

基于区块链的零知识多账本兑换转账方法、装置及存储介质

优先权申明

本申请基于巴黎公约申明享有 2018 年 01 月 24 日递交的申请号为 CN 2018100672929、名称为“基于区块链的零知识多账本兑换转账方法、装置及存储介质”中国专利申请的优先权，该中国专利申请的整体内容以参考的方式结合在本申请中。

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零知识多账本兑换转账方法、装置及存储介质。

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，且在一些场景下还要在能证明多个账本的转账交易是在一个提前设置的合法兑换率域内但第三方无法得知具体兑换率的情况下，来实现多账本转账操作，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。

发明内容

本申请的目的在于提供一种基于区块链的零知识多账本兑换转账方法、装置及存储介质，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，本申请第一方面提供一种基于区块链的零知识多账本兑换转账方法，应用于电子装置，所述基于区块链的零知识多账本兑换转账方法包括：

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、获取数字签名后的第一密文及第一校验密文；所述第一校验密文由所述第一用户通过第一预设兑换计算公式及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加密兑换交易份额，并在所述第二账本的加密兑换交易份额上利用预设的附加隐私参数生成第一校验密文；

C、通过预先设置的若干合法兑换率数值和所述第一密文计算出各个对应的第一验证值密文；并利用各个所述第一验证值密文与所述第一校验密文算出用于验证所述第一账本与所述第二账本交易的预设兑换率是否在预先设置的合法兑

换率数值范围之内的第二验证值密文；

D、若利用所述第二验证值密文证明所述第一账本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内，则基于所述第一密文和所述第一校验密文，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，本申请第二方面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零知识多账本兑换转账系统，所述基于区块链的零知识多账本兑换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；

获取数字签名后的第一密文及第一校验密文；所述第一校验密文由所述第一用户通过第一预设兑换计算公式及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加密兑换交易份额，并在所述第二账本的加密兑换交易份额上利用预设的附加隐私参数生成第一校验密文；

通过预先设置的若干合法兑换率数值和所述第一密文计算出各个对应的第一验证值密文；并利用各个所述第一验证值密文与所述第一校验密文算出用于验证所述第一账本与所述第二账本交易的预设兑换率是否在预先设置的合法兑换率数值范围之内的第二验证值密文；

若利用所述第二验证值密文证明所述第一账本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内，则基于所述第一密文和所述第一校验密文，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，本申请第三方面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零知识多账本兑换转账系统，所述基于区块链的零知识多账本兑换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的基于区块链的零知识多账本兑换转账方法的步骤。

本申请提出的基于区块链的零知识多账本兑换转账方法、装置及存储介质，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，并在所述第二账本的加密兑换交易份额上利用预设的附加隐私参数生成第一校验密文。通过预先设置的若干合法兑换率数值和所述第一密文计算出各个对应的第一验证值密文；并利用各个所述第一验证值密文与所述第一校验密文算出第二验证值密文；若利用所述第二验证值密文证明所述第一账本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内，则基于所述第一密文和所述第一校验密文，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，在交易过程中区块链上的其他节点无法解读具体的兑换交易份额数据，从而有效保证区块链技术场景中交易信息安全。而且，由于在所述第二账本的加密兑换交易份额上利用预设的附加隐私参数生成第一校验密文，该附加隐私参数使得第三方无法得知具体兑换率，同时，通过第二验证值密文可验证所述第一账本与所述第二账本交易的预设兑换率是否在预先设置的合法兑换率数值范围之内。从而在有效保证区块链技术场景中交易信息安全、且能证明多个账本的转账交易是在一个提前设置的合法兑换率域内但第三方无法得知具体兑换率的情况下，实现多账本转账操作。

附图说明

图1为本申请基于区块链的零知识多账本兑换转账系统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零知识多账本兑换转账方法一实施例的流程示意图。

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零知识多账本兑换转账系统。请参阅图1，是本申请基于区块链的零知识多账本兑换转账系统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零知识多账本兑换转账系统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、电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零知识多账本兑换转账系统 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零知识多账本兑换转账系统 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。

基于区块链的零知识多账本兑换转账系统 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,上述基于区块链的零知识多账本兑换转账系统 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。

同时,在区块链智能合约创建时预先设置合法兑换率数值。例如,合法兑换率数值可以记为: $e1, e2, e3, e4, \dots$; 在区块链智能合约创建时可以为多个账本预先设置两两之间的合法兑换率,如人民币账本和美元账本之间的合法兑换率只能是 6.7, 6.8, 6.9, 7.0, ...等。

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 $t'_{lij} = g^{t_{lij}} * h^{z_{lij}}$, 或者, $t'_{lij} = h^{t_{lij}} * g^{z_{lij}}$, 其中, t_{lij} 代表第 i 账本下的第 j 个第一用户账户的兑换交易份额, z_{lij} 代表第 i 账本下的第 j 个第一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, 获取数字签名后的第一密文及第一校验密文; 所述第一校验密文

