(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112262422 B
(45)授权公告日 2024.07.12

(21)申请号 201980038788.6
(22)申请日 2019.03.31
(65)同一申请的已公布的文献号
申请公布号 CN 112262422 A
(43)申请公布日 2021.01.22
(30)优先权数据
2018-077368 2018.04.13 JP
(85)PCT国际申请进入国家阶段日
2020.12.11
(86)PCT国际申请的申请数据
PCT/JP2019/014401 2019.03.31
(87)PCT国际申请的公布数据
WO2019/198548 JA 2019.10.17

(73)专利权人 比特飞翔区块链株式会社
地址 日本东京都港区赤坂九丁目7番1号
(72)发明人 小宫山峰史
(74)专利代理机构 上海华诚知识产权代理有限公司 31300
专利代理师 刘煜

(51)Int.Cl.
*G09C 1/00*(2006.01)
*H04L 9/32*(2006.01)
(56)对比文件
CN 106533661 A,2017.03.22
CN 107038578 A,2017.08.11
审查员 施龙权

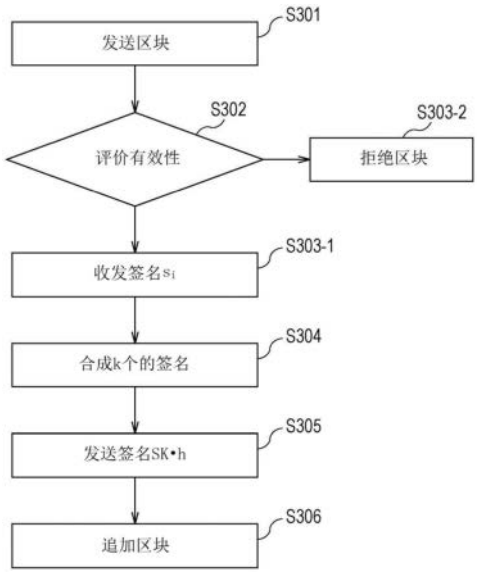
权利要求书2页 说明书7页 附图3页

(54)发明名称

# 区块链网络及用于其的确定方法

(57)摘要

在与区块的选择有关的共识形成需要多个节点的签名的区块链网络中,降低与形成了共识的区块有关的签名处理的复杂度。在完成建立之后,第一节点(110)将包括所生成的区块的第一消息发送到N个节点(S301)。各节点基于共识形成的规则,评价该区块的有效性(S302)。在有效的情况下,该节点向各节点发送具有签名($s_i$)的第二消息,该签名是针对基于私钥份额f($x_i$)的共识形成对象的区块的哈希值h的签名(S303-1)。当在第j个节点上聚集了k个签名之后,该节点合成这些签名并生成对应于公钥(PK)的签名(S304)。共识形成对象的区块被附加签名(SK•h)而追加到各节点的区块链中(S306)。




CN 112262422 B

1.一种用于区块链网络的选择的确定方法,所述区块链网络中,N个节点参与到与区块的所述选择有关的共识形成并需要k个节点的签名,其中,N是2以上的整数,k是满足2≤k≤N的整数,该方法的特征在于,

第i个节点包括:

向所述N个节点发送区块的步骤;

从第j个节点接收将所述区块的哈希值h与未知的(k-1)次多项式f(x)的$x=x_j$时的值即$f(x_j)$相乘而得的签名$s_j$的步骤,其中,j是满足1≤j≤N的整数;

根据与k个节点有关的坐标$(x_j,s_j)$算出f(0)·h的步骤;

将算出的f(0)·h作为与公钥对应的签名附加到所述区块的步骤;以及

将被附加所述签名的所述区块追加到区块链中,确定所述区块的所述选择的步骤,

其中,i是满足1≤i≤N的整数,

这里,$G_1$是以$g_1$为生成元的循环群,$G_2$是以$g_2$为生成元的循环群,$G_T$是以$g_T$为生成元的循环群,能够定义从$G_1\times G_2$向$G_T$的双线性映射e,并且,能够将提供共识形成对象的区块的所述哈希值h的哈希函数定义为从任意的数据向循环群$G_2$的映射,此外,第i个节点能够访问1到N的各j中的$x_j$的值,第j个节点能够访问$f(x_j)$的值。

2.根据权利要求1所述的方法,其特征在于,

f(0)·h的计算使用拉格朗日插值进行。

3.根据权利要求1或2所述的方法,其特征在于,

判定是否具有k个以上的签名,在判定结果为肯定的情况下,执行所述f(0)·h的计算。

4.一种计算机程序产品,包括用于使第i个节点执行用于区块链网络的选择的确定方法的程序,在所述区块链网络中,N个节点参与到与区块的所述选择有关的共识形成并需要k个节点的签名,其中,i是满足1≤i≤N的整数,N是2以上的整数,k是满足2≤k≤N的整数,该计算机程序产品的特征在于,

