

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2022 年 5 月 12 日 (12.05.2022)



(10) 国际公布号
WO 2022/095779 A1

(51) 国际专利分类号:
H04L 67/01 (2022.01)

(21) 国际申请号: PCT/CN2021/126991

(22) 国际申请日: 2021 年 10 月 28 日 (28.10.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011231832.6 2020 年 11 月 6 日 (06.11.2020) CN

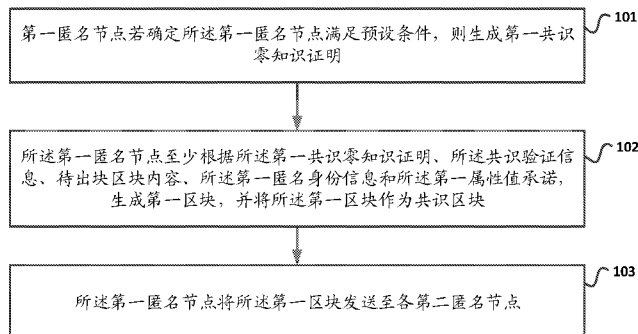
(71) 申请人: 深圳前海微众银行股份有限公司
(**WEBANK CO., LTD.**) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518027 (CN)。香港科技大学 (**THE HONG KONG UNIVERSITY OF SCIENCE**

AND TECHNOLOGY) [CN/CN]; 中国香港特别行政区九龙清水湾, Hong Kong (CN)。

(72) 发明人: 黄晨宇 (**HUANG, Chenyu**); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518027 (CN)。张俊麒 (**ZHANG, Junqi**); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518027 (CN)。胡朝新 (**HU, Chaixin**); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518027 (CN)。苏小康 (**SU, Xiaokang**); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518027 (CN)。张开翔 (**ZHANG, Kaixiang**); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518027 (CN)。范瑞彬 (**FAN, Ruibin**); 中国广东省深圳

(54) **Title:** POW-BASED BLOCKCHAIN CONSENSUS METHOD AND APPARATUS

(54) 发明名称: 一种基于 POW 的区块链共识方法及装置



101 If it is determined that a first anonymous node meets a preset condition, the first anonymous node generates a first consensus zero-knowledge proof
102 The first anonymous node generates a first block at least according to the first consensus zero-knowledge proof, consensus verification information, content of a block to be outputted, first anonymous identity information and a first attribute value commitment, and takes the first block as a consensus block
103 The first anonymous node sends the first block to each second anonymous node

图 1

(57) **Abstract:** Disclosed are a POW-based blockchain consensus method and apparatus. The method comprises: if it is determined that a first anonymous node meets a preset condition, the first anonymous node generates a first consensus zero-knowledge proof; the first anonymous node generates a first block at least according to the first consensus zero-knowledge proof, consensus verification information, content of a block to be outputted, first anonymous identity information and a first attribute value commitment, and takes the first block as a consensus block; and the first anonymous node sends the first block to each second anonymous node. When the described method is applied to financial technology (Fintech), block consensus can be carried out without disclosing actual identity information, so the nodes that have higher attribute values are not vulnerable to targeted malicious attacks.

(57) **摘要:** 本发明公开了一种基于 POW 的区块链共识方法及装置，其中方法为：第一匿名节点若确定所述第一匿名节点满足预设条件，则生成第一共识零知识证明；所述第一匿名节点至少根据所述第一共识零知识证明、所述共识验证信息、待出块区块内容、所述第一匿名身份信息和所述第一属性值承诺，生成第一区块，并将所述第一区块作为共识区块；所述第一匿名节点将所述第一区块发送至各第二匿名节点。上述方法应用于金融科技(Fintech)时，可以在不泄露实际身份信息情况下进行区块共识，那么较高属性值的节点不容易受到针对性的恶意攻击。

市前海深港合作区前湾一路1号A栋201室,
Guangdong 518027 (CN)。 张黔(ZHANG, Qian);
中国广东省深圳市前海深港合作区前湾一路1
号A栋201室, Guangdong 518027 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司
(TDIP & PARTNERS); 中国北京市西城区裕民路
18号北环中心A座2002, Beijing 100029 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家
保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,
BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,
CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT,
JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,
LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,
MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,
PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

一种基于POW的区块链共识方法及装置

相关申请的交叉引用

本申请要求在2020年11月06日提交中国专利局、申请号为202011231832.6、
申请名称为“一种基于POW的区块链共识方法及装置”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。

技术领域

本发明涉及金融科技（Fintech）领域中的区块链（blockchain）领域，尤
其涉及一种基于 POW 的区块链共识方法及装置。

背景技术

随着计算机技术的发展，越来越多的技术应用在金融领域，传统金融业
正在逐步向金融科技（Fintech）转变，但由于金融行业的安全性、实时性要
求，也对技术提出的更高的要求。目前金融科技领域和区块链（blockchain）
领域联系较为紧密。基于工作量证明(Proof-of-Work, PoW)共识算法的区块链
是一种较为常见的区块链。基于 PoW 共识算法的区块链的共识过程中，共识
区块是面向区块链的用户公开的。

但一些信息是较为敏感的信息，如共识区块由哪个区块链节点出块，常
表征了区块链节点的属性值，如果泄露可能导致被攻击者锁定高属性值的目
标。这就给区块链带来了一定的隐私风险，这样以来，常出块的区块链节点
容易受到恶意攻击，从而拖垮整个区块链的性能，这是一个亟待解决的问题。

发明内容

本发明提供一种基于 POW 的区块链共识方法及装置，解决了现有技术中
常出块的区块链节点容易受到恶意攻击的问题。

第一方面，本发明提供一种基于 POW 的区块链共识方法，包括：第一匿

名节点若确定所述第一匿名节点满足预设条件，则生成第一共识零知识证明；所述第一共识零知识证明至少用于验证以下信息的正确性：共识验证信息、第一属性值承诺和第一匿名身份信息；所述第一属性值承诺是至少根据第一实际属性值得到的隐匿信息；所述第一匿名身份信息是至少根据所述第一匿名节点的第一实际身份信息得到的；所述预设条件是根据 PoW 共识算法的特性设定的；所述第一匿名节点至少根据所述第一共识零知识证明、所述共识验证信息、待出块区块内容、所述第一匿名身份信息和所述第一属性值承诺，生成第一区块，并将所述第一区块作为共识区块；所述第一匿名节点将所述第一区块发送至各第二匿名节点。

上述方式下，由于所述第一区块是至少根据所述第一共识零知识证明、所述共识验证信息、待出块区块内容、所述第一匿名身份信息和所述第一属性值承诺生成的，通过第一共识零知识证明可以在不泄露实际身份信息和实际属性值的基础上，对所述第一区块进行验证，从而可以在不泄露实际身份信息情况下进行区块共识，那么较高属性值的节点不容易受到针对性的恶意攻击。