由所述第一用户通过第一预设兑换计算公式及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加密兑换交易份额,并在所述第二账本的加密兑换交易份额上利用预设的附加隐私参数生成第一校验密文。

本实施例中,若为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加密兑换交易份额,并在第二账本的加密兑换交易份额上加上一个附加隐私参数生成第一校验密文,该附加隐私参数为一个隐私公钥,只有交易方知道与该附加隐私参数对应的附加隐私密钥。在第二账本的加密兑换交易份额上加上一个附加隐私参数生成第一校验密文的作用是让第三方可以检验第二账本加密交易份额是在合法交易范围内,但第三方无法得知具体兑换率。

例如,所述第一预设交易兑换计算公式为 $t'_{2ij} = h^{z_{2ij}} * (t'_{1ij})^e = h^{z_{2ij}} * (g^{t_{1ij}} * h^{z_{1ij}})^e = g^{t_{1ij} * e} * h^{z_{1ij} * e * z_{2ij}}$,或者, $t'_{2ij} = h^{t_{1ij} * e} * g^{z_{1ij} * e * z_{2ij}}$,其中, $t_{1ij} * e$ 代表第 i 账本下的第 j 个第二用户账户的兑换交易份额, $z_{1ij} * e$ 代表第 i 账本下的第 j 个第二用户账户的兑换交易份额附加隐私密钥, z_{2ij} 代表第 i 账本下的第 j 个第二用户账户的兑换交易份额附加隐私密钥, 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,通过预先设置的若干合法兑换率数值和所述第一密文计算出各个对应的第一验证值密文;并利用各个所述第一验证值密文与所述第一校验密文算出用于验证所述第一账本与所述第二账本交易的预设兑换率是否在预先设置的合法兑换率数值范围之内的第二验证值密文。

第一用户将第一密文、第一校验密文数字签名后发给第二用户,当获得第二用户对交易份额认同和数字签名后,第一用户将第一密文和第一校验密文发布到区块链网络上的各个节点上,并由区块链网络上的智能合约通过预先设置的所有合法兑换率($e_1, e_2, e_3, e_4, \dots$)和第一密文计算出各个合理第二账本更新数值(即各个合法兑换率对应的第二账本更新数值)对应的第一验证值密文,其中,第一验证值密文与第一校验密文的不同在于所有第一验证值密文都不含有附加隐私参数。此外,第一用户将第一密文、第一校验密文数字签名后发给第二用户后,第二用户对交易份额认同和数字签名后可以直接发布到区块链网络上的各个节点上。

智能合约用各个第一验证值密文与第一校验密文算出验证第一账本与第二账本的交易份额兑换率是否在预先设置的合理兑换率数值之内的第二验证值密文。需要说明的是:每一个第二验证值密文都等同于一个公钥,若第一用户或第二用户要证明第一校验密文在合法兑换范围内,则第一或第二用户必须有对应这个第二验证值密文(公钥)的一个私钥。如果第一校验密文确实在合法兑换范围内,那么第二验证值密文(公钥)就是已知附加到第一校验密文中的附加隐私参数,与第二验证值密文(公钥)对应的私钥就是与第一校验密文中的附加隐私参数(公钥)对应的私钥。

步骤 S4,若利用所述第二验证值密文证明所述第一账本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内,则基于所述第一密文和所述第一校验密文,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,可通过预设的环签名或 Range Proof 验证方式证明所述第一账

本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内。例如，在一种可选的实施方式中，当智能合约上呈现与所有第二账本合法交易份额对应的第二验证值密文（公钥）后，第一用户或第二用户通过所述第一校验密文（公钥）验证通过第一校验密文加密的加密份额是在预设合理交易范围内的数字，则证明所述第一账本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内。

在另一种可选的实施方式中，第一校验密文对应第一密文的合理范围未必是交易兑换率，第一密文和第一校验密文也可以各自代表一个数字（如日期），可以用上述算法检测第一密文代表的数字与第一校验密文代表的数字的相差是否在一个提前预设的范围内，来证明第一校验密文是在预先设置的合理兑换率数值之内，进而证明所述第一账本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内。

若第一校验密文被证明在预先设置的合理兑换率数值之内，则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二用户账户的余额，并根据所述第一校验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。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，并在所述第二账本的加密兑换交易份额上利用预设的附加隐私参数生成第一校验密文。通过预先设置的若干合法兑换率数值和所述第一密文计算出各个对应的第一验证值密文；并利用各个所述第一验证值密文与所述第一校验密文算出第二验证值密文；若利用所述第二验证值密文证明所述第一账本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内，则基于所述第一密文和所述第一校验密文，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，在交易过程中区块链上的其他节点无法解读具体的兑换交易份额数据，从而有效保证区块链技术场景中交易信息安全。而且，由于在所述第二账本的加密兑换交易份额上利用预设的附加隐私参数生成

