

权利要求书

- 1、一种数据处理方法，其特征在于，包括：
交易发起方确定交易数据中需要隐藏的信息；
以所述交易数据为预定单向函数的输入，获取所述预定单向函数输出的交易根，并
5 根据所述交易根构建所述需要隐藏的信息合法的证明数据；
发起将所述证明数据和带有所述交易发起方签名的交易根写入区块链的交易请求，
以使区块链中的节点对所述交易根和所述证明数据进行共识验证，并根据验证结果响应
/拒绝响应所述交易请求。
- 2、根据权利要求 1 所述的方法，其特征在于，在以所述交易数据为预定单向函数
10 的输入之前，还包括：
确定所述交易数据中的交易前的数据和交易后的数据；
其中，以所述交易数据为预定单向函数的输入，获取所述预定单向函数输出的交易
根包括：
以交易前的数据为第一预定单向函数的输入，获取所述第一预定单向函数输出的
15 入交易根；
以交易后的数据为第二预定单向函数的输入，获取所述第二预定单向函数输出的
输出交易根；
将获取的输入交易根和输出交易根作为待上链的交易根。
- 3、根据权利要求 2 所述的方法，其特征在于，以交易后的数据为第二预定单向函
20 数的输入，获取所述第二预定单向函数输出的输出交易根包括：
根据所述交易后的数据和随机数构建预定单向函数树的底层，并确定所述预定单向
函数树的顶层对应的输出交易根。
- 4、根据权利要求 1 所述的方法，其特征在于，所述根据所述交易根构建所述需要
隐藏的信息合法的证明数据包括：
25 以所述交易根和所述需要隐藏的信息为输入进行预定的逻辑运算；
以所述需要隐藏的信息为保护对象，对所述逻辑运算进行零知识证明，获取证明数
据。
- 5、一种数据处理方法，其特征在于，包括：
接收交易发起方发送的交易请求，所述交易请求用于请求将交易根和证明数据写入
30 区块链；所述交易根为以交易数据为预定单向函数的输入获取的，所述证明数据用于证
明所述交易数据中的需要隐藏的信息；

对所述交易根进行验证,获取第一验证结果;根据所述交易根对所述证明数据进行验证,获取第二验证结果;

根据所述第一验证结果和所述第二验证结果响应/拒绝响应所述交易请求。

- 5 6、根据权利要求5所述的方法,其特征在于,所述对所述交易根进行验证包括:
验证所述交易根是否有合法的签名。

7、根据权利要求6所述的方法,其特征在于,验证所述交易根是否有合法的签名包括:

确定与所述交易根中的输出交易根具有关联关系的地址,所述输出交易根为根据所述交易数据中交易后的数据构建的;

- 10 若判断获知地址的数量为1,则验证所述交易根是否有与所述交易发起方对应的签名。

8、根据权利要求5所述的方法,其特征在于,所述对所述交易根进行验证包括:

验证所述交易根中的输出交易根与已上链的输出交易根和输入交易根是否重复;所述输出交易根为根据所述交易数据中交易后的数据构建的。

- 15 9、根据权利要求5所述的方法,其特征在于,所述对所述交易根进行验证包括:

验证所述交易根中的输入交易根与已上链的输出交易根和输入交易根是否重复;所述输入交易根为根据所述交易数据中交易前的数据构建的。

10、根据权利要求5所述的方法,其特征在于,所述根据所述第一验证结果和所述第二验证结果确定响应/拒绝响应所述交易请求包括:

- 20 若所述第一验证结果和所述第二验证结果均为通过,则响应所述交易请求,以将带有交易发起方签名的交易根和证明数据写入区块链;

若所述第一验证结果和/或所述第二验证结果为未通过,则拒绝响应所述交易请求。

11、一种数据处理方法,其特征在于,包括:

交易发起方确定交易数据中的需要隐藏的信息;

- 25 以所述交易数据为预定单向函数的输入,获取所述预定单向函数输出的交易根,并根据所述交易根构建所述需要隐藏的信息合法的证明数据;

向交易接收方发送所述交易根和所述证明数据,由所述交易接收方对所述交易根进行验证,并在验证通过后,发起将所述证明数据和带有所述交易发起方、所述交易接收方签名的交易根写入区块链的交易请求。

- 30 12、一种数据处理方法,其特征在于,包括:

交易接收方接收交易发送方发送的交易根和证明数据;所述交易根为以交易数据为

预定单向函数的输入获取的, 所述证明数据用于证明所述交易数据中的需要隐藏的信息;

根据所述需要隐藏的信息和所述预定单向函数对所述交易根进行验证;

- 5 若验证结果为通过, 则发起将所述证明数据和带有所述交易发起方、所述交易接收方签名的交易根写入区块链的交易请求, 以使区块链中的节点对所述交易根和所述证明数据进行共识验证, 并根据验证结果响应/拒绝响应所述交易请求。

13、一种数据处理方法, 其特征在于, 包括:

