返回的对第二阶段证书同意的信息时，该备份节点进入第三阶段。备份节点利用区块哈希值再生成第三阶段证书，将第三阶段证书发送至其他节点。当第三阶段证书得到了 $2f+1$ 个节点（包括该备份节点本身）的同意，则新生成的区块在区块链系统中的协商工作得以完成。由于区块哈希值可以唯一标识一个区块，
20 因此第二阶段证书和第三阶段证书能够准确反映出被协商的区块。

进一步的，利用 PBFT 机制，可以将区块链系统的执行过程划分为视图，视图中包括一个主节点和多个备份节点。每个视图可以有相应的标识，每个

节点也可以有相应的标识。例如，视图标记为 v ，该视图中共有 N 个节点，则可以将主节点标记为 p ，备份节点以此标记为 $0, 1, \dots, N-1$ ，且满足 $p = v \bmod N$ 。各个节点（包括主节点和备份节点）采用相同的视图标识进行初始化。由于节点可以被划分为不同的视图，备份节点还可以利用区块哈希值、

5 视图标识和节点标识生成第二阶段证书和第三阶段证书。由于第二阶段证书和第三阶段证书中包含了视图标识和节点标识，由此在第二阶段和第三阶段中能够快速识别出是由哪个节点发出的消息，以便其他节点能向该节点返回同意的消息，有利于提高协商效率。

当区块的验证工作和协商工作都完成时，该区块在区块链系统中达成共识。

10 在，主节点和备份节点将达成共识后的区块分别添加至本地联盟链的副本中。从而使得客户终端本次发起的交易能够安全有效的得以实现。

在传统的 PBFT 机制中，区块协商的三个阶段中，每个阶段都需要利用完整的区块信息分别生成对应的证书。协商过程中每个阶段都会通过多个备份节点来传输包括完整区块信息的证书，由此导致协商过程中会消耗大量的

15 网络资源，造成较大的通信开销。而本实施例中，只在协商的第一阶段会使用完整的区块信息来生成第一阶段证书，在第二阶段和第三阶段利用区块哈希值分别生成第二阶段证书和第三阶段证书，由此能够在第二阶段和第三阶段的协商过程中能有效减少网络资源消耗，节省通信开销。

此外，在传统的方式中，验证代码和协商代码是写在一个类的包中。区块的验证和协商只能以串行的方式执行，这两部分的耦合度较高，导致区块的共识效率较低。而本实施例中，验证代码和协商代码分别写在不同的类的包中。每个节点可以分别运行验证代码对应的类和协商代码对应的类，使得区块的验证和协商可以异步执行，降低了验证与协商的耦合度。不仅有利于代码维护，而且能够有效提高区块的共识效率。

20

25 本实施例中，基于以太坊的区块链系统中，主节点接收客户终端发送的交易请求后，调用联盟链中部署的智能合约进行交易处理。主节点利用交易数据生成区块，并且将该区块向区块链系统中的多个备份节点进行广播。备

份节点对接收到的区块进行验证。主节点利用完整的区块信息生成第一阶段证书，将第一阶段证书发送至多个备份节点，多个备份节点根据第一阶段证书中的区块哈希值分别生成第二阶段证书和第三阶段证书，分别利用第二阶段证书和第三阶段证书对区块进行协商，得到协商结果。当区块验证通过且
5 协商成功时，表示区块在区块链系统中达成共识，可以被主节点和备份节点分别写入本地联盟链的副本中。在协商过程中所传输的第二阶段证书和第三阶段证书并不是完整的区块信息，而是可以唯一标识一个区块的区块哈希值。因此能够在区块共识过程中有效减少网络资源消耗，节省通信开销。从而实现了通过联盟链进行交易时有效减少网络资源消耗的问题。

10 在一个实施例中，主节点和备份节点还用于获取本地联盟链中最优区块对应的时间戳，获取第一阶段证书、第二阶段证书和第三阶段证书的生成时间；若第一阶段证书的生成时间或第二阶段证书的生成时间或第三阶段证书的生成时间早于最优区块对应的时间戳，则清除第一阶段证书或第二阶段证书或第三阶段证书。

