

(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
2020 年 4 月 30 日 (30.04.2020)



(10) 国际公布号
WO 2020/082883 A1

- (51) 国际专利分类号:
G06Q 40/04 (2012.01)
- (21) 国际申请号: PCT/CN2019/102777
- (22) 国际申请日: 2019 年 8 月 27 日 (27.08.2019)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201811258150.7 2018年10月26日 (26.10.2018) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 马宝利(MA, Baoli); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 张文彬(ZHANG, Wenbin); 中国浙江省杭州市余杭区文一西路

969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 刘正(LIU, Zheng); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 宋旭阳(SONG, Xuyang); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 崔嘉辉(CUI, Jiahui); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街9号嘉华大厦B座409, Beijing 100085 (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,

(54) Title: OBJECT SELECTION METHOD AND DEVICE AND ELECTRONIC DEVICE

(54) 发明名称: 对象选取方法及装置、电子设备

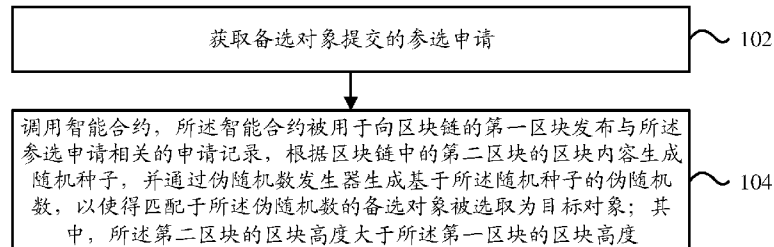


图 1

102 Acquire a candidacy application submitted by a candidate object

104 Invoke an intelligent contract, the intelligent contract being used to issue an application record related to the candidacy application to a first block of a blockchain, generate a random seed according to block content of a second block of the blockchain, and generate a pseudo-random number on the basis of the random seed by means of a pseudo-random number generator such that a candidate object matching the pseudo-random number is selected to be a target object, wherein the block height of the second block is greater than that of the first block

(57) Abstract: An object selection method and device, and an electronic device, which are applied to a blockchain node. The method comprises: acquiring a candidacy application submitted by a candidate object (102); invoking an intelligent contract, the intelligent contract being used to issue an application record related to the candidacy application to a first block of a blockchain, generating a random seed according to block content of a second block of the blockchain, and generating a pseudo-random number on the basis of the random seed by means of a pseudo-random number generator such that a candidate object matching the pseudo-random number is selected to be a target object, wherein the block height of the second block is greater than that of the first block (104).

(57) 摘要: 一种对象选取方法及装置、电子设备, 应用于区块链节点; 方法包括: 获取备选对象提交的参选申请 (102); 调用智能合约, 智能合约被用于向区块链的第一区块发布与参选申请相关的申请记录, 根据区块链中的第二区块的区块内容生成随机种子, 并通过伪随机数发生器生成基于随机种子的伪随机数, 以使得匹配于伪随机数的备选对象被选取为目标对象; 其中, 第二区块的区块高度大于第一区块的区块高度 (104)。

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))。

对象选取方法及装置、电子设备

技术领域

[01] 本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种对象选取方法及装置、电子设备。

5 背景技术

[02] 当某一事件被设定为由预设数量的对象实施时，如果备选对象的数量超出该预设数量，则需要从这些备选对象中进行选择。当这些备选对象对于该事件的实施并无明显区别时，可以从这些备选对象中随机选取上述预设数量的对象。例如，当系统内包含 10 台设备时，如果希望配置为 2 台主设备、8 台从设备的架构，可以从该 10 台设备中随机选取 2 台主设备，则剩余的 8 台设备为从设备。

发明内容

[03] 有鉴于此，本说明书一个或多个实施例提供一种对象选取方法及装置、电子设备。

[04] 为实现上述目的，本说明书一个或多个实施例提供技术方案如下：

[05] 根据本说明书一个或多个实施例的第一方面，提出了一种对象选取方法，应用于区块链节点；所述方法包括：

[06] 获取备选对象提交的参选申请；

[07] 调用智能合约，所述智能合约被用于向区块链的第一区块发布与所述参选申请相关的申请记录，根据区块链中的第二区块的区块内容生成随机种子，并通过伪随机数发生器生成基于所述随机种子的伪随机数，以使得匹配于所述伪随机数的备选对象被选取为目标对象；其中，所述第二区块的区块高度大于所述第一区块的区块高度。

[08] 根据本说明书一个或多个实施例的第二方面，提出了一种对象选取装置，应用于区块链节点；所述装置包括：

[09] 获取单元，获取备选对象提交的参选申请；

[10] 调用单元，调用智能合约，所述智能合约被用于向区块链的第一区块发布与所述参

选申请相关的申请记录，根据区块链中的第二区块的区块内容生成随机种子，并通过伪随机数发生器生成基于所述随机种子的伪随机数，以使得匹配于所述伪随机数的备选对象被选取为目标对象；其中，所述第二区块的区块高度大于所述第一区块的区块高度。

[11]根据本说明书一个或多个实施例的第三方面，提出了一种电子设备，包括：

5 [12]处理器；

[13]用于存储处理器可执行指令的存储器；

[14]其中，所述处理器通过运行所述可执行指令以实现如上述实施例中任一所述的方法。

附图说明

[15]图 1 是一示例性实施例提供的一种对象选取方法的流程图。

10 [16]图 2 是一示例性实施例提供的一种摇号选购不动产的示意图。

[17]图 3 是一示例性实施例提供的一种基于智能合约的摇号过程的示意图。

[18]图 4 是一示例性实施例提供的一种设备的结构示意图。

[19]图 5 是一示例性实施例提供的一种对象选取装置的框图。

具体实施方式

15 [20]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说明书一个或多个实施例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、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

20 [21]需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

25 [22]图 1 是一示例性实施例提供的一种对象选取方法的流程图。如图 1 所示，该方法应用于区块链节点，可以包括以下步骤：

[23] 步骤 102, 获取备选对象提交的参选申请。

[24] 在一实施例中, 备选对象通过提交参选申请, 使得智能合约可以向区块链发布相应的申请记录, 从而确保相应的备选对象能够参与到对象的选取过程中。

5 [25] 在一实施例中, 参选申请可以包含备选对象的身份信息, 比如该备选对象通过私钥生成的签名等, 而该身份信息可以被添加至申请记录中, 以表明该申请记录与该备选对象之间的关联关系。

10 [26] 步骤 104, 调用智能合约, 所述智能合约被用于向区块链的第一区块发布与所述参选申请相关的申请记录, 根据区块链中的第二区块的区块内容生成随机种子, 并通过伪随机数发生器生成基于所述随机种子的伪随机数, 以使得匹配于所述伪随机数的备选对象被选取为目标对象; 其中, 所述第二区块的区块高度大于所述第一区块的区块高度。

15 [27] 在一实施例中, 可以在区块链的客户端上创建交易 (transfer), 从而通过该交易将备选对象对应的申请记录发布至区块链上, 成为区块链的分布式数据库中的一笔数据。需要指出的是: 区块链中的交易, 存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移; 例如, 在传统的比特币区块链网络中, 交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔具有业务意图的业务数据; 例如, 运营方可以基于实际的业务需求搭建一个联盟链, 依托于联盟链部署一些与价值转移无关的其它类型的在线业务(比如, 对象选取业务、租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等), 而在这类联盟链中, 交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求。本说明书中的
20 交易, 应当倾向于理解为广义上的交易。