第一校验密文, 该附加隐私参数使得第三方无法得知具体兑换率, 同时, 通过第二验证值密文可验证所述第一账本与所述第二账本交易的预设兑换率是否在预先设置的合法兑换率数值范围之内。从而在有效保证区块链技术场景中交易信息安全、且能证明多个账本的转账交易是在一个提前设置的合法兑换率域内但第三方无法得知具体兑换率的情况下, 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, 所述基于区块链的零知识多账本兑换转账系统 10 被所述处理器 12 执行实现所述步骤 S4 时, 具体包括:

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, 并根据所述第一校验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合法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, 并根据所述第一校验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, “ $a_{3ij} + t_{ij}$ ”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。

所述根据所述第一校验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 $a_{2ij}' = a_{2ij} / t_{2ij} = (g^{a_{2ij}} * h^{x_{2ij}}) / (g^{(t_{1ij} * e)} * h^{(z_{1ij} * e)} * h^{z_{2ij}}) = g^{(a_{2ij} - (t_{ij} * e))} * h^{(x_{2ij} - (z_{1ij} * e) - z_{2ij})}$, 或者 $a_{2ij}' = h^{(a_{2ij} - (t_{ij} * e))} * g^{(x_{2ij} - (z_{1ij} * e) - z_{2ij})}$, 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, “ $(x_{2ij} - (z_{1ij} * e) - z_{2ij})$ ”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, “ $z_{1ij} * e$ ”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 $a_{4ij}' = a_{4ij} * t_{2ij}' = (g^{a_{4ij}} * h^{y_{4ij}}) * (g^{(t_{1ij} * e)} * h^{(z_{1ij} * e)} * h^{z_{2ij}}) = g^{(a_{4ij} + (t_{1ij} * e))} * h^{(y_{4ij} + (z_{1ij} * e) + z_{2ij})}$, 或者, $a_{4ij}' = h^{(a_{4ij} + (t_{1ij} * e))} * g^{(y_{4ij} + (z_{1ij} * e) + z_{2ij})}$, 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, “ $a_{4ij} + (t_{1ij} * e)$ ”代表第 i 账本下的第 j 个第四账户的新余额, “ $(y_{4ij} + (z_{1ij} * e) + z_{2ij})$ ”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, “ $t_{1ij} * e$ ”代表第 i 账本下的第 j 个第四账户的交易份额, “ $z_{1ij} * e$ ”代表第 i 账本下的第 j 个第四账户的交易份额隐私密钥。

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:

预步骤一: 在区块链智能合约创建之初设置合法兑换率数值。如合法兑换率数值: $r_1, r_2, r_3, r_4 \dots$ 。智能合约可以预先规定合法的兑换率, 如人民币和美元兑换只能是 6.7, 6.8, 6.9, 7.0 ...。

预步骤二: 在区块链智能合约里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“账户隐私密钥”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。例如可用 Pederson Commitment 代表每个账户, 甲账户要用在账本 1 的余额换取以账户乙在账本 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。具体地:

对于账本 1，定义如下：

$a1$ = 甲账户账本 1 余额

$a1'$ = 密码混淆后的甲账户账本 1 余额

$x1$ = 甲账户账本 1 余额隐私密钥

得到甲账户余额： $a1' = g^{a1} * h^{x1}$ 。

定义：

$b1$ = 乙账户人民币余额

$b1'$ = 密码混淆后的乙账户人民币余额

$y1$ = 乙账户人民币余额隐私密钥

得到乙账户余额： $b1' = g^{b1} * h^{y1}$ 。

对于账本 2，定义如下：

$a2$ = 甲账户账本 2 余额

$a2'$ = 密码混淆后的甲账户账本 2 余额

$x2$ = 甲账户账本 2 余额隐私密钥

得到甲账户余额： $a2' = g^{a2} * h^{x2}$

定义：

$b2$ = 乙账户人民币余额

$b2'$ = 密码混淆后的乙账户人民币余额

$y2$ = 乙账户人民币余额隐私密钥

得到乙账户余额： $b2' = g^{b2} * h^{y2}$

实现步骤一：如果甲要用账本 1 的余额交换乙在账本 2 的余额，甲会创建若干密文，第一个是用加法同态密文保护的账本 1 交易份额（第一密文），第二个是用加法同态密文保护的账本 2 交易份额（第一校验密文），第三个是一种证明可以使第三方在零知识环境下验证第一账本和第二账本的兑换率是在法定范围内的第一验证密文及第二验证密文。具体地：