在所述确定方法中,所述第i个节点包括:

向所述N个节点发送区块的步骤;

从第j个节点接收将所述区块的哈希值h与未知的(k-1)次多项式f(x)的$x=x_j$时的值即$f(x_j)$相乘而得的签名$s_j$的步骤,其中,j是满足1≤j≤N的整数;

根据与k个节点有关的坐标$(x_j,s_j)$算出f(0)·h的步骤;

将算出的f(0)·h作为与公钥对应的签名附加到所述区块的步骤;以及

将被附加所述签名的所述区块追加到区块链中,确定所述区块的所述选择的步骤,

这里,$G_1$是以$g_1$为生成元的循环群,$G_2$是以$g_2$为生成元的循环群,$G_T$是以$g_T$为生成元的循环群,能够定义从$G_1\times G_2$向$G_T$的双线性映射e,并且,能够将提供共识形成对象的区块的所述哈希值h的哈希函数定义为从任意的数据向循环群$G_2$的映射,此外,第i个节点能够访问1到N的各j中的$x_j$的值,第j个节点能够访问$f(x_j)$的值。

5.一种构成区块链网络的第i个节点,所述区块链网络中,N个节点参与到与区块的选择有关的共识形成并需要k个节点的签名,其中,i是满足1≤i≤N的整数,N是2以上的整数,k是满足2≤k≤N的整数,该节点的特征在于,

向所述N个节点发送区块;

从第j个节点接收将所述区块的哈希值h与未知的(k-1)次多项式f(x)的$x=x_j$时的值即

$f(x_j)$相乘而得的签名$s_j$,其中,j是满足$1 \leq j \leq N$的整数;

根据与k个节点有关的坐标$(x_j, s_j)$算出$f(0) \cdot h$,将算出的$f(0) \cdot h$作为与公钥对应的签名附加到所述区块的;以及

将被附加所述签名的所述区块追加到区块链中,确定所述区块的所述选择,

这里,$G_1$是以$g_1$为生成元的循环群,$G_2$是以$g_2$为生成元的循环群,$G_T$是以$g_T$为生成元的循环群,能够定义从$G_1 \times G_2$向$G_T$的双线性映射e,并且,能够将提供共识形成对象的区块的所述哈希值h的哈希函数定义为从任意的数据向循环群$G_2$的映射,此外,第i个节点能够访问1到N的各j中的$x_j$的值,第j个节点能够访问$f(x_j)$的值。

# 区块链网络及用于其的确定方法

## 技术领域

[0001] 本发明涉及一种区块链网络及用于该区块链网络的确定方法,更详细地说,涉及一种在与区块的选择有关的共识形成中需要多个节点的签名的区块链网络以及用于该区块链网络的该选择的确定方法。

## 背景技术

[0002] 作为能够代替以往的基于中央集权性的第三方机关的授信机制的技术,区块链受到关注。被称为“区块”的数据单位被提供给参与到针对该区块的共识形成的多个节点,在各个节点中评价(evaluate)该区块的有效性(validity)。通过满足规定条件,各节点从多个有可能的区块中判定对该区块形成了选择的共识(consensus)而接受该区块。更具体地,该区块被追加到各节点所具有的区块链中。由任一节点对各节点提供成为共识形成对象的区块。

[0003] 这里,以怎样的步骤形成共识、或者将什么作为用于共识形成的规定条件这样的共识算法决定区块链网络的可靠性和性能。根据共识算法,例如因通信状况、供电等物理原因而导致无法正常工作的故障(也被称为“良性故障(benign failure)”。)的允许数量不同,另外,不遵循共识算法中定义的规定规则这样的任意的一切故障(也被称为“拜占庭故障(Byzantine failure)”。)的允许数量不同。作为某个节点不遵循规定规则的情况,除了物理上的理由之外,还可以举出存在对该节点的非法访问的情况、该节点的管理者自身有非法意图的情况等。

[0004] 作为共识算法的一例,可以举出需要参与共识形成的N个(N为2以上的整数)节点中的k个(k为满足2≤k≤N的整数)节点的签名的算法。如果考虑N=5、k=3的例子,这意味着需要参与共识形成的节点中的过半数节点的签名。然后,为了表示共识形成完毕并对于共识形成对象的区块确定了选择该区块,需要附加k个以上的签名作为依据。

