

## (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 6 月 27 日 (27.06.2019)



(10) 国际公布号  
**WO 2019/119632 A1**

(51) 国际专利分类号:  
**G06Q 20/38** (2012.01)

(21) 国际申请号: PCT/CN2018/075881

(22) 国际申请日: 2018 年 2 月 8 日 (08.02.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:  
201711382545.3 2017 年 12 月 20 日 (20.12.2017) CN

(71) 申请人: 深圳壹账通智能科技有限公司(ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518000 (CN)。

(72) 发明人: 陆陈一帆(LU, Frank YiFan Chen); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518000 (CN)。 贾牧(JIA, Mu); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518000 (CN)。 谢丹力(XIE, DanLi); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518000 (CN)。

(74) 代理人: 深圳市沃德知识产权代理事务所(普通合伙)(SHENZHEN WORLD INTELLECTUAL PROPERTY AGENCY (GENERAL PARTNERSHIP)); 中国广东省深圳市福田区园岭街道八卦四路 10 号中浩大厦 1528-1530 室于志光, Guangdong 518000 (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,

(54) **Title:** BLOCKCHAIN-BASED TRANSFER METHOD FOR MULTIPLE ACCOUNT BOOKS, ELECTRONIC DEVICE AND READABLE STORAGE MEDIUM

(54) 发明名称: 基于区块链的多账本转账方法、电子装置及可读存储介质

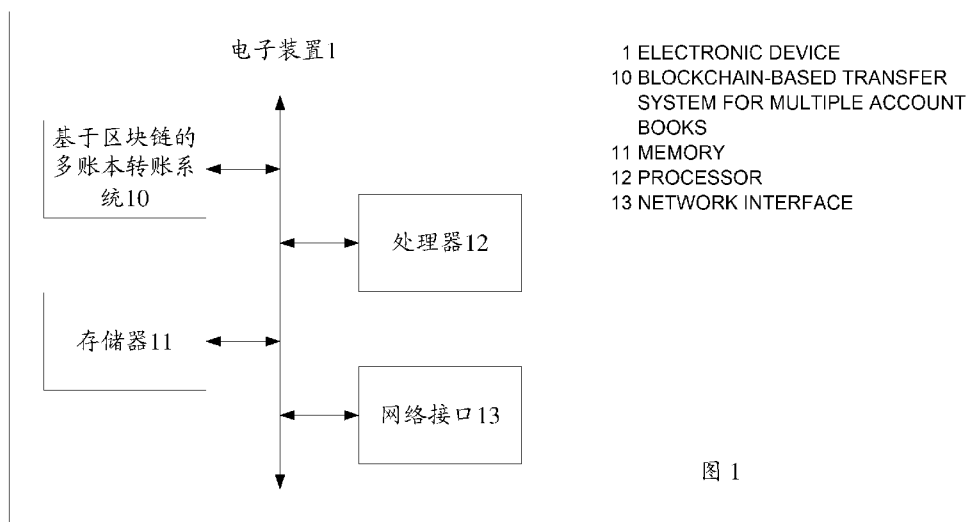


图 1

(57) **Abstract:** The present application relates to a blockchain-based transfer method for multiple account books, an electronic device, and a readable storage medium. The method comprises: if a first user account of a first user under a first account book in a blockchain initiates a transaction request with a second user account of a second user under a second account book, so as to to exchange a preset exchange transaction share at a preset exchange rate, receiving a first ciphertext generated from advanced encryption by the first user, the first ciphertext being generated by encrypting the preset exchange transaction share on the basis of a second preset password formula and a corresponding transaction share privacy key; calculating an exchange transaction share, an encrypted exchange transaction share, and a corresponding transaction share privacy key of the second account book by means of a first preset exchange calculation formula and on the basis of the preset exchange rate and the first ciphertext, and generating a second ciphertext of the second account book; and completing the transaction on the basis of the first ciphertext and the second ciphertext. The application achieves transfer operations

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))。

---

for multiple account books while also ensuring the security of transaction information in a blockchain technology scenario.

(57) 摘要: 本申请涉及一种基于区块链的多账本转账方法、电子装置及可读存储介质, 该方法包括: 若区块链中第一账本下第一用户的第一用户账户发起与第二账本下第二用户的第二用户账户将预设兑换交易份额按预设兑换率进行兑换的交易请求, 接收第一用户预先加密生成的第一密文; 第一密文为预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成; 通过第一预设兑换计算公式并基于预设兑换率和第一密文, 计算出第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥, 并生成第二账本的第二密文; 基于第一密文和第二密文完成交易。本申请能在有效保证区块链技术场景中交易信息安全的情况下, 实现多账本转账操作。

## 基于区块链的多账本转账方法、电子装置及可读存储介质

本申请要求于2017年12月20日提交中国专利局、申请号为201711382545.3、发明名称为“基于区块链的多账本转账方法、电子装置及可读存储介质”的中国专利申请的优先权，其全部内容通过引用结合在申请中。

### 技术领域

本申请涉及计算机技术领域，尤其涉及一种基于区块链的多账本转账方法、电子装置及可读存储介质。

### 背景技术

区块链技术因其具备的去中心化、信息不可篡改性等特点，越来越受到金融、保险等领域的公司的青睐，尤其是运用区块链技术实现多方参与的交易事件（例如，转账交易、支付交易等事件）越来越成为人们关注的焦点，例如，当银行A要卖100票据给银行B，如果这笔交易在区块链上进行，那么所有其他在区块链上的节点都会验证这笔交易，好处是其他参与方可以一起参与确认交易准确性，但又不能解读（解密）数据（又称零知识检测）。

为了保证交易的隐私性，目前业界通常会在交易中采用隐私交易加/解密算法。然而，现有的隐私交易加/解密算法一般仅局限于区块链技术场景下一个账本内的操作，例如把一个资产账本内的x份额从甲账户转到乙账户。然而，在实际区块链技术场景中，每一笔转账都有可能牵扯两个或多个账本，则这种现有隐私交易加/解密算法将无法实现区块链技术场景下的这种隐私交易。

因此，如何在有效保证区块链技术场景中交易信息安全的情况下，实现多账本转账操作，已经成为一种亟待解决的技术问题。

### 发明内容

本申请的目的在于提供一种基于区块链的多账本转账方法、电子装置及可读存储介质，旨在保证交易信息安全的情况下，实现区块链技术场景中的多账本转账操作。

为实现上述目的，本申请提供一种基于区块链的多账本转账方法，应用于电子装置，所述基于区块链的多账本转账方法包括：

A、若区块链中第一账本下第一用户的第一用户账户发起与第二账本下第二用户的第二用户账户的交易请求，则接收所述第一用户预先加密生成的第一密文；所述交易请求为将预设兑换交易份额按预设兑换率进行兑换的请求，所述第一密文为预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成的第一密文；

B、通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，

为所述第二账本计算出所述第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥，并生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文；

5 C、基于所述第一密文和第二密文，并按预设规则完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易。

此外，为实现上述目的，本申请还提供一种电子装置，所述电子装置包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的基于区块链的多账本转账系统，所述基于区块链的多账本转账系统被所述处理器执行  
10 时实现如下步骤：

若区块链中第一账本下第一用户的第一用户账户发起与第二账本下第二用户的第二用户账户的交易请求，则接收所述第一用户预先加密生成的第一密文；所述交易请求为将预设兑换交易份额按预设兑换率进行兑换的请求，所述第一密文为预设兑换交易份额采用第二预设密码公式及对应的交易  
15 份额隐私秘钥进行加密生成的第一密文；

通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，为所述第二账本计算出所述第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥，并生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文；

20 基于所述第一密文和第二密文，并按预设规则完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易。

进一步地，为实现上述目的，本申请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有基于区块链的多账本转账系统，所述基于区块链的多账本转账系统可被至少一个处理器执行，以使所述至少一个处理器  
25 执行如上述的基于区块链的多账本转账方法的步骤。

本申请提出的基于区块链的多账本转账方法、系统及可读存储介质，在区块链中第一账本下第一用户的第一用户账户发起与第二账本下第二用户的第二用户账户将预设兑换交易份额按预设兑换率进行兑换的交易请求后，接收所述第一用户预先为预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成的第一密文；通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，为所述第二账本计算生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文；基于所述第一密文和第二密文，并按预设规则完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易。由于能对第一账  
30 本下第一用户账户的预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成第一密文，并为所述第二账本计算生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文，基于所述第一密文和第二密文来完成所述第一账本下第一用户账户与所述第二账本下第二用户账户的交易操作，在交易过程中只有第一用户或第二用户能解

密所述第一密文或第二密文以获知交易具体的兑换交易份额数据，区块链上的其他节点无法解读具体的兑换交易份额数据，从而在有效保证区块链技术场景中交易信息安全的情况下，实现多账本转账操作。

## 5 附图说明

图 1 为本申请基于区块链的多账本转账系统 10 较佳实施例的运行环境示意图；

图 2 为本申请基于区块链的多账本转账方法一实施例的流程示意图。

## 10 具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本申请，并不用于限定本申请。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。

需要说明的是，在本申请中涉及“第一”、“第二”等的描述仅用于描述目的，而不能理解为指示或暗示其相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。另外，各个实施例之间的技术方案可以相互结合，但是必须是以本领域普通技术人员能够实现为基础，当技术方案的结合出现相互矛盾或无法实现时应当认为这种技术方案的结合不存在，也不在本申请要求的保护范围之内。

本申请提供一种基于区块链的多账本转账系统。请参阅图 1，是本申请基于区块链的多账本转账系统 10 较佳实施例的运行环境示意图。

在本实施例中，所述的基于区块链的多账本转账系统 10 安装并运行于电子装置 1 中。该电子装置 1 可包括，但不仅限于，存储器 11、处理器 12 及网络接口 13。图 1 仅示出了具有组件 11-13 的电子装置 1，但是应理解的是，并不要求实施所有示出的组件，可以替代的实施更多或者更少的组件。

所述电子装置 1 通过网络接口 13 连接网络(图 1 未标出)，获取资讯。所述网络可以是企业内部网 (Intranet)、互联网 (Internet)、全球移动通讯系统 (Global System of Mobile communication, GSM)、宽带码分多址 (Wideband Code Division Multiple Access, WCDMA)、4G 网络、5G 网络、蓝牙 (Bluetooth)、Wi-Fi、通话网络等无线或有线网络。

所述存储器 11 为至少一种类型的可读计算机存储介质，所述存储器 11 在一些实施例中可以是所述电子装置 1 的内部存储单元，例如该电子装置 1 的硬盘或内存。所述存储器 11 在另一些实施例中也可以是所述电子装置 1 的外部存储设备，例如所述电子装置 1 上配备的插接式硬盘，智能存储卡 (Smart Media Card, SMC)，安全数字 (Secure Digital, SD) 卡，闪存卡 (Flash Card) 等。进一步地，所述存储器 11 还可以既包括所述电子装置 1 的内部