[28] 在一实施例中, 由于区块链采用分布式数据库, 使得发布至区块链上的申请记录无法被篡改, 可以确保真实、可靠。

25 [29] 在一实施例中, 当申请记录被发布至区块链中的第一区块, 而随机种子与区块高度大于第一区块的第二区块相关时, 基于区块链中各个区块之间的链式关系, 使得申请记录的加入可以增加随机种子的不确定性, 无法被不法分子预测和设定, 使得基于该随机种子产生的伪随机数同样具备高度随机性, 可以极大地降低不法分子造假作弊的可能性。

[30] 同时, 由于随机种子的生成过程、伪随机数的生成过程均由智能合约实现, 而智能合约被存证于区块链中, 使得该智能合约的内容公开且不可篡改, 使得对于目标对象的选择过程公平、公开、可验证, 进一步降低了不法分子造假作弊的可能性。

[31]在一实施例中，智能合约可以根据每一备选对象已有的数字形式的标识信息，确定与伪随机数之间的匹配情况。例如，该标识信息可以为各个备选对象的用户 ID、公钥的取值等，本说明书并不对此进行限制。

5 [32]在一实施例中，所述智能合约还用于：为每一备选对象分别生成申请编号，每一申请编号对应于唯一的备选对象；其中，当所述伪随机数与任一申请编号相同时，所述任一申请编号对应的备选对象被确定为匹配于所述伪随机数。

[33]在一实施例中，可以按照预设方式为备选对象生成申请编号，比如各个备选对象提交参选申请的顺序、各个备选对象的公钥的取值大小等，本说明书并不对此进行限制。举例而言，所述申请编号与所述备选对象对应的唯一标识的取值相关，所述唯一标识的
10 取值由与区块链中的历史区块相关的哈希值和所述备选用户的公钥进行哈希计算而得到，这样可以增加该唯一标识的取值的随机性，降低被不法分子操控的可能性。

[34]在一实施例中，当所述备选对象的中签率为标准中签率的 x 倍时，所述备选对象存在 x 个申请编号；其中， x 为正整数。比如，当 $x=1$ 时，备选对象存在 1 个申请编号，当 $x=2$ 时，备选对象存在 2 个申请编号；当申请编号的数量越多时，备选对象被选中的
15 概率也越大，即中签率更高。

[35]在一实施例中，智能合约在收到任一对象的参选申请后，可以根据预定义的参选条件判断该任一对象是否符合要求，当符合要求时可以将其设定为上述的备选用户，使其能够参与到对象选取过程中。同时，智能合约可以基于该备选用户的信息，确定其中签率；例如，智能合约可以从区块链账本中查询该备选对象历史上参与对象选取的次数，
20 并按照设定的计算公式确定出中签率，其中该中签率可以与次数呈正相关。

[36]在一实施例中，所述智能合约用于将与区块链中的历史区块相关的哈希值与所述备选对象的公钥进行哈希计算，得到相应的唯一标识；当 x 的取值从小至大地分别包括 $x_1 \sim x_n$ 时，所述智能合约用于依次选取 $x_1 \sim x_n$ ；其中，当选取 x_i 时，所述智能合约将中签率不小于标准中签率的 x_i 倍的备选对象对应的唯一标识按照从小至大依次排列，并在
25 已有申请编号之后、按照排列次序接续生成相应的申请编号， $1 \leq i \leq n$ 。

[37]假定备选对象的数量为 m 个。在依次选取 $x_1 \sim x_n$ 时：首先选取 x_1 并假定 $x_1=1$ ，那么“中签率不小于标准中签率的 x_i 倍的备选对象”为所有的 m 个备选对象，并且此时尚未存在申请编号，因而可以直接生成相应的 m 个申请编号为 $1 \sim m$ ；然后选取 x_2 并假定 $x_2=2$ ，那么“中签率不小于标准中签率的 x_i 倍的备选对象”为 $x_2 \sim x_n$ 倍中签率的备

选对象、不包含 x_1 倍中签率的备选对象，譬如 $x_2 \sim x_n$ 倍中签率的备选对象的数量为 a ，由于已存在上述的申请编号 $1 \sim m$ ，因而可以在 m 之后接续生成 a 个申请编号，即 $m+1 \sim m+a$ ，此时 x_1 倍中签率的备选对象存在 1 个申请编号、 $x_2 \sim x_n$ 倍中签率的备选对象存在 2 个申请编号；然后选取 x_3 并假定 $x_3=3$ ，那么“中签率不小于标准中签率的 x_i 5 倍的备选对象”为 $x_3 \sim x_n$ 倍中签率的备选对象、不包含 $x_1 \sim x_2$ 倍中签率的备选对象，譬如 $x_3 \sim x_n$ 倍中签率的备选对象的数量为 b ，由于已存在上述的申请编号 $1 \sim m+a$ ，因而可以在 $m+a$ 之后接续生成 b 个申请编号，即 $m+a+1 \sim m+a+b$ ，此时 x_1 倍中签率的备选对象存在 1 个申请编号、 x_2 倍中签率的备选对象存在 2 个申请编号、 $x_3 \sim x_n$ 倍中签率的备选对象存在 3 个申请编号。类似地，通过上述方式依次选取至 x_n 后，可以确保备选对象 10 具有的申请编号的数量与其对应的中签率倍数相同。

[38]在一实施例中，所述目标对象的总数为 w ；所述智能合约用于在已选取的目标对象的数量未达到 w 时，将所述随机种子和采样区间 $[M, N]$ 作为输入、通过所述伪随机数发生器生成 1 个伪随机数，其中 M 为申请编号的最小值、 N 为申请编号的最大值。换言之，在每次生成伪随机数时，采用的采样区间均覆盖所有的申请编号，而不会剔除已被 15 选取的目标对象对应的申请编号，可以确保各个备选对象的实际中签概率在每次产生伪随机数时都不变，避免剔除目标对象对应的申请编号而导致其他备选用户的实际中签概率增大，从而确保公平性。

[39]在一实施例中，所述智能合约用于将每一备选对象对应的申请编号存证于区块链中，使得备选用户或监管方可以随时从区块链中对申请编号进行查验，避免发生造假作弊。

20 [40]在一实施例中，所述随机种子还与区块链中的一个或多个其他区块的区块内容相关，使得不法分子即便具备区块攻击能力，也必须分别攻击第二区块和该其他区块才能够达成目的，造成了极高的攻击成本，可以极大地降低不法分子操控随机种子的可能性。

[41]在一实施例中，所述一个或多个其他区块包括：包含至少一条申请记录的区块，使得所有的申请记录均可以影响到随机种子，可以增加随机种子的不确定性，降低被不法 25 分子猜测或操控的可能性。

[42]在一实施例中，所述一个或多个其他区块包括：与所述第二区块相邻的一个或多个区块。比如当该一个或多个其他区块的数量为 r 时，可以选取第二区块之前的 r 个区块；或者，可以在生成第二区块之后，等待区块链中继续产生 r 个区块，并基于该第二区块和该 r 个区块生成随机种子。

