

(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
2023 年 3 月 30 日 (30.03.2023)



(10) 国际公布号
WO 2023/045150 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01) **G06Q 40/04** (2012.01)
- (21) 国际申请号: PCT/CN2021/140630
- (22) 国际申请日: 2021 年 12 月 22 日 (22.12.2021)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202111104734.0 2021 年 9 月 22 日 (22.09.2021) 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)。
- (72) 发明人: 张龙 (**ZHANG, Long**); 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)。 毛嘉宇 (**MAO, Jiayu**); 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)。 储雨知 (**CHU, Yuzhi**); 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)。 王越 (**WANG, Yue**); 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: 北京同立钧成知识产权代理有限公司 (**LEADER PATENT & TRADEMARK FIRM**); 中国北京市海淀区西直门北大街 32 号枫蓝国际 A 座 8F-6, Beijing 100082 (CN)。

(54) **Title:** BLOCK VERIFICATION METHOD

(54) 发明名称: 区块验证方法

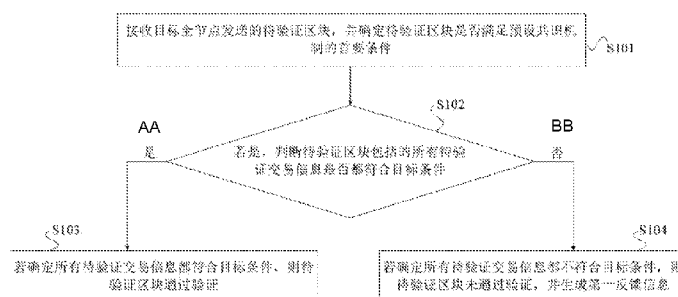


图 2

- S101 Receive a block to be verified sent by a target full node and determine whether the block to be verified satisfies a primary condition of a preset consensus mechanism
- S102 If so, determine whether all transaction information to be verified included in the block to be verified satisfies a target condition
- S103 If determined that all of the transaction information to be verified satisfies the target condition, then the block to be verified is verified
- S104 If determined that all of the transaction information to be verified does not satisfy the target condition, then the block to be verified is not verified and first feedback information is generated
- AA Yes
- BB No

(57) **Abstract:** The present application provides a block verification method, the block verification method being applied to a light node in a blockchain network. The method comprises: first, a light node receives a block to be verified sent by a target full node and determines whether the block to be verified satisfies a primary condition of a preset consensus mechanism; if so, the light node determines whether all transaction information to be verified included in the block to be verified satisfies a target condition, the target condition being obtained according to a transaction state value, and the transaction state value being used for representing transaction information received by the light node; if the light node determines that all the transaction information to be verified satisfies the target condition, then it is determined that the block to be verified is verified, so that the light node implements, on the basis of the transaction state value, block verification of the block to be verified, and the storage of full-amount transaction information is not required, which provides the possibility for a blockchain node to operate in a light-weighted terminal device.

(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))。

(57) 摘要: 本申请提供一种区块验证方法, 该区块验证方法应用于区块链网络中的轻节点。首先, 轻节点接收目标全节点发送的待验证区块并确定待验证区块是否满足预设共识机制的首要条件, 若满足, 轻节点判断待验证区块包括的所有待验证交易信息是否都符合目标条件, 目标条件根据交易状态值获得, 而交易状态值用于表征轻节点已接收到的交易信息。若轻节点确定所有待验证交易信息都符合目标条件, 则确定待验证区块通过验证, 从而轻节点基于交易状态值实现对待验证区块的区块验证, 无需存储全量的交易信息, 为区块链节点运行于轻量化终端设备提供了可能。

区块验证方法

5 本申请要求于 2021 年 09 月 22 日提交中国专利局、申请号为 202111104734.0、申请名称为“区块验证方法”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

本申请涉及金融科技（Fintech）技术领域，尤其涉及一种区块验证方法。

10 背景技术

随着计算机技术以及互联网技术的快速发展，金融科技（Fintech）作为金融与科技深度融合的产物，目前正成为金融行业创新发展的热点，例如，区块链技术在金融行业已被广泛使用。

15 区块链利用块链式数据结构验证与存储数据，并基于分布式节点共识机制生成和更新数据，还利用密码学的方式保证数据传输及访问的安全，以及利用由自动化脚本代码组成的智能合约进行编程及操作数据。因此，区块链提供了高度一致的分布式账本。其中，基于共识机制，任何参与节点独立修改自身账本都无法对整个分布式网络造成影响，这使得区块链具备不可篡改性。在共识机制的实现过程中，参与共识的节点需要进行区块验证，以当验证通过记录区块。

20 然而，在区块验证中，除过验证交易签名的正确性，还要确保交易有效性，即需要基于之前的区块（即交易）进行验证并实时更新默克尔树状态，可见，参与共识的节点需拥有完整路径上的所有交易信息才能完成区块验证。目前，参与共识的节点均为全节点，换言之，全节点上保存了区块链网络的全量数据。全节点一般为共识和挖矿节点。但在实际的区块链应用中，大众或者中小机构参与区块链网络的诉求也越来越强，但大众或者中小机构所涉及的例如智能终端、个人电脑以及传感器等轻量化终端设备，由于其存储开销有限而无法全量存储所有交易信息，进而无法对交易有效性进行验证来完成区块验证，从而导致轻量化终端设备无法参与区块链网络的正常运行。

25 发明内容

本申请提供一种区块验证方法，用于为轻量化终端设备提供一种无需存储全量交易信息也可进行的区块验证方法。

本申请提供一种区块验证方法，应用于区块链网络中的轻节点；所述方法，包括：

接收目标全节点发送的待验证区块，并确定所述待验证区块是否满足预设共识机制的首要条件，所述目标全节点是在所述区块链网络的全节点中选举得到；

35 若是，判断所述待验证区块包括的所有待验证交易信息是否都符合目标条件，所述目标条件根据交易状态值获得，所述交易状态值用于表征所述轻节点已接收到的交易信息；

若确定所述所有待验证交易信息都符合所述目标条件，则所述待验证区块通过验证。

本申请提供一种区块验证方法，该区块验证方法应用于区块链网络中的轻节点。首先，轻节点接收目标全节点发送的待验证区块并确定待验证区块是否满足预设共识机制的首要条件，若满足，轻节点判断待验证区块包括的所有待验证交易信息是否都符合目标条件，目标条件根据交易状态值获得，而交易状态值用于表征轻节点已接收到的交易信息。若轻节点确定所有待验证交易信息都符合目标条件，则确定待验证区块通过验证，从而轻节点基于交易状态值实现对待验证区块的区块验证，无需存储全量的交易信息，为区块链节点运行于轻量化终端设备提供了可能。

附图说明

图1为本申请实施例提供的一种应用场景示意图；

图2为本申请实施例提供的一种区块验证方法的流程示意图；

图3为本申请实施例提供的另一种区块验证方法的流程示意图；

图4为本申请实施例提供的再一种区块验证方法的流程示意图；

图5为本申请实施例提供的一种交易状态值更新过程示意图；

图6为本申请实施例提供的又一种区块验证方法的流程示意图；

图7为本申请实施例提供的又一种区块验证方法的流程示意图；

图8为本申请实施例提供的又一种区块验证方法的流程示意图。

具体实施方式

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描述的实施方式并不代表与本申请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、本申请的一些方面相一致的方法和装置的例子。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”“第四”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例例如能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

在区块链网络中，基于共识机制，任何参与节点独立修改自身账本都无法对整个分布式网络造成影响，这使得区块链具备不可篡改性。也正因为如此，在共识机制的实现过程中，参与共识的节点需要进行区块验证，以当验证通过时记录区块。然而，在区块验证中，除过验证交易签名的正确性，还要确保交易的有效性，即需要基于之前的区块（即交易）进行验证并实时更新默克尔树状态。可见，参与共识的节点需要拥有完整路径上的所有交易信息才能完成区块验证。目前，参与共识的节点均为全节点，换言之，全节点上保存了区块链网络的全量数据。全节点一般为共识和挖矿节点。但在实际的区块链应用中，大众或者中小机构参与区块链网络的诉求也越来越强，但大众或者中小机构所涉及的例如智能终端、个人电脑以及传感器等轻量化终端设备，由于其存储开销有限而无法全量存储所有交易信息，进而无法对交易有效性进行验证

