(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)

WIPO | PCT

(10) 国际公布号
WO 2020/082877 A1

(51) 国际专利分类号:
G06Q 20/10 (2012.01)

(21) 国际申请号: PCT/CN2019/101938

(22) 国际申请日: 2019 年 8 月 22 日 (22.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811259006.5 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)。

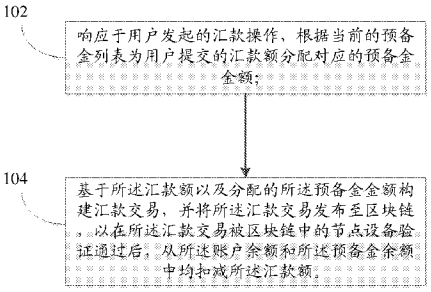
(72) 发明人: 马宝利 (**MA, Baoli**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 刘正 (**LIU, Zheng**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 张文彬 (**ZHANG, Wenbin**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 李漓春 (**LI, Lichun**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 殷山 (**YIN, Shan**); 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,

(54) **Title:** BLOCKCHAIN-BASED REMITTANCE METHOD AND DEVICE

(54) 发明名称: 基于区块链的汇款方法及装置



102 In response to a remittance operation initiated by a user, allocate, according to a current contingency fund list, a corresponding contingency fund amount to a remittance amount indicated by the user

104 Construct a remittance transaction on the basis of the remittance amount and the allocated contingency fund amount, and transmit the remittance transaction to a blockchain, such that both the remittance amount and the contingency balance are deducted from the account balance after the remittance transaction has been authenticated by node equipment in the blockchain

(57) **Abstract:** Provided in one or more embodiments of the present specification are a blockchain-based remittance method and device applied to a user terminal device in a blockchain. An account balance in a user account is at least divided into a contingency balance and a reserve balance. The user account comprises a dynamically updated contingency fund list. The contingency fund list comprises multiple contingency fund amounts. The method comprises: in response to a remittance operation initiated by a user, allocating, according to a current contingency fund list, a corresponding contingency fund amount to a remittance amount indicated by the user; and constructing a remittance transaction on the basis of the contingency fund amount allocated to the remittance amount, and transmitting the remittance transaction to a blockchain, such that the remittance amount is deducted from both the account balance and the contingency balance after the remittance transaction has been authenticated by node equipment in the blockchain.

WO 2020/082877 A1

[见续页]

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))。

(57) 摘要：本说明书一个或多个实施例提供一种基于区块链的汇款方法及装置，应用于区块链的用户端设备，用户账户的账户余额至少被划分为一预备金余额和一备用余额；其中，所述用户账户包括一动态更新的预备金列表；所述预备金列表包括多个预备金金额；所述方法包括：响应于用户发起的汇款操作，根据当前的预备金列表为用户提交的汇款额分配对应的预备金金额；基于所述汇款额的所述预备金金额构建汇款交易，并将所述汇款交易发布至区块链，以在所述汇款交易被区块链中的节点设备验证通过后，从所述账户余额和所述预备金余额中均扣减所述汇款额。

基于区块链的汇款方法及装置

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，尤其涉及一种基于区块链的汇款方法及装置。

背景技术

[02]区块链是一种防篡改的、共享的数字化账本，用于记录公有或私有对等网络中的交易。账本分发给网络中的所有成员节点，在区块中永久记录网络中发生的资产交易的历史记录。由于账本是完全公开的，因此区块链账本本身无隐私保护功能，需通过额外的技术来保护资产交易的隐私。目前已有的隐私保护方案中都利用了零知识证明技术来保证交易金额在一个合理区间。不同于UTXO模型，在账户模型下应用零知识证明技术会带来严重的交易并发性问题，因为上述零知识证明技术与账户的现有余额紧密关联，账户的余额会在并发发送的某一交易被验证后发生改变，从而引起尚未验证的、以原账户余额作为零知识证明的并行发送的其他交易无法通过验证，因此严重阻碍了账户模型下隐私保护方案的实际落地应用。

[03]现有的一种解决方案为基于区块链用户的账户余额生成包含多个预备金金额的预备金列表，并将预备金列表中可用的多个预备金金额指定至多个汇款交易中；区块链的节点针对各个汇款交易所包括的预备金金额进行各个汇款交易是否足以支付的验证，对各个汇款交易的验证分别独立进行，不相互影响，从而使得基于账户模型构建的区块链可以并行发送多个汇款交易。上述技术方案存在一个问题：需要在初始化预备金列表时暂停用户的账户交易，直到初始化完成后才能进行后续的交易，在一定程度上对汇款交易的并发性仍有影响。

发明内容

[04]有鉴于此，本说明书一个或多个实施例提供一种基于区块链的汇款方法及装置、电子设备及计算机可读存储介质。

[05]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：

[06]根据本说明书一个或多个实施例的第一方面，提出了一种基于区块链的汇款方法，应用于区块链的用户端设备，用户账户的账户余额至少被划分为一预备金余额和一备用余额；其中，所述用户账户包括一动态更新的预备金列表；所述预备金列表包括多个预备金金额；

[07]所述方法包括：

[08]响应于用户发起的汇款操作，根据当前的预备金列表为用户提交的汇款额分配对应的预备金金额；基于所述汇款额以及分配的所述预备金金额构建汇款交易，并将所述汇款交易发布至区块链，以在所述汇款交易被区块链中的节点设备验证通过后，从所述账户余额和所述预备金余额中均扣减所述汇款额；

[09]其中，所述预备金列表的创建及更新过程包括：

[10]步骤 A，获得当前的预备金余额，根据当前的预备金余额得到预备金列表；

[11]步骤 B，动态监测当前预备金列表中可用于分配的预备金金额是否低于预设阈值，如果是则将当前的备用余额切换为预备金余额后，执行步骤 A。

[12]根据本说明书一个或多个实施例的第二方面，提出了一种基于区块链的汇款装置，应用于区块链的用户端设备，用户账户的账户余额至少被划分为一预备金余额和一备用余额；其中，所述用户账户包括一动态更新的预备金列表；所述预备金列表包括多个预备金金额；

[13]所述装置包括：

[14]预备金金额分配单元，响应于用户发起的汇款操作，根据预备金列表创建单元提供的当前的预备金列表为用户提交的汇款额分配对应的预备金金额；

[15]汇款交易构建及发布单元，基于所述汇款额以及分配的所述预备金金额构建汇款交易，并将所述汇款交易发布至区块链，以在所述汇款交易被区块链中的节点设备验证通过后，从所述账户余额和所述预备金余额中均扣减所述汇款额；

[16]其中，所述预备金列表创建单元包括：

[17]预备金列表生成模块，获得当前的预备金余额，根据当前的预备金余额得到预备金列表；

[18]预备金列表监测模块，动态监测当前预备金列表中可用于分配的预备金金额是否低于预设阈值。

[19]根据本说明书一个或多个实施例的第三方面，提出了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如上述基于区块链的汇款方法。

[20]根据本说明书一个或多个实施例的第四方面，提出了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行上述基于区块链的汇款方法所述的步骤。

[21]本说明书提供的基于区块链的汇款方法及装置，将用户账户的账户余额至少划分为一预备金余额和一备用余额，基于预备金余额生成预备金列表，可将预备金列表包括的多个预备金金额分配给多个汇款交易，支持并发的多个汇款交易；当预备金列表中可用于分配的预备金金额低于预设阈值时，用户端设备将上述备用余额切换为预备金余额并基于该切换后的预备金余额生成新的预备金列表，在新的预备金列表生成完毕后，更新替换原预备金列表，基于新的预备金列表中的预备金金额可发起新的汇款交易。

[22]在本说明书提供的汇款方法及装置中，上述备用余额可在原预备金列表中的预备金金额消耗至预设的阈值时即开启新的预备金列表的初始化操作，待新的预备金列表生成后，可立即切换成基于新的预备金列表生成汇款交易；新预备金列表生成（或被区块链共识验证）期间用户发送的汇款交易仍基于原预备金列表中可用于分配的预备金金额生成；上述切换预备金余额并初始化新的预备金列表的过程可随着既有预备金列表的使用情况（可用于分配的预备金金额是否低于预设阈值）、或应接收到的新的预备金列表构建指令循环执行，因此全程无需暂停发送汇款的交易，提高交易的并发性，且避免交易中断，最大化了区块链交易的吞吐量。

附图说明

[23]图 1 是一示例性实施例提供的一种基于区块链的汇款方法的流程图。

[24]图 2 是一示例性实施例提供的一种预备金列表的创建及更新过程的流程图。

[25]图 3 是一示例性实施例提供的种在区块链网络中实施汇款交易的示意图。

[26]图 4 是一示例性实施例提供的一种在区块链网络中实施更新预备金列表并汇款交易的流程图。

[27]图 5 是一示例性实施例提供的区块链上用户的账户状态示意图。

[28]图 6 是一示例性实施例提供的一种基于区块链的用户端设备的示意图。

[29]图 7 是一示例性实施例提供的一种基于区块链的汇款装置的示意图。

具体实施方式

[30]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。

[31]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。

[32]图 1 是一示例性实施例提供的一种基于区块链的汇款方法的流程图，应用于区块链的用户端设备，用户账户的账户余额至少被划分为一预备金余额和一备用余额；其中，所述用户账户包括一动态更新的预备金列表；所述预备金列表包括多个预备金金额。

