(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 109361740 A
(43)申请公布日 2019.02.19

(21)申请号 201811131704.7

(22)申请日 2018.09.27

(71)申请人 百度在线网络技术(北京)有限公司
地址 100085 北京市海淀区上地十街10号百度大厦三层

(72)发明人 郑旗 肖伟

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 孟金喆

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 9/32(2006.01)

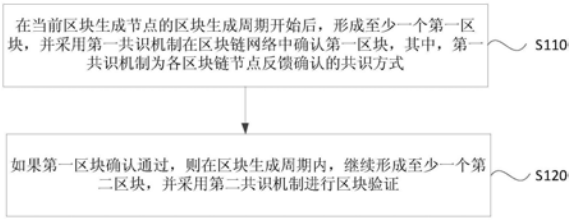
权利要求书2页 说明书10页 附图3页

(54)发明名称

一种区块链的区块生成方法、装置、设备和介质

(57)摘要

本发明实施例公开了一种区块链的区块生成方法、装置、设备和介质。其中，该方法应用于区块生成节点，该方法包括：在当前区块生成节点的区块生成周期开始后，形成至少一个第一区块，并采用第一共识机制在区块链网络中确认所述第一区块，其中，所述第一共识机制为各区块链节点反馈确认的共识方式；如果所述第一区块确认通过，则在所述区块生成周期内，继续形成至少一个第二区块，并采用第二共识机制进行区块验证。通过本发明实施例的技术方案，能够减少区块链中出现的分叉现象。



CN 109361740 A

1.一种区块链的区块生成方法,其特征在于,应用于区块生成节点,所述方法包括:

在当前区块生成节点的区块生成周期开始后,形成至少一个第一区块,并采用第一共识机制在区块链网络中确认所述第一区块,其中,所述第一共识机制为各区块链节点反馈确认的共识方式;

如果所述第一区块确认通过,则在所述区块生成周期内,继续形成至少一个第二区块,并采用第二共识机制进行区块验证。

2.根据权利要求1所述的方法,其特征在于,在当前区块生成节点的区块生成周期开始之前,还包括:

采用第三共识机制确定至少两个备选区块生成节点,并分别确定每个备选区块生成节点的区块生成周期,其中,各备选区块生成节点切换地作为当前区块生成节点。

3.根据权利要求1或2所述的方法,其特征在于,采用第一共识机制在区块链网络中确认所述第一区块,包括:

将所述第一区块的信息在区块链网络中传输,以请求其他区块链节点进行签名确认;

接收其他区块链节点反馈的签名消息;

根据接收到的签名消息确定所述第一区块的确认结果;

如果确认结果为确认通过,则将签名消息中的确认签名携带在第一区块中,并将所述第一区块在区块链网络中传输,以添加至区块链中。

4.根据权利要求3所述的方法,其特征在于,将所述第一区块的信息在区块链网络中传输,以请求其他区块链节点进行签名确认,包括:

将所述第一区块中区块头的部分或全部信息,在区块链网络中传输,以请求其他区块链节点进行签名确认。

5.根据权利要求3所述的方法,其特征在于,根据接收到的签名消息确定所述第一区块的确认结果,包括:

如果根据接收到的签名消息确定出,确认所述第一区块的区块链节点大于设定阈值,则确认结果为确认通过。

6.根据权利要求3所述的方法,其特征在于,根据接收到的签名消息确定所述第一区块的确认结果,包括:

针对每个签名消息,采用发送所述签名消息的区块链节点的公钥对所述签名消息进行解密,以获取第一区块的信息;

将获取的第一区块信息与本地存储的第一区块信息进行比对;

若比对一致,则该签名消息的确认结果为确认通过;

根据各个签名消息的确认结果确定所述第一区块的确认结果。

7.根据权利要求3所述的方法,其特征在于,所述第一共识机制为PBFT或BFT。

8.根据权利要求1或2所述的方法,其特征在于,形成至少一个第二区块,并采用第二共识机制进行区块验证,包括:

形成至少两个第二区块,直至所述区块生成周期结束为止;

自形成第一个第二区块后,将各所述第二区块顺序在区块链网络中传输,以请求区块链节点进行区块验证。

9.根据权利要求1所述的方法,其特征在于,还包括:如果至少一个第一区块确认不通

过，则执行下述至少一项操作：

停止当前区块生成节点在区块生成周期的区块生成操作；

在等待设定时间后，返回执行形成所述第一区块的操作并进行区块确认；

在达到设定条件时，放弃形成的所述第一区块，基于本地区块链的末尾区块形成第二区块，并采用第二共识机制进行验证。

10.根据权利要求9所述的方法，其特征在于，所述设定条件为达到设定等待时长或第一区块确认不通过的次数达到设定上限值。

11.根据权利要求2所述的方法，其特征在于，所述第三共识机制为DPoS。

12.一种区块链的区块生成装置，其特征在于，配置于区块生成节点中，所述装置包括：

第一区块形成模块，用于在当前区块生成节点的区块生成周期开始后，形成至少一个第一区块；

第一区块确认模块，用于采用第一共识机制在区块链网络中确认所述第一区块，其中，所述第一共识机制为各区块链节点反馈确认的共识方式；

第二区块验证模块，用于如果所述第一区块确认通过，则在所述区块生成周期内，继续形成至少一个第二区块，并采用第二共识机制进行区块验证。

13.一种设备，其特征在于，包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-11中任一所述的区块链的区块生成方法。

14.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求1-11中任一所述的区块链的区块生成方法。

一种区块链的区块生成方法、装置、设备和介质

技术领域

[0001] 本发明实施例涉及区块链数据处理技术，尤其涉及一种区块链的区块生成方法、装置、设备和介质。

背景技术

[0002] 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链主要解决陌生节点之间的信任和安全问题，所以其中一个显著特点是分布式区块。

[0003] 具体是，在区块链网络中，各个区块链节点通过某种共识机制确定当前时间段的区块生成节点，该区块生成节点有权力将当前时间段内产生的事务请求进行处理并打包生成区块，传输给其他节点。其他节点则对该区块进行验证，验证成功则添加到每个节点本地的区块链中。若某个节点验证某个区块不成功，则可以不接受并存储该区块。若某个节点同时收到了不同的区块，且都验证成功，那可以都接受，并在本地区块链中分叉存储不同区块。

