

区块链共识方法、装置、介质、电子设备和程序产品

本申请要求于2022年06月02日提交中国专利局、申请号为202210622140.7、申请名称为“区块链共识方法、装置、介质及电子设备”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**

本申请属于区块链技术领域，具体涉及区块链共识。

背景技术

在包括多个区块链节点的区块链网络中，为了实现去中心化的可信环境，所有区块链节点一般需要执行统一的共识算法，以便在各个节点之间进行数据的一致性同步。然而，
10 统一的共识算法难以满足多样化的系统业务需求，存在灵活性差的问题。

发明内容

本申请提供一种区块链共识方法、区块链共识装置、计算机可读介质、电子设备以及计算机程序产品，目的在于提高区块链共识的灵活性。

本申请的其他特性和优点将通过下面的详细描述变得显然，或部分地通过本申请的实
15 践而习得。

根据本申请实施例的一个方面，提供一种区块链共识方法，所述方法由区块链网络中的当前区块链节点执行，该方法包括：

在所述区块链网络中广播对应于至少两个共识阶段的共识请求，所述区块链网络包括至少两种执行不同类型共识算法的区块链节点，所述不同类型共识算法包括第一共识算法
20 和第二共识算法；

分别获取所述区块链网络在各个所述共识阶段中广播的应答消息，所述应答消息是所述区块链节点对所述共识请求做出响应的消息；

统计在相同的共识阶段中发出所述应答消息的区块链节点的节点数量，所述节点数量包括至少两种执行不同类型共识算法的区块链节点的数量；
25

若所述节点数量满足所述第一共识算法的共识条件，在执行所述第一共识算法的区块链节点上达成共识，并向执行所述第二共识算法的区块链节点同步所述第一共识算法的共识结果。

根据本申请实施例的一个方面，提供一种区块链共识装置，该装置包括：

请求模块，被配置为在区块链网络中广播对应于至少两个共识阶段的共识请求，所述
30 区块链网络包括至少两种执行不同类型共识算法的区块链节点，所述不同类型共识算法包括第一共识算法和第二共识算法；

应答模块，被配置为分别获取所述区块链网络在各个所述共识阶段中广播的应答消息，所述应答消息是所述区块链节点对所述共识请求做出响应的消息；

统计模块，被配置为统计在相同的共识阶段中发出所述应答消息的区块链节点的节点
35 数量，所述节点数量包括至少两种执行不同类型共识算法的区块链节点的数量；

同步模块，被配置为若所述节点数量满足第一共识算法的共识条件，在执行所述第一共识算法的区块链节点上达成共识，并向执行所述第二共识算法的区块链节点同步所述第

一共识算法的共识结果。

根据本申请实施例的一个方面，提供一种计算机可读介质，其上存储有计算机程序，该计算机程序被处理器执行时实现如以上技术方案中的区块链共识方法。

根据本申请实施例的一个方面，提供一种电子设备，该电子设备包括：处理器；以及
5 存储器，用于存储所述处理器的可执行指令；其中，所述处理器被配置为经由执行所述可执行指令来执行如以上技术方案中的区块链共识方法。

根据本申请实施例的一个方面，提供一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现如以上技术方案中的区块链共识方法。

在本申请的一些实施例中，该计算机程序产品或计算机程序包括计算机程序，该计算机程序存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机程序，处理器执行该计算机程序，使得该计算机设备执行如以上技术方案中的区块链共识方法。
10

在本申请实施例提供的技术方案中，通过在区块链网络中配置至少两种执行不同类型共识算法的区块链节点，可以在进行节点共识的过程中，统计发出共识应答的区块链节点的节点数量，当节点数量满足其中任意一种共识算法的共识条件时，可以由满足共识条件的区块链节点向未满足共识条件的区块链节点同步共识结果，从而可以提高区块链共识的灵活性。
15

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

20 **附图说明**

图1示出了本申请实施例中的区块链系统的组成示意图；
图2示出了在区块链网络上维护的区块链的组成结构；
图3示意性地示出了应用本申请技术方案的区块链网络的网络架构；
图4示出了本申请一个实施例中区块链共识方法的步骤流程图；
25 图5示出了本申请一个实施例中应答消息的数据结构；
图6示出了本申请一个实施例中基于共识阶段统计节点数量的区块链共识方法；
图7示出了本申请一个实施例中的低容错率共识算法的共识流程；
图8示出了本申请一个实施例中的高容错率共识算法的共识流程；
图9示出了本申请实施例在执行算法切换过程中的场景示例；
30 图10示出了本申请实施例在一个应用场景中执行共识认证的方法步骤流程图；
图11示意性地示出了本申请实施例提供的区块链共识装置的结构框图；
图12示意性地示出了适于用来实现本申请实施例的电子设备的计算机系统结构框图。

具体实施方式

现在将参考附图更全面地描述示例实施方式。然而，示例实施方式能够以多种形式实施，且不应被理解为限于在此阐述的范例；相反，提供这些实施方式使得本申请将更加全面和完整，并将示例实施方式的构思全面地传达给本领域的技术人员。
35

此外，所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多实施例中。

-3-

在下面的描述中，提供许多具体细节从而给出对本申请的实施例的充分理解。然而，本领域技术人员将意识到，可以实践本申请的技术方案而没有特定细节中的一个或更多，或者可以采用其它的方法、组元、装置、步骤等。在其它情况下，不详细示出或描述公知方法、装置、实现或者操作以避免模糊本申请的各方面。

5 附图中所示的方框图仅仅是功能实体，不一定必须与物理上独立的实体相对应。即，可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

10 附图中所示的流程图仅是示例性说明，不是必须包括所有的内容和操作/步骤，也不是必须按所描述的顺序执行。例如，有的操作/步骤还可以分解，而有的操作/步骤可以合并或部分合并，因此实际执行的顺序有可能根据实际情况改变。

在本申请的具体实施方式中，涉及到用户应用区块链产品时产生的请求、应答等相关数据，当本申请的各个实施例运用到具体产品或技术中时，需要获得用户许可或者同意，且相关数据的收集、使用和处理需要遵守相关国家和地区的相关法律法规和标准。

15 区块链是一种在对等网络环境下，通过透明和可信规则构建的防伪造、防篡改和可追溯的共享的具有块链式数据结构（chained-block data structure）的数字化账本。块链式数据结构是将一段时间内发生的事务处理以区块为单位进行存储，并以密码学算法将区块按时间顺序连接成链条的一种数据结构。账本分发给网络中的所有成员节点，在通过哈希密码算法链接的区块的顺序链中，永久记录网络中的对等节点之间发生的资产交易的历史记录。所有经过确认和证明的交易都从链的开头一直链接到最新的区块，因此得名区块链。区块链可以充当单一事实来源，而且区块链网络中的成员只能查看与他们相关的交易。

20 图1示出了本申请实施例中的区块链系统的组成示意图，区块链系统100可以包括至少一个客户端110和区块链网络120，区块链网络120包括至少一个区块链节点121。客户端110可以是智能手机、平板电脑、笔记本电脑、台式电脑、智能穿戴设备、智能车载设备、智能支付终端、面部识别终端等各种电子设备，通过安装相应的客户端应用程序，可以向用户提供区块链数据服务。区块链节点121可以是终端设备或者服务器，例如区块链节点121可以是独立的物理服务器，也可以是多个物理服务器构成的服务器集群，还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、CDN、以及大数据和人工智能平台等基础云计算服务的云服务器。

30 在区块链网络120中，每个区块链节点121在进行正常工作时可以接收到输入信息，并基于接收到的输入信息维护区块链网络内的共享数据。为了保证信息互通，各个区块链节点121之间可以存在信息连接，各个区块链节点121相互可以通过信息连接进行信息传输。例如，当区块链网络120中的任意区块链节点121接收到输入信息，并将输入信息在区块链网络120中进行广播时，区块链网络120中的其他节点设备可以根据共识算法获取该输入信息，将该输入信息作为共享数据进行存储。

35 对于区块链网络120中的每个区块链节点121，均具有与其对应的节点标识，而且区块链网络120中的每个区块链节点121均可以存储同一区块链网络中的其他区块链节点的节点标识，以便后续根据其他区块链节点的节点标识，将生成的区块广播至区块链网络120中的

其他节点。区块链节点121中可维护一个如表1所示的节点标识列表，将节点名称和节点标识对应存储至该节点标识列表中。其中，节点标识可为IP（Internet Protocol，网络之间互联的协议）地址以及其他任一种能够用于标识该节点的信息，表1是以IP地址为例的节点标识列表。

5

表1

节点名称	节点标识
节点1	117.114.151.174
节点2	117.116.189.145
...	...
节点N	119.123.145.223

图2示出了在区块链网络上维护的区块链的组成结构。如图2所示，区块链由多个顺次连接的区块组成，每当有新的数据需要写入区块链时，这些数据会汇总到一个新生成的区块中，新生成的区块将被链接至区块链的末端，通过共识算法可以保证每个节点设备121上新增的区块是完全相同的。在每个区块的区块体中记录了当前区块的数据，同时在其区块头中保存与之相连的前一区块的哈希值（Hash），若前一区块中的交易数据发生变化，那么当前区块的哈希值也将随之改变。因此，上传至区块链网络中的数据难以被篡改，可以提高共享数据的可靠性。

10

图3示意性地示出了应用本申请技术方案的区块链网络的网络架构。如图3所示，在实现网络交易和网络支付的应用场景中，位于区块链网络中的交易主体节点310、交易平台节点320以及资源分配节点330共同维护一条或者多条区块链340。