[43]在一实施例中,所述智能合约用于通过下述公式对所述第二区块和 r 个其他区块(比如上述包含申请记录的一个或多个区块,或者位于第二区块之后的一个或多个区块)的区块内容进行处理,以确定出所述实际结果:

$$H'1=H(Hp, Hr),$$

5 $H'i=H(H'(i-1), H(r-i+1)),$ 其中 $1 < i \leq r;$

[44]其中, H 为预设的哈希函数, Hp 为与所述第二区块的区块内容相关的哈希值, Hi 为与第 i 个其他区块的区块内容相关的哈希值,所述随机种子为 $Hf=H(H'r, Hp)$ 。

[45]在一实施例中,在通过上述公式进行计算的过程中, r 个其他区块之间可以按照预设顺序进行依次排列,形成第1个其他区块、...、第 r 个其他区块,比如该预设顺序
10 可以包括区块高度从小至大的顺序、区块内容的哈希值从小至大的顺序等,本说明书并不对此进行限制。

[46]在一实施例中,所述智能合约用于在区块链中产生第三区块后,生成所述随机种子;其中,所述第三区块的区块高度大于所述第二区块,且高度差为预设数值。换言之,智能合约虽然基于第二区块的区块内容来确定随机种子,但是产生该第二区块后并不立即
15 确定随机种子,而是等待预设数量个区块之后,才确定该随机种子,保证了第二区块的安全性,使得攻击者必须连续攻击第二区块与第三区块之间的所有区块,使得攻击成本极高,可以极大地降低不法分子操控随机种子的可能性。

[47]为了便于理解,下面以选购不动产时的摇号过程为例,对本说明书的对象选取方案进行描述。图2是一示例性实施例提供的一种摇号选购不动产的示意图;如图2所示,
20 假定用户A希望参与针对某一楼盘的摇号,该用户A可以通过安装有客户端的手机21提交申请摇号资格所需的摇号申请,比如身份证明材料、存款证明材料、对应于数字身份的公钥、个人资料等,这取决于楼盘开发商或相关法律法规的要求。

[48]设备22被配置为摇号系统的服务端,该设备22一方面与用户A使用的手机21进行交互、以协助其申请摇号资格,另一方面与设备23进行交互。设备23被配置为区块
25 链中的一个区块链节点,基于设备22所提供的信息,可以配置、发布智能合约,并通过调用智能合约以实现摇号资格的申请和摇号操作等。楼盘开发商或摇号公证部门可以对智能合约进行配置,以设定对摇号资格的申请条件、摇号过程包含的各个阶段(如基于时间划分各个阶段或者基于区块链上的区块高度划分各个阶段等)、每一阶段所采取的处理逻辑等,使得该智能合约可以用于实现本说明书的对象选取方案,以完成相应的

摇号操作。

[49]假定已完成对智能合约的配置过程，并且该智能合约已被发布至区块链中，那么基于该智能合约可以实现如图 3 所示的摇号过程，该过程可以包括以下步骤：

[50]步骤 301，用户申请摇号资格。

- 5 [51]在一实施例中，用户 A 可以通过手机 21 向设备 22 提交摇号申请，并经由设备 23 向区块链中提交包含该摇号申请的交易，该交易的类型可以被配置或标记为申请摇号资格的类型。类似地，其他用户也可以通过上述方式申请摇号资格，从而与用户 A 一并参与摇号。

- 10 [52]除了通过设备 23 向区块链提交包含摇号申请的交易之外，用户 A 也可以通过其他区块链节点向区块链提交包含摇号申请的交易，比如该手机 21 可以被配置为一区块链节点，那么用户 A 可以基于该手机 21 向区块链提交包含摇号申请的交易。

[53]上述包含摇号申请的交易可以被记录至区块链账本中，智能合约可以从区块链账本中进行查询和访问，以获取这些交易中包含的摇号申请，从而验证相应的用户是否可以获得摇号资格。

- 15 [54]在一实施例中，以设备 23 为例，设备 23 可以获知智能合约的名称或位置等信息，使得设备 23 可以直接将摇号申请发送至智能合约，而智能合约可以针对收到的摇号申请进行验证，以确定相应的用户是否可以获得摇号资格。

[55]步骤 302，智能合约验证用户信息。

- 20 [56]在一实施例中，智能合约获得某一用户的摇号申请后，可以按照预先定义的申请条件对该摇号申请进行验证，以确定其是否满足该申请条件；如果满足，则判定相应的用户具备摇号资格，否则判定为不具备摇号资格。

[57]在一实施例中，摇号申请中包含对应用户的公钥和其他个人信息，且摇号申请应当由用户的私钥进行签名，以确保其内容的真实有效、不可篡改。

[58]步骤 303，智能合约将验证结果存证于区块链账本中。

- 25 [59]在一实施例中，通过将验证结果存证于区块链账本中，相当于对验证结果进行公示，使得验证结果透明、可追溯，并且无法随意篡改验证结果，确保对于摇号申请的验证符合要求，避免暗箱操作。

[60]步骤 304，智能合约为通过验证的用户生成资格编号，并将资格编号存证于区块链

账本中。

[61]在一实施例中，假定以区块高度来划分各个阶段，智能合约可以定义申请阶段、编号阶段、摇号阶段等每一阶段对应的区块高度范围，比如申请阶段对应的区块高度为 T0-T1、编号阶段对应的区块高度为 T2-T3、摇号阶段对应的区块高度为 T4-T5。那么，对于申请阶段而言，智能合约可以从区块链账本中读取处于 T0-T1 高度的区块内记录的摇号申请，只有这些摇号申请有可能参与到本次摇号过程中，而其他区块内的摇号申请则无法参与到本次摇号过程中。

[62]在一实施例中，智能合约可以按照预设的方式为通过验证的用户生成资格编号，本说明书并不对此进行限制。举例而言，可以通过如下方式生成资格编号：

[63]首先，确定各个用户的中签率。智能合约可以从区块链账本中读取和统计各个用户在历史上参与的摇号活动，并基于该统计数据确定中签率；例如，当历史上参与的摇号次数不大于第一数值时，中签率可以为标准中签率，当摇号次数大于第一数值、不大于第二数值时，中签率可以为标准中签率的 2 倍，当摇号次数大于第二数值、不大于第三数值时，中签率可以为标准中签率的 3 倍，以此类推。当然，各个用户的中签率也可以通过其他方式计算得到，并记录至区块链账本中，而智能合约只需要从区块链账本中读取通过验证的各个用户分别对应的中签率即可。

[64]其次，智能合约可以基于通过验证的各个用户的公钥 pk、指定的历史区块的哈希值 PreH，分别计算各个用户对应的过渡 ID。例如，智能合约中可以设定有哈希函数 H()，则各个用户对应的过渡 ID 可以为 $H(\text{PreH}, \text{pk})$ ，即通过哈希函数 H() 对哈希值 PreH 和公钥 pk 进行计算，得到相应的哈希值，使得该过渡 ID 具有极高的随机性，无法被不法分子操控。

[65]然后，智能合约可以根据生成的过渡 ID，为各个用户分别赋予相应的资格编号。假定通过验证的用户为 $U_1 \sim U_m$ ，这些用户的中签率分别为标准中签率的 1 倍、2 倍、3 倍...n 倍，那么智能合约可以实施下述操作：

[66]从用户 $U_1 \sim U_m$ 中，选取中签率不小于标准中签率的 1 倍的所有用户，即用户 $U_1 \sim U_m$ 均被选中；按照过渡 ID 从小至大的顺序，对被选中的 m 个用户进行依次排列，然后基于排列次序生成相应的资格编号。由于尚未存在已生成的资格编号，因而此时生成的资格编号可以从头开始，比如为过渡 ID 最小的用户生成资格编号为 1、为过渡 ID 第二小的用户生成资格编号为 2，直至为过渡 ID 最大的用户生成资格编号为 m。因此，针对