- 接收交易接收方发送的交易请求, 所述交易请求用于请求将交易根和证明数据写入区块链; 所述交易根为以交易发起方发起的交易数据为预定单向函数的输入获取的, 所述证明数据用于证明所述交易数据中的需要隐藏的信息;
- 10

对所述交易根进行验证, 获取第一验证结果; 根据所述交易根对所述证明数据进行验证, 获取第二验证结果;

根据所述第一验证结果和所述第二验证结果响应/拒绝响应所述交易请求。

- 14、根据权利要求 13 所述的方法, 其特征在于, 所述对所述交易根进行验证包括:
- 15 确定与所述交易根中的输出交易根具有关联关系的地址, 所述输出交易根为根据所述交易数据中交易后的数据构建的;

若判断获知地址的数量为大于等于预定阈值, 则验证所述交易根是否携带有与所述交易发起方和所述交易接收方对应的签名。

15、一种数据处理装置, 其特征在于, 包括:

- 20 确定单元, 用于确定交易数据中需要隐藏的信息;

处理单元, 用于以所述交易数据为预定单向函数的输入, 获取所述预定单向函数输出的交易根, 并根据所述交易根构建所述需要隐藏的信息合法的证明数据;

- 发起单元, 用于发起将所述证明数据和带有所述交易发起方签名的交易根写入区块链的交易请求, 以使区块链中的节点对所述交易根和所述证明数据进行共识验证, 并根据验证结果响应/拒绝响应所述交易请求。
- 25

16、根据权利要求 15 所述的装置, 其特征在于, 所述确定单元, 还用于确定所述交易数据中的交易前的数据和交易后的数据;

- 其中, 所述处理单元, 具体用于以交易前的数据为第一预定单向函数的输入, 获取所述第一预定单向函数输出的输入交易根; 以交易后的数据为第二预定单向函数的输入, 获取所述第二预定单向函数输出的输出交易根; 将获取的输入交易根和输出交易根作为待上链的交易根。
- 30

17、根据权利要求 16 所述的装置，其特征在于，所述处理单元，具体用于根据所述交易后的数据和随机数构建预定单向函数树的底层，并确定所述预定单向函数树的顶层对应的输出交易根。

18、根据权利要求 15 所述的装置，其特征在于，所述处理单元，具体用于以所述交易根和所述需要隐藏的信息为输入进行预定的逻辑运算；以所述需要隐藏的信息为保护对象，对所述逻辑运算进行零知识证明，获取证明数据。

19、一种数据处理装置，其特征在于，包括：

接收单元，用于接收交易发起方发送的交易请求，所述交易请求用于请求将交易根和证明数据写入区块链；所述交易根为以交易数据为预定单向函数的输入获取的，所述证明数据用于证明所述交易数据中的需要隐藏的信息；

验证单元，用于对所述交易根进行验证，获取第一验证结果；根据所述交易根对所述证明数据进行验证，获取第二验证结果；

响应单元，用于根据所述第一验证结果和所述第二验证结果响应/拒绝响应所述交易请求。

20、根据权利要求 19 所述的装置，其特征在于，所述验证单元，具体用于验证所述交易根是否有合法的签名。

21、根据权利要求 20 所述的方法，其特征在于，所述验证单元，具体用于确定与所述交易根中的输出交易根具有关联关系的地址，所述输出交易根为根据所述交易数据中交易后的数据构建的；若判断获知地址的数量为 1，则验证所述交易根是否有与所述交易发起方对应的签名。

22、根据权利要求 19 所述的装置，其特征在于，所述验证单元，具体用于验证所述交易根中的输出交易根与已上链的输出交易根和输入交易根是否重复；所述输出交易根为根据所述交易数据中交易后的数据构建的。

23、根据权利要求 19 所述的装置，其特征在于，所述验证单元，具体用于验证所述交易根中的输入交易根与已上链的输出交易根和输入交易根是否重复；所述输入交易根为根据所述交易数据中交易前的数据构建的。

24、根据权利要求 19 所述的装置，其特征在于，所述响应单元，具体用于若所述第一验证结果和所述第二验证结果均为通过，则响应所述交易请求，以将带有交易发起方签名的交易根和证明数据写入区块链；若所述第一验证结果和/或所述第二验证结果为未通过，则拒绝响应所述交易请求。

25、一种数据处理装置，其特征在于，包括：

确定单元,用于交易发起方确定交易数据中的需要隐藏的信息;

处理单元,用于以所述交易数据为预定单向函数的输入,获取所述预定单向函数输出的交易根,并根据所述交易根构建所述需要隐藏的信息合法的证明数据;

5 发送单元,用于向交易接收方发送所述交易根和所述证明数据,由所述交易接收方对所述交易根进行验证,并在验证通过后,发起将所述证明数据和带有所述交易发起方、所述交易接收方签名的交易根写入区块链的交易请求。