[33]上述实施例所述的区块链，具体可指一个各节点设备通过共识机制达成的、具有分布式数据存储结构的 P2P 网络系统，该区块链内的数据分布在时间上相连的一个个“区块（block）”之内，后一区块包含前一区块的数据摘要，且根据具体的共识机制（如 POW、POS、DPOS 或 PBFT 等）的不同，达成全部或部分节点的数据全备份。本领域的技术人员熟知，由于区块链系统在相应共识机制下运行，已收录至区块链数据库内的数据很难被任意的节点篡改，例如采用 Pow 共识的区块链，至少需要全网 51%算力的攻击才有可能篡改已有数据，因此区块链系统有着其他中心化数据库系统无法比拟的保证数据安全、防攻击篡改的特性。由此可知，在本说明书所提供的实施例中，被收录至区块链的分布式数据库中的汇款交易及其他交易不易被攻击或篡改，从而为发布至所述区块链的分布式数据库的交易进行了存证。

[34]执行本实施例所述的基于区块链的汇款方法的用户端设备，可以为上述区块链的节点设备，也可为与上述区块链的节点设备连接的客户端设备，在本说明书中不作限定。

[35]将上述区块链作为一个通用的管理对象状态转换的去中心化平台，用户账户就是有

状态的对象，用户账户所包括的内容可以为上述用户账户的状态所包含的内容，本说明书所提供的用户账户包含账户余额信息和用以支持汇款交易的预备金列表。在本说明书中，为了支持用户可无暂停地发送汇款交易，用户账户中包括一动态更新的预备金列表，所述预备金列表包括多个预备金金额。

[36]上述多个预备金金额可被分配在不同的汇款交易中，为每个汇款交易提供足以支付其汇款额的证明。值得注意的是，本说明书所述的“账户”不限于外部所有账户（EOA）及合约账户（Contract），且也不限定上述预备金列表的具体表现形式，只要包含或管理上述多个预备金金额的数据组织形式，如一维表、二维表、树形数据结构等均属于本说明书所述的预备金列表。本说明书所述的预备金余额和备用余额的值可以不显示在区块链的用户账户状态中，而作为用户客户端可显示或管理的内容；当然，上述预备金余额和备用余额的值也可以显示在区块链的用户账户状态中，在本说明书中不作限定。

[37]如图 1 所示，上述汇款方法可以包括以下步骤:

[38]步骤 102，响应于用户发起的汇款操作，根据当前的预备金列表为用户提交的汇款额分配对应的预备金金额;

[39]步骤 104，基于所述汇款额以及分配的所述预备金金额构建汇款交易，并将所述汇款交易发布至区块链，以在所述汇款交易被区块链中的节点设备验证通过后，从所述账户余额和的预备金余额中均扣减所述汇款额。

[40]在上述实施例中，与汇款额对应的预备金金额至少为一个，且与汇款额对应的预备金金额之和应不小于交易的汇款额，从而为该汇款交易提供足以支付的凭证。例如，当前的预备金列表中包含{5,10,15,20}四个预备金金额，对于汇款额为 10 的汇款交易，用户端设备可从上述四个预备金金额中选出一个预备金金额 10（或 15 或 20），将上述一个预备金金额 10（或 15 或 20）分配至上述汇款交易中；对应汇款额为 12 的汇款交易，用户端设备可从上述四份预备金金额中选出一个预备金金额 15（或 20），将上述一个预备金金额 15（或 20）分配至上述汇款交易中，也可以从上述四个预备金金额中选出两个预备金金额 5 和 10（或 5 和 15），将上述两个预备金金额 15（或 20）分配至上述汇款交易中，利用两个预备金金额之和为汇款交易提供足以支付的验证证明。

[41]在一实施例中，汇出方用户与接收方用户可以约定从汇出方区块链账户向接收方区块链账户汇入（或称为转移）对应于该汇款额的资产凭证。资产凭证可以对应于区块链内的代币（token）、数字资产等智能资产，资产凭证还可以对应于区块链外的现金、证

券、优惠券、房产等链外资产，本说明书并不对此进行限制。

[42]汇款交易构建完毕后被用户端设备发送至区块链，并接收区块链中节点设备的验证。由于本说明书所提供的基于区块链的汇款方法可以被应用在基于多种共识机制类型的区块链中，因此本说明书既不限定对上述汇款交易执行验证的区块链节点的数量及类型，也不限制上述验证所包含的内容或流程。不过本领域技术人员应知，上述验证至少包含验证汇款交易中的预备金金额之和是否大于或等于汇款交易的汇款额，以检验用户账户是否有足够的余额支付该汇款交易。当上述汇款交易被区块链的节点设备验证通过后，从用户的账户余额和预备金余额中均扣减所述汇款额。

[43]图 2 示意了上述实施例中预备金列表的创建及更新过程，如图 2 所示该过程可被概括为两个彼此相连的循环步骤:

[44]步骤 A，获得当前的预备金余额，根据当前的预备金余额得到预备金列表;

[45]步骤 B，动态监测当前预备金列表中可用于分配的预备金金额是否低于预设阈值，如果是则将当前的备用余额切换为预备金余额后，执行步骤 A。

[46]在用户注册为上述区块链的用户后，用户可将账户余额至少划分为一初始化的预备金余额和一初始化的备用余额，用户设备首先基于该初始化的预备金余额执行上述步骤 A 所述的过程。

[47]上述当前的备用余额可在切换后生成新的预备金列表中的预备金金额；可选的，在未被触发以生成新的预备金列表之前，该备用余额即可以作为汇款余额以支持用户发起单独的（不并发）汇款交易，也可以作为收款余额用以接收其他账户汇至该用户账户的汇款；而且，当账户余额包括两个或两个以上的备用余额时，其中有些备用余额还可以不参与汇款或收款，仅作为静止的余额，以在合适的时机（如基于原预备金余额生成的预备金列表中可用于分配的预备金金额低于预设阈值时，或接收到用户发送的新的预备金列表构建指令时）被触发以划分得出新的预备金列表中的预备金金额。

[48]在一个示出的实施例中，步骤 A 中所述的根据当前的预备金余额得到预备金列表的过程，包括:

[49]对当前预备金余额进行划分得到多个预备金金额，基于划分得到的多个预备金金额构建预备金列表创建交易;

[50]将所述预备金列表创建交易发布至区块链，以在所述预备金列表创建交易被区块链中的节点设备验证通过后，在所述用户账户基于所述划分得到的多个预备金金额构建预

备金列表。

[51]在上述的实施例中，当前的预备金余额可被划分以得到多个预备金金额，为保证上述多个预备金金额得到区块链节点的共识验证，预备金列表创建交易所包含的、基于当前的预备金余额划分得到的多个预备金金额之和应不大于该预备金余额。由于本说明书所提供的基于区块链的汇款方法可以被应用在基于多种共识机制类型的区块链中，因此本说明书既不限定对上述预备金列表创建交易执行验证的区块链节点的数量及类型，也不限制上述验证所包含的内容或流程。不过本领域技术人员应知，上述验证至少包含验证预备金列表创建交易中的预备金金额之和是否小于或等于当前的预备金余额（或当用户的账户状态中不显示预备金余额时，至少应验证预备金列表创建交易中的预备金金额之和是否小于或等于当前的账户余额），以检验上述预备金余额的有效性。当上述预备金列表创建交易被区块链的节点设备验证通过后，在所述用户账户基于预备金列表创建交易所包括的、所述划分得到的多个预备金金额构建预备金列表。

[52]在又一示出的实施例中，上述根据当前的预备金余额得到预备金列表，包括:

[53]对当前预备金余额进行划分得到多个预备金金额，基于划分得到的多个预备金金额构建预备金列表，并基于所述预备金列表构建预备金列表创建交易;

[54]将所述预备金列表创建交易发布至区块链，以在所述预备金列表创建交易被区块链中的节点设备验证通过后，将所述预备金列表更新至所述用户账户中。

[55]在上述实施例中，当前的预备金余额可被划分以得到多个预备金金额，基于上述多个预备金金额构建预备金列表，并将上述包括基于当前的预备金余额划分得到的多个预备金金额的预备金列表包括在上述预备金列表创建交易中。为保证上述多个预备金金额得到区块链节点的共识验证，预备金列表创建交易所包含的、基于当前的预备金余额划分得到的多个预备金金额之和应不大于该预备金余额。由于本说明书所提供的基于区块链的汇款方法可以被应用在基于多种共识机制类型的区块链中，因此本说明书既不限定对上述预备金列表创建交易执行验证的区块链节点的数量及类型，也不限制上述验证所包含的内容或流程。不过本领域技术人员应知，上述验证至少包含验证预备金列表创建交易中的预备金金额之和是否小于或等于当前的预备金余额（或当用户的账户状态中不显示预备金余额时，至少应验证预备金列表创建交易中的预备金金额之和是否小于或等于当前的账户余额），以检验上述预备金余额的有效性。当上述预备金列表创建交易被区块链的节点设备验证通过后，将预备金列表创建交易所包括的预备金列表更新至所述用户账户中。

