

一种基于区块链的节点管理方法和装置

技术领域

[01]本说明书涉及网络技术领域，尤其涉及一种基于区块链的节点管理方法和装置。

背景技术

- 5 [02]区块链技术，也被称之为分布式账本技术，是一种由若干台计算设备共同参与“记账”，共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台计算设备可以参与数据库记录、并且各计算设备之间可以快速的进行数据同步的特性，使得区块链技术已在众多的领域中广泛的进行应用。

发明内容

- 10 [03]本说明书提供了一种基于区块链的节点管理方法，所述区块链的分布式数据库中存储有节点身份表，其中，所述节点身份表用以记录所述区块链节点的证书和与所述证书对应的所述区块链节点的唯一性标识；所述方法包括：
- [04]区块链已有节点接收目标交易，所述目标交易包括新节点的证书和新节点的唯一性标识；
- 15 [05]验证所述目标交易，以使所述目标交易经过所述区块链的共识验证后将包含所述新节点的唯一性标识和证书的节点身份表对应收录于所述区块链的分布式数据库中。
- [06]在又一示出的实施中，所述验证所述目标交易，包括：
- [07]验证所述新节点的证书，并验证所述新节点的证书对应的节点身份认证机构是否属于所述区块链认可的节点身份认证机构。
- 20 [08]在又一示出的实施中，所述目标交易还包括和区块链中的背书节点至少基于所述新节点的证书所作的数字签名；
- [09]所述验证所述目标交易，包括：
- [10]验证所述区块链的背书节点至少基于所述新节点的证书所作的合法的数字签名是否符合预设的数量。
- 25 [11]在又一示出的实施中，所述的方法还包括：

[12]调用与所述节点身份表管理对应的智能合约，执行所述智能合约声明的节点身份表更新逻辑，验证所述目标交易，在所述验证通过后将所述新节点的唯一性标识和证书对应收录于所述节点身份表。

[13]在又一示出的实施中，所述的方法还包括：

- 5 [14]接收所述新节点的网络地址、所述新节点的唯一性标识和所述新节点所作的数字签名；

[15]从所述区块链的分布式数据库中获取所述节点身份表中，基于所述唯一性识别码获取所述新节点的证书；

[16]基于所述新节点的证书，验证所述数字签名；

- 10 [17]在所述验证通过后，将所述网络地址存储至所述区块链已有节点的本地数据库。

[18]在又一示出的实施中，所述的方法还包括：

[19]向所述新节点发送所述区块链节点的本地数据库存储的区块链中其他已有节点的网络地址。

[20]在又一示出的实施中，所述的方法还包括：

- 15 [21]向所述新节点发送所述区块链已有节点备份的所述区块链的分布式数据库中的数据。

[22]相应的，本说明书还提供了一种基于区块链的节点管理装置，所述区块链的分布式数据库中存储有节点身份表，其中，所述节点身份表用以记录所述区块链节点的证书和与所述证书对应的所述区块链节点的唯一性标识；所述装置包括：

- 20 [23]接收单元，区块链已有节点接收目标交易，所述目标交易包括新节点的证书和新节点的唯一性标识；

[24]验证单元，验证所述目标交易，以使所述目标交易经过所述区块链的共识验证后将包含所述新节点的唯一性标识和证书的节点身份表对应收录于所述区块链的分布式数据库中。

[25]在又一示出的实施中，所述验证单元：

- 25 [26]验证所述新节点的证书，并验证所述新节点的证书对应的节点身份认证机构是否属于所述区块链认可的节点身份认证机构。

[27]在又一示出的实施中，所述目标交易还包括和区块链中的背书节点至少基于所述新

节点的证书所作的数字签名；

[28]所述验证单元：

[29]验证所述区块链的背书节点至少基于所述新节点的证书所作的合法的数字签名是否符合预设的数量。

5 [30]在又一示出的实施中，所述的装置还包括：

[31]智能合约执行单元，调用与所述节点身份表管理对应的智能合约，执行所述智能合约声明的节点身份表更新逻辑，验证所述目标交易，在所述验证通过后将所述新节点的唯一性标识和证书对应收录于所述节点身份表。

