

权利要求书

1. 一种基于区块链的汇款方法, 其中, 汇出方账户包括一预备金列表; 所述预备金列表包括基于汇出方账户的余额划分得到的多个预备金金额;

所述方法包括:

- 5 接收汇出方发送的用于向接收方汇款的第一交易, 所述第一交易包括所述汇出方账户汇入接收方账户的汇款额, 和所述汇出方从所述预备金列表中为所述第一交易分配的至少一个与所述汇款额对应的预备金金额;

 对所述第一交易进行第一交易验证, 所述第一交易验证包括第一验证步骤, 用以验证所述第一交易包括的预备金金额之和是否大于或者等于所述汇款额; 如果是, 所述第

- 10 一交易通过所述第一验证步骤;

 如果所述第一交易通过所述第一交易验证, 从所述汇出方账户的余额扣除所述汇款额, 在接收方账户的余额增加所述汇款额。

 2、根据权利要求 1 所述的方法, 所述第一交易验证还包括第二验证步骤, 用以验证所述第一交易包括的预备金金额是否在所述预备金列表中被标记为已使用状态; 如果

- 15 否, 所述第一交易通过所述第二验证步骤。

 3、根据权利要求 1 所述的方法, 还包括:

 如果所述第一交易通过所述第一交易验证, 将所述第一交易包括的预备金金额在所述预备金列表中标记为已使用状态。

- 4、根据权利要求 1 所述的方法, 所述预备金列表还包括所述多个预备金金额对应的
20 的唯一标识, 所述第一交易还包括与所述至少一个与所述汇款额对应的预备金金额对应的唯一标识;

 所述第一交易验证还包括: 第三验证步骤, 用以验证所述第一交易所包括的预备金金额的唯一标识是否在已完成的汇款交易中被使用过; 如果否, 所述第一交易通过所述第三验证步骤。

- 25 5、根据权利要求 1 所述的方法, 所述汇出方账户的余额、所述接收方账户的余额、所述预备金金额以及所述汇款额被预先进行了同态加密处理;

 所述第一交易还包括: 基于所述第一交易所包括的被加密的预备金金额和被加密的汇款额生成的第一零知识证明;

 所述第一验证步骤包括:

- 30 基于零知识证明算法针对所述第一零知识证明进行零知识验证, 以确认为所述第一交易所分配的预备金金额之和是否大于或者等于所述汇款额; 如果是, 所述第一交易通

过所述第一验证步骤;

所述从所述汇出方账户的余额扣除所述汇款额,在接收方账户的余额增加所述汇款额,包括:

5 从所述汇出方账户的余额同态加密扣除所述汇款额,在接收方账户的余额同态加密增加所述汇款额。

6、根据权利要求 5 所述的方法,所述第一交易还包括:基于被加密的汇款额生成的第二零知识证明;

所述第一交易验证还包括第四验证步骤,所述第四验证步骤包括:基于零知识证明算法针对所述第二零知识证明进行零知识验证,以确认所述汇款额是否大于或者等于零;
10 如果是,所述第一交易通过所述第四验证步骤。

7、根据权利要求 1 所述的方法,还包括:

接收所述汇出方发送的用于初始化预备金列表的第二交易,所述第二交易包括基于汇出方账户的余额划分得到的多个预备金金额;

对所述第二交易进行第二交易验证,所述第二交易验证包括第五验证步骤,用以验证所述第二交易所包括的多个预备金金额之和是否小于或者等于所述汇出方账户的余额;
15 如果是,所述第二交易通过所述第五验证步骤;

如果所述第二交易通过所述第二交易验证,基于所述多个预备金金额构建预备金列表,并将所述预备金列表更新至所述汇出方账户。

8、根据权利要求 7 所述的方法,所述汇出方账户的余额以及所述多个预备金金额
20 被预先进行了同态加密处理;

所述第二交易还包括:基于被加密的所述多个预备金金额和被加密的所述汇出方账户的余额生成的第三零知识证明;

所述第五验证步骤包括:基于零知识证明算法针对所述第三零知识证明进行零知识验证,以确认所述第二交易所包括的多个预备金金额之和是否小于或者等于所述汇出方
25 账户的余额;如果是,所述第二交易通过所述第五验证步骤。

9、根据权利要求 8 所述的方法,所述第二交易还包括基于被加密的所述多个预备金金额生成的第四零知识证明;

所述第二交易验证还包括第六验证步骤,所述第六验证步骤包括:基于零知识证明算法针对所述第四零知识证明进行零知识验证,以确认所述第二交易所包括的多个预备
30 金金额是否均大于或者等于零;如果是,所述第二交易通过所述第六验证步骤。

10、根据权利要求 7 所述的方法,还包括:

将所述预备金列表包括的每个预备金金额均标记为未使用状态。

11、根据权利要求 7 所述的方法，所述预备金列表还包括为每个预备金金额生成的唯一标识。

12、根据权利要求 5 或 6 或 8 或 9 所述的方法，所述零知识证明算法包括区间证明
5 算法。

13. 一种基于区块链的汇款装置，其中，汇出方账户包括一预备金列表；所述预备金列表包括基于汇出方账户的余额划分得到的多个预备金金额；

所述装置包括：

接收单元，接收汇出方发送的用于向接收方汇款的第一交易，所述第一交易包括所
10 述汇出方账户汇入接收方账户的汇款额，和所述汇出方从所述预备金列表中为所述第一交易分配的至少一个与所述汇款额对应的预备金金额；

第一交易验证单元，对所述第一交易进行第一交易验证，所述第一交易验证单元包括第一验证模块，用以验证所述第一交易包括的预备金金额之和是否大于或者等于所述汇款额；

15 账户更新单元，如果所述第一交易通过所述第一交易验证，从所述汇出方账户的余额扣除所述汇款额，在接收方账户的余额增加所述汇款额。

14、根据权利要求 13 所述的装置，所述第一交易验证单元还包括第二验证模块，用以验证所述第一交易包括的预备金金额是否在所述预备金列表中被标记为已使用状态。

20 15、根据权利要求 13 所述的装置，所述账户更新单元：

如果所述第一交易通过所述第一交易验证，将所述第一交易包括的预备金金额在所述预备金列表中标记为已使用状态。

16、根据权利要求 13 所述的装置，所述预备金列表还包括所述多个预备金金额对应的唯一标识，所述第一交易还包括与所述至少一个与所述汇款额对应的预备金金额对
25 应的唯一标识；

所述第一交易验证单元还包括：第三验证模块，用以验证所述第一交易所包括的预备金金额的唯一标识是否在已完成的汇款交易中被使用过。

17、根据权利要求 13 所述的装置，所述汇出方账户的余额、所述接收方账户的余额、所述预备金金额以及所述汇款额被预先进行了同态加密处理；

30 所述第一交易还包括：基于所述第一交易所包括的被加密的预备金金额和被加密的汇款额生成的第一零知识证明；

所述第一验证模块:

基于零知识证明算法针对所述第一零知识证明进行零知识验证,以确认为所述第一交易所分配的预备金金额之和是否大于或者等于所述汇款额;

所述账户更新单元:

- 5 从所述汇出方账户的余额同态加密扣除所述汇款额,在接收方账户的余额同态加密增加所述汇款额。

18、根据权利要求 17 所述的装置,所述第一交易还包括:基于被加密的汇款额生成的第二零知识证明;

- 10 所述第一交易验证单元还包括第四验证模块,所述第四验证模块:基于零知识证明算法针对所述第二零知识证明进行零知识验证,以确认所述汇款额是否大于或者等于零。

19、根据权利要求 13 所述的装置,还包括

所述接收单元,接收所述汇出方发送的用于初始化预备金列表的第二交易,所述第二交易包括基于汇出方账户的余额划分得到的多个预备金金额;

- 15 第二交易验证单元,对所述第二交易进行第二交易验证,所述第二交易验证单元包括第五验证模块,用以验证所述第二交易所包括的多个预备金金额之和是否小于或者等于所述汇出方账户的余额;

所述账户更新单元,如果所述第二交易通过所述第二交易验证,基于所述多个预备金金额构建预备金列表,并将所述预备金列表更新至所述汇出方账户。

- 20 20、根据权利要求 19 所述的装置,所述汇出方账户的余额以及所述多个预备金金额被预先进行了同态加密处理;

所述第二交易还包括:基于被加密的所述多个预备金金额和被加密的所述汇出方账户的余额生成的第三零知识证明;

- 25 所述第五验证模块:基于零知识证明算法针对所述第三零知识证明进行零知识验证,以确认所述第二交易所包括的多个预备金金额之和是否小于或者等于所述汇出方账户的余额。

21、根据权利要求 20 所述的装置,所述第二交易还包括:基于被加密的所述多个预备金金额生成的第四零知识证明;

- 30 所述第二交易验证单元还包括第六验证模块,所述第六验证模块:基于零知识证明算法针对所述第四零知识证明进行零知识验证,以确认所述第二交易所包括的多个预备金金额是否均大于或者等于零。

22、根据权利要求 19 所述的装置,所述账户更新单元:

将所述预备金列表包括的每个预备金金额均标记为未使用状态。

23、根据权利要求 19 所述的装置，所述预备金列表还包括为每个预备金金额生成的唯一标识。

24、根据权利要求 17 或 18 或 20 或 21 所述的装置，所述零知识证明算法包括区间
5 证明算法。

25、一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求 1 到 12 任意一项所述的方法。

26、一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器
10 运行时，执行如权利要求 1 到 12 任意一项所述的方法。