可选的，所述第一匿名节点按照以下方式确定所述第一匿名节点满足预设条件：所述第一匿名节点根据所述第一实际属性值确定所述第一匿名节点的第一挖矿难度值；所述第一匿名节点在预设数域内持续更新挖矿因子，并根据所述第一挖矿难度值和所述挖矿因子确定所述第一匿名节点是否满足预设条件；所述预设条件是基于所述第一挖矿难度值设定的；所述挖矿因子满足所述预设条件的概率和所述第一实际属性值呈正相关。

上述方法中，上述方法中，从而在遵循 POW 共识算法基础上设置所述预设条件，自适应地在区块链中选择出块的节点，提升了选择出块节点的效率。

可选的，所述根据所述第一挖矿难度值和所述挖矿因子确定所述第一匿名节点是否满足预设条件，包括：所述第一匿名节点根据所述挖矿因子和所述待出块区块内容，生成第一哈希值；若所述第一匿名节点确定所述第一哈希值小于第一挖矿难度值，则确定所述第一匿名节点满足预设条件。

上述方法中，通过在每个区块中设置第一挖矿难度值，且通过第一挖矿难度值自适应地选择出共识区块，提升了选择出块节点的效率。

可选的，所述第一匿名节点在预设数域内持续更新挖矿因子的过程中，在生成的挖矿因子未使得所述第一匿名节点满足所述预设条件的期间，若所述第一匿名节点收到了所述各第二匿名节点中任一第二匿名节点的第二区块，
5 则所述第一匿名节点验证所述第二区块；若验证通过，则所述第一匿名节点将所述第二区块作为共识区块。

上述方法中，在生成的挖矿因子未使得所述第一匿名节点满足所述预设条件的期间，通过所述第二区块的验证，确定其是否为共识区块，从而可以
10 独立地一直更新挖矿因子，如果有通过验证的第二区块则不必生成第一区块，从而提升了共识区块的共识效率。

可选的，所述第一区块为所述区块链的第 i 时期中第三区块与第四区块之间的待共识区块；所述第三区块为所述区块链的第 i 时期中的第一个待共识区块；所述第四区块为所述区块链的第 i 时期中的最后一个待共识区块；所述第
15 一匿名身份信息为所述第一匿名节点在所述区块链的第 i 时期的匿名身份信息；所述第一属性值承诺为所述第一匿名节点在所述区块链的第 i 时期的属性值承诺。

上述方式下，通过设置不同时期来绑定匿名身份信息和属性值承诺，而且在第一个区块和第三区块与第四区块之间采用特定的方式生成，从而进一步地增加易出块节点的破解的难度。
20

可选的，在所述区块链的第 i 时期结束后，还包括：所述第一匿名节点生成第二匿名身份信息，作为所述第一匿名节点在所述区块链的第 $i+1$ 时期的匿名身份信息；所述第一匿名节点生成第二属性值承诺，作为所述第一匿名节点在所述区块链的第 $i+1$ 时期的属性值承诺。

上述方式下，在所述区块链的第 i 时期结束后，生成第 $i+1$ 时期的新的匿名身份信息和属性值承诺，从而进一步地增加易出块节点的破解的难度。
25

可选的，所述第三区块是由所述第一匿名节点生成的，所述第一匿名节

点按照以下方式生成第三区块：所述第一匿名节点根据所述第一共识零知识证明、所述共识验证信息、所述第一匿名身份信息和所述第一属性值承诺，生成第三区块。

上述方式下，第一个区块中，只填入所述第一共识零知识证明等必要的身份验证信息，从而节约了第三区块的空间。

可选的，所述第四区块是由所述第一匿名节点生成的，所述第一匿名节点按照以下方式生成第四区块：所述第一匿名节点根据所述第一共识零知识证明、所述共识验证信息、所述待出块区块内容、所述第一匿名身份信息、所述第一属性值承诺、第三匿名身份信息和第三属性值承诺，生成第四区块；所述第三匿名身份信息为在所述区块链的第 $i+1$ 时期中待加入匿名节点的匿名身份信息；所述第三属性值承诺是至少根据所述待加入匿名节点在所述区块链的第 $i+1$ 时期中的实际属性值得到的隐匿信息。

上述方式下，对于第 $i+1$ 时期中待加入匿名节点，直接在第 i 时期的最后一个区块中完成共识，以声明第 $i+1$ 时期中参与区块的合法性，从而增加了区块链的工作效率。

第二方面，本发明提供一种基于 POW 的区块链共识装置，包括：共识模块，用于若确定第一匿名节点满足预设条件，则生成第一共识零知识证明；所述第一共识零知识证明至少用于验证以下信息的正确性：共识验证信息、第一属性值承诺和第一匿名身份信息；所述第一属性值承诺是至少根据第一实际属性值得到的隐匿信息；所述第一匿名身份信息是至少根据第一匿名节点的第一实际身份信息得到的；所述预设条件是根据 PoW 共识算法的特性设定的；以及至少根据所述第一共识零知识证明、所述共识验证信息、待出块区块内容、所述第一匿名身份信息和所述第一属性值承诺，生成第一区块，并将所述第一区块作为共识区块；数据传输模块。用于将所述第一区块发送至各第二匿名节点。

可选的，所述共识模块具体用于：根据所述第一实际属性值确定所述第一匿名节点的第一挖矿难度值；在预设数域内持续更新挖矿因子，并根据所

述第一挖矿难度值和所述挖矿因子确定所述第一匿名节点是否满足预设条件；所述预设条件是基于所述第一挖矿难度值设定的；所述挖矿因子满足所述预设条件的概率和所述第一实际属性值呈正相关。

可选的，所述共识模块具体用于：根据所述挖矿因子和所述待出块区块内容，生成第一哈希值；若确定所述第一哈希值小于第一挖矿难度值，则确定所述第一匿名节点满足预设条件。

可选的，所述共识模块还用于：在预设数域内持续更新挖矿因子的过程中，在生成的挖矿因子未使得所述第一匿名节点满足所述预设条件的期间，若所述数据传输模块收到了所述各第二匿名节点中任一第二匿名节点的第二区块，则验证所述第二区块；若验证通过，则将所述第二区块作为共识区块。

可选的，所述第一区块为所述区块链的第 i 时期中第三区块与第四区块之间的待共识区块；所述第三区块为所述区块链的第 i 时期中的第一个待共识区块；所述第四区块为所述区块链的第 i 时期中的最后一个待共识区块；所述第一匿名身份信息为所述第一匿名节点在所述区块链的第 i 时期的匿名身份信息；所述第一属性值承诺为所述第一匿名节点在所述区块链的第 i 时期的属性值承诺。

可选的，在所述区块链的第 i 时期结束后，所述共识模块还用于：生成第二匿名身份信息，作为所述第一匿名节点在所述区块链的第 $i+1$ 时期的匿名身份信息；生成第二属性值承诺，作为所述第一匿名节点在所述区块链的第 $i+1$ 时期的属性值承诺。