## 发明内容

[0005] 发明要解决的问题

[0006] 然而,根据N和k的值的不同,能够使k个节点的签名满足该共识算法中的规定条件的节点的组合可以想到许多,这可能对于形成了共识的区块而言使签名处理变得复杂。因为例如为了事后验证(verify)某个区块的签名,必须单独地确认附加到该区块的多个签名是否满足规定的条件。

[0007] 本发明鉴于这样的问题而做出,其目的在于,在与区块的选择有关的共识形成需要多个节点的签名的区块链网络以及用于该区块链网络的该选择的确定方法中,降低与形成了共识的区块有关的签名处理的复杂度。

[0008] 用于解决问题的技术手段

[0009] 为了实现这样的目的,本发明的第一方式是一种用于区块链网络的密钥生成方法,在所述区块链网络中,N个节点参与到与区块的选择有关的共识形成并需要k个节点的

签名,其中,N是2以上的整数,k是满足2≤k≤N的整数,该方法的特征在于,第i个节点包括:决定式(1)所表示的(k-1)次多项式$f_i(x)$的步骤;从第j个节点接收$f_j(x_i)$以及0到k-1的各m中的$a_{jm}\cdot g_1$的值的步骤,其中,j是满足1≤j≤N的整数,$x_i$是被提供给第i个节点的整数,$g_1$是循环群$G_1$的生成元;在(k-1)次多项式f(x)未知的状态下算出式(2)所表示的SKi的步骤;以及算出式(3)所表示的PKi的步骤,其中,i是满足1≤i≤N的整数。

[0010] [式1]

[0011] $$f_i(x)=\sum_{m=0}^{k-1}a_{im}x^m \qquad (1)$$

[0012] [式2]

[0013] $$SKi=f(x_i)=\sum_{j=1}^{N}f_j(x_i) \qquad (2)$$

[0014] [式3]

[0015] $$PKi=SKi\cdot g_1=\left(\sum_{j=1}^{N}f_j(x_i)\right)g_1=\left(\sum_{j=1}^{N}\left(\sum_{m=0}^{k-1}a_{jm}{x_i}^m\right)\right)g_1=\sum_{m=0}^{k-1}\left(\sum_{j=1}^{N}a_{jm}g_1\right){x_i}^m \qquad (3)$$

[0016] 另外,本发明的第二方式的特征在于,在第一方式中,还包括从第j个节点接收$PK_j$的步骤。

[0017] 另外,本发明的第三方式的特征在于,在第一方式中,还包括针对第j个节点算出$PK_j$的步骤。

[0018] 另外,本发明的第四方式的特征在于,在第二或第三方式中,还包括根据与k个节点有关的坐标$(x_j,PK_j)$算出$f(0)\cdot g_1$的步骤。

[0019] 另外,本发明的第五方式的特征在于,在第四方式中,$f(0)\cdot g_1$的计算使用拉格朗日插值进行。

[0020] 另外,本发明的第六方式的特征在于,在第四或第五方式中,还包括将计算出的所述f(0)·g1作为公钥PK发送的步骤。

[0021] 另外,本发明的第七方式的特征在于,在第六方式中,所述发送包括所述公钥PK向所述区块链网络外的发送。

[0022] 另外,本发明的第八方式是一种用于区块链网络的选择的确定方法,所述区块链网络中,N个节点参与到与区块的所述选择有关的共识形成并需要k个节点的签名,其中,N是2以上的整数,k是满足2≤k≤N的整数,其特征在于,第i个节点包括:向所述N个节点发送区块的步骤;从第j个节点接收将所述区块的哈希值h与未知的(k-1)次多项式f(x)的$x=x_j$时的值即$f(x_j)$相乘而得的签名$s_j$的步骤,其中,j是满足1≤j≤N的整数;根据与k个节点有关的坐标$(x_j,s_j)$算出$f(0)\cdot h$的步骤;将算出的$f(0)\cdot h$作为与公钥对应的签名附加到所述区块的步骤;以及将被附加所述签名的所述区块追加到区块链中,确定所述区块的所述选择的步骤,其中,i是满足1≤i≤N的整数。这里,$G_1$是以$g_1$为生成元的循环群,$G_2$是以$g_2$为生成元的循环群,$G_T$是以$g_T$为生成元的循环群,能够定义从$G_1\times G_2$向$G_T$的双线性映射e,并且,可以将提供共识形成对象的区块的所述哈希值h的哈希函数定义为从任意的数据向循环群$G_2$

