(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
2019 年 5 月 31 日 (31.05.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/100865 A1

(51) 国际专利分类号:
G06F 21/62 (2013.01)

(21) 国际申请号: PCT/CN2018/110034

(22) 国际申请日: 2018 年 10 月 12 日 (12.10.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201711183322.4 2017年11月23日 (23.11.2017) 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: 王虎森 (**WANG, Husen**); 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,

WO 2019/100865 A1

(54) **Title:** RESOURCE TRANSFER AND CAPITAL TRANSFER METHOD AND APPARATUS

(54) 发明名称: 资源转移和资金转移的方法和装置

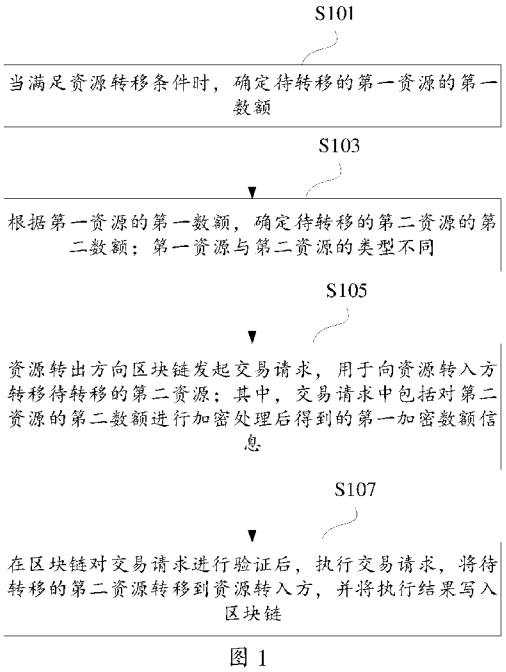

图 1

S101 When a resource transfer condition is satisfied, determine a first amount of a first resource to be transferred

S103 Determine, according to the first amount of the first resource, a second amount of a second resource to be transferred, wherein the type of the first resource is different from that of the second resource

S105. A resource transfer-out party initiates a transaction request to a block chain for transferring, to a resource transfer-in party, the second resource to be transferred, wherein the transaction request comprises first encrypted amount information obtained after encryption processing is carried out on the second amount of the second resource

S107. After the block chain verifies the transaction request, execute the transaction request, transfer, to the resource transfer-in party, the second resource to be transferred, and write an execution result into the block chain

(57) **Abstract:** Disclosed is a resource transfer method based on a block chain. The method comprises: when a resource transfer condition is satisfied, determining a first amount of a first resource to be transferred; determining, according to the first amount of the first resource, a second amount of a second resource to be transferred, wherein the type of the first resource is different from that of the second resource; a resource transfer-out party initiating a transaction request to a block chain for transferring, to a resource transfer-in party, the second resource to be transferred, wherein the transaction request comprises first encrypted amount information obtained

[见续页]

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))。

after encryption processing is carried out on the second amount of the second resource; and after the block chain verifies the transaction request, executing the transaction request, transferring, to the resource transfer-in party, the second resource to be transferred, and writing an execution result into the block chain. Privacy information of the two parties of the resource transfer can be protected during the process of transferring a resource.

(57) 摘要：本申请公开了一种基于区块链的资源转移方法，包括：当满足资源转移条件时，确定待转移的第一资源的第一数额；根据第一资源的第一数额，确定待转移的第二资源的第二数额，第一资源与第二资源的类型不同；资源转出方向区块链发起交易请求，用于向资源转入方转移待转移的第二资源，其中，交易请求中包括对第二资源的第二数额进行加密处理后得到的第一加密数额信息；在区块链对交易请求进行验证后，执行交易请求，将待转移的第二资源转移到资源转入方，并将执行结果写入区块链。从而能够在资源转移过程中能够保护资源转移双方的隐私信息。

资源转移和资金转移的方法和装置

技术领域

本申请涉及计算机技术领域，尤其涉及一种资源转移和资金转移的方法和系统。

背景技术

区块链技术（又称分布式账本技术）是一种特殊的分布式数据库技术，适合存储简单的、有先后关系的、能在系统内验证的数据，利用密码学和共识算法保证了数据的不可篡改和不可伪造。随着计算机和互联网技术的发展，区块链技术以其去中心化、公开透明、不可篡改、可信任等优点，备受青睐，在智能合约、证券交易、电子商务、物联网、社交通讯、文件存储、存在性证明、身份验证、股权众筹等众多领域得到广泛应用。

当将区块链技术应用于资源转移这类交易场景时，由于所有交易信息均需要发送到区块链系统进行验证、实施和上链，参与交易的资源转移双方的隐私信息，例如具体交易信息，所拥有资源的总额，个体隐私信息等都将面临泄露给与本次交易无关的第三方的风险。以将区块链技术应用于互联网银行的借贷业务中为例，借款方向出借方贷款的具体数额等交易信息均需要入链，从而对借贷双方的隐私信息构成威胁。

因此，亟需一种在资源转移过程中能够保护资源转移双方隐私信息的方案。

发明内容

本申请实施例提供一种资源转移方法、装置及对应的电子设备和计算机可读存储介质，目的在于在资源转移过程中能够保护资源转移双方的隐私信息。

本申请实施例还提供一种资金转移方法、装置及对应的电子设备和计

算机可读存储介质，目的在于在资金转移的过程中能够保护资金借贷双方的隐私信息。

本申请实施例采用下述技术方案:

第一方面，本申请实施例提供一种基于区块链的资源转移方法，包括:

当满足资源转移条件时，确定待转移的第一资源的第一数额;

根据所述第一资源的第一数额，确定待转移的第二资源的第二数额;所述第一资源与所述第二资源的类型不同;

资源转出方向区块链发起交易请求，用于向资源转入方转移所述待转移的第二资源;其中，所述交易请求中包括对所述第二资源的第二数额进行加密处理后得到的第一加密数额信息;

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的第二资源转移到所述资源转入方，并将执行结果写入所述区块链。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述交易请求中包括的所述第一加密数额信息，通过采用第一加密函数对所述第二资源的第二数额进行加密处理得到;

其中，所述第一加密函数的一个输入为所述第二资源的第二数额，另一个输入为所述资源转入方的公钥。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述交易请求中还包括所述资源转入方的公钥的标识信息。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述资源转入方的公钥的标识信息为所述资源转入方的公钥的哈希值。

优选地，在第一方面提供的基于区块链的资源转移方法中，根据所述第一资源的第一数额，确定待转移的第二资源的第二数额，包括:

根据所述第一资源的第一数额，采用单向函数确定所述第二资源的第二数额。

优选地，在第一方面提供的基于区块链的资源转移方法中，采用单向

函数确定所述第二资源的第二数额，包括:

将所述第一资源的第一数额和一随机数作为所述单向函数的输入，将所述单向函数的输出确定为所述第二资源的第二数额。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述资源转出方向区块链发起的所述交易请求中，还包括加密后的所述随机数。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述资源转移条件包括允许所述资源转入方借取所述第一资源；则确定待转移的第一资源的第一数额，包括:

将允许所述资源转入方借取的第一资源的额度，作为所述待转移的第一资源的第一数额。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述资源转移条件包括所述资源转出方已接收到所述资源转入方归还的第一资源；则确定待转移的第一资源的第一数额，包括:

将所述归还的第一资源的数额，确定为所述待转移的第一资源的第一数额。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述资源转移条件包括所述资源转入方与所述资源转出方已达成资源借取协议，所述资源借取协议中包含所述资源转出方向所述资源转入方申请借取的第一资源的数额；则确定待转移的第一资源的第一数额，包括:

将所述申请借取的第一资源的数额，确定为所述待转移的第一资源的第一数额。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述交易请求中还包括零知识证明，用于证明执行所述交易请求之后所述资源转出方将要持有的第二资源的余额与所述第二数额的和，等于所述资源转出方在发起所述交易请求前所持有的第二资源的数额。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述零知识证明还用于证明所述第二数额大于零，所述资源转出方在发起所述交易

请求前所持有的第二资源的数额大于零，并且，执行所述交易请求之后所述资源转出方将要持有的第二资源的余额不小于零。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述交易请求中还包括所述资源转出方参与的上一次资源转移交易的标识信息。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述资源转出方参与的上一次资源转移交易的标识信息，具体为所述区块链中记录的、所述上一次资源转移交易的哈希值。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述交易请求中还包括对执行所述交易请求之后所述资源转出方将要持有的第二资源的余额进行加密处理后得到的第二加密数额信息。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述交易请求中包括的所述第二加密数额信息，通过采用第二加密函数对执行所述交易请求之后所述资源转出方将要持有的第二资源的余额进行加密处理得到；

其中，所述第二加密函数的一个输入为所述第二资源的余额，另一个输入为所述资源转出方的公钥。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述交易请求中还包括所述资源转出方的公钥的标识信息。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述资源转出方的公钥的标识信息为所述资源转出方的公钥的哈希值。

优选地，在第一方面提供的基于区块链的资源转移方法中，所述第一资源具体为资金，所述第二资源具体为代币。

第二方面，本申请实施例还提供了一种基于区块链的资金转移方法，包括：

当满足转移条件时，确定待转移的资金的第一数额；

根据所述资金的第一数额，确定待转移的代币的第二数额；所述资金与所述代币的类型不同；

转出方向区块链发起交易请求，用于向转入方转移所述待转移的代币；其中，所述交易请求中包括对所述代币的第二数额进行加密处理后得到的第一加密数额信息；

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的代币转移到所述转入方，并将执行结果写入所述区块链。

第三方面，本申请实施例提供了一种基于区块链的资源转移装置，包括：

第一数额确定模块，当满足资源转移条件时，确定待转移的第一资源的第一数额；

第二数额确定模块，根据所述第一资源的第一数额，确定待转移的第二资源的第二数额；所述第一资源与所述第二资源的类型不同；

交易请求发起模块，资源转出方向区块链发起交易请求，用于向资源转入方转移所述待转移的第二资源；其中，所述交易请求中包括对所述第二资源的第二数额进行加密处理后得到的第一加密数额信息；

入链模块，在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的第二资源转移到所述资源转入方，并将执行结果写入所述区块链。

第四方面，本申请实施例还提供一种电子设备，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

当满足资源转移条件时，确定待转移的第一资源的第一数额；

根据所述第一资源的第一数额，确定待转移的第二资源的第二数额；所述第一资源与所述第二资源的类型不同；

资源转出方向区块链发起交易请求，用于向资源转入方转移所述待转移的第二资源；其中，所述交易请求中包括对所述第二资源的第二数额进行加密处理后得到的第一加密数额信息；

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的第二资源转移到所述资源转入方，并将执行结果写入所述区块链。

第五方面，本申请实施例还提供一种计算机可读存储介质，所述计算机可读存储介质存储一个或多个程序，所述一个或多个程序包括指令，所述指令当被包括多个应用程序的电子设备执行时，能够使所述电子设备执行以下操作:

当满足资源转移条件时，确定待转移的第一资源的第一数额;

根据所述第一资源的第一数额，确定待转移的第二资源的第二数额;所述第一资源与所述第二资源的类型不同;

资源转出方向区块链发起交易请求，用于向资源转入方转移所述待转移的第二资源;其中，所述交易请求中包括对所述第二资源的第二数额进行加密处理后得到的第一加密数额信息;

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的第二资源转移到所述资源转入方，并将执行结果写入所述区块链。

第六方面，本申请实施例提供一种基于区块链的资金转移装置，包括:

资金数额确定模块，当满足转移条件时，确定待转移的资金的第一数额;

代币数额确定模块，根据所述资金的第一数额，确定待转移的代币的第二数额;所述资金与所述代币的类型不同;

交易请求发起模块，转出方向区块链发起交易请求，用于向转入方转移所述待转移的代币;其中，所述交易请求中包括对所述代币的第二数额进行加密处理后得到的第一加密数额信息;

入链模块，在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的代币转移到所述转入方，并将执行结果写入所述区块链。

第七方面，本申请实施例提供一种电子设备，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

当满足转移条件时，确定待转移的资金的第一数额；

根据所述资金的第一数额，确定待转移的代币的第二数额；所述资金与所述代币的类型不同；

转出方向区块链发起交易请求，用于向转入方转移所述待转移的代币；其中，所述交易请求中包括对所述代币的第二数额进行加密处理后得到的第一加密数额信息；

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的代币转移到所述转入方，并将执行结果写入所述区块链。

第八方面，本申请实施例提供一种计算机可读存储介质，所述计算机可读存储介质存储一个或多个程序，所述一个或多个程序包括指令，所述指令当被包括多个应用程序的电子设备执行时，能够使所述电子设备执行以下操作：

当满足转移条件时，确定待转移的资金的第一数额；

根据所述资金的第一数额，确定待转移的代币的第二数额；所述资金与所述代币的类型不同；

转出方向区块链发起交易请求，用于向转入方转移所述待转移的代币；其中，所述交易请求中包括对所述代币的第二数额进行加密处理后得到的第一加密数额信息；

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的代币转移到所述转入方，并将执行结果写入所述区块链。

第九方面，本申请实施例提供一种基于区块链的资源转移方法，包括：

当满足资源转移条件时，确定待转移的第一资源的第一数额；

根据所述第一资源的第一数额，采用单向函数确定待转移的第二资源

的第二数额；所述第一资源与所述第二资源的类型不同；

资源转出方向区块链发起交易请求，用于向资源转入方转移所述待转移的第二资源；其中，所述交易请求中包括与所述第二资源的第二数额相对应的信息；

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的第二资源转移到所述资源转入方，并将执行结果写入所述区块链。