26、一种数据处理装置,其特征在于,包括:

10 接收单元,用于接收交易发送方发送的交易根和证明数据;所述交易根为以交易数据为预定单向函数的输入获取的,所述证明数据用于证明所述交易数据中的需要隐藏的信息;

验证单元,用于根据所述需要隐藏的信息和所述预定单向函数对所述交易根进行验证;

15 发起单元,用于若验证结果为通过,则发起将所述证明数据和带有所述交易发起方、所述交易接收方签名的交易根写入区块链的交易请求,以使区块链中的节点对所述交易根和所述证明数据进行共识验证,并根据验证结果响应/拒绝响应所述交易请求。

27、一种数据处理装置,其特征在于,包括:

接收单元,用于接收交易接收方发送的交易请求,所述交易请求用于请求将交易根和证明数据写入区块链;所述交易根为以交易发起方发起的交易数据为预定单向函数的输入获取的,所述证明数据用于证明所述交易数据中的需要隐藏的信息;

20 验证单元,用于对所述交易根进行验证,获取第一验证结果;根据所述交易根对所述证明数据进行验证,获取第二验证结果;

响应单元,用于根据所述第一验证结果和所述第二验证结果响应/拒绝响应所述交易请求。

25 28、根据权利要求 27 所述的装置,其特征在于,所述验证单元,具体用于确定与所述交易根中的输出交易根具有关联关系的地址,所述输出交易根为根据所述交易数据中交易后的数据构建的;若判断获知地址的数量为大于等于预定阈值,则验证所述交易根是否携带有与所述交易发起方和所述交易接收方对应的签名。

29、一种数据处理装置,包括:

处理器;以及

30 被安排成存储计算机可执行指令的存储器,所述可执行指令在被执行时使所述处理器执行以下操作:

- 确定交易数据中需要隐藏的信息;
- 以所述交易数据为预定单向函数的输入, 获取所述预定单向函数输出的交易根, 并根据所述交易根构建所述需要隐藏的信息合法的证明数据;
- 发起将所述证明数据和带有所述交易发起方签名的交易根写入区块链的交易请求,
- 5 以使区块链中的节点对所述交易根和所述证明数据进行共识验证, 并根据验证结果响应/拒绝响应所述交易请求。

- 30、一种数据处理装置, 包括:
- 处理器; 以及
- 被安排成存储计算机可执行指令的存储器, 所述可执行指令在被执行时使所述处理
- 10 器执行以下操作:
- 接收交易发起方发送的交易请求, 所述交易请求用于请求将交易根和证明数据写入区块链; 所述交易根为以交易数据为预定单向函数的输入获取的, 所述证明数据用于证明所述交易数据中的需要隐藏的信息;
- 对所述交易根进行验证, 获取第一验证结果; 根据所述交易根对所述证明数据进行
- 15 验证, 获取第二验证结果;
- 根据所述第一验证结果和所述第二验证结果响应/拒绝响应所述交易请求。

- 31、一种数据处理装置, 包括:
- 处理器; 以及
- 被安排成存储计算机可执行指令的存储器, 所述可执行指令在被执行时使所述处理
- 20 器执行以下操作:
- 确定交易数据中的需要隐藏的信息;
- 以所述交易数据为预定单向函数的输入, 获取所述预定单向函数输出的交易根, 并根据所述交易根构建所述需要隐藏的信息合法的证明数据;
- 向交易接收方发送所述交易根和所述证明数据, 由所述交易接收方对所述交易根进
- 25 行验证, 并在验证通过后, 发起
- 将所述证明数据和带有所述交易发起方、所述交易接收方签名的交易根写入区块链的交易请求。

- 32、一种数据处理装置, 包括:
- 处理器; 以及
- 30 被安排成存储计算机可执行指令的存储器, 所述可执行指令在被执行时使所述处理
- 器执行以下操作:

接收交易发送方发送的交易根和证明数据；所述交易根为以交易数据为预定单向函数的输入获取的，所述证明数据用于证明所述交易数据中的需要隐藏的信息；

根据所述需要隐藏的信息和所述预定单向函数对所述交易根进行验证；

- 5 若验证结果为通过，则发起将所述证明数据和带有所述交易发起方、所述交易接收方签名的交易根写入区块链的交易请求，以使区块链中的节点对所述交易根和所述证明数据进行共识验证，并根据验证结果响应/拒绝响应所述交易请求。

33、一种数据处理装置，包括：

处理器；以及

- 10 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

接收交易接收方发送的交易请求，所述交易请求用于请求将交易根和证明数据写入区块链；所述交易根为以交易发起方发起的交易数据为预定单向函数的输入获取的，所述证明数据用于证明所述交易数据中的需要隐藏的信息；

- 15 对所述交易根进行验证，获取第一验证结果；根据所述交易根对所述证明数据进行验证，获取第二验证结果；

根据所述第一验证结果和所述第二验证结果响应/拒绝响应所述交易请求。