中签率不小于标准中签率的 1 倍的所有用户,此时可以生成相应的 m 个资格编号,分别为上述的 $1\sim m$;换言之,此时每一用户分别具有 1 个对应的资格编号。

[67]进一步地,从用户 $U1\sim Um$ 中,选取中签率不小于标准中签率的 2 倍的所有用户,即中签率为标准中签率的 $2\sim n$ 倍的用户,假定这些用户的数量为 a ;按照过渡 ID 从小至大的顺序,对被选中的 a 个用户进行依次排列,然后基于排列次序生成相应的资格编号。由于存在已生成的资格编号 $1\sim m$,因而此时接续生成资格编号,比如为过渡 ID 最小的用户生成资格编号为 $m+1$ 、为过渡 ID 第二小的用户生成资格编号为 $m+2$,直至为过渡 ID 最大的用户生成资格编号为 $m+a$ 。因此,针对中签率不小于标准中签率的 2 倍的所有用户,此时可以生成相应的 a 个资格编号,分别为上述的 $m+1\sim m+a$ 。此时,对于中签率为标准中签率的 1 倍的用户,每一用户存在 1 个资格编号;而对于中签率不小于标准中签率的 2 倍的用户,每一用户存在 2 个资格编号。

[68]进一步地,从用户 $U1\sim Um$ 中,选取中签率不小于标准中签率的 3 倍的所有用户,即中签率为标准中签率的 $3\sim n$ 倍的用户,假定这些用户的数量为 b ;按照过渡 ID 从小至大的顺序,对被选中的 b 个用户进行依次排列,然后基于排列次序生成相应的资格编号。由于存在已生成的资格编号 $1\sim m+a$,因而此时接续生成资格编号,比如为过渡 ID 最小的用户生成资格编号为 $m+a+1$ 、为过渡 ID 第二小的用户生成资格编号为 $m+a+2$,直至为过渡 ID 最大的用户生成资格编号为 $m+a+b$ 。因此,针对中签率不小于标准中签率的 3 倍的所有用户,此时可以生成相应的 b 个资格编号,分别为上述的 $m+a+1\sim m+a+b$ 。此时,对于中签率为标准中签率的 1 倍的用户,每一用户存在 1 个资格编号;而对于中签率不小于标准中签率的 2 倍的用户,每一用户存在 2 个资格编号;而对于中签率不小于标准中签率的 3 倍的用户,每一用户存在 3 个资格编号。

[69]以此类推,智能合约可以针对每一中签率,分别通过上述方式对相应用户分配对应的资格编号,最终使得中签率为标准中签率的 i 倍的用户,能够分配得到 i 个资格编号,其中 $1\leq i\leq n$ 。

[70]在一实施例中,通过将所有参与摇号的用户对应的资格编号存证于区块链账本中,使得各个用户的资格编号公开、透明、可查询且不可篡改,因而在后续的摇号过程中,可以基于该资格编号准确地确定各个用户是否摇中,具有极高的公平性、公开性和可信度。

[71]步骤 305,智能合约监控区块链账本中已生成的区块,在最近区块的区块高度达到 P 时,等待区块链账本中继续生成 Q 个区块后,转入步骤 306。

[72]在一实施例中，P和Q均为预定义的任意取值。当摇号阶段对应的区块高度范围为T4-T5时，应当确保 $T4 < P \leq P+Q < T5$ ；换言之，Q的取值可以为0，即区块高度到达P后即可转入步骤306，而并非必须等待。当 $Q > 0$ 时，Q的取值与区块链中生成区块的速度相关，只需要确保在Q个区块后，该高度为P的区块不会发生变化即可；而通过等待Q个区块，可以保证高度为P的区块的安全性，攻击者必须连续攻击高度为P和P+Q之间的所有区块，使得攻击成本极高，可以极大地降低不法分子操控摇号的可能性。

[73]步骤306，智能合约生成随机种子。

[74]在一实施例中，智能合约可以分别确定出高度为P的区块，以及区块链中包含与本次摇号相关的摇号申请的r个区块，并分别获取这些区块的哈希值（哈希值与对应区块的区块内容相关），比如：高度为P的区块对应于哈希值 H_p ，而r个区块对应的哈希值分别为 $H_1 \sim H_r$ （譬如可以按照区块高度从小至大的顺序进行排列）。进一步的，智能合约可以按照下述公式进行计算：

$$H'_1 = H(H_p, H_r),$$

$$H'_i = H(H'(i-1), H(r-i+1)), \text{ 其中 } 1 < i \leq r;$$

[75]其中，H为预设的哈希函数， $H(H_p, H_r)$ 表示通过该哈希函数H对 H_p 和 H_r 进行哈希运算、得到相应的哈希值为 H'_1 ；类似地， $H(H'(i-1), H(r-i+1))$ 表示通过该哈希函数H对 $H'(i-1)$ 和 $H(r-i+1)$ 进行哈希运算、得到相应的哈希值为 H'_i 。最终，可以计算得到计算结果为 H'_r ，而随机种子为 $H_f = H(H'_r, H_p)$ ，使得所有用户提供的摇号申请均可以对随机种子的取值产生影响，而不法分子无法对所有用户提交的摇号申请进行控制，因而无法对随机种子的取值进行操控。

[76]当然，这里除了选用包含摇号申请的r个区块之外，还可以选用其他类型的区块，本说明书并不对此进行限制。例如，在等待高度为P的区块生成后，继续等待上述的Q个区块，并基于该Q个区块和高度为P的区块生成随机种子；其中：

$$H'_1 = H(H_p, H_Q),$$

$$H'_i = H(H'(i-1), H(Q-i+1)), \text{ 其中 } 1 < i \leq Q;$$

[77]其中，H为预设的哈希函数， $H(H_p, H_Q)$ 表示通过该哈希函数H对 H_p 和 H_Q （假定高度为P的区块的哈希值为 H_p ，此后的Q个区块的哈希值分别为 $H_1, H_2, \dots, H_Q$ ）进行哈希运算、得到相应的哈希值为 H'_1 ；类似地， $H(H'(i-1), H(Q-i+1))$ 表示通过该哈希函数H对 $H'(i-1)$ 和 $H(Q-i+1)$ 进行哈希运算、得到相应的哈希值为 H'_i 。最终，可以计

算得到计算结果为 $H'Q$ ，而随机种子为 $Hf=H(H'Q, H_p)$ 。

[78] 步骤 307，智能合约生成中签号码，将中签号码存证于区块链账本中。

[79] 在一实施例中，智能合约可以调用设定的伪随机数发生器，以用于生成中签号码。

针对为伪随机数发生器的输入数据可以包括：随机种子和采样区间；其中：随机种子为
5 上述过程中生成的 Hf ，而采样区间可以根据各个用户的资格编号的取值范围而生成，
比如当资格编号的最小值为 1、最大值为 Y 时，可以将采样区间设定为 $[1, Y]$ ，使得伪随机数发生器生成的中签号码处于该范围 $[1, Y]$ 中。