[32]在又一示出的实施中，所述的装置还包括获取单元和存储单元，

10 [33]所述接收单元，接收所述新节点的网络地址、所述新节点的唯一性标识和所述新节点所作的数字签名；

[34]所述获取单元，从所述区块链的分布式数据库中获取所述节点身份表中，基于所述唯一性识别码获取所述新节点的证书；

[35]所述验证单元，基于所述新节点的证书，验证所述数字签名；

15 [36]所述存储单元，在所述验证通过后，将所述网络地址存储至所述区块链已有节点的本地数据库。

[37]在又一示出的实施中，所述的装置还包括：

[38]发送单元，向所述新节点发送所述区块链节点的本地数据库存储的区块链中其他已有节点的网络地址。

20 [39]在又一示出的实施中，所述的装置还包括：

[40]发送单元，向所述新节点发送所述区块链已有节点备份的所述区块链的分布式数据库中的数据。

[41]本说明书还提供了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述基于区块链的节点管理方法所述的步骤。

25

[42]本说明书还提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行上述基于区块链的节点管理方法所述的步骤。

[43]本说明书提供的基于区块链的节点管理方法和装置，通过在区块链的分布式数据库内建立存储节点身份表，收录可加入该区块链的节点的证书，从而防止任意节点无需经过链内的节点共识或同意而加入区块链，提供了区块链的安全性。

附图说明

5 [44]图 1 为本说明书一示例性实施例提供的区块链的节点管理方法的流程图；

[45]图 2 为本说明书一示例性实施例提供的区块链的节点管理装置的示意图；

[46]图 3 为运行本说明书所提供的区块链的节点管理装置实施例的一种硬件结构图。

具体实施方式

10 [47]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述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。

15 [48]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。

20 [49]如图 1 所示，本说明书一示意性实施例提供了一种基于区块链的节点管理方法，所述区块链的分布式数据库中存储有用以记录可信节点的身份证书的可信节点表，所述节点身份表用以记录所述区块链节点的证书和与所述证书对应的所述区块链节点的唯一性标识。

25 [50]本实施例所述的区块链，具体可指一个各节点设备通过共识机制达成的、具有分布式数据存储结构的 P2P 网络系统，该区块链内的数据分布在时间上相连的一个个“区块（block）”之内，后一区块包含前一区块的数据摘要，且根据具体的共识机制（如 POW、POS、DPOS 或 PBFT 等）的不同，达成全部或部分节点设备的数据全备份。本领域的技术人员熟知，由于区块链系统在相应共识机制下运行，已收录至区块链数据库内的数

据很难被任意的节点设备篡改，例如采用 Pow 共识的区块链，至少需要全网 51%算力的攻击才有可能篡改已有数据，因此区块链系统有着其他中心化数据库系统所法比拟的保证数据安全、防攻击篡改的特性。

5 [51]本说明书所述的区块链节点，不仅可包括备份有区块链的分布式数据库的全量数据的全节点设备，还可包括备份有区块链的分布式数据库的部分数据的轻节点设备，以及其他的终端设备或客户端，在本说明书中不做限定。

[52]在本说明书中所描述的交易（transaction），是指用户通过区块链的节点设备创建，并需要最终发布至区块链的分布式数据库中的一笔数据。其中，区块链中的交易，存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移；
10 例如，在传统的比特币区块链网络中，交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔任意的数据：例如，运营方可以基于实际的业务需求搭建一个联盟链，依托于联盟链部署一些与价值转移无关的其它类型的在线业务（比如，租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等），而在这类联盟链中，交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务
15 请求；又如，该交易还可以是用户向区块链发送的、用以更改用户的账户状态的数据（如账户余额等）。因此，只要是用户向区块链的分布式数据库发布的任意数据，无论该任意数据被保存在区块的区块体、区块头还是其他位置，均可属于本发明所述的“交易”。

