

(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



(10) 国际公布号

WO 2020/082873 A1

(43) 国际公布日
2020 年 4 月 30 日 (30.04.2020)

(51) 国际专利分类号:
G06Q 20/38 (2012.01)

(21) 国际申请号: PCT/CN2019/101681

(22) 国际申请日: 2019 年 8 月 21 日 (21.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811249392.X 2018 年 10 月 25 日 (25.10.2018) 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: 谢桂鲁 (XIE, Guilu); 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, 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))。

(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

调用用于选取对象的智能合约, 所述智能合约用于根据备选对象提供的种子数据生成随机种子, 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

102

图 1

102 Invoke an intelligent contract used to select an object, the intelligent contract being used to generate a random seed according to seed data provided by a candidate object, 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

(57) Abstract: Provided in one or more embodiments of the present description are an object selection method and device and an electronic device, which are applied to a blockchain node. The method comprises: invoking an intelligent contract used to select an object, the intelligent contract being used to generate a random seed according to seed data provided by a candidate object, 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.

(57) 摘要: 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, 应用于区块链节点; 所述方法包括: 调用用于选取对象的智能合约, 所述智能合约用于根据备选对象提供的种子数据生成随机种子, 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。



WO 2020/082873 A1

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
10 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
15 块链节点；所述方法包括：

[06] 调用用于选取对象的智能合约，所述智能合约用于根据备选对象提供的种子数据生成随机种子，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。

[07] 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
20 块链节点；所述装置包括：

[08] 调用单元，调用用于选取对象的智能合约，所述智能合约用于根据备选对象提供的种子数据生成随机种子，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。

[09] 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：

25 [10] 处理器；

[11]用于存储处理器可执行指令的存储器;

[12]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

[13]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。

5 [14]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。

[15]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。

[16]图 4 是一示例性实施例提供的一种设备的结构示意图。

[17]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

10 [18]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述实施方式并不代表与本发明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、本发明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。

15 [19]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。

20 [20]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:

[21]步骤 102,调用用于选取对象的智能合约,所述智能合约用于根据备选对象提供的种子数据生成随机种子,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。

25 [22]在一实施例中,由于随机种子是基于备选对象提供的种子数据而产生,使得该随机种子具备真正的高度随机性,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，从而防止不法分子造假作弊。同时，由于随机种子的生成过程、伪随机数的生成过程均有智能合约实现，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。

5 [23]在一实施例中，所述智能合约用于在每次收到备选对象提供的种子数据后，按照预设算法对所述随机种子实施与所述种子数据相关的更新处理。随机种子的初始取值可以为预设初始值；或者，当收到备选对象提供的第一个种子数据后，可以将该第一个种子数据作为随机种子的初始取值。当随机种子为 Z1 时，若收到备选对象提供的种子数据 1，可以基于预设算法对随机种子 Z1 和该种子数据 1 进行计算，使得随机种子被更新为
10 Z2；进一步地，若收到备选对象提供的种子数据 2，可以基于预设算法对随机种子 Z2 和该种子数据 2 进行计算，使得随机种子被更新为 Z3，直至备选对象提供的所有种子数据都参与了对随机种子的更新处理。

[24]在一实施例中，所述智能合约用于在收到备选对象提供的所有种子数据后，对所有种子数据进行拼接，并按照预设算法对所述随机种子的初始取值实施与拼接后数据相关的
15 的更新处理；其中，所述随机种子的初始取值为预设初始值。例如，智能合约中可以描述用于接收种子数据的时间段，使得备选对象在该时间段内提供的种子数据，可以用于对随机种子进行更新，则智能合约在该时间段的终止时刻之前，不会对备选对象提供的种子数据进行处理，而是在该终止时刻到达之后，将该时间段内收到的所有种子数据进行拼接后，将拼接后种子数据应用于对随机种子进行更新，比如按照预设算法对该拼接
20 后种子数据与随机种子的初始取值进行计算，从而得到更新后的随机种子。

[25]在一实施例中，随机种子的预设初始值可以包括下述任一：实施赋值操作时（即需要向随机种子赋予该预设初始值的时刻）的时间戳、区块链中的历史区块（例如区块链中最近生成的一个区块）的哈希值、区块链中的历史区块中的指定交易（例如按照交易时刻排列的第 a 笔交易，a 为预设数值）的哈希值。

25 [26]在一实施例中，上述的预设算法可以包括消息摘要算法，可以计算随机种子与种子数据的哈希值，以作为更新后的随机种子。当然，该预设算法还可以包括其他类型的算法，本说明书并不对此进行限制。