[80] 假定中签数量为 w ，当已中签的用户数量小于 w 时，智能合约可以通过伪随机数发生器生成匹配于随机种子 Hf 、采样区间 $[1, Y]$ 的中签号码，并在确定出匹配于中签号码
10 的资格编号后，确认该资格编号对应的用户是否先前已中签，若未中签则确认该用户被抽中，否则本次中签号码无效，需要继续抽取。虽然在此过程中，不断产生已中签的用户，但是应当确保采样区间始终不变、不剔除已中签用户对应的资格编号，以确保每一用户对应的实际中签概率在整个过程中不会发生变化，不会由于剔除已中签用户而导致实际中签概率增大，可以保证摇号的公平性。

[81] 在一实施例中，通过将中签号码存证于区块链账本上，使得用户或监管方可以随时
15 进行查证核验，避免不法分子进行篡改。以用户 A 为例，用户 A 可以通过手机 21 向设备 22 发起查询请求，设备 22 可以通过设备 23 对区块链账本进行查询，并将查询到的摇号结果返回手机 21，以由用户 A 进行查看，确保自己是否具备不动产的选购权限；类似地，当用户 A 对摇号过程存在异议时，同样可以通过上述过程，对区块链账本中的
20 相关数据进行追溯查询，整个过程及其产生的数据均公开透明。

[82] 图 4 是一示例性实施例提供的一种设备的示意结构图。请参考图 4，在硬件层面，该设备包括处理器 402、内部总线 404、网络接口 406、内存 408 以及非易失性存储器 410，当然还可能包括其他业务所需要的硬件。处理器 402 从非易失性存储器 410 中读取对应的计算机程序到内存 408 中然后运行，在逻辑层面上形成对象选取装置。当然，
25 除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限于各个逻辑单元，也可以是硬件或逻辑器件。

[83] 请参考图 5，在软件实施方式中，该对象选取装置应用于区块链节点；该装置可以包括：

[84]获取单元 51, 获取备选对象提交的参选申请;

[85]调用单元 52, 调用智能合约, 所述智能合约被用于向区块链的第一区块发布与所述参选申请相关的申请记录, 根据区块链中的第二区块的区块内容生成随机种子, 并通过伪随机数发生器生成基于所述随机种子的伪随机数, 以使得匹配于所述伪随机数的备选对象被选取为目标对象; 其中, 所述第二区块的区块高度大于所述第一区块的区块高度。

[86]可选的, 所述智能合约还用于: 为每一备选对象分别生成申请编号, 每一申请编号对应于唯一的备选对象; 其中, 当所述伪随机数与任一申请编号相同时, 所述任一申请编号对应的备选对象被确定为匹配于所述伪随机数。

[87]可选的, 所述申请编号与所述备选对象对应的唯一标识的取值相关, 所述唯一标识的取值由与区块链中的历史区块相关的哈希值和所述备选用户的公钥进行哈希计算而得到。

[88]可选的, 当所述备选对象的中签率为标准中签率的 x 倍时, 所述备选对象存在 x 个申请编号; 其中, x 为正整数。

[89]可选的, 所述智能合约用于将与区块链中的历史区块相关的哈希值与所述备选对象的公钥进行哈希计算, 得到相应的唯一标识;

[90]当 x 的取值从小至大地分别包括 $x_1 \sim x_n$ 时, 所述智能合约用于依次选取 $x_1 \sim x_n$; 其中, 当选取 x_i 时, 所述智能合约将中签率不小于标准中签率的 x_i 倍的备选对象对应的唯一标识按照从小至大依次排列, 并在已有申请编号之后、按照排列次序接续生成相应的申请编号, $1 \leq i \leq n$ 。

[91]可选的, 所述目标对象的总数为 w ; 所述智能合约用于在已选取的目标对象的数量未达到 w 时, 将所述随机种子和采样区间 $[M, N]$ 作为输入、通过所述伪随机数发生器生成 1 个伪随机数, 其中 M 为申请编号的最小值、 N 为申请编号的最大值。

[92]可选的, 所述智能合约用于将每一备选对象对应的申请编号存证于区块链中。

[93]可选的, 所述随机种子还与区块链中的一个或多个其他区块的区块内容相关。

[94]可选的, 所述一个或多个其他区块包括: 包含至少一条申请记录的区块。

[95]可选的, 所述一个或多个其他区块包括: 与所述第二区块相邻的一个或多个区块。

[96]可选的, 所述智能合约用于通过下述公式对所述第二区块和 r 个其他区块的区块内容进行处理, 以确定出所述实际结果:

$$H'1=H(Hp, Hr),$$

$$H'i=H(H'(i-1), H(r-i+1)), \text{ 其中 } 1 < i \leq r;$$

[97] 其中，H 为预设的哈希函数，Hp 为与所述第二区块的区块内容相关的哈希值，Hi 为与第 i 个其他区块的区块内容相关的哈希值，所述随机种子为 $Hf=H(H'r, Hp)$ 。

- 5 [98] 可选的，所述智能合约用于在区块链中产生第三区块后，生成所述随机种子；其中，所述第三区块的区块高度大于所述第二区块，且高度差为预设数值。

[99] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、
10 媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[100] 在一个典型的配置中，计算机包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

[101] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM)
15 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存(flash RAM)。内存是计算机可读介质的示例。

[102] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只
20 读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带、磁盘存储、量子存储器、基于石墨烯的存储介质或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可
25 读介质不包括暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

[103] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不

排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[104] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[105] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[106] 应当理解，尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[107] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。

权利要求书

1. 一种对象选取方法，应用于区块链节点；所述方法包括：

获取备选对象提交的参选申请；

5 调用智能合约，所述智能合约被用于向区块链的第一区块发布与所述参选申请相关的申请记录，根据区块链中的第二区块的区块内容生成随机种子，并通过伪随机数发生器生成基于所述随机种子的伪随机数，以使得匹配于所述伪随机数的备选对象被选取为目标对象；其中，所述第二区块的区块高度大于所述第一区块的区块高度。

2. 根据权利要求 1 所述的方法，所述智能合约还用于：为每一备选对象分别生成申请编号，每一申请编号对应于唯一的备选对象；其中，当所述伪随机数与任一申请编
10 号相同时，所述任一申请编号对应的备选对象被确定为匹配于所述伪随机数。

3. 根据权利要求 2 所述的方法，所述申请编号与所述备选对象对应的唯一标识的取值相关，所述唯一标识的取值由与区块链中的历史区块相关的哈希值和所述备选用户的公钥进行哈希计算而得到。

4. 根据权利要求 2 所述的方法，当所述备选对象的中签率为标准中签率的 x 倍时，
15 所述备选对象存在 x 个申请编号；其中， x 为正整数。

5. 根据权利要求 4 所述的方法，

所述智能合约用于将与区块链中的历史区块相关的哈希值与所述备选对象的公钥进行哈希计算，得到相应的唯一标识；

20 当 x 的取值从小至大地分别包括 $x_1 \sim x_n$ 时，所述智能合约用于依次选取 $x_1 \sim x_n$ ；其中，当选取 x_i 时，所述智能合约将中签率不小于标准中签率的 x_i 倍的备选对象对应的唯一标识按照从小至大依次排列，并在已有申请编号之后、按照排列次序接续生成相应的申请编号， $1 \leq i \leq n$ 。

6. 根据权利要求 2 所述的方法，所述目标对象的总数为 w ；所述智能合约用于在已选取的目标对象的数量未达到 w 时，将所述随机种子和采样区间 $[M, N]$ 作为输入、通
25 过所述伪随机数发生器生成 1 个伪随机数，其中 M 为申请编号的最小值、 N 为申请编号的最大值。