[53]在传统区块链中，区块链的分布式数据库中并不记录节点的身份；用户通过区块链网络注册协议加入区块链后，通常会将注册用户身份（或账户身份）绑定在运行注册协
20 议的节点设备上，并在网络路由表中显示与该节点绑定的用户身份。例如，在以太坊区块链中，用户通过在节点设备上运行网络注册协议，获取到用户账户，并以将形如 `enode://pubkey1@ip1:port1` 的信息加入该区块链的网络路由表，以供与区块链中的其他节点进行通信。上述路由信息会暴露区块链中的用户所在的节点 IP 及端口信息，造成不安全的隐患。

25 [54]在本实施例中，为方便对区块链的节点进行管理，经过区块链节点的共识，在上述区块链的分布式数据库中存储有节点身份表，用以记录该区块链网络中的节点的证书和与所述证书对应的所述区块链节点的唯一性标识。节点的证书可包括节点对应的公钥和节点身份认证机构至少对节点的公钥所作的数字签名，还可以包括节点的 ID 名称、所属机构、物理地址等身份信息。本说明书并不限定证书所遵循的协议类型，如 TLS 证书
30 等通过 CA 认证机构认证的证书均可应用至本说明提供的实施例中。节点身份认证机构

可包括上述区块链系统的管理机构、或上述区块链中信用较高的用户等，在此不作限定。上述区块链节点的唯一性标识可以包括节点的名称、节点的身份编码、节点的公钥等。经区块链上的节点的共识，利用节点身份表管理区块链上的节点，增加了区块链系统的安全性。

5 [55]本实施例所提供的区块链的节点管理方法包括：

[56]步骤 102，区块链节点接收目标交易，所述目标交易包括新节点的证书和新节点的唯一性标识。

[57]待加入区块链的新节点可通过链外通信、或运行节点加入协议的方式，与区块链内的任一具有节点身份表管理权限的身份管理节点通信，将自身的证书及唯一性标识发送
10 给上述身份管理节点，以使上述身份管理节点通过向区块链中发送用以更新节点身份表的目标交易，将目标交易在区块链内进行传播，因此区块链节点可接收到该目标交易。

[58]上述目标交易，既可以包含该区块链内已有节点的证书及其对应的唯一性标识，以在该节点身份表更新交易被区块链共识后将包含已有节点和上述新节点的证书、及其对应的唯一性标识的节点身份表更新于所述区块链的分布式数据库；也可以仅包含新增的
15 节点的证书及其唯一性标识，以在该节点身份表更新交易被区块链共识后将新增的节点的证书及其唯一性标识更新于所述区块链的分布式数据库为节点身份表设置的状态中。

[59]步骤 104，验证所述目标交易，以使所述目标交易经过所述区块链的共识验证后将包含所述新节点的唯一性标识和证书的节点身份表对应收录于所述区块链的分布式数据库中。

20 [60]区块链已有节点在接收到目标交易后，基于该区块链对目标交易的验证规则，对该目标交易进行验证，以使所述目标交易经过所述区块链的共识验证后将包含所述新节点的唯一性标识和证书的节点身份表对应收录于所述区块链的分布式数据库中。

[61]本实施例所述的区块链中已有节点对上述目标交易的验证，通常可包括对该目标交易的内容的验证，如利用节点身份认证机构的公钥验证新节点的证书是否合法，且验证
25 签署该新节点证书的节点身份认证机构是否属于该区块链认可的节点身份认证机构。

[62]为保证安全性，通常在区块链中加入新节点还需经过一些已有节点的背书，所述“背书”通常通过这些节点至少基于所述新节点证书进行数字签名来表现，在本说明书中，将上述对新节点进行“背书”的节点称为“背书节点”。因此上述验证还可包括对该目标交易中包含的所述区块链的背书节点至少基于所述新节点的证书所作的数字签名的

验证,并计算上述已被验证合法的数字签名是否满足预设的数量,亦即要有符合预设的数量的背书节点对该新节点的加入进行背书,方可使上述节点身份表更新交易通过验证。

[63]本领域的技术人员应知,将上述目标交易收录到所述区块链的分布式数据库中的具体步骤,可以包括:

5 [64]所述区块链中具有记账权限的节点将所述目标交易加入到候选区块,加入位置包括但不限于区块体或区块头;

[65]从所述具有记账权限的节点中确定满足所述区块链共识机制的共识记账节点;

[66]所述共识记账节点向所述区块链的节点广播所述候选区块;