来完成区块验证，从而导致轻量化终端设备无法参与区块链网络的正常运行。

针对现有技术中存在的上述问题，本申请提供一种区块验证方法，该区块验证方法应用于区块链网络中的轻节点。本申请提供的区块验证方法的发明构思在于：轻节点接收目标全节点发送的待验证区块，首先判断待验证区块是否满足预设共识机制的首要条件，在当满足时，进一步判断待验证区块包括的所有待验证交易信息是否都符合目标条件，其中，目标条件是根据交易状态值获得，而交易状态值可以表征该轻节点已接收到的交易信息，从而当所有待验证交易信息都符合目标条件时，确定待验证区块通过验证。可见，本申请提供的区块验证方法中，在对待验证区块是否满足预设共识机制的首要条件进行判断之后，基于交易状态值即可实现对待验证区块的验证，不同于现有技术需进行默克尔树证明等步骤，无需存储全量的交易信息即可实现区块验证，为区块链节点运行于轻量化终端设备提供可能。并且，由于交易状态值只需较小空间便可实现存储，存储空间还不会随着待验证区块的增多而增大，因而更加有利于轻量化终端设备在区块链网络中的应用。

以下，对本申请实施例的示例性应用场景进行介绍。

图 1 为本申请实施例提供的一种应用场景示意图，如图 1 所示，区块链网络包含多个区块链节点，例如区块链节点 11、区块链节点 12、区块链节点 13 以及区块链节点 14，其中区块链节点 11 至区块链节点 14 均为全节点，全节点是指需存储区块链网络的全量交易信息，一般为共识节点和挖矿节点。其中，轻节点 15 中所配置的处理器的通过执行本申请实施例提供的区块验证方法，无需存储全量的交易信息即可实现对待验证区块的验证，在验证通过时可参与至区块链网络中进行区块链的正常运行。轻节点 15 可以例如移动终端、个人电脑或者传感器等存储开销十分有限的轻量化终端设备，移动终端可以例如智能手机、智能手表等可穿戴设备。

需要说明的是，图 1 中示意性列举了区块链网络中全节点的数量为四个，轻节点的数量为一个。在实际工况中，对于区块链网络中全节点和轻节点的数量不作限定，具体由实际情况决定。另外，图 1 中轻节点 15 以智能手机为例示出。

需要说明的是，上述应用场景仅仅是示意性的，本申请实施例提供的区块验证方法包括但不限于上述应用场景。

图 2 为本申请实施例提供的一种区块验证方法的流程示意图。如图 2 所示，本申请实施例提供的区块验证方法应用于区块链网络中的轻节点，该方法包括：

S101：接收目标全节点发送的待验证区块，并确定待验证区块是否满足预设共识机制的首要条件。

其中，目标全节点是在区块链网络的全节点中选举得到。

轻节点接收目标全节点发送的待验证区块，待验证区块由目标全节点根据业务需要从自身交易池中选择交易信息并对选择到的交易信息进行打包形成的。例如，目标全节点打包形成新的区块，需将新的区块广播给区块链网络中的其他节点，轻节点则可以接收到目标全节点发送的该新的区块，该新的区块即为待验证区块。

目标全节点是从区块链网络的全节点中选举得到的。例如，区块链网络中的全节点执行交易信息时，需基于预设共识机制，从所有全节点中选举出一个全节点以对外广播区块，被选举出的全节点即被定义为目标全节点。比如，预设共识机制以工作量证明（Proof of

Work, 简称 PoW) 共识机制为例, 从全节点选举目标全节点的方式可以通过计算哈希值实现。例如, 每个全节点都会计算一个符合难度条件的哈希值, 当某一全节点首个计算出该哈希值, 则该全节点被选举为目标全节点, 其中, 符合难度条件的哈希值也可称为困难值。进而该目标全节点会将困难值和其根据业务需求从自身交易池中选择出的交易信息进行打包形成上述新的区块, 也即待验证区块, 并将该待验证区块广播给其他节点。

轻节点接收到待验证区块后, 会确定待验证区块是否满足预设共识机制的首要条件。

例如, 假设预设共识机制为 PoW 共识机制, 则本步骤 S101 中轻节点确定待验证区块是否满足预设共识机制的首要条件可能的实现方式如图 3 所示。图 3 为本申请实施例提供的另一种区块验证方法的流程示意图。如图 3 所示, 本申请实施例包括:

S1011: 验证待验证区块的困难值是否正确。

其中, PoW 共识机制的首要条件包括困难值。

S1012: 若是, 确定待验证区块满足首要条件。

S1013: 若否, 确定待验证区块未通过验证, 并生成第二反馈信息。

其中, 第二反馈信息用于指示轻节点拒绝待验证区块。

轻节点接收到待验证区块后, 若预设共识机制为 PoW 共识机制, 预设共识机制的首要条件, 也即 PoW 共识机制的首要条件则包括困难值。因而, 轻节点确定待验证区块是否满足预设共识机制的首要条件, 也就是轻节点验证待验证区块的困难值是否正确, 若正确, 则确定待验证区块满足首要条件。反之, 若不正确, 则待验证区块不满足首要条件, 则可确定待验证区块未通过验证, 并且, 轻节点可以生成第二反馈信息, 通过第二反馈信息指示轻节点拒绝待验证区块。

本申请实施例提供的区块验证方法, 轻节点接收目标全节点发送的待验证区块, 确定待验证区块是否满足预设共识机制的首要条件。例如, 假设预设共识机制为 PoW 共识机制, 轻节点通过验证待验证区块的困难值是否正确确定其是否满足预设共识机制的首要条件。若正确, 则确定待验证区块满足预设共识机制的首要条件。反之, 若不正确, 则表明待验证区块未通过验证, 并生成第二反馈信息, 以指示轻节点拒绝待验证区块。从而为待验证区块完成区块验证提供前提条件。

需要说明的是, 确定待验证区块是否满足预设共识机制的首要条件可以理解为验证待验证区块对应交易签名的正确性, 显然, 预设共识机制包括但不限于 PoW 共识机制。当预设共识机制为其他共识机制时, 则可以通过其他的预设共识机制所对应的具体方式验证交易签名的正确性以判断待验证区块是否满足预设共识机制的首要条件。

通过上述描述可知, 在验证困难值正确时, 则确定待验证区块满足预设共识机制的首要条件时, 进一步执行步骤 S102。而若验证困难值不正确, 则表明待验证区块不满足预设共识机制的首要条件, 待验证区块未通过验证。

S102: 若是, 判断待验证区块包括的所有待验证交易信息是否都符合目标条件。

其中, 目标条件根据交易状态值获得, 交易状态值用于表征轻节点已接收到的交易信息。

在确定待验证区块满足预设共识机制的首要条件后, 进一步判断待验证区块包括的所有待验证交易信息是否都符合目标条件, 以对待验证区块包括的待验证交易信息的有效性进行验证, 以此完成区块验证。

例如,在本申请实施例中,轻节点可以通过交易状态值来反馈其已接收到的交易信息,并根据其维护的交易状态值获得目标条件,进而则可以通过判断待验证区块包括的所有待验证交易信息是否都符合目标条件,来实现对待验证区块所包括的所有待验证交易信息有效性的验证。

5 其中,待验证交易信息是指待验证区块中所包含的各交易信息,即目标全节点打包形成待验证区块时所选择的交易信息,例如,目标全节点将 m ($1 \leq m \leq n$) 起交易信息打包形成了待验证区块,假设待验证区块以 B_1 表示,那么 B_1 中的交易信息也即所有待验证交易信息可以通过如下集合表示:

$$\{T_1, T_2, T_3, \dots, T_m\}, (1 \leq m \leq n)$$

10 轻节点判断待验证区块 B_1 包括的所有待验证交易信息是否都符合目标条件,其中,目标条件根据轻节点所维护的交易状态值获得,而其维护的交易状态值可以反馈其接收到交易信息。鉴于此,判断待验证区块包括的所有待验证交易信息是否都符合目标条件中的该目标条件,可以理解为,判断待验证区块包括的该 m 起待验证交易信息是否均存在于其维护的交易状态值中。换言之,若 m 起待验证交易信息均存在于其所维护的交易状态值中,则表明待验证区块包括的所有待验证交易信息都符合目标条件。反之,若 m 起待验证交易信息中任意一起都不存在于其维护的交易状态值中,则表明待验证区块包括的所有待验证交易信息都不符合目标条件。