[27]在一实施例中，所述随机种子的取值还与所述种子数据的接收时间戳相关，使得随机种子的取值同时受到种子数据和接收时间戳的影响，可以进一步增加随机种子被更新
30 后的随机性，从而提升对目标对象进行选取时的公平性，避免不法分子造假作弊。

[28]在一实施例中，可以向所述备选对象提供所述智能合约支持的多个备选的伪随机数发生器，以由所述备选用户进行选择，可以进一步体现出公平、公开，并且增加了随机性。例如，可以预先在智能合约中定义多种伪随机数发生器，而备选对象在提供种子数据的同时，还可以提交对伪随机数发生器的选择信息，使得智能合约可以通过统计各个备选对象的选择信息，确定各个伪随机数发生器对应的被选择次数，从而将被选择次数排列于预设名次（如被选择次数排列于第一、被选择次数排列于第三或其他任意名次）的伪随机数发生器应用于生成伪随机数。

[29]在一实施例中，所述智能合约还用于：将所述种子数据和/或所述随机种子存证于区块链中，使得备选用户或监管方可以随时从区块链中对种子数据、随机种子等进行查证，以确保随机种子的更新过程不会发生造假作弊，或者及时发现可能的造假作弊情况。

[30]在一实施例中，所述智能合约还用于：将所述伪随机数存证于区块链中，使得备选用户或监管方可以随时从区块链中对伪随机数、伪随机数发生器与随机种子之间的关系进行验证，以确保伪随机数的生成过程不会发生造假作弊，或者及时发现可能的造假作弊情况。

[31]在一实施例中，所述智能合约还用于：对任一对象的资格注册信息进行验证，并在验证通过后将所述任一对象的资格信息存证于区块链中，以使所述任一对象成为所述备选对象；其中，所述资格注册信息包括所述任一对象的公钥，且所述资格注册信息由所述任一对象的私钥进行签名。通过验证资格注册信息，可以确保备选对象都满足预设要求。由于资格注册信息由私钥进行签名，使得每一对象的身份信息都明确、可追溯，避免暗箱操作。

[32]在一实施例中，所述种子数据由所述备选对象通过私钥进行签名；所述智能合约还用于：对收到的种子数据进行签名验证，以确保备选对象提供的种子数据不会被不法分子篡改。

[33]在一实施例中，备选对象的数量为多个，智能合约可以从这些备选对象中选取部分对象，以作为预设数量的目标对象，该预设数量可以为一个或多个。

[34]在一实施例中，备选对象可以包括任意类型的对象，这取决于所应用的场景，本说明书并不对此进行限制。例如，在向出租车派发叫车任务时，备选对象可以为出租车牌照号，用于为每一叫车任务随机指派一辆出租车；再例如，在配置多台电子设备构成的设备系统时，备选对象可以为设备 ID，用于选取指定数量的电子设备以作为主设备。

[35]在一实施例中，每一备选对象可以存在对应的唯一编号，比如该唯一编号可以为备选对象的排序号码等，本说明书并不对此进行限制。通过将基于随机种子生成的伪随机数与各个备选对象对应的唯一编号进行比较，可以确定与伪随机数相同的唯一编号，从而将该唯一编号对应的备选对象选取为目标对象。当然，还可以通过其他方式在伪随机数与备选对象之间进行匹配，从而确定出被选取的目标对象。

[36]在一实施例中，所述智能合约还向链外系统发送通知消息，所述通知消息包含所述目标对象的信息，以指示所述链外系统向所述目标对象赋予预设权限，使得该目标对象可以实施相关操作，而其他未被选取为目标对象的备选对象则不具有该预设权限、无法实施相关操作。

[37]例如，对于需要控制车辆数量的地区，所述链外系统可以包括车辆牌照管理系统，而所述预设权限包括对车辆牌照的选取权限，备选对象为希望选取车辆牌照的用户；那么，目标对象可以选取车辆牌照，而未被选取为目标对象的备选对象则无法选取车辆牌照，从而实现对车辆数量的控制。又例如，对于需要摇号买房的地区，所述链外系统包括不动产管理系统，所述预设权限包括对不动产的选购权限，备选对象为希望选购某一楼盘的不动产的用户；那么，当备选对象的数量超出该楼盘的不动产总数时，可以基于该不动产总数选取目标对象，使得该目标对象可以选购该楼盘的不动产，而未被选取为目标对象的备选对象则无法选购该楼盘的不动产。

[38]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，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 输入注册摇号资格所需的资格注册信息，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）。类似地，如果用户 B 希望参与摇号，可以通过安装有客户端的手机 22 输入注册摇号资格所需的资格注册，其他用户的情况此处不再一一赘述。