存储单元也包括外部存储设备。所述存储器 11 用于存储安装于所述电子装置 1 的应用软件及各类数据，例如所述基于区块链的多账本转账系统 10 的程序代码等。所述存储器 11 还可以用于暂时地存储已经输出或者将要输出的数据。

所述处理器 12 在一些实施例中可以是一中央处理器 (Central Processing Unit, CPU)，微处理器或其他数据处理芯片，用于运行所述存储器 11 中存储的程序代码或处理数据，例如执行所述基于区块链的多账本转账系统 10 等。

所述网络接口 13 可包括无线网络接口或有线网络接口，该网络接口 13 通常用于在所述电子装置 1 与其他电子设备之间建立通信连接。

基于区块链的多账本转账系统 10 包括至少一个存储在所述存储器 11 中的计算机可读指令，该至少一个计算机可读指令可被所述处理器 12 执行，以实现本申请各实施例。

其中，上述基于区块链的多账本转账系统 10 被所述处理器 12 执行时实现如下步骤：

步骤 S1，若区块链中第一账本下第一用户的第一用户账户发起与第二账本下第二用户的第二用户账户的交易请求，则接收所述第一用户预先加密生成的第一密文；所述交易请求为将预设兑换交易份额按预设兑换率进行兑换的请求，所述第一密文为预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成的第一密文。

本实施例中，首先由区块链中的用户或者机构将自己在每一个账本下每一个用户账户的余额采用第一预设密码公式及对应的余额隐私秘钥进行加密，并将自己在每一个账本下每一个用户账户加密后的余额通过区块链的智能合约写到该区块链的各个节点上的共享资产账本上。例如，采用 Pederson Commitment 算法，所述第一预设密码公式为  $a'_{ij} = g^{a_{ij}} * h^{x_{ij}}$ ，或者， $a'_{ij} = h^{a_{ij}} * g^{x_{ij}}$ ，其中， $a_{ij}$  代表第 i 账本下的第 j 个用户账户的余额， $x_{ij}$  代表第 i 账本下的第 j 个用户账户的余额隐私秘钥， $a'_{ij}$  代表第 i 账本下的第 j 个用户账户的加密余额，g 和 h 为离散对数问题中的基， $h = g^c$ ，c 为未知数，i 和 j 为正整数。

在第一账本（例如，该第一账本可以是人民币账本）下第一用户的第一用户账户发起与第二账本（例如，该第二账本可以是美元账本）下第二用户的第二用户账户将预设兑换交易份额按预设兑换率进行兑换（该预设兑换交易份额和该预设兑换率可在智能合约中提前设置）的交易请求之前，由该第一用户为该预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成第一密文。例如，所述第二预设密码公式为  $t'_{lij} = g^{t_{lij}} * h^{z_{ij}}$ ，或者， $t'_{lij} = h^{t_{lij}} * g^{z_{ij}}$ ，其中， $t_{lij}$  代表第 i 账本下的第 j 个用户账户的兑换交易份额， $z_{ij}$  代表第 i 账本下的第 j 个用户账户的兑换交易份额隐私秘钥， $t'_{lij}$  代表第 i 账本下的第 j 个第一用户账户的加密兑换交易份额，g 和 h 为基，h 是 g 的一个 n 次方，n 为正整数，i 和 j 为正整数。

步骤 S2，通过第一预设兑换计算公式并基于所述预设兑换率和所述第

一密文，为所述第二账本计算出所述第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥，并生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文。

本实施例中，若确认该交易是将该预设兑换交易份额采用预设兑换率  $e$ （例如，人民币对美元的兑换率是 7，那么  $e=7$ ）进行兑换，则由智能合约通过第一预设兑换计算公式并基于所述预设兑换率  $e$  和第一密文，为第二账本计算出第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥，并在智能合约里面直接生成第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文。例如，所述第一预设交易兑换计算公式为  $t'_{2ij} = (t'_{1ij})^e = (g^{t_{ij}} * h^{z_{ij}})^e$ ， $t'_{2ij} = g^{t_{ij} * e} * h^{z_{ij} * e}$ ，或者， $t'_{2ij} = h^{t_{ij} * e} * g^{z_{ij} * e}$ ，其中， $t_{ij} * e$  代表第  $i$  账本下的第  $j$  个用户账户的兑换交易份额， $z_{ij} * e$  代表第  $i$  账本下的第  $j$  个用户账户的兑换交易份额隐私秘钥， $t'_{2ij}$  代表第  $i$  账本下的第  $j$  个第二用户账户的加密兑换交易份额， $g$  和  $h$  为基， $h$  是  $g$  的一个  $n$  次方， $n$  为正整数， $i$  和  $j$  为正整数。

步骤 S3，基于所述第一密文和第二密文，并按预设规则完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易。

本实施例中，可基于所述第一密文和第二密文完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易。例如，可将预设兑换交易份额按预设兑换率在所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户之间进行转账交易。还可将第一用户在所述第一账本（例如，该第一账本可以是人民币账本）以及所述第二账本（例如，该第二账本可以是美元账本）下的所有用户账户同时进行更新（例如余额更新），将第二用户在所述第一账本（例如，该第一账本可以是人民币账本）以及所述第二账本（例如，该第二账本可以是美元账本）下的所有用户账户同时进行更新（例如余额更新）。例如，如果甲要与乙用人民币兑换美元，则本实施例中甲和乙的人民币和美元的账户可以实现同时更新，完成区块链技术场景下多账本转账的隐私交易。

与现有技术相比，本实施例在区块链中第一账本下第一用户的第一用户账户发起与第二账本下第二用户的第二用户账户将预设兑换交易份额按预设兑换率进行兑换的交易请求后，接收所述第一用户预先为预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成的第一密文；通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，为所述第二账本计算生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文；基于所述第一密文和第二密文，并按预设规则完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易。由于能对第一账本下第一用户账户的预设兑换交易份

额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成第一密文，并为所述第二账本计算生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文，基于所述第一密文和第二密文来完成所述第一账本下第一用户账户与所述第二账本下第二用户账户的交易操作，在交易过程中只有第一用户或第二用户能解密所述第一密文或第二密文以获知交易具体的兑换交易份额数据，区块链上的其他节点无法解读具体的兑换交易份额数据，从而在有效保证区块链技术场景中交易信息安全的情况下，实现多账本转账操作。

在一可选的实施例中，在上述图 1 的实施例的基础上，所述基于区块链的多账本转账系统 10 被所述处理器 12 执行实现所述步骤 S3 时，具体包括：

接收电子签名后的第一密文；所述电子签名后的第一密文为所述第一用户将所述第一密文发给所述第二用户后，若所述第二用户根据所述第一密文确认预设兑换交易份额和预设兑换率，则所述第二用户对所述第一密文进行电子签名生成。将所述电子签名后的第一密文写到区块链的各个节点上的共享资产账本上。本实施例中，第一用户将第一密文发给第二用户；若该第二用户确认该预设兑换交易份额和预设兑换率，则该第二用户对该第一密文进行电子签名，并将电子签名后的第一密文通过该区块链的智能合约写到该区块链的各个节点上的共享资产账本上，或者，该第二用户将电子签名后的第一密文送给该第一用户，供该第一用户将电子签名后的第一密文通过该区块链的智能合约写到该区块链的各个节点上的共享资产账本上。

根据所述第一密文更新所述第一账本下第一用户的第一用户账户的余额和所述第一账本下第二用户的第三账户的余额，并根据所述第二密文更新所述第二账本下第二用户的第二用户账户的余额和所述第二账本下第一用户的第四账户的余额。

本实施例中，在该第一账本（例如，该第一账本可以是人民币账本）下第一用户的第一用户账户发起与第二账本（例如，该第二账本可以是美元账本）下第二用户的第二用户账户的预设交易份额和预设兑换价的交易请求后，该区块链的智能合约根据所述第一密文更新该第一账本下第一用户的第一用户账户的余额和该第一账本下第二用户的第三账户的余额，并根据所述第二密文更新该第二账本下第一用户的第四账户的余额和该第二账本下第二用户的第二用户账户的余额。其中，第一用户账户和第四账户都是第一用户的账户，分别为第一用户在该第一账本和该第二账本下的账户，例如，第一用户账户为第一用户的人民币账本账户，第四账户为第一用户的美元账本账户。第二用户账户和第三账户都是第二用户的账户，分别为第二用户在该第二账本和该第一账本下的账户，例如，第二用户账户为第二用户的美元账本账户，第三账户为第二用户的人民币账本账户。

具体地，所述根据所述第一密文更新该第一账本下第一用户的第一用户账户的余额和该第一账本下第二用户的第三账户的余额的步骤包括：

智能合约根据第一预设余额计算公式在该第一账本下第一用户的第一用户账户的余额中扣除所述预设兑换交易份额,计算出该第一账本下第一用户的第一用户账户的第一新余额,并将计算出的第一新余额更新到共享资产账本上。例如,所述第一预设余额计算公式为  $a_{1ij}'' = a_{1ij}'/t_{1ij}' = (g^{a_{1ij}} * h^{x_{1ij}})/(g^{t_{1ij}} * h^{z_{1ij}}) = g^{(a_{1ij}-t_{1ij})} * h^{(x_{1ij}-z_{1ij})}$ , 或者,  $a_{1ij}'' = h^{(a_{1ij}-t_{1ij})} * g^{(x_{1ij}-z_{1ij})}$ 。其中,  $a_{1ij}$  代表第 i 账本下的第 j 个第一用户账户的余额,  $x_{1ij}$  代表第 i 账本下的第 j 个第一用户账户的余额隐私密钥,  $a_{1ij}''$  代表第 i 账本下的第 j 个第一用户账户的加密新余额, g 和 h 为基, h 是 g 的一个 n 次方, i 和 j 为正整数, “ $a_{1ij}-t_{1ij}$ ”代表第 i 账本下的第 j 个第一用户账户的新余额, “ $x_{1ij}-z_{1ij}$ ”代表第 i 账本下的第 j 个第一用户账户的新混淆余额隐私密钥,  $t_{1ij}$  代表第 i 账本下的第 j 个第一用户账户的交易份额,  $z_{1ij}$  代表第 i 账本下的第 j 个第一用户账户的交易份额隐私密钥。