在经过判断后,若判断出待验证区块包括的所有待验证交易信息都符合目标条件,则表明待验证区块包括的所有待验证交易信息的有效性通过验证,即执行步骤 S103。反之,若确定所有待验证交易信息都不符合目标条件,即执行步骤 S104。

20 S103: 若确定所有待验证交易信息都符合目标条件,则待验证区块通过验证。

S104: 若确定所有待验证交易信息都不符合目标条件,则待验证区块未通过验证,并生成第一反馈信息。

其中,第一反馈信息用于指示轻节点拒绝待验证区块。

25 若轻节点确定出待验证区块包括的所有待验证交易信息都符合目标条件,则表明轻节点对待验证区块包括的所有待验证交易信息的交易有效性验证通过,再结合之前待验证区块满足预设共识机制的首要条件的前提,可以确定待验证区块通过验证,完成对待验证区块的验证。

反之,若确定所有待验证交易信息都不符合目标条件,则表明轻节点对待验证区块包括的所有待验证交易信息的交易有效性验证未通过,则可以确定待验证区块未通过验证。

30 进而还生成第一反馈信息,通过第一反馈信息指示轻节点拒绝待验证区块。

可选地,若确定待验证区块通过验证,则轻节点记录待验证区块并向目标全节点发送验证信息,通过验证信息使得目标全节点获知轻节点对于待验证区块的验证已通过。在当目标全节点接收一定数量的验证信息后即可完成对待验证区块的上链。目标全节点接收到一定数量的验证信息即为目标全节点接收到超过预设数量的验证信息。例如,每个对于交易信息有效性验证通过的节点均会向目标全节点反馈验证信息,当目标全节点接收到超过其发送待验证区块的节点总数的 51% 数量的验证信息时,即目标全节点接收到超过预设数量的验证信息,对于目标全节点而言,其完成了对待验证区块的上链。

本申请实施例提供的区块验证方法应用于区块链网络中的轻节点。首先,轻节点接收

目标全节点发送的待验证区块，并确定待验证区块是否满足预设共识机制的首要条件。若满足，轻节点判断待验证区块包括的所有待验证交易信息是否都符合目标条件，该目标条件根据轻节点所维护的交易状态值获得，而交易状态值用来表征轻节点已接收到的交易信息，轻节点则无需存储全量的交易信息。经过判断，若确定待验证区块包括的所有待验证交易信息都符合目标条件，则待验证区块通过验证。本申请实施例提供的区块验证方法中，轻节点在确定待验证区块满足预设共识机制的首要条件时，基于其所维护的交易状态值判断待验证区块包括的所有待验证交易信息是否都符合目标条件，以达到对待验证区块的验证。对轻节点而言无需存储全量的交易信息也可以实现区块验证，为区块链节点运行于轻量化终端设备提供可能。

在上述实施例的描述中，交易状态值反馈轻节点已接收到的交易信息。具体地，在接收目标全节点发送的待验证区块之前，每当轻节点接收到目标账户发送的交易信息，根据预设更新策略以及当前次接收到的交易信息更新交易状态值，从而通过所维护的交易状态值反馈其已接收到的交易信息。

例如，当区块链网络初始化完成或，则会有多起交易发起，目标账户会选择区块链网络中的任何一个区块链节点发送交易信息。当区块链网络中的全节点接收到目标账户发送的交易信息后，会将其放入自身交易池。而对于轻节点而言，该轻节点不需保存交易信息，而是根据交易信息以及预设更新策略更新交易状态值，通过维护交易状态值代替存储全量的交易信息。

在一种可能的设计中，轻节点根据预设更新策略以及当前次接收到的交易信息更新交易状态值可能的实现方式如图4所示。图4为本申请实施例提供的再一种区块验证方法的流程示意图。如图4所示，本申请实施例提供的区块验证方法，包括：

S201：获取当前哈希值。

其中，当前哈希值为当前次接收到的交易信息的哈希值。

S202：根据当前哈希值、预设更新算法以及当前的交易状态值生成目标交易状态值。

其中，预设更新算法包括目标参数以及目标特征函数，目标参数为互为质数的第一参数和第二参数的乘积。

S203：利用预设更新方式以及目标交易状态值更新交易状态值。

其中，预设更新策略包括预设更新算法以及预设更新方式。

轻节点每当接收到目标账户发送的交易信息，获取当前次接收到的交易信息的哈希值，即获取当前哈希值。然后根据当前哈希值、预设更新算法以及当前的交易状态值生成目标交易状态值，再利用预设更新方式和目标交易状态值更新交易状态值，例如所采用的预设更新方式为将当前的交易状态值更新为目标交易状态值，从而完成对交易状态值的更新。

图5为本申请实施例提供的一种交易状态值更新过程示意图。如图5所示，假设以 T_1 至 T_n 表示轻节点接收到目标账户发送的第1至第 n 起交易信息， $H(T_1)$ 至 $H(T_n)$ 分别表示第1起至第 n 起交易信息的哈希值，即各当前哈希值， $TxState_1$ 至 $TxState_n$ 则表示轻节点针对接收到的每起交易信息所对应维护的各交易状态值。

继续参照图5，在区块链网络初始化阶段，也即在轻节点首次接收目标账户发送的交易信息之前，轻节点的交易状态值以 $TxState_0$ 表示，该 $TxState_0$ 为轻节点随机生成的初始的交易状态值。轻节点接收到第1起交易信息，则将 $TxState_0$ 更新为 $TxState_1$ 。轻节点接收

到第 2 起交易信息, 则将 $TxState_1$ 更新为 $TxState_2$, 依次类推, 轻节点接收到第 n 起交易信息, 轻节点的交易状态值则更新为 $TxState_n$ 。 $TxState_1$ 至 $TxState_n$ 也即轻节点针对每次接收到的目标账户发送的交易信息所对应维护的交易状态值, $TxState_1$ 至 $TxState_n$ 分别表示第 1 起至第 n 起交易信息各自对应的目标交易状态值。

5 当区块链网络初始化完成后会有目标账户发起交易, 相应地, 轻节点会接收目标账户发送的交易信息。因而, 在轻节点首次接收目标账户发送的交易信息之前, 也即区块链网络的初始化阶段, 轻节点会随机生成初始的交易状态值。换言之, 在区块链网络的初始化阶段, 也即第 0 个区块时, 轻节点随机生成初始的交易状态值, 该初始的交易状态值就是第 0 个区块时轻节点所对应维护的交易状态值。在本申请实施例中, 该初始的交易状态值为任意质数的预设常识, 例如以 g 表示, 对于该任意质数的具体取值, 本申请实施例不作限定。

由于 $TxState_0$ 为初始的交易状态值, 其为任意质数的预设常数, 即存在如下公式 (1):

$$TxState_0 = g \quad (1)$$

对于第 1 起交易信息 T_1 , 获取的当前哈希值 $H(T_1)$ 可以如下公式 (2) 表示:

$$H(T_1) = Hash(T_1) \quad (2)$$

15 则根据当前哈希值、预设更新算法以及当前的交易状态值 (即初始的交易状态值) 生成的目标交易状态值 (即第 1 起交易信息对应的目标交易状态值 $TxState_1$) 可以如下公式 (3) 表示:

$$TxState_1 = (TxState_0)^{H(T_1)} \bmod N = g^{H(T_1)} \bmod N \quad (3)$$

20 以此类推, 对于第 i ($1 \leq i \leq n$) 起交易信息, 获取该 T_i 起交易信息的哈希值, 即当前哈希值如公式 (4) 所示:

$$H(T_i) = Hash(T_i), (1 \leq i \leq n) \quad (4)$$

然后, 根据 $H(T_i)$ 、预设更新算法以及当前的交易状态值 (即 T_{i-1} 起交易信息对应的交易状态值) 得到第 i 起交易信息的目标交易状态值 $TxState_i$ 如下公式 (5) 所示:

$$TxState_i = (TxState_{i-1})^{H(T_i)} \bmod N, (1 \leq i \leq n) \quad (5)$$

25 其中, $TxState_{i-1}$ 表示接收到第 i 起交易信息时的当前的交易状态值, $H(T_i)$ 表示第 i 起交易信息的当前哈希值, $TxState_i$ 表示接收到第 i 起交易信息对应的目标交易状态值, 将当前的交易状态值 $TxState_{i-1}$ 更新为目标交易状态值 $TxState_i$ 完成当前次交易状态值的更新, 符号 “ $\bmod$ ” 表示取模运算, N 表示目标参数。