15 在基于以太坊的区块链系统中，对区块的协商过程中会生成大量的证书，每个节点都会相应的记录大量的证书，包括第一阶段证书、第二阶段证书和第三阶段证书。在传统的 PBFT 机制中，为了降低节点的内存消耗，可以通过检查点协议对失效的证书进行删除。但是传统的检查点协议中，需要多个节点之间定时协商，对失效的证书按照 PBFT 机制进行共识，在达成共识之
20 后，各个节点对失效的证书进行删除。由于共识过程中，需要进行三个阶段的协商，每个阶段的协商都需要传输相应的证书，由此导致共识过程中会耗费较多的网络资源。

本实施例中，各个节点可以根据联盟链中最优区块的时间戳进行证书清除。联盟链是以链表的形式按照区块的生成时间相连而成，当一个区块添加到联盟链中，则说明在该区块的时间戳之前的证书都已经被校验过，即节点
25 中这些证书相关的状态已经广播完毕，并可以进行清除，而证书的信息可以通过区块的形式永远保存在该节点中。因此，各个节点可以对本地的添加区

块事件进行监听，每当有区块添加到联盟链的副本中时，将该区块时间戳之前存储在该节点本地的证书进行清除。整个过程不需要节点间相互通信，同时也可以保证证书及时的清理，有效节省了网络资源的消耗。

5 在一个实施例中，备份节点包括第一备份节点和第二备份节点，当第一备份节点本地联盟链副本的区块数量少于第二备份节点本地联盟链副本的区块数量时，第一备份节点向其他备份节点请求本地联盟链副本中需要添加的区块对应的区块哈希值，若接收到的区块哈希值中存在相同的哈希值且相同的数量超过阈值，则根据区块哈希值在本地获取第一阶段证书，通过第一阶段证书将对应区块添加至本地联盟链副本中。

10 以太坊中包含了节点间同步区块的解决方案，即当一个节点发现自身维护的区块链与其可信任的节点维护的区块链的最优区块的区块号相差一定大小时，该节点会向其信任的节点（一般为开发者维护的节点）索要区块并将区块添加到区块链中。而在联盟链中并不存在完全可信的节点，因此这一方案在联盟链中并不可行。

15 本实施例中，当某节点（主节点或备份节点）的联盟链副本的状态与其他节点的联盟链副本的状态不一致时，例如，当第一备份节点本地联盟链副本的区块数量少于第二备份节点本地联盟链副本的区块数量时，第一备份节点可以向所属视图中的 $2f+1$ 个节点请求其联盟链副本需要添加的区块对应的区块哈希值。区块哈希值是可以唯一标识区块的 256 位字节数组。当有不少于 $f+1$ 个节点返回的区块哈希值一致时，表示该区块哈希值对应的区块在区块链系统中达成共识。第一备份节点在本地查询该区块对应的第一阶段证书，如果查询到第一阶段证书，则根据第一阶段证书可以获得完整的区块信息，由此可以直接将所需区块添加至本地联盟链副本中，实现了与其他节点联盟链的同步。在这个过程中，第一备份节点不需向其他备份节点或主节点
20 索取区块，通过本地存储的第一阶段证书既可以完成区块添加，有效节省了网络资源的消耗。

在一个实施例中，主节点和多个备份节点组成相应的视图；当主节点发

生故障时，多个备份节点还用于获取所属视图中的所有备份节点对应的加入区块链的时间、性能指数和响应次数；根据加入区块链的时间、性能指数和响应次数中选举新的主节点。

在传统的 PBFT 机制中，还提供了视图切换协议。视图可以按上述实施
5 例中提及的方式进行标识。当主节点发生故障时，下一个编号的备份节点即可成为新的主节点。视图也随之发生切换，视图编号增加 1。例如，视图标记为 v ，该视图中共有 N 个节点，则可以将主节点标记为 p ，备份节点以此标记为 $0, 1, \dots, N-1$ 。当主节点发生故障时，编号为 0 的备份节点即成为新的主节点，视图编号为 $v+1$ 。

10 本实施例中，主节点的异常判断可以通过各个节点的本地联盟链副本中的最优区块的时间戳与阈值进行判断。其中，阈值可以是区块链系统达成一致的最长时间，一个区块从生成到添加到区块链的时间小于阈值。