的映射。此外,第i个节点能够访问1到N的各j中的$x_j$的值,第j个节点能够访问$f(x_j)$的值。

[0023] 另外,本发明的第九方式的特征在于,在第八方式中,f(0)·h的计算使用拉格朗日插值进行。

[0024] 另外,本发明的第十方式的特征在于,在第八或第九方式中,判定是否具有k个以上的签名,在判定结果为肯定的情况下,执行所述f(0)·h的计算。

[0025] 发明效果

[0026] 根据本发明的一个方式,能够通过使用N个的一组私钥份额(秘密鍵シェア)中的规定数量k个的私钥份额的签名,来生成未知的私钥的签名,由此通过单一的签名来表示已经达成了与区块的选择有关的共识。

## 附图说明

[0027] 图1是表示本发明的第一实施方式中的区块链网络的图。

[0028] 图2是本发明的第一实施方式中的密钥生成方法的流程图。

[0029] 图3是本发明的第二实施方式中的与区块的选择有关的确定方法的流程图。

## 具体实施方式

[0030] 以下,参照附图详细说明本发明的实施方式。

[0031] (第一实施方式)

[0032] 图1表示本发明的第一实施方式的区块链网络。网络100例如将N设为5,具有第一节点110、第二节点120、第三节点130、第四节点140以及第五节点150。如针对第一节点110所图示,各节点是具备通信接口等通信部111、处理器、CPU等处理部112、以及包括存储器、硬盘等存储装置或存储介质的存储部113的计算机,并且能够通过执行规定的程序来实现以下说明的各处理,该节点110有时包括一个或多个的装置或服务器,另外,该程序有时包括一个或多个程序,并且可以记录在计算机可读存储介质中作为非临时性的程序产品。关于其他的节点,其硬件结构也相同。以下,以第一节点110为中心进行说明,但在其他节点中也可以进行相同的处理。另外,有时网络100中也包含不参与共识形成的节点。

[0033] 在规定的程序中,规定了与共识算法有关的规则以及与建立(セットアップ)有关的规则,可以预先存储在能够由存储部113或第一节点110经由网络访问的存储装置或存储介质中。

[0034] 将为了使参与共识形成的N个节点从能够相互通信的状态转移到能够执行与区块的选择有关的共识形成的状态而应该执行的过程称为“建立”。当在网络100的外部或内部接收到建立的请求时,开始建立,在图1中示出了从外部发送该请求的例子。该请求可以包括共识形成所需的签名数量k,还可以预先在与建立有关的规则中定义。另外,该请求可以包括对参与共识形成的N个节点的指定,该指定还可以预先在与建立有关的规则中定义。

[0035] 当以任意的形式确定了N和k的值并且前进到执行建立过程时,各节点保持被分配给参与共识形成的节点整体的一个公钥、被分配给参与共识形成的各节点的N个公钥份额、以及被分配给该节点的一个私钥份额。另外,各节点也保持N和k的值或k/N的值。N的值也可以根据公钥份额的数量求出。

[0036] 私钥与公钥具有能够通过该公钥来验证由该私钥签名的明文的关系,关于私钥份

额和与其对应的公钥份额也同样。这里,“私钥份额”是指以使能够使用N个的一组私钥份额中的规定数量k个的私钥份额的签名来生成私钥的签名的方式,指定所生成的一组私钥份额中的任意一个。因此,可以基于k个私钥份额来生成对应于公钥的签名,而无需知道该私钥,并且可以将该签名附加到作为共识形成对象的区块。所附加的签名可以通过公钥验证。

[0037] 如果进一步地说明图1的例子,则将分配给网络100整体的一个公钥记为PK(Public Key的简称),将与该公钥对应的私钥记为SK(Secret Key的简称),将分别分配给第一节点110、第二节点120、第三节点130、第四节点140、第五节点150的公钥份额和私钥份额分别记为PK1和SK1、PK2和SK2、PK3和SK3、PK4和SK4、PK5和SK5。在建立之后,例如,第一节点将PK、PK1到PK5以及SK1存储在该节点的存储部113中,或者存储在能够与该节点通信的存储装置或存储介质中。所存储的这些数据在以后的共识形成或其确定过程中,可以从该节点访问。

[0038] 这里,公钥PK是最终附加的签名的验证所需要的,但是在建立阶段有时也不生成公钥PK。进行签名的验证的节点或装置只要在验证时具有公钥PK即可,在初始设定的时间点未必需要网络100的各节点具有公钥PK。

[0039] 图2表示本实施方式的这些密钥生成方法的流程。这里,作为一例,考虑(k-1)次多项式f(x),并将$f(x_i)$的值(i是表示第i个节点的1到N的整数,$x_i$是任意的整数)作为针对各节点的私钥份额SKi。