30 在上述描述的基础上, 进一步地, 若轻节点接收到 n 起交易, 则所对应的目标交易状态值, 也就是轻节点当前所维护的交易状态值 $TxState_n$, 可以如下公式 (6) 所示:

$$TxState_n = g^{H(T_1) * H(T_2) * \dots * H(T_n)} \bmod N = g^{\prod_{i=1}^n H(T_i)} \bmod N, (1 \leq i \leq n) \quad (6)$$

其中, 如公式 (6) 所示的表达式即为预设更新算法, 初始的交易状态值 g 的幂次方即 $H(T_1) * H(T_2) * \dots * H(T_n)$ 可以被定义为目标特征函数。

35 另外, 上述的 N 表示目标参数, 其中该 N 的取值为第一参数和第二参数的乘积, 并且第一参数和第二参数互为质数, 例如第一参数和第二参数分别为两大质数。假设第一参数和第二参数分别采用 p 和 q 表示, 则存在如下公式 (7):

$$N = p * q \quad (7)$$

其中, 第一参数和第二参数的取值可以根据实际情况设置。为了便于轻节点维护交易

状态值，第一参数和第二参数可以采用数值较大的质数。

例如，假设 n 的取值为 5，即轻节点接收到目标账户发送的 5 起交易信息，并假设每起交易信息的哈希值分别如下公式（8）至（12）所示：

$$H(T_1) = Hash(T_1) = 10000667 \quad (8)$$

$$H(T_2) = Hash(T_2) = 99997867 \quad (9)$$

$$H(T_3) = Hash(T_3) = 27648197 \quad (10)$$

$$H(T_4) = Hash(T_4) = 81480011 \quad (11)$$

$$H(T_5) = Hash(T_5) = 45224017 \quad (12)$$

则轻节点接收到的目标账户发送的 5 起交易信息后所维护的交易状态值 $TxState_5$ 如下公式（13）所示：

$$TxState_5 = g^{10000667*99997867*27648197*81480011*45224017} \bmod N \quad (13)$$

通过上述实施例描述以及举例说明可知，交易状态值 $TxState_n$ 隐式的包含了 n 起交易信息。换言之，通过轻节点的交易状态值可以反馈出轻节点所接收到的交易信息，即交易状态值可以表征轻节点已接收到的交易信息。因而，轻节点无需保存交易信息，只需根据交易信息和预设更新策略更新交易状态值，达到通过维护交易状态值来反馈其已接收到的交易信息的目的。

交易状态值只需几兆空间便可存储，无需较大存储空间。例如，交易状态值 $TxState_n$ 为一小于目标参数 N 的数值。而目标参数 N 可以为两大质数 p 和 q 的乘积，目前最大质数为 $2^{57885161}-1$ 位，因此交易状态值 $TxState_n$ 最多需要 57885161bit 即可存储，可见其存储容量不会超过 7MB。因此对于轻节点而言，其只需要 7MB 的存储空间便可通过本申请实施例提供的区块验证方法实现区块验证。

图 6 为本申请实施例提供的又一种区块验证方法的流程示意图。如图 6 所示，本申请实施例提供的区块验证应用于区块链网络中的轻节点，该方法包括：

S301：每当接收到目标账户发送的交易信息，根据预设更新策略以及当前次接收到的交易信息更新交易状态值。

步骤 S301 的实现方式、原理以及技术效果与图 4 的实现方式、原理以及技术效果相类似，详细内容可参考前述描述，在此不再赘述。

S302：接收目标全节点发送的待验证区块，并确定待验证区块是否满足预设共识机制的首要条件。

其中，目标全节点是在区块链网络的全节点中选举得到。

步骤 S302 的实现方式、原理以及技术效果与步骤 S101 的实现方式、原理以及技术效果相类似，详细内容可参考前述描述，在此不再赘述。

通过前述实施例的描述可知，对于判断待验证区块包括的所有目标验证交易信息是否都符合目标条件，可以等同于判断待验证区块包括的所有待验证交易信息是否均存在于其维护的交易状态值。由于交易状态值 $TxState_n$ 涉及有限域的取模运算，因而是无法证明其因子的存在性的，但是可以反向证明因子的不存在性。换言之，若要确定待验证交易信息均存在于交易状态值 $TxState_n$ 中，只需确定待验证交易信息中的任意一起待验证交易信息都不存在于交易状态值 $TxState_n$ 中是不成立的即可。

以下步骤 S303 至步骤 S306，详细说明如何通过判断待验证区块中的任意一起待验证

交易信息都不存在于交易状态值 $TxState_n$ 中是否成立, 来实现对待验证区块包括的所有待验证交易信息是否都符合目标条件的判断。

S303: 若是, 根据各当前哈希值以及目标特征函数得到目标特征值。

S304: 判断任意待验证交易信息的哈希值是否都与目标特征值互为质数关系。

5 S305: 若是, 则确定所有待验证交易信息都不符合目标条件。

S306: 若否, 则确定所有待验证交易信息都符合目标条件。

轻节点每接收到一起交易信息更新交易状态值时, 均会获取到当前次接收到的交易信息的哈希值, 换言之, 轻节点获取了其所接收到的每起交易信息的哈希值, 即轻节点获取了各当前哈希值。因而, 轻节点根据各当前哈希值以及目标特征函数可以得到目标特征值,

10 该目标特征值以 W_n 表示, 则存在如下公式 (14):

$$W_n = H(T_1) * H(T_2) * \dots * H(T_n) = \prod_{i=1}^n H(T_i) \quad (14)$$

其中, 若轻节点接收到目标账户发送的 n 起交易信息, 则 $H(T_1)$ 、 $H(T_2)$ 、...、 $H(T_n)$ 分别表示各当前哈希值, $H(T_1) * H(T_2) * \dots * H(T_n)$ 表示目标特征函数, 该目标特征函数基于预设更新算法得到, W_n 则表示通过各当前哈希值以及目标特征函数得到的目标特征值。

15 进一步, 通过判断任意待验证交易信息的哈希值是否与目标特征值互为质数关系来实现对所有待验证交易信息是否都符合目标条件的判断。

例如, 假设以 $H(T')$ 即 $Hash(T')$ 表示任意待验证交易信息的哈希值, 若 $Hash(T')$ 与 W_n 各自表示的数值互为质数关系, 则表明 $Hash(T')$ 不能被 W_n 整除。结合公式 (6) 的表达式可知, 若 $Hash(T')$ 不能被 W_n 整除, 即 $Hash(T')$ 不为 $TxState_n$ 幂次方的因子, 也即任意待验证交易信息 T' 不存在于交易状态值 $TxState_n$ 中, 其中 $TxState_n$ 幂次方的因子即公式 (6) 中预设常识 g 的幂次方, 其为目标特征函数 W_n 所表示的数值。也就是说, 若 $Hash(T')$ 与 W_n 各自表示的数值互为质数关系成立, 则相当于任意待验证交易信息 T' 不存在于交易状态值 $TxState_n$ 中是成立的。故而, 当判断任意待验证交易信息的哈希值与目标特征值都互为质数关系成立时, 任意待验证交易信息 T' 不存在于交易状态值 $TxState_n$ 中成立, 则表明所有
25 待验证交易信息都不符合目标条件。