在其中一个实施例中，当主节点或备份节点中的交易列表不为空时，若最优区块时间戳与当前时间间隔大于阈值，则确定主节点出现异常；或者当
15 主节点或备份节点中的交易列表为空时，如果阈值时间内没有区块添加到本地联盟链副本中，则确定主节点发生异常。由此通过最优区块对应的的时间戳与阈值，能够快速有效的确认区块链系统中的主节点是否发生异常。

在确定主节点发生异常时，多个备份节点选举新的主节点，触发视图切换。多个备份节点可以根据以下规则进行选举，得到新的主节点：备份节点
20 加入到区块链系统中的时间；备份节点的性能指数；备份节点的响应次数。备份节点加入区块链系数的时间具有第一权重，备份节点的性能参数具有第二权重，备份节点的响应次数具有第三权重。备份节点利用第一权重、第二权重和第三权重分别计算其他节点的权重值，根据权重值选举出新的主节点。新的主节点和其他备份节点组成新的视图，从而完成视图切换。

25 由于在选举中考虑到了备份节点加入区块链系统的时间长短、备份节点的性能指数和响应次数等，由此能够确保选举得到的新的主节点的性能是众多从节点中性能最优的。从而能够使得切换后的视图更加稳健。

在一个实施例中，如图 4 所示，一种基于以太坊区块链的交易数据处理方法，应该理解的是，虽然图 4 的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，其可以以其他的顺序执行。而且，图 4 中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，其执行顺序也不必然是依次进行，而是可以与其他步骤或者其他步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。包括以下步骤：

步骤 402，主节点接收客户终端发送的交易请求，根据交易请求调用本地联盟链副本中部署的智能合约进行交易处理，得到交易数据；

步骤 404，主节点利用交易数据生成区块，对区块的交易数据进行验证；区块具有对应的区块信息；

步骤 406，主节点利用完整的区块信息生成第一阶段证书，将第一阶段证书发送至多个备份节点，以使得备份节点根据第一阶段证书中的区块哈希值分别生成第二阶段证书和第三阶段证书，接收备份节点分别利用第二阶段证书和第三阶段证书对区块进行协商所得到的协商结果；

步骤 408，当区块验证通过且协商结果为协商成功时，主节点将区块添加至本地联盟链的副本中。

本实施例中，主节点和备份节点上都分别在本地存储了联盟链的副本。联盟链上还可以部署智能合约，主节点可以接收客户终端发送的交易请求，通过调用智能合约进行交易，得到交易数据。主节点利用交易数据生成区块。主节点将新生成的区块向多个备份节点进行广播。备份节点接收该区块，对区块进行共识。共识包括验证和协商两部分。验证可以是多个节点（包括主节点和备份节点）分别在本地对区块的交易数据进行验证。协商需要多个节点通过三个阶段的协商达成一致。

根据 PBFT 机制，区块的协商需要经过三个阶段，包括：预准备阶段（也可以称为第一阶段）、准备阶段（也可以称为第二阶段）和确认阶段（也可以

称为第三阶段)。每个阶段都具有相应的证书。主节点利用完整的区块信息生成第一阶段证书，将第一阶段证书发送至多个备份节点。主节点进入第二阶段状态（即准备状态）。备份节点收到第一阶段证书时，即接收到区块完整的区块信息，同时该备份节点进入第二阶段状态。备份节点对第一阶段证书进行保存。由此使得每个备份节点中记录了新生成的区块对应的区块信息。备份节点根据完整的区块信息计算对应的区块哈希值，利用区块哈希值生成第二阶段证书。将第二阶段证书发送给其他节点（包括主节点和其他备份节点）。其他节点对第二阶段证书进行校验，校验通过之后，可以返回对第二阶段证书同意的信息。当第二阶段信息经过 $2f$ 个节点的同意，即该备份节点接收到 $2f$ 个节点返回的对第二阶段证书同意的信息时，该备份节点进入第三阶段。备份节点利用区块哈希值再生成第三阶段证书，将第三阶段证书发送至其他节点。当第三阶段证书得到了 $2f+1$ 个节点（包括该备份节点本身）的同意，则新生成的区块在区块链系统中的协商工作得以完成。由于区块哈希值可以唯一标识一个区块，因此第二阶段证书和第三阶段证书能够准确反映出被协商的区块。