智能合约根据第二预设余额计算公式在该第一账本下第二用户的第三账户的余额中增加所述预设兑换交易份额,计算出该第一账本下第二用户的第三账户的第二新余额,并将计算出的第二新余额更新到共享资产账本上。例如,所述第二预设余额计算公式为  $a_{3ij}'' = a_{3ij}' * t_{1ij}' = (g^{a_{3ij}} * h^{y_{3ij}}) * (g^{t_{1ij}} * h^{z_{1ij}}) = g^{(a_{3ij}+t_{1ij})} * h^{(y_{3ij}+z_{1ij})}$ , 或者,  $a_{3ij}'' = h^{(a_{3ij}+t_{1ij})} * g^{(y_{3ij}+z_{1ij})}$ ,  $a_{3ij}$  代表第 i 账本下的第 j 个第三账户的余额,  $y_{3ij}$  代表第 i 账本下的第 j 个第三账户的余额隐私密钥,  $a_{3ij}''$  代表第 i 账本下的第 j 个第三账户的加密新余额, g 和 h 为基, h 是 g 的一个 n 次方, i 和 j 为正整数, “ $a_{3ij}+t_{1ij}$ ”代表第 i 账本下的第 j 个第三账户的新余额, “ $y_{3ij}+z_{1ij}$ ”代表第 i 账本下的第 j 个第三账户的新混淆余额隐私密钥,  $t_{1ij}$  代表第 i 账本下的第 j 个第三账户的交易份额,  $z_{1ij}$  代表第 i 账本下的第 j 个第三账户的交易份额隐私密钥。

所述根据所述第二密文更新该第二账本下第一用户的第四账户的余额和该第二账本下第二用户的第二用户账户的余额的步骤包括:

智能合约根据第三预设余额计算公式在该第二账本下第二用户的第二用户账户的余额中扣除所述预设兑换交易份额,计算出该第二账本下第二用户的第二用户账户的第三新余额,并将计算出的第三新余额更新到共享资产账本上。例如,所述第三预设余额计算公式为  $a_{2ij}'' = a_{2ij}'/t_{2ij}' = (g^{a_{2ij}} * h^{x_{2ij}})/(g^{(t_{1ij} * e)} * h^{(z_{1ij} * e)}) = g^{(a_{2ij}-(t_{1ij} * e))} * h^{(x_{2ij}-(z_{1ij} * e))}$ , 或者  $a_{2ij}'' = h^{(a_{2ij}-(t_{1ij} * e))} * g^{(x_{2ij}-(z_{1ij} * e))}$ , 其中,  $a_{2ij}$  代表第 i 账本下的第 j 个第二用户账户的余额,  $x_{2ij}$  代表第 i 账本下的第 j 个第二用户账户的余额隐私密钥,  $a_{2ij}''$  代表第 i 账本下的第 j 个第二用户账户的加密新余额, g 和 h 为基, h 是 g 的一个 n 次方, i 和 j 为正整数, “ $a_{2ij}-(t_{1ij} * e)$ ”代表第 i 账本下的第 j 个第二用户账户的新余额, “ $x_{2ij}-(z_{1ij} * e)$ ”代表第 i 账本下的第 j 个第二用户账户的新混淆余额隐私密钥, “ $t_{1ij} * e$ ”代表第 i 账本下的第 j 个第二用户账户的交易份额, “ $z_{1ij} * e$ ”代表第 i 账本下的第 j 个第二用户账户的交易份额隐私密钥。

智能合约根据第四预设余额计算公式在该第二账本下第一用户的第四账户的余额中增加所述预设兑换交易份额,计算出该第二账本下第一用户的

第四账户的第四新余额，并将计算出的第四新余额更新到共享资产账本上。例如，所述第四预设余额计算公式为  $a_{4ij}'' = a_{4ij}' * t_{2ij}' = (g^{a_{4ij}} * h^{y_{4ij}})^* (g^{(t_{ij} * e)} * h^{(z_{ij} * e)}) = g^{(a_{4ij} + (t_{ij} * e))} * h^{(y_{4ij} + (z_{ij} * e))}$ ，或者， $a_{4ij}'' = h^{(a_{4ij} + (t_{ij} * e))} * g^{(y_{4ij} + (z_{ij} * e))}$ ， $a_{4ij}$  代表第 i 账本下的第 j 个第四账户的余额， $y_{4ij}$  代表第 i 账本下的第 j 个第四账户的余额隐私密钥， $a_{4ij}''$  代表第 i 账本下的第 j 个第四账户的加密新余额，g 和 h 为基，h 是 g 的一个 n 次方，i 和 j 为正整数，“ $a_{4ij} + (t_{ij} * e)$ ”代表第 i 账本下的第 j 个第四账户的新余额，“ $y_{4ij} + (z_{ij} * e)$ ”代表第 i 账本下的第 j 个第四账户的新混淆余额隐私密钥，“ $t_{ij} * e$ ”代表第 i 账本下的第 j 个第四账户的交易份额，“ $z_{ij} * e$ ”代表第 i 账本下的第 j 个第四账户的交易份额隐私密钥。

进一步地，第三预设余额计算公式也可以是在该第一账本下第二用户的第三账户的余额中增加所述预设兑换交易份额，计算出该第一账本下第二用户的第三账户的第二新余额，并将计算出的第二新余额更新到共享资产账本上。第三预设余额计算公式也可以是在该第二账本下第一用户的第四账户的余额中扣除所述预设兑换交易份额，计算出该第二账本下第一用户的第四账户的第四新余额，并将计算出的第四新余额更新到共享资产账本上。

在一可选的实施例中，所述步骤 S2 替换为如下步骤：

接收电子签名后的第一密文和第二密文，并将电子签名后的第一密文和第二密文写到区块链的各个节点上的共享资产账本上；其中，所述电子签名后的第一密文和第二密文的生成过程如下：

由所述第一用户通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，为所述第二账本计算出所述第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私密钥，并生成所述第二账本的加密兑换交易份额及对应的交易份额隐私密钥的第二密文；所述第一用户将所述第一密文和所述第二密文发给所述第二用户；若所述第二用户确认所述预设兑换交易份额和预设兑换率，则所述第二用户对所述第一密文和所述第二密文进行电子签名。

本实施例中，若确认为该预设兑换交易份额采用预设兑换率 e，则由第一用户通过第一预设兑换计算公式并基于所述预设兑换率 e 和第一密文，为第二账本计算出第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私密钥，并生成第二账本的加密兑换交易份额及对应的交易份额隐私密钥的第二密文。该第一用户将第一密文和第二密文发给第二用户。若该第二用户确认该预设兑换交易份额和预设兑换率，则该第二用户对该第一密文和第二密文进行电子签名，并将电子签名后的第一密文和第二密文通过该区块链的智能合约写到该区块链的各个节点上的共享资产账本上，或者，该第二用户将电子签名后的第一密文和第二密文发送给该第一用户，供该第一用户将电子签名后的第一密文和第二密文通过该区块链的智能合约写到该区块链的各个节点上的共享资产账本上。

进一步地,在上述实施例的基础上,本实施例中还可以依此创建第三个,第四个甚至更多账本的同时转账。例如,如果有第三账本需要实时进行份额兑换,可以通过以下几个步骤实现:(1)、在智能合约上设定第三账本与第一账本或与第二账本的兑换额  $f$ ; (2)、由智能合约或第一用户通过第一预设兑换计算公式和兑换额  $f$  计算出需要在第三账本上对应账户的转账额; (3)、在第三账本上设立第五预设余额计算公式和第六预设余额计算公式,通过智能合约增加并扣除对应账户上的份额。

在一具体的实施方式中,以下以账本 1 和账本 2 为例进行举例说明:

步骤一:为每一个账本下每一个用户账户的余额用一种具有加法同态特性的密码公式加密,只有账户的拥有者可以通过自己的“账户隐私秘钥”解密读取自己账户的余额。在此以 Pederson Commitment 以及 ECC (椭圆曲线) 为例进行说明,当然,也不限定采用其他如 RSA、Diffie-Hellman 等。

如可用 Pederson Commitment 代表每个账户,甲账户要用在账本 1 的余额换取账户乙在账本 2 的余额,例如甲用人民币(账本 1)跟乙兑换美元(账本 2),甲会在账本 1 把部分人民币余额转给乙,而乙则会在账本 2 把自己的美元转给甲。对于账本 1,定义  $a_1$ =甲账户账本 1 余额,  $a_1'$ =密码混淆后的甲账户账本 1 余额,  $x_1$ =甲账户账本 1 余额隐私秘钥,则甲账户余额为:  
 $a_1' = g^{a_1} * h^{x_1}$  (椭圆曲线公式为:  $a_1' = a_1G + x_1H$ )。定义  $b_1$ =乙账户人民币余额,  $b_1'$ =密码混淆后的乙账户人民币余额,  $y_1$ =乙账户人民币余额隐私秘钥,则乙账户余额为:  $b_1' = g^{b_1} * h^{y_1}$  (椭圆曲线公式为:  $b_1' = b_1G + y_1H$ )。对于账本 2,定义  $a_2$ =甲账户账本 2 余额,  $a_2'$ =密码混淆后的甲账户账本 2 余额,  $x_2$ =甲账户账本 2 余额隐私秘钥,则甲账户余额为:  $a_2' = g^{a_2} * h^{x_2}$  (椭圆曲线公式为:  $a_2' = a_2G + x_2H$ )。定义  $b_2$ =乙账户人民币余额,  $b_2'$ =密码混淆后的乙账户人民币余额,  $y_2$ =乙账户人民币余额隐私秘钥,则乙账户余额为:  $b_2' = g^{b_2} * h^{y_2}$  (椭圆曲线公式为:  $b_2' = b_2G + y_2H$ )。

步骤二:如果甲要用账本 1 的余额交换乙在账本 2 的余额,甲会创建两个密文,第一个是用加法同态密文保护的账本 1 交易份额,第二个是通过加密混淆的账本 1 与账本 2 的兑换价(如汇率)。

转账发起方(甲)会自行生成第一密文用的同态隐私秘钥和第二密文用的隐私秘钥并将它们和第一密文与第二密文发给交易对方(乙),并在获得乙认可和对第一密文和第二密文数字签名后将整个交易以及乙方的签名发到区块链网络上(乙方数字签名代表对交易份额与兑换率的认可),如发到区块链的智能合约上。如定义  $t$ =账本 1 交易份额,  $t'$ =密码混淆后的交易份额,  $z$ =交易份额隐私秘钥,则第一密文(交易份额)为:  $t' = g^t * h^z$  (椭圆曲线公式为:  $t' = tG + zH$ )。定义  $e$ = 兑换率。

步骤三:区块链在收到交易请求后,会在更新账本 1 的同时更新账本 2,更新账本 2 的步骤有如下三个子步骤:

步骤三 A, 在账本 1 的甲账户余额中扣除交易份额, 并同时在账本 1 的乙账户余额中增加交易份额。甲账户在账本 1 新份额:  $a1'' = a1' / t'$ ,  $a1'' = (g^{a1} * h^{x1}) / (g^t * h^z)$ ,  $a1'' = g^{(a1-t)} * h^{(x1-z)}$  (椭圆曲线公式为:  $a1'' = (a1-t)G + (x1-z)H$ )。甲账户新余额  $a1' = a1 - t$ , 甲账户新混淆隐私秘钥  $x1' = (x1 - z)$ , 乙账户在账本 1 新份额:  $b1'' = b1' * t'$ ,  $b1'' = (g^{b1} * h^{y1}) * (g^t * h^z)$ ,  $b1'' = g^{(b1+t)} * h^{(y1+z)}$  (椭圆曲线公式为:  $b1'' = (b1+t)G + (y1+z)H$ )。乙账户新余额  $b1' = b1 + t$ , 乙账户新混淆隐私秘钥  $y1' = y1 + z$ 。

步骤三 B, 区块链上的智能合约通过交易额 (第一密文) 与兑换率算出需要在账本 2 进行转账操作对应的交易份额。该操作需在不对交易额解密的情况下进行, 第一密文 (交易份额):  $t' = g^t * h^z$  (椭圆曲线公式为:  $t' = tG + zH$ ), 定义交易兑换率:  $e$ 。

在不解密状态下算出甲账户和乙账户在账本 2 转让的份额; 由于  $t$  代表账本 1 交易份额,  $e$  代表兑换率, 所以  $te$  代表账户甲和账户乙在账本 2 的转让份额。则账本 2 交易份额  $t2 = t * e = te$ , 账本 2 交易份额 (密文)  $t2' = (g^t * h^z)^e = (g^{te} * h^{ze})$  (椭圆曲线公式为:  $t2' = (tG + zH) * e = teG + zeH$ )。

步骤三 C, 在账本 2 的甲账户余额中加上交易份额, 并同时在账本 2 乙账户余额中减去交易份额。甲账户在账本 2 新份额:  $a2'' = a2' * t2'$ ,  $a2'' = (g^{a2} * h^{x2}) * (g^{te} * h^{ze})$ ,  $a2'' = g^{(a2+te)} * h^{(x2+ze)}$  (椭圆曲线公式为:  $a2'' = (a2+te)G + (x2+ze)H$ )。甲账户新余额  $a2' = a2 + te$ , 甲账户新混淆隐私秘钥  $x2' = x2 + ze$ 。乙账户在账本 1 新份额:  $b2'' = b2' / t'$ ,  $b2'' = (g^{b2} * h^{y2}) / (g^t * h^z)$ ,  $b2'' = g^{(b2-te)} * h^{(y2-ze)}$  (椭圆曲线公式为:  $b2'' = (b2-te)G + (y2-ze)H$ ), 乙账户新余额  $b2' = b2 - te$ , 乙账户新混淆隐私秘钥  $y2' = y2 - ze$ 。

如图 2 所示, 图 2 为本申请基于区块链的多账本转账方法一实施例的流程示意图, 该基于区块链的多账本转账方法包括以下步骤:

步骤 S10, 若区块链中第一账本下第一用户的第一用户账户发起与第二账本下第二用户的第二用户账户的交易请求, 则接收所述第一用户预先加密生成的第一密文; 所述交易请求为将预设兑换交易份额按预设兑换率进行兑换的请求, 所述第一密文为预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成的第一密文。

本实施例中, 首先由区块链中的用户或者机构将自己在每一个账本下每一个用户账户的余额采用第一预设密码公式及对应的余额隐私秘钥进行加密, 并将自己在每一个账本下每一个用户账户加密后的余额通过区块链的智能合约写到该区块链的各个节点上的共享资产账本上。例如, 采用 Pederson Commitment 算法, 所述第一预设密码公式为  $a'_{ij} = g^{a_{ij}} * h^{x_{ij}}$ , 或者,  $a'_{ij} = h^{a_{ij}} * g^{x_{ij}}$ , 其中,  $a_{ij}$  代表第  $i$  账本下的第  $j$  个用户账户的余额,  $x_{ij}$  代表第  $i$  账本下的第  $j$  个用户账户的余额隐私秘钥,  $a'_{ij}$  代表第  $i$  账本下的第  $j$  个用户账户的加密余额,  $g$  和  $h$  为离散对数问题中的基,  $h = g^c$ ,  $c$  为未知数,  $i$  和  $j$  为正

整数。

在第一账本（例如，该第一账本可以是人民币账本）下第一用户的第一用户账户发起与第二账本（例如，该第二账本可以是美元账本）下第二用户的第二用户账户将预设兑换交易份额按预设兑换率进行兑换（该预设兑换交易份额和该预设兑换率可在智能合约中提前设置）的交易请求之前，由该第一用户为该预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成第一密文。例如，所述第二预设密码公式为  $t'_{1ij}=g^{t_{ij}} * h^{z_{ij}}$ ，或者， $t'_{1ij}=h^{t_{ij}} * g^{z_{ij}}$ ，其中， $t_{ij}$  代表第  $i$  账本下的第  $j$  个用户账户的兑换交易份额， $z_{ij}$  代表第  $i$  账本下的第  $j$  个用户账户的兑换交易份额隐私秘钥， $t'_{1ij}$  代表第  $i$  账本下的第  $j$  个第一用户账户的加密兑换交易份额， $g$  和  $h$  为基， $h$  是  $g$  的一个  $n$  次方， $n$  为正整数， $i$  和  $j$  为正整数。

步骤 S20，通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，为所述第二账本计算出所述第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥，并生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文。

本实施例中，若确认该交易是将该预设兑换交易份额采用预设兑换率  $e$ （例如，人民币对美元的兑换率是 7，那么  $e=7$ ）进行兑换，则由智能合约通过第一预设兑换计算公式并基于所述预设兑换率  $e$  和第一密文，为第二账本计算出第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥，并在智能合约里面直接生成第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文。例如，所述第一预设交易兑换计算公式为  $t'_{2ij}=(t'_{1ij})^e=(g^{t_{ij}} * h^{z_{ij}})^e$ ， $t'_{2ij}=g^{t_{ij}*e} * h^{z_{ij}*e}$ ，或者， $t'_{2ij}=h^{t_{ij}*e} * g^{z_{ij}*e}$ ，其中， $t_{ij}*e$  代表第  $i$  账本下的第  $j$  个用户账户的兑换交易份额， $z_{ij}*e$  代表第  $i$  账本下的第  $j$  个用户账户的兑换交易份额隐私秘钥， $t'_{2ij}$  代表第  $i$  账本下的第  $j$  个第二用户账户的加密兑换交易份额， $g$  和  $h$  为基， $h$  是  $g$  的一个  $n$  次方， $n$  为正整数， $i$  和  $j$  为正整数。

步骤 S30，基于所述第一密文和第二密文，并按预设规则完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易。

本实施例中，可基于所述第一密文和第二密文完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易。例如，可将预设兑换交易份额按预设兑换率在所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户之间进行转账交易。还可将第一用户在所述第一账本（例如，该第一账本可以是人民币账本）以及所述第二账本（例如，该第二账本可以是美元账本）下的所有用户账户同时进行更新（例如余额更新），将第二用户在所述第一账本（例如，该第一账本可以是人民币账本）以及所述第二账本（例如，该第二账本可以是美元账本）下的所有用户账户同时进行更新（例如余额更新）。例如，如果甲要与

乙用人民币兑换美元，则本实施例中甲和乙的人民币和美元的账户可以实现同时更新，完成区块链技术场景下多账本转账的隐私交易。

与现有技术相比，本实施例在区块链中第一账本下第一用户的第一用户  
5 账户发起与第二账本下第二用户的第二用户账户将预设兑换交易份额按预设  
兑换率进行兑换的交易请求后，接收所述第一用户预先为预设兑换交易份  
额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成的第一  
密文；通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，  
10 为所述第二账本计算生成所述第二账本的加密兑换交易份额及对应的交易  
份额隐私秘钥的第二密文；基于所述第一密文和第二密文，并按预设规则完  
成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的  
第二用户账户的交易。由于能对第一账本下第一用户账户的预设兑换交易份  
额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成第一密  
15 文，并为所述第二账本计算生成所述第二账本的加密兑换交易份额及对应的  
交易份额隐私秘钥的第二密文，基于所述第一密文和第二密文来完成所述第  
一账本下第一用户账户与所述第二账本下第二用户账户的交易操作，在交易  
过程中只有第一用户或第二用户能解密所述第一密文或第二密文以获知交  
易具体的兑换交易份额数据，区块链上的其他节点无法解读具体的兑换交易  
20 份额数据，从而在有效保证区块链技术场景中交易信息安全的情况下，实现  
多账本转账操作。

在一可选的实施例中，在上述实施例的基础上，所述步骤 S30 具体包括：

接收电子签名后的第一密文；所述电子签名后的第一密文为所述第一用  
户将所述第一密文发给所述第二用户后，若所述第二用户根据所述第一密文  
25 确认预设兑换交易份额和预设兑换率，则所述第二用户对所述第一密文进行  
电子签名生成。将所述电子签名后的第一密文写到区块链的各个节点上的共  
享资产账本上。本实施例中，第一用户将第一密文发给第二用户；若该第二  
用户确认该预设兑换交易份额和预设兑换率，则该第二用户对该第一密文进  
行电子签名，并将电子签名后的第一密文通过该区块链的智能合约写到该区  
30 块链的各个节点上的共享资产账本上，或者，该第二用户将电子签名后的第  
一密文送给该第一用户，供该第一用户将电子签名后的第一密文通过该区  
块链的智能合约写到该区块链的各个节点上的共享资产账本上。

根据所述第一密文更新所述第一账本下第一用户的第一用户账户的余  
额和所述第一账本下第二用户的第三账户的余额，并根据所述第二密文更新  
35 所述第二账本下第二用户的第二用户账户的余额和所述第二账本下第一用  
户的第四账户的余额。

本实施例中，在该第一账本（例如，该第一账本可以是人民币账本）下  
第一用户的第一用户账户发起与第二账本（例如，该第二账本可以是美元账  
本）下第二用户的第二用户账户的预设交易份额和预设兑换价的交易请求

后,该区块链的智能合约根据所述第一密文更新该第一账本下第一用户的第一用户账户的余额和该第一账本下第二用户的第三账户的余额,并根据所述第二密文更新该第二账本下第一用户的第四账户的余额和该第二账本下第二用户的第二用户账户的余额。其中,第一用户账户和第四账户都是第一用户的账户,分别为第一用户在该第一账本和该第二账本下的账户,例如,第一用户账户为第一用户的人民币账本账户,第四账户为第一用户的美元账本账户。第二用户账户和第三账户都是第二用户的账户,分别为第二用户在该第二账本和该第一账本下的账户,例如,第二用户账户为第二用户的美元账本账户,第三账户为第二用户的人民币账本账户。