可选的，所述第三区块是由所述第一匿名节点生成的，所述共识模块还用于：按照以下方式生成第三区块：根据所述第一共识零知识证明、所述共识验证信息、所述第一匿名身份信息和所述第一属性值承诺，生成第三区块。

可选的，所述第四区块是由所述第一匿名节点生成的，所述共识模块还用于：按照以下方式生成第四区块：根据所述第一共识零知识证明、所述共识验证信息、所述待出块区块内容、所述第一匿名身份信息、所述第一属性值承诺、第三匿名身份信息和第三属性值承诺，生成第四区块；所述第三匿

名身份信息为在所述区块链的第 $i+1$ 时期中待加入匿名节点的匿名身份信息；
所述第三属性值承诺是至少根据所述待加入匿名节点在所述区块链的第 $i+1$
时期中的实际属性值得到的隐匿信息。

上述第二方面及第二方面各个可选装置的有益效果，可以参考上述第一
5 方面及第一方面各个可选方法的有益效果，这里不再赘述。

第三方面，本发明提供一种计算机设备，包括程序或指令，当所述程序
或指令被执行时，用以执行上述第一方面及第一方面各个可选的方法。

第四方面，本发明提供一种存储介质，包括程序或指令，当所述程序或
指令被执行时，用以执行上述第一方面及第一方面各个可选的方法。

10 本发明的这些方面或其他方面在以下实施例的描述中会更加简明易懂。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中
所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发
15 明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动性
的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例提供的一种基于 POW 的区块链共识方法对应的流程
示意图；

图 2 为本发明实施例提供的一种基于 POW 的区块链共识系统的系统架构
20 示意图；

图 3 为本发明实施例提供的一种基于 POW 的区块链共识方法对应的具体
流程示意图；

图 4 为本发明实施例提供的一种基于 POW 的区块链共识装置的结构示意
图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本

发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

5 下面首先给出本申请中出现的名词及释义。

 ZKP(Zero-Knowledge Proof, 零知识证明): 证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

 zk-SNARK(zero-knowledge succinct non-interactive argument of knowledge, 简洁化的非交互式计算可靠的零知识证明): 是零知识证明的一种实现方式，
10 它允许用户以非交互式的方式提供证明，且该证明可以用很短的时间验证。应用于 Zcash 等匿名电子货币。

 (佩德森)Pedersen 承诺: 一种密码学承诺。包含两个阶段: 在承诺阶段，它允许承诺方通过承诺函数 $COMM(m, r)$ 将消息正整数 m 通过密文的形式发送 r 为随机正整数，它可以保证承诺方不会修改消息的同时对他人隐藏消息本身；
15 在打开阶段，承诺方可以公开消息，接收端以此来验证消息是否和承诺阶段一致。Pedersen 承诺满足隐藏性(Hiding)，绑定性 (Binding) 和同态性(homomorphic)。我们主要会利用其中的同态性即 $COMM(a, b) + COMM(c, d) = COMM(a + c, b + d)$ 。

 客户: 使用区块链进行记账的用户。

20 验证者: 进行交易验证，将认证后的交易打包进区块链的节点。

 ID (Identity, 身份证标识号): 代表验证者的标识号。

 PoW(Proof-of-Work, 工作量证明): 是一种对应服务与资源滥用、或是拒绝服务攻击的经济对策。一般是要求用户进行一些耗时适当的复杂运算，并且答案能被服务方快速验算，以此耗用的时间、设备与能源做为担保成本，
25 以确保服务与资源是被真正的需求所使用。常用于区块链中的公有链。

 在金融机构 (银行机构、保险机构或证券机构) 在进行业务 (如银行的贷款业务、存款业务等) 运转过程中，和区块链 (blockchain) 领域联系较为

紧密。在 PoW 共识算法的区块链中，共识区块是面向区块链的用户公开的。但一些信息是较为敏感的信息，如果泄露可能导致被攻击者锁定高属性值的目标。这就给区块链带来了一定的隐私风险，这种情况不符合银行等金融机构的需求，无法保证金融机构各项业务的高效运转。为此，如图 1 所示，本
5 申请提供一种基于 POW 的区块链共识方法。

步骤 101: 第一匿名节点若确定所述第一匿名节点满足预设条件，则生成第一共识零知识证明。

步骤 102: 所述第一匿名节点至少根据所述第一共识零知识证明、所述共识验证信息、待出块区块内容、所述第一匿名身份信息和所述第一属性值承诺，生成第一区块，并将所述第一区块作为共识区块。
10

步骤 103: 所述第一匿名节点将所述第一区块发送至各第二匿名节点。

步骤 101~步骤 103 中，所述第一共识零知识证明至少用于验证以下信息的正确性：共识验证信息、第一属性值承诺和第一匿名身份信息；所述第一属性值承诺是至少根据第一实际属性值得到的隐匿信息；所述第一匿名身份信息是至少根据所述第一匿名节点的第一实际身份信息得到的；所述预设条件是
15 根据 PoW 共识算法的特性设定的。

一种可选实施方式（以下称为时期的实施方式）中，可以引入时期，所述第一区块为所述区块链的第 i 时期中第三区块与第四区块之间的待共识区块；所述第三区块为所述区块链的第 i 时期中的第一个待共识区块；所述第四区块为所述区块链的第 i 时期中的最后一个待共识区块。
20

所述第一匿名身份信息为所述第一匿名节点在所述区块链的第 i 时期的匿名身份信息；所述第一属性值承诺为所述第一匿名节点在所述区块链的第 i 时期的属性值承诺。

上述方式下，通过设置不同时期来绑定匿名身份信息和属性值承诺，而且在第一个区块即第三区块与最后一个区块即第四区块之间的第一区块，采用特定的方式生成，从而进一步地增加易出块节点的破解的难度。
25

需要说明的是，图 1 示出的方法引入时期后，可以通过图 2 示出的系统

架构具体实现。图 2 示出的系统架构包含三个模块：隐私保护的属性值承诺和数值操作模块，隐私保护的基于属性的共识模块，隐私保护的属性和属性值承诺更换模块。具体工作流程如图 2 所示，通过图 2 示出的系统架构可以在步骤 101~步骤 103 的方法中引入时期。

5 具体来说，将时间分为不同的时期，每个时期（如第 i 时期，是某一个时期）仅允许经过认证的匿名节点（本申请中，也可以称为验证者）加入区块链。在每个时期开始前，当验证者加入区块链后，它将会通过隐私保护的属性和属性值承诺更换模块拥有匿名身份信息和属性值承诺（如属性值承诺为 Pedersen 承诺）。

10 匿名节点（验证者）之间会互相确认在这个时期参与的所有验证者的匿名身份信息和属性值承诺。在时期开始后，每个验证者都会观察其他验证者的行为并通过隐私保护的属性值承诺和数值操作模块来对每一个验证者进行属性值承诺的更新。