优选地，在第九方面提供的基于区块链的资源转移方法中，根据所述第一资源的第一数额，采用单向函数确定待转移的第二资源的第二数额，包括：

将所述第一资源的第一数额和一随机数作为所述单向函数的输入，将所述单向函数的输出确定为所述第二资源的第二数额。

优选地，在第九方面提供的基于区块链的资源转移方法中，所述资源转出方向区块链发起的所述交易请求中，还包括加密后的所述随机数。

优选地，在第九方面提供的基于区块链的资源转移方法中，所述第一资源具体为资金，所述第二资源具体为代币。

第十方面，本申请实施例提供一种基于区块链的资金转移方法，包括：

当满足转移条件时，确定待转移的资金的第一数额；

根据所述资金的第一数额，采用单向函数确定待转移的代币的第二数额；所述资金与所述代币的类型不同；

转出方向区块链发起交易请求，用于向转入方转移所述待转移的代币；其中，所述交易请求中包括与所述代币的第二数额相对应的信息；

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的代币转移到所述转入方，并将执行结果写入所述区块链。

本申请实施例采用的上述至少一个技术方案能够达到以下有益效果：

本申请实施例提供的技术方案，在满足资源转移条件时，确定待转移的第一资源的第一数额，并在此基础上，将第一资源的第一数额转换为资

源类型不同的第二资源的第二数额，进而发起用于转移第二数额的交易请求，并通过对第二数额进行加密处理得到加密数额信息（也就是加密后的第二数额），从而在区块链针对该交易请求进行验证、实施和上链时，可以通过对第二数额进行加密处理的方式隐藏资源转出方与资源转入方之间的具体交易信息，具体表现为待转移的第一资源的第一数额的信息，从而能够在资源转移过程中保护资源转移双方的隐私信息。

附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

图 1 为本申请实施例提供的一种资源转移方法的流程示意图；

图 2 为本申请实施例提供的一种资金转移方法的流程示意图；

图 3 为本申请实施例提供的资金转移方法在资金借贷场景下发放代币阶段的业务流程示意图；

图 4 为本申请实施例提供的资金转移方法在资金借贷场景下申请贷款阶段的业务流程示意图；

图 5 为本申请实施例提供的资金转移方法在资金借贷场景下还款阶段的业务流程示意图；

图 6 为本申请实施例提供的另一种资源转移方法的流程示意图；

图 7 为本申请实施例提供的另一种资金转移方法的流程示意图；

图 8 为本申请实施例提供的一种资源转移装置的结构示意图；

图 9 为本申请实施例提供的一种电子设备的结构示意图；

图 10 为本申请实施例提供的一种资金转移装置的结构示意图；

图 11 为本申请实施例提供的又一种电子设备的结构示意图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

本申请中所称的资源，可以具体化为数据资源、资金资源等可以在多方之间转移的资源类型。在基于区块链技术构建的资源管理平台上，资源持有者之间可以在满足资源转移条件时进行资源的转移。具体的，可以在确定待转移的资源的数额后，由资源转出方向区块链发起交易请求；区块链对交易请求进行验证、实施，资源转出方将待转移的资源转移到资源转入方后，区块链将该交易请求的执行结果写入区块链。为解决交易入链后对资源转移双方的隐私信息构成威胁的问题，本申请实施例提供了基于区块链的资源转移方法。以下将结合附图，详细说明本申请各实施例提供的技术方案。

参见图 1 所示，一种基于区块链的资源转移方法，适用于资源转出方，具体包括:

S101: 当满足资源转移条件时，确定待转移的第一资源的第一数额。

可以理解到，当满足资源转移条件，需要进行资源转移之前，资源转出方需要确定待转移的资源的类型及其数额，也就是待转移的第一资源的第一数额。除此之外，资源转出方也要确定出该次资源转移的对象，即接收被转移的资源的资源转入方。

需要说明的是，在不同的应用场景下，出于不同的业务目的，资源转移条件也会不同，具体的资源转移条件可以根据资源转移双方的约定或者资源转移所依托的业务平台的业务流程设置确定。更进一步地，在资源转移所依托的业务平台上，根据实际业务流程的需要，可能会需要进行多次资源转移，以实现业务流程中不同阶段的不同目的。出于不同目的进行的资源转移，转移的资源的类型、数额以及参与资源转移的资源转出方和资

源转入方也都可能不同，资源转出方为实现资源的转移而发起的交易请求的内容和格式也都可能不同。后文将针对多种不同的情况展开举例说明。

S103：根据第一资源的第一数额，确定待转移的第二资源的第二数额；第一资源与第二资源的类型不同。

需要说明的是，第一资源和第二资源的类型并不相同。执行步骤S103，将第一资源转换为第二资源，相对应地，资源的数额也从第一资源的第一数额转换为第二资源的第二数额。因此，在进一步进行资源转移时，可以将对第一资源的转移转换为对第二资源的转移。第一资源和第二资源的关系，可以理解为，第一资源为资源转移双方实质上需要转移的资源类型（例如，在借贷场景下，第一资源可以具体化为资金，对应到真实的货币），而第二资源为资源转移时实际转移的资源类型（例如，在借贷场景下，第二资源可以具体化为代币，是一种虚拟的货币）。从保护资源转移双方的隐私信息的角度，也可以认为第二资源是第一资源的保护外壳，本申请实施例在进行资源转移时，将在实际业务中有实质价值的第一资源转换为显性的、可以没有实质价值的第二资源进行转换，因此，即使被实际转移的第二资源的第二数额的相关信息被写入区块链，具有实际价值的第一资源的第一数额的信息仍然被隐藏，从而有利于保护资源转移这一交易的隐私。

还需要说明的是，第一资源和第二资源之间，除了类型不同之外，两种资源的数额之间还存在对应关系，或者说数额的转换关系，具体的转换关系可以根据业务平台的需要进行设置。

例如，第一资源和第二资源的数额可以直接相等，即二者1:1的进行转换。这种情况下，虽然资源转移双方之外的第三方可能通过第二资源的第二数额能够推知第一资源的第一数额，但是，由于本申请实施例在后续步骤发起的交易请求中，并非直接携带第二数额的信息，而是对第二数额进行加密处理，在交易请求中携带加密处理后得到的第一加密数额信息。因此，仍然可以保护资源转移的实质数额的信息，从而保护交易隐私。

又例如，第一资源和第二资源的数额可以按照预设的转换系数或者函

数关系进行转换，通过保护这种转换系数或者函数关系，也能够对资源转移的实质数额（也就是第一资源的第一数额）进行保护。可以理解到，参与资源转移的双方需要知晓这种转换系数或者函数关系，以便实现资源类型的反向转换（即由第二类型的第二数额转换为第一类型的第一数额），从而达到资源转移的最终目的。

更进一步地，第一资源和第二资源的数额优选通过单向函数实现转换，也就是说，根据第一资源的第一数额，采用单向函数确定第二资源的第二数额。具体地，可以将第一资源的第一数额和一随机数作为单向函数的输入，将单向函数的输出确定为第二资源的第二数额。采用这种方式，利用单向函数的特性，即使在后续发起的交易请求中不对第二数额进行加密处理，而是直接将通过单向函数转换得到的第二数额放入交易请求中，也能在一定程度上保护资源转移的实质数额（也就是第一资源的第一数额）。当然，在此基础上，对第二数额进行进一步的加密处理以得到第一加密数额信息，并将第一加密数额信息携带在资源转出方发起的交易请求中，能够更好的保护资源转移交易的隐私信息。

在采用单向函数实现第一资源与第二资源间的数额转换时，资源转出方还需要将进行转换时使用的随机数（作为单向函数的一个输入）发送给资源转入方，以便资源转入方进行资源类型的反向转换，推知第一资源的第一数额。在具体实施时，可以在资源转出方向区块链发起交易请求之前，对这一随机数进行加密，进而发起的交易请求中携带的为加密后的随机数，从而避免了随机数的泄密，进而保护了资源转移交易的隐私信息。具体地，可以借助资源转入方的公钥对随机数进行加密，从而只有资源转入方的私钥才能对该随机数进行解密，进而利用该随机数实现资源类型的反向转换，也就是从第二资源的第二数额推知第一资源的第一数额。

S105：资源转出方向区块链发起交易请求，用于向资源转入方转移待转移的第二资源；其中，交易请求中包括对第二资源的第二数额进行加密处理后得到的第一加密数额信息。

本申请实施例中，执行步骤S105之前，可以还包括对第二资源的第二数额进行加密处理，得到第一加密数额信息的步骤。无论第一资源与第二资源之间的转换关系是否能够被资源转移双方以外的第三方知晓，只要对第二数额的信息进行加密处理，就能够保护资源转移交易的具体数额信息，从而保护资源转移双方的隐私。

需要说明的是，交易请求中包括的第一加密数额信息，可以通过采用第一加密函数（记为enc(x,y)）对第二资源的第二数额进行加密处理得到。其中，第一加密函数的一个输入为第二资源的第二数额（记为 quota_c），另一个输入为资源转入方的公钥（记为pk_c）。可以理解到，若资源转入方的公钥为非对称密钥，则该第一加密函数为非对称加密函数；若资源转入方的公钥为对称密钥，则该第一加密函数为对称加密函数。

可选的，还可以将资源转入方的公钥的标识信息作为交易请求的一部分发送到区块链系统，供区块链系统在验证、实施后上链。具体地，可以采用资源转入方的公钥的哈希值（记为hash(pk_c)）作为公钥的标识信息。

此时，资源转出方发起的交易请求TX的交易格式可表示为：

TX=(enc(pk_c, quota_c), hash(pk_c))

需要说明的是，在不同的应用场景下，基于不同的资源转移条件和目的，交易请求中携带的信息将有所不同。后续将详细举例说明。

S107：在区块链对交易请求进行验证后，执行交易请求，将待转移的第二资源转移到资源转入方，并将执行结果写入区块链。

需要说明的是，区块链系统接收到资源转出方发起的交易请求后，区块链的各节点将对交易请求进行验证。当达成共识，交易请求验证通过后，资源转出方进一步执行该交易请求，将待转移的第二资源转移到资源转入方。可以理解到，被转移的第二资源的数额为第二数额。资源转移结束后，将该交易请求的执行结果写入区块链。

还需要说明的是，区块链系统的各节点对交易请求进行验证时，主要验证交易请求的格式是否符合约定（例如交易请求中的字段个数，各字段

的长度，某字段的内容等），而对于交易请求中携带的加密信息，例如第一加密数额信息，单向函数中加密后的随机数等信息，将直接验证通过，进而执行交易请求。

可以理解到，当区块链中的节点对资源转出方的交易请求验证通过后，资源转出方会将第二资源（数额为第二数额）转移到资源转入方。资源转入方接收到转移来的第二资源后，可以根据第一资源与第二资源的转换关系，确定本次资源转移交易实质转移的第一资源的数额是否为第一数额。

采用本申请实施例提供的技术方案，在满足资源转移条件时，确定待转移的第一资源的第一数额，并在此基础上，将第一资源的第一数额转换为资源类型不同的第二资源的第二数额，进而发起用于转移第二数额的交易请求，并通过对第二数额进行加密处理得到加密数额信息（也就是加密后的第二数额），从而在区块链针对该交易请求进行验证、实施和上链时，可以通过对第二数额进行加密处理的方式隐藏资源转出方与资源转入方之间的具体交易信息，具体表现为待转移的第一资源的第一数额的信息，从而能够在资源转移过程中保护资源转移双方的隐私信息。

在本申请实施例中，在进行资源转移时首要保护的就是具体的交易数额信息，也就是待转移的第一资源的第一数额。在不同的应用场景下，资源转移条件也有所不同，确定出待转移的第一资源的第一数额的方式、以及确定出的第一数额也不尽相同。以下将举例说明。

（1）当资源转移条件为允许资源转入方借取第一资源时，可以理解为资源转出方或业务系统中约定的其他参与方已经对资源转入方借取第一资源的资格和能力进行了审查，并确定了允许资源转入方借取的第一资源的额度。此时，资源转出方向资源转入方转移资源的目的，可以理解为业务系统批准资源转入方进行第一资源的借取，并向资源转入方发放允许借取第一资源的数额的凭证。在此场景下，资源转出方为业务系统中约定的发放额度凭证的业务参与方，资源转入方为被允许借取第一资源的业务参与方。还可以理解到，在完成本次资源转移之后，资源转入方所持有的第二

资源的数额，反映的就是资源转入方能够借取的资源的额度。

因而，此时在确定待转移的第一资源的第一数额时，可将允许资源转入方借取的第一资源的额度，作为待转移的第一资源的第一数额。在此基础上根据第一资源的第一数额确定出的第二资源的第二数额，也能反映允许资源转入方借取资源的额度。因此，资源转出方发起的转移第二资源的交易请求中，包含的第一加密数额信息（该信息通过对第二数额进行加密处理后得到）也能反映允许资源转入方借取第一资源的数额，该第一加密数额信息也就是向资源转入方发放的、允许借取第一资源的凭证。由于该第一加密数额信息对于资源转移双方之外的第三方而言是密文数据（无法知晓第二资源的第二数额），因此，这种方式能够保护资源转入方被批准借取第一资源的额度这一隐私信息，达到本申请实施例的技术目的。

还需要说明的是，将业务系统批准资源转入方进行第一资源的借取后向资源转入方发放额度凭证的这一交易请求写入区块链，有利于监管和限制资源转入方借取第一资源的数额不超过允许的额度，进而保护借出资源的一方的利益。

（2）当资源转移条件为资源转出方已接收到资源转入方归还的第一资源时，可以理解为，在实际业务流程中，资源转入方为第一资源的借入方，资源转出方为第一资源的借出方。资源转入方将需归还的第一资源转移到资源转出方，以归还向资源转出方借取的第一资源，这一过程并不写入区块链；当资源转出方接收到资源转入方在链下归还的第一资源后，资源转出方执行本申请实施例的资源转移方法，将与归还的第一资源的数额相对应的第二资源转移到资源转入方。此时，进行资源转移的目的在于，在资源转入方将借取的资源归还后，为其恢复额度或者补足额度。