[0004] 现有区块链网络采用的一些共识机制，例如PoW、PoS和DPoS，这类共识机制的特点是，一次共识能够确定多个区块生成节点，各自按照规则生成区块。这就存在同一时间有不止一个区块生成节点生成区块的情况，则会产生区块链分叉，需要进行分叉处理。而分叉会导致某个分支的区块被丢弃，这会降低用户体验，也会影响智能合约的执行。

发明内容

[0005] 本发明实施例提供一种区块链的区块生成方法、装置、设备和介质，以减少区块链中出现的分叉现象。

[0006] 第一方面，本发明实施例提供了一种区块链的区块生成方法，应用于区块生成节点，该方法包括：

[0007] 在当前区块生成节点的区块生成周期开始后，形成至少一个第一区块，并采用第一共识机制在区块链网络中确认所述第一区块，其中，所述第一共识机制为各区块链节点反馈确认的共识方式；

[0008] 如果所述第一区块确认通过，则在所述区块生成周期内，继续形成至少一个第二区块，并采用第二共识机制进行区块验证。

[0009] 第二方面，本发明实施例还提供了一种区块链的区块生成装置，配置于区块生成节点中，该装置包括：

[0010] 第一区块形成模块，用于在当前区块生成节点的区块生成周期开始后，形成至少一个第一区块；

[0011] 第一区块确认模块，用于采用第一共识机制在区块链网络中确认所述第一区块，其中，所述第一共识机制为各区块链节点反馈确认的共识方式；

[0012] 第二区块验证模块，用于如果所述第一区块确认通过，则在所述区块生成周期内，

继续形成至少一个第二区块，并采用第二共识机制进行区块验证。

[0013] 第三方面，本发明实施例还提供了一种设备，该设备包括：

[0014] 一个或多个处理器；

[0015] 存储装置，用于存储一个或多个程序；

[0016] 当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现第一方面所述的区块链的区块生成方法。

[0017] 第四方面，本发明实施例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，该程序被处理器执行时实现第一方面所述的区块链的区块生成方法。

[0018] 本发明实施例提供的区块链的区块生成方法、装置、设备和介质，在当前区块生成节点的区块生成周期开始后，先采用第一共识机制对当前区块生成节点形成的第一区块进行反馈确认，并在第一区块确认通过后，在区块生成周期内继续形成多个第二区块，降低了由于网络传输时延、计算时延等问题造成分叉的现象，提升了用户体验；同时，当前区块生成节点可以采用第二共识机制对形成的第二区块进行区块验证，第二共识机制可以与第一共识机制不同，从而发挥第二共识机制的优势。

附图说明

[0019] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本发明的某些实施例，因此不应被看作是对范围的限定，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相关的附图。

[0020] 图1A是本发明实施例一中提供的一种区块链的区块生成方法的流程图；

[0021] 图1B和图1C是本发明实施例所适用的区块链的示意图；

[0022] 图2是本发明实施例二中提供的一种区块链的区块生成方法的流程图；

[0023] 图3是本发明实施例三中提供的一种区块链的区块生成装置的结构示意图；

[0024] 图4是本发明实施例四中提供的一种设备的结构示意图。

具体实施方式

[0025] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部结构。

[0026] 实施例一

[0027] 图1A为本发明实施例一提供的一种区块链的区块生成方法的流程图，本实施例可适用于如何降低区块链中出现的分叉现象的情况。所适用的区块链可以是公有链、私有链或者联盟链。本发明实施例的方案应用于区块链中的区块生成节点，该方法可以由区块链的区块生成装置或电子设备来执行，该装置可采用硬件和/或软件的方式实现，并可集成于承载区块链节点的计算设备中。参见图1A，该具体包括如下步骤：

[0028] S110，在当前区块生成节点的区块生成周期开始后，形成至少一个第一区块，并采用第一共识机制在区块链网络中确认第一区块，其中，第一共识机制为各区块链节点反馈确认的共识方式。

[0029] 其中，区块生成周期是指区块链节点作为区块生成节点的时间段，也可以说是区块链节点有权力对区块链中的事务请求进行处理打包形成区块的时间段。可选的，区块链中能够作为区块生成节点的各个区块链节点的区块生成周期可以是预先确定的，各个区块链节点轮换地做当前区块生成节点。示例性的，在当前区块生成节点的区块生成周期开始之前还可以包括：采用第三共识机制确定至少两个备选区块生成节点，并分别确定每个备选区块生成节点的区块生成周期，其中，各备选区块生成节点切换地作为当前区块生成节点。

[0030] 其中，第三共识机制可以是基于区块链网络包含的节点的经济实力、硬件能力及稳定性等证明因素，从区块链网络包含的节点中选择多个具有竞争区块生成权的备选区块生成节点。如可以是DPoS(Delegated proof of stake，授权权益证明机制)，该DPoS的一个特性是具有一个预先确定的处理周期。当采用DPoS基于各节点的经济实力、硬件能力及稳定性等证明因素，从区块链网络包含的各节点中筛选出N个备选区块生成节点时，也会确定各备选区块生成节点的区块生成顺序。将一个处理周期平均分为N个时间段，并按照区块生成顺序将对应的时间段分配给各备选区块生成节点，在一个时间段内由一个固定的区块生成节点进行区块生成操作。其中，处理周期是指基于DPoS所选择的N个备选区块生成节点的更新周期，例如DPoS可以3个半小时选一次备选区块生成节点。

[0031] 可选的，各个备选区块生成节点作为当前区块生成节点时，在自己的区块生成周期所产生区块的个数可以不同，也可以相同，由其硬件能力、稳定性及算力等决定。每个备选区块生成节点在作为当前区块生成节点时，能够生成一个或多个区块，其中可以包括一个第一区块，还可以包括一个或多个第二区块。第一区块是指当前区块生成节点在区块生成周期开始后，生成的第一个区块；对应的，第二个区块是指当前区块生成节点在区块生成周期内，形成第一区块之后，继续形成的区块，即第二个区块开始至该区块生成周期结束之间所有的区块。