当区块的验证工作和协商工作都完成时，该区块在区块链系统中达成共识。在，主节点和备份节点将达成共识后的区块分别添加至本地联盟链的副本中。从而使得客户终端本次发起的交易能够安全有效的得以实现。

本实施例中，在协商过程中传输的第二阶段证书和第三阶段证书并不是完整的区块信息，而是可以唯一标识一个区块的区块哈希值。因此能够在区块共识过程中有效减少网络资源消耗，节省通信开销。从而实现了通过联盟链进行交易时有效减少网络资源消耗的问题。

在一个实施例中，该方法还包括：主节点获取本地联盟链中最优区块对应的时间戳；主节点获取第一阶段证书、第二阶段证书和第三阶段证书的生成时间；若第一阶段证书的生成时间或第二阶段证书的生成时间或第三阶段证书的生成时间早于最优区块对应的时间戳，则清除第一阶段证书或第二阶段证书或第三阶段证书。

本实施例中，主节点可以根据本地联盟链副本中最优区块的时间戳进行证书清除。证书包括第一阶段证书、第二阶段证书和第三阶段证书。联盟链是以链表的形式按照区块的生成时间相连而成，当一个区块添加到联盟链中，则说明在该区块的时间戳之前的证书都已经被校验过，即主节点中这些证书相关的状态已经广播完毕，并可以进行清除，而证书的信息可以通过区块的形式永远保存在该节点中。因此，主节点可以对本地的添加区块事件进行监听，每当有区块添加到联盟链的副本中时，将该区块时间戳之前存储在该节点本地的证书进行清除。整个过程不需要节点间相互通信，同时也可以保证证书及时的清理，有效节省了网络资源的消耗。

10 在一个实施例中，该方法还包括：当本地联盟链副本中的区块数量少于第一备份节点中的区块数量时，向其他备份节点发送需要添加的区块对应的区块哈希值的获取请求；接收其他备份节点返回的区块哈希值，若接收到的多个区块哈希值中存在相同的哈希值且相同的数量超过阈值，则根据区块哈希值在本地获取第一阶段证书；通过第一阶段证书将对应区块添加至本地联盟链副本中。

当主节点的联盟链副本的状态与备份节点的联盟链副本的状态不一致时，例如，当主节点本地联盟链副本的区块数量少于第一备份节点本地联盟链副本的区块数量时，主节点可以向所属视图中的 $2f+1$ 个备份节点请求其联盟链副本需要添加的区块对应的区块哈希值。区块哈希值是可以唯一标识区块的 256 位字节数组。当有不少于 $f+1$ 个备份节点返回的区块哈希值一致时，表示该区块哈希值对应的区块在区块链系统中达成共识。主节点在本地查询该区块对应的第一阶段证书，如果查询到第一阶段证书，则根据第一阶段证书可以获得完整的区块信息，由此可以直接将所需区块添加至主节点本地的联盟链副本中，实现了与其他备份节点联盟链的同步。在这个过程中，主节点不需向其他备份节点索取区块，通过本地存储的第一阶段证书既可以完成区块添加，有效节省了网络资源的消耗。

在一个实施例中，如图 5 所示，提供了一种基于以太坊区块链的交易数

据处理方法，应该理解的是，虽然图 5 的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，其可以以其他的顺序执行。而且，图 5 中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，其执行顺序也不必然是依次进行，而是可以与其他步骤或者其他步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。包括以下步骤：

步骤 502，备份节点接收主节点广播的区块，区块是主节点在接收到客户终端发送的交易请求时调用联盟链中部署的智能合约进行交易得到交易数据，并利用交易数据生成的；区块具有对应的区块信息；

步骤 504，备份节点接收区块，对区块的交易数据进行验证；

步骤 506，备份节点接收主节点利用完整的区块信息生成的第一阶段证书，根据第一阶段证书中的区块哈希值分别生成第二阶段证书和第三阶段证书，分别利用第二阶段证书和第三阶段证书对区块进行协商，得到协商结果；