10 [67]在所述候选区块通过所述区块链符合预设数量的节点的验证认可后,所述候选区块被视为最新区块,加入到所述区块链的分布式数据库中。

[68]在上述的实施例,具有记账权限的节点是指具有生成候选区块权限的节点,可包括具有较高信用用户的节点、或上述区块链中的其他节点。根据所述区块链的共识机制,可从上述对所述候选区块具有记账权限的节点中确定共识记账节点,上述共识机制可以包括工作量证明机制(PoW)、或权利证明机制(PoS)、或股份授权证明机制(DPoS)

15 等,或联盟链通常采用的拜占庭容错算法共识机制PBFT等。

[69]在又一示出的实施方式中,上述将新节点的证书和唯一性标识收录于节点身份表还可通过调用智能合约的方式来实现,该智能合约内存储有节点身份表,用以对区块链网络中的节点进行管理。上述目标交易可包含新增的节点的证书及其唯一性标识,及其所调用的智能合约的地址及接口,以在该目标交易所调用的智能合约的运行结果被区块链
20 共识后,将新增的节点的证书及其唯一性标识更新于所述智能合约存储的节点身份表中。

[70]因此,上述实施例所述的基于区块链的节点管理方法还包括:调用与所述节点身份表管理对应的智能合约,执行所述智能合约声明的节点身份表更新逻辑,验证所述目标交易,在所述验证通过后将所述新节点的唯一性标识和证书对应收录于所述节点身份表。

[71]类似的,在本实施例所述的智能合约所执行的节点身份表更新逻辑中,验证所述目标交易通常可包括对目标交易的内容的验证,如利用节点身份认证机构的公钥验证上述
25 新节点的证书,且验证该节点身份认证机构是否属于该区块链认可的节点身份认证机构;还可包括对所述区块链的背书节点至少基于所述新节点的证书所作的数字签名的验证,并计算上述已被验证合法的数字签名是否满足预设的数量,亦即要有符合预设的数量的背书节点对该新节点的加入进行背书,方可使上述节点身份表更新交易通过上述智能合

约的合法性验证。

[72]利用智能合约管理更新区块链的节点身份表，该智能合约可在任意时刻应区块链的具有节点身份表管理权限的节点发送的目标交易而被调用，从而在区块链各节点的共识下管理更新该节点身份表，提高了区块链节点管理的安全性、合法性和公平性。

- 5 [73]经过步骤 102 至 104 的执行，上述待加入区块链的新节点已经具备了加入上述区块链的权限。在具备了加入上述区块链的权限后，上述新节点可通过链外通信或其他方式获知上述区块链中至少一个已有节点的网络地址，并通过该网络地址与上述至少一个已有节点开展通信连接。本说明书各实施例所述的网络地址，通常可以包括节点所在的 IP 地址及端口等内容。

- 10 [74]在又一示出的实施例中，本说明书所提供的基于区块链的节点管理方法还包括步骤 106 至 110。

[75]步骤 106，接收所述新节点的网络地址、所述新节点的唯一性标识和所述新节点所作的数字签名。

- 15 [76]通过与上述新节点产生链外通信连接，上述新节点可将自身的网络地址、唯一性标识（如名称、或硬件地址、或身份编码或公钥等）及所述新节点所作的数字签名发送至上述产生通信连接的区块链的已有节点；相应地，上述区块链已有节点接收上述新节点的网络地址、所述新节点的唯一性标识和所述新节点所作的数字签名。

- [77]值得注意的是，上述新节点所作的数字签名是上述新节点利用已被上述节点身份表收录的证书中的公钥对应私钥所作的数字签名，该数字签名可以基于任何内容而作，例如可以基于该新节点的网络地址、或新节点的唯一性标识、或其他内容，其目的在于方便与之进行通信连接的已有节点可以基于上述节点身份表中收录的新节点的证书对该数字签名进行验证，以确认与其通信的新节点是否确实是经过区块链共识认可的新节点。值得注意的是，当上述新节点所作的数字签名是基于其他内容时，上述新节点应将其所签署的内容也发送至上述区块链已有节点，方便其对数字签名进行验证。