[0040] 首先,第i个节点决定以$a_{im}$(m是从0到k-1的整数)为系数的(k-1)次多项式$f_i(x)$(S201)。各节点可以根据建立规则,选择或生成$a_{im}$并存储,由此计算$f_i(x)$。

[0041] [式4]

[0042] $$f_i(x)=\sum_{m=0}^{k-1}a_{im}x^m$$

[0043] 接着,第i个节点使用循环群$G_1$的生成元$g_1$,向其他节点发送0至k-1的各m中的$a_{im}\cdot g_1$的值或包含该值的消息(S202)。另外,第i个节点向第j个节点(j是1到N的整数)发送$f_i(x_j)$的值或包含该值的消息。这里,$f_i(x_j)$的发送可以在m和$a_{im}\cdot g_1$之前发送,也可以与m和$a_{im}\cdot g_1$同时发送。

[0044] 生成元$g_1$设为被存储在各节点中并且是已知的,或者被从任何节点提供给参与共识形成的N个节点使得N个节点分别能够访问而使用。同样地,对第i个节点提供私钥份额$f(x_i)$的整数$x_i$的值设为N个节点分别能够访问并使用。例如,这些值可以存储在各节点的存储部中,或者存储在从各节点可以访问的存储装置或存储介质中。

[0045] 然后,在第j个节点中,对1到N的i加上$f_i(x_j)$,算出$f(x_j)$、即私钥份额$SK_j$(S204)。多项式f(x)定义如下:

[0046] [式5]

[0047] $$f(x)=\sum_{m=0}^{k-1}a_m x^m$$

[0048] 虽然对任何一个节点而言都不知道,但通过如下式那样考虑$f(x_j)$,各节点不知道f(x)自身就能够在各节点中算出$f(x_j)$的值。

[0049] [式6]

[0050] $$f(x_j)=\sum_{i=1}^{N}f_i(x_j)=\sum_{i=1}^{N}\left(\sum_{m=0}^{k-1}a_{im}\,{x_j}^m\right)=\sum_{m=0}^{k-1}\left(\sum_{i=1}^{N}a_{im}\right){x_j}^m=\sum_{m=0}^{k-1}a_m{x_j}^m$$

[0051] 另外,由于各节点可以在其自己的节点处算出m和$a_{im}\cdot g_1$,并且已经接收到其他节点的m和$a_{im}\cdot g_1$,因此可以根据下式算出$SK_j\cdot g_1$来作为公钥份额$PK_j$(S205)。

[0052] [式7]

[0053] $$SKj\cdot g_1=f(x_j)\cdot g_1=\left(\sum_{m=0}^{k-1}a_m{x_j}^m\right)g_1=\left(\sum_{m=0}^{k-1}\left(\sum_{i=1}^{N}a_{im}\right){x_j}^m\right)g_1=\sum_{m=0}^{k-1}\left(\sum_{i=1}^{N}a_{im}g_1\right){x_j}^m$$

[0054] 因为m和$a_{im}\cdot g_1$以及$x_i$对于所有的i都是已知的,所以对于全部的节点而言,不知道f(x)也能够通过该公式算出公钥份额PKi。

[0055] 这样得到的公钥份额和私钥份额的配对,是将提供共识形成对象的区块的哈希值h的哈希函数作为从任意的数据向以$g_2$为生成元的循环群$G_2$的映射,将h乘以$SK_j$而得的$SK_j\cdot h$作为签名$s_j$,通过定义从$G_1\times G_2$向以$g_T$为生成元的循环群$G_T$的映射e且是满足下式的双线性映射,可知作为加密方式成立。此处,a和b是任意整数。

[0056] [式8]

[0057] $$e(ag_1,bg_2)=g_T^{ab}$$

[0058] 即,在第i个节点中,在从第j个节点接收到共识形成对象的区块的哈希值h和签名$s_j$时,使用根据上述算法已知的公钥份额$PK_j$。

[0059] [式9]

[0060] $e(PKj,h)=e(SKj\cdot g_1,h)=e(g_1,SKj\cdot h)=e(g_1,s_j)$

[0061] 因此,可以使用已知的生成元$g_1$来验证从第j个节点接收到的签名$s_j$。可以通过预先在建立规则中定义哈希函数,在各节点中根据共识形成对象的区块算出哈希值。

[0062] 在上述说明中,是以将(k-1)次多项式函数f(x)的值定为私钥份额,将该私钥份额乘以循环群的生成元而得的值作为公钥份额的签名方式为前提,但只要能够使用N个一组的私钥份额中的规定数量k个的私钥份额的签名来生成私钥的签名,则也可以采用不同的签名方式。另外,此时优选可以在各个节点中分散地生成各个私钥份额,而不是将由网络100的任一节点或其外部的节点所生成的一组私钥份额提供给各节点。