[0032] 本实施例中，第一共识机制为各区块链节点反馈确认的共识方式，即当前区块生成节点所形成的区块需要发送到区块链网络中，让各区块链节点进行确认并反馈。该第一共识机制具有先共识后写入的特点，能够保证添加至区块链上的区块是唯一的，不会造成分叉。如可以是BFT(Byzantine Fault Tolerance，拜占庭容错)机制、PBFT(Practical Byzantine Fault Tolerance，实用拜占庭容错)机制、SBFT(Simplified Byzantine Fault Tolerance，简化拜占庭容错)机制或DBFT(Delegated Byzantine Fault Tolerance，授权拜占庭容错)机制等。

[0033] 具体的，在当前区块生成节点的区块生成周期开始，且形成第一个区块即第一区块后，为了避免由于网络传输时延、计算时延等问题，从而造成分叉，当前区块生成节点可以采用第一共识机制将第一区块发送至区块链网络，以使各区块链节点对该区块进行确认并反馈；当前区块生成节点接收各区块链节点的反馈信息，依据各区块链节点的反馈信息确定第一区块是否确认通过。

[0034] S120，如果第一区块确认通过，则在区块生成周期内，继续形成至少一个第二区块，并采用第二共识机制进行区块验证。

[0035] 其中，第二共识机制可以与第三共识机制相同；也可以是各区块链节点已达成共识的，且区别于第一共识机制和第三共识机制的其他共识机制。可选的，第二共识机制与第

一共识机制不同;第二共识机制与第三共识机制相同,为DPoS共识机制。

[0036] 本实施例中,如果第一区块确认通过,则说明该第一区块被大多数区块链节点认同,即第一区块的区块标识与大多数节点都认可的前一个区块的区块标识是连续的。前一个区块,理论上应该是前一个区块生成节点所形成的最后一个区块,但有可能因为网络传输时延或其他故障等,导致一个或多个节点没有收到最后一个区块进行验证存储。下面以图1B的情况为例进行说明。

[0037] 如图1B和1C所示,基于DPoS共识机制预先确定每个备选区块生成节点的区块生成周期,各个备选区块生成节点轮换的作当前区块生成节点,且采用PBFT共识机制对产生的第一区块进行验证。以当前区块生成节点为B节点,前一区块生成节点为A节点,且节点A在其所在区块生成周期形成了5个区块为例进行说明。

[0038] 如图1B,若节点B全部接收到了节点A所形成的5个区块,在其区块生成周期开始,基于本地区块链的末尾区块即节点A形成的第5个区块,形成第一区块,也就是B节点形成的第6个区块;节点B采用PBFT共识机制在区块链网络中确认第一区块,如果第一区块确定通过,则说明大多数节点都认可节点B形成的第6个区块的区块标识与前一区块(第5个区块)的区块标识是连续的,也就是说大多数节点都接收到了节点A的第5个区块。且由于当前区块生成节点是基于前一个区块生成节点所形成的最后一个区块的区块标识形成的第一区块,即当前区块生成节点与前一区块生成节点交界处不存在分叉。

[0039] 如图1C,若节点B未完全接收到了节点A所形成的5个区块(假设未接收到第5个区块),在其区块生成周期开始,基于本地区块链的末尾区块即节点A形成的第4个区块,形成第一区块,也就是B节点形成的第5个区块;节点B采用PBFT共识机制在区块链网络中确认第一区块,如果第一区块确定通过,则说明大多数节点都认可节点B形成的第5个区块的区块标识与本地区块链中最后一个区块(A节点的第4个区块)的区块标识是连续的,也就是说大多数节点都未接收到了节点A的第5个区块。此时,节点A形成的第5个区块将被丢弃,节点B形成的第5个区块直接连接到节点A形成的第4个区块的后面。

[0040] 如果至少一个第一区块确认不通过,则说明在切换当前区块生成节点时,各区块链节点所确认的前一个节点的最后一个区块是不同的,因此,有大量节点无法确认新区块生成节点所生成的第一个区块。即第一区块的区块标识与前一个区块生成节点所形成的最后一个区块的区块标识是不连续的,此时当前区块生成节点将执行下述至少一项操作:1)停止当前区块生成节点在区块生成周期的区块生成操作;2)在等待设定时间后,返回执行形成第一区块的操作并进行区块确认;3)在达到设定条件时,放弃形成的第一区块,基于本地区块链的末尾区块形成第二区块,并采用第二共识机制进行验证。其中,设定条件为达到设定等待时长或第一区块确认不通过的次数达到设定上限值;设定等待时长是指当前区块生成节点从区块生成周期开始,允许重复执行第一区块形成及确认操作最大时限;设定上限值可以依据当前区块生成节点历史区块生成周期内所形成区块的数量等确定。

[0041] 如果至少一个第一区块确认不通过,当前区块生成节点将停止继续形成第二区块的操作;并在等待设定时间后,可以返回执行重新形成第一区块的操作,并采用第一共识机制在区块链网络中确认重新形成的第一区块;若重新形成的第一区块确认通过,则执行步骤S120继续形成至少一个第二区块及区块验证的操作;若重新形成的第一区块仍然确认不通过,且等待时长达到设定等待时长或第一区块确认不通过的次数达到设定上限值,则默

认当前区块生成节点接收到了前一区块生成节点所形成的最后一个区块即本地区块链的末尾区块，当前区块生成节点将放弃形成的第一区块，并基于本地区块链的末尾区块的区块标识等形成第二区块，直至区块生成周期结束为止，将形成的各第二区块顺序在区块链网络中传输，以请求区块链节点进行区块验证。当然，当前区块生成节点也可以不放弃第一区块，而直接不经反馈确认即认可第一区块。