因而，此时在确定待转移的第一资源的第一数额时，可以将归还的第一资源的数额，确定为待转移的第一资源的第一数额。进行资源转移时，将数额与第一资源的第一数额相对应的第二资源转移到资源转入方，以便恢复其借取资源的额度。可以理解到，在完成本次资源转移之后，资源转

入方所持有的第二资源的数额，反映的就是资源转入方能够借取的资源的剩余额度。

在资源转出方发起交易请求时，将依据第一资源的第一数额确定出的第二资源的第二数额进行加密处理，可以保护资源转入方实际归还的资源的数额这一隐私数据，达到本申请的技术目的。

还需要说明的是，在资源借取方归还第一资源后，向资源借取方转移对应数额的第二资源，并将转移第二资源的交易写入区块链，一方面为资源借取方恢复额度或者补足额度，以便保障资源借取方的正常交易，另一方面有利于监管和限制资源借取方借取资源的数额，从而保护资源借出方的利益。

（3）当资源转移条件为资源转入方与资源转出方已达成资源借取协议时，资源借取协议中包含资源转出方向资源转入方申请借取的第一资源的数额。对应到实际业务流程中，该场景下的资源转出方为第一资源的借取方，资源转入方为第一资源的借出方。在双方达成资源借取协议后，借取方（对应到此场景下的资源转出方）将自己所持有的第二资源中对申请借取的第一资源的数额相对应的部分转移到借出方（对应到此场景下的资源转入方），这一过程写入区块链；借出方在收到被转移的第二资源后，进一步将资源借取协议中约定的应借给借入方的第一资源转移给借取方，这一过程无需写入区块链，在链下采用常规业务手段实施即可。

在此场景下，借取方（资源转出方）将自己所持有的第二资源中与申请借取的第一资源的数额相对应的部分转移到借出方（资源转入方），进行这一资源转移并将资源转移的交易写入区块链的目的，可以理解为，一方面，资源转出方向资源转入方证明自己借取资源的额度（体现为在资源转移前，资源转出方所持有的第二资源的数额）满足本次申请借取的资源的数额要求，以便资源转出方能够向资源转入方借取具有实际价值的第一资源；另一方面，资源转出方在转移出对应数额的第二资源后，自己所持有的第二资源的数额将相应减少，也就相当于扣减了允许资源转出方借取资

源的额度，将这一额度被扣减的交易写入区块链，有利于监管和限制资源借取方借取资源的数额，从而保护资源借出方的利益。

在这一场景下，可以将资源借取协议中申请借取的第一资源的数额，确定为待转移的第一资源的第一数额，进而在此基础上确定待转移的第二资源的第二数额，以便进行第二资源的转移。

可以理解到，在上述举例的第（3）类场景下，申请借取第一资源的资源借取方（在本次资源转移过程中充当资源转出方）的额度需要受到限制，因此，为了实现资源转移，资源转出方需要向区块链上除参与本次资源转移交易的节点（资源转出方和资源转入方所对应的节点）之外的节点，证明本次资源转移交易的合法性。

优选地，可以在资源转出方发起的交易请求中加入零知识证明，用于证明执行交易请求之后资源转出方将要持有的第二资源的余额与第二数额的和，等于资源转出方在发起交易请求前所持有的第二资源的数额。利用零知识证明，资源转出方就可以在不暴露任何具体信息（包括资源转移的数额等）的情况下，向区块链上的各节点证明相关内容的真实性，具体的，可以理解为证明上述“执行交易请求之后资源转出方将要持有的第二资源的余额与第二数额的和，等于资源转出方在发起交易请求前所持有的第二资源的数额”这一论断为真。

具体地，将资源转出方将要持有的第二资源的余额记为 quota_c’，将待转移的第二资源的第二数额记为 quota_d，将资源转出方在发起交易请求前所持有的第二资源的数额记为 quota_c，则上述零知识证明函数 proof(x)可表达为 proof(quota_c’=(quota_c-quota_d))。该零知识证明函数证明的就是：等式(quota_c’=(quota_c- quota_d))确实成立。

在此基础上，资源转出方向区块链发起的交易请求 TX，其交易格式可以表示为：

Tx=(enc(pk_d, quota_d),hash(pk_d), proof((quota_c- quota_d- quota_c’==0)))

进一步地，资源转出方还可以利用零知识证明向区块链中的各节点证明以下事项：资源转出方转出的第二资源的数额，即第二数额 quota_d 大于零，资源转出方在发起交易请求前所持有的第二资源的数额 quota_c 大于零，并且，执行交易请求之后资源转出方将要持有的第二资源的余额 quota_c'不小于零。从而，该零知识证明函数可以表达为：

proof((quota_c- quota_d- quota_c' ==0)&& (quota_c>0) && (quota_d>0) && (quota_c' ⩾0))

此时，资源转出方向区块链发起的交易请求 TX，其交易格式可以表示为：

Tx=(enc(pk_d, quota_d),hash(pk_d), proof((quota_c- quota_d- quota_c' ==0)&& (quota_c>0) && (quota_d>0) && (quota_c' ⩾0)))

进一步优选地，交易请求中还可以包括资源转出方参与的上一次资源转移交易的标识信息（可记为 Tx_in），可具体取为区块链中记录的、上一次资源转移交易的哈希值。需要说明的是，资源转出方参与的上一次资源转移交易，可以是借取资源的交易，也可以是确认借取额度的交易，还可以是归还资源后增补额度的交易。将资源转出方参与的上一次资源转移交易的标识信息发送到区块链中进行验证，有利于保证资源转出方（作为资源借取方）所持第二资源数额变化的连贯性。此时，资源转出方向区块链发起的交易请求 TX，其交易格式可以表示为：

Tx=(Tx_in, (enc(pk_d, quota_d), hash(pk_d)), proof((quota_c-quota_d-quota_c' ==0)&& (quota_c>0) && (quota_d>0) && (quota_c' >0)))

进一步优选地，交易请求中还可包括对执行交易请求之后资源转出方将要持有的第二资源的余额（记为 quota_c'）进行加密处理后得到的第二加密数额信息。具体地，可通过采用第二加密函数（记为 enc(x, y)）对执行交易请求之后资源转出方将要持有的第二资源的余额 quota_c'进行加密处理。其中，第二加密函数的一个输入为第二资源的余额（记为 quota_c'），另一个输入为资源转出方的公钥（记为 pk_c）。可以理解到，若资源转出方的公

钥为非对称密钥，则该第二加密函数为非对称加密函数；若资源转出方的公钥为对称密钥，则该第二加密函数为对称加密函数。

可选的，还可以将资源转出方的公钥的标识信息作为交易请求的一部分发送到区块链系统，供区块链系统在验证、实施后上链。具体地，可以采用资源转出方的公钥的哈希值（记为 hash(pk_c)）作为公钥的标识信息。则此时，资源转出方发起的交易请求 TX 的交易格式可表示为:

Tx=(Tx_in, (enc(pk_d, quota_d), hash(pk_d)), (enc(pk_c, quota_c’), hash(pk_c)), proof((quota_c- quota_d- quota_c’ ==0)&& (quota_c>0) && (quota_d>0) && (quota_c’ >0)))

以上从多个角度对本申请实施例提供的资源转移方法在不同场景下、基于不同目的进行资源转移时的具体实现进行了举例说明。在不同的资源转移条件下，进行资源转移的目的不同，参与资源转移方在业务流程中的角色不同。无论出于何种目的进行资源转移，在向区块链发起用于转移第二数额的交易请求时，都可以通过对第二数额进行加密处理的方式隐藏资源转出方与资源转入方之间的具体交易信息，具体表现为待转移的第一资源的第一数额的信息，从而能够在资源转移过程中保护资源转移双方的隐私信息。

在一种场景下，第一资源具体化为资金，第二资源具体化为代币。这一场景下涉及到基于区块链的资金转移方法，参见图 2 所示，包括:

S201: 当满足转移条件时，确定待转移的资金的第一数额;

S203: 根据资金的第一数额，确定待转移的代币的第二数额；资金与代币的类型不同;

S205: 转出方向区块链发起交易请求，用于向转入方转移待转移的代币；其中，交易请求中包括对代币的第二数额进行加密处理后得到的第一加密数额信息;

S207: 在区块链对交易请求进行验证后，执行交易请求，将待转移的代币转移到转入方，并将执行结果写入区块链。

可以理解到，上述基于区块链的资金转移方法在具体实施上的各方面，与前述实施例的基于区块链的资源转移方法相同，因此，前述实施例中关于资源转移方法的阐释与说明均适用于此资金借贷场景下的资源借贷方法。以下将主要以资金借贷的业务流程为例，说明本实施例的具体实施。

在资金借贷这一应用场景下，业务流程可以包括信用评估和代币发放阶段、贷款申请和发放阶段、以及还款阶段等。

（一）信用评估和代币发放阶段

在进行信用评估时，可以预先确定一个特定机构 A，对用户的信用等级进行评估，并就用户的贷款发放额度给出具有公信力的结论。可以理解到，这一特定机构 A 的确定，可以通过资金监管部门按照相关规定审核和指定，也可以由参与放贷的机构进行推举或约定产生。该特定机构 A 的职能主要在于根据用户的相关信息对用户进行信用评估，并确定该用户的贷款发放额度（以真实货币，即资金的形式体现，也就是本申请实施例中前文所述的第一资源的第一数额）。

在具体实施时，拟申请贷款的用户 C 的相关信息往往涉及到用户 C 的个人隐私，例如用户的姓名、身份证号等个人信息，以及用户的收入数据、消费信息、还款状况等涉及到用户 C 的资金调度能力的信息。为保护用户 C 的隐私，用户 C 向特定机构 A 提供的信息并不向其他机构披露，例如发放贷款的机构等，而仅供特定机构 A 知晓。

在对拟申请贷款的用户 C 进行信用评估后允许其贷款、并为其确定贷款发放额度的情况下，特定机构 A 将评估结果（包括贷款发放额度）发送到预设的特定机构 B，由特定机构 B 向拟申请贷款的用户 C 发放与贷款发放额度相对应的数额的代币（以虚拟货币的形式体现，也就是本申请实施例中前文所述的第二资源）。在具体实施时，特定机构 A 和特定机构 B 可以由同一实体机构兼任。

可以理解到，在信用评估和代币发放阶段，当允许拟申请贷款的用户 C 贷款时（相当于满足转移条件），将允许用户 C 借取的贷款发放额度确定为

待转移的资金的第一数额，并在此基础上确定出待转移的代币的第二数额（如前述实施例中所述，可以有多种方式实现资金的第一数额与代币的第二数额之间的对应）。此时，转出方具体化为上述特定机构 B，转入方具体化为拟申请贷款的用户 C，转出方向区块链发起的交易请求中，包括对代币的第二数额（记为 quota_c）进行加密处理后得到的第一加密数额信息。

具体地，可以通过采用第一加密函数（记为 enc(x,y)）对代币的第二数额 quota_c 进行加密处理得到。其中，第一加密函数的一个输入为代币的第二数额 quota_c，另一个输入为转入方（也就是用户 C）的公钥（记为 pk_c）。可以理解到，若转入方的公钥为非对称密钥，则该第一加密函数为非对称加密函数；若转入方的公钥为对称密钥，则该第一加密函数为对称加密函数。

进一步地，还可以将转入方的公钥 pk_c 的标识信息作为交易请求的一部分发送到区块链系统，供区块链系统在验证、实施后上链。具体地，可以采用转入方的公钥的哈希值（记为 hash(pk_c)）作为公钥的标识信息。此时，转出方（即特定机构 B）发起的交易请求 TX 的交易格式可表示为：

TX=(enc(pk_c, quota_c), hash(pk_c))

在本申请实施例中，用户 C 所持有的代币的数额（此处体现为 quota_c）能够反映用户 C 允许借取的实际资金的数额（也就是贷款发放额度）。可以理解到，当用户 C 已借取了部分资金（实际借取的资金的数额应不大于上述贷款发放额度）时，用户 C 所持有的代币的数额将减少，表示用户 C 能够借取的资金的额度被扣减；而当用户 C 将已借取的资金归还时，用户 C 所持有的代币的数额将会增加，表示用户 C 能够借取的资金的额度被恢复或补足。

需要说明的是，在业务流程中，可以定时或周期性地对用户 C 重新进行信用评估，从而调整用户的贷款发放额度。当额度提高时，特定机构 B 可以执行上述资金转移过程向用户 C 发放额度的差值，此时，将额度的差值确定为待转移的资金的第一数额。当额度降低时，可以要求用户在指定

时间内向特定机构 B 返还额度的差值，在这一资金转移的过程中，用户 C 将作为转出方，特定机构 B 将作为转入方，将额度的差值确定为待转移的资金的第一数额。

可以理解到，若用户逾期未将因额度降低而需返还的额度差值返还给特定机构 B，则特定机构 B 可以向所有的贷款发放机构发送黑名单，限制用户 C 办理贷款，而仅允许接收用户 C 还款，直至用户 C 返还额度的差值。

通过上述方式，将代表贷款额度的代币发放到用户 C，并将这一发放过程写入区块链，有利于对用户 C 的贷款额度进行监管，从而降低了贷款发放机构放贷的风险，维护了交易安全。

为便于理解，图 3 给出了在信用评估和发放代币阶段的业务流程示意图，具体如下：

首先，用户 C 向进行信用评估的机构 A 提交个人资料，供机构 A 对本人的信用进行评估。

其次，机构 A 根据信用评估的结果决定是否允许用户 C 贷款，确定允许的贷款额度（相当于第一资源的第一数额，资金的第一数额，体现为真实货币），并向用户 C 反馈信用评估的结果。

再次，机构 A 将允许用户 C 贷款的额度的信息发送至机构 B，进行代币发放。机构 B 根据额度的信息确定与贷款额度相对应的代币的数额（相当于第二资源的第二数额，代币的第二数额，体现为虚拟货币）。