7. 根据权利要求 2 所述的方法，所述智能合约用于将每一备选对象对应的申请编号存证于区块链中。

8. 根据权利要求 1 所述的方法，所述随机种子还与区块链中的一个或多个其他区
30 块的区块内容相关。

9. 根据权利要求 8 所述的方法，所述一个或多个其他区块包括：包含至少一条申

请记录的区块。

10. 根据权利要求 8 所述的方法, 所述一个或多个其他区块包括: 与所述第二区块相邻的一个或多个区块。

11. 根据权利要求 8 所述的方法, 所述智能合约用于通过下述公式对所述第二区块和 r 个其他区块的区块内容进行处理, 以确定出所述实际结果:

$$H'1=H(H_p, H_r),$$

$$H'i=H(H'(i-1), H(r-i+1)), \text{ 其中 } 1 < i \leq r;$$

其中, H 为预设的哈希函数, H_p 为与所述第二区块的区块内容相关的哈希值, H_i 为与第 i 个其他区块的区块内容相关的哈希值, 所述随机种子为 $H_f=H(H'r, H_p)$ 。

12. 根据权利要求 1 所述的方法, 所述智能合约用于在区块链中产生第三区块后, 生成所述随机种子; 其中, 所述第三区块的区块高度大于所述第二区块, 且高度差为预设数值。

13. 一种对象选取装置, 应用于区块链节点; 所述装置包括:

获取单元, 获取备选对象提交的参选申请;

调用单元, 调用智能合约, 所述智能合约被用于向区块链的第一区块发布与所述参选申请相关的申请记录, 根据区块链中的第二区块的区块内容生成随机种子, 并通过伪随机数发生器生成基于所述随机种子的伪随机数, 以使得匹配于所述伪随机数的备选对象被选取为目标对象; 其中, 所述第二区块的区块高度大于所述第一区块的区块高度。

14. 根据权利要求 13 所述的装置, 所述智能合约还用于: 为每一备选对象分别生成申请编号, 每一申请编号对应于唯一的备选对象; 其中, 当所述伪随机数与任一申请编号相同时, 所述任一申请编号对应的备选对象被确定为匹配于所述伪随机数。

15. 根据权利要求 14 所述的装置, 所述申请编号与所述备选对象对应的唯一标识的取值相关, 所述唯一标识的取值由与区块链中的历史区块相关的哈希值和所述备选用户的公钥进行哈希计算而得到。

16. 根据权利要求 14 所述的装置, 当所述备选对象的中签率为标准中签率的 x 倍时, 所述备选对象存在 x 个申请编号; 其中, x 为正整数。

17. 根据权利要求 16 所述的装置,

所述智能合约用于将与区块链中的历史区块相关的哈希值与所述备选对象的公钥进行哈希计算, 得到相应的唯一标识;

当 x 的取值从小至大地分别包括 $x_1 \sim x_n$ 时, 所述智能合约用于依次选取 $x_1 \sim x_n$; 其中, 当选取 x_i 时, 所述智能合约将中签率不小于标准中签率的 x_i 倍的备选对象对应的

唯一标识按照从小至大依次排列，并在已有申请编号之后、按照排列次序接续生成相应的申请编号， $1 \leq i \leq n$ 。

18. 根据权利要求 14 所述的装置，所述目标对象的总数为 w ；所述智能合约用于在已选取的目标对象的数量未达到 w 时，将所述随机种子和采样区间 $[M, N]$ 作为输入、

5 通过所述伪随机数发生器生成 1 个伪随机数，其中 M 为申请编号的最小值、 N 为申请编号的最大值。

19. 根据权利要求 14 所述的装置，所述智能合约用于将每一备选对象对应的申请编号存证于区块链中。

10 20. 根据权利要求 13 所述的装置，所述随机种子还与区块链中的一个或多个其他区块的区块内容相关。

21. 根据权利要求 20 所述的装置，所述一个或多个其他区块包括：包含至少一条申请记录的区块。

22. 根据权利要求 20 所述的装置，所述一个或多个其他区块包括：与所述第二区块相邻的一个或多个区块。

15 23. 根据权利要求 20 所述的装置，所述智能合约用于通过下述公式对所述第二区块和 r 个其他区块的区块内容进行处理，以确定出所述实际结果：

$$H'1 = H(H_p, H_r),$$

$$H'i = H(H'(i-1), H(r-i+1)), \text{ 其中 } 1 < i \leq r;$$

20 其中， H 为预设的哈希函数， H_p 为与所述第二区块的区块内容相关的哈希值， H_i 为与第 i 个其他区块的区块内容相关的哈希值，所述随机种子为 $H_f = H(H'r, H_p)$ 。

24. 根据权利要求 13 所述的装置，所述智能合约用于在区块链中产生第三区块后，生成所述随机种子；其中，所述第三区块的区块高度大于所述第二区块，且高度差为预设数值。

25. 一种电子设备，包括：

25 处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器通过运行所述可执行指令以实现如权利要求 1-12 中任一项所述的方法。