[56]本领域的技术人员应知，预备金列表中的每个预备金金额是为汇款交易提供足以支付的余额凭证，基于同一预备金金额重复分配的汇款交易无法通过区块链节点的验证。随着越来越多汇款交易的发出，用户账户中当前的预备金列表中可用于分配的预备金金额越来越少。为了在切换准备新的预备金列表时不用暂停发送汇款交易，可以为现有的预备金列表中可用于分配的预备金金额设置一阈值，该阈值既可以是预备金金额的总额度阈值（即剩余可用的预备金金额可支付的最大汇款额阈值），也可以是预备金金额的个数阈值（即剩余可用的预备金余额最多还可用于发送的汇款交易的个数阈值），在用户端设备动态监测到现有的预备金列表中的可用于分配的预备金金额低于上述预设阈值时，则将当前的备用余额切换为预备金余额后，执行上述实施例中步骤 A 所述的过程。可选的，上述将当前的备用余额切换为预备金余额的步骤还可应用户发出的指令而被触发。

[57]区块链的节点设备（包括用户端设备）发布、共识验证、在用户账户的状态中更新新的预备金列表的过程通常需要消耗一定的时间，具体消耗时长与该区块链的共识机制、出块频率等相关。在此期间，若用户有新的汇款交易的发送需求，由于用户账户中当前的预备金列表仍处在生效状态，可仍基于当前预备金列表中可用于分配的预备金金额构建汇款交易。在新的预备金列表被更新至用户账户后，该新的预备金列表即可作为用户账户中当前的预备金列表，用户即可基于该当前预备金金列表构建汇款交易，并向区块链发布汇款交易；相应的，在上述汇款交易被区块链中的节点设备验证通过后，从所述账户余额和所述切换后的预备金余额中均扣减所述汇款额。

[58]本说明书提供的汇款方法，由于用户账户中始终存在一生效的预备金列表，因此而无需暂停汇款交易，最大化了交易吞吐量。

[59]在一示出的实施例中，为分辨预备金列表中可用于分配的预备金金额，可以标记预备金列表中的预备金金额的使用状态。当一包括预备金金额的汇款交易被区块链中的节点设备验证通过，并在区块链的分布式数据库内收录该汇款交易、且更新该汇款交易的汇出方用户的账户余额时，该汇款交易所包含的预备金金额应在汇出方账户的预备金列表中被标识为已使用状态（状态 3），本领技术人员熟知，上述被收录在区块链的分布式数据库中的汇款交易可称为“已完成的汇款交易”。对于新的尚未完成的汇款交易，区块链中的节点设备可验证上述新的尚未完成的汇款交易中的预备金金额在汇出方用户账户的预备金列表中的状态是否为已使用状态：如果是已使用状态，则该项验证不通过，相应的新的尚未完成的汇款交易可以被退回；如果不是已使用状态，则该项验证通

过。类似地，当该新的汇款交易通过验证后在区块链的分布式数据库中更新时，区块链节点也应将该新的汇款交易中包含的预备金金额在汇出方用户账户的预备金列表中更新为“已使用状态”。

[60]更优的，用户端设备还可将未被使用过的、亦即还未被分配至任何汇款交易的预备金金额可在预备金列表中标记为未使用状态（状态 1）；一预备金金额一旦被分配于一个汇款交易，该预备金金额可在用户账户的预备金列表中即刻被标识为被使用状态（状态 2），亦即在用户端保存的当前预备金列表中将上述预备金金额标定为被使用状态（状态 2）。由此，用户端设备仅能分配未使用状态（状态 1）的预备金金额用于新的汇款交易，且在分配后将该被分配的预备金金额随即在本地更改为被使用状态（状态 2），以防止对同一预备金金额的重复分配。

[61]在一示出的实施例中，在根据当前的预备金余额得到预备金列表之后，将切换前的预备金余额切换为备用余额。

[62]在用户端设备根据上述实施例所述的过程根据当前的预备金金额得到预备金列表之后，此时，由于新的预备金列表已经作为当前预备金列表可用于新的汇款交易，原预备金列表可以停止用作汇款交易，相应的，原预备金余额可被切换为备用余额，以在现有当前的预备金列表中的预备金金额低于预设阈值或接收到新的预备金列表构建指令时，基于该当前的预备余额构建新的预备金列表。

[63]更优地，为优化管理用户账户中的各余额，本说明书所述的备用余额可用作收款余额，当其他用户发起对上述用户账户的汇款交易被区块链的节点设备验证通过后，该汇款交易中的汇款额将被增加至所述收款余额和所述账户余额。

[64]为保护区块链用户的账户隐私安全，在现有的一些区块链中，用户的账户余额、及汇款交易的交易额均被加密；本说明书所提供的汇款方法也可以用于隐私模式的区块链中。

[65]在一示出的实施例中，区块链用户账户的账户余额、预备金列表中的预备金金额、用户设备发起的汇款交易中的汇款额均被预先进行了加密处理。由于汇款交易所包括的汇款额及预备金金额均为加密状态，为保证区块链节点可以验证上述被分配至汇款交易的预备金金额足以支付本次汇款，上述汇款交易中还应包括用以证明为所述汇款交易包括的预备金金额之和大于或等于所述汇款交易的汇款额的第一零知识证明。

[66]相应地，由于用户账户的账户余额及用户基于切换后的预备金余额划分得到的多个

预备金金额均被预先进行了加密处理，为保证区块链节点可以验证预备金列表创建交易所包含的预备金金额之和没有超出用户的账户余额，上述预备金列表创建交易还应包括用以证明基于切换后的预备金余额划分出的多个预备金金额之和小于或等于所述用户的账户余额的第二零知识证明。

[67]零知识证明，通常指的是证明者（被验证者）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。在本说明书中，用户端设备可通过提供第一零知识证明，使得区块链中的节点（验证者）在不获知汇款额、及预备金金额的具体值的情况下，可以相信为汇款交易所分配的预备金金额的具体值之和大于或者等于所述汇款额的具体值，足以支付上述汇款交易，亦即使得区块链中的节点（验证者）基于零知识证明算法针对所述第一零知识证明进行零知识验证，以确认为所述汇款交易所分配的预备金金额之和是否大于或者等于所述汇款额。同理，用户端设备可通过提供第二零知识证明，使得区块链中的节点（验证者）在不获知用户账户的账户余额、及预备金列表创建交易所包含的预备金金额的实际值（明文）情况下，可以相信预备金列表创建交易中所包含的多个预备金金额之和是否不大于上述用户账户的账户余额。

[68]在一示出的实施例中，当用户账户中的预备金余额、备用余额也被显示在用户账户的状态中，即区块链上的其他节点可通过查询用户账户状态，获知本用户设备的预备金余额和备用余额时，为保护用户的账户隐私安全，用户账户的预备金余额和备用余额也被预先进行了加密处理，此时上述的第二零知识证明可用于证明基于切换后的预备金余额划分出的多个预备金金额之和小于或等于所述切换后的预备金余额。由于上述切换后的预备金余额是基于账户余额划分得到的，该预备金余额必定小于账户余额，所以上述的第二零知识证明也可为区块链节点验证预备金列表创建交易所包含的预备金金额之和不大于账户余额提供了有效的证明。

[69]本说明书并不限定上述密码学加密算法的类型，可以包括加法同态加密算法或全同态加密算法，还可包括同态承诺算法（如 Pederson Commitment 等），只要确保该加密算法能够满足加法同态并且能够支持验证一明文数据属于某个区间的零知识证明，使得加密的汇出方用户的账户余额（或预备金余额）可直接扣除加密的汇款额，加密的接收方用户的账户余额可直接增加加密的汇款额。

[70]例如，上述区块链可以支持基于椭圆曲线的 Pedersen Commitment 承诺算法，用以保证区块链中被加密的数额可以在加密状态被验证数额范围、且可实现加法同态。

[71]本说明书并不限定上述第一零知识证明、第二零知识证明的具体类型，例如可以采

用相关技术中的区间证明（Range Proof）技术，譬如 Bulletproofs 方案或“zksnark”通用零知识证明技术等。

[72]在又一示出的实施例中，为防止区块链中用户节点作恶对区块链进行攻击，上述汇款交易中还可包括用以证明所述汇款额大于或等于零的第三零知识证明，上述第三零知识证明可基于所述被加密的汇款额生成，使得区块链中的节点（验证者）在不获知汇款额的实际值（明文）情况下，可以验证汇款交易的汇款额不小于零。

[73]在又一示出的实施例中，为防止区块链中用户节点作恶生成无效的预备金金额，预备金列表创建交易中还可包括用以证明上述预备金列表创建交易所包含的每个预备金金额均大于或等于零的第四零知识证明，上述第四零知识证明可基于各个预备金金额生成，使得区块链中的节点（验证者）在不获知各个预备金金额的实际值（明文）情况下，可以验证预备金列表创建交易中包含的每个预备金金额均大于或等于零。

[74]在本说明书又一示出的实施例中，上述汇款交易及预备金列表创建交易还可包括用户端设备基于用户账户的私钥所作的数字签名，用以供区块链的节点对电子签名进行验证，防止其他节点冒充汇出方而发布上述第一交易，发布错误信息、恶意扰乱交易秩序。