15 每经过一段时间（如每次新增的共识区块后），验证者若为领导节点，便将交易和所有验证者更新的属性值承诺打包进入区块中并发布，所有验证者通过隐私保护的共识模块来验证并确认正确的区块并将达成共识的区块加入最终的区块链中。

20 当到了该时期的结束时，验证者可以选择通过隐私保护的属性和属性值承诺更换模块来更换自己的匿名身份信息和属性值承诺，此后验证者可以进入到下一个时期进行区块链的验证和维护；验证者也可以选择退出区块链。

 基于时期的实施方式，第三区块可以按照以下方式生成：

 所述第一匿名节点根据所述第一共识零知识证明、所述共识验证信息、所述第一匿名身份信息和所述第一属性值承诺，生成第三区块。

25 上述方式下，第一个区块中，只填入所述第一共识零知识证明等必要的身份验证信息，从而节约了第三区块的空间。

 基于时期的实施方式，第四区块可以按照以下方式生成：

 所述第一匿名节点根据所述第一共识零知识证明、所述共识验证信息、

所述待出块区块内容、所述第一匿名身份信息、所述第一属性值承诺、第三匿名身份信息和第三属性值承诺，生成第四区块；所述第三匿名身份信息为在所述区块链的第 $i+1$ 时期中待加入匿名节点的匿名身份信息。

所述第三属性值承诺是至少根据所述待加入匿名节点在所述区块链的第 $i+1$ 时期中的实际属性值得到的隐匿信息。

上述方式下，对于第 $i+1$ 时期中待加入匿名节点，直接在第 i 时期的最后一个区块中完成共识，以声明第 $i+1$ 时期中参与区块的合法性，从而增加了区块链的工作效率。

基于时期的实施方式，还可以执行如下步骤：

所述第一匿名节点生成第二匿名身份信息，作为所述第一匿名节点在所述区块链的第 $i+1$ 时期的匿名身份信息；所述第一匿名节点生成第二属性值承诺，作为所述第一匿名节点在所述区块链的第 $i+1$ 时期的属性值承诺。

具体来说，在匿名节点（验证者）工作过程中，它会观察验证者的行为并依此为其他验证者打分，其他验证者亦会对该验证者的行为进行监督并进行打分。在基于承诺的 BFT 共识中，验证者的行为可以定义为对于交易认证的投票，它从每一笔交易认证中获得的承诺值为 $S * V$ 其中 V 是交易金额（正整数）， S 是奖励系数（整数）。

当验证者和最终区块上的该笔交易认证结果交易一致则奖励系数为 1。而当认证结果不一致则为负数 -10，意味着验证者没有正确履行自己的责任或对系统作恶，因此扣除一定分数。本方案主要着重在隐私保护，并不是在如何通过行为进行承诺值计算，因此不会限定承诺值计算的方法且可以适用于保护各种不同的承诺值方案的隐私。

举例来说，在两个区块中该验证者获得的分数为整数 ΔR ，其他验证者可以通过将 $\text{COMM}(\Delta R, 0)$ 加到 $\hat{R}$ 上来得到正确的承诺值承诺。由 Pedersen 承诺的同态性可得 $\text{COMM}(\Delta R, 0) + \hat{R} = \text{COMM}(\Delta R, 0) + \text{COMM}(R, r) = \text{COMM}(R + \Delta R, r)$ ，因此对承诺的加法操作可以将获得的分数正确的加到未被揭示的承诺值 R 上。

一种可选实施方式下，步骤 101 中可以按照以下方式（下面称为挖矿因子的实施方式）确定所述第一匿名节点满足预设条件：

所述第一匿名节点根据所述第一实际属性值确定所述第一匿名节点的第一挖矿难度值；所述第一匿名节点在预设数域内持续更新挖矿因子，并根据所述第一挖矿难度值和所述挖矿因子确定所述第一匿名节点是否满足预设条件。

所述预设条件是基于所述第一挖矿难度值设定的；所述挖矿因子满足所述预设条件的概率和所述第一实际属性值呈正相关。

举例来说，根据所述第一实际属性值 R 确定所述第一匿名节点的第一挖矿难度值 D 的关系为 $R=10*D-1$ ，第一实际属性值 R 为 10，那么第一挖矿难度值 D 便为 99。挖矿因子为 nonce ，预设数域为 $[1,10000]$ ， nonce 在预设数域内随机取值，预设数域按照预设映射关系映射的值域为 $[1, 200]$ ，预设映射关系可以设置为非单调的函数关系，以免第一匿名节点随机取值。预设条件为， nonce 映射得到的数值在区间 $[1,2*D]$ 内，显然， R 越大， D 越大，所述挖矿因子满足所述预设条件的概率就越大。

挖矿因子的实施方式中，具体来说，根据所述第一挖矿难度值和所述挖矿因子确定所述第一匿名节点是否满足预设条件的具体过程可以如下：

所述第一匿名节点根据所述挖矿因子和所述待出块区块内容，生成第一哈希值；若所述第一匿名节点确定所述第一哈希值小于第一挖矿难度值，则确定所述第一匿名节点满足预设条件。

上述实施方式可以通过隐私保护的共识模块实现，本模块可以让匿名节点（验证者）在共识中挖矿的难度和属性值相关。验证者可以通过 zk-SNARK 证明自己的合法性，同时不需要透露自己的属性值给其他验证者，其他验证者可以快速地验证这一证明而不需要知道该验证者的属性值。

该模块的流程如下图 3 所示。

(1)验证者通过自己的属性值决定自己挖掘的难度正整数 D 。例如，当自己的属性在正整数 L_i 和正整数 H_i 之间的时候，它挖掘出的区块的哈希值需要小于

正整数 D_i ;

(2)验证者会将正整数计数值 N (nonce) 从 0 开始增加, 每加一次会判断包含 N 的区块的哈希值是否满足挖掘难度 D , 即 $H(B||N) < D$, 其中 B 为除了共识证明域的区块内容。

5 挖矿因子的实施方式中, 具体来说, 还可能出现如下情形:

所述第一匿名节点在预设数域内持续更新挖矿因子的过程中, 在生成的挖矿因子未使得所述第一匿名节点满足所述预设条件的期间, 若所述第一匿名节点收到了所述各第二匿名节点中任一第二匿名节点的第二区块, 则所述第一匿名节点验证所述第二区块; 若验证通过, 则所述第一匿名节点将所述
10 第二区块作为共识区块。

上述实施方式在图 3 中的步骤如下:

(3)若找到正确的 N , 则验证者用 zk-SNARK 生成 $Z1$, 并将其放在区块的共识证明域上。 $Z1$ 包含了以下信息的证明: 1) $\hat{R}$ 、ID是按照正确的公式生成。
2) 属性值 R 对应的难度 D 是正确的。3) $H(B||N) < D$, 其中 B 为除了公式证明
15 域的区块内容。验证者将正确的区块发送给其他验证者并进行下一轮区块的挖掘。