步骤 508，当区块验证通过且协商结果为协商成功时，备份节点将区块添加至本地联盟链的副本中。

本实施例中，主节点和备份节点上都分别在本地存储了联盟链的副本。联盟链上还可以部署智能合约，主节点可以接收客户终端发送的交易请求，通过调用智能合约进行交易，得到交易数据。主节点利用交易数据生成区块。主节点将新生成的区块向多个备份节点进行广播。备份节点接收该区块，对区块进行共识。共识包括验证和协商两部分。验证可以是多个节点（包括主节点和备份节点）分别在本地对区块的交易数据进行验证。协商需要多个节点通过三个阶段的协商达成一致。

根据 PBFT 机制，区块的协商需要经过三个阶段，包括：预准备阶段（也可以称为第一阶段）、准备阶段（也可以称为第二阶段）和确认阶段（也可以称为第三阶段）。每个阶段都具有相应的证书。主节点利用完整的区块信息生

- 成第一阶段证书，将第一阶段证书发送至多个备份节点。主节点进入第二阶段状态（即准备状态）。备份节点收到第一阶段证书时，即接收到区块完整的区块信息，同时该备份节点进入第二阶段状态。备份节点对第一阶段证书进行保存。由此使得每个备份节点中记录了新生成的区块对应的区块信息。备份节点根据完整的区块信息计算对应的区块哈希值，利用区块哈希值生成第二阶段证书。将第二阶段证书发送给其他节点（包括主节点和其他备份节点）。其他节点对第二阶段证书进行校验，校验通过之后，可以返回对第二阶段证书同意的信息。当第二阶段信息经过 $2f$ 个节点的同意，即该备份节点接收到 $2f$ 个节点返回的对第二阶段证书同意的信息时，该备份节点进入第三阶段。
- 10 备份节点利用区块哈希值再生成第三阶段证书，将第三阶段证书发送至其他节点。当第三阶段证书得到了 $2f+1$ 个节点（包括该备份节点本身）的同意，则新生成的区块在区块链系统中的协商工作得以完成。由于区块哈希值可以唯一标识一个区块，因此第二阶段证书和第三阶段证书能够准确反映出被协商的区块。
- 15 当区块的验证工作和协商工作都完成时，该区块在区块链系统中达成共识。在，主节点和备份节点将达成共识后的区块分别添加至本地联盟链的副本中。从而使得客户终端本次发起的交易能够安全有效的得以实现。
- 本实施例中，在协商过程中传输的第二阶段证书和第三阶段证书并不是完整的区块信息，而是可以唯一标识一个区块的区块哈希值。因此能够在区块共识过程中有效减少网络资源消耗，节省通信开销。从而实现了通过联盟链进行交易时有效减少网络资源消耗的问题。
- 20 在一个实施例中，该方法还包括：当主节点发生故障时，备份节点获取所属视图中的所有备份节点对应的加入区块链的时间、性能指数和响应次数；根据加入区块链的时间、性能指数和响应次数中选举新的主节点。
- 25 本实施例中，当备份节点中的交易列表不为空时，若最优区块时间戳与当前时间间隔大于阈值，则确定主节点出现异常；或者当备份节点中的交易列表为空时，如果阈值时间内没有区块添加到本地联盟链副本中，则确定主

节点发生异常。

在确定主节点发生异常时，多个备份节点选举新的主节点，触发视图切换。多个备份节点可以根据备份节点加入到区块链系统中的时间；备份节点的性能指数；备份节点的响应次数进行选举，得到新的主节点。新的主节点和其他备份节点组成新的视图，从而完成视图切换。

由于在选举中考虑到了备份节点加入区块链系统的时间长短、备份节点的性能指数和响应次数等，由此能够确保选举得到的新的主节点的性能是众多从节点中性能最优的。从而能够使得切换后的视图更加稳健。

在一个实施例中，该方法还包括：备份节点获取本地联盟链中最优区块对应的时间戳；备份节点获取第一阶段证书、第二阶段证书和第三阶段证书的生成时间；若第一阶段证书的生成时间或第二阶段证书的生成时间或第三阶段证书的生成时间早于最优区块对应的时间戳，则清除第一阶段证书或第二阶段证书或第三阶段证书。