[75]本说明书提供的基于区块链的汇款方法，通过将用户账户的账户余额至少划分为一预备金余额和一备用余额，基于预备金余额构建包含多个预备金金额的预备金列表，为用户账户并发汇款交易提供可支付证明；在上述预备金列表中的可用预备金金额低于预设阈值时，或接到新的预备金列表构建指令时，再将上述备用余额切换为预备金月，基于上述切换后的预备金余额构建包含多个预备金金额的新的预备金列表；在新的预备金列表被区块链节点验证通过、新的预备金列表被更新至用户账户后，用户账户再基于新的预备金列表构建新的汇款交易。上述预备金列表切换的过程中，汇款交易可仍基于原预备金列表构建而无需暂停；且而上述切换预备金余额并创建新的预备金列表的过程可随着当前预备金列表的使用情况（可用于分配的预备金金额是否低于预设阈值）、或应接收到的新的预备金列表构建指令循环执行，因此全程无需暂停发送汇款的交易，提高交易的并发性，且避免交易中断，最大化了区块链交易的吞吐量。

[76]为了便于理解，下面以区块链网络中的汇款交易为例，对本说明书的技术方案进行详细说明。图 3 是一示例性实施例提供的一种在区块链网络中实施汇款交易和预备金列表交易的示意图。假定用户 A 使用的汇出方设备为用户设备 1，譬如该用户设备 1 上登录有对应于用户 A 的用户账号；类似地，用户 B 使用的接收方设备为用户设备 2。用户设备 1 上可以运行有区块链的客户端程序，使得该用户设备 1 在区块链网络中存在对应

的区块链节点，比如图 2 所示的节点 1。类似地，用户设备 2 上可以运行有区块链的客户端程序，使得该用户设备 2 在区块链网络中存在对应的区块链节点，比如图 3 所示的节点 2。区块链网络中还存在其他区块链节点，比如图 3 所示的节点 i 等。通过上述的节点 1、节点 2、节点 i 等，使得用户 A 与用户 B 之间的汇款交易、及用户 A 发送的预备金列表创建交易可以经由区块链网络实施，相关交易信息可以被记录至各个区块链节点分别维护的区块链账本中，可以避免发生篡改，并有助于后续查验。

[77]例如，由用户 A 向用户 B 进行区块链汇款。用户 A 在注册账户后，首先应发送预备金列表创建交易以初始化其账户中的预备金列表。其中，本说明书中的“用户”可以表现为所登录的用户账号，而该用户账号实际可以归属于个人或组织，本说明书并不对此进行限制。

[78]如图 5 所示，在上述区块链中，用户 A 的账户余额 s_A 被分为两个子余额：s_A_1 和 s_A_2，用户 B 的账户余额 s_B 也被分为两个子余额：s_B_1 和 s_B_2。用户 A 的账户余额 s_A、子余额 s_A_1 和 s_A_2 及用户 B 的账户余额 s_B、子余额 s_B_1 和 s_B_2 均基于加密算法被加密：

S_A=HE(s_A)，S_A_1=HE(s_A_1)，S_A_2=HE(s_A_2);

S_B=HE(s_B)，S_B_1=HE(s_B_1)，S_B_2=HE(s_B_2)。

[79]在一实施例中，上述加密算法可以为 Pederson Commitment 同态承诺算法。

[80]初始时，子余额 s_A_1 作为预备金余额，s_A_2 作为收款余额，子余额 s_B_1 作为预备金余额，s_B_2 作为收款余额。

[81]图 4 示意了用户 A 设置预备金列表 M_A 并基于预备金列表 M_A 发起汇款交易的过程。设置用户 A 的预备金列表 M_A 的过程包括以下步骤：

[82]步骤 401，用户 A 建立预备金列表 M_A，上述预备金列表 M_A 包括用户 A 针对子余额 s_A_1 划分得到的、被基于上述的同态加密算法 HE 加密的、多个预备金金额 $M_A[1]$，$M_A[2]$，…，$M_A[L_A]$，并在上述预备金列表中将上述预备金金额 $M_A[1]$，$M_A[2]$，…，$M_A[L_A]$的使用状态标记为“未使用状态”。

[83]具体实现时，用户 A 可对子余额 s_A_1 或子余额 s_A_1 的部分余额进行划分，得到上述多个预备金金额的明文 $m_a[1]$，$m_a[2]$，…，$m_a[L_A]$，并基于上述同态加密算法对上述多个预备金金额加密，以得到预备金金额密文 $M_A[1]$，$M_A[2]$，…，$M_A[L_A]$；用户 A 也可以对子余额 s_A_1 的密文 S_A_1 直接进行划分以得到 $M_A[1]$，$M_A[2]$，…，$M_A[L_A]$，

并基于上述同态加密算法的进行逆运算，获知上述预备金金额密文对应的明文 $m_a[1]$，$m_a[2]$，…，$m_a[L_A]$。用户 A 可将上述预备金金额的明文 $m_a[1]$，$m_a[2]$，…，$m_a[L_A]$与密文 $M_A[1]$，$M_A[2]$，…，$M_A[L_A]$的对应关系独自保存，以方便用户 A 在具体的汇款交易中选取合适的预备金金额。或者，用户 A 可仅在本地用户端保存上述预备金金额的明文，用户端周期性地从区块链上同步账户数据，将从区块链上获取的加密数据解密后，即可得到已被使用的预备金金额。

[84] 步骤 402，用户 A 生成零知识证明 $PF[s\_A\_1 \geqslant (m_a[1]+m_a[2]+\cdots+m_a[L_A])]$，用于证明上述预备金列表 M_A 中的 $M_A[1], M_A[2], \cdots, M_A[L_A]$对应的预备金金额 $m_a[1], m_a[2], \cdots, m_a[L_A]$之和小于或者等于用户 A 的子余额 s_A_1，上述零知识证明 $PF[s_A_1 \geqslant (m_a[1]+m_a[2]+\cdots+m_a[L_A])]$不使用预备金金额 $m_a[1]$，$m_a[2]$，…，$m_a[L\text{-}A]$及 s_A_1 的值，即可使验证者相信 $m_a[1]$，$m_a[2]$，…，$m_a[L_A]$之和小于或者等于 s_A_1。在一实施例中，上述零知识证明 $PF[s_A_1 \geqslant (m_a[1]+m_a[2]+\cdots+m_a[L_A])]$可使用 zksnark 等通用零知识证明技术或 Bulletproof 方案等区间证明技术。

[85] 步骤 403，用户 A 生成零知识证明 $PF(m_a[i] \geqslant 0)$，用以证明上述预备金列表 M_A 中的 $M_A[1]$，$M_A[2]$，…，$M_A[L_A]$对应的预备金金额 $m_a[1]$，$m_a[2]$，…，$m_a[L_A]$均不小于零。上述零知识证明 $PF(m_a[i] \geqslant 0)$不使用预备金金额 $m_a[i]$的值即可使验证者相信 $m_a[i] \geqslant 0$。在一实施例中，上述零知识证明 $PF(m_a[i] \geqslant 0)$可使用 Borromean 环签名方案或 zksnark 等通用零知识证明技术方案等区间证明技术。

[86] 步骤 404，用户 A 基于 M_A、$PF[s\_A\_1 \geqslant (m_a[1]+m_a[2]+\cdots+m_a[L\text{-}A])]$、$PF(m_a[i] \geqslant 0)$生成数字签名 $Sign\ A_s$。

[87] 步骤 405，用户 A 向所述区块链发送交易 T_s 以确定上述的预备金列表 M_A，上述交易 T_s 包括 M_A、$PF[s\_A\_1 \geqslant (m_a[1]+m_a[2]+\cdots+m_a[L_A])]$、$PF(m_a[i] \geqslant 0)$，其中 1<=i<=L_A，和 $Sign\ A_s$。

[88] 步骤 406，区块链的节点接收上述交易 T_s。

[89] 步骤 407，区块链的节点执行对上述交易 T_s 的电子签名 $Sign\ A_s$ 验证，如果通过，执行下个步骤。

[90] 步骤 408，区块链的节点基于零知识证明算法对 $PF[s_A_1 \geqslant (m_a[1]+m_a[2]+\cdots+m_a[L_A])]$进行零知识验证，以确认 $m_a[1]$，$m_a[2]$，…，$m_a[L_A]$之和是否小于或者等于所述用户 A 的子余额 s_A_1；如果是，执行下个步骤。

[91] 步骤 409，区块链的节点基于零知识证明算法对 PF(m_a [i] ⩾0)进行零知识验证，以确认(m_a [i] ⩾0 均不小于零，其中 1<=i<=L_A；如果是，执行下个步骤。

[92] 步骤 410，区块链的节点将通过验证的交易 T_s 收录至所述区块链的分布式数据库，并将预备金列表 M_A 更新至所述用户 A 的账户状态。

[93] 至此，区块链的节点完成了对用户 A 的预备金列表 M_A 的更新，本领域的技术人员熟知，在设置或更新用户 A 的预备金列表 M_A 的实际实施过程中，还可包括许多其他的验证步骤，例如防重放的验证等，在此不做限定；而且本说明书并不限定生成各个证明或电子签名的先后顺序，也不限定区块链中的节点对汇出方提出的交易 Ts 中各项证明或电子签名的验证的先后顺序，图 4 仅仅是本说明书提供的设置用户的预备金列表的方法的一种实施例，本说明书不限于此。用户 B 账户中的预备金列表 MB 的设置过程与上述步骤 401 至 410 的过程相似，在此不再赘述。