然后，机构 B（作为资源转出方，转出方）向区块链平台发起交易请求，该交易请求中包含代币数额的信息。为保护隐私，该信息为对代币数额进行加密处理后的加密信息。区块链平台对该交易请求的合法性进行验证确认后，允许机构 B 实施该交易请求；并在机构 B 向用户 C（作为资源转入方，转入方）转移对应数额的代币后，将交易的实施结果写入区块链。

至此完成了对用户 C 的信用评估和代币发放。用户 C 所持有的代币的数额反映允许用户 C 借取的贷款的额度。

（二）贷款申请和发放阶段

当用户 C 需要申请贷款时，可以与发贷机构 D 达成贷款协议（相当于资源转移过程中的资源借取协议），确定用户 C 申请借取的资金的数额（相当于第一资源的第一数额）。在贷款协议达成后，根据协议中确定的申请借取的资金的第一数额确定相对应的代币的第二数额（相当于第二资源的第二数额）。用户 C 向发贷机构 D 发送所持有的代币，代币的数额为第二数额，记为 quota_d，并可以进一步将所持有代币的余额（记为 quota_c'）返回自己的账户。发贷机构 D 接收到用户 C 发送的代币（虚拟货币）后，即可将资金（真实货币）发送给用户 C，以便用户 C 取得申请借取的资金。

在上述过程中，用户 C 向区块链发送交易请求，以将数额为 quota_d 的代币发送到发贷机构 D。该交易请求中，可包含对 quota_d 进行加密处理得到的第一加密数额信息，反映将要转移到机构 D 的代币的数额；还可包含对用户 C 所持代币的余额 quota_c'进行加密处理得到的第二加密数额信息，反映将要返回用户 C 的自有账户的代币的余额；还可进一步包含用户 C 参与的上一次资金转移交易的标识信息（可记为 Tx_in），可具体取为区块链中记录的、上一次资金转移交易的哈希值，也可以是预设的用于区分不同交易的标识符，反映用户 C 所持有代币的数额 quota_c 的确定依据。

除此之外，用户 C 向区块链发送的交易请求中，还可以加入零知识证明，用于证明执行交易请求之后转出方（用户 C）将要持有的代币的余额 quota_c'与转移的代币数额 quota_d 的和，等于转出方（用户 C）在发起交易请求前所持有的代币的数额 quota_c，也就是，利用零知识证明证明等式（(quota_c- quota_d) = quota_c'）成立。进一步地，还可以利用零知识证明证明转出方（用户 C）转出的代币的数额 quota_d 大于零，转出方（用户 C）在发起交易请求前所持有的代币的数额 quota_c 大于零，并且，执行交易请求之后转出方（用户 C）将要持有的代币的余额 quota_c'不小于零。

因此，用户 C 向区块链发起的交易请求，其交易格式可表示为：

Tx=(Tx_in, enc(pk_d, quota_d), hash(pk_d), enc(pk_c, quota_c'), hash(pk_c), proof((quota_c- quota_d- quota_c' ==0)&& (quota_c>0) &&

(quota_d>0) && (quota_c' >0)))

在上述交易请求中，Tx_in 可以理解为本次交易的输入，反映用户 C（此处为转出方）所持有的代币的数额的来源。enc(pk_d, quota_d), hash(pk_d)可以理解为本次交易的第一个输出，反映用户 C 向机构 D 发送的代币的数额 quota_d，亦能反映机构 D 接收到用户 C 发送的代币的数额。enc(pk_c, quota_c'), hash(pk_c)可以理解为本次交易的第二个输出，反映用户 C 在完成代币转移后剩余的代币的数额 quota_c'，相当于用户 C 发送代币后获得的找零。零知识证明用于向区块链中未参与本次交易的节点证明本次交易的合法性，同时并不泄露本次交易的具体数额，保护了交易双方的隐私。

通过将这一交易上链，可以将参与交易的双方（用户 C 和发贷机构 D）所持代币的变化状态写入区块链，从而能够监管交易的合法性，避免用户 C 超过贷款额度申请贷款。同时，通过对转移代币的具体数额进行加密处理，并通过零知识证明证明合法性，也保护了交易双方的隐私。

为便于理解，图 4 给出了贷款申请和发放阶段的业务流程示意图，具体如下：

首先，用户 C 向贷款发放的机构 D 提出贷款申请。在与机构 D 达成贷款协议后，用户 C 根据贷款协议的约定确定贷款的金额（相当于第一资源的第一数额，资金的第一数额，体现为真实货币），再据此确定与贷款的金额相对应的代币的数额（相当于第二资源的第二数额，代币的第二数额，体现为虚拟货币）。

其次，用户 C（作为资源转出方，转出方）向区块链平台发起交易请求，该交易请求中包含代币数额的信息。为保护隐私，该信息为对代币数额进行加密处理后的加密信息。区块链平台对该交易请求的合法性进行验证确认后，允许用户 C 实施该交易请求；并在用户 C 向机构 D（作为资源转入方，转入方）转移对应数额的代币后，将交易的实施结果写入区块链。

然后，机构 D 在接收到用户 C 转移的代币后，向对应数额的贷款发放给用户 C。

至此用户 C 完成了贷款的申请，机构 D 完成了贷款的发放。可以理解到，在交易完成后，用户 C 所持有的代币的数额将被扣减，所持有的代币的余额反映允许用户 C 借取的贷款的剩余额度。

（三）还款阶段

当用户 C 需要向发贷机构 D 还款时，用户 C 先向发贷机构 D 的银行账户进行汇款，用真实货币（相当于第一资源）归还借款。而后发贷机构 D 在接收到用户 C 归还的真实货币后，通过向区块链发起交易请求，将与用户 C 归还的真实货币数额相对应的代币（相当于第二资源）转移给用户 C，从而为用户 C 恢复或者补足贷款额度。

具体地，转出方（此处为发贷机构 D）发起的交易请求 TX 的交易格式可表示为：

TX=(enc(pk_c, quota_d), hash(pk_c))

该交易请求可以理解为，采用加密函数对发贷机构 D（资金转出方）接收到的资金的数额相对应的代币的数额 quota_d 进行加密处理，其中，加密函数的一个输入为代币的数额 quota_d，另一个输入为用户 C（资金转入方）的公钥 pk_c。除此之外，还将用户 C 的公钥的标识信息，例如公钥 pk_c 的哈希值 hash(pk_c)，作为交易请求的一部分发送到区块链系统。

为便于理解，图 5 给出了还款阶段的业务流程示意图，具体如下：

首先，用户 C 将需归还的资金发送给发放贷款的机构 D，实现真实货币的归还。

其次，机构 D 确认接收到用户 C 还款的资金的金额（相当于第一资源的第一数额，资金的第一数额，体现为真实货币），并在此基础上确定与还款的金额相对应的代币的数额（相当于第二资源的第二数额，代币的第二数额，体现为虚拟货币）。

再次，机构 D（作为资源转出方，转出方）向区块链平台发起交易请求，该交易请求中包含代币数额的信息。为保护隐私，该信息为对代币数额进行加密处理后的加密信息。区块链平台对该交易请求的合法性进行验

证确认后，允许机构 D 实施该交易请求；并在机构 D 向用户 C（作为资源转入方，转入方）转移对应数额的代币后，将交易的实施结果写入区块链。

至此用户 C 完成了贷款的归还，机构 D 完成了贷款的收回。可以理解到，在交易完成后，用户 C 所持有的代币的数额将增加，所持有的代币的数额反映允许用户 C 借取的贷款的额度。

在上述各个阶段中，均采用了本申请实施例提供的资金转移方法，通过将代表真实货币的资金的数额转换为代表虚拟货币的代币的数额，并通过对在区块链中流通的代币数额进行加密处理的方式，保护了交易双方的隐私。即使有多家放贷机构加入区块链平台进行贷款的发放，用户在多家发放机构申请的贷款的总数额也不会超过被允许的贷款额度，从而降低了发贷机构的放贷风险。这会因为，如以上示例中所述，反映贷款额度的代币由特定的机构 B 发放，用户所持代币的数额也会随着用户的借贷、还款行为相应变化，且带来这些变化过程的交易均被写入区块链，利用区块链技术本身的公开、透明、不可篡改的特性，就能够保证代币数额的真实性和可靠性，进而确保用户无法超额申请贷款。

与此同时，上述反映贷款额度的代币的变化的交易中，转移的代币的数额均已进行加密处理，从而隐藏了交易双方的具体交易信息，因此，也能够在资金转移过程中保护资金转移双方的隐私信息。

本申请实施例还提供了一种基于区块链的资源转移方法，参见图 6 所示，包括:

S301: 当满足资源转移条件时，确定待转移的第一资源的第一数额;

S303: 根据第一资源的第一数额，采用单向函数确定待转移的第二资源的第二数额；第一资源与第二资源的类型不同;

S305: 资源转出方向区块链发起交易请求，用于向资源转入方转移待转移的第二资源；其中，交易请求中包括与第二资源的第二数额相对应的信息;

S307：在区块链对交易请求进行验证后，执行交易请求，将待转移的第二资源转移到资源转入方，并将执行结果写入区块链。

该实施例中，将实际需要转移的第一资源转换为第二资源进行转移，通过对第二资源的转移就能够达到资源转移的目的，同时，通过单向函数实现第一资源和第二资源之间的数额转换，利用单向函数的特性，使得交易双方之外第三方无法根据第二资源的第二数额推知第一资源的第一数额，从而可以隐藏实际转移的第一资源的数额，起到保护交易隐私的作用。

更进一步地，根据第一资源的第一数额，采用单向函数确定第二资源的第二数额时，可以将第一资源的第一数额和一随机数作为单向函数的输入，将单向函数的输出确定为第二资源的第二数额。采用这种方式，利用单向函数的特性，即使在后续发起的交易请求中不对第二数额进行加密处理，而是直接将通过单向函数转换得到的第二数额放入交易请求中，也能在一定程度上保护资源转移的实质数额（也就是第一资源的第一数额）。当然，在此基础上，对第二数额进行进一步的加密处理以得到第一加密数额信息，并将第一加密数额信息携带在资源转出方发起的交易请求中，能够更好的保护资源转移交易的隐私信息。

在采用单向函数实现第一资源与第二资源间的数额转换时，资源转出方还需要将进行转换时使用的随机数（作为单向函数的一个输入）发送给资源转入方，以便资源转入方进行资源类型的反向转换，推知第一资源的第一数额。在具体实施时，可以在资源转出方向区块链发起交易请求之前，对这一随机数进行加密，则发起的交易请求中携带的为加密后的随机数，从而避免了随机数的泄密，保护了资源转移交易的隐私信息。具体地，可以借助资源转入方的公钥对随机数进行加密，从而只有资源转入方的私钥才能对该随机数进行解密，以便保护交易隐私。

需要说明的是，在采用单向函数进行第一资源和第二资源的数额转换时，每一次交易所采用的随机数应是变化的，从而避免交易数额信息的泄露。

可以理解到，本实施例中也可应用于资金借贷这一应用场景。在该场景下，第一资源具体为资金，第二资源具体为代币。所对应的基于区块链的资金转移方法，参见图 7 所示，包括:

S401: 当满足转移条件时，确定待转移的资金的第一数额;

S403: 根据资金的第一数额，采用单向函数确定待转移的代币的第二数额; 资金与代币的类型不同;

S405: 转出方向区块链发起交易请求，用于向转入方转移待转移的代币; 其中，交易请求中包括与代币的第二数额相对应的信息;

S407: 在区块链对交易请求进行验证后，执行交易请求，将待转移的代币转移到转入方，并将执行结果写入区块链。

需要说明的是，本实施例中采用单向函数实现第一资源与第二资源的转换（或者资金的数额与代币的数额的转换）的方式，与前述多个实施例可以组合实施，也都适用于各具体的业务流程，此处不再赘述。

与图 1 提供的基于区块链的资源转移方法相对应地，本申请实施例还提供了一种基于区块链的资源转移装置，参见图 8 所示，包括:

第一数额确定模块 101，当满足资源转移条件时，确定待转移的第一资源的第一数额;

第二数额确定模块 103，根据第一资源的第一数额，确定待转移的第二资源的第二数额; 第一资源与第二资源的类型不同;

交易请求发起模块 105，资源转出方向区块链发起交易请求，用于向资源转入方转移待转移的第二资源; 其中，交易请求中包括对第二资源的第二数额进行加密处理后得到的第一加密数额信息;

入链模块 107，在区块链对交易请求进行验证后，执行交易请求，将待转移的第二资源转移到资源转入方，并将执行结果写入区块链。

图 9 是本申请的一个实施例电子设备的结构示意图。请参考图 9，在硬件层面，该电子设备包括处理器，可选地还包括内部总线、网络接口、存储器。其中，存储器可能包含内存，例如高速随机存取存储器(Random-Access

Memory，RAM)，也可能还包括非易失性存储器（non-volatile memory），例如至少 1 个磁盘存储器等。当然，该电子设备还可能包括其他业务所需要的硬件。

处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是 ISA(Industry Standard Architecture，工业标准体系结构）总线、PCI(Peripheral Component Interconnect，外设部件互连标准)总线或EISA(Extended Industry Standard Architecture，扩展工业标准结构）总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 9 中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

存储器，用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器，并向处理器提供指令和数据。

处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成基于区块链的资源转移装置。处理器，执行存储器所存放的程序，并具体用于执行以下操作：

当满足资源转移条件时，确定待转移的第一资源的第一数额；

根据第一资源的第一数额，确定待转移的第二资源的第二数额；第一资源与第二资源的类型不同；

资源转出方向区块链发起交易请求，用于向资源转入方转移待转移的第二资源；其中，交易请求中包括对第二资源的第二数额进行加密处理后得到的第一加密数额信息；

在区块链对交易请求进行验证后，执行交易请求，将待转移的第二资源转移到资源转入方，并将执行结果写入区块链。

上述如本申请图 1 所示实施例揭示的基于区块链的资源转移装置执行的方法可以应用于处理器中，或者由处理器实现。处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处