(4)若验证者还未找到正确的 N 时, 当其在收到其他验证者发送的区块后验证 $\pi1$, 若正确则将该区块加入到区块链中。若不正确则继续寻找 N 。

如图 4 所示, 本发明提供一种基于 POW 的区块链共识装置, 包括: 共识
20 模块 401, 用于若确定第一匿名节点满足预设条件, 则生成第一共识零知识证明; 所述第一共识零知识证明至少用于验证以下信息的正确性: 共识验证信息、第一属性值承诺和第一匿名身份信息; 所述第一属性值承诺是至少根据第一实际属性值得到的隐匿信息; 所述第一匿名身份信息是至少根据第一匿名节点的第一实际身份信息得到的; 所述预设条件是根据 PoW 共识算法的特性设定的; 以及至少根据所述第一共识零知识证明、所述共识验证信息、待
25 出块区块内容、所述第一匿名身份信息和所述第一属性值承诺, 生成第一区块, 并将所述第一区块作为共识区块; 数据传输模块 402。用于将所述第一区

块发送至各第二匿名节点。

可选的，所述共识模块 401 具体用于：根据所述第一实际属性值确定所述第一匿名节点的第一挖矿难度值；在预设数域内持续更新挖矿因子，并根据所述第一挖矿难度值和所述挖矿因子确定所述第一匿名节点是否满足预设条件；所述预设条件是基于所述第一挖矿难度值设定的；所述挖矿因子满足所述预设条件的概率和所述第一实际属性值呈正相关。

可选的，所述共识模块 401 具体用于：根据所述挖矿因子和所述待出块区块内容，生成第一哈希值；若确定所述第一哈希值小于第一挖矿难度值，则确定所述第一匿名节点满足预设条件。

可选的，所述共识模块 401 还用于：在预设数域内持续更新挖矿因子的过程中，在生成的挖矿因子未使得所述第一匿名节点满足所述预设条件的期间，若所述数据传输模块 402 收到了所述各第二匿名节点中任一第二匿名节点的第二区块，则验证所述第二区块；若验证通过，则将所述第二区块作为共识区块。

可选的，所述第一区块为所述区块链的第 i 时期中第三区块与第四区块之间的待共识区块；所述第三区块为所述区块链的第 i 时期中的第一个待共识区块；所述第四区块为所述区块链的第 i 时期中的最后一个待共识区块；所述第一匿名身份信息为所述第一匿名节点在所述区块链的第 i 时期的匿名身份信息；所述第一属性值承诺为所述第一匿名节点在所述区块链的第 i 时期的属性值承诺。

可选的，在所述区块链的第 i 时期结束后，所述共识模块 401 还用于：生成第二匿名身份信息，作为所述第一匿名节点在所述区块链的第 $i+1$ 时期的匿名身份信息；生成第二属性值承诺，作为所述第一匿名节点在所述区块链的第 $i+1$ 时期的属性值承诺。

可选的，所述第三区块是由所述第一匿名节点生成的，所述共识模块 401 还用于：按照以下方式生成第三区块：根据所述第一共识零知识证明、所述共识验证信息、所述第一匿名身份信息和所述第一属性值承诺，生成第三区

块。

可选的，所述第四区块是由所述第一匿名节点生成的，所述共识模块 401 还用于：按照以下方式生成第四区块：根据所述第一共识零知识证明、所述共识验证信息、所述待出块区块内容、所述第一匿名身份信息、所述第一属性值承诺、第三匿名身份信息和第三属性值承诺，生成第四区块；所述第三匿名身份信息为在所述区块链的第 $i+1$ 时期中待加入匿名节点的匿名身份信息；所述第三属性值承诺是至少根据所述待加入匿名节点在所述区块链的第 $i+1$ 时期中的实际属性值得到的隐匿信息。

基于同一发明构思，本发明实施例还提供了一种计算机设备，包括程序或指令，当所述程序或指令被执行时，如本发明实施例提供的基于 POW 的区块链共识方法及任一可选方法被执行。

基于同一发明构思，本发明实施例还提供了一种计算机可读存储介质，包括程序或指令，当所述程序或指令被执行时，如本发明实施例提供的基于 POW 的区块链共识方法及任一可选方法被执行。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权利要求

1、一种基于 POW 的区块链共识方法，其特征在于，包括：

第一匿名节点若确定所述第一匿名节点满足预设条件，则生成第一共识零知识证明；所述第一共识零知识证明至少用于验证以下信息的正确性：共识验证信息、第一属性值承诺和第一匿名身份信息；所述第一属性值承诺是至少根据第一实际属性值得到的隐匿信息；所述第一匿名身份信息是至少根据所述第一匿名节点的第一实际身份信息得到的；所述预设条件是根据 PoW 共识算法的特性设定的；

所述第一匿名节点至少根据所述第一共识零知识证明、所述共识验证信息、待出块区块内容、所述第一匿名身份信息和所述第一属性值承诺，生成第一区块，并将所述第一区块作为共识区块；

所述第一匿名节点将所述第一区块发送至各第二匿名节点。

2、如权利要求 1 所述的方法，其特征在于，所述第一匿名节点按照以下方式确定所述第一匿名节点满足预设条件：

所述第一匿名节点根据所述第一实际属性值确定所述第一匿名节点的第一挖矿难度值；

所述第一匿名节点在预设数域内持续更新挖矿因子，并根据所述第一挖矿难度值和所述挖矿因子确定所述第一匿名节点是否满足预设条件；所述预设条件是基于所述第一挖矿难度值设定的；所述挖矿因子满足所述预设条件的概率和所述第一实际属性值呈正相关。

3、如权利要求 2 所述的方法，其特征在于，所述根据所述第一挖矿难度值和所述挖矿因子确定所述第一匿名节点是否满足预设条件，包括：

所述第一匿名节点根据所述挖矿因子和所述待出块区块内容，生成第一哈希值；

若所述第一匿名节点确定所述第一哈希值小于第一挖矿难度值，则确定所述第一匿名节点满足预设条件。

4、如权利要求 2 所述的方法，其特征在于，还包括：

所述第一匿名节点在预设数域内持续更新挖矿因子的过程中，在生成的挖矿因子未使得所述第一匿名节点满足所述预设条件的期间，若所述第一匿名节点收到了所述各第二匿名节点中任一第二匿名节点的第二区块，则所述
5 第一匿名节点验证所述第二区块；