[94] 图 4 中的区块链执行用户 A 向用户 B 汇款转账的过程如下:

[95] 步骤 411，用户 A 基于上述同态加密算法生成汇款额密文 S_t=HE(s_t)，其中 s_t 为用户 A 向用户 B 转账的汇款额。

[96] 步骤 412，用户 A 从预备金列表 M_A 中选取一个未使用过的、且其明文 m_A[k]足以支付汇款额 s_t 的预备金金额密文 M_A[k]，并将该预备金金额密文 M_A[k]标记为被使用状态，以使 M_A[k]不可再被指定在其他新的汇款交易中。

[97] 步骤 413，用户 A 生成零知识证明 Pf（m_A[k]⩾s_t），用以证明 M_A[k]对应的预备金金额 m_A[k]足以支付本次汇款额 s_t；上述零知识证明 Pf（m_A[k]⩾s_t）不使用 m_A[k]及 s_t 的值，即可使验证者相信 m_A[k]⩾s_t。

[98] 步骤 414，用户 A 生成零知识证明 Pf（s_t⩾0），用以证明汇款额 s_t 不小于零；上述上述零知识证明 Pf（s_t⩾0）不使用 s_t 的值，即可使验证者相信 s_t⩾0。

[99] 步骤 415，用户 A 基于 St、M_A[k]、Pf（m_A[k]⩾s_t）、Pf（s_t⩾0）生成数字签名 Sign A_t。

[100] 步骤 416，用户 A 向所述区块链发送交易 T_t 以向用户 B 汇款转账，交易 T_t 包括 S_t、M_A[k]、Pf（m_A[k]⩾s_t）、Pf（s_t⩾0）及 Sign A_t，上述内容均为密文状态，因此保护了用户 A、B 的汇款交易隐私性。

[101] 步骤 417，区块链的节点接收上述交易 T_t。

[102] 步骤418，区块链的节点执行对上述交易T_t的电子签名Sign A_t验证，如果通过，执行下个步骤。

[103] 步骤419，区块链的节点验证上述T_t所包含的$M_A[k]$是否为已使用状态；如果否，执行下个步骤。

[104] 步骤420，区块链的节点基于零知识证明算法对PF（$m_a[k] \geqslant s\_t$）进行零知识验证，以确认$M_A[k]$对应的预备金金额是否大于或者等于所述汇款额；如果是，执行下个步骤。

[105] 步骤421，区块链的节点基于零知识证明算法对PF（$s\_t \geqslant 0$）进行零知识验证，以确认本次汇款交易的汇款额密文S_t对应的汇款额实际值不小于零；如果是，执行下个步骤。

[106] 步骤422，区块链的节点将通过验证的交易T_t收录至所述区块链的分布式数据库，并在用户A的账户余额密文S_A、和子账户余额密文S_A_1中均基于同态运算性质扣除所述汇款额密文S_t，在用户B的账户余额密文S_B和子账户余额密文S_B_2中均基于同态运算性质增加所述汇款额密文S_t，以使上述用户A的账户余额更新为（s_A-s_t），A的汇款子账户余额s_A_1更新为（s_A_1-s_t），用户B的账户余额更新为（s_B+s_t），B的收款子账户余额s_B_2更新为（s_B_2+s_t）；并将用户A的预备金列表M_A中$M_A[k]$对应的状态更改为已使用状态。

[107] 另外，本领域的技术人员熟知，在汇款交易的实际实施过程中，还可包括许多其他的验证步骤，例如防重放的验证等，在此不做限定；而且本说明书并不限定生成各个证明或电子签名的先后顺序，也不限定区块链中的节点对汇出方提出的交易T_t中各项证明或电子签名的验证的先后顺序，图4仅仅是本说明书提供的基于区块链的汇款方法的一种实施例，本说明书不限于此。

[108] 虽然图4中使用连续的编号表示了用户A初始化设置预备金列表及用户A向用户B汇款的过程，但是这并不表示用户A在每次发起汇款交易之前均需设置其账户中的预备金列表。本领域技术人员熟知，用户在注册成为该区块链的用户后的第一次汇款交易之前，需要初始化设置其账户中的预备金列表；当上述预备金列表中的被加密的预备金金额被使用完毕、或剩余的被加密的预备金金额对应的预备金金额已经不再足以支付下一汇款交易，用户才需重新设置其账户中的预备金列表；用户还根据自身的具体需求可周期性更新上述预备金列表。

[109] 随着用户 A 发送的汇款交易的增多，预备金列表 M_A 中可用的预备金金额逐渐变少，用户 A 的设备节点 1 监控预备金列表 M_A 中可用的预备金金额的数值总和、或监控预备金列表 M_A 中可用的预备金金额的个数之和，当上述数值总和、或个数之和低于设定的阈值时，用户 A 将其子账户 s_A_1 与 s_A_2 互相切换，基于新的预备金余额 s_A_2 来生成新的预备金列表 M_A'。新的预备金列表 M_A'的构建过程与步骤 401-410 类似，在此不再赘述，M_A'被更新至用户 A 的账户后，将替代原预备金列表 M_A 以作为新的有效的预备金列表为汇款交易提供可支付证明。

[110] 图 2 示意了上述的用户 A 账户中的预备金列表的创建及更新过程，由图 2 可以看出，通过子账户余额的循环切换，用户 A 的账户中始终存在一个有效的预备金列表可为并发的汇款交易提供多个预备金金额，从而使得用户 A 无需暂停汇款交易以更新预备金列表，保证了汇款交易的最大化并发提交和执行。而且，在本实施例提供的汇款交易方法中，由于分别设置了用于汇款和用于收款的两个子账户余额，假设在用户 A 向 B 执行汇款交易时，有其他用户 C 也在向用户 A 发起汇款交易，这些所有的交易可以同时被提交和执行；因为整个交易的执行过程中利用到的零知识证明只和相关的预备金金额有关，账户的余额可以随意的增加或扣减。

[111] 值得注意的是，如图 5 所示，用户 A 的子账户余额 S_A_2 在初始时用作收款交易，当用户设备监测到预备金列表 M_A 中的预备金金额低于预设的阈值时，需将子账户余额 S_A_1 与子账户余额 S_A_2 的功能互相切换，S_A_1 作为收款余额，S_A_2 作为预备金余额。在将 S_A_2 作为预备金余额以执行新的预备金列表的构建之前，用户设备需等待一段时间，直至上述切换之前区块链上其他用户发往用户 A 的子账户余额 S_A_2 的交易均被更新显示在用户 A 的账户余额 S_A 和子账户余额 S_A_2 之后，子账户余额 S_A_2 的值不再变化后，再基于 S_A_2 构建新的预备金列表，以防由于 S_A_2 的值的变化导致基于 S_A_2 的值生成的 $PF[s_A_2 \geqslant (m_a[1]+m_a[2]+\cdots+m_a[L_A])]$无法通过区块链节点的验证。上述等待时间可依区块链的成块频率而定，例如，约等待 3-5 个成块时间。

[112] 图 6 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 6，在硬件层面，该设备包括处理器 602、内部总线 604、网络接口 606、内存 608 以及非易失性存储器 610，当然还可能包括其他业务所需要的硬件。处理器 602 从非易失性存储器 610 中读取对应的计算机程序到内存 608 中然后运行，在逻辑层面上形成区块链交易装置。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定于各个逻辑单元，也可以是硬件或逻辑器件。

[113] 请参考图 7，本说明书还提供了一种基于区块链的汇款装置 70，应用于区块链的用户端设备，用户账户的账户余额至少被划分为一预备金余额和一备用余额；其中，所述用户账户包括一动态更新的预备金列表；所述预备金列表包括多个预备金金额；

[114] 所述装置 70 包括：

[115] 预备金金额分配单元 702，响应于用户发起的汇款操作，根据预备金列表创建单元 704 提供的当前的预备金列表为用户提交的汇款额分配对应的预备金金额；

[116] 汇款交易构建及发布单元 706，基于所述汇款额以及分配的所述预备金金额构建汇款交易，并将所述汇款交易发布至区块链，以在所述汇款交易被区块链中的节点设备验证通过后，从所述账户余额和所述预备金余额中均扣减所述汇款额；

[117] 其中，所述预备金列表创建单元 704 包括：

[118] 预备金列表生成模块 7042，获得当前的预备金余额，根据当前的预备金余额得到预备金列表；

[119] 预备金列表监测模块 7044，动态监测当前预备金列表中可用于分配的预备金金额是否低于预设阈值。

[120] 在一示出的实施例中，所述预备金列表生成模块 7042：

[121] 对当前预备金余额进行划分得到多个预备金金额，基于划分得到的多个预备金金额构建预备金列表创建交易；

[122] 将所述预备金列表创建交易发布至区块链，以在所述预备金列表创建交易被区块链中的节点设备验证通过后，在所述用户账户基于所述划分得到的多个预备金金额构建预备金列表。

[123] 在一示出的实施例中，所述预备金列表生成模块 7042：

[124] 对当前预备金余额进行划分得到多个预备金金额，基于划分得到的多个预备金金额构建预备金列表，并基于所述预备金列表构建预备金列表创建交易；

[125] 将所述预备金列表创建交易发布至区块链，以在所述预备金列表创建交易被区块链中的节点设备验证通过后，将所述预备金列表更新至所述用户账户中。

[126] 在一示出的实施例中，所述装置 70 还包括:

[127] 切换单元 708，在根据当前的预备金余额得到预备金列表之后，将切换前的预备金余额切换为备用余额。

[128] 在一示出的实施例中，所述备用余额为收款余额；其中，当其他用户发起对所述用户账户的汇款交易被区块链的节点设备验证通过后，该汇款交易中的汇款额将被增加至所述收款余额和所述账户余额。

[129] 在一示出的实施例中，所述用户账户的账户余额、所述预备金金额和所述汇款额均被预先进行了加密处理;

[130] 所述汇款交易还包括第一零知识证明，用以证明为所述汇款交易包括的预备金金额之和大于或等于所述汇款交易的汇款额;

[131] 所述预备金列表创建交易还包括第二零知识证明，用以证明基于切换后的预备金余额划分出的多个预备金金额之和小于或等于所述用户的账户余额。

[132] 在一示出的实施例中，所述用户账户的预备金余额和备用余额被预先进行了加密处理，所述第二零知识证明用以证明基于切换后的预备金余额划分出的多个预备金金额之和小于或等于所述切换后的预备金余额。

[133] 在一示出的实施例中，所述汇款交易还包括第三零知识证明，用以证明所述汇款额大于或等于零。

[134] 在一示出的实施例中，所述预备金列表创建交易还包括第四零知识证明，用以证明基于切换后的预备金余额划分出的多个预备金金额均大于或等于零。

[135] 上述装置中各个单元和模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，相关之处参见方法实施例的部分说明即可，在此不再赘述。

[136] 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。

[137] 与上述方法实施例相对应，本说明书的实施例还提供了一种计算机设备，该计算机设备包括存储器和处理器。其中，存储器上存储有能够由处理器运行的计算机程序;

处理器在运行存储的计算机程序时，执行本说明书实施例中基于区块链的汇款方法的各个步骤。对基于区块链的汇款方法的各个步骤的详细描述请参见之前的内容，不再重复。

[138] 与上述方法实施例相对应，本说明书的实施例还提供了一种计算机可读存储介质，该存储介质上存储有计算机程序，这些计算机程序在被处理器运行时，执行本说明书实施例中基于区块链的汇款方法的各个步骤。对基于区块链的汇款方法的各个步骤的详细描述请参见之前的内容，不再重复。

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

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

[141] 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。

[142] 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。

[143] 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、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，磁带磁磁盘存储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。

[144] 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。

[145] 本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。因此，本说明书的实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书的实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

权利要求书

1、一种基于区块链的汇款方法，应用于区块链的用户端设备，用户账户的账户余额至少被划分为一预备金余额和一备用余额；其中，所述用户账户包括一动态更新的预备金列表；所述预备金列表包括多个预备金金额；

所述方法包括：

响应于用户发起的汇款操作，根据当前的预备金列表为用户提交的汇款额分配对应的预备金金额；基于所述汇款额以及分配的所述预备金金额构建汇款交易，并将所述汇款交易发布至区块链，以在所述汇款交易被区块链中的节点设备验证通过后，从所述账户余额和所述预备金余额中均扣减所述汇款额；

其中，所述预备金列表的创建及更新过程包括：

步骤 A，获得当前的预备金余额，根据当前的预备金余额得到预备金列表；

步骤 B，动态监测当前预备金列表中可用于分配的预备金金额是否低于预设阈值，如果是则将当前的备用余额切换为预备金余额后，执行步骤 A。

2、根据权利要求 1 所述的方法，所述根据当前的预备金余额得到预备金列表，包括：

对当前预备金余额进行划分得到多个预备金金额，基于划分得到的多个预备金金额构建预备金列表创建交易；

将所述预备金列表创建交易发布至区块链，以在所述预备金列表创建交易被区块链中的节点设备验证通过后，在所述用户账户基于所述划分得到的多个预备金金额构建预备金列表。

3、根据权利要求 1 所述的方法，所述根据当前的预备金余额得到预备金列表，包括：

对当前预备金余额进行划分得到多个预备金金额，基于划分得到的多个预备金金额构建预备金列表，并基于所述预备金列表构建预备金列表创建交易；

将所述预备金列表创建交易发布至区块链，以在所述预备金列表创建交易被区块链中的节点设备验证通过后，将所述预备金列表更新至所述用户账户中。

4、根据权利要求 1 所述的方法，还包括：

在根据当前的预备金余额得到预备金列表之后，将切换前的预备金余额切换为备用余额。

5、根据权利要求 4 所述的方法，所述备用余额为收款余额；其中，当其他用户发起对所述用户账户的汇款交易被区块链的节点设备验证通过后，该汇款交易中的汇款额

将被增加至所述收款余额和所述账户余额。

6、根据权利要求 2 或 3 所述的方法，所述用户账户的账户余额、所述预备金金额和所述汇款额均被预先进行了加密处理；

所述汇款交易还包括第一零知识证明，用以证明为所述汇款交易包括的预备金金额之和大于或等于所述汇款交易的汇款额；

所述预备金列表创建交易还包括第二零知识证明，用以证明基于切换后的预备金余额划分出的多个预备金金额之和小于或等于所述用户的账户余额。

7、根据权利要求 2 或 3 所述的方法，所述用户账户的预备金余额和备用余额被预先进行了加密处理，第二零知识证明用以证明基于切换后的预备金余额划分出的多个预备金金额之和小于或等于所述切换后的预备金余额。

8、根据权利要求 6 所述的方法，所述汇款交易还包括第三零知识证明，用以证明所述汇款额大于或等于零。

9、根据权利要求 6 所述的方法，所述预备金列表创建交易还包括第四零知识证明，用以证明基于切换后的预备金余额划分出的多个预备金金额均大于或等于零。

10、一种基于区块链的汇款装置，应用于区块链的用户端设备，用户账户的账户余额至少被划分为一预备金余额和一备用余额；其中，所述用户账户包括一动态更新的预备金列表；所述预备金列表包括多个预备金金额；

所述装置包括：

预备金金额分配单元，响应于用户发起的汇款操作，根据预备金列表创建单元提供的当前的预备金列表为用户提交的汇款额分配对应的预备金金额；

汇款交易构建及发布单元，基于所述汇款额以及分配的所述预备金金额构建汇款交易，并将所述汇款交易发布至区块链，以在所述汇款交易被区块链中的节点设备验证通过后，从所述账户余额和所述预备金余额中均扣减所述汇款额；

其中，所述预备金列表创建单元包括：

预备金列表生成模块，获得当前的预备金余额，根据当前的预备金余额得到预备金列表；

预备金列表监测模块，动态监测当前预备金列表中可用于分配的预备金金额是否低于预设阈值。

11、根据权利要求 10 所述的装置，所述预备金列表生成模块：

对当前预备金余额进行划分得到多个预备金金额，基于划分得到的多个预备金金额构建预备金列表创建交易；

将所述预备金列表创建交易发布至区块链，以在所述预备金列表创建交易被区块链中的节点设备验证通过后，在所述用户账户基于所述划分得到的多个预备金金额构建预备金列表。

12、根据权利要求 10 所述的装置，所述预备金列表生成模块:

对当前预备金余额进行划分得到多个预备金金额，基于划分得到的多个预备金金额构建预备金列表，并基于所述预备金列表构建预备金列表创建交易;

将所述预备金列表创建交易发布至区块链，以在所述预备金列表创建交易被区块链中的节点设备验证通过后，将所述预备金列表更新至所述用户账户中。

13、根据权利要求 10 所述的装置，还包括:

切换单元，在根据当前的预备金余额得到预备金列表之后，将切换前的预备金余额切换为备用余额。

14、根据权利要求 13 所述的装置，所述备用余额为收款余额；其中，当其他用户发起对所述用户账户的汇款交易被区块链的节点设备验证通过后，该汇款交易中的汇款额将被增加至所述收款余额和所述账户余额。

15、根据权利要求 11 或 12 所述的装置，所述用户账户的账户余额、所述预备金金额和所述汇款额均被预先进行了加密处理;

所述汇款交易还包括第一零知识证明，用以证明为所述汇款交易包括的预备金金额之和大于或等于所述汇款交易的汇款额;

所述预备金列表创建交易还包括第二零知识证明，用以证明基于切换后的预备金余额划分出的多个预备金金额之和小于或等于所述用户的账户余额。

16、根据权利要求 11 或 12 所述的装置，所述用户账户的预备金余额和备用余额被预先进行了加密处理，第二零知识证明用以证明基于切换后的预备金余额划分出的多个预备金金额之和小于或等于所述切换后的预备金余额。

