

权利要求书

1、一种基于区块链的交易方法，包括：

根据承诺随机数和交易额，计算交易额承诺；

根据汇出方账户的同态加密公钥和所述交易额，使用同态加密算法对所述承诺随机数

5 数进行加密，得到承诺随机数第一密文；

根据汇入方账户的同态加密公钥和所述交易额，使用同态加密算法对所述承诺随机数进行加密，得到承诺随机数第二密文；

向所述区块链提交交易数据；所述交易数据包括所述交易额承诺、所述承诺随机数第一密文和所述承诺随机数第二密文；以便于将所述交易额承诺和所述承诺随机数第一密文记入所述汇出方账户，以及将所述交易额承诺和所述承诺随机数第二密文记入所述汇入方账户。

2、如权利要求 1 所述的方法，所述汇出方账户在所述区块链中登记有汇出方余额承诺和汇出方随机数密文；其中，所述汇出方余额承诺基于汇出方随机数和汇出方余额计算得到；所述汇出方随机数密文由同态加密算法基于所述汇出方余额对所述汇出方随机数进行加密得到；

所述汇入方账户在所述区块链中登记有汇入方余额承诺和汇入方随机数密文；其中，所述汇入方余额承诺基于汇入方随机数和汇入方余额计算得到；所述汇入方随机数密文由同态加密算法基于所述汇入方余额对所述汇入方随机数进行加密得到。

3、如权利要求 2 所述的方法，采用如下方式将所述交易额承诺和所述承诺随机数第一密文记入所述汇出方账户：

基于所述交易额承诺更新所述汇出方余额承诺，基于所述承诺随机数第一密文更新所述汇出方随机数密文；

采用如下方式将所述交易额承诺和所述承诺随机数第二密文记入所述汇入方账户：

基于所述交易额承诺更新所述汇入方余额承诺，基于所述承诺随机数第二密文更新所述汇入方随机数密文。

4、如权利要求 3 所述的方法，更新后的汇出方余额承诺为所述汇出方余额承诺和所述交易额承诺的商；更新后的汇出方随机数密文为所述汇出方随机数密文和所述承诺随机数第一密文的商；

更新后的汇入方余额承诺为所述汇入方余额承诺和所述交易额承诺的积；更新后的汇入方随机数密文为所述汇入方随机数密文和所述承诺随机数第二密文的积。

5、如权利要求 1 所述的方法，在向所述区块链提交交易数据之前，所述方法还包

括:

生成第一零知识证明; 所述第一零知识证明用于验证: 所述交易额不小于 0;

相应地, 所述交易数据还包括所述第一零知识证明。

6、如权利要求 1 所述的方法, 在向所述区块链提交交易数据之前, 所述方法还包

5 括:

生成第二零知识证明; 所述第二零知识证明用于验证: 所述交易额不大于汇出方余额;

相应地, 所述交易数据还包括所述第二零知识证明。

7、如权利要求 1 所述的方法, 在向所述区块链提交交易数据之前, 所述方法还包

10 括:

生成第三零知识证明; 所述第三零知识证明用于验证: 用于计算交易额承诺的承诺随机数、用于计算承诺随机数第一密文的承诺随机数、和用于计算承诺随机数第二密文的承诺随机数一致, 且用于计算交易额承诺的交易额、用于计算承诺随机数第一密文的交易额、和用于计算承诺随机数第二密文的交易额一致;

15 相应地, 所述交易数据还包括所述第三零知识证明。

8、如权利要求 1 所述的方法, 在向所述区块链提交交易数据之前, 所述方法还包括:

使用所述汇出方账户的签名私钥对所述交易数据进行签名, 得到签名数据;

相应地, 所述交易数据还包括所述签名数据。

20 9、如权利要求 1 所述的方法, 所述根据承诺随机数和交易额, 计算交易额承诺, 包括:

根据第一承诺随机数和第一交易额, 计算第一交易额承诺; 根据第二承诺随机数和第二交易额, 计算第二交易额承诺;

25 所述根据汇出方账户的同态加密公钥和所述交易额, 使用同态加密算法对所述承诺随机数进行加密, 得到承诺随机数第一密文, 包括:

根据汇出方账户的同态加密公钥和所述第一交易额, 使用同态加密算法对所述第一承诺随机数进行加密, 得到承诺随机数第一密文;

所述根据汇入方账户的同态加密公钥和所述交易额, 使用同态加密算法对所述承诺随机数进行加密, 得到承诺随机数第二密文, 包括:

30 根据汇入方账户的同态加密公钥和所述第二交易额, 使用同态加密算法对所述第二承诺随机数进行加密, 得到承诺随机数第二密文;

相应地,所述交易数据包括所述第一交易额承诺、所述第二交易额承诺、所述承诺随机数第一密文和所述承诺随机数第二密文;以便于将所述第一交易额承诺和所述承诺随机数第一密文记入所述汇出方账户,以及将所述第二交易额承诺和所述承诺随机数第二密文记入所述汇入方账户。

- 5 10、如权利要求 9 所述的方法,在向所述区块链提交交易数据之前,所述方法还包括:

生成第四零知识证明;所述第四零知识证明用于验证:用于计算第一交易额承诺的第一交易额与用于计算第二交易额承诺的第二交易额一致;

相应地,所述交易数据还包括所述第四零知识证明。

- 10 11、一种基于区块链的交易装置,包括:

计算单元,用于根据承诺随机数和交易额,计算交易额承诺;

第一加密单元,用于根据汇出方账户的同态加密公钥和所述交易额,使用同态加密算法对所述承诺随机数进行加密,得到承诺随机数第一密文;

- 15 第二加密单元,用于根据汇入方账户的同态加密公钥和所述交易额,使用同态加密算法对所述承诺随机数进行加密,得到承诺随机数第二密文;

提交单元,用于向所述区块链提交交易数据;所述交易数据包括所述交易额承诺、所述承诺随机数第一密文和所述承诺随机数第二密文;以便于将所述交易额承诺和所述承诺随机数第一密文记入所述汇出方账户,以及将所述交易额承诺和所述承诺随机数第二密文记入所述汇入方账户。

- 20 12、一种汇出方设备,包括:

存储器,用于存储计算机指令;

处理器,用于执行计算机指令以实现如权利要求 1-10 中任一项所述的方法。