若验证通过，则所述第一匿名节点将所述第二区块作为共识区块。

5、如权利要求 1 至 4 任一项所述的方法，其特征在于，所述第一区块为所述区块链的第 i 时期中第三区块与第四区块之间的待共识区块；所述第三区块为所述区块链的第 i 时期中的第一个待共识区块；所述第四区块为所述区块
10 链的第 i 时期中的最后一个待共识区块；所述第一匿名身份信息为所述第一匿名节点在所述区块链的第 i 时期的匿名身份信息；所述第一属性值承诺为所述第一匿名节点在所述区块链的第 i 时期的属性值承诺。

6、如权利要求 5 所述的方法，其特征在于，在所述区块链的第 i 时期结束后，还包括：

15 所述第一匿名节点生成第二匿名身份信息，作为所述第一匿名节点在所述区块链的第 $i+1$ 时期的匿名身份信息；

所述第一匿名节点生成第二属性值承诺，作为所述第一匿名节点在所述区块链的第 $i+1$ 时期的属性值承诺。

7、如权利要求 5 所述的方法，其特征在于，所述第三区块是由所述第一匿名节点生成的，所述第一匿名节点按照以下方式生成第三区块：
20

所述第一匿名节点根据所述第一共识零知识证明、所述共识验证信息、所述第一匿名身份信息和所述第一属性值承诺，生成第三区块。

8、如权利要求 5 所述的方法，其特征在于，所述第四区块是由所述第一匿名节点生成的，所述第一匿名节点按照以下方式生成第四区块：

25 所述第一匿名节点根据所述第一共识零知识证明、所述共识验证信息、所述待出块区块内容、所述第一匿名身份信息、所述第一属性值承诺、第三匿名身份信息和第三属性值承诺，生成第四区块；

所述第三匿名身份信息为在所述区块链的第 $i+1$ 时期中待加入匿名节点的匿名身份信息；所述第三属性值承诺是至少根据所述待加入匿名节点在所述区块链的第 $i+1$ 时期中的实际属性值得到的隐匿信息。

9、一种基于 POW 的区块链共识装置，其特征在于，包括：

5 共识模块，用于若确定第一匿名节点满足预设条件，则生成第一共识零知识证明；所述第一共识零知识证明至少用于验证以下信息的正确性：共识验证信息、第一属性值承诺和第一匿名身份信息；所述第一属性值承诺是至少根据第一实际属性值得到的隐匿信息；所述第一匿名身份信息是至少根据所述第一匿名节点的第一实际身份信息得到的；所述预设条件是根据 PoW 共识算法的特性设定的；以及