具体地,所述根据所述第一密文更新该第一账本下第一用户的第一用户账户的余额和该第一账本下第二用户的第三账户的余额的步骤包括:

智能合约根据第一预设余额计算公式在该第一账本下第一用户的第一用户账户的余额中扣除所述预设兑换交易份额,计算出该第一账本下第一用户的第一用户账户的第一新余额,并将计算出的第一新余额更新到共享资产账本上。例如,所述第一预设余额计算公式为  $a_{lij}'' = a_{lij}' / t_{lij}' = (g^{a_{lij}} * h^{x_{lij}}) / (g^{t_{ij}} * h^{z_{ij}}) = g^{(a_{lij}-t_{ij})} * h^{(x_{lij}-z_{ij})}$ , 或者,  $a_{lij}'' = h^{(a_{lij}-t_{ij})} * g^{(x_{lij}-z_{ij})}$ 。其中,  $a_{lij}$  代表第  $i$  账本下的第  $j$  个第一用户账户的余额,  $x_{lij}$  代表第  $i$  账本下的第  $j$  个第一用户账户的余额隐私密钥,  $a_{lij}''$  代表第  $i$  账本下的第  $j$  个第一用户账户的加密新余额,  $g$  和  $h$  为基,  $h$  是  $g$  的一个  $n$  次方,  $i$  和  $j$  为正整数, “ $a_{lij}-t_{ij}$ ” 代表第  $i$  账本下的第  $j$  个第一用户账户的新余额, “ $x_{lij}-z_{ij}$ ” 代表第  $i$  账本下的第  $j$  个第一用户账户的新混淆余额隐私密钥,  $t_{ij}$  代表第  $i$  账本下的第  $j$  个第一用户账户的交易份额,  $z_{ij}$  代表第  $i$  账本下的第  $j$  个第一用户账户的交易份额隐私密钥。

智能合约根据第二预设余额计算公式在该第一账本下第二用户的第三账户的余额中增加所述预设兑换交易份额,计算出该第一账本下第二用户的第三账户的第二新余额,并将计算出的第二新余额更新到共享资产账本上。例如,所述第二预设余额计算公式为  $a_{3ij}'' = a_{3ij}' * t_{lij}' = (g^{a_{3ij}} * h^{y_{3ij}}) * (g^{t_{ij}} * h^{z_{ij}}) = g^{(a_{3ij}+t_{ij})} * h^{(y_{3ij}+z_{ij})}$ , 或者,  $a_{3ij}'' = h^{(a_{3ij}+t_{ij})} * g^{(y_{3ij}+z_{ij})}$ ,  $a_{3ij}$  代表第  $i$  账本下的第  $j$  个第三账户的余额,  $Y_{3ij}$  代表第  $i$  账本下的第  $j$  个第三账户的余额隐私密钥,  $a_{3ij}''$  代表第  $i$  账本下的第  $j$  个第三账户的加密新余额,  $g$  和  $h$  为基,  $h$  是  $g$  的一个  $n$  次方,  $i$  和  $j$  为正整数, “ $a_{3ij}+t_{ij}$ ” 代表第  $i$  账本下的第  $j$  个第三账户的新余额, “ $y_{3ij}+z_{ij}$ ” 代表第  $i$  账本下的第  $j$  个第三账户的新混淆余额隐私密钥,  $t_{ij}$  代表第  $i$  账本下的第  $j$  个第三账户的交易份额,  $z_{ij}$  代表第  $i$  账本下的第  $j$  个第三账户的交易份额隐私密钥。

所述根据所述第二密文更新该第二账本下第一用户的第四账户的余额和该第二账本下第二用户的第二用户账户的余额的步骤包括:

智能合约根据第三预设余额计算公式在该第二账本下第二用户的第二用户账户的余额中扣除所述预设兑换交易份额,计算出该第二账本下第二用户的第二用户账户的第三新余额,并将计算出的第三新余额更新到共享资产

账本上。例如，所述第三预设余额计算公式为  $a_{2ij}'' = a_{2ij}' / t_{2ij}' = (g^{a_{2ij}} * h^{x_{2ij}}) / (g^{(t_{ij} * e)} * h^{(z_{ij} * e)}) = g^{(a_{2ij} - (t_{ij} * e))} * h^{(x_{2ij} - (z_{ij} * e))}$ ，或者  $a_{2ij}'' = h^{(a_{2ij} - (t_{ij} * e))} * g^{(x_{2ij} - (z_{ij} * e))}$ ，其中， $a_{2ij}$  代表第 i 账本下的第 j 个第二用户账户的余额， $x_{2ij}$  代表第 i 账本下的第 j 个第二用户账户的余额隐私密钥， $a_{2ij}'$  代表第 i 账本下的第 j 个第二用户账户的加密新余额，g 和 h 为基，h 是 g 的一个 n 次方，i 和 j 为正整数，“ $a_{2ij} - (t_{ij} * e)$ ”代表第 i 账本下的第 j 个第二用户账户的新余额，“ $x_{2ij} - (z_{ij} * e)$ ”代表第 i 账本下的第 j 个第二用户账户的新混淆余额隐私密钥，“ $t_{ij} * e$ ”代表第 i 账本下的第 j 个第二用户账户的交易份额，“ $z_{ij} * e$ ”代表第 i 账本下的第 j 个第二用户账户的交易份额隐私密钥。

智能合约根据第四预设余额计算公式在该第二账本下第一用户的第四账户的余额中增加所述预设兑换交易份额，计算出该第二账本下第一用户的第四账户的第四新余额，并将计算出的第四新余额更新到共享资产账本上。例如，所述第四预设余额计算公式为  $a_{4ij}'' = a_{4ij}' * t_{2ij}' = (g^{a_{4ij}} * h^{y_{4ij}}) * (g^{(t_{ij} * e)} * h^{(z_{ij} * e)}) = g^{(a_{4ij} + (t_{ij} * e))} * h^{(y_{4ij} + (z_{ij} * e))}$ ，或者， $a_{4ij}'' = h^{(a_{4ij} + (t_{ij} * e))} * g^{(y_{4ij} + (z_{ij} * e))}$ ， $a_{4ij}$  代表第 i 账本下的第 j 个第四账户的余额， $y_{4ij}$  代表第 i 账本下的第 j 个第四账户的余额隐私密钥， $a_{4ij}'$  代表第 i 账本下的第 j 个第四账户的加密新余额，g 和 h 为基，h 是 g 的一个 n 次方，i 和 j 为正整数，“ $a_{4ij} + (t_{ij} * e)$ ”代表第 i 账本下的第 j 个第四账户的新余额，“ $y_{4ij} + (z_{ij} * e)$ ”代表第 i 账本下的第 j 个第四账户的新混淆余额隐私密钥，“ $t_{ij} * e$ ”代表第 i 账本下的第 j 个第四账户的交易份额，“ $z_{ij} * e$ ”代表第 i 账本下的第 j 个第四账户的交易份额隐私密钥。

进一步地，第三预设余额计算公式也可以是在该第一账本下第二用户的第三账户的余额中增加所述预设兑换交易份额，计算出该第一账本下第二用户的第三账户的第二新余额，并将计算出的第二新余额更新到共享资产账本上。第三预设余额计算公式也可以是在该第二账本下第一用户的第四账户的余额中扣除所述预设兑换交易份额，计算出该第二账本下第一用户的第四账户的第四新余额，并将计算出的第四新余额更新到共享资产账本上。

在一可选的实施例中，所述步骤 S20 可替换为如下步骤：

接收电子签名后的第一密文和第二密文，并将电子签名后的第一密文和第二密文写到区块链的各个节点上的共享资产账本上；其中，所述电子签名后的第一密文和第二密文的生成过程如下：

由所述第一用户通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，为所述第二账本计算出所述第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私密钥，并生成所述第二账本的加密兑换交易份额及对应的交易份额隐私密钥的第二密文；所述第一用户将所述第一密文和所述第二密文发给所述第二用户；若所述第二用户确认所述预设兑换交易份额和预设兑换率，则所述第二用户对所述第一密文和所述第二密文进行电子签名。

本实施例中，若确认为该预设兑换交易份额采用预设兑换率  $e$ ，则由第一用户通过第一预设兑换计算公式并基于所述预设兑换率  $e$  和第一密文，为第二账本计算出第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥，并生成第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文。该第一用户将第一密文和第二密文发给第二用户。若该第二用户确认该预设兑换交易份额和预设兑换率，则该第二用户对该第一密文和第二密文进行电子签名，并将电子签名后的第一密文和第二密文通过该区块链的智能合约写到该区块链的各个节点上的共享资产账本上，或者，该第二用户将电子签名后的第一密文和第二密文发送给该第一用户，供该第一用户将电子签名后的第一密文和第二密文通过该区块链的智能合约写到该区块链的各个节点上的共享资产账本上。

进一步地，在上述实施例的基础上，本实施例中还可以依此创建第三个，第四个甚至更多账本的同时转账。例如，如果有第三账本需要实时进行份额兑换，可以通过以下几个步骤实现：(1)、在智能合约上设定第三账本与第一账本或与第二账本的兑换额  $f$ ；(2)、由智能合约或第一用户通过第一预设兑换计算公式和兑换额  $f$  计算出需要在第三账本上对应账户的转账额；(3)、在第三账本上设立第五预设余额计算公式和第六预设余额计算公式，通过智能合约增加并扣除对应账户上的份额。

在一具体的实施方式中，以下以账本 1 和账本 2 为例进行举例说明：

步骤一：为每一个账本下每一个用户账户的余额用一种具有加法同态特性的密码公式加密，只有账户的拥有者可以通过自己的“账户隐私秘钥”解密读取自己账户的余额。在此以 Pederson Commitment 以及 ECC（椭圆曲线）为例进行说明，当然，也不限定采用其他如 RSA、Diffie-Hellman 等。