[0042] 继续参见图1C，以当前区块生成节点为B节点，前一区块生成节点为A节点，且A节点形成了5个区块为例进行说明。由于网络传输时延等问题，若B节点未接收到A节点的第5个区块，则B节点当前形成的第一区块，也就是B节点形成的第5个区块，如果B节点形成的第5个区块确认不通过，则说明大多数节点不认可B节点形成的第5个区块的区块标识与本地区块链中最后一个区块的区块标识连续；B节点将停止执行第6个区块生成操作；若B节点在等待设定时间后，例如5s后，B节点基于节点A形成的第5个区块重新执行第一区块的生成操作并进行区块确认，若确认通过，则说明B节点当前已接收到A节点形成的第5个区块，此时第一区块为第6个区块，如图1B所示，并执行后续步骤S120；若B节点基于节点A形成的第4个区块重新执行第一区块的生成操作并进行区块确认，若确认通过，则说明大多数节点都未接收到了节点A的第5个区块，此时节点B形成的第5个区块直接连接到节点A形成的第4个区块的后面。

[0043] 此外，若B节点在每次达到等待设定时间后，B节点基于节点A形成的第4个区块执行上述第一区块的生成操作并进行区块确认，且第一区块确认一直不通过，并且此时达到设定条件，B节点可以放弃或不放弃当前形成的第一区块，也就是B节点形成的第5个区块，默认接收到A节点发送的第5个区块，将第5个区块作为本地区块链的末尾区块，形成第6个区块，以及区块生成周期内的所有其他第二区块。

[0044] 如果第一区块确认通过，当前区块生成节点可以在其区块生成周期内，继续形成一个或多个第二区块，直至区块生成周期结束为止；当前区块生成节点在形成一个或多个第二区块后，可以依据本地存储的通信机制，采用第二共识机制将一个或多个第二区块按照形成顺序传输到区块链网络，以使各区块链节点对接收到的区块进行区块验证，并在验证通过后存储在本地区块链上。可选的，形成至少一个第二区块，并采用第二共识机制进行区块验证可以包括：形成至少两个第二区块，直至区块生成周期结束为止；自形成第一个第二区块后，将各第二区块顺序在区块链网络中传输，以请求区块链节点进行区块验证。

[0045] 需要说明的是，当前区块生成节点本地存储的通信机制规定了当前区块生成节点向区块链网络传输各第二区块的方式，如可以是一个一个传输，还可以是一起传输，也可以是固定数量如5个第二区块传输一次等。

[0046] 本发明实施例提供的技术方案，在当前区块生成节点的区块生成周期开始后，先采用第一共识机制对当前区块生成节点形成的第一区块进行反馈确认，并在第一区块确认通过后，在区块生成周期内继续形成多个第二区块，降低了由于网络传输时延、计算时延等问题造成分叉的现象，提升了用户体验；本实施例基于第一共识机制和第三共识机制确定的区块生成周期，为解决分叉现象提供了一种简单有效的解决方案。同时，当前区块生成节点可以采用第二共识机制对形成的第二区块进行区块验证，第二共识机制可以与第一共识机制不同，从而发挥第二共识机制的优势。

[0047] 实施例二

[0048] 图2为本发明实施例二提供的一种区块链的区块生成方法的流程图，本实施例在上述实施例的基础上，进一步对采用第一共识机制在区块链网络中确认第一区块进行解释说明，其中，本实施例中所采用的第一共识机制可以是BFT、PBFT、SBFT、DBFT中的任意一个，如可以是PBFT或BFT。参见图2，该具体包括如下步骤：

[0049] S210，在当前区块生成节点的区块生成周期开始后，形成至少一个第一区块。

[0050] S220，将第一区块的信息在区块链网络中传输，以请求其他区块链节点进行签名确认。

[0051] 其中，第一区块的信息是指能够唯一识别第一区块的信息，可以是整个区块数据，也可以是第一区块的区块标识。为了缓解区块传输压力，第一区块的信息优选为第一区块的区块标识，而区块标识是依据区块头中的部分或全部信息确定的。示例性的，将第一区块的信息在区块链网络中传输，以请求其他区块链节点进行签名确认可以包括：将第一区块中区块头的部分或全部信息，在区块链网络中传输，以请求其他区块链节点进行签名确认。其中，区块头中的信息可以包括前一区块标识、区块创建的时间戳、随机数、目标哈希及该区块内的事务数据所建立的梅克尔树根等。

[0052] 具体的，当前区块生成节点将第一区块中区块头的部分或全部信息传输到区块链网络中，以请求其他区块链节点进行签名确认；其他区块链节点接收到当前区块生成节点发送的第一区块中区块头的部分或全部信息后，先依据区块头的部分或全部信息确定第一区块的区块标识，查看第一区块的区块标识是否与前一区块的区块标识连续，若连续，则采用私钥对接收到的信息进行签名确认；若不连续，则不进行签名确认或反馈不包括第一区块的信息的签名消息等。

[0053] S230，接收其他区块链节点反馈的签名消息。

[0054] 其中，签名消息中可以包括第一区块的信息、确认签名以及发送该签名消息的区块链节点的节点标识等。可选的，签名消息的数量小于或等于参与签名确认的区块链节点数量。具体的，在当前区块生成节点将第一区块信息传输至区块链网络中，以请求其他区块链节点对第一区块的信息进行签名确认之后，当前区块生成节点将接收区块链中其他区块链节点反馈的签名消息。

[0055] S240，根据接收到的签名消息确定第一区块的确认结果。

[0056] 具体的，由于签名消息是区块链节点采用私钥进行签名得到的，因此，本步骤中，当前区块生成节点接收到其他区块链节点反馈的签名消息后，需采用各签名消息对应的区块链节点的公钥对各签名消息进行解密；而后可以依据各解密后的签名消息，统计确认第一区块的区块链节点数量，若确认第一区块的区块链节点数量超过参与签名确认的区块链节点数量的一半或预先设定的比例值，则确定第一区块的确认结果为确认通过；否则确定第一区块得确认结果为确认不通过。

[0057] 示例性的，根据接收到的签名消息确定第一区块的确认结果可以包括：如果根据接收到的签名消息确定出，确认第一区块的区块链节点大于设定阈值，则确认结果为确认通过；否则确认结果为确认不通过。其中，设定阈值是指预先依据区块链网络中节点的数量设定的比例值，可根据实际情况进行修正。

