

一种数据处理方法和装置

技术领域

[01] 本发明涉及计算机技术领域，尤其涉及一种数据处理方法和装置。

5 背景技术

[02] “区块链”技术最初是由一位化名“中本聪”的人为一种数字货币-比特币而设计出的一种特殊的分布式数据库技术。它适合存储简单的、有先后关系的、能在系统内验证的数据，并用密码学和共识算法保证了存储的数据的不可篡改、不可伪造以及全网公开透明。

10 [03] 由于每个账户里的资产、交易记录都是公开的，因此，当任意一个账户获取到其他账户的账户地址时，即可通过区块链查询到其他账户里的所有资产和历史交易。

[04] 需要提供更加可靠的方案。

发明内容

15 [05] 本说明书实施例提供一种数据处理方法和装置，用于解决现有的区块链技术容易出现数据被泄露的问题。

[06] 本说明书实施例提供一种数据处理方法，包括：

[07] 交易发起方确定交易数据中需要隐藏的信息；

20 [08] 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；

[09] 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。

[10] 可选的，在以所述交易数据为预定单向函数的输入之前，还包括：

25 [11] 确定所述交易数据中的交易前的数据和交易后的数据；

- [12]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:
- [13]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;
- 5 [14]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;
- [15]将获取的输入交易根和输出交易根作为待上链的交易根。
- [16]可选的,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包括:
- 10 [17]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]可选的,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:
- [19]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;
- [20]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。
- 15 [21]本说明书实施例提供一种数据处理方法,包括:
- [22]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;
- 20 [23]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;
- [24]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]可选的,所述对所述交易根进行验证包括:
- [26]验证所述交易根是否有合法的签名。
- 25 [27]可选的,验证所述交易根是否有合法的签名包括:
- [28]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;

- [29]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。
- [30]可选的，所述对所述交易根进行验证包括：
- [31]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。
- [32]可选的，所述对所述交易根进行验证包括：
- [33]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。
- [34]可选的，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：
- [35]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；
- [36]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。
- [37]本说明书实施例提供一种数据处理方法，包括：
- [38]交易发起方确定交易数据中的需要隐藏的信息；
- [39]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；
- [40]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。
- [41]本说明书实施例提供一种数据处理方法，包括：
- [42]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；
- [43]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；
- [44]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。

[45]本说明书实施例提供一种数据处理方法，包括：

[46]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；

[47]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；

[48]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。

[49]可选的，所述对所述交易根进行验证包括：

[50]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；

[51]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。

[52]本说明书实施例提供一种数据处理装置，包括：

[53]确定单元，用于确定交易数据中需要隐藏的信息；

[54]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；

[55]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。

[56]可选的，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；

[57]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。

[58]可选的，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。

[59]可选的，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。

5 [60]本说明书实施例提供一种数据处理装置，包括：

[61]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；

10 [62]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；

[63]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。

[64]可选的，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。

15 [65]可选的，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。

[66]可选的，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。

20 [67]可选的，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。

[68]可选的，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；

25 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。

[69]本说明书实施例提供一种数据处理装置，包括：

[70]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；

[71]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；

[72]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。

5 [73]本说明书实施例提供一种数据处理装置，包括：

[74]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；

10 [75]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；

[76]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。

[77]本说明书实施例提供一种数据处理装置，包括：

15 [78]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；

[79]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；

20 [80]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。

[81]可选的，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。

25

[82]本说明书实施例提供一种数据处理装置，包括：

[83]处理器；以及

[84]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:

[85]确定交易数据中需要隐藏的信息;

[86]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 [87]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。

[88]本说明书实施例提供一种数据处理装置,包括:

[89]处理器;以及

- 10 [90]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:

[91]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;

- 15 [92]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;

[93]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。

[94]本说明书实施例提供一种数据处理装置,包括:

[95]处理器;以及

- 20 [96]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:

[97]确定交易数据中的需要隐藏的信息;

[98]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;