[39]设备 23 被配置为摇号系统的服务端，该设备 23 一方面与用户 A-B 等使用的手机 21-22 等进行交互、以协助其注册摇号资格，另一方面与设备 24 进行交互。设备 24 被配置为区块链中的一个区块链节点，基于设备 23 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注册和摇号操作等。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注册条件、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。

[40]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:

5 [41]步骤301,用户注册摇号资格。

[42]在一实施例中,以上述的用户A为例,该用户A可以通过手机21向设备23提交资格注册信息,并经由设备24向区块链中提交包含该资格注册信息的交易,该交易的类型可以被配置或标记为注册摇号资格的类型。类似地,其他用户也可以通过上述方式注册摇号资格。

10 [43]除了通过设备24向区块链提交包含资格注册信息的交易之外,用户A也可以通过其他区块链节点向区块链提交包含资格注册信息的交易,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向区块链提交包含资格注册信息的交易。

[44]上述包含资格注册信息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资格注册信息,从而验证相应的用户
15 是否可以获得摇号资格。

[45]在一实施例中,以设备24为例,设备24可以获知智能合约的名称或位置等信息,使得设备24可以直接将资格注册信息发送至智能合约,而智能合约可以针对收到的资格注册信息进行验证,以确定相应的用户是否可以获得摇号资格。

[46]步骤302,智能合约验证用户信息。

20 [47]在一实施例中,智能合约获得某一用户的资格注册信息后,可以按照预先定义的注册条件对该资格注册信息进行验证,以确定其是否满足该注册条件;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。

[48]在一实施例中,资格注册信息中包含对应用户的公钥和其他个人信息,且资格注册信息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。

25 [49]步骤303,智能合约将验证结果提交至区块链,以存证于区块链账本中。

[50]在一实施例中,通过将验证结果存证于区块链账本中,使得验证结果透明、可追溯,并且无法随意篡改验证结果,确保对于资格注册信息的验证符合要求,避免暗箱操作。

[51]步骤304,智能合约为通过验证的用户生成资格编号,并将资格编号的分配信息提

交至区块链，以存证于区块链账本中。

[52]在一实施例中，智能合约可以通过预设方式生成资格编号，比如按照公钥的取值大小、资格注册信息的接收时刻的早晚等进行排序，并将顺序号作为相应的资格编号。当然，还可以通过其他方式生成资格编号，本说明书并不对此进行限制。

5 [53]在一实施例中，如果按照公钥的取值大小生成资格编号，智能合约需要等待收到所有用户提交的资格注册信息之后，才能够获得各个用户的公钥，从而为所有通过验证的用户生成资格编号。

[54]在一实施例中，如果按照资格注册信息的接收时刻生成资格编号，智能合约可以在每收到一条资格注册信息后，就为相应的用户生成资格编号。

10 [55]在一实施例中，假定以时间段来划分各个阶段，智能合约可以定义有用户注册阶段的起始时刻、终止时刻，那么智能合约只针对该起始时刻与终止时刻之间收到的资格注册信息进行资格验证、生成资格编号，而在用户注册阶段之外收到的资格注册信息则判定为无效。

[56]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，
15 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。

[57]步骤 305，用户提交种子数据。

[58]与步骤 301 相类似的，用户 A 可以将种子数据通过手机 21 发送至设备 23，并经由
20 设备 24 将种子数据发布至区块链，从而由智能合约从区块链账本中获取该种子数据；或者，当手机 21 被配置为区块链节点时，可由该手机 21 将用户 A 设定的种子数据发布至区块链，并由智能合约从区块链账本中获取该种子数据；或者，设备 24 可以直接将种子数据发送至智能合约。此处不再一一赘述。

[59]在一实施例中，种子数据可以为用户所提供的任意内容。实际上，正是由于种子数
25 据的内容随意、不可控，使得在基于种子数据对随机种子进行更新时，增加了随机种子的内容随机性，使得随机种子的更新结果不易受到操控，避免不法分子借此操纵摇号过程。

[60]步骤 306，智能合约获取种子数据后，实施签名验证。

[61]在一实施例中, 智能合约可以读取收到的种子数据的签名信息; 如果种子数据未签名, 则智能合约无法确定该种子数据的来源, 可以判定为签名验证未通过; 如果种子数据的签名并不属于步骤 302 中通过验证的用户, 则智能合约可以判定为种子数据的来源不合法, 可以判定为签名验证未通过; 如果种子数据的签名属于步骤 302 中通过验证的用户, 则智能合约可以进一步判定该种子数据是否为本次摇号过程中首次收到, 若非首次收到可以判定为未通过验证, 若首次收到则可以判定为通过签名验证。