- 25 [78]步骤 108，从所述区块链的分布式数据库中获取所述节点身份表中，基于所述唯一性识别码获取所述新节点的证书。

[79]基于以上多个实施例提供的节点身份表的更新方法，上述区块链中的已有节点可以从被区块链的分布式数据库收录的目标交易中、或节点身份表状态中、或调用运行上述用于存储及管理节点身份表的智能合约等方式，基于所述新节点发送的唯一性识别码检

索获取对应的新节点的证书。

[80]步骤 110, 基于所述新节点的证书, 验证所述数字签名。

[81]从所述新节点的证书中获取所述新节点的公钥, 利用新节点的公钥对新节点所作的数字签名进行验证, 如果上述验证通过, 则证明与区块链的上述已有节点进行通信连接的上述新节点确实为已经过区块链各节点共识验证的可信节点。

[82]步骤 112, 在所述验证通过后, 将所述网络地址存储至所述已有节点的本地数据库。

[83]为方便区块链内的节点更新同步区块链分布式数据库中的数据, 区块链中的每个节点需获知其他至少一个区块链节点的网络地址, 以完成数据的传递、广播或同步, 区块链的节点可以将其他区块链节点的网络地址保存在本地数据库中, 如配置专门的 Config 文件收录其他区块链节点的 IP 地址及端口。因此, 在上述区块链已有节点验证上述新节点的证书被收录于节点身份表, 确定该新节点确为区块链共识同意加入的可信节点时, 应将该新节点的网络地址存储至本地数据库中, 例如, 将该新节点的网络地址收录在上述专门配置的 Config 文件中。

[84]通过以上步骤, 上述新节点即可以区块链节点的身份与已有节点进行区块数据的同步, 亦即向所述新节点发送所述已有节点备份的所述区块链的分布式数据库中的数据。在一示出的实施方式中, 上述区块数据的同步可以包括以下步骤:

[85]新节点设备向区块链网络上的已有节点发起区块数据的同步请求; 从已有节点上同步现有的区块数据, 上述已有节点通常为上述新节点的周围邻近的节点, 进一步地, 为提高初始区块数据下载的进程, 可采用“区块报头先行”(header first)的下载方式, 先行从邻节点下载所有现有区块的区块头, 并在区块头下载完毕后, 新节点可并行地从多个邻节点同时下载不同高度区间的区块, 大大提升现有的区块数据的同步速度; 同步完成后, 进行区块数据验证, 上述区块数据验证过程包括区块的格式校验(包括版本、时间戳)、区块头哈希值的校验、及对所有交易按交易验证规则进行校验等, 上述对所有交易按交易验证规则进行校验, 包括如交易的格式是否正确、按照交易的数据结构生成的 Merkle Root 是否正确等多项内容, 以检验已有区块数据的正确性; 上述区块数据检验完毕后, 作为区块链节点参与到所述区块链运行中来, 接收、验证、存储经区块链的节点共识产生的新的区块, 等等。

[86]在上述实施方式中, 为方便上述新节点可以并行地从多个邻节点同时下载不同高度区间的区块, 以提高数据同步效率, 在又一示出的实施方式中, 上述实施例中的已有节

点可向所述新节点发送所述已有节点的本地数据库存储的其他已有节点的网络地址，以方便上述新节点进行通信连接。类似的，上述其他已有节点也通过执行如上述实施例所述的步骤 102 至 112 所述的步骤后，认可上述新节点为该区块链的可信节点，从而与上述新节点开展数据同步，向所述新节点发送所述已有节点备份的所述区块链的分布式数据库中的数据。

[87]以上多个实施例提供的基于区块链的节点管理方法，通过在区块链的分布式数据库内建立存储节点身份表，收录可加入该区块链的节点的证书，从而防止任意节点无需经过链内的节点共识或同意而加入区块链，提供了区块链的安全性。上述区块链中的已有节点通过与新节点链外通信，验证新节点是否属于已被区块链的节点共识同意接收的可信节点，并在通过验证后将该新节点作为区块链中的节点、在本地数据库中收录该区块链新节点的网络地址，以方便该已有节点和新节点进行区块链网络内的通信和数据传输或广播。