理器可以是通用处理器，包括中央处理器（Central Processing Unit，CPU）、网络处理器（Network Processor，NP）等；还可以是数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（Field－Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

该电子设备还可执行图 1 中基于区块链的资源转移装置执行的方法，并实现基于区块链的资源转移装置在图 1 所示实施例的功能，本申请实施例在此不再赘述。

本申请实施例还提出了一种计算机可读存储介质，该计算机可读存储介质存储一个或多个程序，该一个或多个程序包括指令，该指令当被包括多个应用程序的电子设备执行时，能够使该电子设备执行图 1 所示实施例中基于区块链的资源转移装置执行的方法，并具体用于执行:

当满足资源转移条件时，确定待转移的第一资源的第一数额;

根据第一资源的第一数额，确定待转移的第二资源的第二数额；第一资源与第二资源的类型不同;

资源转出方向区块链发起交易请求，用于向资源转入方转移待转移的第二资源；其中，交易请求中包括对第二资源的第二数额进行加密处理后得到的第一加密数额信息;

在区块链对交易请求进行验证后，执行交易请求，将待转移的第二资源转移到资源转入方，并将执行结果写入区块链。

与图 2 提供的基于区块链的资金转移方法相对应地，本申请实施例还提供一种基于区块链的资金转移装置，参见图 10 所示，包括：

资金数额确定模块 201，当满足转移条件时，确定待转移的资金的第一数额；

代币数额确定模块 203，根据资金的第一数额，确定待转移的代币的第二数额；资金与代币的类型不同；

交易请求发起模块 205，转出方向区块链发起交易请求，用于向转入方转移待转移的代币；其中，交易请求中包括对代币的第二数额进行加密处理后得到的第一加密数额信息；

入链模块 207，在区块链对交易请求进行验证后，执行交易请求，将待转移的代币转移到转入方，并将执行结果写入区块链。

图 11 是本申请的一个实施例电子设备的结构示意图。请参考图 11，在硬件层面，该电子设备包括处理器，可选地还包括内部总线、网络接口、存储器。其中，存储器可能包含内存，例如高速随机存取存储器(Random-Access Memory，RAM)，也可能还包括非易失性存储器（non-volatile memory），例如至少 1 个磁盘存储器等。当然，该电子设备还可能包括其他业务所需要的硬件。

处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是 ISA(Industry Standard Architecture，工业标准体系结构）总线、PCI(Peripheral Component Interconnect，外设部件互连标准)总线或 EISA(Extended Industry Standard Architecture，扩展工业标准结构）总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 11 中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

存储器，用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器，并向处理器提供指令和数据。

处理器从非易失性存储器中读取对应的计算机程序到内存中然后运

行，在逻辑层面上形成基于区块链的资金转移装置。处理器，执行存储器所存放的程序，并具体用于执行以下操作：

当满足转移条件时，确定待转移的资金的第一数额；

根据资金的第一数额，确定待转移的代币的第二数额；资金与代币的类型不同；

转出方向区块链发起交易请求，用于向转入方转移待转移的代币；其中，交易请求中包括对代币的第二数额进行加密处理后得到的第一加密数额信息；

在区块链对交易请求进行验证后，执行交易请求，将待转移的代币转移到转入方，并将执行结果写入区块链。

上述如本申请图 2 所示实施例揭示的基于区块链的资金转移装置执行的方法可以应用于处理器中，或者由处理器实现。处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器，包括中央处理器（Central Processing Unit，CPU）、网络处理器（Network Processor，NP）等；还可以是数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（Field－Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

该电子设备还可执行图 2 中基于区块链的资金转移装置执行的方法，

并实现基于区块链的资金转移装置在图 2 所示实施例的功能，本申请实施例在此不再赘述。

本申请实施例还提出了一种计算机可读存储介质，该计算机可读存储介质存储一个或多个程序，该一个或多个程序包括指令，该指令当被包括多个应用程序的电子设备执行时，能够使该电子设备执行图 2 所示实施例中基于区块链的资金转移装置执行的方法，并具体用于执行:

当满足转移条件时，确定待转移的资金的第一数额;

根据资金的第一数额，确定待转移的代币的第二数额；资金与代币的类型不同;

转出方向区块链发起交易请求，用于向转入方转移待转移的代币；其中，交易请求中包括对代币的第二数额进行加密处理后得到的第一加密数额信息;

在区块链对交易请求进行验证后，执行交易请求，将待转移的代币转移到转入方，并将执行结果写入区块链。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明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，本发明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。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产

生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

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。

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。

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、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。

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。

本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请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，本申请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。

以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

权利要求书

1、一种基于区块链的资源转移方法，包括:

当满足资源转移条件时，确定待转移的第一资源的第一数额;

根据所述第一资源的第一数额，确定待转移的第二资源的第二数额;所述第一资源与所述第二资源的类型不同;

资源转出方向区块链发起交易请求，用于向资源转入方转移所述待转移的第二资源;其中，所述交易请求中包括对所述第二资源的第二数额进行加密处理后得到的第一加密数额信息;

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的第二资源转移到所述资源转入方，并将执行结果写入所述区块链。

2、根据权利要求 1 所述方法，所述交易请求中包括的所述第一加密数额信息，通过采用第一加密函数对所述第二资源的第二数额进行加密处理得到;

其中，所述第一加密函数的一个输入为所述第二资源的第二数额，另一个输入为所述资源转入方的公钥。

3、根据权利要求 2 所述方法，所述交易请求中还包括所述资源转入方的公钥的标识信息。

4、根据权利要求 3 所述方法，所述资源转入方的公钥的标识信息为所述资源转入方的公钥的哈希值。

5、根据权利要求 1 所述方法，根据所述第一资源的第一数额，确定待转移的第二资源的第二数额，包括:

根据所述第一资源的第一数额，采用单向函数确定所述第二资源的第二数额。

6、根据权利要求 5 所述方法，采用单向函数确定所述第二资源的第二数额，包括:

将所述第一资源的第一数额和一随机数作为所述单向函数的输入，将所述单向函数的输出确定为所述第二资源的第二数额。

7、根据权利要求 6 所述方法，所述资源转出方向区块链发起的所述交易请求中，还包括加密后的所述随机数。

8、根据权利要求 1~7 之任一所述方法，所述资源转移条件包括允许所述资源转入方借取所述第一资源；则确定待转移的第一资源的第一数额，包括：

将允许所述资源转入方借取的第一资源的额度，作为所述待转移的第一资源的第一数额。

9、根据权利要求 1~7 之任一所述方法，所述资源转移条件包括所述资源转出方已接收到所述资源转入方归还的第一资源；则确定待转移的第一资源的第一数额，包括：

将所述归还的第一资源的数额，确定为所述待转移的第一资源的第一数额。

10、根据权利要求 1~7 之任一所述方法，所述资源转移条件包括所述资源转入方与所述资源转出方已达成资源借取协议，所述资源借取协议中包含所述资源转出方向所述资源转入方申请借取的第一资源的数额；则确定待转移的第一资源的第一数额，包括：

将所述申请借取的第一资源的数额，确定为所述待转移的第一资源的第一数额。

11、根据权利要求 10 所述方法，所述交易请求中还包括零知识证明，用于证明执行所述交易请求之后所述资源转出方将要持有的第二资源的余额与所述第二数额的和，等于所述资源转出方在发起所述交易请求前所持有的第二资源的数额。

12、根据权利要求 11 所述方法，所述零知识证明还用于证明所述第二数额大于零，所述资源转出方在发起所述交易请求前所持有的第二资源的数额大于零，并且，执行所述交易请求之后所述资源转出方将要持有的第

二资源的余额不小于零。

13、根据权利要求 10 所述方法，所述交易请求中还包括所述资源转出方参与的上一次资源转移交易的标识信息。

14、根据权利要求 13 所述方法，所述资源转出方参与的上一次资源转移交易的标识信息，具体为所述区块链中记录的、所述上一次资源转移交易的哈希值。

15、根据权利要求 10 所述方法，所述交易请求中还包括对执行所述交易请求之后所述资源转出方将要持有的第二资源的余额进行加密处理后得到的第二加密数额信息。

16、根据权利要求 15 所述方法，所述交易请求中包括的所述第二加密数额信息，通过采用第二加密函数对执行所述交易请求之后所述资源转出方将要持有的第二资源的余额进行加密处理得到；

其中，所述第二加密函数的一个输入为所述第二资源的余额，另一个输入为所述资源转出方的公钥。

17、根据权利要求 16 所述方法，所述交易请求中还包括所述资源转出方的公钥的标识信息。

18、根据权利要求 17 所述方法，所述资源转出方的公钥的标识信息为所述资源转出方的公钥的哈希值。

19、根据权利要求 1~7、11~18 之任一所述方法，所述第一资源具体为资金，所述第二资源具体为代币。

20、一种基于区块链的资金转移方法，包括：

当满足转移条件时，确定待转移的资金的第一数额；

根据所述资金的第一数额，确定待转移的代币的第二数额；所述资金与所述代币的类型不同；

转出方向区块链发起交易请求，用于向转入方转移所述待转移的代币；其中，所述交易请求中包括对所述代币的第二数额进行加密处理后得到的第一加密数额信息；

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的代币转移到所述转入方，并将执行结果写入所述区块链。

21、一种基于区块链的资源转移装置，包括:

第一数额确定模块，当满足资源转移条件时，确定待转移的第一资源的第一数额;

第二数额确定模块，根据所述第一资源的第一数额，确定待转移的第二资源的第二数额；所述第一资源与所述第二资源的类型不同;

交易请求发起模块，资源转出方向区块链发起交易请求，用于向资源转入方转移所述待转移的第二资源；其中，所述交易请求中包括对所述第二资源的第二数额进行加密处理后得到的第一加密数额信息;

入链模块，在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的第二资源转移到所述资源转入方，并将执行结果写入所述区块链。

22、一种电子设备，包括:

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作:

当满足资源转移条件时，确定待转移的第一资源的第一数额;

根据所述第一资源的第一数额，确定待转移的第二资源的第二数额;所述第一资源与所述第二资源的类型不同;

资源转出方向区块链发起交易请求，用于向资源转入方转移所述待转移的第二资源；其中，所述交易请求中包括对所述第二资源的第二数额进行加密处理后得到的第一加密数额信息;

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的第二资源转移到所述资源转入方，并将执行结果写入所述区块链。

23、一种计算机可读存储介质，所述计算机可读存储介质存储一个或

多个程序，所述一个或多个程序包括指令，所述指令当被包括多个应用程序的电子设备执行时，能够使所述电子设备执行以下操作：

当满足资源转移条件时，确定待转移的第一资源的第一数额；

根据所述第一资源的第一数额，确定待转移的第二资源的第二数额；所述第一资源与所述第二资源的类型不同；

资源转出方向区块链发起交易请求，用于向资源转入方转移所述待转移的第二资源；其中，所述交易请求中包括对所述第二资源的第二数额进行加密处理后得到的第一加密数额信息；

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的第二资源转移到所述资源转入方，并将执行结果写入所述区块链。

24、一种基于区块链的资金转移装置，包括：

资金数额确定模块，当满足转移条件时，确定待转移的资金的第一数额；

代币数额确定模块，根据所述资金的第一数额，确定待转移的代币的第二数额；所述资金与所述代币的类型不同；

交易请求发起模块，转出方向区块链发起交易请求，用于向转入方转移所述待转移的代币；其中，所述交易请求中包括对所述代币的第二数额进行加密处理后得到的第一加密数额信息；

入链模块，在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的代币转移到所述转入方，并将执行结果写入所述区块链。

25、一种电子设备，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

当满足转移条件时，确定待转移的资金的第一数额；

根据所述资金的第一数额，确定待转移的代币的第二数额；所述资金与所述代币的类型不同；

转出方向区块链发起交易请求，用于向转入方转移所述待转移的代币；其中，所述交易请求中包括对所述代币的第二数额进行加密处理后得到的第一加密数额信息；

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的代币转移到所述转入方，并将执行结果写入所述区块链。

26、一种计算机可读存储介质，所述计算机可读存储介质存储一个或多个程序，所述一个或多个程序包括指令，所述指令当被包括多个应用程序的电子设备执行时，能够使所述电子设备执行以下操作：

当满足转移条件时，确定待转移的资金的第一数额；

根据所述资金的第一数额，确定待转移的代币的第二数额；所述资金与所述代币的类型不同；

转出方向区块链发起交易请求，用于向转入方转移所述待转移的代币；其中，所述交易请求中包括对所述代币的第二数额进行加密处理后得到的第一加密数额信息；

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的代币转移到所述转入方，并将执行结果写入所述区块链。

27、一种基于区块链的资源转移方法，包括：

当满足资源转移条件时，确定待转移的第一资源的第一数额；

根据所述第一资源的第一数额，采用单向函数确定待转移的第二资源的第二数额；所述第一资源与所述第二资源的类型不同；

资源转出方向区块链发起交易请求，用于向资源转入方转移所述待转移的第二资源；其中，所述交易请求中包括与所述第二资源的第二数额相对应的信息；

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的第二资源转移到所述资源转入方，并将执行结果写入所述区块

链。

28、根据权利要求 27 所述方法，根据所述第一资源的第一数额，采用单向函数确定待转移的第二资源的第二数额，包括:

将所述第一资源的第一数额和一随机数作为所述单向函数的输入，将所述单向函数的输出确定为所述第二资源的第二数额。

29、根据权利要求 28 所述方法，所述资源转出方向区块链发起的所述交易请求中，还包括加密后的所述随机数。

30、根据权利要求 27~29 之任一所述方法，所述第一资源具体为资金，所述第二资源具体为代币。

31、一种基于区块链的资金转移方法，包括:

当满足转移条件时，确定待转移的资金的第一数额;

根据所述资金的第一数额，采用单向函数确定待转移的代币的第二数额; 所述资金与所述代币的类型不同;

转出方向区块链发起交易请求，用于向转入方转移所述待转移的代币; 其中，所述交易请求中包括与所述代币的第二数额相对应的信息;

在所述区块链对所述交易请求进行验证后，执行所述交易请求，将所述待转移的代币转移到所述转入方，并将执行结果写入所述区块链。

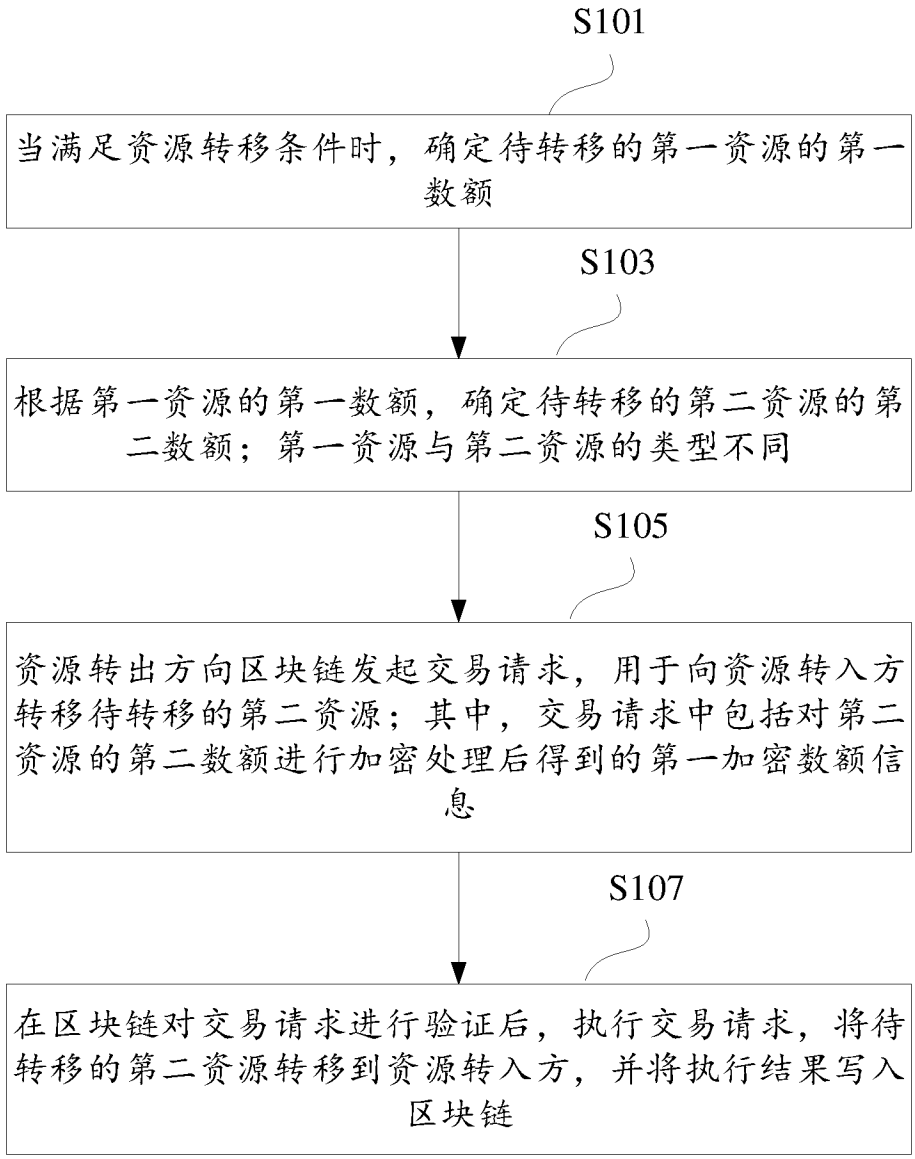
S101
当满足资源转移条件时，确定待转移的第一资源的第一数额
S103
根据第一资源的第一数额，确定待转移的第二资源的第二数额；第一资源与第二资源的类型不同
S105
资源转出方向区块链发起交易请求，用于向资源转入方转移待转移的第二资源；其中，交易请求中包括对第二资源的第二数额进行加密处理后得到的第一加密数额信息
S107
在区块链对交易请求进行验证后，执行交易请求，将待转移的第二资源转移到资源转入方，并将执行结果写入区块链

图 1

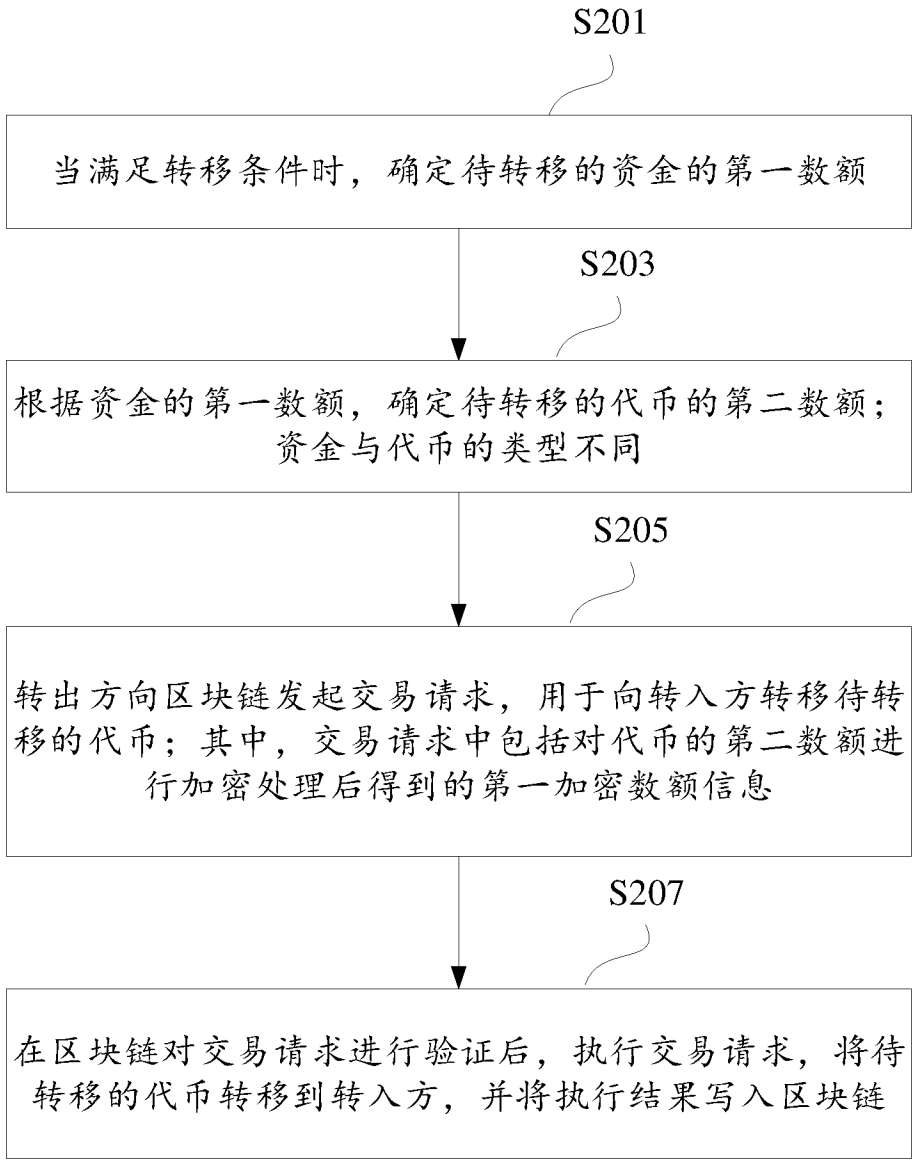
S201
当满足转移条件时，确定待转移的资金的第一数额
S203
根据资金的第一数额，确定待转移的代币的第二数额；资金与代币的类型不同
S205
转出方向区块链发起交易请求，用于向转入方转移待转移的代币；其中，交易请求中包括对代币的第二数额进行加密处理后得到的第一加密数额信息
S207
在区块链对交易请求进行验证后，执行交易请求，将待转移的代币转移到转入方，并将执行结果写入区块链

图 2

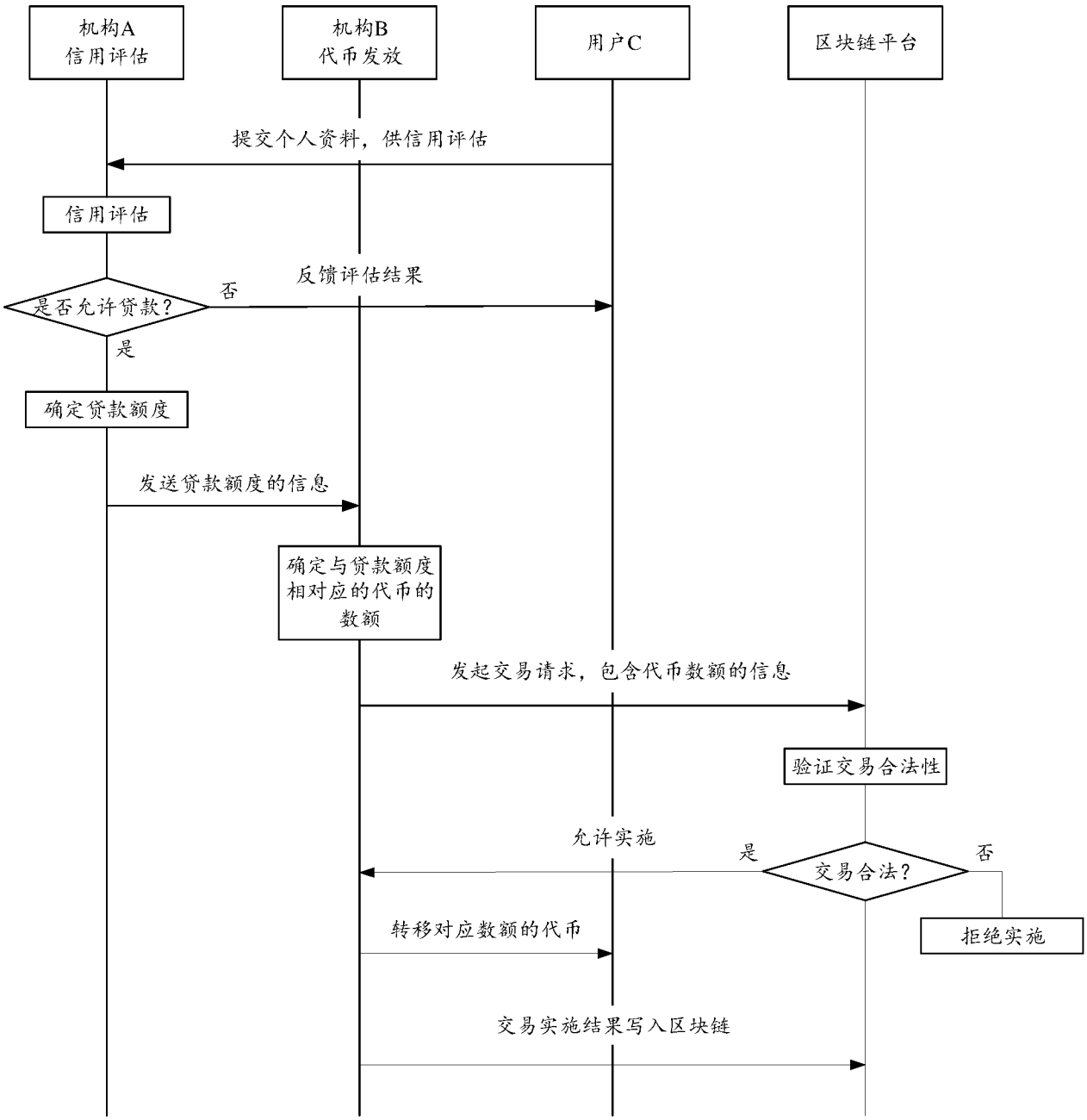
机构A
信用评估
机构B
代币发放
用户C
区块链平台
提交个人资料，供信用评估
信用评估
反馈评估结果
是否允许贷款?
否
是
确定贷款额度
发送贷款额度的信息
确定与贷款额度相对应的代币的数额
发起交易请求，包含代币数额的信息
验证交易合法性
允许实施
是
交易合法?
否
拒绝实施
转移对应数额的代币
交易实施结果写入区块链