反之, 若任意待验证交易信息的哈希值都与目标特征值不互为质数关系, 换言之, 若任意待验证交易信息的哈希值都能被目标特征值整除, 则任意待验证交易信息的哈希值是交易状态值的幂次方的因子, 也即任意待验证交易信息存在于交易状态值中, 故而, 所有待验证交易信息都符合目标条件。

30 而判断任意待验证交易信息的哈希值是否都与目标特征值互为质数关系, 可以通过确定目标条件函数是否存在整数解得以实现。在一种可能的设计中, 步骤 S304 可能的实现方式如图 7 所示。图 7 为本申请实施例提供的又一种区块验证方法的流程示意图。如图 7 所示, 本申请实施例包括:

S3041: 确定目标条件函数是否存在整数解。

35 其中, 目标条件函数由任意待验证交易信息的哈希值和目标特征值生成。

S3042: 若是, 则任意待验证交易信息的哈希值都与目标特征值均互为质数关系。

S3043: 若否, 则任意待验证交易信息的哈希值与目标特征值均非互为质数关系。

目标条件函数由任意待验证交易信息的哈希值 $Hash(T')$ 和目标特征值生成。

例如, 对于任何整数 a 、 b , 如果 a 和 b 互质, 则存在整数解 $\langle x, y \rangle$ 使得如下公式 (15)

成立:

$$ax + by = 1 \quad (15)$$

比如 2 和 3 互质, 那么 $2x+3y=1$, 显然存在整数解 $(-1, 1)$ 可使得公式 (15) 成立。

而对于整数 a 和 b , 如果 a 和 b 不互质, 则意味着 a 和 b 存在最大公约数, 假设最大
5 公约数为 c , 且 c 为大于 1 的整数, 并假设 $|a| > |b|$, 则肯定存整数 m 和 n 使得如下公式
(16) 和 (17) 存在:

$$a = m * c \quad (16)$$

$$b = n * c \quad (17)$$

结合公式 (16) 和 (17) 则存在如下公式 (18):

$$10 \quad ax + by = m * cx + n * cy = 1 \Rightarrow mx + ny = \frac{1}{c} \quad (18)$$

如果 $ax+by=1$ 在 a 和 b 不互质的情况下还存在整数解, 那么 $mx+ny$ 一定为整数, 但是
由于 c 也为整数, 所以 $1/c$ 一定不为整数, 所以 $mx+ny=1/c$ 一定不成立。故而可以得知,
当 a 和 b 不互质的情况, $ax+by=1$ 一定不存在整数解。

基于以上描述, 则可以由任意待验证交易信息的哈希值 $Hash(T')$ 和目标特征值生成如
15 下公式 (19) 所示的目标条件函数:

$$x * H(T') + y * W_n = 1 \quad (19)$$

其中, 若表示任意待验证交易信息的哈希值 $H(T)$ 即 $Hash(T)$ 与表示目标特征值的 W_n
互为质数关系, 则如公式 (19) 表示的目标条件函数存在整数解 $\langle x, y \rangle$ 。反之, 若表示任意
待验证交易信息的哈希值与表示目标特征值的非互为质数关系, 则如公式 (19) 表示的目标
20 条件函数不存在整数解 $\langle x, y \rangle$ 。

因此, 判断任意待验证交易信息的哈希值是否都与目标特征值互为质数关系, 可以通
过判断目标条件函数是否存在整数解得以实现。

故而, 若轻节点确定出由任意待验证交易信息的哈希值和目标特征值所生成的目标条
件函数存在整数解, 则表明任意待验证交易信息的哈希值与目标特征值均互为质数关系。
25 反之, 若轻节点确定出由任意待验证交易信息的哈希值和目标特征值所生成的目标条件函
数不存在整数解, 则表明任意待验证交易信息的哈希值与目标特征值均不互为质数关系。

通过上述实施例的描述可知, 轻节点接收到目标全节点发送的待验证区块后, 首先对
待验证区块的困难值正确与否进行验证以确定出待验证区块是否满足预设共识机制的首要
条件。在困难值正确的情况下, 进一步对待验证区块的有效性进行验证来完成区块验证。

其中, 轻节点在对待验证区块的有效性验证时, 可以基于其维护的交易状态值进行。具体
地, 轻节点确定由待验证区块包括的任意待验证交易信息的哈希值以及目标特征值所生成
的目标条件函数是否存在整数解。若存在整数解, 则表明任意待验证交易信息的哈希值与
目标特征值都互为质数关系, 即目标特征值无法整除任意待验证交易信息的哈希值, 任意
待验证交易信息的哈希值不为交易状态值的幂次方的因子, 所有待验证交易信息都不符合
30 目标条件, 则可在步骤 S305 后执行步骤 S307。反之, 若轻节点确定由待验证区块包括的
任意待验证交易信息的哈希值以及目标特征值所生成的目标条件函数不存在整数解, 则表
明任意待验证交易信息的哈希值与目标特征值都非互为质数关系, 即目标特征值可以整除
任意待验证交易信息的哈希值, 任意待验证交易信息的哈希值为交易状态值的幂次方的因
子, 则可以确定所有待验证交易信息都符合目标条件, 则可以在步骤 S306 后执行步骤 S308。

S307: 待验证区块未通过验证, 并生成第一反馈信息。

其中, 第一反馈信息用于指示轻节点拒绝待验证区块。

S308: 待验证区块通过验证, 记录待验证区块并向目标全节点发送验证信息。

5 若所有待验证交易信息都不符合目标条件, 则待验证区块未通过验证, 轻节点可以通过生成第一反馈信息来指示自身拒绝待验证区块。

而若所有待验证交易信息都符合目标条件, 则表明待验证区块通过验证, 进而轻节点会记录待验证区块并向目标全节点发送验证信息。当目标全节点接收一定数量的验证信息后即表示其完成对待验证区块的上链。

10 本申请实施例提供的区块验证方法应用于区块链网络中的轻节点。轻节点每当接收到目标账户发送的交易信息, 根据预设更新策略以及当前次接收到的交易信息更新交易状态值。并且, 轻节点接收目标全节点发送的待验证区块后首先确定待验证区块是否满足预设共识机制的首要条件, 若满足, 则根据各当前哈希值以及目标特征函数得到目标特征值, 并通过判断任意待验证交易信息的哈希值是否都与目标特征值互为质数关系, 来确定所有待验证交易信息是否都符合目标条件。经过判断, 若任意待验证交易信息的哈希值都与目标特征值互为质数关系, 则所有待验证交易信息都不符合目标条件。而若任意待验证交易信息的哈希值与目标特征值都不互为质数关系, 则所有待验证交易信息都符合目标条件, 待验证区块通过验证, 轻节点会记录待验证区块并向目标全节点发送验证信息。本申请实施例提供的区块验证方法, 轻节点每当接收到交易信息时都更新交易状态值, 从而通过维护交易状态值代替存储全量的交易信息, 并进一步基于所维护的交易状态值, 通过判断任意待验证交易信息的哈希值是否都与目标特征值互为质数关系, 来实现待验证区块包括的所有待验证交易信息是否都符合目标条件的判断, 达到对待验证区块的验证, 从而无需存储全量的交易信息即可进行区块验证, 为区块链节点运行于轻量化终端设备提供可能。

20 进一步地, 为了避免交易信息发生重复即双花现象, 轻节点确定待验证区块通过验证之后, 还包括如图 8 所示步骤。图 8 为本申请实施例提供的又一种区块验证方法的流程示意图。如图 8 所示, 本申请实施例包括:

S401: 根据所有待验证交易信息以及目标特征函数生成目标数据。

25 S402: 根据目标数据、目标特征值以及预设特征函数更新当前的交易状态值, 以删除所有待验证交易信息。

30 在待验证区块通过验证后, 为了防止交易信息发生重复现象, 则需要对轻节点当前的交易状态值进行更新, 以从轻节点所维护的交易状态值中删除已完成验证的待验证区块所涉及的交易信息, 即删除待验证区块包括的所有待验证交易信息。