[62]因此, 用户通过自身持有的私钥对种子数据进行签名, 便于确认该种子数据的来源, 还可以避免对种子数据的重复使用; 同时, 通过对种子数据进行签名, 可以避免不法分子对种子数据进行篡改, 防止随机种子的更新结果被操控。

[63]步骤 307, 智能合约基于种子数据更新随机种子, 并将种子数据提交至区块链, 以存证于区块链账本中。

[64]在一实施例中, 可以基于预设的哈希算法对种子数据和随机种子进行计算, 并用计算得到的数值对随机种子进行更新, 得到更新后的随机种子。比如该哈希算法可以包括 SHA256 等, 本说明书并不对此进行限制。通过将种子数据应用于对随机种子进行更新, 并且该种子数据由参与摇号的用户提供、具有极大的随机性, 因而可使随机种子产生随机、不可预先猜测出的变化, 可以避免不法分子对随机种子的取值进行操控。

[65]在一实施例中, 在针对随机种子进行赋值时, 可以选取当前时刻的时间戳, 并将该时间戳的哈希值设置为随机种子的初始值。当然, 还可以通过其他方式设置随机种子的初始值, 本说明书并不对此进行限制。

[66]在一实施例中, 步骤 305~307 对应于种子生成阶段, 智能合约中可以定义有该种子生成阶段的起始时刻、终止时刻, 以用于划分和限定该种子生成阶段。在该起始时刻与终止时刻之间的时间段内, 具有摇号资格的每个用户都可以提供种子数据, 比如由用户 1~用户 n 分别提供相应的种子数据 1~种子数据 n, 那么智能合约的处理方式可以为:

[67]一种情况下, 智能合约每当收到一个种子数据时, 就对随机种子进行更新, 直至所有种子数据都被应用于对随机种子实施更新。比如, 随机种子在初始时为 Z1; 当收到种子数据 1 后, 可以将 Z1 与种子数据 1 进行哈希计算, 并将得到的哈希值更新为随机种子 Z2; 进一步的, 当收到种子数据 2 后, 可以将 Z2 与种子数据 2 进行哈希计算, 并将得到的哈希值更新为随机种子 Z3; 当收到种子数据 n 后, 可以将 Zn 与种子数据 n 进行哈希计算, 并将得到的哈希值更新为随机种子 Zn+1, 该随机种子 Zn+1 被作为最

终取值。

[68] 另一种情况下，智能合约可以获取在种子生成阶段内收到的所有种子数据，比如种子数据 1~种子数据 n，并对这些种子数据进行拼接后，得到拼接后种子数据；然后，智能合约可以将该拼接后种子数据与随机种子的初始值进行哈希计算，得到更新后的随机种子。

[69] 在一实施例中，智能合约可以将收到的种子数据存证于区块链账本中，该种子数据包含对应用户的签名，可以验证该种子数据的来源，并且防止对该种子数据进行篡改。进一步的，智能合约还可以将各个种子数据与对应的更新前随机种子、更新后随机种子相关联地存证于区块链账本中，以便于用户或监管方进行核对查验，防止不法分子进行篡改。

[70] 步骤 308，智能合约根据随机种子生成中签号码，并将中签号码发布至区块链，以存证于区块链账本中。

[71] 在一实施例中，智能合约中定义有伪随机数发生器，通过向该伪随机数发生器输入随机种子和取值范围，即可生成相应的伪随机数。其中，输入的随机种子可以为经由种子数据更新后得到的最终取值，该随机种子的最终取值受到了种子数据的影响，使得不法分子无法预测或操控，使得伪随机数具有真正的随机特性；同时，输入的取值范围可以为上述步骤中生成的资格编号的取值范围，因而生成的伪随机数为中签号码，可以命中某一资格编号，使得该资格编号对应的用户获得不动产的选购权限。

[72] 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 23 发起查询请求，设备 23 可以通过设备 24 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。

[73] 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，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。

[74]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:

5 [75]调用单元 51,调用用于选取对象的智能合约,所述智能合约用于根据备选对象提供的种子数据生成随机种子,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。

[76]可选的,所述智能合约用于在每次收到备选对象提供的种子数据后,按照预设算法对所述随机种子实施与所述种子数据相关的更新处理;其中,所述随机种子的初始取值
10 为预设初始值或首个由备选对象提供的种子数据。

[77]可选的,所述智能合约用于在收到备选对象提供的所有种子数据后,对所有种子数据进行拼接,并按照预设算法对所述随机种子的初始取值实施与拼接后数据相关的更新处理;其中,所述随机种子的初始取值为预设初始值。