对于第一密文，转账发起方（甲）会自行生成第一密文用的同态隐私密钥和第一校验密文用的隐私密钥和附加参数并将它们和第一密文与第一校验密文发给交易对手（乙），并在获得乙认可和对第一密文和第一校验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）。

定义：

t = 账本 1 交易份额

$t1'$ = 密码混淆后的第二账本交易份额

$z1$ = 第一账本交易份额隐私密钥

得到第一密文（账本 1 交易份额）： $t1' = g^t * h^{z1}$

对于第一校验密文，定义：

e = 兑换率，实际上应当是法定兑换率范围（ $r1, r2, r3, r4$ ）中的一位

$t * e = te$ = 密码混淆后的第二账本交易份额

$z2$ = 第二账本交易份额附加隐私密钥

$t2'$ = 账本 2 交易份额

得到第一校验密文（账本 2 交易份额）： $t2' = g^{te} * h^{z1e} * h^{z2}$

对于第一验证密文，由于 e 必须是提前设定的合理兑换率数值（ $r1, r2, r3, r4$ ）中的一个，当第一账本交易额是 t 的时候，第二账本交易额必须是 $t*r1, t*r2, t*r3, t*r4$ 中的一个。假设 $e = r2$ ，第二账本交易额是 $t * r2$ ，通过第一密文和合理兑

汇率数值, 区块链智能合约可以轻松算出混淆过的第二账本的合理交易份额, 则:

第一验证密文如下:

$$t21 = (g^t * h^{z1})^{r1} = g^{(t*r1)} * h^{(z1*r1)}$$

$$t22 = (g^t * h^{z1})^{r2} = g^{(t*r2)} * h^{(z1*r2)}$$

$$t23 = (g^t * h^{z1})^{r3} = g^{(t*r3)} * h^{(z1*r3)}$$

$$t24 = (g^t * h^{z1})^{r4} = g^{(t*r4)} * h^{(z1*r4)}$$

由于对兑换率隐私需求, 交易发起方不能直接提供 $t21-t24$ 中的任何一个数额, 所以交易发起方会在提供的第二账本中的交易份额中增加一个混淆密钥 $z2$, 因此第一校验密文变成 $t2' = t22' = g^{(t*e)} * h^{(z1*e)} * h^{z2} = g^{(t*r2)} * h^{(z1*r2)} * h^{z2}$ 。由于混淆密钥 $z2$ 的存在, 区块链上的任何一方都不知道, 第二账本交易份额属于从 $t21-t24$ 中任何一个份额中演变的, 也不确定交易否还在合理兑换率范围内。因此交易发起方必须提供第二账本交易份额还在合理兑换率范围内的证据。

本实施例中可以用环签名来提供这个证据, 在这个环签名中的 4 个 (在此仅以 4 个为例进行说明, 还可以为很多个) 公私钥分别是:

sk1 : $t21$ 私钥

sk2 : $t22$ 私钥

sk3 : $t23$ 私钥

sk4 : $t24$ 私钥

对于第二验证密文, 每个私钥都会有把每个第二账本交易份额转换成与正确交易份额产生的同样的密文:

$$t2' = (g^{(t*r1)} * h^{(z1*r1)} * h^{sk1})$$

$$t2' = (g^{(t*r2)} * h^{(z1*r2)} * h^{sk2})$$

$$t2' = (g^{(t*r3)} * h^{(z1*r3)} * h^{sk3})$$

$$t2' = (g^{(t*r4)} * h^{(z1*r4)} * h^{sk4})$$

第二验证密文 ($pk1, pk2, pk3, pk4$):

$$pk1 = h^{sk1} = (g^{(t*r1)} * h^{(z1*r1)} * h^{sk1}) / (g^{(t*r1)} * h^{(z1*r1)}) = h^?$$

$$pk2 = h^{sk2} = (g^{(t*r2)} * h^{(z1*r2)} * h^{sk2}) / (g^{(t*r2)} * h^{(z1*r2)}) = h^{sk2} =$$

h^{z2}

$$pk3 = h^{sk3} = (g^{(t*r3)} * h^{(z1*r3)} * h^{sk3}) / (g^{(t*r3)} * h^{(z1*r3)}) = h^?$$

$$pk4 = h^{sk4} = (g^{(t*r4)} * h^{(z1*r4)} * h^{sk4}) / (g^{(t*r4)} * h^{(z1*r4)}) = h^?$$

很明显, 交易发起方只有在当兑换率是 $r2$ 的时候, 知道对应的私钥是 $z2$ 。通过 $z2$, $pk1, pk2, pk3, pk4$, 和少量参数, 生成环签名证据 (s) 证明兑换率是合理兑换率数值中的一个。

实现步骤二 A: 智能合约要验证第一账本与第二账本交易份额在合理兑换率数值之内。例如, 可通过环签名或 Range Proof 验证第一账本与第二账本交易份额在合理兑换率数值之内。