10

至少根据所述第一共识零知识证明、所述共识验证信息、待出块区块内容、所述第一匿名身份信息和所述第一属性值承诺，生成第一区块，并将所述第一区块作为共识区块；

数据传输模块，用于将所述第一区块发送至各第二匿名节点。

15 10、一种计算机设备，其特征在于，包括程序或指令，当所述程序或指令被执行时，如权利要求 1 至 8 中任意一项所述的方法被执行。

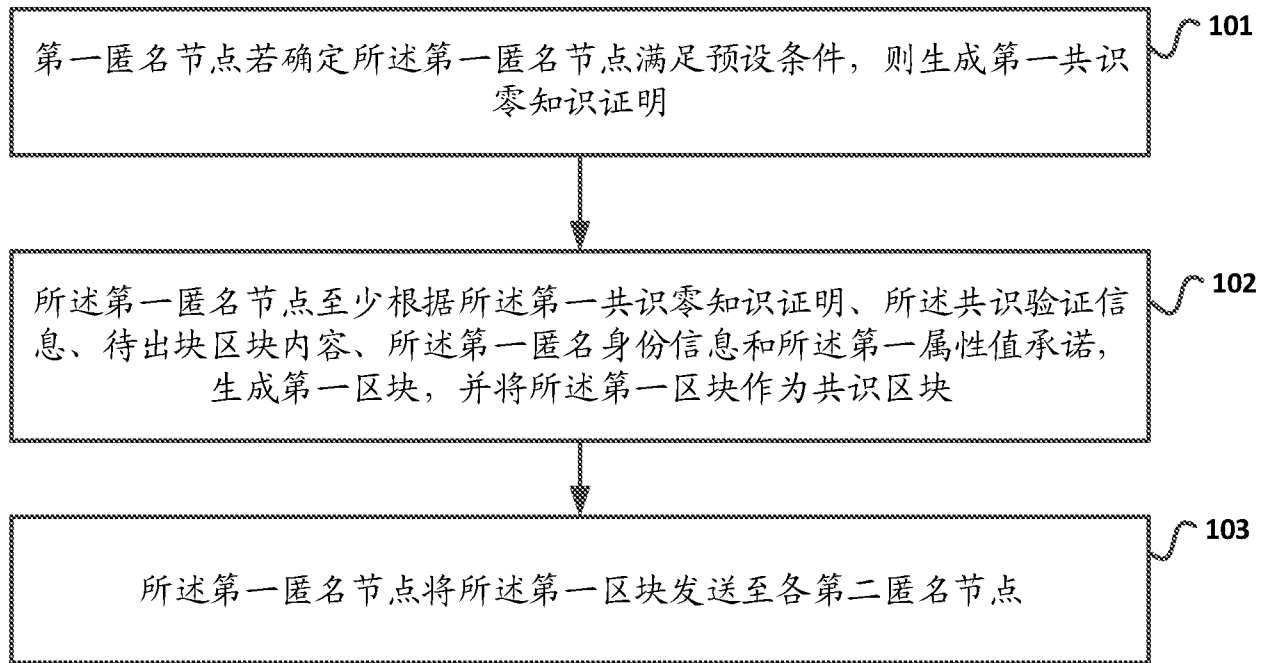


图 1

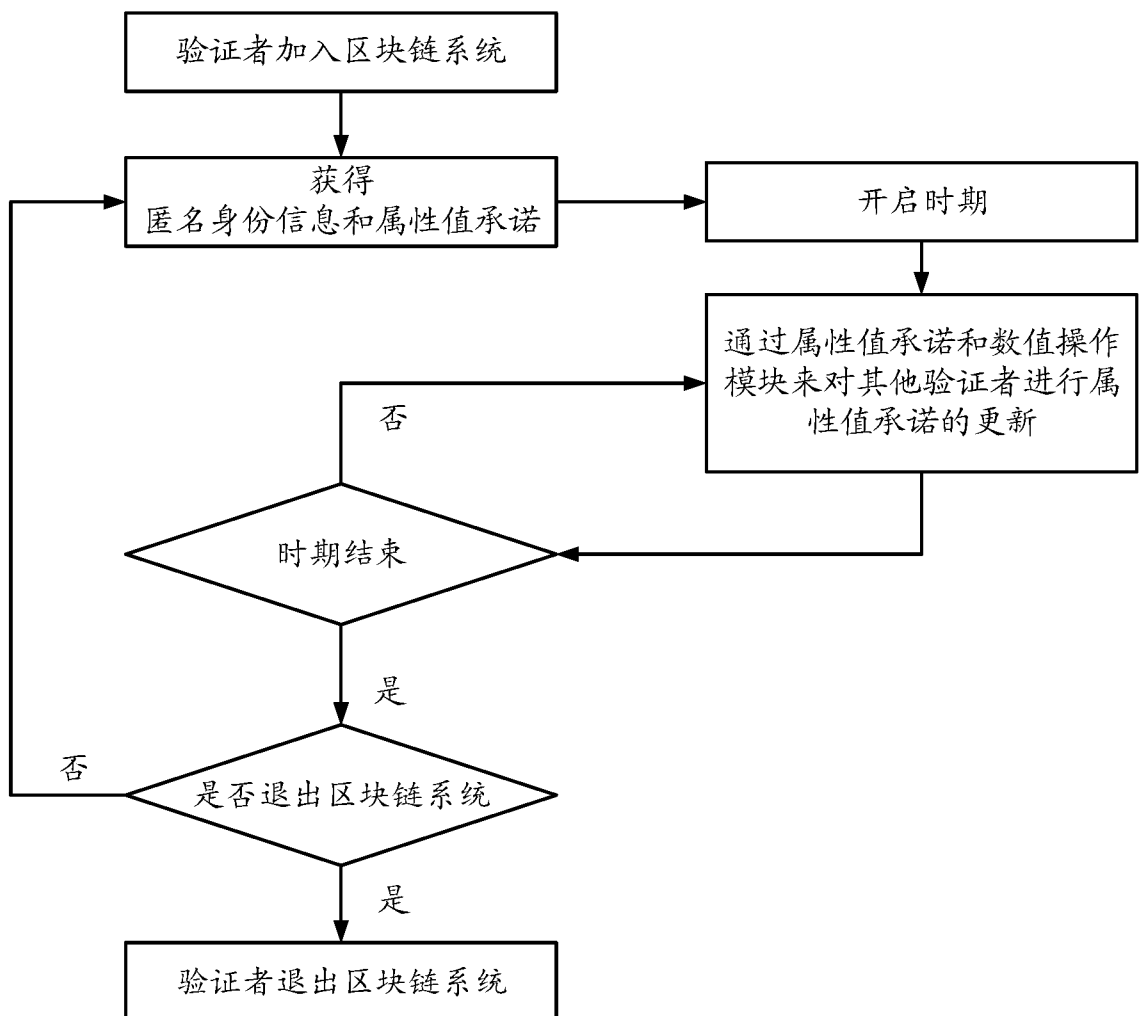


图 2

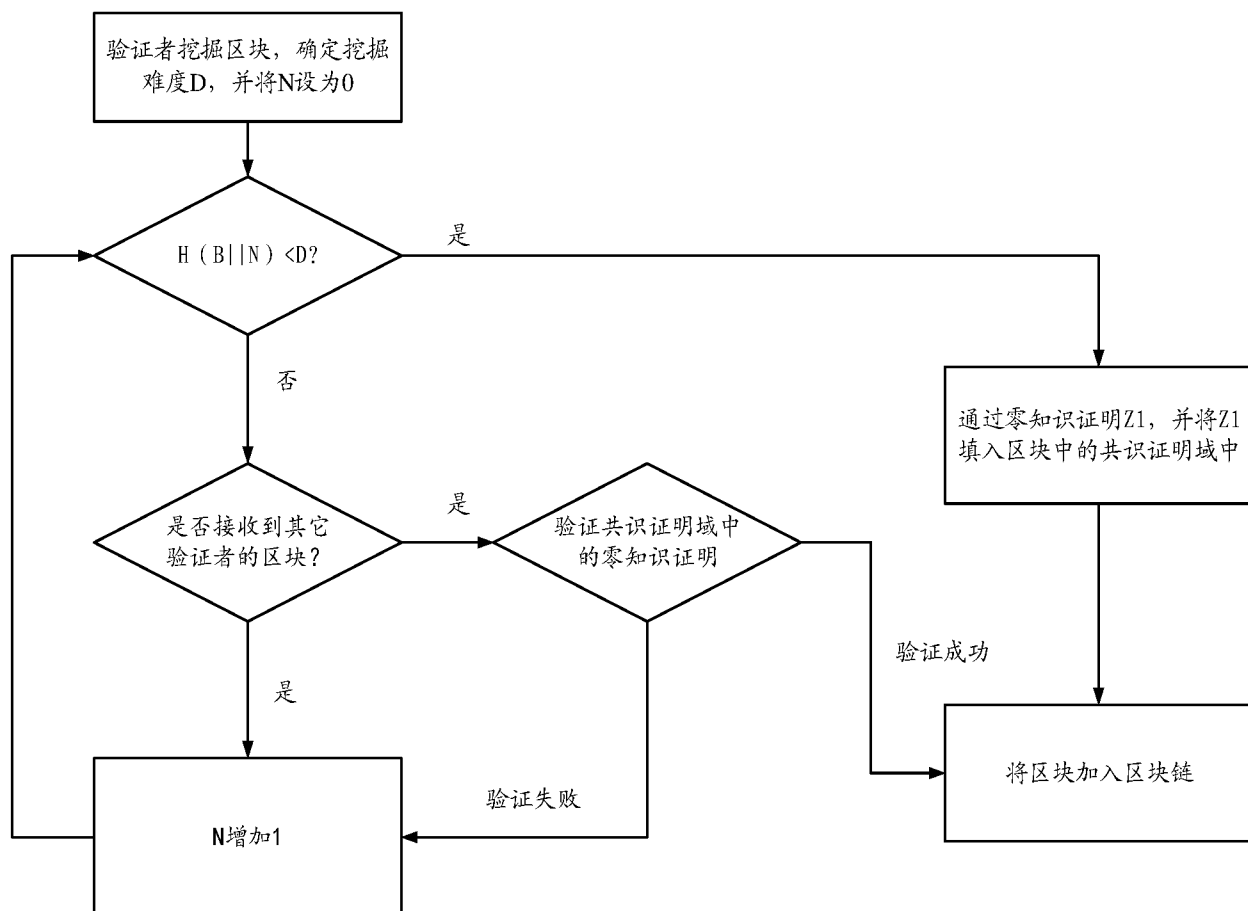


图 3

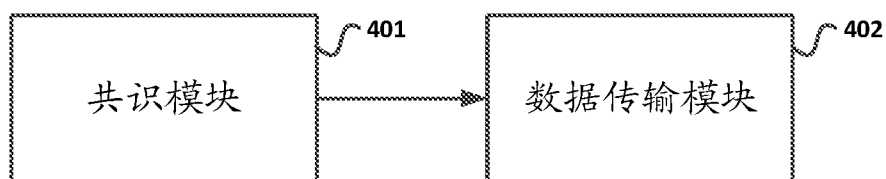


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/126991

A. CLASSIFICATION OF SUBJECT MATTER

H04L 67/01(2022.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; VEN; WOTXT; EPTXT; USTXT; CNKI; 3GPP: 区块链, 分布式账本, 共识, 零知识证明, 工作量证明, 区块, 生成, 匿名, 隐匿, 隐私, 安全, 攻击, 验证, 属性值承诺, block chain, distributed ledger, consensus, zero knowledge proof, ZPK, PoW, block, generate, anonymous, privacy, safe, attack, verify, pedersen