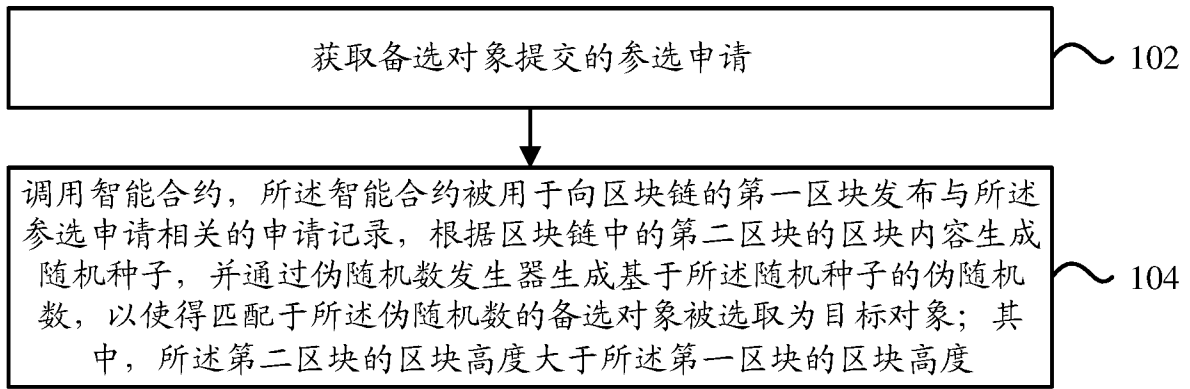


图 1

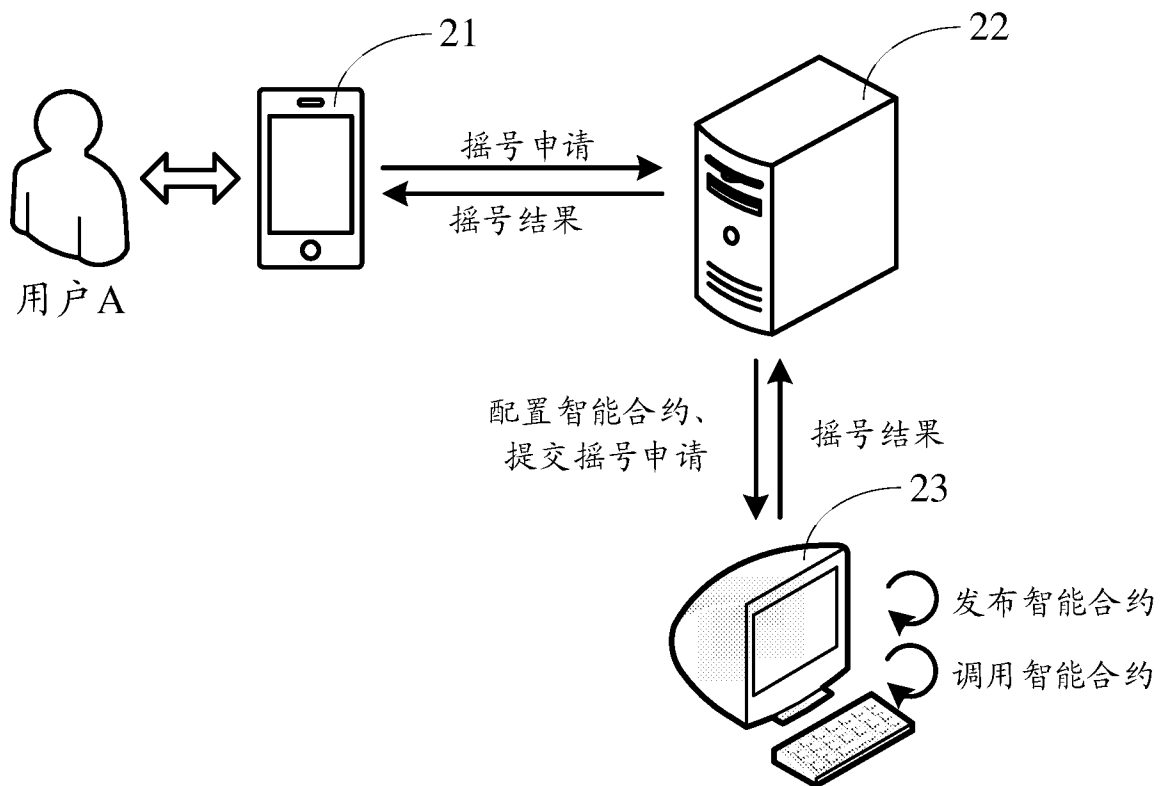


图 2

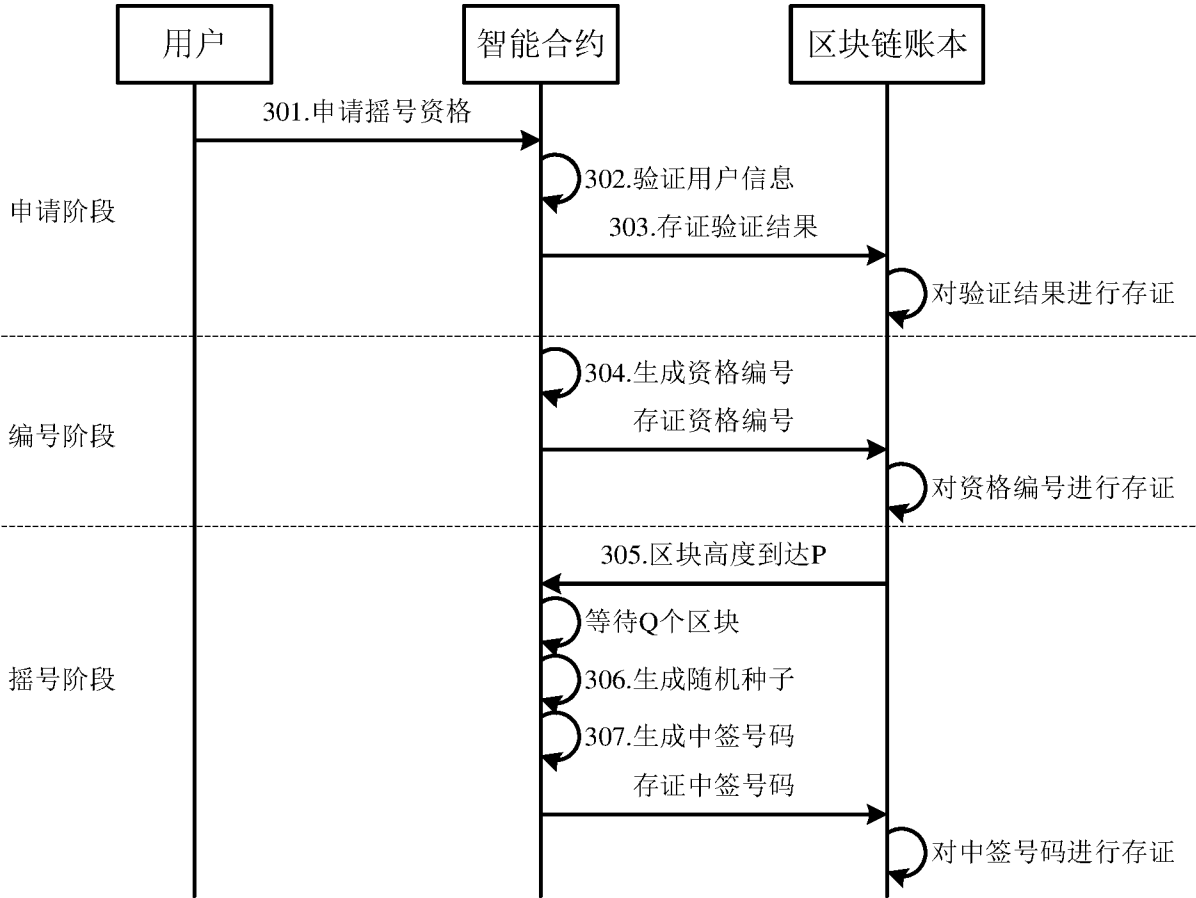


图 3

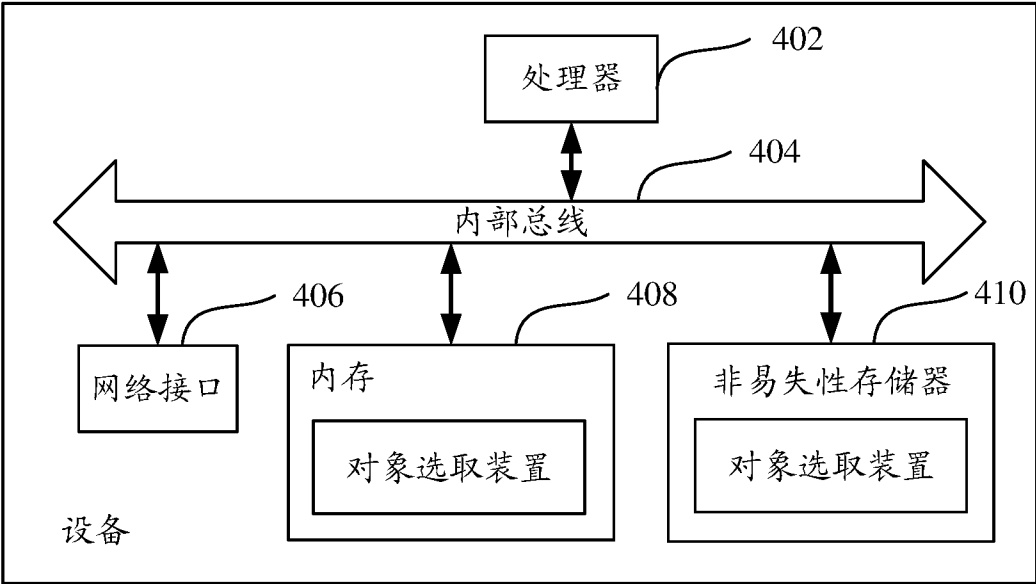


图 4

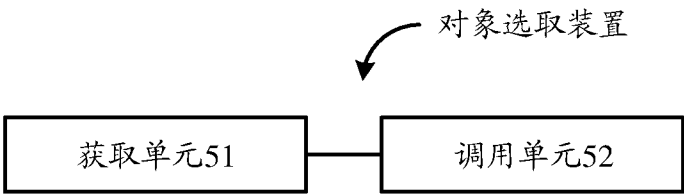


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/102777

A. CLASSIFICATION OF SUBJECT MATTER

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)