假设待验证区块包括 m 起待验证交易信息, 因而可以基于目标特征函数以及所有待验证交易信息生成如下公式 (20) 所示的目标数据 W_m :

$$W_m = \prod_{i=1}^m H(T_i) \quad (20)$$

35 其中, $H(T_i)$ (i 的取值从 1 至 m) 表示待验证区块中该 m 起的所有待验证交易信息的哈希值, 目标数据则基于该 m 起的所有待验证交易信息的哈希值和目标特征函数得到。

目标特征值 w_n 如前述公式 (14) 所示。预设特征函数如下公式 (21) 所示:

$$TxRoot_{n-m} = \frac{w_n}{w_m} \bmod N \quad (21)$$

其中, 通过目标数据、目标特征值以及公式 (21) 所示的预设特征函数生成最终的交

易状态值 $TxRoot_{n-m}$ ，以将轻节点在完成区块验证后的当前的交易状态值 $TxState_n$ 更新为最终的交易状态值 $TxRoot_{n-m}$ ，通过该最终的交易状态值 $TxRoot_{n-m}$ 表征轻节点已从交易状态值 $TxState_n$ 中删除了待验证区块所包括的所有 m 起待验证交易信息，进而则可再继续接收新的交易信息。

- 5 本申请实施例提供的区块验证方法，在待验证区块通过验证之后，为了防止交易信息发生重复，根据所有待验证交易信息以及目标特征函数生成目标数据，并根据该目标数据、目标特征值以及预设特征函数生成最终的交易状态值，以将当前的交易状态值更新为最终的交易状态值，从轻节点的交易状态值中删除通过验证的待验证区块所包括的所有待验证交易信息。可见，基于其所维护的交易状态值可以防止交易信息发生重复问题。并且，待验证区块通过验证后，对其所维护的交易状态值进行更新后再重新接收新的交易信息，可以
- 10 可以保证轻节点的存储空间不会随着其接收到的交易信息和待验证区块的不断累计而发生变化，从而更加有利于区块链节点运行于轻量化终端设备中。

- 15 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他实施方案。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。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由权利要求书指出。

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书来限制。

权 利 要 求 书

1、一种区块验证方法，其特征在于，应用于区块链网络中的轻节点；所述方法，包括：

接收目标全节点发送的待验证区块，并确定所述待验证区块是否满足预设共识机制的首要条件，所述目标全节点是在所述区块链网络的全节点中选举得到；

若是，判断所述待验证区块包括的所有待验证交易信息是否都符合目标条件，所述目标条件根据交易状态值获得，所述交易状态值用于表征所述轻节点已接收到的交易信息；

若确定所述所有待验证交易信息都符合所述目标条件，则所述待验证区块通过验证。

2、根据权利要求1所述的区块验证方法，其特征在于，在所述接收目标全节点发送的待验证区块之前，还包括：

每当接收到目标账户发送的所述交易信息，根据预设更新策略以及当前次接收到的交易信息更新所述交易状态值。

3、根据权利要求2所述的区块验证方法，其特征在于，所述根据预设更新策略以及当前次接收到的交易信息更新交易状态值，包括：

获取当前哈希值，所述当前哈希值为所述当前次接收到的交易信息的哈希值；

根据所述当前哈希值、预设更新算法以及当前的交易状态值生成目标交易状态值，所述预设更新算法包括目标参数和目标特征函数，所述目标参数为互为质数的第一参数和第二参数的乘积；

利用预设更新方式以及所述目标交易状态值更新所述交易状态值；

其中，所述预设更新策略包括所述预设更新算法和所述预设更新方式。

4、根据权利要求3所述的区块验证方法，其特征在于，在所述轻节点首次接收所述目标账户发送的交易信息之前，还包括：

随机生成初始的交易状态值，所述初始的交易状态值为任意质数的预设常数。

5、根据权利要求3或4所述的区块验证方法，其特征在于，所述判断所述待验证区块包括的所有待验证交易信息是否都符合目标条件，包括：

根据各当前哈希值以及所述目标特征函数得到目标特征值；

判断任意待验证交易信息的哈希值是否都与所述目标特征值互为质数关系；

若是，则确定所述所有待验证交易信息都不符合所述目标条件；

若否，则确定所述所有待验证交易信息都符合所述目标条件。

6、根据权利要求5所述的区块验证方法，其特征在于，所述判断任意待验证交易信息的哈希值是否都与所述目标特征值互为质数关系，包括：

确定目标条件函数是否存在整数解，所述目标条件函数由所述任意待验证交易信息的哈希值和所述目标特征值生成；

若是，则确定所述任意待验证交易信息的哈希值都与所述目标特征值均互为所述质数关系；

若否，则确定所述任意待验证交易信息的哈希值与所述目标特征值均非互为所述质数关系。

7、根据权利要求 1-6 任一项所述的区块验证方法，其特征在于，若确定所述所有待验证交易信息都不符合所述目标条件，则所述待验证区块未通过验证，并生成第一反馈信息，所述第一反馈信息用于指示所述轻节点拒绝所述待验证区块。

5 8、根据权利要求 1-7 任一项所述的区块验证方法，其特征在于，若所述预设共识机制为 PoW 共识机制，所述确定所述待验证区块是否满足预设共识机制的首要条件，包括：