[78]可选的,所述预设初始值包括下述任一:实施赋值操作时的时间戳、区块链中的历史区块的哈希值、区块链中的历史区块中的指定交易的哈希值。
15

[79]可选的,所述随机种子的取值还与所述种子数据的接收时间戳相关。

[80]可选的,还包括:

[81]提供单元 52,向所述备选对象提供所述智能合约支持的多个备选的伪随机数发生器,以由所述备选用户进行选择。

20 [82]可选的,所述智能合约还用于:将所述种子数据和/或所述随机种子存证于区块链中。

[83]可选的,所述智能合约还用于:将所述伪随机数存证于区块链中。

[84]可选的,所述智能合约还用于:对任一对象的资格注册信息进行验证,并在验证通过后将所述任一对象的资格信息存证于区块链中,以使所述任一对象成为所述备选对象;其中,所述资格注册信息包括所述任一对象的公钥,且所述资格注册信息由所述任一对象的私钥进行签名。
25

[85]可选的,所述种子数据由所述备选对象通过私钥进行签名;所述智能合约还用于:对收到的种子数据进行签名验证。

[86]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、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。

- 5 [87] 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。

[88] 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) 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。

- 10 [89] 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、
15 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。

- [90] 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。
- 20

- [91] 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。
- 25 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。

[92] 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。

- 5 [93]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”。
- 10 [94]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：

调用用于选取对象的智能合约，所述智能合约用于根据备选对象提供的种子数据生成随机种子，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
5 所述伪随机数的备选对象被选取为目标对象。

2. 根据权利要求 1 所述的方法，所述智能合约用于在每次收到备选对象提供的种子数据后，按照预设算法对所述随机种子实施与所述种子数据相关的更新处理；其中，所述随机种子的初始取值为预设初始值或首个由备选对象提供的种子数据。

3. 根据权利要求 1 所述的方法，所述智能合约用于在收到备选对象提供的所有种
10 子数据后，对所有种子数据进行拼接，并按照预设算法对所述随机种子的初始取值实施与拼接后数据相关的更新处理；其中，所述随机种子的初始取值为预设初始值。

4. 根据权利要求 2 或 3 所述的方法，所述预设初始值包括下述任一：实施赋值操作时的时间戳、区块链中的历史区块的哈希值、区块链中的历史区块中的指定交易的哈希值。

5. 根据权利要求 1 所述的方法，所述随机种子的取值还与所述种子数据的接收时间戳相关。

6. 根据权利要求 1 所述的方法，还包括：

向所述备选对象提供所述智能合约支持的多个备选的伪随机数发生器，以由所述备选用户进行选择。

7. 根据权利要求 1 所述的方法，所述智能合约还用于：将所述种子数据和/或所述随机种子存证于区块链中。

8. 根据权利要求 1 所述的方法，所述智能合约还用于：将所述伪随机数存证于区块链中。

9. 根据权利要求 1 所述的方法，所述智能合约还用于：对任一对象的资格注册信息
25 信息进行验证，并在验证通过后将所述任一对象的资格信息存证于区块链中，以使所述任一对象成为所述备选对象；其中，所述资格注册信息包括所述任一对象的公钥，且所述资格注册信息由所述任一对象的私钥进行签名。

10. 根据权利要求 9 所述的方法，所述种子数据由所述备选对象通过私钥进行签名；所述智能合约还用于：对收到的种子数据进行签名验证。

11. 一种对象选取装置，应用于区块链节点；所述装置包括：

调用单元，调用用于选取对象的智能合约，所述智能合约用于根据备选对象提供的

种子数据生成随机种子，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。

12. 根据权利要求 11 所述的装置，所述智能合约用于在每次收到备选对象提供的种子数据后，按照预设算法对所述随机种子实施与所述种子数据相关的更新处理；其中，
5 所述随机种子的初始取值为预设初始值或首个由备选对象提供的种子数据。

13. 根据权利要求 11 所述的装置，所述智能合约用于在收到备选对象提供的所有种子数据后，对所有种子数据进行拼接，并按照预设算法对所述随机种子的初始取值实施与拼接后数据相关的更新处理；其中，所述随机种子的初始取值为预设初始值。

14. 根据权利要求 12 或 13 所述的装置，所述预设初始值包括下述任一：实施赋值
10 操作时的时间戳、区块链中的历史区块的哈希值、区块链中的历史区块中的指定交易的哈希值。