15

交易主体节点310是为用户提供交易服务的区块链节点，例如可以是与用户进行网络交易的商户或者个人卖家。

交易平台节点320是为网络交易提供交易场景的区块链节点，例如可以是电商网站、网络商城或者提供网络交易服务的各种业务平台。

20

资源分配节点330是为网络交易提供资金管理和分配服务的区块链节点，例如可以是第三方支付机构。

当用户与交易主体节点310进行网络交易时，可以通过在资源分配节点330上开通的账户向交易主体节点310支付交易资金，交易平台节点320作为交易场景的提供方，需要从该交易资金中抽取一定数额的资金作为平台服务费用。为实现在交易主体节点310和交易平台节点320之间进行可信的资金分配，可以基于区块链网络订立相应的用于进行资金分配的智能合约（如分账合同），当产生网络交易时，资源分配节点330可以按照该智能合约向交易场景中的各个对象进行资金分配，各个区块链节点上进行网络交易产生的交易数据均可以通过区块链340进行上链保存，去中心化的数据保存可以有效避免信任危机。

25

由于节点宕机、网络故障、软件错误、恶意节点等错误，可能造成各个区块链节点间保存的数据不一致的问题。共识算法定义了一套节点间网络交互的分布式算法，保证了在出现上述错误的系统环境中，仍然可以保证各个区块链节点间数据的一致性。在本申请的相关技术中，一个区块链网络中的所有区块链节点均需要采用统一的共识算法进行共识认

30

证，以便保证共识过程和共识结果的一致性。然而，在实际的区块链业务处理过程中，使用区块链服务的上层业务系统会随着用户需求的不断变更，在性能、可用性、容错性、扩展性等方面有着不同的诉求。而目前的区块链网络由于采用的都是单一的共识算法，无法匹配上层业务系统的要求。如果需要在区块链网络上变更区块链节点的共识算法，则必须控制整体区块链网络停止服务，等待完成对全部区块链节点的算法变更后，再重新启用配置有新的共识算法的区块链网络。这种共识算法的切换方式容易导致长时间、高频次的服务中断，不仅存在共识算法切换效率低下的问题，而且严重影响区块链网络的服务连续性和稳定可靠性。

针对相关技术中存在的以上技术问题，本申请提供一种能够对多种不同类型的共识算法之间在线灵活切换的方案，可以使区块链系统在不停止服务的情况下，实时变更共识算法以满足业务系统的要求。

下面结合具体实施方式对本申请提供的区块链共识方法、区块链共识装置、计算机可读介质、电子设备以及计算机程序产品等技术方案做出详细说明。

图4示出了本申请一个实施例中区块链共识方法的步骤流程图，该区块链共识方法可以由图1所示的客户端或者区块链节点执行，为了便于说明，以区块链网络中的任意一个区块链节点作为当前区块链节点，将当前区块链节点作为执行本申请实施例的执行主体，该当前区块链节点可以设置有图1所示的客户端，即本申请实施例以当前区块链节点上执行的区块链共识方法作为示例进行说明。如图4所示，本申请实施例中的区块链共识方法包括如下的S410至S440。

S410：在区块链网络中广播对应于至少两个共识阶段的共识请求，区块链网络包括至少两种执行不同类型共识算法的区块链节点。

本申请实施例中的区块链网络可以包括公有链(Public Block Chain)、私有链(Private Block Chain)或者联盟链(Consortium Block Chain)中的任意一种。其中，去中心化程度最高的是公有链。加入公有链的节点/参与者都可以读取链上的数据、发布交易以及竞争新区块的记账权等；而且，各节点/参与者可自由加入以及退出公有链。私有链则相反，私有链的记账权限由某个组织或者机构控制，数据读取权限也受该组织或机构的控制，参与者少且不能随意加入到私有链，需经过组织或者机构的审核。联盟链也称为共同体区块链，是指其共识过程受到预选节点控制的区块链，是公有链和私有链的混合，可实现“部分去中心化”。链上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。通过联盟链，新来的参与者可以加入已形成的区块链并共享数据，而不必从头开始构建它。不论是公有链、私有链还是联盟链，都可能提供智能合约的功能。区块链上的智能合约是在区块链系统上可以被交易触发执行的合约。智能合约可以通过代码的形式定义。

智能合约(Smart contract)：也称为链码(Chaincode)或应用代码，是一种旨在以信息化方式传播、验证或执行合同的计算机协议，部署在区块链网络的节点中的程序，承载了执行交易的业务逻辑，运行在隔离运行环境中(例如容器或虚拟机)。区块链系统中的各个节点根据特定条件自动执行的合约程序，可以对链上存储的数据进行操作，是业务主体与区块链

进行交互、利用区块链实现业务逻辑的重要途径。智能合约的目的是提供优于传统合约的安全方法，并减少与合约相关的其他交易成本，它允许在没有第三方的情况下进行可信交易，这些交易可追溯且不可逆转。

基于智能合约生成的交易数据需要通过共识算法在不同的区块链节点之间进行共识认证，从而保证每个区块链节点上可以保存一致的交易数据。在本申请的一个实施例中，当用户通过运行区块链系统的客户端进行网络交易并产生交易数据后，可以由客户端向与之通信的区块链节点发送共识请求，接收到共识请求的区块链节点可以在区块链网络上对其进行广播发送，使得共识请求能够被传输至区块链网络中的所有区块链节点。

在本申请实施例中，区块链网络上可以同时运行至少两种不同类型的共识算法，例如区块链网络中的一部分区块链节点执行第一共识算法，另外一部分区块链节点执行不同于第一共识算法的第二共识算法。第一共识算法与第二共识算法可以具有相同的共识条件，或者可以具有不同的共识条件。第一共识算法和第二共识算法可以具有相同数量的共识阶段或者具有不同数量的共识阶段。

在本申请的一个实施例中，可以从区块链网络中选取一个或者多个区块链节点作为处理共识请求的主节点，区块链网络中除主节点以外的其他区块链节点作为从节点。当客户端产生共识请求时，可以首先将共识请求发送至主节点，由主节点再将共识请求分发至各个从节点。主节点可以通过投票选举、轮流指定或者随机选取等方式产生。

S420: 分别获取区块链网络在各个共识阶段中广播的应答消息，应答消息是区块链节点对共识请求做出响应的消息。

当区块链网络中的区块链节点接收到共识请求后，可以对共识请求做出响应，生成应答消息并在区块链网络上广播应答消息。

在本申请的一个实施例中，区块链节点可以对接收到的共识请求进行共识验证，并在验证通过后向区块链网络上广播发送应答消息。区块链节点对共识请求的共识验证可以包括签名验证和数据验证两个方面。其中，签名验证用于验证共识请求的来源可靠性，数据验证用于验证共识请求的内容真实性。

在本申请的一个实施例中，区块链网络中广播的共识请求携带有发出共识请求的区块链节点的数字签名，区块链网络中广播的应答消息同样也携带有发出应答消息的区块链节点的数字签名。区块链网络中的各个区块链节点可以持有组成非对称密钥对的公钥和私钥，在对共识请求或者应答消息进行数字签名时，可以先通过摘要提取算法对数据内容提取内容摘要，然后再使用私钥对内容摘要进行加密处理形成数字签名，该数字签名可以通过公钥进行验证。

内容摘要是与一项数据内容唯一对应的具有固定长度的字符串，它由一个单向哈希加密函数对数据内容进行作用而产生。如果数据内容在网络传输过程中被篡改，则通过对数据内容在传输前后的内容摘要进行比较，就可以判别数据内容是否发生改变。因此，基于内容摘要能够验证数据内容的完整性。内容摘要采用单向哈希函数将待传输的数据内容明文映射成为一串密文，这一串密文亦称为数字指纹。内容摘要有固定的长度，且不同的明文摘要成密文，其结果总是不同的，而同样的明文其摘要必定一致。本申请实施例中的摘

要提取算法例如可以包括MD(Message Digest, 消息摘要算法)、SHA(Secure Hash Algorithm, 安全散列算法)、MAC(Message Authentication Code, 消息认证码算法)等算法。

数字签名是一个带有密钥的消息摘要算法, 这个密钥包括了公钥和私钥, 用于验证数据完整性、认证数据来源和抗否认, 遵循OSI参考模型、私钥签名和公钥验证。也是非对称加密算法和消息摘要算法的结合体, 常见的数字签名算法主要有RSA、DSA、ECDSA三种。

5 基于RSA算法可以先生成一对RSA密钥, 其中之一是保密密钥, 由业务主体保存; 另一个为公开密钥, 可对外公开, 甚至可在网络服务器中注册。为提高保密强度, RSA密钥至少为500位长, 一般推荐使用1024位。这就使加密的计算量很大。为减少计算量, 在传送信息时, 常采用传统加密方法与公开密钥加密方法相结合的方式, 即信息采用改进的DES
10 或IDEA对话密钥加密, 然后使用RSA密钥加密对话密钥和信息摘要。对方收到信息后, 用不同的密钥解密并可核对信息摘要。

DSA(Digital Signature Algorithm, 数字签名算法)的一个重要特点是两个素数公开。如此一来, 当使用其他主体的 p 和 q 时, 即使不知道私钥, 也能够确认它们是否是随机产生的, 或者是经过伪造或修改而产生的。

15 ECDSA(Elliptic Curve Digital Signature Algorithm, 椭圆曲线数字签名算法), 是ECC(Elliptic Curves Cryptography, 椭圆曲线密码编码学)与DSA的结合, 整个签名过程与DSA类似, 不一样的是签名中采取的算法为ECC, 最后签名出来的值也是分为 r 和 s 两项参数。

在本申请的一个实施例中, 在完成对共识请求的签名验证后, 可以对共识请求中携带的数据内容进行数据验证。数据验证的方法例如可以包括将共识请求中携带的数据内容与
20 当前区块链节点本地缓存的数据内容进行一致性校验。若验证通过, 则表明发出共识请求的区块链节点与当前区块链节点缓存有相同的数据内容, 且该项数据内容在网络传输过程中未被修改。

S430: 统计在相同的共识阶段中发出应答消息的区块链节点的节点数量, 节点数量包括至少两种执行不同类型共识算法的区块链节点的数量。

25 当区块链节点接收到区块链网络中广播发送的应答消息后, 可以通过解析应答消息确定每个应答消息的消息来源, 对具有不同消息来源的应答消息进行统计, 可以得到发出应答消息的区块链节点的节点数量。该节点数量表示区块链网络中对共识请求做出响应的执行不同类型共识算法的区块链节点的数量。

