

权利要求书

1. 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，其特征在于，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。

2. 如权利要求 1 所述的基于区块链的零知识多账本兑换转账方法，其特征在于，所述获取数字签名后的第一密文及第一校验密文的步骤包括：

所述第一用户将计算生成的第一密文、第一校验密文数字签名后发给所述第二用户，当获得所述第二用户对交易份额认同和数字签名后，所述第一用户将所述第一密文和所述第一校验密文发布到区块链网络上的各个节点上；或者，所述第一用户将计算生成的第一密文、第一校验密文数字签名后发给所述第二用户，所述第二用户对交易份额认同和数字签名后直接发布到区块链网络上的各个节点上；

从区块链网络上获取到发布的数字签名后的第一密文及第一校验密文。

3. 如权利要求 1 所述的基于区块链的零知识多账本兑换转账方法，其特征在于，该方法还包括：

通过预设的环签名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。

4. 如权利要求 2 所述的基于区块链的零知识多账本兑换转账方法，其特征在于，该方法还包括：

通过预设的环签名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。

5. 如权利要求 3 所述的基于区块链的零知识多账本兑换转账方法，其特征在于，该方法还包括：

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，由所述第一用户或所述第二用户通过所述第一校验密文中的附加隐私参数对应的私钥和所有第二验证值密文验证通过所述第一校验密文中的加密兑换交易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。

6. 如权利要求 4 所述的基于区块链的零知识多账本兑换转账方法, 其特征在于, 该方法还包括:

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, 由所述第一用户或所述第二用户通过所述第一校验密文中的附加隐私参数对应的私钥和所有第二验证值密文验证通过所述第一校验密文中的加密兑换交易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。

7. 如权利要求 1 所述的基于区块链的零知识多账本兑换转账方法, 其特征在于, 所述步骤 D 包括:

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一用户的第四账户的余额和所述第二账本下第二用户的第二用户账户的余额。

8. 如权利要求 2 所述的基于区块链的零知识多账本兑换转账方法, 其特征在于, 所述步骤 D 包括:

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一用户的第四账户的余额和所述第二账本下第二用户的第二用户账户的余额。

9. 如权利要求 7 所述的基于区块链的零知识多账本兑换转账方法, 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:

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。

10. 如权利要求 8 所述的基于区块链的零知识多账本兑换转账方法, 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:

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 所述的基于区块链的零知识多账本兑换转账方法, 其特征在于, 所述根据所述第一校验密文更新所述第二账本下第一用户的第四账户的余额和所述第二账本下第二用户的第二用户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;

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 所述的基于区块链的零知识多账本兑换转账方法,其特征在于,所述根据所述第一校验密文更新所述第二账本下第一用户的第四账户的余额和所述第二账本下第二用户的第二用户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;

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. 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。

14. 如权利要求 13 所述的电子装置,其特征在于,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实现获取数字签名后的第一密文及第一校验密文的步骤时,具体包括:

所述第一用户将计算生成的第一密文、第一校验密文数字签名后发给所述第二用户,当获得所述第二用户对交易份额认同和数字签名后,所述第一用户将所述第一密文和所述第一校验密文发布到区块链网络上的各个节点上;或者,所述第一用户将计算生成的第一密文、第一校验密文数字签名后发给所述第二用户,所述第二用户对交易份额认同和数字签名后直接发布到区块链网络上的各个节点上;

从区块链网络上获取到发布的数字签名后的第一密文及第一校验密文。

15. 如权利要求 13 所述的电子装置, 其特征在于, 所述处理器还用于执行所述基于区块链的零知识多账本兑换转账系统, 以实现以下步骤:

通过预设的环签名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。

16. 如权利要求 14 所述的电子装置, 其特征在于, 所述处理器还用于执行所述基于区块链的零知识多账本兑换转账系统, 以实现以下步骤:

通过预设的环签名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。

17. 如权利要求 15 所述的电子装置, 其特征在于, 所述处理器还用于执行所述基于区块链的零知识多账本兑换转账系统, 以实现以下步骤:

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, 由所述第一用户或所述第二用户通过所述第一校验密文中的附加隐私参数对应的私钥和所有第二验证值密文验证通过所述第一校验密文中的加密兑换交易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。

18. 如权利要求 16 所述的电子装置, 其特征在于, 所述处理器还用于执行所述基于区块链的零知识多账本兑换转账系统, 以实现以下步骤:

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, 由所述第一用户或所述第二用户通过所述第一校验密文中的附加隐私参数对应的私钥和所有第二验证值密文验证通过所述第一校验密文中的加密兑换交易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。

19. 如权利要求 13 所述的电子装置, 其特征在于, 所述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的步骤包括:

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一用户的第四账户的余额和所述第二账本下第二用户的第二用户账户的余额。

20. 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。