[0058] 为了降低区块链分叉的概率，以及保证区块数据的安全；本实施例中，可选的，根据接收到的签名消息确定第一区块的确认结果还可以包括：针对每个签名消息，采用发送

签名消息的区块链节点的公钥对签名消息进行解密，以获取第一区块的信息；将获取的第一区块信息与本地存储的第一区块信息进行比对；若比对一致，则该签名消息的确认结果为确认通过；根据各个签名消息的确认结果确定第一区块的确认结果。

[0059] 具体的，针对每个签名消息，当前区块生成节点可以依据该签名消息中包括的节点标识获取对应的区块链节点的公钥，采用该区块链节点的公钥对该签名消息进行解密，若无法解密或解密后不包括任何内容，则剔除该签名消息；若解密成功，则从解密成功的签名消息中获取第一区块的信息；将从该签名消息中获取的第一区块信息与本地存储的第一区块信息进行比较，若两者一致，则确认该签名消息的确认结果为确认通过；若不一致，则确认该签名消息的确认结果为确认不通过。当前区块生成节点在确认获取的各签名消息的确认结果后，可以统计各签名消息的确认结果，依据统计结果确定第一区块的确认结果。可选的，若统计结果中确认通过的区块链节点所占的比例大于设定阈值，则确定第一区块的确认结果为确认通过；否则确定第一区块的确认结果为确认不通过。

[0060] S250，如果确认结果为确认通过，则将签名消息中的确认签名携带在第一区块中，并将第一区块在区块链网络中传输，以添加至区块链中。

[0061] 本步骤中，若当前区块生成节点确定第一区块的确认结果为确认通过，则从确认结果为确认通过的签名消息中提取对应的确认签名，将各确认签名添加到第一区块中，并将第一区块传输到区块链网络中，以请求其他区块链节点将第一区块添加到各自的本地区块链中。其他节点可以对区块中各个签名消息进行解密和验证，以确定该区块是否经过大多数节点的确认。

[0062] S260，如果第一区块确认通过，则在区块生成周期内，继续形成至少一个第二区块，并采用第二共识机制进行区块验证。

[0063] 本发明实施例提供的技术方案，在当前区块生成节点的区块生成周期开始后，基于BPFT或PFT先共识后写入的特点，对当前区块生成节点形成的第一区块进行反馈确认，并在第一区块确认通过后，将第一区块添加到区块链中，而后在区块生成周期内继续形成多个第二区块，能够保证添加至区块链上的区块是唯一的，降低了由于网络传输时延、计算时延等问题造成分叉的现象，提升了用户体验；本实施例基于第一共识机制和第三共识机制确定的区块生成周期，为解决分叉现象提供了一种简单有效的解决方案。

[0064] 实施例三

[0065] 图3为本发明实施例三提供的一种区块链的区块生成装置的结构示意图，该装置可配置于区块链的区块生成节点中，可执行本发明任意实施例所提供的区块链的区块生成方法，具备执行方法相应的功能模块和有益效果。如图3所示，该装置包括：

[0066] 第一区块形成模块310，用于在当前区块生成节点的区块生成周期开始后，形成至少一个第一区块；

[0067] 第一区块确认模块320，用于采用第一共识机制在区块链网络中确认第一区块，其中，第一共识机制为各区块链节点反馈确认的共识方式；

[0068] 第二区块验证模块330，用于如果第一区块确认通过，则在区块生成周期内，继续形成至少一个第二区块，并采用第二共识机制进行区块验证。

[0069] 本发明实施例提供的技术方案，在当前区块生成节点的区块生成周期开始后，先采用第一共识机制对当前区块生成节点形成的第一区块进行反馈确认，并在第一区块确认

通过后，在区块生成周期内继续形成多个第二区块，降低了由于网络传输时延、计算时延等问题造成分叉的现象，提升了用户体验；同时，当前区块生成节点可以采用第二共识机制对形成的第二区块进行区块验证，第二共识机制可以与第一共识机制不同，从而发挥第二共识机制的优势。

[0070] 示例性的，上述装置还可以包括：

[0071] 区块周期确定模块，用于在当前区块生成节点的区块生成周期开始之前，采用第三共识机制确定至少两个备选区块生成节点，并分别确定每个备选区块生成节点的区块生成周期，其中，各备选区块生成节点切换地作为当前区块生成节点。