[0063] 另外,在上述的说明中,以第j个节点中的公钥份额$PK_j$以及私钥份额$SK_j$为例进行了说明,但在对以第i个节点为中心而在第i个节点进行的处理进行记述的情况下,当然下标将被适当变更。

[0064] (第二实施方式)

[0065] 图3示出了本发明的第二实施方式的与区块的选择有关的确定方法的流程。从完成建立的状态开始,第一节点110生成区块,并向参与共识形成的N个节点发送包含该区块的第一消息(S301)。发送节点自身也可以接收该区块。这里,可以在节点之间直接或间接地收发消息,可以向构成网络100的其他节点发送与共识形成有关的数据并且从其他节点接收数据。

[0066] 接收到第一消息的各节点根据各自具有的程序中规定的共识形成的规则,评价该

区块的有效性(S302)。有效性评价的细节可以包括发送者是否是合法的发送节点、区块的数据格式是否满足与用途相应的规定格式或其他规定条件、是否产生分支等各种规则,并且可以因节点的不同而存在不同的规则。另外,在进行有效性的评价之后,也可以需要与其他节点的消息的收发。

[0067] 在被评价为有效的情况下,则该节点向各节点发送具有签名$s_i$的第二消息,该签名$s_i$是针对基于该节点能够访问的私钥份额$f(x_i)$的共识形成对象的区块的哈希值h的签名(S303-1)。签名可以通过将提供给该节点的私钥份额乘以哈希值来进行。发送目的地也可以包含自身节点。在被评价为无效的情况下,拒绝该区块(S303-2)。

[0068] 当在第j个节点聚集了k个签名之后,该节点合成这些签名,并生成对应于公钥PK的签名(S304)。具体而言,各节点定期或间断地判定k/N的条件是否得到满足,在得到满足的情况下,能够根据接收到的k个或k个以上的私钥份额的签名,算出$f(0)\cdot h$作为与公钥PK对应的私钥SK的签名$SK\cdot h$。这里,如果k个以上的点$(x_i,f(x_i))$已知,则可以唯一地确定(k-1)次多项式$f(x)$,使用将$f(0)$的值认为是未知的私钥SK的值的情况。如果根据k个签名已知k个点$(x_i,f(x_i)\cdot h)$,则得以确定函数$f(x)\cdot h$。$f(0)\cdot h$的计算例如可以使用拉格朗日插值来进行。

[0069] 此外,例如能够通过拉格朗日插值,根据k个以上的点$(x_j,PK_j)=(x_j,f(x_j)\cdot g_1)$算出公钥PK,这可以在建立阶段进行并根据需要分发,也可以在验证时或验证之前由进行签名的验证的网络100的内部或外部的节点或装置基于k个公钥份额$PK_j$生成。

[0070] 然后,如果需要,则将所生成的单个签名$SK\cdot h$广播或发送至其它节点(S305)。由于已经进行了k个以上的节点的有效性的评价,所以可以在成功合成的时间点将区块追加到该节点所具有的区块链中,但作为一例,成功合成后的节点可以将合成后的签名发送到其它节点,然后各节点可以根据接收到规定数量以上的合成后的签名这一情况,追加区块。

[0071] 最后,共识形成对象的区块被附加签名$SK\cdot h$而追加到各节点的区块链中(S306)。由此,该区块在网络100中的选择确定。

[0072] 在上述说明中,考虑了对各节点提供一个私钥份额的情况,但也可以考虑对一个节点提供的份额数设为多个的情况。另外,在上面的说明中,尽管没有提及作为有效性评价对象的区块的细节,但是该区块可以包括一个或多个交易,或者可以包括任意的一个或多个数据。而且,关于具有多个节点的计算机网络对于未必形成链的一个或多个数据的有效性的评价,也可以应用本发明的精神。

[0073] 此外,需要注意的是,如果没有“仅基于”,“仅根据××”、“仅××的情况”这样“仅”的记载,则假定在本说明书中可以考虑附加信息。

[0074] 另外,为了慎重起见,即使在某些方法、程序、终端、装置、服务器或系统(以下为“方法等”)中有进行与本说明书中记述的动作不同的动作的方面,但本发明的各方式以与本说明书中描述的动作中的任一个相同的动作为对象,另外指出,存在与本说明书中描述的动作不同的动作的该方法等并不排除在本发明各方面的范围外。