实现步骤二 B: 在账本 1 的甲账户余额中增加交易份额, 并同时到账本 1 乙账户余额中扣除交易份额。具体地:

甲账户在账本 1 新份额: $a1'' = a1' * t'$

$$a1'' = (g^{a1} * h^{x1}) * (g^t * h^{z1})$$

$$a1'' = g^{(a1+t)} * h^{(x1+z1)}$$

甲账户新余额 = $a1+t$

甲账户新混淆隐私秘钥 $x1' = (x1+z1)$ 。

乙账户在账本 1 新份额: $b1'' = b1' / t'$

$$b1'' = (g^{b1} * h^{y1}) / (g^t * h^{z1})$$

$$b1'' = g^{(b1-t)} * h^{(y1-z1)}$$

乙账户新余额 $b1' = b1 - t$

乙账户新混淆隐私秘钥 $y1' = y1 - z1$ 。

实现步骤二 C：在账本 2 的甲账户余额中扣除交易份额，并同时到账本 2 乙账户余额中增加上交易份额。具体地：

甲账户在账本 2 新份额： $a2'' = a2' / t2'$

$$a2'' = (g^{a2} * h^{x2}) / (g^{(t*c)} * h^{(z1*c)} * h^{z2})$$

$$a2'' = g^{(a2-te)} * h^{(x2-z1*c-z2)}$$

甲账户新余额 = $a2 - te$

甲账户新混淆隐私秘钥 $x2' = (x2 - z1 * e - z2)$ 。

乙账户在账本 2 新份额： $b2'' = b2' * te'$

$$b2'' = (g^{b2} * h^{y2}) * (g^{(t*c)} * h^{(z1*c)} * h^{z2})$$

$$b2'' = g^{(b2+te)} * h^{(y2+z1*c+z2)}$$

乙账户新余额 $b2' = b2 + te$

乙账户新混淆隐私秘钥 $y2' = y2 + z1 * e + z2$ 。

如图 2 所示，图 2 为本申请基于区块链的零知识多账本兑换转账方法一实施例的流程示意图，该基于区块链的零知识多账本兑换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。

同时，在区块链智能合约创建时预先设置合法兑换率数值。例如，合法兑换率数值可以记为： $e1, e2, e3, e4, \dots$ ；在区块链智能合约创建时可以为多个账本预先设置两两之间的合法兑换率，如人民币账本和美元账本之间的合法兑换率只能是 6.7, 6.8, 6.9, 7.0, ...等。

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 个第一用户账户的兑换交易份额， z_{lij} 代表第 i 账本下的第 j 个第一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 S20，获取数字签名后的第一密文及第一校验密文；所述第一校验密文

由所述第一用户通过第一预设兑换计算公式及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加密兑换交易份额,并在所述第二账本的加密兑换交易份额上利用预设的附加隐私参数生成第一校验密文。

本实施例中,若为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加密兑换交易份额,并在第二账本的加密兑换交易份额上加上一个附加隐私参数生成第一校验密文,该附加隐私参数为一个隐私公钥,只有交易方知道与该附加隐私参数对应的附加隐私密钥。在第二账本的加密兑换交易份额上加上一个附加隐私参数生成第一校验密文的作用是让第三方可以检验第二账本加密交易份额是在合法交易范围内,但第三方无法得知具体兑换率。

例如,所述第一预设交易兑换计算公式为 $t'_{2ij} = h^{z_{2ij}} * (t'_{1ij})^e = h^{z_{2ij}} * (g^{t_{1ij}} * h^{z_{1ij}})^e = g^{t_{1ij} * e} * h^{z_{1ij} * e * z_{2ij}}$, 或者, $t'_{2ij} = h^{t_{1ij} * e} * g^{z_{1ij} * e * z_{2ij}}$, 其中, $t_{1ij} * e$ 代表第 i 账本下的第 j 个第二用户账户的兑换交易份额, $z_{1ij} * e$ 代表第 i 账本下的第 j 个第二用户账户的兑换交易份额隐私密钥, z_{2ij} 代表第 i 账本下的第 j 个第二用户账户的兑换交易份额附加隐私密钥, 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, 通过预先设置的若干合法兑换率数值和所述第一密文计算出各个对应的第一验证值密文; 并利用各个所述第一验证值密文与所述第一校验密文算出用于验证所述第一账本与所述第二账本交易的预设兑换率是否在预先设置的合法兑换率数值范围之内的第二验证值密文。