[88]与上述流程实现对应，本说明书的实施例还提供了一种区块链的节点管理装置。上述装置可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为逻辑意义上的装置，是通过所在设备的 CPU(Central Process Unit，中央处理器)将对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，除了图 3 所示的 CPU、内存以及存储器之外，网络风险业务的实现装置所在的设备通常还包括用于进行无线信号收发的芯片等其他硬件，和/或用于实现网络通信功能的板卡等其他硬件。

[89]图 2 所示为一种基于区块链的节点管理装置 20，所述区块链的分布式数据库中存储有节点身份表，其中，所述节点身份表用以记录所述区块链节点的证书和与所述证书对应的所述区块链节点的唯一性标识；所述装置 20 包括：

[90]接收单元 202，区块链已有节点接收目标交易，所述目标交易包括新节点的证书和新节点的唯一性标识；

[91]验证单元 204，验证所述目标交易，以使所述目标交易经过所述区块链的共识验证后将包含所述新节点的唯一性标识和证书的节点身份表对应收录于所述区块链的分布式数据库中。

[92]在又一示出的实施中，所述验证单元 204：

[93]验证所述新节点的证书，并验证所述新节点的证书对应的节点身份认证机构是否属于所述区块链认可的节点身份认证机构。

- [94]在又一示出的实施中，所述目标交易还包括和区块链中的背书节点至少基于所述新节点的证书所作的数字签名；
- [95]所述验证单元 204：
- [96]验证所述区块链的背书节点至少基于所述新节点的证书所作的合法的数字签名是否符合预设的数量。
- [97]在又一示出的实施中，所述的装置 20 还包括：
- [98]智能合约执行单元 208，调用与所述节点身份表管理对应的智能合约，执行所述智能合约声明的节点身份表更新逻辑，验证所述目标交易，在所述验证通过后将所述新节点的唯一性标识和证书对应收录于所述节点身份表。
- 10 [99]在又一示出的实施中，所述的装置 20 还包括获取单元 210 和存储单元 212，
- [100] 所述接收单元 202，接收所述新节点的网络地址、所述新节点的唯一性标识和所述新节点所作的数字签名；
- [101] 所述获取单元 210，从所述区块链的分布式数据库中获取所述节点身份表中，基于所述唯一性识别码获取所述新节点的证书；
- 15 [102] 所述验证单元 204，基于所述新节点的证书，验证所述数字签名；
- [103] 所述存储单元 212，在所述验证通过后，将所述网络地址存储至所述区块链已有节点的本地数据库。
- [104] 在又一示出的实施中，所述的装置 20 还包括：
- [105] 发送单元 214，向所述新节点发送所述区块链节点的本地数据库存储的区块链中
- 20 其他已有节点的网络地址。
- [106] 在又一示出的实施中，所述的装置 20 还包括：
- [107] 发送单元 214，向所述新节点发送所述区块链已有节点备份的所述区块链的分布式数据库中的数据。
- [108] 上述装置中各个单元或模块的功能和作用的实现过程具体详见上述方法中对应
- 25 步骤的实现过程，相关之处参见方法实施例的部分说明即可，在此不再赘述。
- [109] 以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理

模块,即可以位于一个地方,或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部单元或模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

[110] 上述实施例阐明的装置、单元、模块,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。

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

[112] 与上述方法实施例相对应,本说明书的实施例还提供了一种计算机可读存储介质,该存储介质上存储有计算机程序,这些计算机程序在被处理器运行时,执行本说明书实施例中基于区块链的节点管理方法的各个步骤。对基于区块链的节点管理方法的各个步骤的详细描述请参见之前的内容,不再重复。

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

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

[115] 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。

[116] 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。

[117] 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, 5 磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质, 可用于存储可以被计算设备访问的信息。按照本文中的界定, 计算机可读介质不包括暂存电脑可读媒体(transitory media), 如调制的数据信号和载波。

[118] 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 10 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。

[119] 本领域技术人员应明白, 本说明书的实施例可提供为方法、系统或计算机程序产品。因此, 本说明书的实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且, 本说明书的实施例可采用在一个或多个其中包含有计 15 算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。