[0075] 符号说明

[0076] 100 网络

[0077] 110 第一节点

[0078] 111 通信部

[0079] 112 处理部

[0080] 113 存储部

[0081] 120 第二节点

[0082] 130 第三节点

[0083] 140 第四节点

[0084] 150 第五节点。

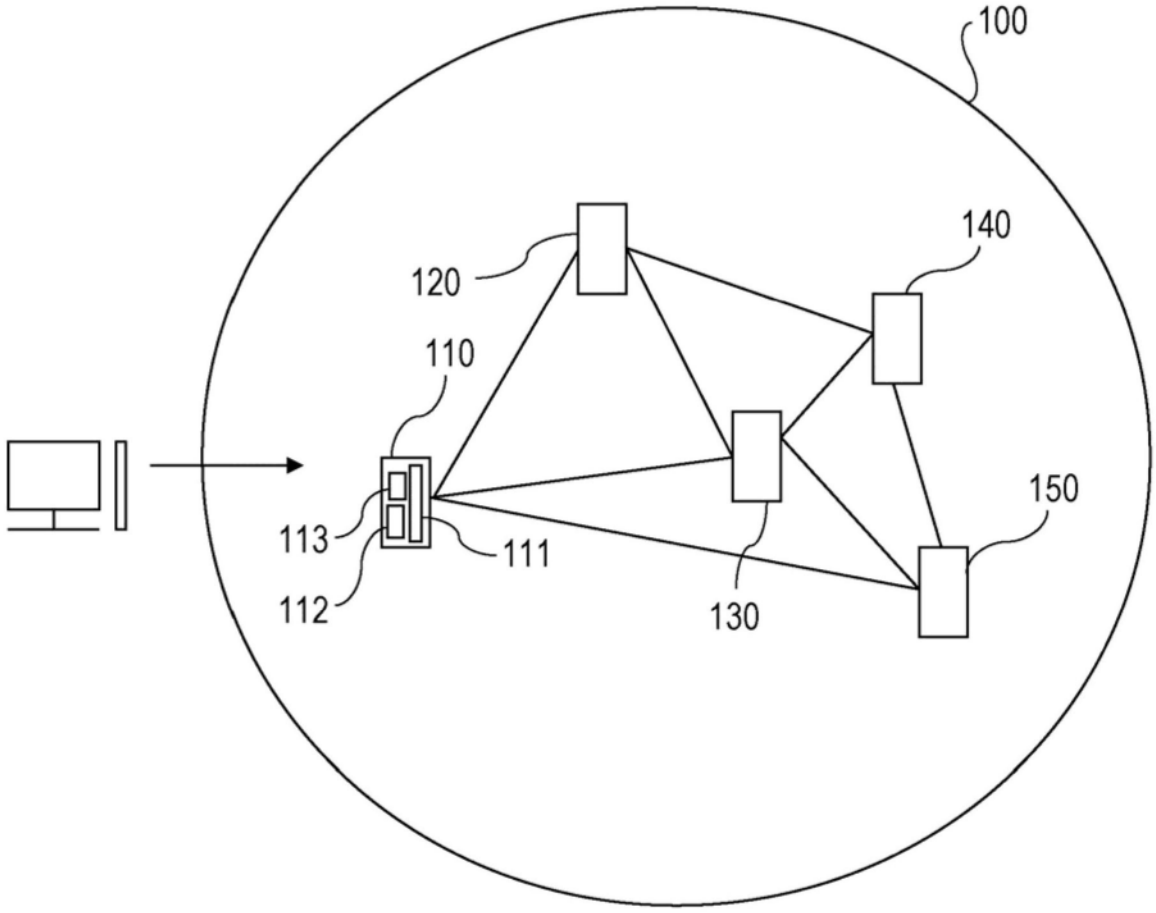



图1

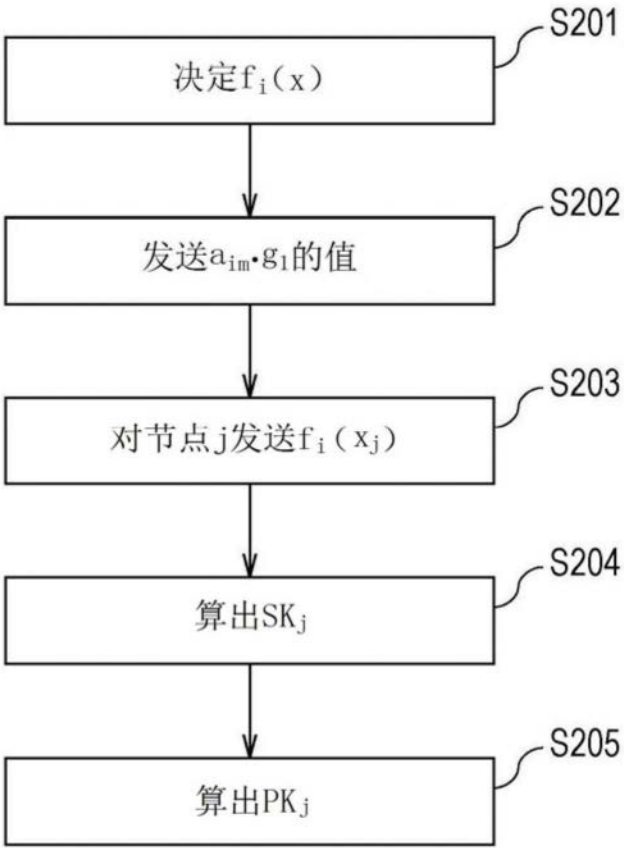