第一用户将第一密文、第一校验密文数字签名后发给第二用户, 当获得第二用户对交易份额认同和数字签名后, 第一用户将第一密文和第一校验密文发布到区块链网络上的各个节点上, 并由区块链网络上的智能合约通过预先设置的所有合法兑换率($e_1, e_2, e_3, e_4, \dots$)和第一密文计算出各个合理第二账本更新数值(即各个合法兑换率对应的第二账本更新数值)对应的第一验证值密文, 其中, 第一验证值密文与第一校验密文的不同在于所有第一验证值密文都不含有附加隐私参数。此外, 第一用户将第一密文、第一校验密文数字签名后发给第二用户后, 第二用户对交易份额认同和数字签名后可以直接发布到区块链网络上的各个节点上。

智能合约用各个第一验证值密文与第一校验密文算出验证第一账本与第二账本的交易份额兑换率是否在预先设置的合理兑换率数值之内的第二验证值密文。需要说明的是: 每一个第二验证值密文都等同于一个公钥, 若第一用户或第二用户要证明第一校验密文在合法兑换范围内, 则第一或第二用户必须有对应这个第二验证值密文(公钥)的一个私钥。如果第一校验密文确实在合法兑换范围内, 那么第二验证值密文(公钥)就是已知附加到第一校验密文中的附加隐私参数, 与第二验证值密文(公钥)对应的私钥就是与第一校验密文中的附加隐私参数(公钥)对应的私钥。

步骤 S40, 若利用所述第二验证值密文证明所述第一账本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内, 则基于所述第一密文和所述第一校验密文, 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, 可通过预设的环签名或 Range Proof 验证方式证明所述第一账

本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内。例如，在一种可选的实施方式中，当智能合约上呈现与所有第二账本合法交易份额对应的第二验证值密文（公钥）后，第一用户或第二用户通过所述第一校验密文（公钥）验证通过第一校验密文加密的加密份额是在预设合理交易范围内的数字，则证明所述第一账本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内。

在另一种可选的实施方式中，第一校验密文对应第一密文的合理范围未必是交易兑换率，第一密文和第一校验密文也可以各自代表一个数字（如日期），可以用上述算法检测第一密文代表的数字与第一校验密文代表的数字的相差是否在一个提前预设的范围内，来证明第一校验密文是在预先设置的合理兑换率数值之内，进而证明所述第一账本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内。

若第一校验密文被证明在预先设置的合理兑换率数值之内，则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二用户账户的余额，并根据所述第一校验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。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，并在所述第二账本的加密兑换交易份额上利用预设的附加隐私参数生成第一校验密文。通过预先设置的若干合法兑换率数值和所述第一密文计算出各个对应的第一验证值密文；并利用各个所述第一验证值密文与所述第一校验密文算出第二验证值密文；若利用所述第二验证值密文证明所述第一账本与所述第二账本交易的预设兑换率在预先设置的合法兑换率数值范围之内，则基于所述第一密文和所述第一校验密文，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，在交易过程中区块链上的其他节点无法解读具体的兑换交易份额数据，从而有效保证区块链技术场景中交易信息安全。而且，由于在所述第二账本的加密兑换交易份额上利用预设的附加隐私参数生成

第一校验密文, 该附加隐私参数使得第三方无法得知具体兑换率, 同时, 通过第二验证值密文可验证所述第一账本与所述第二账本交易的预设兑换率是否在预先设置的合法兑换率数值范围之内。从而在有效保证区块链技术场景中交易信息安全、且能证明多个账本的转账交易是在一个提前设置的合法兑换率域内但第三方无法得知具体兑换率的情况下, 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 S40 具体包括:

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, 并根据所述第一校验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合法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, 并根据所述第一校验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_{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。

所述根据所述第一校验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 $a_{2ij}' = a_{2ij} / t_{2ij} = (g^{a_{2ij}} * h^{x_{2ij}}) / (g^{(t_{1ij} * e)} * h^{(z_{1ij} * e)} * h^{z_{2ij}}) = g^{(a_{2ij} - (t_{1ij} * e))} * h^{(x_{2ij} - (z_{1ij} * e) - z_{2ij})}$, 或者 $a_{2ij}' = h^{(a_{2ij} - (t_{1ij} * e))} * g^{(x_{2ij} - (z_{1ij} * e) - z_{2ij})}$, 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, “ $(x_{2ij} - (z_{1ij} * e) - z_{2ij})$ ” 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 $a_{4ij}' = a_{4ij} * t_{2ij} = (g^{a_{4ij}} * h^{y_{4ij}}) * (g^{(t_{1ij} * e)} * h^{(z_{1ij} * e)} * h^{z_{2ij}}) = g^{(a_{4ij} + (t_{1ij} * e))} * h^{(y_{4ij} + (z_{1ij} * e) + z_{2ij})}$, 或者, $a_{4ij}' = h^{(a_{4ij} + (t_{1ij} * e))} * g^{(y_{4ij} + (z_{1ij} * e) + z_{2ij})}$, 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, “ $a_{4ij} + (t_{1ij} * e)$ ” 代表第 i 账本下的第 j 个第四账户的新余额, “ $(y_{4ij} + (z_{1ij} * e) + z_{2ij})$ ” 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, “ $t_{1ij} * e$ ” 代表第 i 账本下的第 j 个第四账户的交易份额, “ $z_{1ij} * e$ ” 代表第 i 账本下的第 j 个第四账户的交易份额隐私密钥。