如可用 Pederson Commitment 代表每个账户，甲账户要用在账本 1 的余额换取账户乙在账本 2 的余额，例如甲用人民币（账本 1）跟乙兑换美元（账本 2），甲会在账本 1 把部分人民币余额转给乙，而乙则会在账本 2 把自己的美元转给甲。对于账本 1，定义  $a_1$ =甲账户账本 1 余额， $a_1'$ =密码混淆后的甲账户账本 1 余额， $x_1$ =甲账户账本 1 余额隐私秘钥，则甲账户余额为： $a_1' = g^{a_1} * h^{x_1}$ （椭圆曲线公式为： $a_1' = a_1G + x_1H$ ）。定义  $b_1$ =乙账户人民币余额， $b_1'$ =密码混淆后的乙账户人民币余额， $y_1$ =乙账户人民币余额隐私秘钥，则乙账户余额为： $b_1' = g^{b_1} * h^{y_1}$ （椭圆曲线公式为： $b_1' = b_1G + y_1H$ ）。对于账本 2，定义  $a_2$ =甲账户账本 2 余额， $a_2'$ =密码混淆后的甲账户账本 2 余额， $x_2$ =甲账户账本 2 余额隐私秘钥，则甲账户余额为： $a_2' = g^{a_2} * h^{x_2}$ （椭圆曲线公式为： $a_2' = a_2G + x_2H$ ）。定义  $b_2$ =乙账户人民币余额， $b_2'$ =密码混淆后的乙账户人民币余额， $y_2$ =乙账户人民币余额隐私秘钥，则乙账户余额为： $b_2' = g^{b_2} * h^{y_2}$ （椭圆曲线公式为： $b_2' = b_2G + y_2H$ ）。

步骤二：如果甲要用账本 1 的余额交换乙在账本 2 的余额，甲会创建两

个密文，第一个是用加法同态密文保护的账本 1 交易份额，第二个是通过加密混淆的账本 1 与账本 2 的兑换价（如汇率）。

转账发起方（甲）会自行生成第一密文用的同态隐私秘钥和第二密文用的隐私秘钥并将它们和第一密文与第二密文发给交易对方（乙），并在获得乙认可和对第一密文和第二密文数字签名后将整个交易以及乙方的签名发到区块链网络上（乙方数字签名代表对交易份额与兑换率的认可），如发到区块链的智能合约上。如定义  $t$  = 账本 1 交易份额， $t'$  = 密码混淆后的交易份额， $z$  = 交易份额隐私秘钥，则第一密文（交易份额）为： $t' = g^t * h^z$ （椭圆曲线公式为： $t' = tG + zH$ ）。定义  $e$  = 兑换率。

步骤三：区块链在收到交易请求后，会在更新账本 1 的同时更新账本 2，更新账本 2 的步骤有如下三个子步骤：

步骤三 A，在账本 1 的甲账户余额中扣除交易份额，并同时到账本 1 的乙账户余额中增加交易份额。甲账户在账本 1 新份额： $a1'' = a1' / t'$ ， $a1'' = (g^{a1} * h^{x1}) / (g^t * h^z)$ ， $a1'' = g^{(a1-t)} * h^{(x1-z)}$ （椭圆曲线公式为： $a1'' = (a1-t)G + (x1-z)H$ ）。甲账户新余额  $a1'' = a1 - t$ ，甲账户新混淆隐私秘钥  $x1' = (x1 - z)$ ，乙账户在账本 1 新份额： $b1'' = b1' * t'$ ， $b1'' = (g^{b1} * h^{y1}) * (g^t * h^z)$ ， $b1'' = g^{(b1+t)} * h^{(y1+z)}$ （椭圆曲线公式为： $b1'' = (b1+t)G + (y1+z)H$ ）。乙账户新余额  $b1' = b1 + t$ ，乙账户新混淆隐私秘钥  $y1' = y1 + z$ 。

步骤三 B，区块链上的智能合约通过交易额（第一密文）与兑换率算出需要在账本 2 进行转账操作对应的交易份额。该操作需在不对交易额解密的情况下进行，第一密文（交易份额）： $t' = g^t * h^z$ （椭圆曲线公式为： $t' = tG + zH$ ），定义交易兑换率： $e$ 。

在不解密状态下算出甲账户和乙账户在账本 2 转让的份额；由于  $t$  代表账本 1 交易份额， $e$  代表兑换率，所以  $te$  代表账户甲和账户乙在账本 2 的转让份额。则账本 2 交易份额  $t2 = t * e = te$ ，账本 2 交易份额（密文） $t2' = (g^t * h^z)^e = (g^{te} * h^{ze})$ （椭圆曲线公式为： $t2' = (tG + zH) * e = teG + zeH$ ）。

步骤三 C，在账本 2 的甲账户余额中加上交易份额，并同时到账本 2 乙账户余额中减去交易份额。甲账户在账本 2 新份额： $a2'' = a2' * t2'$ ， $a2'' = (g^{a2} * h^{x2}) * (g^{te} * h^{ze})$ ， $a2'' = g^{(a2+te)} * h^{(x2+ze)}$ （椭圆曲线公式为： $a2'' = (a2+te)G + (x2+ze)H$ ）。甲账户新余额  $a2' = a2 + te$ ，甲账户新混淆隐私秘钥  $x2' = x2 + ze$ 。乙账户在账本 1 新份额： $b2'' = b2' / t'$ ， $b2'' = (g^{b2} * h^{y2}) / (g^t * h^z)$ ， $b2'' = g^{(b2-te)} * h^{(y2-ze)}$ （椭圆曲线公式为： $b2'' = (b2-te)G + (y2-ze)H$ ），乙账户新余额  $b2' = b2 - te$ ，乙账户新混淆隐私秘钥  $y2' = y2 - ze$ 。

此外，本申请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有基于区块链的多账本转账系统，所述基于区块链的多账本转账系统可被至少一个处理器执行，以使所述至少一个处理器执行如上述实施例中的基于区块链的多账本转账方法的步骤，该基于区块链的多账本转账方法的步骤 S10、S20、S30 等具体实施过程如上文所述，在此不再赘述。

需要说明的是，在本文中，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、物品或者装置不仅包括那些要素，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、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件来实现，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端设备（可以是手机，计算机，服务器，空调器，或者网络设备等等）执行本申请各个实施例所述的方法。

以上参照附图说明了本申请的优选实施例，并非因此局限本申请的权利范围。上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。另外，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

本领域技术人员不脱离本申请的范围和实质，可以有多种变型方案实现本申请，比如作为一个实施例的特征可用于另一实施例而得到又一实施例。凡在运用本申请的技术构思之内所作的任何修改、等同替换和改进，均应在本申请的权利范围之内。

## 权 利 要 求 书

1. 一种基于区块链的多账本转账方法，应用于电子装置，其特征在于，所述基于区块链的多账本转账方法包括：

5 A、若区块链中第一账本下第一用户的第一用户账户发起与第二账本下第二用户的第二用户账户的交易请求，则接收所述第一用户预先加密生成的第一密文；所述交易请求为将预设兑换交易份额按预设兑换率进行兑换的请求，所述第一密文为预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成的第一密文；

10 B、通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，为所述第二账本计算出所述第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥，并生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文；

15 C、基于所述第一密文和第二密文，并按预设规则完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易。

2. 如权利要求 1 所述的基于区块链的多账本转账方法，其特征在于，所述步骤 C 包括：

20 接收电子签名后的第一密文；所述电子签名后的第一密文为所述第一用户将所述第一密文发给所述第二用户后，若所述第二用户根据所述第一密文确认预设兑换交易份额和预设兑换率，则所述第二用户对所述第一密文进行电子签名生成；

将所述电子签名后的第一密文写到区块链的各个节点上的共享资产账本上；

25 根据所述第一密文更新所述第一账本下第一用户的第一用户账户的余额和所述第一账本下第二用户的第三账户的余额，并根据所述第二密文更新所述第二账本下第二用户的第二用户账户的余额和所述第二账本下第一用户的第四账户的余额。

3. 如权利要求 2 所述的基于区块链的多账本转账方法，其特征在于，所述根据所述第一密文更新所述第一账本下第一用户的第一用户账户的余额和所述第一账本下第二用户的第三账户的余额的步骤包括：

35 根据第一预设余额计算公式在所述第一账本下第一用户的第一用户账户的余额中扣除所述预设兑换交易份额，计算出所述第一账本下第一用户的第一用户账户的第一新余额，并将计算出的第一新余额更新到共享资产账本上；

根据第二预设余额计算公式在所述第一账本下第二用户的第三账户的余额中增加所述预设兑换交易份额，计算出所述第一账本下第二用户的第三账户的第二新余额，并将计算出的第二新余额更新到共享资产账本上。

4. 如权利要求 2 所述的基于区块链的多账本转账方法, 其特征在于, 所述根据所述第二密文更新所述第二账本下第二用户的第二用户账户的余额和所述第二账本下第一用户的第四账户的余额的步骤包括:

5 根据第三预设余额计算公式在所述第二账本下第二用户的第二用户账户的余额中扣除所述预设兑换交易份额, 计算出所述第二账本下第二用户的第二用户账户的第三新余额, 并将计算出的第三新余额更新到共享资产账本上;

10 根据第四预设余额计算公式在所述第二账本下第一用户的第四账户的余额中增加所述预设兑换交易份额, 计算出所述第二账本下第一用户的第四账户的第四新余额, 并将计算出的第四新余额更新到共享资产账本上。

5. 如权利要求 3 所述的基于区块链的多账本转账方法, 其特征在于, 所述根据所述第二密文更新所述第二账本下第二用户的第二用户账户的余额和所述第二账本下第一用户的第四账户的余额的步骤包括:

15 根据第三预设余额计算公式在所述第二账本下第二用户的第二用户账户的余额中扣除所述预设兑换交易份额, 计算出所述第二账本下第二用户的第二用户账户的第三新余额, 并将计算出的第三新余额更新到共享资产账本上;

20 根据第四预设余额计算公式在所述第二账本下第一用户的第四账户的余额中增加所述预设兑换交易份额, 计算出所述第二账本下第一用户的第四账户的第四新余额, 并将计算出的第四新余额更新到共享资产账本上。

25 6. 如权利要求 4 或 5 所述的基于区块链的多账本转账方法, 其特征在于, 所述第三预设余额计算公式还用于在所述第一账本下第二用户的第三账户的余额中增加所述预设兑换交易份额, 计算出所述第一账本下第二用户的第三账户的第二新余额; 或者, 所述第三预设余额计算公式还用于在所述第二账本下第一用户的第四账户的余额中扣除所述预设兑换交易份额, 计算出所述第二账本下第一用户的第四账户的第四新余额。

7. 如权利要求 1 所述的基于区块链的多账本转账方法, 其特征在于, 所述步骤 B 替换为如下步骤:

30 接收电子签名后的第一密文和第二密文, 并将电子签名后的第一密文和第二密文写到区块链的各个节点上的共享资产账本上; 其中, 所述电子签名后的第一密文和第二密文的生成过程如下:

35 由所述第一用户通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文, 为所述第二账本计算出所述第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥, 并生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文; 所述第一用户将所述第一密文和所述第二密文发给所述第二用户; 若所述第二用户确认所述预设兑换交易份额和预设兑换率, 则所述第二用户对所述第一密文和所述第二密文进行电子签名。