[0072] 示例性的，第一区块确认模块320可以包括：

[0073] 信息传输单元，用于将第一区块的信息在区块链网络中传输，以请求其他区块链节点进行签名确认；

[0074] 签名消息接收单元，用于接收其他区块链节点反馈的签名消息；

[0075] 确认结果确定单元，用于根据接收到的签名消息确定第一区块的确认结果；

[0076] 区块传输单元，用于如果确认结果为确认通过，则将签名消息中的确认签名携带在第一区块中，并将第一区块在区块链网络中传输，以添加至区块链中。

[0077] 示例性的，信息传输单元具体用于：

[0078] 将第一区块中区块头的部分或全部信息，在区块链网络中传输，以请求其他区块链节点进行签名确认。

[0079] 示例性的，确认结果确定单元具体用于：

[0080] 如果根据接收到的签名消息确定出，确认第一区块的区块链节点大于设定阈值，则确认结果为确认通过。

[0081] 示例性的，确认结果确定单元还具体用于：

[0082] 针对每个签名消息，采用发送签名消息的区块链节点的公钥对签名消息进行解密，以获取第一区块的信息；

[0083] 将获取的第一区块信息与本地存储的第一区块信息进行比对；

[0084] 若比对一致，则该签名消息的确认结果为确认通过；

[0085] 根据各个签名消息的确认结果确定第一区块的确认结果。

[0086] 示例性的，第一共识机制可以为PBFT或BFT。

[0087] 示例性的，第二区块验证模块330具体用于：

[0088] 形成至少两个第二区块，直至区块生成周期结束为止；

[0089] 自形成第一个第二区块后，将各第二区块顺序在区块链网络中传输，以请求区块链节点进行区块验证。

[0090] 示例性的，如果至少一个第一区块确认不通过，则第一区块确认模块320还可以用于执行下述至少一项操作：

[0091] 停止当前区块生成节点在区块生成周期的区块生成操作；

[0092] 在等待设定时间后，返回执行形成所述第一区块的操作并进行区块确认；

[0093] 在达到设定条件时，放弃形成的所述第一区块，基于本地区块链的末尾区块形成第二区块，并采用第二共识机制进行验证。

[0094] 示例性的，设定条件为达到设定等待时长或第一区块确认不通过的次数达到设定

上限值。

[0095] 可选的，第三共识机制可以为DPoS。

[0096] 实施例四

[0097] 图4为本发明实施例四提供的一种设备的结构示意图。图4示出了适于用来实现本发明实施方式的示例性设备12的框图。图4显示的设备12仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。设备12典型的是承担区块链系统节点功能的计算设备。

[0098] 如图4所示，设备12以通用计算设备的形式表现。设备12的组件可以包括但不限于：一个或者多个处理器或者处理单元16，系统存储器28，连接不同系统组件(包括系统存储器28和处理单元16)的总线18。

[0099] 总线18表示几类总线结构中的一种或多种，包括存储器总线或者存储器控制器，外围总线，图形加速端口，处理器或者使用多种总线结构中的任意总线结构的局域总线。举例来说，这些体系结构包括但不限于工业标准体系结构(ISA)总线，微通道体系结构(MAC)总线，增强型ISA总线、视频电子标准协会(VESA)局域总线以及外围组件互连(PCI)总线。

[0100] 设12典型地包括多种计算机系统可读介质。这些介质可以是任何能够被设备12访问的可用介质，包括易失性和非易失性介质，可移动的和不可移动的介质。

[0101] 系统存储器28可以包括易失性存储器形式的计算机系统可读介质，例如随机存取存储器(RAM)30和/或高速缓存存储器32。设备12可以进一步包括其它可移动/不可移动的、易失性/非易失性计算机系统存储介质。仅作为举例，存储系统34可以用于读写不可移动的、非易失性磁介质(图4未显示，通常称为“硬盘驱动器”)。尽管图4中未示出，可以提供用于对可移动非易失性磁盘(例如“软盘”)读写的磁盘驱动器，以及对可移动非易失性光盘(例如CD-ROM,DVD-ROM或者其它光介质)读写的光盘驱动器。在这些情况下，每个驱动器可以通过一个或者多个数据介质接口与总线18相连。系统存储器28可以包括至少一个程序产品，该程序产品具有一组(例如至少一个)程序模块，这些程序模块被配置以执行本发明各实施例的功能。

[0102] 具有一组(至少一个)程序模块42的程序/实用工具40，可以存储在例如系统存储器28中，这样的程序模块42包括但不限于操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。程序模块42通常执行本发明所描述的实施例中的功能和/或方法。

[0103] 设备12也可以与一个或多个外部设备14(例如键盘、指向设备、显示器24等)通信，还可与一个或者多个使得用户能与该设备12交互的设备通信，和/或与使得该设备12能与一个或多个其它计算设备进行通信的任何设备(例如网卡，调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口22进行。并且，设备12还可以通过网络适配器20与一个或者多个网络(例如局域网(LAN)，广域网(WAN)和/或公共网络，例如因特网)通信。如图所示，网络适配器20通过总线18与设备12的其它模块通信。应当明白，尽管图中未示出，可以结合设备12使用其它硬件和/或软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0104] 处理单元16通过运行存储在系统存储器28中的程序，从而执行各种功能应用以及数据处理，例如实现本发明实施例所提供的区块链的区块生成方法。

[0105] 实施例五

[0106] 本发明实施例五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，该程序被处理器执行时可实现上述实施例所提供的区块链的区块生成方法。该计算机可读存储介质，可以配置于区块链节点上。

[0107] 本发明实施例的计算机存储介质，可以采用一个或多个计算机可读的介质的任意组合。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。计算机可读存储介质例如可以是——但不限于——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(非穷举的列表)包括：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中，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。

[0108] 计算机可读的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。计算机可读的信号介质还可以是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。

[0109] 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、电线、光缆、RF等等，或者上述的任意合适的组合。

[0110] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明操作的计算机程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如Java、Smalltalk、C++，还包括常规的过程式程序设计语言—诸如”C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)—连接到用户计算机，或者，可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0111] 注意，上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员会理解，本发明不限于这里所述的特定实施例，对本领域技术人员来说能够进行各种明显的变化、重新调整和替代而不会脱离本发明的保护范围。因此，虽然通过以上实施例对本发明进行了较为详细的说明，但是本发明不仅仅限于以上实施例，在不脱离本发明构思的情况下，还可以包括更多其他等效实施例，而本发明的范围由所附的权利要求范围决定。

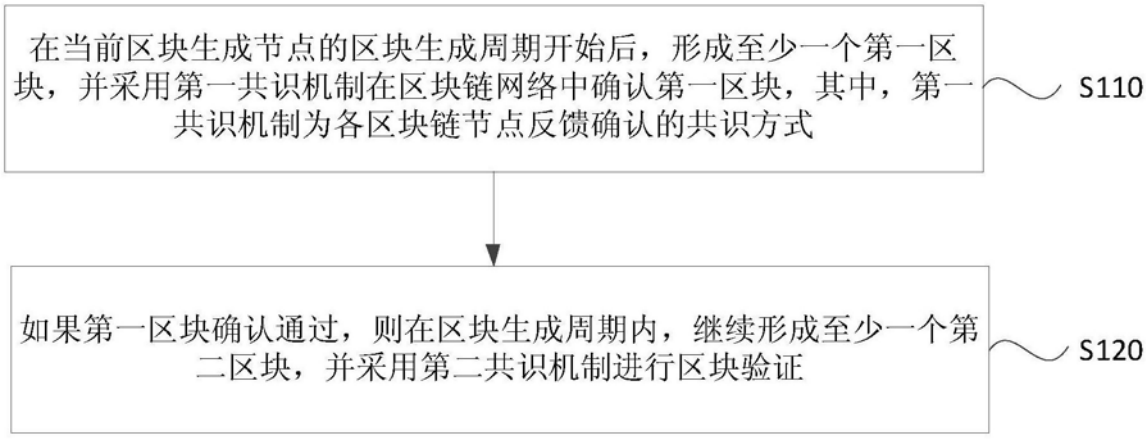

在当前区块生成节点的区块生成周期开始后，形成至少一个第一区块，并采用第一共识机制在区块链网络中确认第一区块，其中，第一共识机制为各区块链节点反馈确认的共识方式
S110
如果第一区块确认通过，则在区块生成周期内，继续形成至少一个第二区块，并采用第二共识机制进行区块验证
S120