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:

预步骤一: 在区块链智能合约创建之初设置合法兑换率数值。如合法兑换率数值: $r_1, r_2, r_3, r_4 \dots$ 。智能合约可以预先规定合法的兑换率, 如人民币和美元兑换只能是 6.7, 6.8, 6.9, 7.0 ...。

预步骤二: 在区块链智能合约里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“账户隐私密钥”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。例如可用 Pederson Commitment 代表每个账户, 甲账户要用在账本 1 的余额换取以账户乙在账本 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。具体地:

对于账本 1, 定义如下:

a_1 = 甲账户账本 1 余额

$a1'$ = 密码混淆后的甲账户账本 1 余额

$x1$ = 甲账户账本 1 余额隐私密钥

得到甲账户余额: $a1' = g^{a1} * h^{x1}$ 。

定义:

$b1$ = 乙账户人民币余额

$b1'$ = 密码混淆后的乙账户人民币余额

$y1$ = 乙账户人民币余额隐私密钥

得到乙账户余额: $b1' = g^{b1} * h^{y1}$ 。

对于账本 2, 定义如下:

$a2$ = 甲账户账本 2 余额

$a2'$ = 密码混淆后的甲账户账本 2 余额

$x2$ = 甲账户账本 2 余额隐私密钥

得到甲账户余额: $a2' = g^{a2} * h^{x2}$

定义:

$b2$ = 乙账户人民币余额

$b2'$ = 密码混淆后的乙账户人民币余额

$y2$ = 乙账户人民币余额隐私密钥

得到乙账户余额: $b2' = g^{b2} * h^{y2}$

实现步骤一: 如果甲要用账本 1 的余额交换乙在账本 2 的余额, 甲会创建若干密文, 第一个是用加法同态密文保护的账本 1 交易份额 (第一密文), 第二个是用加法同态密文保护的账本 2 交易份额 (第一校验密文), 第三个是一种证明可以使第三方在零知识环境下验证第一账本和第二账本的兑换率是在法定范围内的第一验证密文及第二验证密文。具体地:

对于第一密文, 转账发起方 (甲) 会自行生成第一密文用的同态隐私密钥和第一校验密文用的隐私密钥和附加参数并将它们和第一密文与第一校验密文发给交易对手 (乙), 并在获得乙认可和对第一密文和第一校验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)。

定义:

t = 账本 1 交易份额

$t1'$ = 密码混淆后的第二账本交易份额

$z1$ = 第一账本交易份额隐私密钥

得到第一密文 (账本 1 交易份额): $t1' = g^t * h^{z1}$

对于第一校验密文, 定义:

e = 兑换率, 实际上应当是法定兑换率范围 ($r1, r2, r3, r4$) 中的一位

$t * e = te$ = 密码混淆后的第二账本交易份额

$z2$ = 第二账本交易份额附加隐私密钥

$t2'$ = 账本 2 交易份额

得到第一校验密文 (账本 2 交易份额): $t2' = g^{te} * h^{z1e} * h^{z2}$

对于第一验证密文, 由于 e 必须是提前设定的合理兑换率数值 ($r1, r2, r3, r4$) 中的一个, 当第一账本交易额是 t 的时候, 第二账本交易额必须是 $t*r1, t*r2, t*r3, t*r4$ 中的一个。假设 $e = r2$, 第二账本交易额是 $t * r2$, 通过第一密文和合理兑换率数值, 区块链智能合约可以轻松算出混淆过的第二账本的合理交易份额, 则:

第一验证密文如下：

$$\begin{aligned}t21 &= (g^t * h^{z1})^{r1} = g^{(t*r1)} * h^{(z1*r1)} \\t22 &= (g^t * h^{z1})^{r2} = g^{(t*r2)} * h^{(z1*r2)} \\t23 &= (g^t * h^{z1})^{r3} = g^{(t*r3)} * h^{(z1*r3)} \\t24 &= (g^t * h^{z1})^{r4} = g^{(t*r4)} * h^{(z1*r4)}\end{aligned}$$

由于对兑换率隐私需求，交易发起方不能直接提供 $t21-t24$ 中的任何一个数额，所以交易发起方会在提供的第二账本中的交易份额中增加一个混淆密钥 $z2$ ，因此第一校验密文变成 $t2' = t22' = g^{(t*e)} * h^{(z1*e)} * h^{z2} = g^{(t*r2)} * h^{(z1*r2)} * h^{z2}$ 。由于混淆密钥 $z2$ 的存在，区块链上的任何一方都不知道，第二账本交易份额属于从 $t21-t24$ 中任何一个份额中演变的，也不确定交易否还在合理兑换率范围内。因此交易发起方必须提供第二账本交易份额还在合理兑换率范围内的证据。