在本申请的一个实施例中, 每个区块链节点均可以接收并统计来自其他区块链节点发出的应答消息。例如, 区块链网络中包括有 n 个区块链节点, 则每个区块链节点最多可以接收到由其他区块链节点发出的 $n-1$ 个应答消息。与此同时, 每个区块链节点自身也会对外发送应答消息。因此, 一个区块链节点统计到发出应答消息的区块链节点的节点数量最大为
30 区块链网络中的区块链节点的总数量。由每个区块链节点分别进行消息来源统计, 可以提高共识过程的可信度。

35 在本申请的一个实施例中, 可以由区块链网络中的一个或者多个主节点对应答消息进行来源统计, 而其他从节点则无需进行数量统计。例如在一次共识过程中, 通过投票选举、轮流指定或者随机选取等方式产生主节点, 主节点在向区块链网络中发送共识请求后, 可

以监测区块链网络中从节点返回的应答消息，并统计发出应答消息的从节点的节点数量。通过主节点进行消息来源统计的好处在于，可以降低其他从节点的计算成本，避免产生多余的数据开销。

在本申请的一个实施例中，为了提高共识效率，可以在预设的时间范围内统计发出应答消息的区块链节点的节点数量。如果在超出时间范围之外接收到新的应答消息，则可以将其丢弃而不再统计。

在本申请的一个实施例中，统计节点数量的时间范围可以是根据当前区块链节点收到共识请求的第一时间点作为范围起始点的具有指定时间长度的固定时间窗口，也可以是根据当前区块链节点发出应答消息的第二时间点作为范围起始点的具有指定时间长度的固定时间窗口。

在本申请的一个实施例中，统计节点数量的时间范围可以是根据最近一次接收到应答消息的第三时间点以及预设的时间长度确定范围结束点的具有变化长度的动态时间窗口。例如，一个区块链节点最近一次接收到应答消息为时间点A，基于时间长度B，可以确定时间范围的范围结束点为A+B。若在时间点A至A+B之间，区块链节点未接收到新的应答消息，则可以停止进行应答消息的来源统计。若在时间点A至A+B之间，区块链节点又接收到新的应答消息，例如在时间点C接收到新的应答消息，则可以将时间范围的范围结束点更新为C+B。以此类推，直至区块链节点长时间未接收到新的应答消息，便可以停止进行应答消息的来源统计。

在本申请的一个实施例中，对应答消息进行来源统计的时间范围可以是具有静态起始点和动态结束点的时间范围，例如以接收到共识请求、发出应答消息或者第一次接收到应答消息中的任意一个时间点作为静态起始点，以最近一次接收到新的应答消息和预设的时间长度确定动态结束点。利用动态变化的时间范围进行消息来源统计，能够在提高统计效率的同时确保数据统计的准确性，避免因时间范围过长而影响共识进度，同时也避免因时间范围过短而导致的数据统计不全面的问题。

S440：若节点数量满足第一共识算法的共识条件，在执行第一共识算法的区块链节点上达成共识，并向执行第二共识算法的区块链节点同步第一共识算法的共识结果，第一共识算法和第二共识算法是不同类型的共识算法。

共识算法的共识条件是用于确定能否获得共识结果的判断条件，例如一个共识算法的共识条件可以是统计发出应答消息的区块链节点的节点数量超过区块链节点总数量的预设比例。在区块链网络中配置的不同类型的共识算法，可以具有相同的共识条件，也可以具有不同的共识条件。

在本申请的一个实施例中，区块链网络中的区块链节点可以根据自身执行的共识算法，对统计得到的节点数量是否满足共识条件作出判断。例如，若当前区块链节点执行的共识算法为第一共识算法，则可以根据统计得到的节点数量判断是否满足第一共识算法的共识条件；若当前区块链节点执行的共识算法为第二共识算法，则可以根据统计得到的节点数量判断是否满足第二共识算法的共识条件。

在本申请的一个实施例中，区块链网络中的一部分区块链节点执行第一共识算法，另

一部分区块链节点执行第二共识算法；其中，第一共识算法的共识条件是统计发出应答消息的区块链节点的节点数量占区块链节点总数量的比例超过第一比例阈值，第二共识算法的共识条件是统计发出应答消息的区块链节点的节点数量占区块链节点总数量的比例超过第二比例阈值，第二比例阈值大于第一比例阈值。若统计得到的节点数量与区块链节点总数的比值大于第一比例阈值，但小于第二比例阈值，则可以确定该节点数量满足第一共识算法的共识条件，但不满足第二共识算法的共识条件。在此基础上，执行第一共识算法的区块链节点能够获得共识成功的共识结果，执行第二共识算法的区块链节点虽然未能共识成功，但可以通过执行第一共识算法的区块链节点向执行第二共识算法的区块链节点进行数据同步，使得执行第二共识算法的区块链节点也能完成共识。

10 在本申请实施例提供的区块链共识方法中，通过在区块链网络中配置至少两种执行不同类型共识算法的区块链节点，可以在进行节点共识的过程中，统计发出共识应答消息的区块链节点的节点数量，当节点数量满足其中任意一种共识算法的共识条件时，可以由满足共识条件的区块链节点向未满足共识条件的区块链节点同步共识结果，从而可以提高区块链共识的灵活性。

15 在本申请的一个实施例中，不同类型的共识算法具有不同数量的共识阶段，应答消息中携带区块链节点的算法类型和节点签名，算法类型用于指示区块链节点执行的共识算法，节点签名包括区块链节点在各个共识阶段的数字签名。

图5示出了本申请一个实施例中应答消息的数据结构。如图5所示，基于某一种共识算法生成的应答消息可以包括类型字段501、签名字段502以及数据字段503。

20 类型字段501用于指示发出应答消息的区块链节点所执行的共识算法的算法类型，例如可以包括CFT类共识算法或者BFT类共识算法。

CFT类共识算法，即故障容错算法（Crash Fault Tolerance algorithm, CFT），指的是面对故障类错误时，可以保证节点数据一致性的一类共识算法。故障类错误包括节点宕机、网络错误等良性错误。

25 BFT类共识算法，即拜占庭容错算法（Byzantine Fault Tolerance algorithm, BFT），指的是面对拜占庭类错误时，可以保证节点数据一致性的一类共识算法。拜占庭类错误包括了上述故障类错误，以及软件错误、恶意节点等恶性错误。

签名字段502用于保存发出应答消息的区块链节点在各个共识阶段的数字签名，例如可以包括预准备阶段签名、准备阶段签名和提交阶段签名。

30 执行CFT类共识算法的区块链节点在生成应答消息时，可以使用数据结构中的预准备阶段签名和提交阶段签名；执行BFT类共识算法的区块链节点在生成应答消息时，可以使用全部三个阶段的签名。

在本申请的一个实施例中，一个阶段的应答消息携带了在其之前所有阶段的数字签名。例如，第一阶段的应答消息中携带第一阶段的数字签名，第二阶段的应答消息中同时携带第一阶段和第二阶段的数字签名，第三阶段的应答消息中同时携带第一、第二、第三阶段的数字签名。

数据字段503用于保存请求共识认证的数据，例如可以是网络交易的交易数据。

本申请实施例提供的应答消息数据结构，可以同时适用于多种不同类型的共识算法，使得具有不同数量共识阶段的共识算法能够通过相同的应答消息进行共识认证，提高了区块链网络对于不同共识算法的匹配多样性。

5 对于具有不同数量的共识阶段的共识算法，由于区块链网络中的各个区块链节点在计算能力和网络传输速度方面存在一定差异，在进行共识认证的过程中，每个区块链节点所处的共识阶段也可能不同。因此，当前一个区块链节点接收到其他区块链节点发出的应答消息时，需要根据应答消息识别对应的共识阶段，从而有效统计处于不同共识阶段的区块链节点的节点数量。图6示出了本申请一个实施例中基于共识阶段统计节点数量的区块链共识方法。如图6所示，该方法包括如下的S610至S670。

10 S610：在区块链网络中广播对应于至少两个共识阶段的共识请求，区块链网络包括至少两种执行不同类型共识算法的区块链节点。

在本申请实施例中，区块链网络上可以同时运行至少两种不同类型的共识算法，例如区块链网络中的一部分区块链节点执行第一共识算法，另外一部分区块链节点执行不同于第一共识算法的第二共识算法。第一共识算法与第二共识算法可以具有相同的共识条件，
15 或者可以具有不同的共识条件。

在本申请的一个实施例中，可以从区块链网络中选取一个或者多个区块链节点作为处理共识请求的主节点，区块链网络中除主节点以外的其他区块链节点作为从节点。当客户端产生共识请求时，可以首先将共识请求发送至主节点，由主节点再将共识请求分发至各个从节点。主节点可以通过投票选举、轮流指定或者随机选取等方式产生。

20 S620：分别获取区块链网络在各个共识阶段中广播的应答消息，应答消息是区块链节点对共识请求做出响应的消息。

当区块链网络中的区块链节点接收到共识请求后，可以对共识请求做出响应，生成应答消息并在区块链网络上广播应答消息。

在本申请的一个实施例中，区块链节点可以对接收到的共识请求进行共识验证，并在验证通过后向区块链网络上广播发送应答消息。区块链节点对共识请求的共识验证可以包括签名验证和数据验证两个方面。其中，签名验证用于验证共识请求的来源可靠性，数据验证用于验证共识请求的内容真实性。

在本申请的一个实施例中，区块链网络中广播的共识请求携带有发出共识请求的区块链节点的数字签名，区块链网络中广播的应答消息同样也携带有发出应答消息的区块链节点的数字签名。区块链网络中的各个区块链节点可以持有组成非对称密钥对的公钥和私钥，在对共识请求或者应答消息进行数字签名时，可以先通过摘要提取算法对数据内容提取内容摘要，然后再使用私钥对内容摘要进行加密处理形成数字签名，该数字签名可以通过公钥进行验证。