本实施例中，备份节点可以根据本地联盟链副本中最优区块的时间戳进行证书清除。证书包括第一阶段证书、第二阶段证书和第三阶段证书。联盟链是以链表的形式按照区块的生成时间相连而成，当一个区块添加到联盟链中，则说明在该区块的时间戳之前的证书已经被校验过，即备份节点中这些证书相关的状态已经广播完毕，并可以进行清除，而证书的信息可以通过区块的形式永远保存在该节点中。因此，备份节点可以对本地的添加区块事件进行监听，每当有区块添加到联盟链的副本中时，将该区块时间戳之前存储在该节点本地的证书进行清除。整个过程不需要节点间相互通信，同时也可以保证证书及时的清理，有效节省了网络资源的消耗。

在一个实施例中，提供了一种计算机设备，如区块链系统中的主节点或备份节点等，其中主节点或备份节点可以是台式电脑、笔记本电脑或服务器等。如图 6 所示，该计算机设备包括通过系统总线连接的处理器、存储器和网络接口。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该计算机设备的非易失

性存储介质存储有操作系统和计算机可读指令。该计算机设备的内存储器为非易失性存储介质中的操作系统和计算机可读指令的运行提供环境。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机可读指令被处理器执行时以实现一种基于以太坊区块链的交易数据处理方法。本领域技术人员可以理解，图 6 中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

在一个实施例中，提供了一种计算机设备，包括存储器和一个或多个处理器，所述存储器中储存有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述一个或多个处理器执行以下步骤：

主节点接收客户终端发送的交易请求，根据交易请求调用本地联盟链副本中部署的智能合约进行交易处理，得到交易数据；

主节点利用交易数据生成区块，对区块的交易数据进行验证；区块具有对应的区块信息；

主节点利用完整的区块信息生成第一阶段证书，将第一阶段证书发送至多个备份节点，以使得备份节点根据第一阶段证书中的区块哈希值分别生成第二阶段证书和第三阶段证书，接收备份节点分别利用第二阶段证书和第三阶段证书对区块进行协商所得到的协商结果；及

当区块验证通过且协商结果为协商成功时，主节点将区块添加至本地联盟链的副本中。

在一个实施例中，计算机可读指令被所述处理器执行时，使得所述一个或多个处理器还执行以下步骤：

主节点获取本地联盟链中最优区块对应的时间戳；

主节点获取第一阶段证书、第二阶段证书和第三阶段证书的生成时间；及

若第一阶段证书的生成时间或第二阶段证书的生成时间或第三阶段证书

的生成时间早于最优区块对应的时间戳，则清除第一阶段证书或第二阶段证书或第三阶段证书。

在一个实施例中，计算机可读指令被所述处理器执行时，使得所述一个或多个处理器还执行以下步骤：

- 5 当主节点本地联盟链副本中的区块数量少于第一备份节点中的区块数量时，向其他备份节点发送需要添加的区块对应的区块哈希值的获取请求；

接收其他备份节点返回的区块哈希值，若接收到的多个区块哈希值中存在相同的哈希值且相同的数量超过阈值，则根据区块哈希值在本地获取第一阶段证书；及

- 10 通过第一阶段证书将对应区块添加至本地联盟链副本中。

在一个实施例中，提供了一种计算机设备，包括存储器和一个或多个处理器，所述存储器中储存有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述一个或多个处理器执行以下步骤：

- 15 备份节点接收主节点广播的区块，区块是主节点在接收到客户终端发送的交易请求时调用联盟链中部署的智能合约进行交易得到交易数据，并利用交易数据生成的；区块具有对应的区块信息；

备份节点对接收到的区块的交易数据进行验证；

- 20 备份节点接收主节点利用完整的区块信息生成的第一阶段证书，根据第一阶段证书中的区块哈希值分别生成第二阶段证书和第三阶段证书，分别利用第二阶段证书和第三阶段证书对区块进行协商，得到协商结果；及