8. 一种电子装置, 其特征在于, 所述电子装置包括存储器、处理器, 所

述存储器上存储有可在所述处理器上运行的基于区块链的多账本转账系统，所述基于区块链的多账本转账系统被所述处理器执行时实现如下步骤：

若区块链中第一账本下第一用户的第一用户账户发起与第二账本下第二用户的第二用户账户的交易请求，则接收所述第一用户预先加密生成的第一密文；所述交易请求为将预设兑换交易份额按预设兑换率进行兑换的请求，所述第一密文为预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成的第一密文；

通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，为所述第二账本计算出所述第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥，并生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文；

基于所述第一密文和第二密文，并按预设规则完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易。

9. 如权利要求 8 所述的电子装置，其特征在于，所述基于所述第一密文和第二密文，并按预设规则完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易的步骤包括：

接收电子签名后的第一密文；所述电子签名后的第一密文为所述第一用户将所述第一密文发给所述第二用户后，若所述第二用户根据所述第一密文确认预设兑换交易份额和预设兑换率，则所述第二用户对所述第一密文进行电子签名生成；

将所述电子签名后的第一密文写到区块链的各个节点上的共享资产账本上；

根据所述第一密文更新所述第一账本下第一用户的第一用户账户的余额和所述第一账本下第二用户的第三账户的余额，并根据所述第二密文更新所述第二账本下第二用户的第二用户账户的余额和所述第二账本下第一用户的第四账户的余额。

10. 如权利要求 9 所述的电子装置，其特征在于，所述根据所述第一密文更新所述第一账本下第一用户的第一用户账户的余额和所述第一账本下第二用户的第三账户的余额的步骤包括：

根据第一预设余额计算公式在所述第一账本下第一用户的第一用户账户的余额中扣除所述预设兑换交易份额，计算出所述第一账本下第一用户的第一用户账户的第一新余额，并将计算出的第一新余额更新到共享资产账本上；

根据第二预设余额计算公式在所述第一账本下第二用户的第三账户的余额中增加所述预设兑换交易份额，计算出所述第一账本下第二用户的第三账户的第二新余额，并将计算出的第二新余额更新到共享资产账本上。

11. 如权利要求 9 所述的电子装置，其特征在于，所述根据所述第二密文更新所述第二账本下第二用户的第二用户账户的余额和所述第二账本下第一用户的第四账户的余额的步骤包括：

根据第三预设余额计算公式在所述第二账本下第二用户的第二用户账户的余额中扣除所述预设兑换交易份额，计算出所述第二账本下第二用户的第二用户账户的第三新余额，并将计算出的第三新余额更新到共享资产账本上；

5 根据第四预设余额计算公式在所述第二账本下第一用户的第四账户的余额中增加所述预设兑换交易份额，计算出所述第二账本下第一用户的第四账户的第四新余额，并将计算出的第四新余额更新到共享资产账本上。

12. 如权利要求 10 所述的电子装置，其特征在于，所述根据所述第二密文更新所述第二账本下第二用户的第二用户账户的余额和所述第二账本下  
10 第一用户的第四账户的余额的步骤包括：

根据第三预设余额计算公式在所述第二账本下第二用户的第二用户账户的余额中扣除所述预设兑换交易份额，计算出所述第二账本下第二用户的第二用户账户的第三新余额，并将计算出的第三新余额更新到共享资产账本上；

15 根据第四预设余额计算公式在所述第二账本下第一用户的第四账户的余额中增加所述预设兑换交易份额，计算出所述第二账本下第一用户的第四账户的第四新余额，并将计算出的第四新余额更新到共享资产账本上。

13. 如权利要求 11 或 12 所述的电子装置，其特征在于，所述第三预设余额计算公式还用于在所述第一账本下第二用户的第三账户的余额中增加  
20 所述预设兑换交易份额，计算出所述第一账本下第二用户的第三账户的第二新余额；或者，所述第三预设余额计算公式还用于在所述第二账本下第一用户的第四账户的余额中扣除所述预设兑换交易份额，计算出所述第二账本下第一用户的第四账户的第四新余额。

14. 如权利要求 8 所述的电子装置，其特征在于，所述通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，为所述第二账本计算出  
25 所述第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥，并生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文的步骤可替换为如下步骤：

接收电子签名后的第一密文和第二密文，并将电子签名后的第一密文和  
30 第二密文写到区块链的各个节点上的共享资产账本上；其中，所述电子签名后的第一密文和第二密文的生成过程如下：

由所述第一用户通过第一预设兑换计算公式并基于所述预设兑换率和  
所述第一密文，为所述第二账本计算出所述第二账本的兑换交易份额、加密  
兑换交易份额及对应的交易份额隐私秘钥，并生成所述第二账本的加密兑换  
35 交易份额及对应的交易份额隐私秘钥的第二密文；所述第一用户将所述第一密文和所述第二密文发给所述第二用户；若所述第二用户确认所述预设兑换交易份额和预设兑换率，则所述第二用户对所述第一密文和所述第二密文进行电子签名。

15. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质

上存储有基于区块链的多账本转账系统，所述基于区块链的多账本转账系统被处理器执行时实现如下步骤：

若区块链中第一账本下第一用户的第一用户账户发起与第二账本下第二用户的第二用户账户的交易请求，则接收所述第一用户预先加密生成的第一密文；所述交易请求为将预设兑换交易份额按预设兑换率进行兑换的请求，所述第一密文为预设兑换交易份额采用第二预设密码公式及对应的交易份额隐私秘钥进行加密生成的第一密文；

通过第一预设兑换计算公式并基于所述预设兑换率和所述第一密文，为所述第二账本计算出所述第二账本的兑换交易份额、加密兑换交易份额及对应的交易份额隐私秘钥，并生成所述第二账本的加密兑换交易份额及对应的交易份额隐私秘钥的第二密文；

基于所述第一密文和第二密文，并按预设规则完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易。

16. 如权利要求 15 所述的计算机可读存储介质，其特征在于，所述基于所述第一密文和第二密文，并按预设规则完成所述第一账本下第一用户的第一用户账户与所述第二账本下第二用户的第二用户账户的交易的步骤包括：

接收电子签名后的第一密文；所述电子签名后的第一密文为所述第一用户将所述第一密文发给所述第二用户后，若所述第二用户根据所述第一密文确认预设兑换交易份额和预设兑换率，则所述第二用户对所述第一密文进行电子签名生成；

将所述电子签名后的第一密文写到区块链的各个节点上的共享资产账本上；

根据所述第一密文更新所述第一账本下第一用户的第一用户账户的余额和所述第一账本下第二用户的第三账户的余额，并根据所述第二密文更新所述第二账本下第二用户的第二用户账户的余额和所述第二账本下第一用户的第四账户的余额。

17. 如权利要求 16 所述的计算机可读存储介质，其特征在于，所述根据所述第一密文更新所述第一账本下第一用户的第一用户账户的余额和所述第一账本下第二用户的第三账户的余额的步骤包括：

根据第一预设余额计算公式在所述第一账本下第一用户的第一用户账户的余额中扣除所述预设兑换交易份额，计算出所述第一账本下第一用户的第一用户账户的第一新余额，并将计算出的第一新余额更新到共享资产账本上；

根据第二预设余额计算公式在所述第一账本下第二用户的第三账户的余额中增加所述预设兑换交易份额，计算出所述第一账本下第二用户的第三账户的第二新余额，并将计算出的第二新余额更新到共享资产账本上。

18. 如权利要求 16 所述的计算机可读存储介质，其特征在于，所述根据所述第二密文更新所述第二账本下第二用户的第二用户账户的余额和所述第二账本下第一用户的第四账户的余额的步骤包括：

根据第三预设余额计算公式在所述第二账本下第二用户的第二用户账户的余额中扣除所述预设兑换交易份额，计算出所述第二账本下第二用户的第二用户账户的第三新余额，并将计算出的第三新余额更新到共享资产账本上；

- 5       根据第四预设余额计算公式在所述第二账本下第一用户的第四账户的余额中增加所述预设兑换交易份额，计算出所述第二账本下第一用户的第四账户的第四新余额，并将计算出的第四新余额更新到共享资产账本上。

19. 如权利要求 17 所述的计算机可读存储介质，其特征在于，所述根据所述第二密文更新所述第二账本下第二用户的第二用户账户的余额和所述  
10       第二账本下第一用户的第四账户的余额的步骤包括：

根据第三预设余额计算公式在所述第二账本下第二用户的第二用户账户的余额中扣除所述预设兑换交易份额，计算出所述第二账本下第二用户的第二用户账户的第三新余额，并将计算出的第三新余额更新到共享资产账本上；

- 15       根据第四预设余额计算公式在所述第二账本下第一用户的第四账户的余额中增加所述预设兑换交易份额，计算出所述第二账本下第一用户的第四账户的第四新余额，并将计算出的第四新余额更新到共享资产账本上。

20. 如权利要求 18 或 19 所述的计算机可读存储介质，其特征在于，所述第三预设余额计算公式还用于在所述第一账本下第二用户的第三账户的  
20       余额中增加所述预设兑换交易份额，计算出所述第一账本下第二用户的第三账户的第二新余额；或者，所述第三预设余额计算公式还用于在所述第二账本下第一用户的第四账户的余额中扣除所述预设兑换交易份额，计算出所述第二账本下第一用户的第四账户的第四新余额。