17、根据权利要求 15 所述的装置，所述汇款交易还包括第三零知识证明，用以证明所述汇款额大于或等于零。

18、根据权利要求 15 所述的装置，所述预备金列表创建交易还包括第四零知识证明，用以证明基于切换后的预备金余额划分出的多个预备金金额均大于或等于零。

19、一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求 1 到 9 任意一项所述的方法。

20、一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器

运行时，执行如权利要求 1 到 9 任意一项所述的方法。

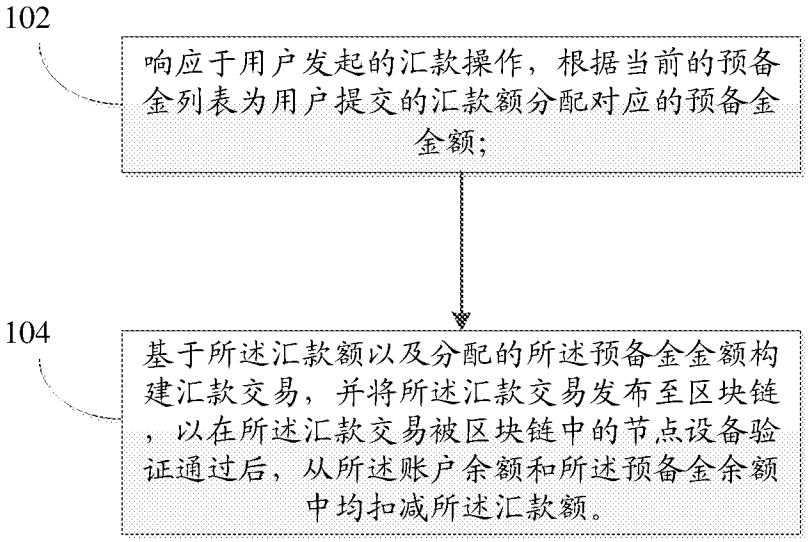

102
响应于用户发起的汇款操作，根据当前的预备金列表为用户提交的汇款额分配对应的预备金金额；
104
基于所述汇款额以及分配的所述预备金金额构建汇款交易，并将所述汇款交易发布至区块链，以在所述汇款交易被区块链中的节点设备验证通过后，从所述账户余额和所述预备金余额中均扣减所述汇款额。

图 1

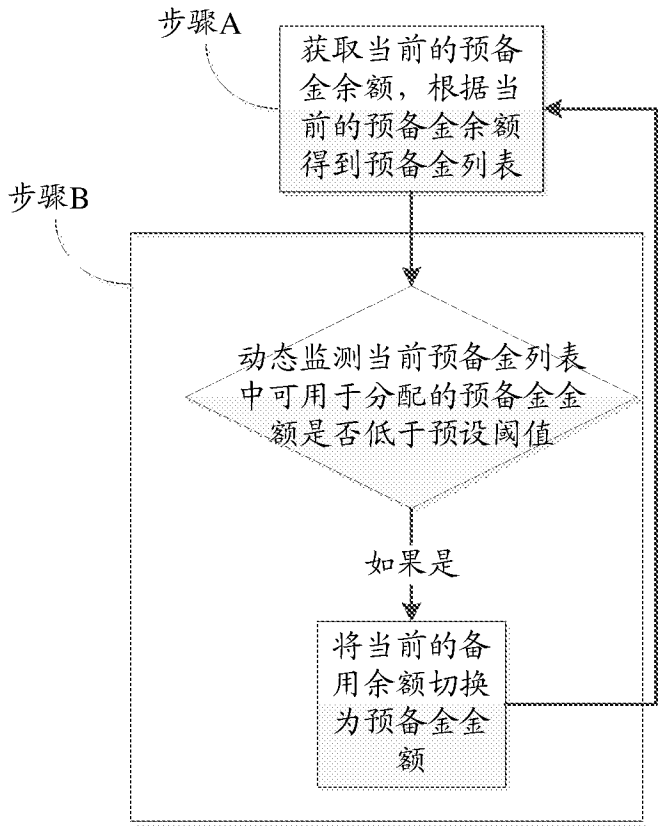

步骤A
获取当前的预备金余额，根据当前的预备金余额得到预备金列表
步骤B
动态监测当前预备金列表中可用于分配的预备金金额是否低于预设阈值
如果是
将当前的备用余额切换为预备金金额

图 2

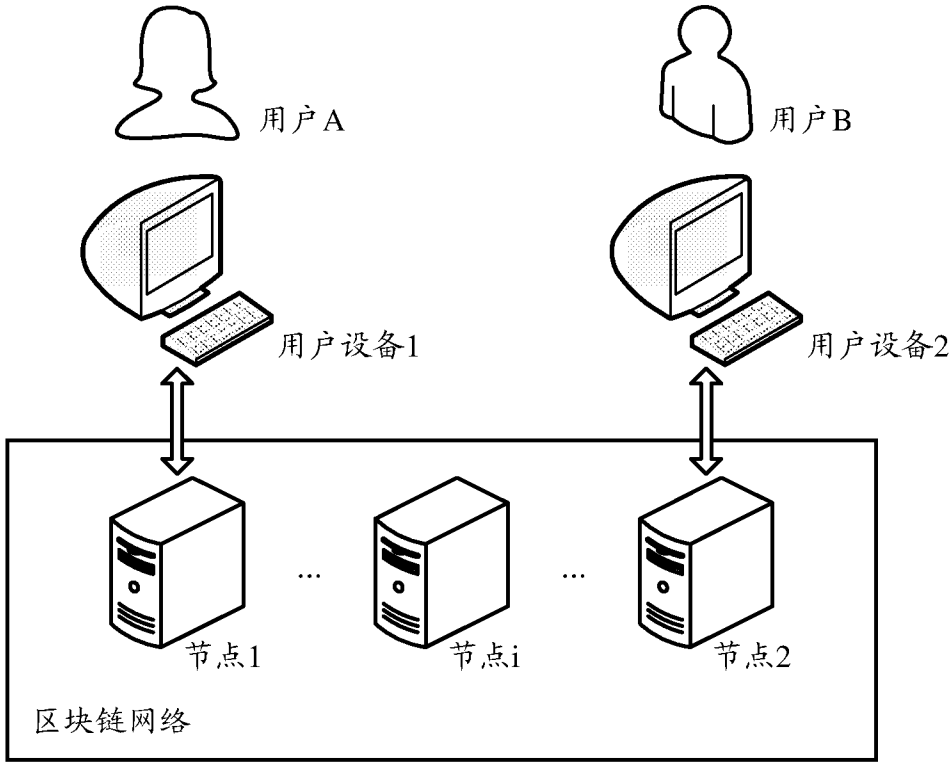


图 3

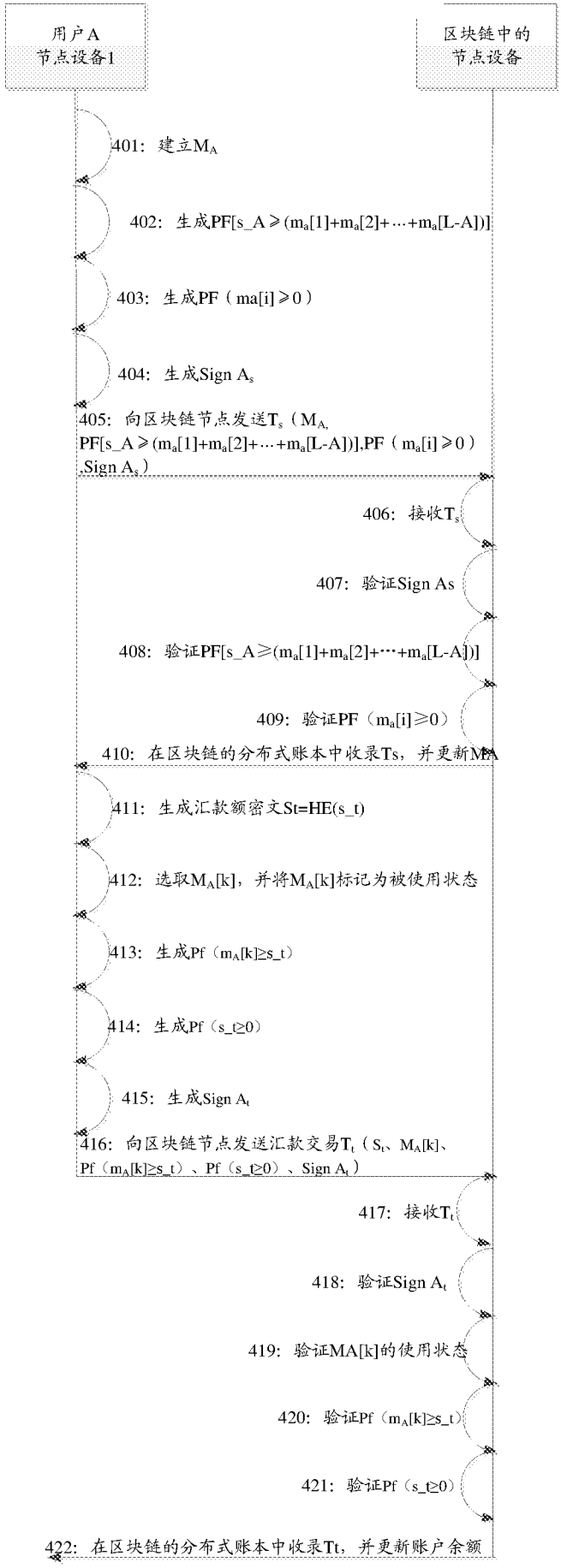

用户A
节点设备1
区块链中的
节点设备
401：建立M_A
402：生成PF[s_A⩾(m_a[1]+m_a[2]+…+m_a[L-A])]
403：生成PF（ma[i]⩾0）
404：生成Sign A_s
405：向区块链节点发送T_s（M_A,
PF[s_A⩾(m_a[1]+m_a[2]+…+m_a[L-A])],PF（m_a[i]⩾0）
,Sign A_s）
406：接收T_s
407：验证Sign As
408：验证PF[s_A⩾(m_a[1]+m_a[2]+…+m_a[L-A])]
409：验证PF（m_a[i]⩾0）
410：在区块链的分布式账本中收录Ts，并更新MA
411：生成汇款额密文St=HE(s_t)
412：选取M_A[k]，并将M_A[k]标记为被使用状态
413：生成Pf（m_A[k]≥s_t）
414：生成Pf（s_t≥0）
415：生成Sign A_t
416：向区块链节点发送汇款交易T_t（S_t、M_A[k]、
Pf（m_A[k]≥s_t）、Pf（s_t≥0）、Sign A_t）
417：接收T_t
418：验证Sign A_t
419：验证MA[k]的使用状态
420：验证Pf（m_A[k]≥s_t）
421：验证Pf（s_t≥0）
422：在区块链的分布式账本中收录Tt，并更新账户余额