当区块验证通过且协商结果为协商成功时，备份节点将区块添加至本地联盟链的副本中。

在一个实施例中，计算机可读指令被所述处理器执行时，使得所述一个或多个处理器还执行以下步骤：

- 25 当主节点发生故障时，备份节点获取所属视图中的所有备份节点对应的加入区块链的时间、性能指数和响应次数；及

根据加入区块链的时间、性能指数和响应次数中选举新的主节点。

在一个实施例中，计算机可读指令被所述处理器执行时，使得所述一个或多个处理器还执行以下步骤：

备份节点获取本地联盟链中最优区块对应的时间戳；

备份节点获取第一阶段证书、第二阶段证书和第三阶段证书的生成时间；

5 及

若第一阶段证书的生成时间或第二阶段证书的生成时间或第三阶段证书的生成时间早于最优区块对应的时间戳，则清除第一阶段证书或第二阶段证书或第三阶段证书。

10 在一个实施例中，提供了一个或多个存储有计算机可读指令的计算机可读非易失性存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行以下步骤：

主节点接收客户终端发送的交易请求，根据交易请求调用本地联盟链副本中部署的智能合约进行交易处理，得到交易数据；

15 主节点利用交易数据生成区块，对区块的交易数据进行验证；区块具有对应的区块信息；

主节点利用完整的区块信息生成第一阶段证书，将第一阶段证书发送至多个备份节点，以使得备份节点根据第一阶段证书中的区块哈希值分别生成第二阶段证书和第三阶段证书，接收备份节点分别利用第二阶段证书和第三阶段证书对区块进行协商所得到的协商结果；及

20 当区块验证通过且协商结果为协商成功时，主节点将区块添加至本地联盟链的副本中。

在一个实施例中，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器还执行以下步骤：

主节点获取本地联盟链中最优区块对应的时间戳；

25 主节点获取第一阶段证书、第二阶段证书和第三阶段证书的生成时间；

及

若第一阶段证书的生成时间或第二阶段证书的生成时间或第三阶段证书

的生成时间早于最优区块对应的时间戳，则清除第一阶段证书或第二阶段证书或第三阶段证书。

在一个实施例中，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器还执行以下步骤：

- 5 当主节点本地联盟链副本中的区块数量少于第一备份节点中的区块数量时，向其他备份节点发送需要添加的区块对应的区块哈希值的获取请求；

接收其他备份节点返回的区块哈希值，若接收到的多个区块哈希值中存在相同的哈希值且相同的数量超过阈值，则根据区块哈希值在本地获取第一阶段证书；及

- 10 通过第一阶段证书将对应区块添加至本地联盟链副本中。

在一个实施例中，提供了一个或多个存储有计算机可读指令的计算机可读非易失性存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行以下步骤：

- 15 备份节点接收主节点广播的区块，区块是主节点在接收到客户终端发送的交易请求时调用联盟链中部署的智能合约进行交易得到交易数据，并利用交易数据生成的；区块具有对应的区块信息；

备份节点对接收到的区块的交易数据进行验证；

- 20 备份节点接收主节点利用完整的区块信息生成的第一阶段证书，根据第一阶段证书中的区块哈希值分别生成第二阶段证书和第三阶段证书，分别利用第二阶段证书和第三阶段证书对区块进行协商，得到协商结果；及

当区块验证通过且协商结果为协商成功时，备份节点将区块添加至本地联盟链的副本中。

在一个实施例中，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器还执行以下步骤：

- 25 当主节点发生故障时，备份节点获取所属视图中的所有备份节点对应的加入区块链的时间、性能指数和响应次数；及

根据加入区块链的时间、性能指数和响应次数中选举新的主节点。

在一个实施例中，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器还执行以下步骤：

备份节点获取本地联盟链中最优区块对应的时间戳；

备份节点获取第一阶段证书、第二阶段证书和第三阶段证书的生成时间；

5 及

若第一阶段证书的生成时间或第二阶段证书的生成时间或第三阶段证书的生成时间早于最优区块对应的时间戳，则清除第一阶段证书或第二阶段证书或第三阶段证书。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流
10 程，是可以通过计算机可读指令来指令相关的硬件来完成，所述的计算机可读指令可存储于一个或多个非易失性计算机可读存储介质中，该计算机可读指令在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory, ROM）等。

以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未
15 对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

以上所述实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干
20 变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。