图 3

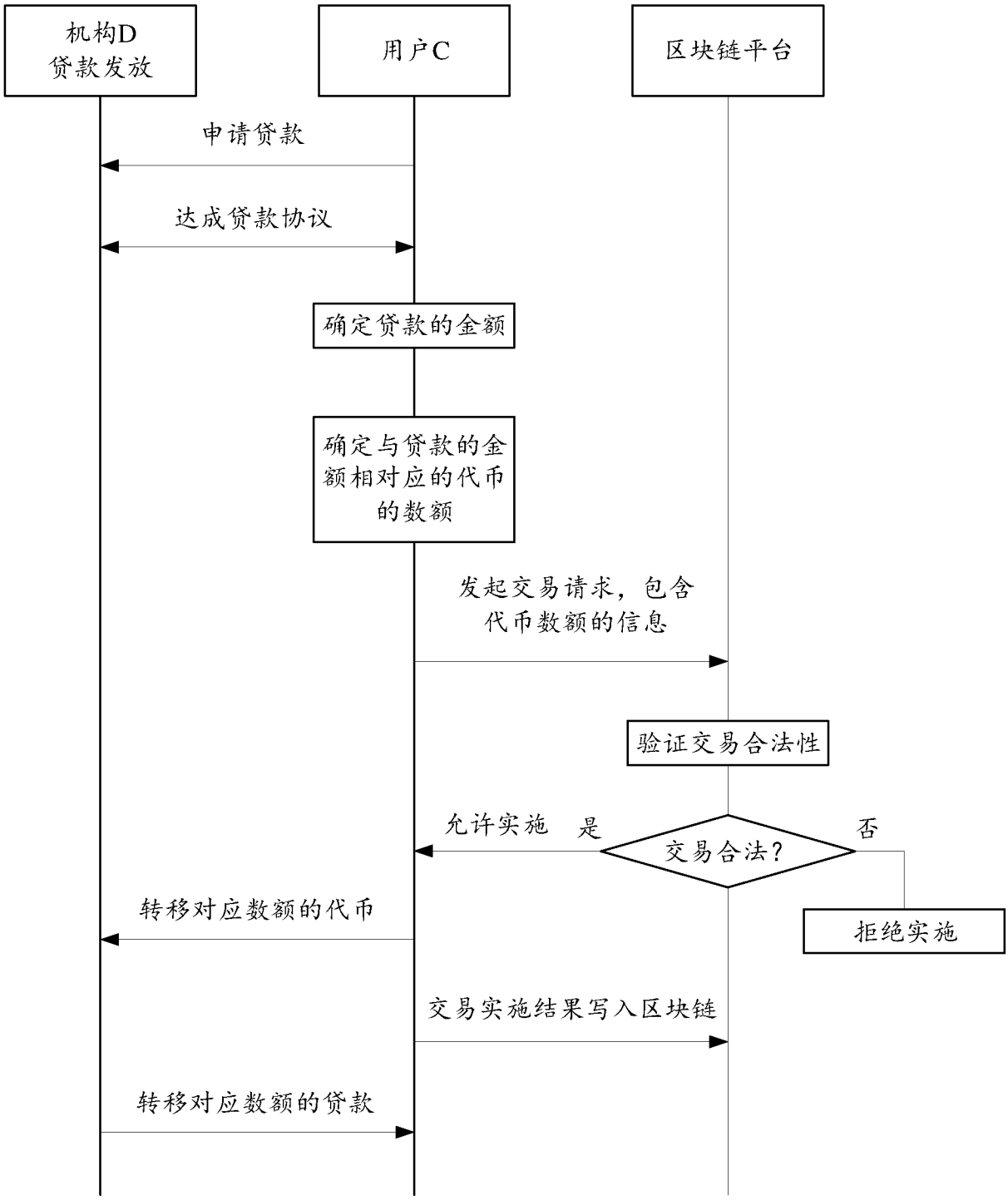
机构D
贷款发放
用户C
区块链平台
申请贷款
达成贷款协议
确定贷款的金额
确定与贷款的金额相对应的代币的数额
发起交易请求，包含代币数额的信息
验证交易合法性
允许实施
是
交易合法?
否
拒绝实施
转移对应数额的代币
交易实施结果写入区块链
转移对应数额的贷款

图 4

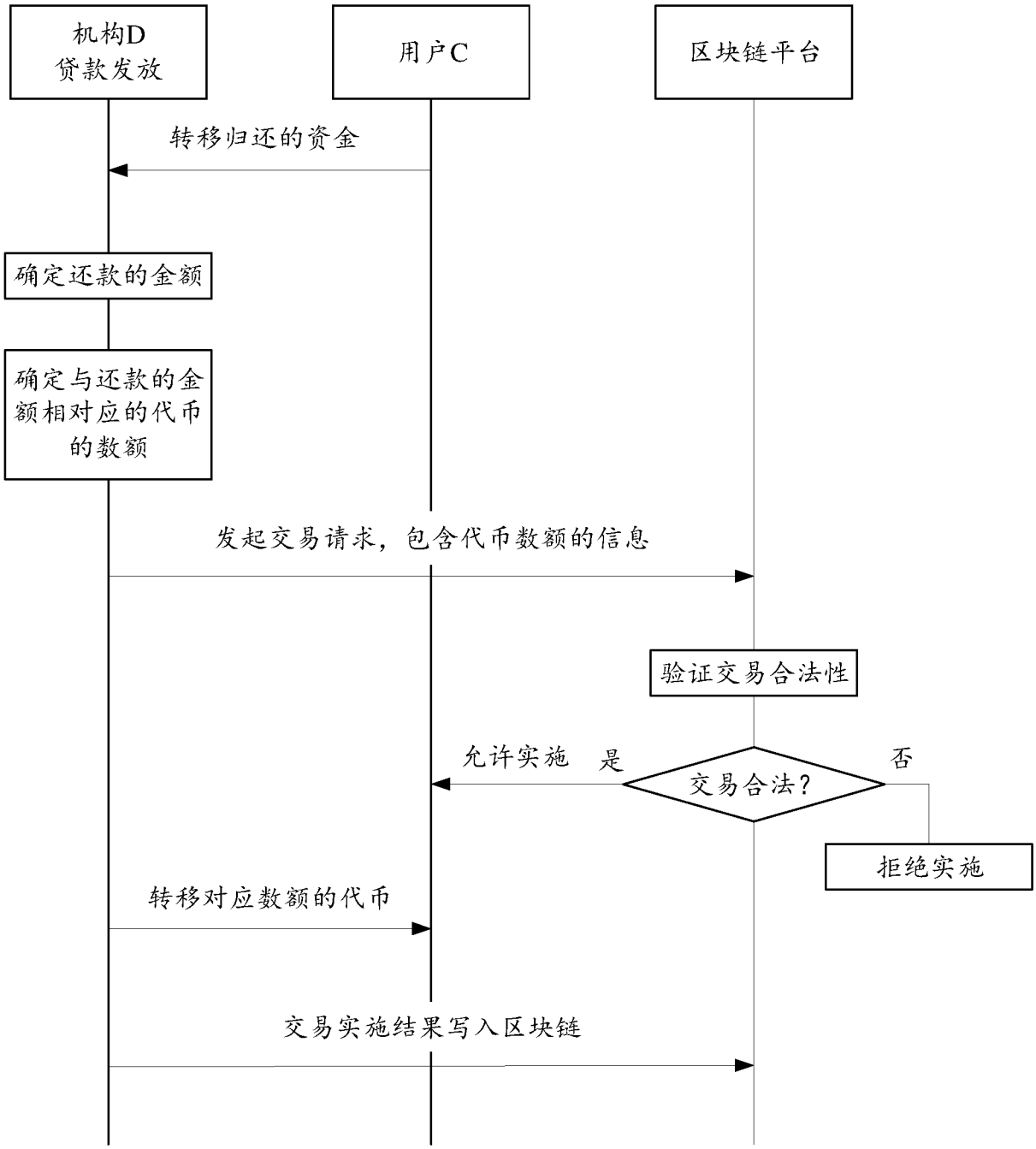
机构D
贷款发放
用户C
区块链平台
转移归还的资金
确定还款的金额
确定与还款的金额相对应的代币的数额
发起交易请求，包含代币数额的信息
验证交易合法性
允许实施
是
交易合法？
否
拒绝实施
转移对应数额的代币
交易实施结果写入区块链

图 5

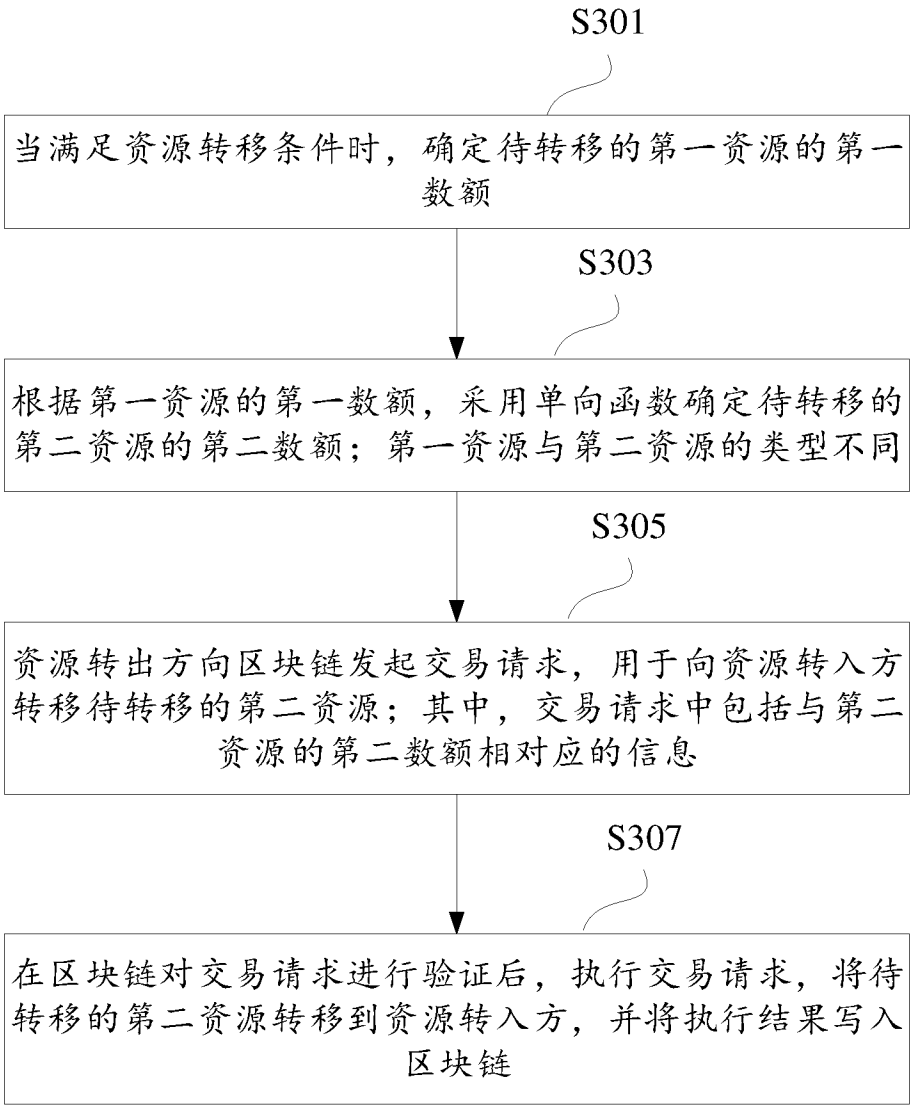
S301
当满足资源转移条件时，确定待转移的第一资源的第一数额
S303
根据第一资源的第一数额，采用单向函数确定待转移的第二资源的第二数额；第一资源与第二资源的类型不同
S305
资源转出方向区块链发起交易请求，用于向资源转入方转移待转移的第二资源；其中，交易请求中包括与第二资源的第二数额相对应的信息
S307
在区块链对交易请求进行验证后，执行交易请求，将待转移的第二资源转移到资源转入方，并将执行结果写入区块链

图 6

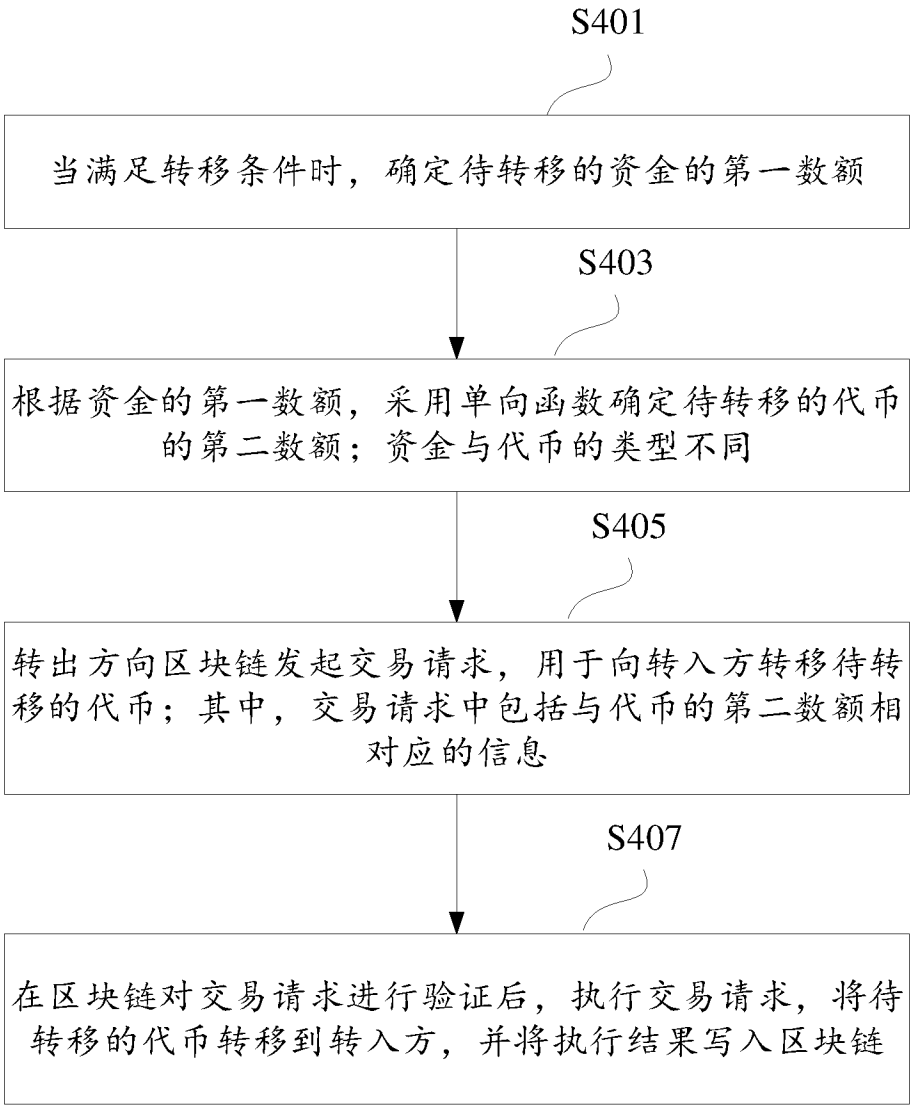
S401
当满足转移条件时，确定待转移的资金的第一数额
S403
根据资金的第一数额，采用单向函数确定待转移的代币的第二数额；资金与代币的类型不同
S405
转出方向区块链发起交易请求，用于向转入方转移待转移的代币；其中，交易请求中包括与代币的第二数额相对应的信息
S407
在区块链对交易请求进行验证后，执行交易请求，将待转移的代币转移到转入方，并将执行结果写入区块链