图1A

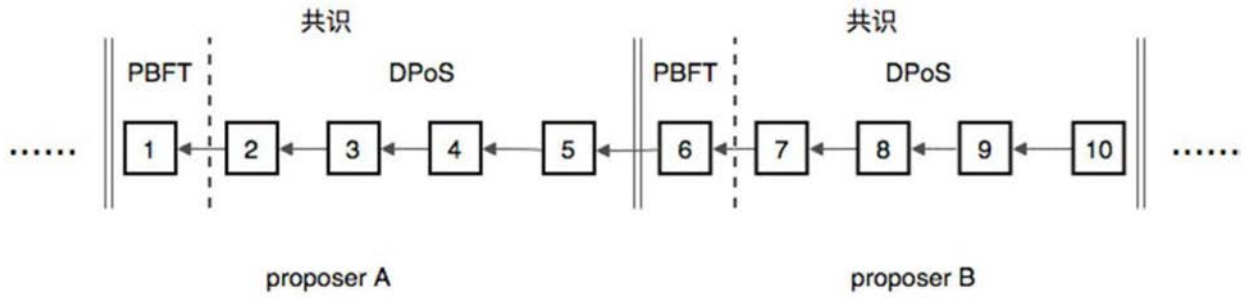

共识
共识
PBFT
DPoS
PBFT
DPoS
1
2
3
4
5
6
7
8
9
10
proposer A
proposer B

图1B

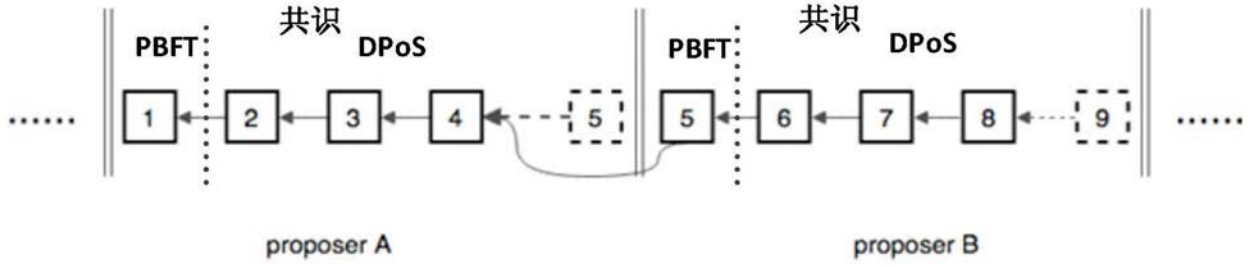

共识
共识
PBFT
DPoS
PBFT
DPoS
1
2
3
4
5
5
6
7
8
9
proposer A
proposer B

图1C

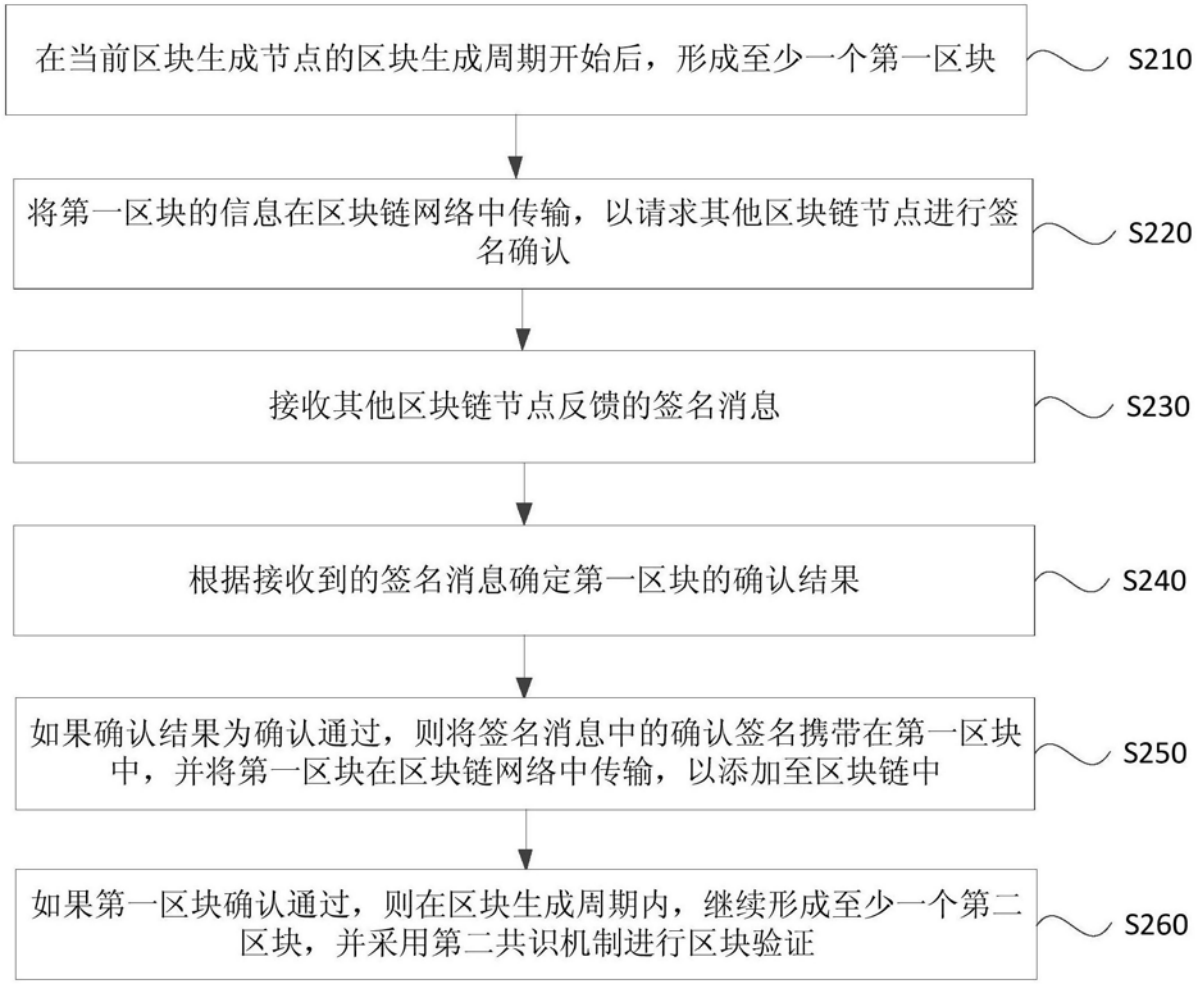

在当前区块生成节点的区块生成周期开始后，形成至少一个第一区块
S210
将第一区块的信息在区块链网络中传输，以请求其他区块链节点进行签名确认