在本申请的一个实施例中，在完成对共识请求的签名验证后，可以对共识请求中携带的数据内容进行数据验证。数据验证的方法例如可以包括将共识请求中携带的数据内容与当前区块链节点本地缓存的数据内容进行一致性校验。若验证通过，则表明发出共识请求的区块链节点与当前区块链节点缓存有相同的数据内容，且该项数据内容在网络传输过程

中未被修改。

S630: 解析应答消息, 得到应答消息中携带的算法类型和节点签名。

应答消息中携带区块链节点的算法类型和节点签名, 算法类型用于指示区块链节点执行的共识算法, 节点签名包括区块链节点在各个共识阶段的数字签名。

- 5 通过解析应答消息可以得到如图6所示的数据结构, 根据其中的类型字段可以得到算法类型, 根据其中的签名字段可以得到与各个共识阶段相对应的节点签名。

S640: 根据算法类型识别消息发送节点执行的共识算法, 消息发送节点为发出应答消息的区块链节点。

- 10 对于区块链网络中的每个区块链节点, 均具有与其对应的节点标识, 而且区块链网络中的每个区块链节点均可以存储有区块链网络中其他区块链节点的节点标识, 以便后续根据其他区块链节点的节点标识, 将生成的共识请求、应答消息、待上链的区块等数据广播至区块链网络中的其他区块链节点。每个区块链节点中可维护一个节点标识列表, 将节点名称和节点标识对应存储至该节点标识列表中。其中, 节点标识可为IP (Internet Protocol, 网络之间互联的协议) 地址以及其他任一种能够用于标识该区块链节点的信息。

- 15 当一个区块链节点向区块链网络中广播发送应答消息时, 可以向应答消息中封装自身的节点标识。在当前区块链节点接收到区块链网络上广播的应答消息时, 可以根据应答消息中解析得到的节点标识确定发出该应答消息的消息发送节点。根据应答消息中解析得到的算法类型可以确定消息发送节点执行的共识算法。

S650: 根据节点签名识别消息发送节点所处的共识阶段。

- 20 通过解析应答消息, 可以读取其签名字段得到与各个共识阶段相对应的节点签名。由于各个区块链节点在共识进度上可能存在差异, 区块链网络上广播的应答消息也可能携带对应不同共识阶段的节点签名。例如, 某一区块链节点处于预准备阶段, 则由其发出的应答消息中将携带预准备阶段的节点签名; 又例如, 某一区块链节点已完成预准备阶段的共识认证, 当前处于准备阶段, 则由其发出的应答消息中将携带预准备阶段和准备阶段两部分
- 25 的节点签名。

在本申请的一个实施例中, 通过解析应答消息, 可以筛选其中存在节点签名的一个或者多个共识阶段。根据各个共识阶段的执行顺序, 可以确定消息发送节点当前所处的共识阶段。

- 30 若签名字段中仅有一个共识阶段存在节点签名, 则可以确定消息发送节点处于该共识阶段。例如, 一个应答消息的签名字段仅有预准备阶段存在节点签名, 其他共识阶段对应的签名字段为空值, 则可以确定发出该应答消息的消息发送节点当前处于预准备阶段。

- 若签名字段中具有至少两个共识阶段存在节点签名, 则可以根据至少两个共识阶段的执行顺序, 将执行顺序在后的共识阶段确定为消息发送节点当前所处的共识阶段。例如, 一个应答消息的签名字段在预准备阶段和准备阶段均存在节点签名, 其他共识阶段对应的
- 35 签名字段为空值; 由于共识算法中的准备阶段在预准备阶段之后执行, 可以确定该应答消息的消息发送节点当前处于准备阶段。

S660: 根据消息发送节点执行的共识算法以及消息发送节点所处的共识阶段, 统计与

当前区块链节点处于相同共识阶段的消息发送节点的节点数量。

根据消息发送节点执行的共识算法，可以消息发送节点与当前区块链节点是否执行相同类型的共识算法。如果消息发送节点与当前区块链节点执行相同类型的共识算法，则可以直接根据消息发送节点所处的共识阶段确定消息发送节点与当前区块链节点是否处于相同的共识阶段。如果消息发送节点与当前区块链节点执行不同类型的共识算法，则需要根据预先配置的匹配关系确定消息发送节点所处的共识阶段是否与当前区块链节点相同。

在统计与当前区块链节点处于相同共识阶段的消息发送节点的节点数量之前，当前区块链节点可以先获取不同类型共识算法之间的共识阶段的匹配关系。若消息发送节点与当前区块链节点执行不同类型的共识算法，则根据匹配关系确定与当前区块链节点处于相同共识阶段的消息发送节点。

任意两种不同类型的共识算法，均可以根据匹配关系确定各个区块链节点是否处于相同的共识阶段。例如，消息发送节点执行第一共识算法和第二共识算法中的一个，当前区块链节点执行第一共识算法和第二共识算法中的另一个。其中，第一共识算法包括N个共识阶段，第二共识算法包括M个共识阶段；不同类型共识算法之间的共识阶段的匹配关系包括：第一共识算法与第二共识算法的前P个共识阶段相互匹配，P为N-1和M-1中的较小值；第一共识算法的后N-P个共识阶段与第二共识算法的后M-P个共识阶段相互匹配。

举例而言，第一共识算法为CFT类共识算法，其包括两个共识阶段，即准备阶段和提交阶段；第二共识算法为BFT类共识算法，其包括三个共识阶段，即预准备阶段、准备阶段和提交阶段。

基于以上匹配关系可知，第一共识算法的前一个共识阶段与第二共识算法的前一个共识阶段相互匹配；即，CFT类共识算法的准备阶段与BFT类共识算法的预准备阶段相互匹配。第二共识算法的后一个共识阶段与第二共识算法的后两个共识阶段相互匹配；即CFT类共识算法的提交阶段与BFT类共识算法的准备阶段和提交阶段相互匹配。

在此基础上，若一个区块链节点处于CFT类共识算法的准备阶段，且另一个区块链节点处于BFT类共识算法的预准备阶段，则可以确定二者处于相同的共识阶段；同理，若一个区块链节点处于CFT类共识算法的提交阶段，且另一个区块链节点处于BFT类共识算法的准备阶段或者提交阶段，则可以确定二者处于相同的共识阶段。

在本申请的一个实施例，在统计与当前区块链节点处于相同共识阶段的消息发送节点的节点数量之后，当前区块链节点可以根据自身所处的共识阶段确定后续的执行动作。若当前区块链节点所处的共识阶段是所执行共识算法的最后一个共识阶段，则根据节点数量是否满足该共识算法的共识条件，确定该共识算法的共识结果；若当前区块链节点所处的共识阶段不是所执行共识算法的最后一个共识阶段，则根据节点数量是否满足该共识算法的共识条件，确定是否执行该共识算法的下一个共识阶段。

例如，当前区块链节点所处的共识阶段为CFT类共识算法的准备阶段，经过统计与其处于相同共识阶段（包括CFT类共识算法的准备阶段或者BFT类共识算法的预准备阶段）的区块链节点的节点数量，可以判断该节点数量是否满足CFT类共识算法的共识条件。如果满足CFT类共识算法的共识条件，则可以进入提交阶段；如果不满足CFT类共识算法的共识

条件,则需要继续等待接收其他区块链节点发出的应答消息,并实时更新统计的节点数量。

在本申请的一个实施例中,每个区块链节点均可以接收并统计来自其他区块链节点发出的应答消息。例如,区块链网络中包括有 n 个区块链节点,则每个区块链节点最多可以接收到由其他区块链节点发出的 $n-1$ 个应答消息。与此同时,每个区块链节点自身也会对外发

5 送应答消息。因此,一个区块链节点统计到发出应答消息的区块链节点的节点数量最大为区块链网络中的区块链节点的总数量。由每个区块链节点分别进行消息来源统计,可以提高共识过程的可信度。

在本申请的一个实施例中,可以由区块链网络中的一个或者多个主节点对应答消息进行来源统计,而其他从节点则无需进行数量统计。例如在一次共识过程中,通过投票选举、

10 轮流指定或者随机选取等方式产生主节点,主节点在向区块链网络中发送共识请求后,可以监测区块链网络中从节点返回的应答消息,并统计发出应答消息的从节点的节点数量。通过主节点进行消息来源统计的好处在于,可以降低其他从节点的计算成本,避免产生多余的数据开销。

在本申请的一个实施例中,为了提高共识效率,可以在预设的时间范围内统计发出应答消息的区块链节点的节点数量。如果在超出时间范围之外接收到新的应答消息,则可以将其丢弃而不再统计。

15

在本申请的一个实施例中,统计节点数量的时间范围可以是根据当前区块链节点收到共识请求的第一时间点作为范围起始点的具有指定时间长度的固定时间窗口,也可以是根据当前区块链节点发出应答消息的第二时间点作为范围起始点的具有指定时间长度的固定

20 时间窗口。

在本申请的一个实施例中,统计节点数量的时间范围可以是根据最近一次接收到应答消息的第三时间点以及预设的时间长度确定范围结束点的具有变化长度的动态时间窗口。例如,一个区块链节点最近一次接收到应答消息为时间点 A ,基于时间长度 B ,可以确定时间范围的范围结束点为 $A+B$ 。若在时间点 A 至 $A+B$ 之间,区块链节点未接收到新的应答消息,

25 则可以停止进行应答消息的来源统计。若在时间点 A 至 $A+B$ 之间,区块链节点又接收到新的应答消息,例如在时间点 C 接收到新的应答消息,则可以将时间范围的范围结束点更新为 $C+B$ 。以此类推,直至区块链节点长时间未接收到新的应答消息,便可以停止进行应答消息的来源统计。

在本申请的一个实施例中,对应答消息进行来源统计的时间范围可以是具有静态起始点和动态结束点的时间范围,例如以接收到共识请求、发出应答消息或者第一次接收到应答消息中的任意一个时间点作为静态起始点,以最近一次接收到新的应答消息和预设的时间长度确定动态结束点。利用动态变化的时间范围进行消息来源统计,能够在提高统计效率的同时确保数据统计的准确性,避免因时间范围过长而影响共识进度,同时也避免因时间范围过短而导致的数据统计不全面的问题。