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112436944 A (SHENZHEN QIANHAI WEBANK CO., LTD. et al.) 02 March 2021 (2021-03-02) claims 1-10	1-10
A	CN 107124403 A (ZHU, Qingming) 01 September 2017 (2017-09-01) entire document	1-10
A	CN 110933088 A (SHENZHEN QIYUAN INFORMATION SERVICE CO., LTD.) 27 March 2020 (2020-03-27) entire document	1-10
A	US 2019251553 A1 (ALIBABA GROUP HOLDING LTD.) 15 August 2019 (2019-08-15) entire document	1-10
A	US 2019370793 A1 (DECENTRALIZED FINANCE LABS INC.) 05 December 2019 (2019-12-05) entire document	1-10



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

13 January 2022

Date of mailing of the international search report

19 January 2022

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088, China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/126991

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	112436944	A	02 March 2021	None			
CN	107124403	A	01 September 2017	None			
CN	110933088	A	27 March 2020	None			
US	2019251553	A1	15 August 2019	PL	3542336	T3	12 July 2021
				AU	2018347190	A1	21 May 2020
				AU	2018347190	B2	22 October 2020
				CN	110419055	A	05 November 2019
				CA	3041160	A1	18 April 2019
				MX	2019004658	A	12 August 2019
				ZA	201902549	B	18 December 2019
				JP	2020503718	A	30 January 2020
				JP	6817429	B2	20 January 2021
				ES	2863559	T3	11 October 2021
				BR	112019008160	A2	10 September 2019
				BR	112019008160	B1	24 August 2021
				KR	20200054131	A	19 May 2020
				KR	102215773	B1	17 February 2021
				TW	202018572	A	16 May 2020
				RU	2729595	C1	11 August 2020
				WO	2019072268	A2	18 April 2019
				WO	2019072268	A3	22 August 2019
				SG	11201903586 S	A	30 May 2019
				EP	3542336	A2	25 September 2019
				EP	3542336	A4	20 November 2019
				EP	3542336	B1	27 January 2021
				PH	12019500890	A1	25 November 2019
				EP	3829104	A1	02 June 2021
US	2019370793	A1	05 December 2019	None			

国际检索报告

国际申请号

PCT/CN2021/126991

A. 主题的分类 H04L 67/01 (2022.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类																				
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNABS; CNTXT; VEN; WOTXT; EPTXT; USTXT; CNKI; 3GPP: 区块链, 分布式账本, 共识, 零知识证明, 工作量证明, 区块, 生成, 匿名, 隐匿, 隐私, 安全, 攻击, 验证, 属性值承诺, block chain, distributed ledger, consensus, zero knowledge proof, ZPK, PoW, block, generate, anonymous, privacy, safe, attack, verify, pedersen																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 112436944 A (深圳前海微众银行股份有限公司等) 2021年3月2日 (2021 - 03 - 02) 权利要求1-10</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>CN 107124403 A (朱清明) 2017年9月1日 (2017 - 09 - 01) 全文</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>CN 110933088 A (深圳启元信息服务有限公司) 2020年3月27日 (2020 - 03 - 27) 全文</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>US 2019251553 A1 (ALIBABA GROUP HOLDING LTD) 2019年8月15日 (2019 - 08 - 15) 全文</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>US 2019370793 A1 (DECENTRALIZED FINANCE LABS INC) 2019年12月5日 (2019 - 12 - 05) 全文</td> <td>1-10</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 112436944 A (深圳前海微众银行股份有限公司等) 2021年3月2日 (2021 - 03 - 02) 权利要求1-10	1-10	A	CN 107124403 A (朱清明) 2017年9月1日 (2017 - 09 - 01) 全文	1-10	A	CN 110933088 A (深圳启元信息服务有限公司) 2020年3月27日 (2020 - 03 - 27) 全文	1-10	A	US 2019251553 A1 (ALIBABA GROUP HOLDING LTD) 2019年8月15日 (2019 - 08 - 15) 全文	1-10	A	US 2019370793 A1 (DECENTRALIZED FINANCE LABS INC) 2019年12月5日 (2019 - 12 - 05) 全文	1-10
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
PX	CN 112436944 A (深圳前海微众银行股份有限公司等) 2021年3月2日 (2021 - 03 - 02) 权利要求1-10	1-10																		
A	CN 107124403 A (朱清明) 2017年9月1日 (2017 - 09 - 01) 全文	1-10																		
A	CN 110933088 A (深圳启元信息服务有限公司) 2020年3月27日 (2020 - 03 - 27) 全文	1-10																		
A	US 2019251553 A1 (ALIBABA GROUP HOLDING LTD) 2019年8月15日 (2019 - 08 - 15) 全文	1-10																		
A	US 2019370793 A1 (DECENTRALIZED FINANCE LABS INC) 2019年12月5日 (2019 - 12 - 05) 全文	1-10																		
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																				
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																				
国际检索实际完成的日期 2022年1月13日		国际检索报告邮寄日期 2022年1月19日																		
ISA/CN的名称和邮寄地址 中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		授权官员 朱秀玲 电话号码 86-(010)-62089127																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/126991

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	112436944	A	2021年3月2日	无			
CN	107124403	A	2017年9月1日	无			
CN	110933088	A	2020年3月27日	无			
US	2019251553	A1	2019年8月15日	PL	3542336	T3	2021年7月12日
				AU	2018347190	A1	2020年5月21日
				AU	2018347190	B2	2020年10月22日
				CN	110419055	A	2019年11月5日
				CA	3041160	A1	2019年4月18日
				MX	2019004658	A	2019年8月12日
				ZA	201902549	B	2019年12月18日
				JP	2020503718	A	2020年1月30日
				JP	6817429	B2	2021年1月20日
				ES	2863559	T3	2021年10月11日
				BR	112019008160	A2	2019年9月10日
				BR	112019008160	B1	2021年8月24日
				KR	20200054131	A	2020年5月19日
				KR	102215773	B1	2021年2月17日
				TW	202018572	A	2020年5月16日
				RU	2729595	C1	2020年8月11日
				WO	2019072268	A2	2019年4月18日
				WO	2019072268	A3	2019年8月22日
				SG	11201903586S	A	2019年5月30日
				EP	3542336	A2	2019年9月25日
				EP	3542336	A4	2019年11月20日
				EP	3542336	B1	2021年1月27日
				PH	12019500890	A1	2019年11月25日
				EP	3829104	A1	2021年6月2日
US	2019370793	A1	2019年12月5日	无			