15. 根据权利要求 11 所述的装置，所述随机种子的取值还与所述种子数据的接收时间戳相关。

16. 根据权利要求 11 所述的装置，还包括：
15 提供单元，向所述备选对象提供所述智能合约支持的多个备选的伪随机数发生器，以由所述备选用户进行选择。

17. 根据权利要求 11 所述的装置，所述智能合约还用于：将所述种子数据和/或所述随机种子存证于区块链中。

18. 根据权利要求 11 所述的装置，所述智能合约还用于：将所述伪随机数存证于
20 区块链中。

19. 根据权利要求 11 所述的装置，所述智能合约还用于：对任一对象的资格注册信息进行验证，并在验证通过后将所述任一对象的资格信息存证于区块链中，以使所述任一对象成为所述备选对象；其中，所述资格注册信息包括所述任一对象的公钥，且所述资格注册信息由所述任一对象的私钥进行签名。

20. 根据权利要求 19 所述的装置，所述种子数据由所述备选对象通过私钥进行签名；所述智能合约还用于：对收到的种子数据进行签名验证。

21. 一种电子设备，包括：

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 1-10 中任一项所述的方法。

调用用于选取对象的智能合约，所述智能合约用于根据备选对象提供的种子数据生成随机种子，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 102

图 1

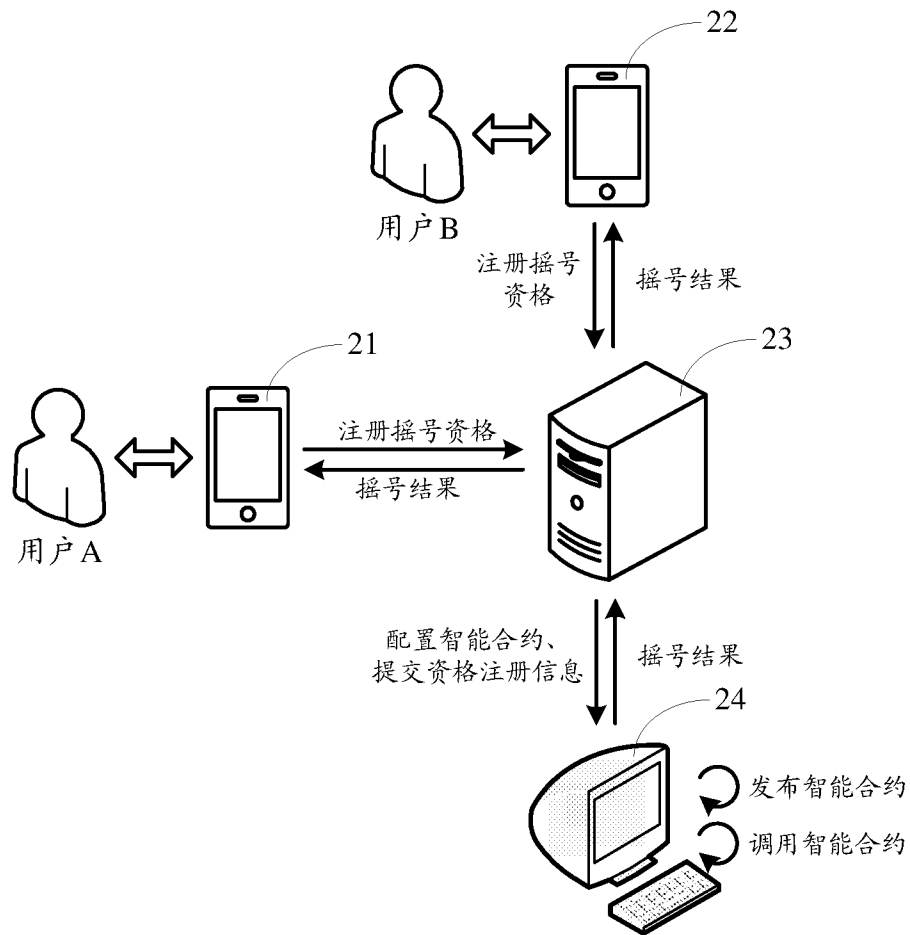


图 2

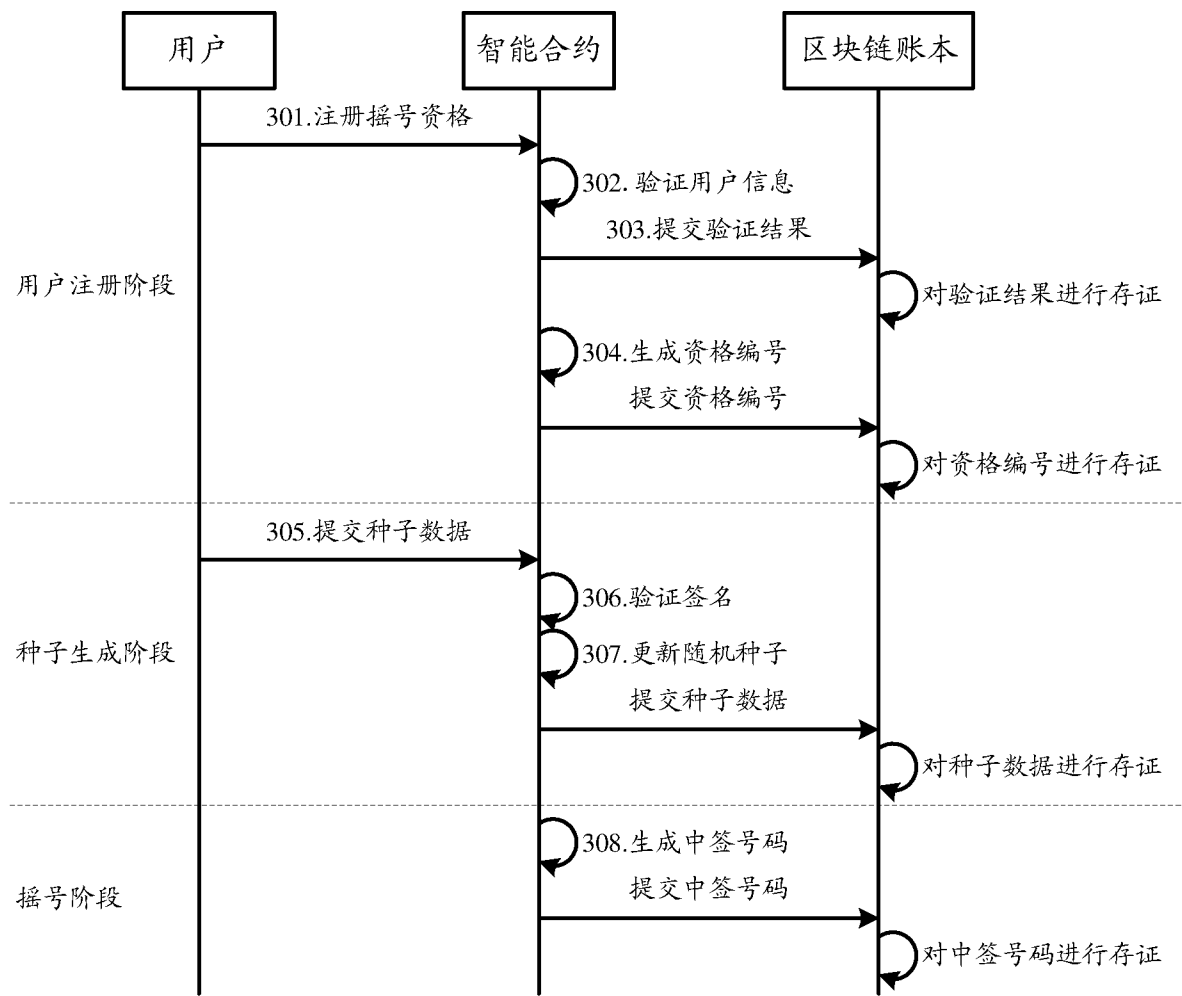


图 3

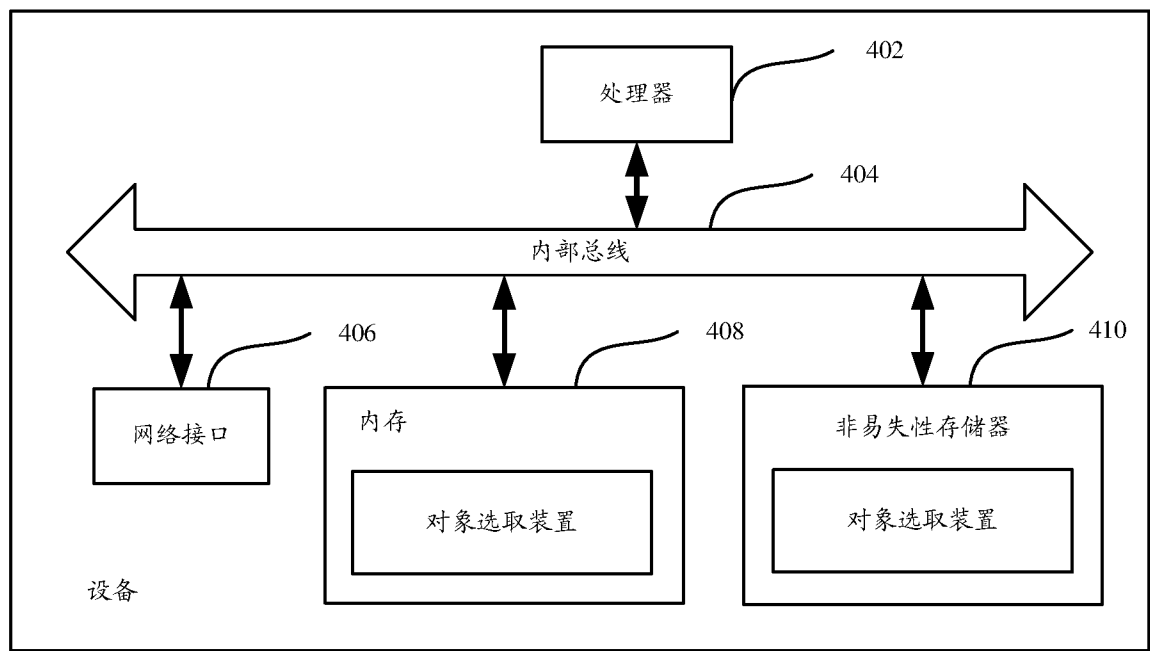


图 4

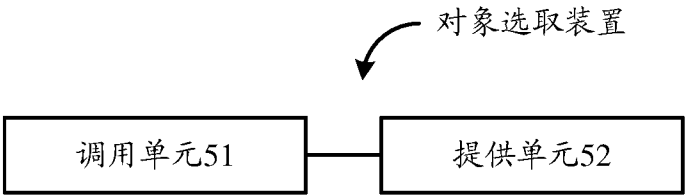


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/101681

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(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; G06F

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)

CNKI; CNPAT; WPI; EPODOC: 筛选, 抽签, 摇号, 随机数, 区块链, 区块, 智能合约, 种子, 目标, 匹配, filter, random, number, block, block chain, smart contract, seed, target, match+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109615370 A (ALIBABA GROUP HOLDING LIMITED) 12 April 2019 (2019-04-12) claims 1-21	1-21