30

S670: 若节点数量满足第一共识算法的共识条件,在执行所述第一共识算法的区块链节点上达成共识,并向执行第二共识算法的区块链节点同步第一共识算法的共识结果,第一共识算法和第二共识算法是不同类型的共识算法。

35

共识算法的共识条件是用于确定能否获得共识结果的判断条件，例如一个共识算法的共识条件可以是统计得到发出应答消息的区块链节点的节点数量超过区块链节点总数的预设比例。在区块链网络中配置的不同类型的共识算法，可以具有相同的共识条件，也可以具有不同的共识条件。

- 5 在本申请的一个实施例中，区块链网络中的区块链节点可以根据自身执行的共识算法，对统计得到的节点数量是否满足共识条件作出判断。例如，若当前区块链节点执行的共识算法为第一共识算法，则可以根据统计得到的节点数量判断是否满足第一共识算法的共识条件；若当前区块链节点执行的共识算法为第二共识算法，则可以根据统计得到的节点数量判断是否满足第二共识算法的共识条件。
- 10 在本申请的一个实施例中，区块链网络中的一部分区块链节点执行第一共识算法，另一部分区块链节点执行第二共识算法；其中，第一共识算法的共识条件是统计得到发出应答消息的区块链节点的节点数量占区块链节点总数的比例超过第一比例阈值，第二共识算法的共识条件是统计得到发出应答消息的区块链节点的节点数量占区块链节点总数的比例超过第二比例阈值，第二比例阈值大于第一比例阈值。若统计得到的节点数量与区块链节点总数的比值大于第一比例阈值，但小于第二比例阈值，则可以确定该节点数量满足第一共识算法的共识条件，但不满足第二共识算法的共识条件。在此基础上，执行第一共识算法的区块链节点能够获得共识成功的共识结果，执行第二共识算法的区块链节点虽然未能共识成功，但可以通过执行第一共识算法的区块链节点向执行第二共识算法的区块链节点进行数据同步，使得执行第二共识算法的区块链节点也能完成共识。
- 15 在本申请的一个实施例中，第一共识算法为低容错率共识算法和高容错率共识算法中的一种，第二共识算法为低容错率共识算法和高容错率共识算法中与第一共识算法不同的另一种。低容错率共识算法的共识条件为发出应答消息的区块链节点与所有区块链节点的数量比例大于第一比例阈值，高容错率共识算法的共识条件为发出应答消息的区块链节点与所有区块链节点的数量比例大于第二比例阈值，第一比例阈值小于第二比例阈值。第一比例阈值和第二比例阈值均为大于0且小于1的常数。例如，第一比例阈值为1/2，第二比例阈值为2/3。
- 20 若发出应答消息的区块链节点与所有区块链节点的数量比例小于1/2，则节点数量既不满足低容错率共识算法的共识条件也不满足高容错率共识算法的共识条件，执行两种共识算法的所有区块链节点均无法完成共识认证。
- 25 若发出应答消息的区块链节点与所有区块链节点的数量比例大于1/2且小于2/3，则节点数量满足低容错率共识算法的共识条件但不满足高容错率共识算法的共识条件，执行低容错率共识算法的区块链节点能够完成共识认证，而执行高容错率共识算法的区块链节点无法完成共识认证。在此基础上，执行低容错率共识算法的区块链节点可以向执行高容错率共识算法的区块链节点同步共识结果，从而能够使区块链网络中的所有区块链节点均完成共识认证。
- 30 若发出应答消息的区块链节点与所有区块链节点的数量比例大于2/3，则节点数量既满足低容错率共识算法的共识条件也满足高容错率共识算法的共识条件，执行两种共识算法
- 35

的所有区块链节点均可以完成共识认证。

在本申请的一个实施例中，低容错率共识算法具有第一数量的共识阶段，高容错率共识算法具有第二数量的共识阶段，第一数量小于第二数量。通过增加共识阶段的数量可以提高共识算法的容错率。

- 5 在本申请的一个实施例中，低容错率共识算法的共识阶段包括依次执行的准备阶段和提交阶段，高容错率共识算法的共识阶段包括依次执行的预准备阶段、准备阶段和提交阶段，低容错率共识算法的准备阶段与高容错率共识算法的预准备阶段相匹配，低容错率共识算法的提交阶段与高容错率共识算法的准备阶段和提交阶段相匹配。

- 10 图7示出了本申请一个实施例中的低容错率共识算法的共识流程，低容错率共识算法例如可以是CFT类共识算法中的Paxos算法。本申请实施例中的低容错率共识算法基于两阶段的节点间交互，其优点是节点间交互较为简单，因此实现更为容易，性能较高。

如图7所示，基于低容错率共识算法进行共识认证的流程可以包括如下步骤。

S701：客户端发送共识请求到主节点。共识请求例如可以是向区块链写入数据的写数据请求。

- 15 S702：主节点执行第一阶段节点交互（准备阶段），将认证请求分发到其他的从节点上。当从节点接收到认证请求并进行共识处理后，可以向主节点返回应答消息。

- 在准备阶段，主节点向其他从节点发送的认证请求中携带有需要写入区块链的数据，以及利用主节点的私钥对该数据进行摘要处理和加密处理后得到主节点的数字签名。以图5所示的数据结构为例，在主节点向从节点发送的认证请求中，携带有写入字段“预准备阶段签名”的主节点数字签名。
- 20

- 当从节点接收到主节点发送的认证请求时，可以利用主节点的公钥对认证请求中携带的数字签名进行签名验证。签名验证通过后，从节点可以利用自身的私钥对需要写入区块链的数据进行摘要处理和加密处理后得到从节点数字签名。以图5所示的数据结构为例，在从节点向主节点返回的准备阶段的应答消息中，携带有写入字段“预准备阶段签名”的主节点数字签名和从节点数字签名。
- 25

S703：当主节点收到超过1/2总节点数的应答消息时（包含主节点自身），主节点执行第二阶段（提交阶段），主节点提交数据并通知其他从节点提交数据。当从节点接收到提交通知后，可以向自身保存的区块链写入数据，并向主节点返回应答消息。

- 30 当主节点接收到从节点返回的准备阶段应答消息时，可以收集聚合各个应答消息中携带的从节点数字签名。

- 在进入提交阶段后，主节点可以向各个从节点发送携带有聚合后数字签名的提交通知。以图5所示的数据结构为例，在主节点向从节点发送的提交通知中，携带有写入字段“预准备阶段签名”的主节点数字签名和多个从节点数字签名，同时还携带有写入字段“提交阶段签名”的主节点数字签名。其中，字段“预准备阶段签名”中的主节点数字签名和从节点数字签名的数量应当超过总节点数量的1/2，即满足低容错率共识算法在准备阶段的共识条件。
- 35

当从节点接收到主节点发送的提交通知时，可以采用与前一阶段相同的方式进行签名

验证,并在验证通过后向应答消息中写入自身的从节点数字签名。以图5所示的数据结构为例,在从节点向主节点返回的提交阶段的应答消息中,携带有写入字段“预准备阶段签名”的主节点数字签名和多个从节点数字签名,同时还携带有写入字段“提交阶段签名”的主节点数字签名和该从节点自身的从节点数字签名。

- 5 S704: 主节点返回给客户端数据写入成功的应答,此时客户端可以确定数据已经成功写入了整个区块链系统中。

主节点接收到从节点返回的提交阶段应答消息时,可以收集聚合各个应答消息中携带的从节点数字签名。以图5所示的数据结构为例,在主节点向客户端返回的应答消息中,携带有写入字段“预准备阶段签名”的主节点数字签名和多个从节点数字签名,同时还携带有写入字段“提交阶段签名”的主节点数字签名和多个从节点数字签名。其中,字段“预准备阶段签名”中的主节点数字签名和从节点数字签名的数量应当超过总节点数量的1/2,字段“提交阶段签名”中的主节点数字签名和从节点数字签名的数量也应当超过总节点数量的1/2,即满足低容错率共识算法在准备阶段和提交阶段的共识条件。

- 10 图8示出了本申请一个实施例中的高容错率共识算法的共识流程,高容错率共识算法例如可以是BFT类共识算法中的PBFT算法。相对于CFT类共识算法,BFT类共识算法需要在软件错误或者节点作恶的情况下仍然保证系统的一致性,因此BFT类算法的节点交互更复杂,一般需要三个阶段的交互;容错节点数更少,一般可容忍1/3的错误节点。

如图8所示,基于高容错率共识算法进行共识认证的流程可以包括如下步骤。

- 15 S801: 客户端发送共识请求到主节点。共识请求例如可以是向区块链写入数据的写数据请求。

S802: 主节点执行第一阶段节点交互(预准备阶段),将认证请求分发到其他的从节点上。当从节点接收到认证请求并进行共识处理后,可以向主节点返回应答消息。这一阶段的目的是确认多个从节点收到的请求是相同的,以防止主节点作恶,发送给不同从节点不同的消息。

- 20 25 在预准备阶段,主节点向其他从节点发送的认证请求中携带有需要写入区块链的数据,以及利用主节点的私钥对该数据进行摘要处理和加密处理后得到主节点的数字签名。以图5所示的数据结构为例,在主节点向从节点发送的认证请求中,携带有写入字段“预准备阶段签名”的主节点数字签名。

- 30 当从节点接收到主节点发送的认证请求后,可以利用主节点的公钥对认证请求中携带的数字签名进行签名验证。签名验证通过后,从节点可以利用自身的私钥对需要写入区块链的数据进行摘要处理和加密处理后得到从节点数字签名。以图5所示的数据结构为例,在从节点向主节点返回的预准备阶段的应答消息中,携带有写入字段“预准备阶段签名”的主节点数字签名和从节点数字签名。