本实施例中可以用环签名来提供这个证据，在这个环签名中的 4 个（在此仅以 4 个为例进行说明，还可以为很多个）公私钥分别是：

sk1 : t21 私钥
sk2 : t22 私钥
sk3 : t23 私钥
sk4 : t24 私钥

对于第二验证密文，每个私钥都会有把每个第二账本交易份额转换成与正确交易份额产生的同样的密文：

$$\begin{aligned}t2' &= (g^{(t*r1)} * h^{(z1*r1)} * h^{sk1}) \\t2' &= (g^{(t*r2)} * h^{(z1*r2)} * h^{sk2}) \\t2' &= (g^{(t*r3)} * h^{(z1*r3)} * h^{sk3}) \\t2' &= (g^{(t*r4)} * h^{(z1*r4)} * h^{sk4})\end{aligned}$$

第二验证密文 (pk1, pk2, pk3, pk4) :

$$\begin{aligned}pk1 &= h^{sk1} = (g^{(t*r1)} * h^{(z1*r1)} * h^{sk1}) / (g^{(t*r1)} * h^{(z1*r1)}) = h^? \\pk2 &= h^{sk2} = (g^{(t*r2)} * h^{(z1*r2)} * h^{sk2}) / (g^{(t*r2)} * h^{(z1*r2)}) = h^{sk2} = \\&h^{z2}\end{aligned}$$

$$\begin{aligned}pk3 &= h^{sk3} = (g^{(t*r3)} * h^{(z1*r3)} * h^{sk3}) / (g^{(t*r3)} * h^{(z1*r3)}) = h^? \\pk4 &= h^{sk4} = (g^{(t*r4)} * h^{(z1*r4)} * h^{sk4}) / (g^{(t*r4)} * h^{(z1*r4)}) = h^?\end{aligned}$$

很明显，交易发起方只有在当兑换率是 $r2$ 的时候，知道对应的私钥是 $z2$ 。通过 $z2$, $pk1$, $pk2$, $pk3$, $pk4$, 和少量参数, 生成环签名证据 (s) 证明兑换率是合理兑换率数值中的一个。

实现步骤二 A: 智能合约要验证第一账本与第二账本交易份额在合理兑换率数值之内。例如，可通过环签名或 Range Proof 验证第一账本与第二账本交易份额在合理兑换率数值之内。

实现步骤二 B: 在账本 1 的甲账户余额中增加交易份额，并同时在账本 1 乙账户余额中扣除交易份额。具体地：

$$\begin{aligned}\text{甲账户在账本 1 新份额: } a1'' &= a1' * t' \\a1'' &= (g^{a1} * h^{x1}) * (g^t * h^{z1}) \\a1'' &= g^{(a1+t)} * h^{(x1+z1)} \\ \text{甲账户新余额} &= a1+t \\ \text{甲账户新混淆隐私秘钥 } x1' &= (x1+z1)。 \\ \text{乙账户在账本 1 新份额: } b1'' &= b1' / t' \\b1'' &= (g^{b1} * h^{y1}) / (g^t * h^{z1}) \\b1'' &= g^{(b1-t)} * h^{(y1-z1)}\end{aligned}$$

乙账户新余额 $b1' = b1 - t$

乙账户新混淆隐私密钥 $y1' = y1 - z1$ 。

实现步骤二 C：在账本 2 的甲账户余额中扣除交易份额，并同时在账本 2 乙账户余额中增加上交易份额。具体地：

甲账户在账本 2 新份额： $a2'' = a2' / t2'$

$a2'' = (g^{a2} * h^{x2}) / (g^{(t * e)} * h^{(z1 * e)} * h^{z2})$

$a2'' = g^{(a2 - te)} * h^{(x2 - z1 * e - z2)}$

甲账户新余额 = $a2 - te$

甲账户新混淆隐私密钥 $x2' = (x2 - z1 * e - z2)$ 。

乙账户在账本 2 新份额： $b2'' = b2' * te'$

$b2'' = (g^{b2} * h^{y2}) * (g^{(t * e)} * h^{(z1 * e)} * h^{z2})$

$b2'' = g^{(b2 + te)} * h^{(y2 + z1 * e + z2)}$

乙账户新余额 $b2' = b2 + te$

乙账户新混淆隐私密钥 $y2' = y2 + z1 * e + z2$ 。

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零知识多账本兑换转账系统，所述基于区块链的零知识多账本兑换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零知识多账本兑换转账方法的步骤，该基于区块链的零知识多账本兑换转账方法的步骤 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）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。