图 7

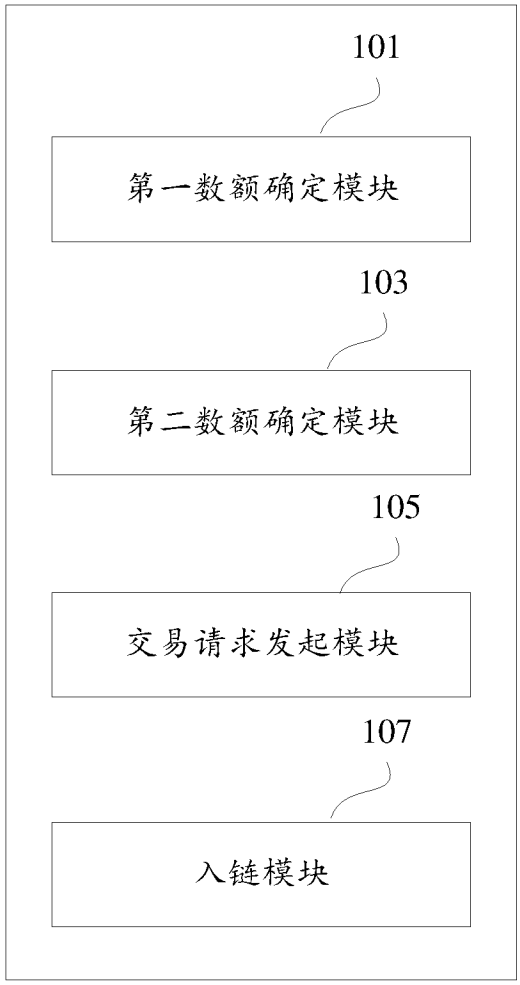
101
第一数额确定模块
103
第二数额确定模块
105
交易请求发起模块
107
入链模块

图 8

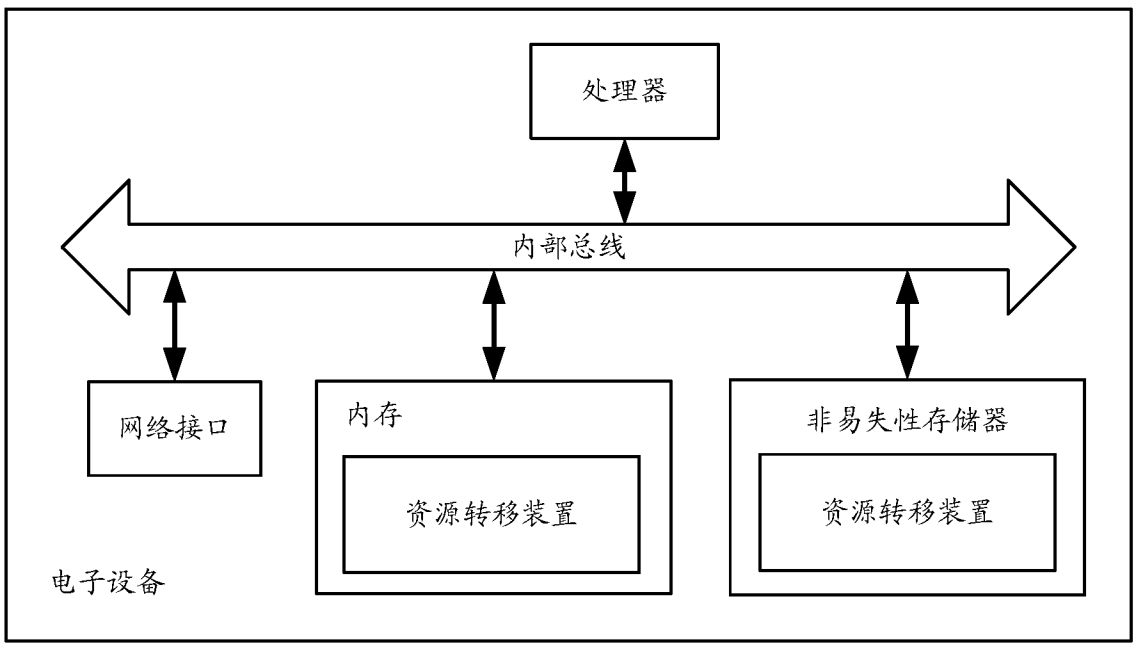
处理器
内部总线
网络接口
内存
资源转移装置
非易失性存储器
资源转移装置
电子设备

图 9

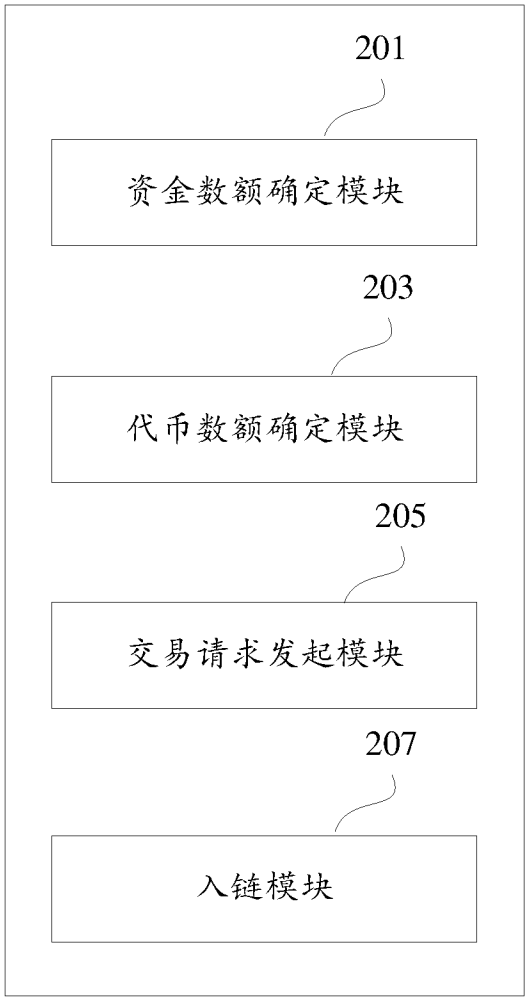
201
资金数额确定模块
203
代币数额确定模块
205
交易请求发起模块
207
入链模块

图 10

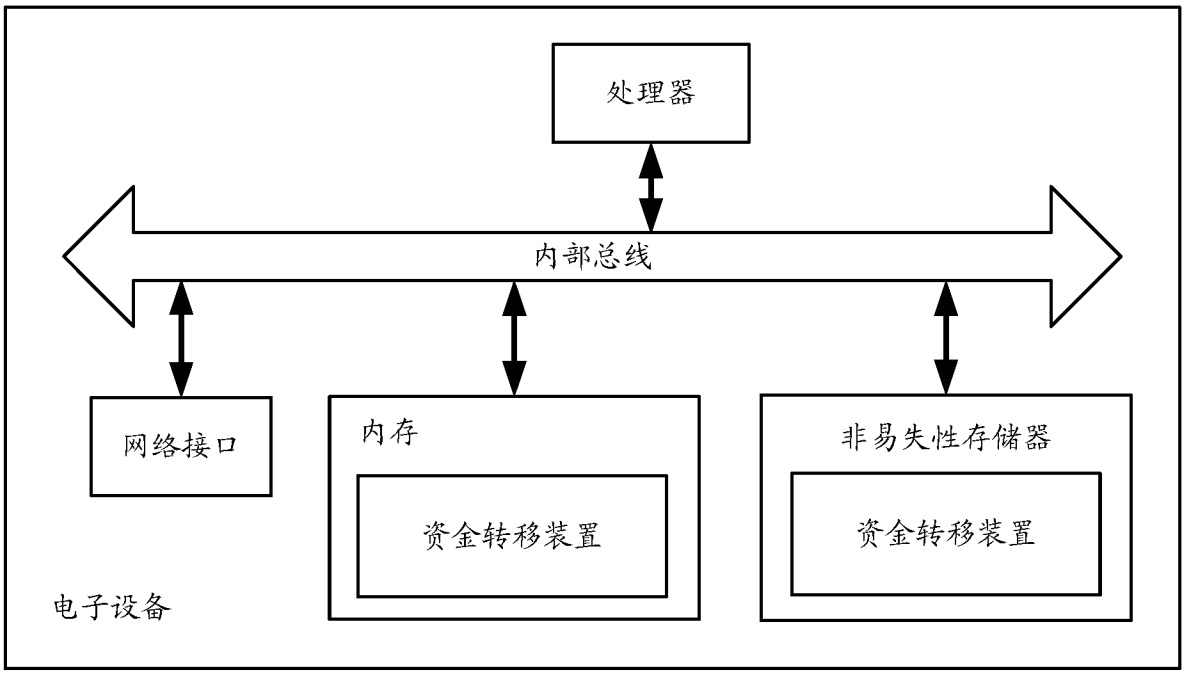
处理器
内部总线
网络接口
内存
资金转移装置
非易失性存储器
资金转移装置
电子设备

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/110034

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62(2013.01)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)

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)

CNABS, CNKI, DWPI, SIPOABS: 区块链, 资源, 资金, 货币, 代币, 资产, 虚拟货币, 转移, 迁移, 加密, 密钥, 数额, 数量, 金额, 验证, 校验, 转换, 类型, 种类, 哈希, 单向函数, blockchain, funds, resource, money, currency, virtual currency, token, assets, property, transfer, shift, divert, migrate, move, convert, transform, encrypt, key, amount, quantity, verify, check, inspect, kind, type, class, Hash, one way function

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 108009441 A (ALIBABA GROUP HOLDING LIMITED) 08 May 2018 (2018-05-08) claims 1-31	1-31
Y	CN 106960388 A (BANKNOTE CREDIT CARD INDUSTRY DEVELOPMENT CO., LTD. BEIJING SMART CARD TECHNOLOGY RESEARCH INSTITUTE) 18 July 2017 (2017-07-18) description, paragraphs 0036-0048 and 0079-0081, and claims 1-3	1-31
Y	CN 107358424 A (THE PEOPLE'S BANK OF CHINA, DIGITAL CURRENCY INSTITUTE) 17 November 2017 (2017-11-17) claim 1	1-31
A	CN 106846666 A (BEIJING YUNZHI TECHNOLOGY CO., LTD.) 13 June 2017 (2017-06-13) entire document	1-31
A	US 2017236102 A1 (D+H USA CORPORATION) 17 August 2017 (2017-08-17) entire document	1-31

☑ 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	Date of mailing of the international search report
26 December 2018	**14 January 2019**

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/110034

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017300876 A1 (PRICEWATERHOUSECOOPERS LLP) 19 October 2017 (2017-10-19) entire document	1-31

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/110034

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	108009441	A	08 May 2018	None			
CN	106960388	A	18 July 2017	None			
CN	107358424	A	17 November 2017	None			
CN	106846666	A	13 June 2017	None			
US	2017236102	A1	17 August 2017	WO	2017139688	A1	17 August 2017
US	2017300876	A1	19 October 2017	WO	2017180846	A1	19 October 2017

国际检索报告

国际申请号
PCT/CN2018/110034

A. 主题的分类

G06F 21/62(2013.01)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)

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））

CNABS,CNKI,DWPI,SIPOABS:区块链，资源，资金，货币，代币，资产，虚拟货币，转移，迁移，加密，密钥，数额，数量，金额，验证，校验，转换，类型，种类，哈希，单向函数，blockchain, funds, resource, money, currency, virtual currency, token, assets, property, transfer, shift, divert, migrate, move, convert, transform, encrypt, key, amount, quantity, verify, check, inspect, kind, type, class, Hash, one way function

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 108009441 A (阿里巴巴集团控股有限公司) 2018年 5月 8日 (2018-05-08) 权利要求1-31	1-31
Y	CN 106960388 A (中钞信用卡产业发展有限公司北京智能卡技术研究院) 2017年 7月 18日 (2017-07-18) 说明书第0036-0048、0079-0081段，权利要求1-3	1-31
Y	CN 107358424 A (中国人民银行数字货币研究所) 2017年 11月 17日 (2017-11-17) 权利要求1	1-31
A	CN 106846666 A (北京云知科技有限公司) 2017年 6月 13日 (2017-06-13) 全文	1-31
A	US 2017236102 A1 (D+H USA CORPORATION) 2017年 8月 17日 (2017-08-17) 全文	1-31
A	US 2017300876 A1 (PRICEWATERHOUSECOOPERS LLP) 2017年 10月 19日 (2017-10-19) 全文	1-31

☐ 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
2018年 12月 26日	2019年 1月 14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 邓隽 电话号码 86-(10)-62411644

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/110034

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	108009441	A	2018年 5月 8日	无			
CN	106960388	A	2017年 7月 18日	无			
CN	107358424	A	2017年 11月 17日	无			
CN	106846666	A	2017年 6月 13日	无			
US	2017236102	A1	2017年 8月 17日	WO	2017139688	A1	2017年 8月 17日
US	2017300876	A1	2017年 10月 19日	WO	2017180846	A1	2017年 10月 19日