- 35 S803: 当主节点收到超过2/3总节点数的预准备阶段的应答消息时(包含主节点自身),主节点执行第二阶段(准备阶段),主节点将消息签名再发送给其他从节点。从节点会验证消息签名数是否大于2/3节点总数,如果大于2/3则从节点返回给主节点成功投票的应答消息。

当主节点接收到从节点返回的预准备阶段应答消息时,可以收集聚合各个应答消息中

携带的从节点数字签名。

在进入准备阶段后，主节点可以向各个从节点发送携带有聚合后数字签名的准备消息。以图5所示的数据结构为例，在主节点向从节点发送的准备消息中，携带有写入字段“预准备阶段签名”的主节点数字签名和多个从节点数字签名，同时还携带有写入字段“准备阶段签名”的主节点数字签名。其中，字段“预准备阶段签名”中的主节点数字签名和从节点数字签名的数量应当超过总节点数量的2/3，即满足高容错率共识算法在预准备阶段的共识条件。

当从节点接收到主节点发送的准备消息后，可以采用与前一阶段相同的方式进行签名验证，并在验证通过后向应答消息中写入自身的从节点数字签名。以图5所示的数据结构为例，在从节点向主节点返回的准备阶段的应答消息中，携带有写入字段“预准备阶段签名”的主节点数字签名和多个从节点数字签名，同时还携带有写入字段“提交阶段签名”的主节点数字签名和该从节点自身的从节点数字签名。

S804：当主节点收到超过2/3总节点数的应答消息时（包含主节点自身），主节点执行第三阶段（提交阶段），主节点提交数据并通知其他从节点提交数据。当从节点接收到提交通知后，可以向自身保存的区块链写入数据，并向主节点返回应答消息。

当主节点接收到从节点返回的准备阶段应答消息时，可以收集聚合各个应答消息中携带的从节点数字签名。

在进入提交阶段后，主节点可以向各个从节点发送携带有聚合后数字签名的提交通知。以图5所示的数据结构为例，在主节点向从节点发送的提交通知中，携带有写入字段“预准备阶段签名”的主节点数字签名和多个从节点数字签名，同时还携带有写入字段“准备阶段签名”的主节点数字签名和多个从节点数字签名，以及写入字段“提交阶段签名”的主节点数字签名。其中，字段“预准备阶段签名”中的主节点数字签名和从节点数字签名的数量应当超过总节点数量的2/3，字段“准备阶段签名”中的主节点数字签名和从节点数字签名的数量也应当超过总节点数量的2/3，即满足高容错率共识算法在预准备阶段和准备阶段的共识条件。

当从节点接收到主节点发送的准备消息时，可以采用与前一阶段相同的方式进行签名验证，并在验证通过后向应答消息中写入自身的从节点数字签名。以图5所示的数据结构为例，在从节点向主节点返回的提交阶段的应答消息中，携带有写入字段“预准备阶段签名”的主节点数字签名和多个从节点数字签名，同时还携带有写入字段“准备阶段签名”的主节点数字签名和多个从节点数字签名，以及写入字段“提交阶段签名”的主节点数字签名和该从节点自身的从节点数字签名。

S805：主节点返回给客户端数据写入成功的应答，此时客户端可以确定数据已经成功写入了整个区块链系统中。

主节点接收到从节点返回的提交阶段应答消息时，可以收集聚合各个应答消息中携带的从节点数字签名。以图5所示的数据结构为例，在主节点向客户端返回的应答消息中，携带有写入字段“预准备阶段签名”的主节点数字签名和多个从节点数字签名，同时还携带有写入字段“准备阶段签名”的主节点数字签名和多个从节点数字签名，以及写入字段“提

交阶段签名”的主节点数字签名和多个从节点数字签名。其中，字段“预准备阶段签名”中的主节点数字签名和从节点数字签名的数量应当超过总节点数量的2/3，字段“准备阶段签名”中的主节点数字签名和从节点数字签名的数量也应当超过总节点数量的2/3，字段“提交阶段签名”中的主节点数字签名和从节点数字签名的数量也应当超过总节点数量的2/3，即满足高容错率共识算法在预准备阶段、准备阶段和提交阶段的共识条件。

5 在相关技术的区块链系统中，其中一类系统追求系统性能，采用了CFT类的共识，如Fabric；另一类追求更广泛的容错性，采用了BFT类的共识，如Tendermint。在实际的企业级应用中，使用区块链服务的上层业务系统会随着用户需求的不断变更，在性能、可用性、容错性、扩展性等方面有着不同的诉求。而目前的区块链系统由于采用的都是单一的共识
10 算法，无法匹配上层业务系统的要求。本申请实施例提供一种在CFT和BFT算法之间在线灵活切换的方案，可以使区块链系统在不停止服务的情况下，变更共识算法以满足业务系统的要求。

在本申请的一个实施例中，在区块链网络中广播共识请求的过程中，可以对区块链网络中的部分或者全部的区块链节点进行算法切换，以变更部分或者全部的区块链节点执行的
15 的共识算法。

当一部分区块链节点完成算法切换，而另一部分区块链节点未完成算法切换时，区块链网络中将存在至少两种执行不同共识算法的区块链节点。在此基础上，可以利用本申请上述实施例进行共识认证。

在本申请的一个实施例中，对区块链网络中的部分或者全部的区块链节点进行算法切换的方法可以包括：
20

对区块链网络进行可信度预测，以确定区块链网络的运行环境是否为可信环境；

若区块链网络的运行环境为可信环境，则将区块链网络中执行低容错率共识算法部分或者全部的区块链节点切换为执行高容错率共识算法；

若区块链网络的运行环境为非可信环境，则将区块链网络中执行高容错率共识算法部分或者全部的区块链节点切换为执行低容错率共识算法。
25

在本申请的一个实施例中，对区块链网络进行可信度预测的方法可以包括：

获取区块链网络中各个区块链节点的运行时长；

若运行时长低于时长阈值，则确定区块链节点为非可信节点；

若区块链网络中的非可信节点的数量大于数量阈值，则确定区块链网络的运行环境为
30 非可信环境；

若区块链网络中的非可信节点的数量小于数量阈值，则确定区块链网络的运行环境为可信环境。

举例而言，在供应链管理的场景中，区块链系统往往是由供应链流程中某一环的企业发起，此时可以认为区块链系统处于可信的环境中，不需要考虑有恶意节点的情况，可以
35 使用简单的CFT算法作为共识算法；当供应链中的其他企业加入到区块链系统中时，要防止其他企业有故意作恶的情况，可以执行本申请实施例的算法切换步骤，在不停止服务的情况下，将共识算法切换成BFT类算法；当区块链系统已经稳定运行了一段时间，各个参

与企业可以被认为是可信的节点后，可以再执行本申请实施例的算法切换步骤，将共识算法切换为CFT类算法，提高区块链系统的性能。

图9示出了本申请实施例在执行算法切换过程中的场景示例。以四个节点的算法切换作为示例，各个区块链节点在算法切换的不同时刻下将执行不同的共识算法。

5 当区块链网络中存在不同分布比例的两种共识算法时，可以形成如图8所示的五种场景。在CFT共识切换至BFT共识中，节点由全部都是CFT共识算法逐步切换为全部都是BFT类共识算法，即场景一逐步变化为场景五。在BFT共识切换至CFT共识中，节点由全部都是BFT共识算法逐步切换为全部都是CFT类共识算法，即场景五逐步变化为场景一。

表2为五种场景下执行不同共识算法的区块链节点占总节点数的比例关系。

10

表2

场景	CFT类节点占总结点数比例	BFT类节点占总结点数比例
场景一	= 1	= 0
场景二	> 1/2	< 1/2
场景三	< 1/2 且 > 1/3	> 1/2 且 < 2/3
场景四	< 1/3	> 2/3
场景五	= 0	= 1

以下分别说明五种应用场景下的共识方案。

场景一：

在场景一中，因为所有节点的共识算法都是CFT，所以此场景相当于单独使用CFT算法的场景。只要所有节点都按照本地的CFT算法步骤，系统数据就可以达成一致。

15

场景二：

在场景二中，只有节点一的共识算法是BFT算法，其余三个节点都是CFT算法。此时CFT节点总数（3）大于总节点数（4）的1/2，按照CFT算法的共识条件，3个CFT节点之间可以达成共识。达成共识后，节点一同步共识结果，可以保证系统数据一致。

场景三：

20

在场景三中，CFT节点数不能满足CFT算法要求的大于1/2的共识条件，同时BFT节点数也不能满足BFT算法要求的大于2/3的共识条件。此时按照正常的CFT算法或BFT算法，系统内所有节点均无法达成共识。

在该场景下，本申请实施例可以使用具有如图5所示数据结构的应答消息进行节点间的数据交互。

25

参考图5所示，该数据结构中包括预准备阶段签名、准备阶段签名和提交阶段签名三个签名字段。CFT共识节点使用其中的预准备阶段签名和提交阶段签名；BFT共识节点使用全部三个阶段的签名。

图10示出了本申请实施例在一个应用场景中执行共识认证的方法步骤流程图。如图10

所示,在如上的场景三中,执行共识认证的方法可以包括如下步骤。

S1001: 主节点接收客户端发送的共识请求。

S1002: 主节点向从节点发送<预准备>消息。

S1003: 从节点向主节点回复<预准备>消息。

- 5 CFT类共识算法的准备阶段与BFT类共识算法的预准备阶段相互匹配,因此使用CFT类共识算法的节点可以将<预准备>消息当做<准备>消息对待。此时使用CFT类共识的从节点和使用BFT类共识的从节点都会向主节点回复<预准备>消息。

S1004: 主节点判断是否收到超过总节点数量2/3比例的<预准备>消息。

- 10 若未超过2/3,则返回S1003,继续接收其他从节点回复的<预准备>消息。若超过2/3,则完成预准备阶段的共识认证,进入准备阶段,并执行S1005。

S1005: 主节点向从节点发送<准备>消息。

S1006: 判断接收到<准备>消息的从节点是否为执行CFT类共识算法的CFT节点。若判断结果为是,则执行S1007。若判断结果为否,则表示该从节点为执行BFT类共识算法的BFT节点,跳转至S10010。