X	CN 107820690 A (CLOUDMINDS TECHNOLOGIES CHENGDU CO., LTD.) 20 March 2018 (2018-03-20) description, paragraphs [0037]-[0115] and [0136]-[0166]	1-21
A	CN 108170403 A (BEIJING ORACLE CHAIN TECHNOLOGY CO., LTD.) 15 June 2018 (2018-06-15) entire document	1-21
A	US 2018267789 A1 (FUJITSU LIMITED) 20 September 2018 (2018-09-20) entire document	1-21
A	CN 108648323 A (GUANGZHOU SENDI COMPUTER SYSTEM CO., LTD.) 12 October 2018 (2018-10-12) entire document	1-21



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

18 October 2019

Date of mailing of the international search report

21 November 2019

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/CN2019/101681

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109615370	A	12 April 2019	None			
CN	107820690	A	20 March 2018	WO	2019036831	A1	28 February 2019
CN	108170403	A	15 June 2018	None			
US	2018267789	A1	20 September 2018	EP	3379408	A1	26 September 2018
				JP	2018156079	A	04 October 2018
CN	108648323	A	12 October 2018	None			

国际检索报告

国际申请号

PCT/CN2019/101681

A. 主题的分类

G06Q 20/38 (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; G06F

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))

CNKI; CNPAT; WPI; EPDOC: 筛选, 抽签, 摇号, 随机数, 区块链, 区块, 智能合约, 种子, 目标, 匹配, filter, random, number, block, block chain, smart contract, seed, target, match+

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 109615370 A (阿里巴巴集团控股有限公司) 2019年 4月 12日 (2019 - 04 - 12) 权利要求1-21	1-21
X	CN 107820690 A (达闼科技成都有限公司) 2018年 3月 20日 (2018 - 03 - 20) 说明书第37-115, 136-166段	1-21
A	CN 108170403 A (北京欧链科技有限公司) 2018年 6月 15日 (2018 - 06 - 15) 全文	1-21
A	US 2018267789 A1 (FUJITSU LIMITED) 2018年 9月 20日 (2018 - 09 - 20) 全文	1-21
A	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) 全文	1-21

☐ 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 10月 18日

国际检索报告邮寄日期

2019年 11月 21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

汪德闯

电话号码 86-(10)-53961791

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/101681

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	109615370	A	2019年 4月 12日	无			
CN	107820690	A	2018年 3月 20日	W0	2019036831	A1	2019年 2月 28日
CN	108170403	A	2018年 6月 15日	无			
US	2018267789	A1	2018年 9月 20日	EP	3379408	A1	2018年 9月 26日
				JP	2018156079	A	2018年 10月 4日
CN	108648323	A	2018年 10月 12日	无			