图 4

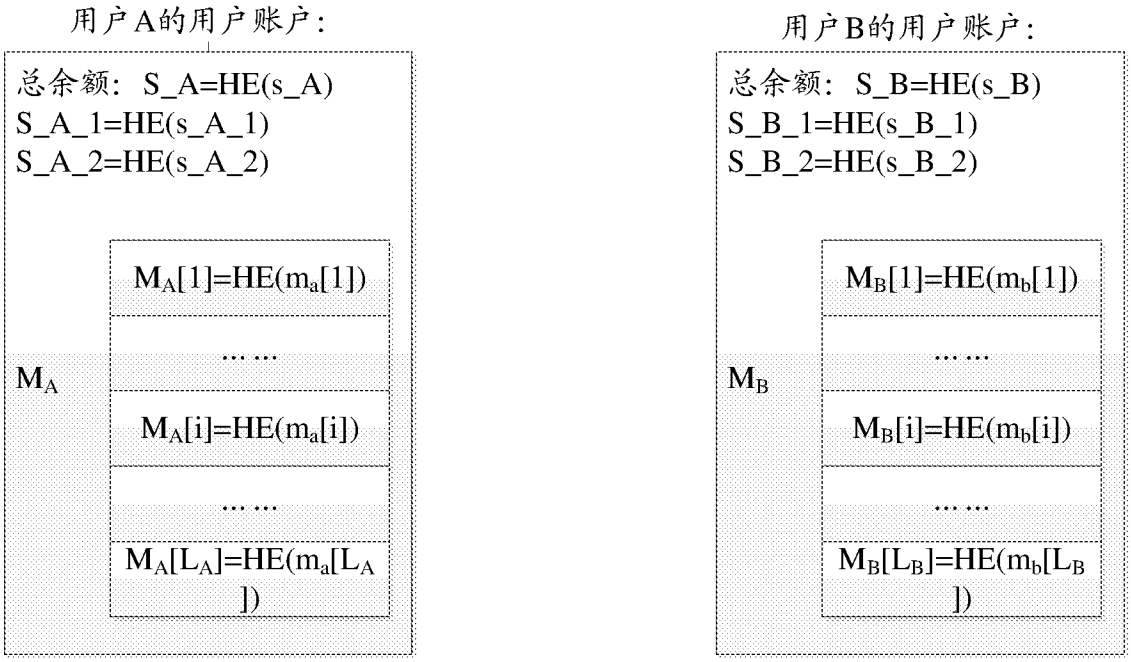

用户A的用户账户：
总余额：S_A=HE(s_A)
S_A_1=HE(s_A_1)
S_A_2=HE(s_A_2)
M_A
$M_A[1]=HE(m_a[1])$
……
$M_A[i]=HE(m_a[i])$
……
$M_A[L_A]=HE(m_a[L_A])$
用户B的用户账户：
总余额：S_B=HE(s_B)
S_B_1=HE(s_B_1)
S_B_2=HE(s_B_2)
M_B
$M_B[1]=HE(m_b[1])$
……
$M_B[i]=HE(m_b[i])$
……
$M_B[L_B]=HE(m_b[L_B])$

图 5

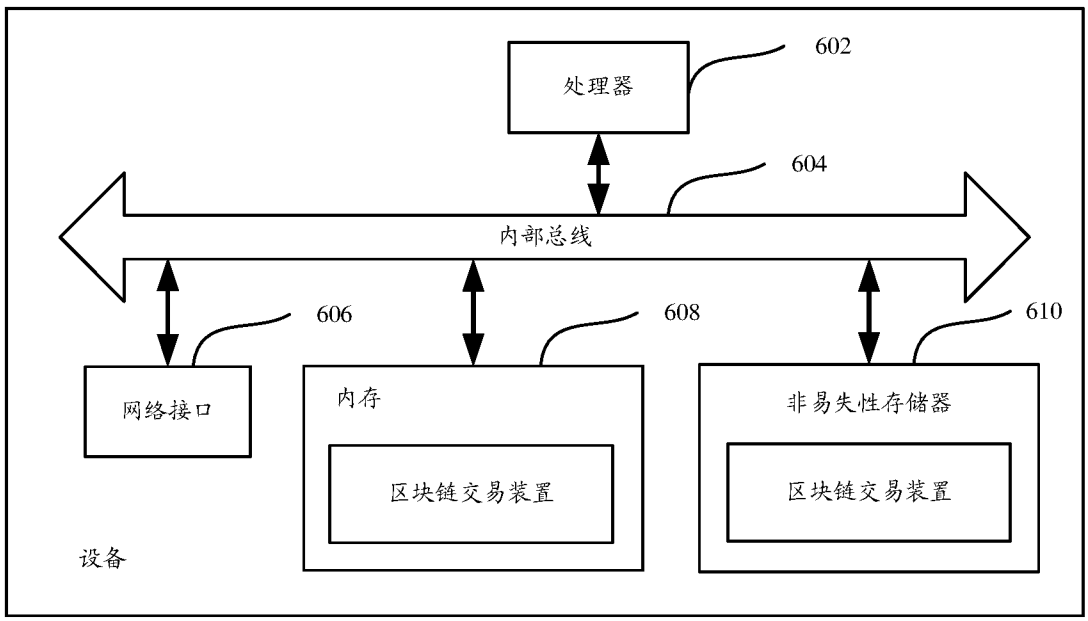

处理器
602
604
内部总线
606
608
610
网络接口
内存
区块链交易装置
非易失性存储器
区块链交易装置
设备

图 6

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/101938

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/10(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, EPODOC, CNPAT, CNKI, IEEE: 区块, 余额, 汇款, 交易, 账户, 预备, 备用, 保证, 并发, block, chain, balance, transaction, EOA, contract, preliminary, metal, account, reserve

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109508970 A (ALIBABA GROUP HOLDING LIMITED) 22 March 2019 (2019-03-22) claims 1-20	1-20
A	CN 108600301 A (QINGDAO MOYIKE BLOCKCHAIN CO., LTD.) 28 September 2018 (2018-09-28) description, paragraphs [0041]-[0054]	1-20
A	US 2017310653 A1 (SONY CORPORATION) 26 October 2017 (2017-10-26) entire document	1-20
A	CUI, Gaoying et al. "Application of Block Chain in Multi-level Demand Response Reliable Mechanism" *2017 3rd International Conference on Information Management,* 31 December 2017 (2017-12-31), pp. 337-341	1-20

☐ 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	Date of mailing of the international search report
25 October 2019	**20 November 2019**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/101938

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109508970 A	22 March 2019	None	
CN 108600301 A	28 September 2018	None	
US 2017310653 A1	26 October 2017	EP 3236403 A3	01 November 2017
		CN 107306183 A	31 October 2017
		EP 3236403 A2	25 October 2017

国际检索报告

国际申请号
PCT/CN2019/101938

A. 主题的分类

G06Q 20/10(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,EPODOC,CNPAT,CNKI,IEEE: 区块，余额，汇款，交易，账户，预备，备用，保证， 并发，block, chain, balance, transaction, EOA, contract, preliminary, metal, account, reserve

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 109508970 A (阿里巴巴集团控股有限公司) 2019年 3月 22日 (2019-03-22) 权利要求1-20	1-20
A	CN 108600301 A (青岛墨一客区块链有限公司) 2018年 9月 28日 (2018-09-28) 说明书第[0041]-[0054]段	1-20
A	US 2017310653 A1 (SONY CORPORATION) 2017年 10月 26日 (2017-10-26) 全文	1-20
A	CUI, Gaoying等. "Application of Block Chain in Multi-level Demand Response Reliable Mechanism" 2017 3rd International Conference on Information Management, 2017年 12月 31日 (2017-12-31), 第337-341页	1-20

☐ 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	国际检索报告邮寄日期
2019年 10月 25日	2019年 11月 20日

ISA/CN的名称和邮寄地址	受权官员
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	杨威明
传真号 (86-10)62019451	电话号码 86-10-53961571

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/101938

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	109508970	A	2019年 3月 22日	无			
CN	108600301	A	2018年 9月 28日	无			
US	2017310653	A1	2017年 10月 26日	EP	3236403	A3	2017年 11月 1日
				CN	107306183	A	2017年 10月 31日
				EP	3236403	A2	2017年 10月 25日