S220
接收其他区块链节点反馈的签名消息
S230
根据接收到的签名消息确定第一区块的确认结果
S240
如果确认结果为确认通过，则将签名消息中的确认签名携带在第一区块中，并将第一区块在区块链网络中传输，以添加至区块链中
S250
如果第一区块确认通过，则在区块生成周期内，继续形成至少一个第二区块，并采用第二共识机制进行区块验证
S260

图2


310
320
330
第一区块形成模块
第一区块确认模块
第二区块验证模块

图3

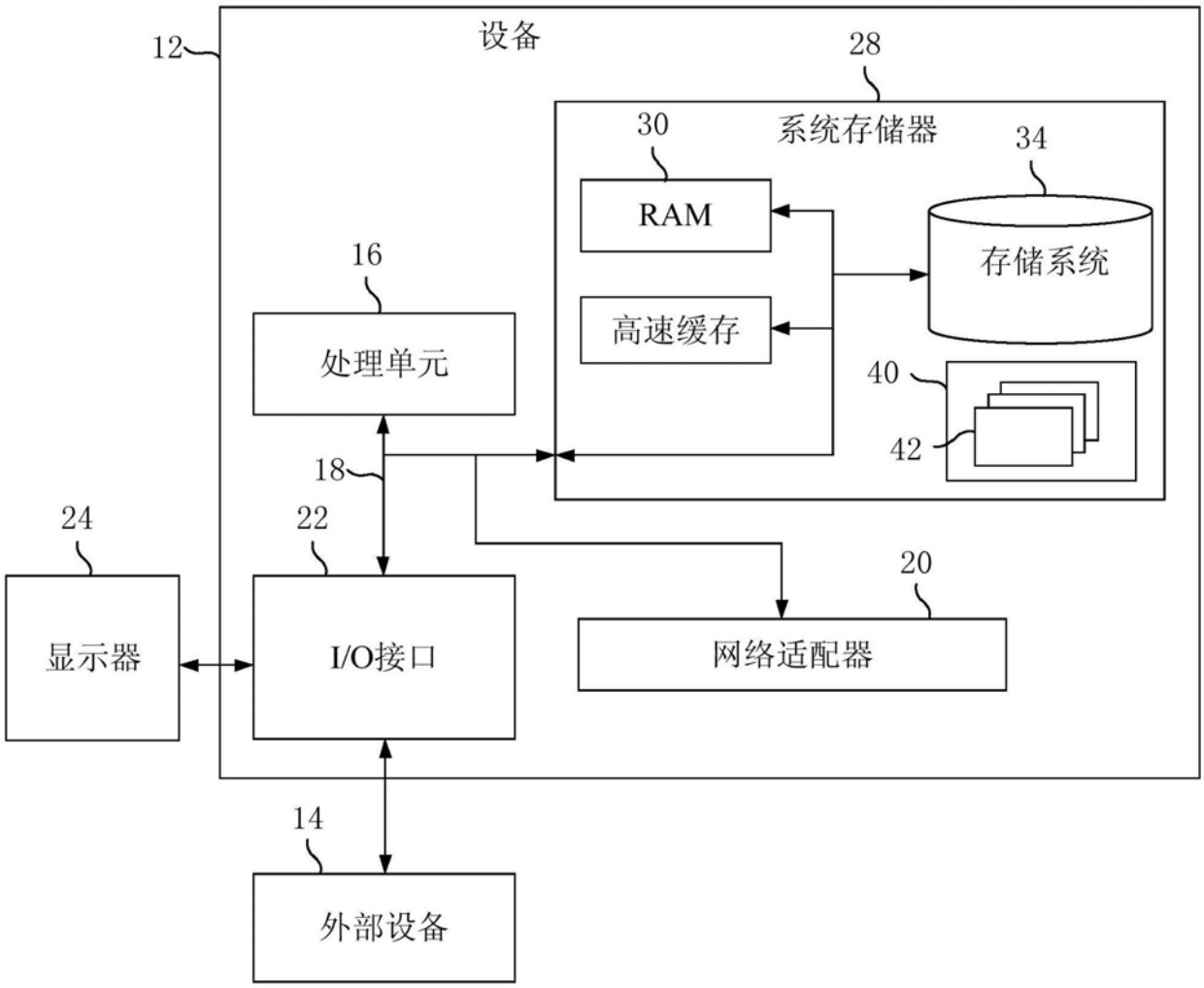

12
设备
28
30
系统存储器
34
RAM
存储系统
16
高速缓存
处理单元
40
42
18
24
22
20
显示器
I/O接口
网络适配器
14
外部设备

图4