验证所述待验证区块的困难值是否正确，所述 PoW 共识机制的首要条件包括所述困难值；

若是，确定所述待验证区块满足所述首要条件；

10 若否，确定所述待验证区块未通过验证，并生成第二反馈信息，所述第二反馈信息用于指示所述轻节点拒绝所述待验证区块。

9、根据权利要求 6 所述的区块验证方法，其特征在于，在确定所述待验证区块通过验证之后，还包括：

根据所述所有待验证交易信息以及所述目标特征函数生成目标数据；

15 根据所述目标数据、所述目标特征值以及预设特征函数更新当前的交易状态值，以删除所述所有待验证交易信息。

10、根据权利要求 1-9 任一项所述的区块验证方法，其特征在于，若确定所述待验证区块通过验证，则记录所述待验证区块并向所述目标全节点发送验证信息。

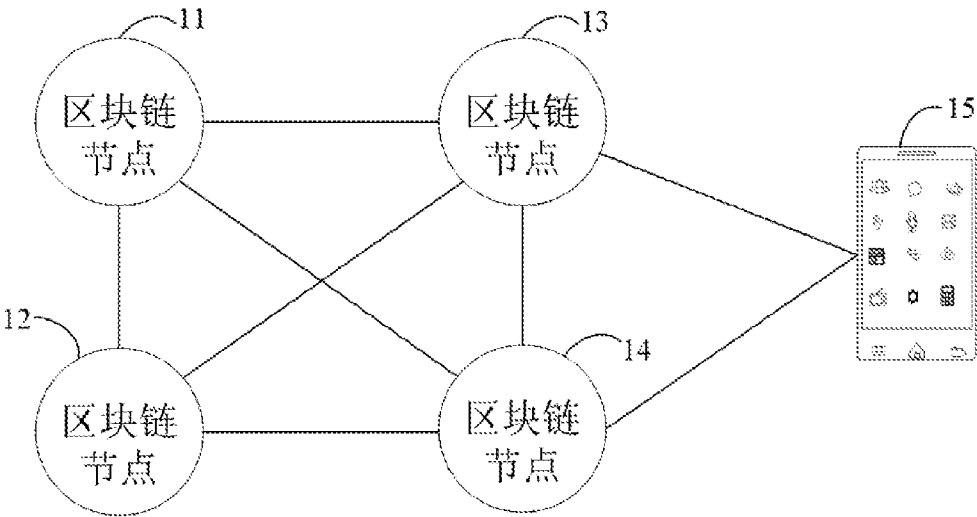


图 1

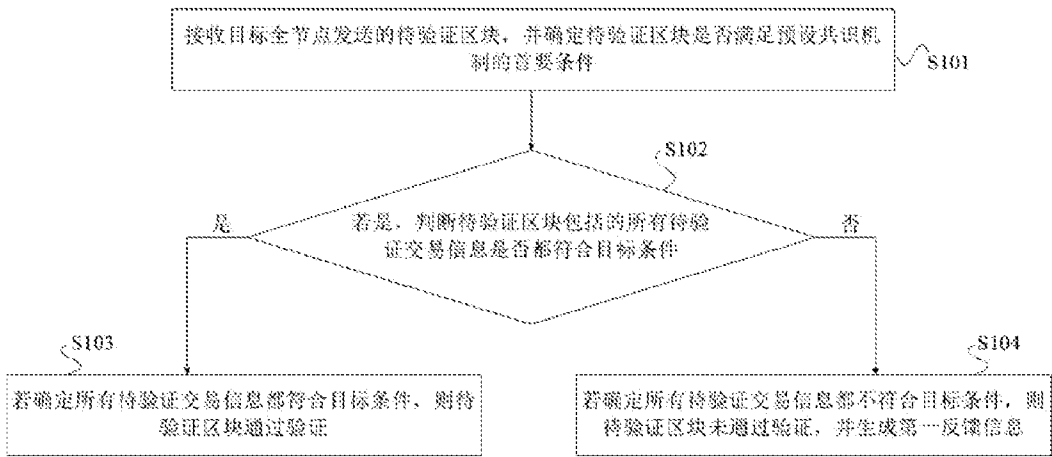


图 2

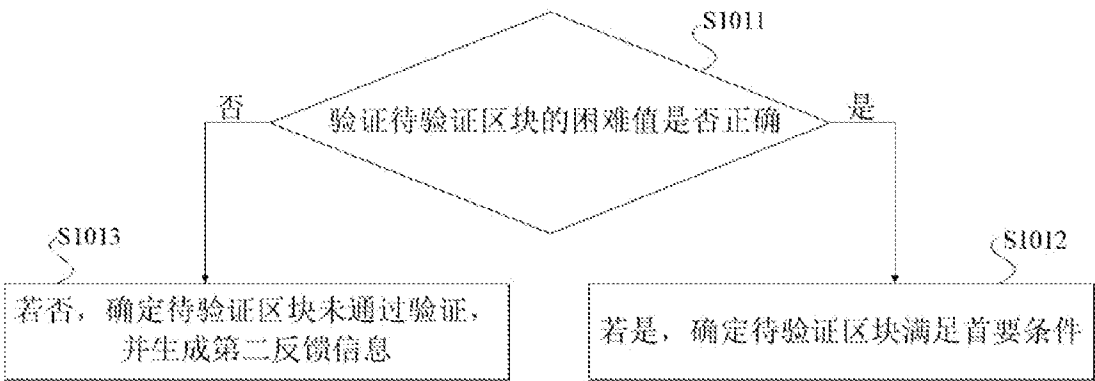


图 3

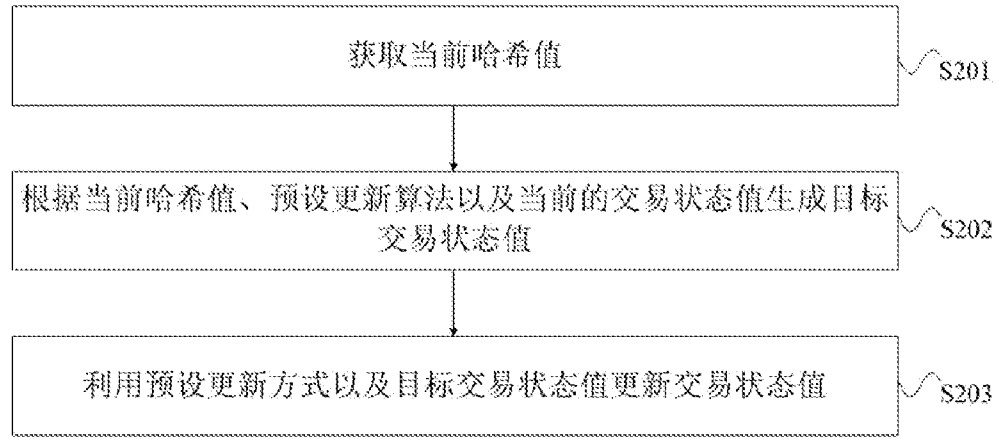


图 4

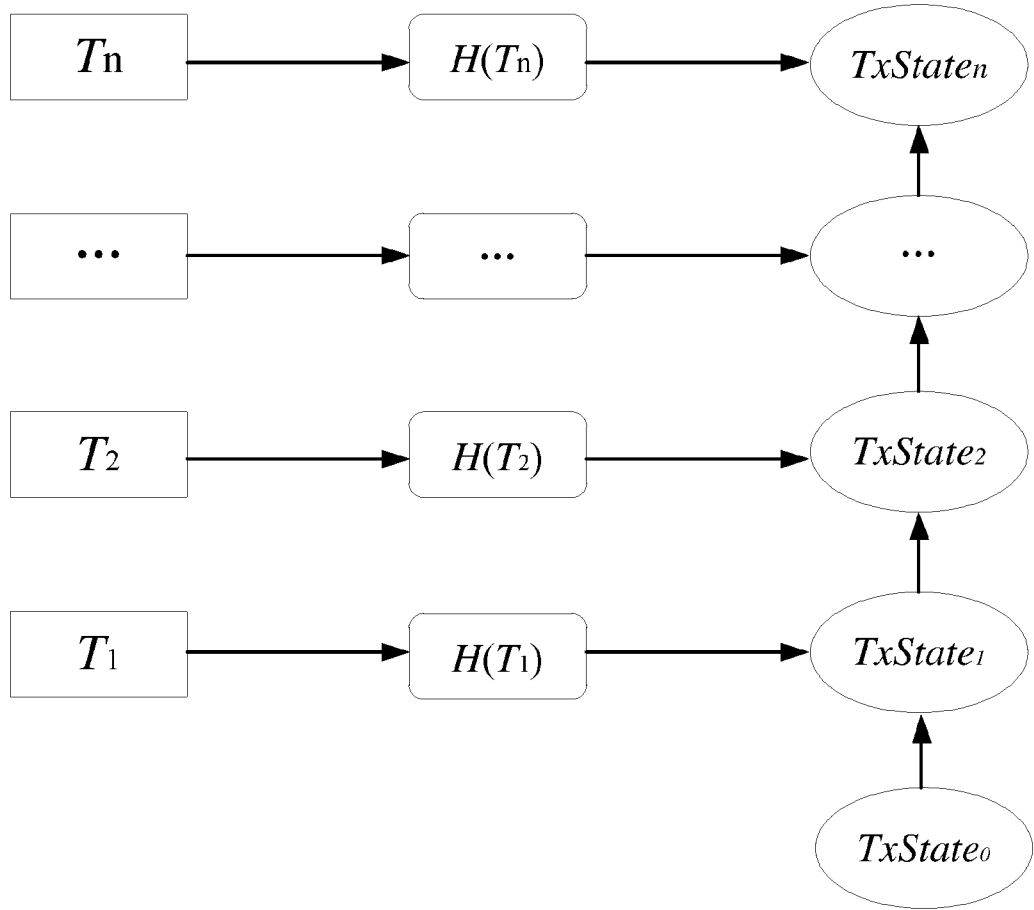


图 5

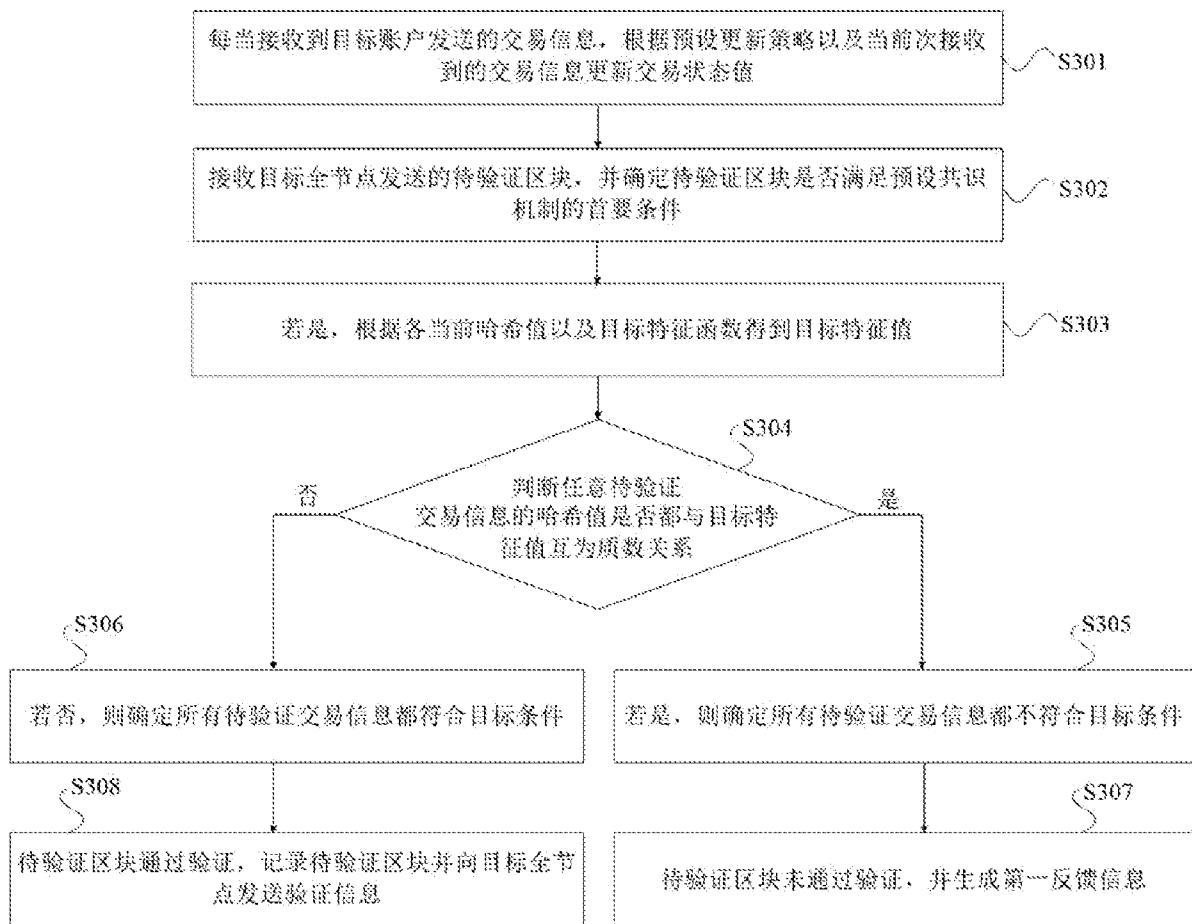


图 6

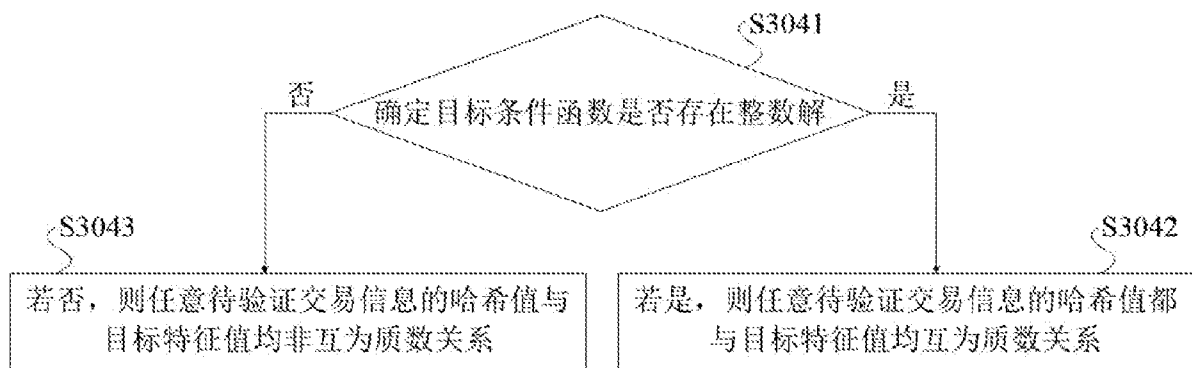


图 7

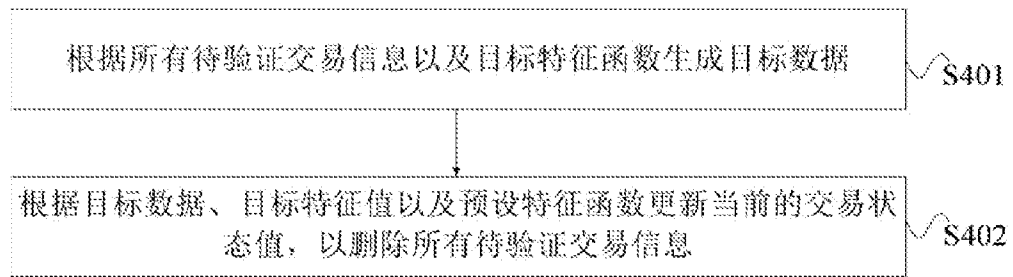


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/140630

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; G06Q 40/04(2012.01)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; G06Q

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)

CNTXT; CNABS; CNKI; WPABS; ENTXT; IEEE: 交易, 区块, 待验证, 共识, 签名, 哈希, 轻节点, 轻量节点, trade, transaction, deal, block, verified, consensus, sign, HASH, light w node, SPV, simplified w payment w verification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 113556238 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 26 October 2021 (2021-10-26) claims 1-10	1-10
X	CN 111010284 A (SHENZHEN ONETHING TECHNOLOGY CO., LTD.) 14 April 2020 (2020-04-14) description, paragraphs 52-148, and figures 1-3	1-10
A	CN 108921556 A (SHANGHAI DAJIAYING INFORMATION TECHNOLOGY CO., LTD.) 30 November 2018 (2018-11-30) entire document	1-10
A	CN 110602116 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 20 December 2019 (2019-12-20) entire document	1-10
A	CN 108985772 A (SHANGHAI DAJIAYING INFORMATION TECHNOLOGY CO., LTD.) 11 December 2018 (2018-12-11) 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

02 June 2022

Date of mailing of the international search report