- 15 S1007: 从节点提交数据。

当使用CFT类共识算法的从节点从主节点收到<准备>消息时,可以说明主节点已经收到了大于2/3的<预准备>消息。这大于CFT算法要求的1/2条件,所以此时执行CFT类共识算法的从节点可以将<准备>消息当做是<提交>消息,直接提交数据,此时使用CFT类共识算法的节点可以达成共识,数据一致。

- 20 S1008: 从节点向主节点回复<提交>消息。

执行CFT类共识算法的从节点在完成提交数据后,返回给主节点<提交>消息,以使其他BFT类节点达成<准备>+<提交>总数达到2/3的提交条件。然后,执行S1010。

S1009: 从节点向主节点回复<准备>消息。

S1010: 主节点判断是否收到超过总节点数量2/3比例的<准备>消息。

- 25 若判断未超过2/3,则继续执行S1011。若判断超过2/3,则完成准备阶段的共识认证,进入提交阶段,并跳转执行S1012。

S1011: 主节点判断是否收到超过总节点数量2/3比例的<准备>消息和<提交>消息。

- 30 CFT类共识算法的提交阶段与BFT类共识算法的准备阶段和提交阶段相互匹配。因此,当主节点收到CFT节点回复的<提交>消息应答时,主节点可以把<提交>消息应答当做<准备>消息应答来对待。在此基础上,若判断主节点收到超过总节点数量2/3比例的<准备>消息和<提交>消息,则完成准备阶段的共识认证,进入提交阶段,并继续执行S1012。若判断主节点未收到超过总节点数量2/3比例的<准备>消息和<提交>消息,则返回S1005,由主节点继续向其他从节点发送<准备>消息。

S1012: 主节点向从节点发送<提交>消息。

- 35 S1013: 各个从节点提交数据并向主节点返回<提交>消息,系统达成共识。

使用BFT类共识的节点可以达到大于2/3的<准备>消息应答条件。此时BFT类共识节点按照BFT类算法的步骤可以达成共识,并且可以保证数据与CFT类节点的一致性。

场景四:

在场景四中, 节点四执行CFT类共识算法, 其余三个节点执行BFT类共识算法。此时BFT节点总数(3)大于总结点数(4)的2/3, 按照BFT类共识算法, 3个BFT节点之间可以达成共识。达成共识后, 节点四同步共识结果, 可以保证系统数据一致性。

5 场景五:

在场景五中, 所有节点都执行BFT类共识算法, 按照BFT类共识算法的步骤, 系统可以达成一致性共识。

10 基于以上各个应用场景的说明可知, 本申请实施例提供的在线共识算法切换方案可以支持在不停止服务的情况下切换共识算法, 使得区块链系统更加灵活地适配上层业务的需求, 可以使得区块链系统更加广泛地应用到不同场景中。

应当注意, 尽管在附图中以特定顺序描述了本申请中方法的各个步骤, 但是, 这并非要求或者暗示必须按照该特定顺序来执行这些步骤, 或是必须执行全部所示的步骤才能实现期望的结果。附加的或备选的, 可以省略某些步骤, 将多个步骤合并为一个步骤执行, 以及/或者将一个步骤分解为多个步骤执行等。

15 以下介绍本申请的装置实施例, 可以用于执行本申请上述实施例中的区块链共识方法。图11示意性地示出了本申请实施例提供的区块链共识装置的结构框图。如图11所示, 区块链共识装置1100包括:

请求模块1110, 被配置为在区块链网络中广播对应于至少两个共识阶段的共识请求, 所述区块链网络包括至少两种执行不同类型共识算法的区块链节点;

20 应答模块1120, 被配置为分别获取所述区块链网络在各个所述共识阶段中广播的应答消息, 所述应答消息是所述区块链节点对所述共识请求做出响应的消息, 所述不同类型共识算法包括第一共识算法和第二共识算法;

统计模块1130, 被配置为统计在相同的共识阶段中发出所述应答消息的区块链节点的节点数量, 所述节点数量包括至少两种执行不同类型共识算法的区块链节点的数量;

25 同步模块1140, 被配置为若所述节点数量满足所述第一共识算法的共识条件, 在执行所述第一共识算法的区块链节点上达成共识, 并向执行所述第二共识算法的区块链节点同步所述第一共识算法的共识结果。

30 在本申请的一个实施例中, 基于以上各实施例, 不同类型的共识算法具有不同数量的共识阶段, 所述应答消息中携带区块链节点的算法类型和节点签名, 所述算法类型用于指示所述区块链节点执行的共识算法, 所述节点签名包括所述区块链节点在各个共识阶段的数字签名。

在本申请的一个实施例中, 基于以上各实施例, 统计模块1030可以进一步包括:

解析模块, 被配置为解析所述应答消息, 得到所述应答消息中携带的算法类型和节点签名;

35 算法识别模块, 被配置为根据所述算法类型识别消息发送节点执行的共识算法, 所述消息发送节点为发出所述应答消息的区块链节点;

阶段识别模块, 被配置为根据所述节点签名识别所述消息发送节点所处的共识阶段;

数量统计模块,被配置为根据所述消息发送节点执行的共识算法以及所述消息发送节点所处的共识阶段,统计与当前区块链节点处于相同共识阶段的消息发送节点的节点数量。

在本申请的一个实施例中,基于以上各实施例,统计模块1030还可以进一步包括:

关系获取模块,被配置为获取不同类型共识算法之间的共识阶段的匹配关系;

- 5 节点确定模块,被配置为若所述消息发送节点与当前区块链节点执行不同类型的共识算法,则根据所述匹配关系确定与当前区块链节点处于相同共识阶段的消息发送节点。

在本申请的一个实施例中,基于以上各实施例,所述第一共识算法包括N个共识阶段,所述第二共识算法包括M个共识阶段;不同类型共识算法之间的共识阶段的匹配关系包括:

- 10 所述第一共识算法与所述第二共识算法的前P个共识阶段相互匹配,P为N-1和M-1中的较小值;

所述第一共识算法的后N-P个共识阶段与所述第二共识算法的后M-P个共识阶段相互匹配。

在本申请的一个实施例中,基于以上各实施例,在统计与当前区块链节点处于相同共识阶段的消息发送节点的节点数量之后,统计模块1030还可以进一步包括:

- 15 共识结果确定模块,被配置为若所述当前区块链节点所处的共识阶段是所执行共识算法的最后一个共识阶段,则根据所述节点数量是否满足所执行共识算法的共识条件,确定共识算法的共识结果;

- 20 共识阶段执行模块,被配置为若所述当前区块链节点所处的共识阶段不是所执行共识算法的最后一个共识阶段,则根据所述节点数量是否满足所执行共识算法的共识条件,确定是否执行共识算法的下一个共识阶段。

在本申请的一个实施例中,基于以上各实施例,所述第一共识算法为低容错率共识算法和高容错率共识算法中的一种,所述第二共识算法为所述低容错率共识算法和高容错率共识算法中与所述第一共识算法不同的另一种;

- 25 所述低容错率共识算法的共识条件为发出应答消息的区块链节点与所有区块链节点的数量比例大于第一比例阈值,所述高容错率共识算法的共识条件为发出应答消息的区块链节点与所有区块链节点的数量比例大于第二比例阈值,所述第一比例阈值小于所述第二比例阈值。

- 30 在本申请的一个实施例中,基于以上各实施例,所述低容错率共识算法具有第一数量的共识阶段,所述高容错率共识算法具有第二数量的共识阶段,所述第一数量小于所述第二数量。

- 35 在本申请的一个实施例中,基于以上各实施例,所述低容错率共识算法的共识阶段包括依次执行的准备阶段和提交阶段,所述高容错率共识算法的共识阶段包括依次执行的预准备阶段、准备阶段和提交阶段,所述低容错率共识算法的准备阶段与所述高容错率共识算法的预准备阶段相匹配,所述低容错率共识算法的提交阶段与所述高容错率共识算法的准备阶段和提交阶段相匹配。

在本申请的一个实施例中,基于以上各实施例,区块链共识装置1000还可以进一步包括:

算法切换模块,被配置为对所述区块链网络中的部分或者全部的区块链节点进行算法切换,以变更所述部分或者全部的区块链节点执行的共识算法。

在本申请的一个实施例中,基于以上各实施例,算法切换模块可以进一步包括:

可信度检测模块,被配置为对所述区块链网络进行可信度预测,以确定所述区块链网络的运行环境是否为可信环境;

第一算法切换模块,被配置为若所述区块链网络的运行环境为可信环境,则将所述区块链网络中执行低容错率共识算法部分或者全部的区块链节点切换为执行高容错率共识算法;

第二算法切换模块,被配置为若所述区块链网络的运行环境为非可信环境,则将所述区块链网络中执行高容错率共识算法部分或者全部的区块链节点切换为执行低容错率共识算法。

在本申请的一个实施例中,基于以上各实施例,对所述区块链网络进行可信度预测,可信度检测模块可以进一步包括:

时长获取模块,被配置为获取所述区块链网络中各个区块链节点的运行时长;

非可信节点确定模块,被配置为若所述运行时长低于时长阈值,则确定所述区块链节点为非可信节点;

非可信环境确定模块,被配置为若所述区块链网络中的非可信节点的数量大于数量阈值,则确定所述区块链网络的运行环境为非可信环境;