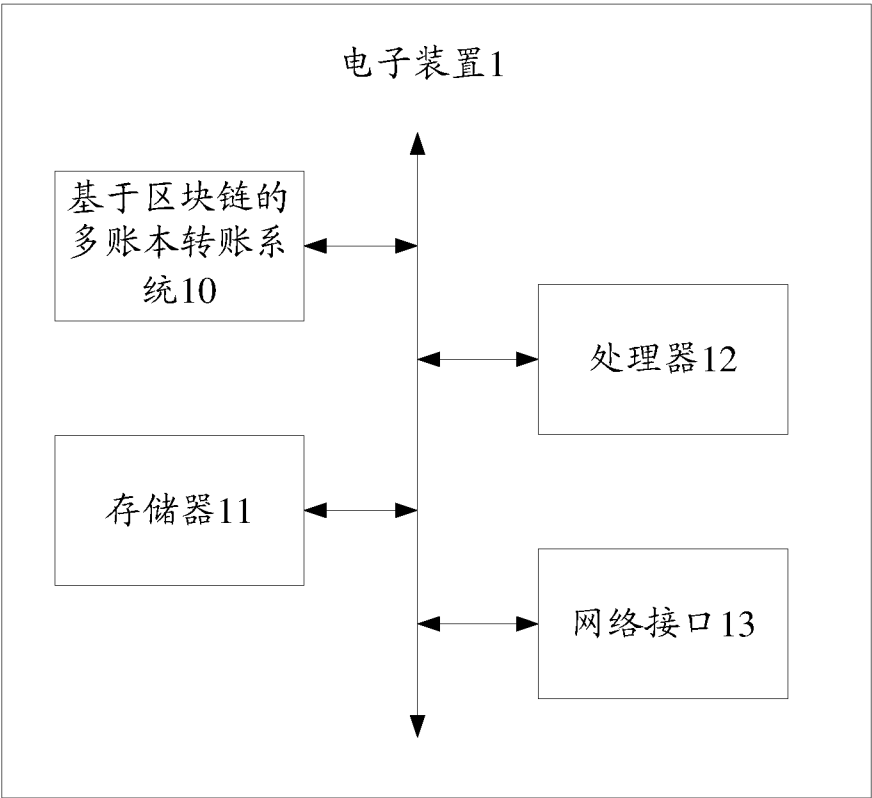


图 1

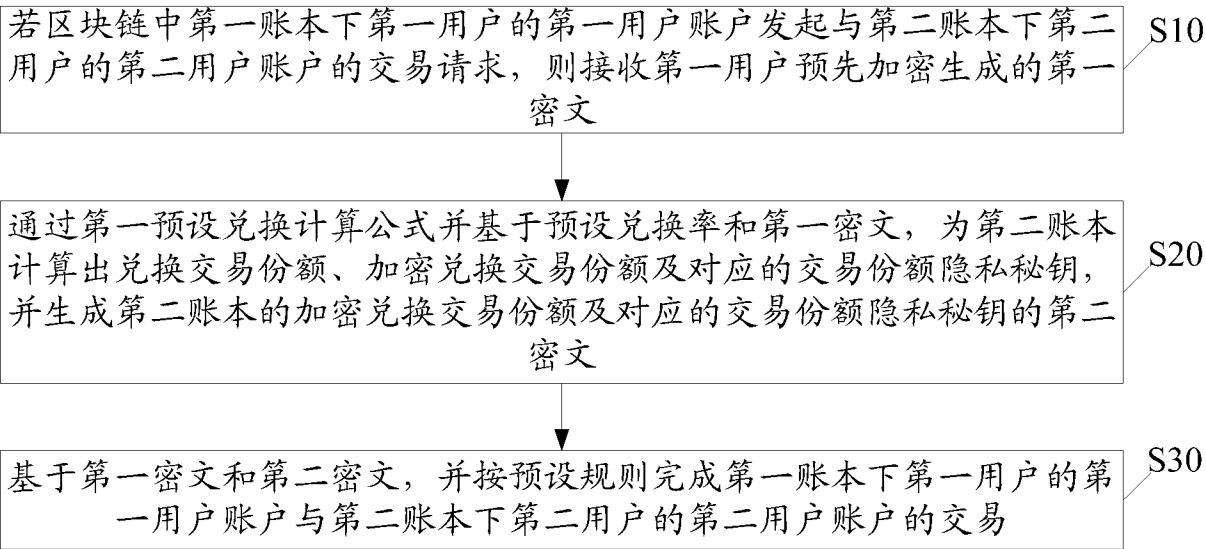


图 2

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/075881

**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

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: 区块链 账本 账户 用户 交易 兑换 数字签名 数字证书 密钥 私钥 加密 密文 block chain blockchain multi book user account transact+ exchange trading digital signature certificate DC private key encrypt+ ciphertext cryptograph

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                                 | Relevant to claim No. |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| X         | CN 107077675 A (SHENZHEN QIANHAI CLOUDMINDS TECHNOLOGY CO., LTD.) 18 August 2017 (2017-08-18)<br>description, paragraphs [0048]-[0130], and figures 1-6            | 1-20                  |
| A         | CN 106960388 A (BANKNOTE CREDIT CARD INDUSTRY DEVELOPMENT CO., LTD. BEIJING SMART CARD TECHNOLOGY RESEARCH INSTITUTE) 18 July 2017 (2017-07-18)<br>entire document | 1-20                  |
| A         | CN 107240001 A (BEIJING HUITONG JINCAI INFORMATION TECHNOLOGY CO., LTD. ET AL.) 10 October 2017 (2017-10-10)<br>entire document                                    | 1-20                  |
| A         | CN 105681301 A (HANGZHOU COMPLEX BEAUTY TECHNOLOGY CO., LTD.) 15 June 2016 (2016-06-15)<br>entire document                                                         | 1-20                  |
| A         | WO 2017000061 A1 (ROYAL BANK OF CANADA) 05 January 2017 (2017-01-05)<br>entire document                                                                            | 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

“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

“&amp;” document member of the same patent family

Date of the actual completion of the international search

20 August 2018

Date of mailing of the international search report

10 September 2018

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China  
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/CN2018/075881**

| Patent document<br>cited in search report |            |    | Publication date<br>(day/month/year) | Patent family member(s) |             |    | Publication date<br>(day/month/year) |
|-------------------------------------------|------------|----|--------------------------------------|-------------------------|-------------|----|--------------------------------------|
| CN                                        | 107077675  | A  | 18 August 2017                       | WO                      | 2018120057  | A1 | 05 July 2018                         |
| CN                                        | 106960388  | A  | 18 July 2017                         | None                    |             |    |                                      |
| CN                                        | 107240001  | A  | 10 October 2017                      | None                    |             |    |                                      |
| CN                                        | 105681301  | A  | 15 June 2016                         | None                    |             |    |                                      |
| WO                                        | 2017000061 | A1 | 05 January 2017                      | US                      | 2016210626  | A1 | 21 July 2016                         |
|                                           |            |    |                                      | WO                      | 2016115620  | A1 | 28 July 2016                         |
|                                           |            |    |                                      | CN                      | 107408253   | A  | 28 November 2017                     |
|                                           |            |    |                                      | CA                      | 2991073     | A1 | 05 January 2017                      |
|                                           |            |    |                                      | CA                      | 2974151     | A1 | 28 July 2016                         |
|                                           |            |    |                                      | EP                      | 3317833     | A1 | 09 May 2018                          |
|                                           |            |    |                                      | AU                      | 2016208989  | A1 | 03 August 2017                       |
|                                           |            |    |                                      | EP                      | 3248159     | A1 | 29 November 2017                     |
|                                           |            |    |                                      | AU                      | 2016287789  | A1 | 01 February 2018                     |
|                                           |            |    |                                      | KR                      | 20180026498 | A  | 12 March 2018                        |

## 国际检索报告

国际申请号

PCT/CN2018/075881

|                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                              |                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------------------------|
| <b>A. 主题的分类</b><br>G06Q 20/38 (2012.01) i<br><br>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>B. 检索领域</b><br>检索的最低限度文献 (标明分类系统和分类号)<br>G06Q<br><br>包含在检索领域中的除最低限度文献以外的检索文献<br><br>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))<br>WPI, EPDOC, CNPAT, CNKI: 区块链 账本 账户 用户 交易 兑换 数字签名 数字证书 密钥 私钥 加密 密文 block chain<br>blockchain multi book user account transact+ exchange trading digital signature certificate DC private<br>key encrypt+ ciphertext cryptograph                                   |                                                                                              |                                  |
| <b>C. 相关文件</b>                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                              |                                  |
| 类 型*                                                                                                                                                                                                                                                                                                                                                                                              | 引用文件, 必要时, 指明相关段落                                                                            | 相关的权利要求                          |
| X                                                                                                                                                                                                                                                                                                                                                                                                 | CN 107077675 A (深圳前海达闼云端智能科技有限公司) 2017年 8月 18日 (2017 - 08 - 18)<br>说明书第[0048]-[0130]段, 附图1-6 | 1-20                             |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | 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)<br>全文                 | 1-20                             |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | CN 107240001 A (北京汇通金财信息科技有限公司 等) 2017年 10月 10日 (2017 - 10 - 10)<br>全文                       | 1-20                             |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | CN 105681301 A (杭州复杂美科技有限公司) 2016年 6月 15日 (2016 - 06 - 15)<br>全文                             | 1-20                             |
| A                                                                                                                                                                                                                                                                                                                                                                                                 | WO 2017000061 A1 (ROYAL BANK OF CANADA) 2017年 1月 5日 (2017 - 01 - 05)<br>全文                   | 1-20                             |
| <input type="checkbox"/> 其余文件在C栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。                                                                                                                                                                                                                                                                                                              |                                                                                              |                                  |
| * 引用文件的具体类型:<br>“A” 认为不特别相关的表示了现有技术一般状态的文件<br>“E” 在国际申请日的当天或之后公布的在先申请或专利<br>“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)<br>“O” 涉及口头公开、使用、展览或其他方式公开的文件<br>“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<br>“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<br>“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<br>“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<br>“&” 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 8月 20日                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                              | 2018年 9月 10日                     |
| ISA/CN的名称和邮寄地址                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                              | 受权官员                             |
| 中华人民共和国国家知识产权局 (ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10) 62019451                                                                                                                                                                                                                                                                                                                       |                                                                                              | 李婷婷<br><br>电话号码 86-(10)-53961728 |

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2018/075881

| 检索报告引用的专利文件 |            |    | 公布日<br>(年/月/日) | 同族专利 |             |    | 公布日<br>(年/月/日) |
|-------------|------------|----|----------------|------|-------------|----|----------------|
| CN          | 107077675  | A  | 2017年 8月 18日   | WO   | 2018120057  | A1 | 2018年 7月 5日    |
| CN          | 106960388  | A  | 2017年 7月 18日   | 无    |             |    |                |
| CN          | 107240001  | A  | 2017年 10月 10日  | 无    |             |    |                |
| CN          | 105681301  | A  | 2016年 6月 15日   | 无    |             |    |                |
| WO          | 2017000061 | A1 | 2017年 1月 5日    | US   | 2016210626  | A1 | 2016年 7月 21日   |
|             |            |    |                | WO   | 2016115620  | A1 | 2016年 7月 28日   |
|             |            |    |                | CN   | 107408253   | A  | 2017年 11月 28日  |
|             |            |    |                | CA   | 2991073     | A1 | 2017年 1月 5日    |
|             |            |    |                | CA   | 2974151     | A1 | 2016年 7月 28日   |
|             |            |    |                | EP   | 3317833     | A1 | 2018年 5月 9日    |
|             |            |    |                | AU   | 2016208989  | A1 | 2017年 8月 3日    |
|             |            |    |                | EP   | 3248159     | A1 | 2017年 11月 29日  |
|             |            |    |                | AU   | 2016287789  | A1 | 2018年 2月 1日    |
|             |            |    |                | KR   | 20180026498 | A  | 2018年 3月 12日   |