09 June 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

International application No.

PCT/CN2021/140630

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 112396423 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 23 February 2021 (2021-02-23) entire document	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/140630

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	113556238	A	26 October 2021	None	
CN	111010284	A	14 April 2020	None	
CN	108921556	A	30 November 2018	None	
CN	110602116	A	20 December 2019	None	
CN	108985772	A	11 December 2018	None	
CN	112396423	A	23 February 2021	None	

国际检索报告

国际申请号

PCT/CN2021/140630

A. 主题的分类

H04L 9/32 (2006.01) i; G06Q 40/04 (2012.01) 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; G06Q

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))

CNTXT; CNABS; CNKI; WPABS; ENTXT; IEEE: 交易, 区块, 待验证, 共识, 签名, 哈希, 轻节点, 轻量节点, trade, transaction, deal, block, verified, consensus, sign, HASH, light w node, SPV, simplified w payment w verification

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 113556238 A (深圳前海微众银行股份有限公司) 2021年10月26日 (2021 - 10 - 26) 权利要求1-10	1-10
X	CN 111010284 A (深圳市网心科技有限公司) 2020年4月14日 (2020 - 04 - 14) 说明书第52-148段, 附图1-3	1-10
A	CN 108921556 A (上海达家迎信息科技有限公司) 2018年11月30日 (2018 - 11 - 30) 全文	1-10
A	CN 110602116 A (腾讯科技深圳有限公司) 2019年12月20日 (2019 - 12 - 20) 全文	1-10
A	CN 108985772 A (上海达家迎信息科技有限公司) 2018年12月11日 (2018 - 12 - 11) 全文	1-10
A	CN 112396423 A (腾讯科技深圳有限公司) 2021年2月23日 (2021 - 02 - 23) 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6月2日

国际检索报告邮寄日期

2022年6月9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

受权官员

罗芳洁

电话号码 86- (010) -62411638

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/140630

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	113556238	A	2021年10月26日	无	
CN	111010284	A	2020年4月14日	无	
CN	108921556	A	2018年11月30日	无	
CN	110602116	A	2019年12月20日	无	
CN	108985772	A	2018年12月11日	无	
CN	112396423	A	2021年2月23日	无	