可信环境确定模块,被配置为若所述区块链网络中的非可信节点的数量小于数量阈值,则确定所述区块链网络的运行环境为可信环境。

本申请各实施例中提供的区块链共识装置的具体细节已经在对应的方法实施例中进行了详细的描述,此处不再赘述。

图12示意性地示出了用于实现本申请实施例的电子设备的计算机系统结构框图。

需要说明的是,图12示出的电子设备的计算机系统1200仅是一个示例,不应对本申请实施例的功能和使用范围带来任何限制。

如图12所示,计算机系统1200包括中央处理器1201(Central Processing Unit, CPU),其可以根据存储在只读存储器1202(Read-Only Memory, ROM)中的程序或者从存储部分1208加载到随机访问存储器1203(Random Access Memory, RAM)中的程序而执行各种适当的动作和处理。在随机访问存储器1203中,还存储有系统操作所需的各种程序和数据。中央处理器1201、在只读存储器1202以及随机访问存储器1203通过总线1204彼此相连。输入/输出接口1205(Input/Output接口,即I/O接口)也连接至总线1204。

以下部件连接至输入/输出接口1205:包括键盘、鼠标等的输入部分1206;包括诸如阴极射线管(Cathode Ray Tube, CRT)、液晶显示器(Liquid Crystal Display, LCD)等以及扬声器等的输出部分1207;包括硬盘等的存储部分1208;以及包括诸如局域网卡、调制解调器等的网络接口卡的通信部分1209。通信部分1209经由诸如因特网的网络执行通信处理。驱动器1210也根据需要连接至输入/输出接口1205。可拆卸介质1211,诸如磁盘、光盘、磁光盘、半导体存储器等等,根据需要安装在驱动器1210上,以便于从其上读出的计算机程

序根据需被安装入存储部分1208。

特别地，根据本申请的实施例，各个方法流程图中所描述的过程可以被实现为计算机软件程序。例如，本申请的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的
5 实施例中，该计算机程序可以通过通信部分1209从网络上被下载和安装，和/或从可拆卸介质1211被安装。在该计算机程序被中央处理器1201执行时，执行本申请的系统中限定的各种功能。

需要说明的是，本申请实施例所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但
10 不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（Erasable Programmable Read Only Memory, EPROM）、闪存、光纤、便携式紧凑磁盘只读存储器（Compact Disc Read-Only Memory, CD-ROM）、光存储器件、
15 磁存储器件、或者上述的任意合适的组合。在本申请中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本申请中，计算机可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读信号介质还可以是
20 计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于：无线、有线等等，或者上述的任意合适的组合。

附图中的流程图和框图，图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。
25 也要注意的，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

应当注意，尽管在上文详细描述中提及了用于动作执行的设备的若干模块或者单元，但是这种划分并非强制性的。实际上，根据本申请的实施方式，上文描述的两个或更多模块或者单元的特征和功能可以在一个模块或者单元中具体化。反之，上文描述的一个模块或者单元的特征和功能可以进一步划分为由多个模块或者单元来具体化。
30

通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式

—25—

可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本申请实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是CD-ROM，U盘，移动硬盘等）中或网络上，包括若干指令以使得一台计算设备（可以是个人计算机、服务器、触控终端、或者网络设备等等）执行根据本申请实施方式的方法。

5

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。

10

应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

权 利 要 求

1. 一种区块链共识方法，所述方法由区块链网络中的当前区块链节点执行，所述方法包括：

在所述区块链网络中广播对应于至少两个共识阶段的共识请求，所述区块链网络包括至少两种执行不同类型共识算法的区块链节点，所述不同类型共识算法包括第一共识算法和第二共识算法；

分别获取所述区块链网络在各个所述共识阶段中广播的应答消息，所述应答消息是所述区块链节点对所述共识请求做出响应的消息；

统计在相同的共识阶段中发出所述应答消息的区块链节点的节点数量，所述节点数量包括至少两种执行不同类型共识算法的区块链节点的数量；

若所述节点数量满足所述第一共识算法的共识条件，在执行所述第一共识算法的区块链节点上达成共识，并向执行所述第二共识算法的区块链节点同步所述第一共识算法的共识结果。

2. 根据权利要求1所述的区块链共识方法，不同类型的共识算法具有不同数量的共识阶段，所述应答消息中携带区块链节点的算法类型和节点签名，所述算法类型用于指示所述区块链节点执行的共识算法，所述节点签名包括所述区块链节点在各个共识阶段的数字签名。

3. 根据权利要求2所述的区块链共识方法，所述统计在相同的共识阶段中发出所述应答消息的区块链节点的节点数量，包括：

解析所述应答消息，得到所述应答消息中携带的算法类型和节点签名；

根据所述算法类型识别消息发送节点执行的共识算法，所述消息发送节点为发出所述应答消息的区块链节点；

根据所述节点签名识别所述消息发送节点所处的共识阶段；

根据所述消息发送节点执行的共识算法以及所述消息发送节点所处的共识阶段，统计与所述当前区块链节点处于相同共识阶段的消息发送节点的节点数量。

4. 根据权利要求3所述的区块链共识方法，在所述统计与所述当前区块链节点处于相同共识阶段的消息发送节点的节点数量之前，所述方法还包括：

获取所述不同类型共识算法之间的共识阶段的匹配关系；

若所述消息发送节点与所述当前区块链节点执行不同类型的共识算法，则根据所述匹配关系确定与所述当前区块链节点处于相同共识阶段的消息发送节点。

5. 根据权利要求4所述的区块链共识方法，所述第一共识算法包括N个共识阶段，所述第二共识算法包括M个共识阶段；所述不同类型共识算法之间的共识阶段的匹配关系包括：

所述第一共识算法与所述第二共识算法的前P个共识阶段相互匹配，P为N-1和M-1中的较小值；

所述第一共识算法的后N-P个共识阶段与所述第二共识算法的后M-P个共识阶段相互匹配。

6. 根据权利要求3所述的区块链共识方法, 在所述统计与所述当前区块链节点处于相同共识阶段的消息发送节点的节点数量之后, 所述方法还包括:

若所述当前区块链节点所处的共识阶段是所执行共识算法的最后一个共识阶段, 则根据所述节点数量是否满足所执行共识算法的共识条件, 确定共识算法的共识结果;

5 若所述当前区块链节点所处的共识阶段不是所执行共识算法的最后一个共识阶段, 则根据所述节点数量是否满足所执行共识算法的共识条件, 确定是否执行共识算法的下一个共识阶段。

7. 根据权利要求1所述的区块链共识方法, 所述第一共识算法为低容错率共识算法和高容错率共识算法中的一种, 所述第二共识算法为所述低容错率共识算法和高容错率共识算法中与所述第一共识算法不同的另一种;

所述低容错率共识算法的共识条件为发出应答消息的区块链节点与所有区块链节点的数量比例大于第一比例阈值, 所述高容错率共识算法的共识条件为发出应答消息的区块链节点与所有区块链节点的数量比例大于第二比例阈值, 所述第一比例阈值小于所述第二比例阈值。

15 8. 根据权利要求7所述的区块链共识方法, 所述低容错率共识算法具有第一数量的共识阶段, 所述高容错率共识算法具有第二数量的共识阶段, 所述第一数量小于所述第二数量。

9. 根据权利要求8所述的区块链共识方法, 所述低容错率共识算法的共识阶段包括依次执行的准备阶段和提交阶段, 所述高容错率共识算法的共识阶段包括依次执行的预准备阶段、准备阶段和提交阶段, 所述低容错率共识算法的准备阶段与所述高容错率共识算法的预准备阶段相匹配, 所述低容错率共识算法的提交阶段与所述高容错率共识算法的准备阶段和提交阶段相匹配。

10. 根据权利要求1所述的区块链共识方法, 在所述区块链网络中广播共识请求的过程中, 所述方法还包括:

25 对所述区块链网络中的部分或者全部的区块链节点进行算法切换, 以变更所述部分或者全部的区块链节点执行的共识算法。

11. 根据权利要求10所述的区块链共识方法, 所述对所述区块链网络中的部分或者全部的区块链节点进行算法切换, 包括:

30 对所述区块链网络进行可信度预测, 以确定所述区块链网络的运行环境是否为可信环境;

若所述区块链网络的运行环境为可信环境, 则将所述区块链网络中执行低容错率共识算法部分或者全部的区块链节点切换为执行高容错率共识算法;

若所述区块链网络的运行环境为非可信环境, 则将所述区块链网络中执行高容错率共识算法部分或者全部的区块链节点切换为执行低容错率共识算法。

35 12. 根据权利要求11所述的区块链共识方法, 所述对所述区块链网络进行可信度预测, 包括:

获取所述区块链网络中各个区块链节点的运行时长;

若所述运行时长低于时长阈值，则确定所述区块链节点为非可信节点；

若所述区块链网络中的非可信节点的数量大于数量阈值，则确定所述区块链网络的运行环境为非可信环境；

若所述区块链网络中的非可信节点的数量小于数量阈值，则确定所述区块链网络的运行环境为可信环境。

5

13. 一种区块链共识装置，包括：

请求模块，被配置为在区块链网络中广播对应于至少两个共识阶段的共识请求，所述区块链网络包括至少两种执行不同类型共识算法的区块链节点，所述不同类型共识算法包括第一共识算法和第二共识算法；

10

应答模块，被配置为分别获取所述区块链网络在各个所述共识阶段中广播的应答消息，所述应答消息是所述区块链节点对所述共识请求做出响应的消息；

统计模块，被配置为统计在相同的共识阶段中发出所述应答消息的区块链节点的节点数量，所述节点数量包括至少两种执行不同类型共识算法的区块链节点的数量；

同步模块，被配置为若所述节点数量满足所述第一共识算法的共识条件，在执行所述第一共识算法的区块链节点上达成共识，并向执行所述第二共识算法的区块链节点同步所述第一共识算法的共识结果。

15

14. 一种计算机可读介质，所述计算机可读介质上存储有计算机程序，所述计算机程序被处理器执行时实现权利要求1至12中任意一项所述的区块链共识方法。

15. 一种电子设备，包括：

20

处理器；以及

存储器，用于存储所述处理器的可执行指令；

其中，所述处理器配置为经由执行所述可执行指令使得所述电子设备执行权利要求1至12中任意一项所述的区块链共识方法。

16. 一种计算机程序产品，包括计算机程序，所述计算机程序被处理器执行时实现权利要求1至12中任意一项所述的区块链共识方法。

25