S201
决定$f_i(x)$
S202
发送$a_{im} \cdot g_l$的值
S203
对节点j发送$f_i(x_j)$
S204
算出$SK_j$
S205
算出$PK_j$

图2

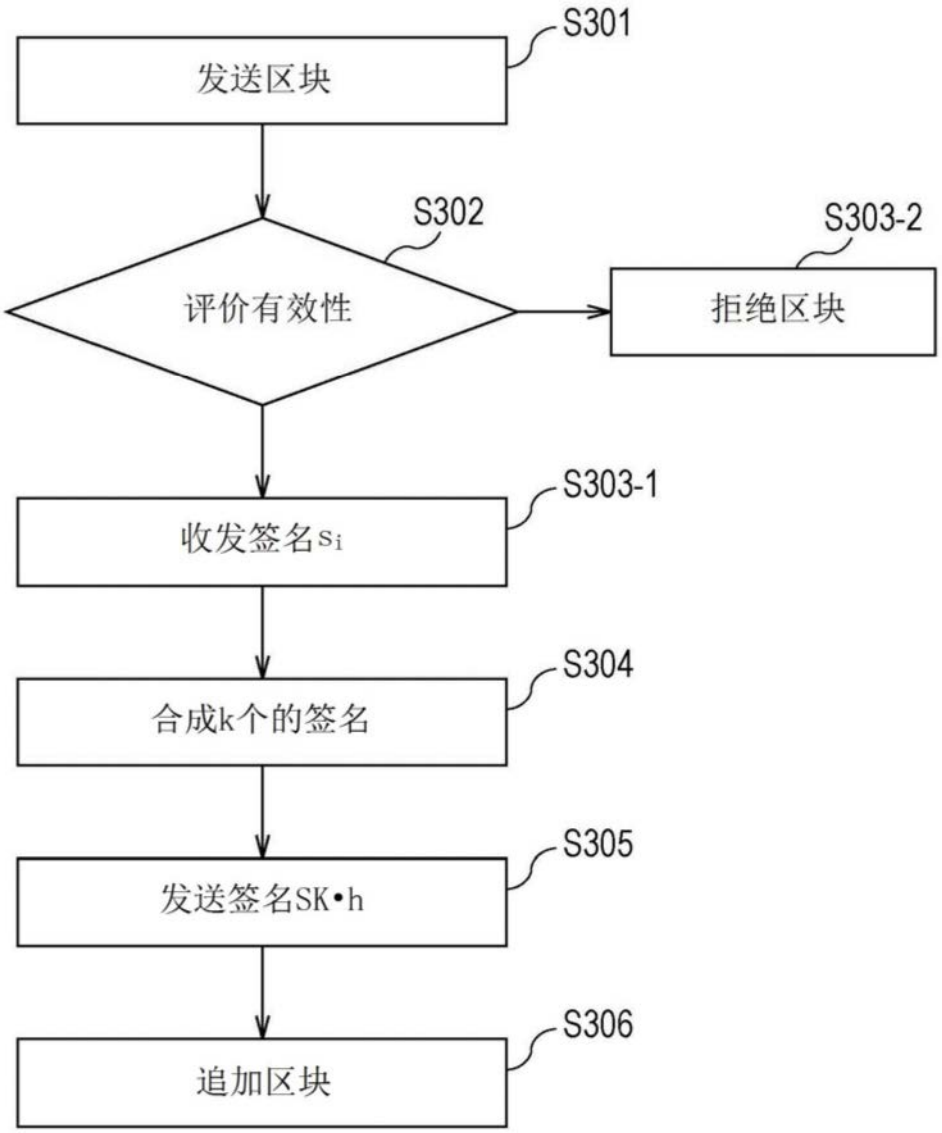

S301
发送区块
S302
评价有效性
S303-2
拒绝区块
S303-1
收发签名$s_i$
S304
合成k个的签名
S305
发送签名SK•h
S306
追加区块

图3