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)

WPI; CNPAT; CNKI; EPDOC: 阿里, 区块链, 区块, 伪随机数, 哈希, 种子, 随机, 摇号, 参选, 备选, 编号, 合约, ALi, block chain, blockchain, node?, standby, pseudo?, number, select+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 108648323 A (GUANGZHOU SENDI COMPUTER SYSTEM CO., LTD.) 12 October 2018 (2018-10-12) description, pages 3-9, and figures 1-7	1-25
PX	CN 109615370 A (ALIBABA GROUP HOLDING LIMITED) 12 April 2019 (2019-04-12) description, pages 2-8, and figures 1-5	1-25
PX	CN 109584432 A (ALIBABA GROUP HOLDING LIMITED) 05 April 2019 (2019-04-05) description, pages 2-9, and figures 1-5	1-25
PX	CN 109242677 A (ALIBABA GROUP HOLDING LIMITED) 18 January 2019 (2019-01-18) description, pages 1-6, and figures 1-5	1-25
A	CN 108269090 A (INSTITUTE OF SOFTWARE, CHINESE ACADEMY OF SCIENCE) 10 July 2018 (2018-07-10) entire document	1-25
A	CN 108665272 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 16 October 2018 (2018-10-16) entire document	1-25



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

“D” document cited by the applicant in the international application

“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

05 November 2019

Date of mailing of the international search report

28 November 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration
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/CN2019/102777

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2009169489 A (OKI ELECTRIC IND. CO., LTD.) 30 July 2009 (2009-07-30) entire document	1-25

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/102777

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	108648323	A	12 October 2018	None	
CN	109615370	A	12 April 2019	None	
CN	109584432	A	05 April 2019	None	
CN	109242677	A	18 January 2019	None	
CN	108269090	A	10 July 2018	None	
CN	108665272	A	16 October 2018	None	
JP	2009169489	A	30 July 2009	None	

国际检索报告

国际申请号

PCT/CN2019/102777

A. 主题的分类 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) 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)) WPI; CNPAT; CNKI; EPDOC: 阿里, 区块链, 区块, 伪随机数, 哈希, 种子, 随机, 摇号, 参选, 备选, 编号, 合约, ALi, block chain, blockchain, node?, standby, pseudo?, number, select+																										
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>X</td> <td>CN 108648323 A (广州市申迪计算机系统有限公司) 2018年 10月 12日 (2018 - 10 - 12) 说明书第3-9页及附图1-7</td> <td>1-25</td> </tr> <tr> <td>PX</td> <td>CN 109615370 A (阿里巴巴集团控股有限公司) 2019年 4月 12日 (2019 - 04 - 12) 说明书第2-8页及附图1-5</td> <td>1-25</td> </tr> <tr> <td>PX</td> <td>CN 109584432 A (阿里巴巴集团控股有限公司) 2019年 4月 5日 (2019 - 04 - 05) 说明书第2-9页及附图1-5</td> <td>1-25</td> </tr> <tr> <td>PX</td> <td>CN 109242677 A (阿里巴巴集团控股有限公司) 2019年 1月 18日 (2019 - 01 - 18) 说明书第1-6页及附图1-5</td> <td>1-25</td> </tr> <tr> <td>A</td> <td>CN 108269090 A (中国科学院软件研究所) 2018年 7月 10日 (2018 - 07 - 10) 全文</td> <td>1-25</td> </tr> <tr> <td>A</td> <td>CN 108665272 A (百度在线网络技术北京有限公司) 2018年 10月 16日 (2018 - 10 - 16) 全文</td> <td>1-25</td> </tr> <tr> <td>A</td> <td>JP 2009169489 A (OKI ELECTRIC IND. CO. LTD.) 2009年 7月 30日 (2009 - 07 - 30) 全文</td> <td>1-25</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	X	CN 108648323 A (广州市申迪计算机系统有限公司) 2018年 10月 12日 (2018 - 10 - 12) 说明书第3-9页及附图1-7	1-25	PX	CN 109615370 A (阿里巴巴集团控股有限公司) 2019年 4月 12日 (2019 - 04 - 12) 说明书第2-8页及附图1-5	1-25	PX	CN 109584432 A (阿里巴巴集团控股有限公司) 2019年 4月 5日 (2019 - 04 - 05) 说明书第2-9页及附图1-5	1-25	PX	CN 109242677 A (阿里巴巴集团控股有限公司) 2019年 1月 18日 (2019 - 01 - 18) 说明书第1-6页及附图1-5	1-25	A	CN 108269090 A (中国科学院软件研究所) 2018年 7月 10日 (2018 - 07 - 10) 全文	1-25	A	CN 108665272 A (百度在线网络技术北京有限公司) 2018年 10月 16日 (2018 - 10 - 16) 全文	1-25	A	JP 2009169489 A (OKI ELECTRIC IND. CO. LTD.) 2009年 7月 30日 (2009 - 07 - 30) 全文	1-25
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																								
X	CN 108648323 A (广州市申迪计算机系统有限公司) 2018年 10月 12日 (2018 - 10 - 12) 说明书第3-9页及附图1-7	1-25																								
PX	CN 109615370 A (阿里巴巴集团控股有限公司) 2019年 4月 12日 (2019 - 04 - 12) 说明书第2-8页及附图1-5	1-25																								
PX	CN 109584432 A (阿里巴巴集团控股有限公司) 2019年 4月 5日 (2019 - 04 - 05) 说明书第2-9页及附图1-5	1-25																								
PX	CN 109242677 A (阿里巴巴集团控股有限公司) 2019年 1月 18日 (2019 - 01 - 18) 说明书第1-6页及附图1-5	1-25																								
A	CN 108269090 A (中国科学院软件研究所) 2018年 7月 10日 (2018 - 07 - 10) 全文	1-25																								
A	CN 108665272 A (百度在线网络技术北京有限公司) 2018年 10月 16日 (2018 - 10 - 16) 全文	1-25																								
A	JP 2009169489 A (OKI ELECTRIC IND. CO. LTD.) 2009年 7月 30日 (2009 - 07 - 30) 全文	1-25																								
☐ 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 2019年 11月 5日		国际检索报告邮寄日期 2019年 11月 28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 王海峰 电话号码 86- (10) -53962363																								

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/102777

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	108648323	A	2018年 10月 12日	无	
CN	109615370	A	2019年 4月 12日	无	
CN	109584432	A	2019年 4月 5日	无	
CN	109242677	A	2019年 1月 18日	无	
CN	108269090	A	2018年 7月 10日	无	
CN	108665272	A	2018年 10月 16日	无	
JP	2009169489	A	2009年 7月 30日	无	