- 25 [99]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。

- [100] 本说明书实施例提供一种数据处理装置，包括：
- [101] 处理器；以及
- [102] 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：
- 5 [103] 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；
- [104] 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；
- [105] 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
- 10 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。
- [106] 本说明书实施例提供一种数据处理装置，包括：
- [107] 处理器；以及
- [108] 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：
- 15 [109] 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；
- [110] 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；
- 20 [111] 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。
- [112] 本说明书实施例采用的上述至少一个技术方案能够达到以下有益效果：
- [113] 可见，本实施例首先通过单向函数保证交易数据的真实性和不可篡改，然后，通过构建证明数据来证明需要隐藏的信息的合法性，而又不会向非交易参与方透露任何需要隐藏的信息。与现有中任意一个节点的数据被泄露将会导致所有数据被泄露的方案
- 25 相比，基本是节点中的数据被泄露，攻击者依然无法查看到各方节点的隐私数据，因此，能达到提高区块链数据安全性的目的。

附图说明

[114] 此处所说明的附图用来提供对本发明的进一步理解，构成本发明的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

5 [115] 图 1a 和图 1b 为本说明书实施例提供一种数据处理方法的应用场景示意图图；

[116] 图 2 为本说明书实施例 1 提供一种数据处理方法的流程示意图；

[117] 图 3 为本说明书实施例 2 提供一种数据处理方法的流程示意图；

[118] 图 4 为本说明书实施例 3 提供一种数据处理方法的流程示意图；

[119] 图 5 为本说明书实施例 4 提供一种数据处理方法的流程示意图；

10 [120] 图 6a 为本说明书实施例 5 提供一种数据处理方法中构建交易根的流程示意图；

[121] 图 6b 为本说明书实施例 5 提供一种数据处理方法中构建证明数据的流程示意图；

[122] 图 7 为本说明书实施例 6 提供一种数据处理装置的结构示意图；

15 [123] 图 8 为本说明书实施例 7 提供一种数据处理装置的结构示意图；

[124] 图 9 为本说明书实施例 8 提供一种数据处理装置的结构示意图；

[125] 图 10 为本说明书实施例 9 提供一种数据处理装置的结构示意图；

[126] 图 11 为本说明书实施例 10 提供一种数据处理装置的结构示意图；

[127] 图 12 为本说明书实施例 11 提供一种电子设备的结构示意图。

20

具体实施方式

[128] 为使本发明的目的、技术方案和优点更加清楚，下面将结合本发明具体实施例及相应的附图对本发明技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，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，都属于本发明保护的范围。

25

[129] 需要说明的是，单向函数为，满足对于所有属于 f 定义域的任一 x ，可以很容易计算 $f(x) = y$ ；对于几乎所有属于 f 值域的任一 y ，则在计算上不可能求出 x 使得 $y = f(x)$ 。即：对于任何输入，容易计算输出，但是已知输出，很难推断输入。

[130] 零知识证明为，证明者能够在不向验证者提供任何有用的信息（受保护/隐藏信息）的情况下，使验证者相信某个论断是正确的。

[131] 参见图 1a，本发明的一个应用场景可以为：

[132] 区块链上的节点 A 需要将一笔钱由节点 A 对应的交易发起方的第一账户转账至该交易发起方的第二账户，或者，将第一账户和第二账户进行合并。在将转账/合并以交易的形式请求写入区块链之前，节点 A 先确定该交易的交易数据中的需要隐藏的信息，例如：第一账户和第二账户的输入（如：交易前的余额）、输出（如：交易后的余额）等。然后，计算出该交易的交易根，并基于交易根构建需要隐藏的信息的证明数据，以证明需要隐藏的信息的合法性、真实性等。然后，将交易根和证明数据以交易的形式请求写入区块链中。

[133] 不难理解的是，区块链允许同一个人申请多个账户，但区块链是签名机制为每人分配唯一对应的签名。因此，在交易发生在同一人 A 的不同账户之间时，交易仅有 A 的签名即可。

[134] 参见图 1b，本发明的另一个应用场景可以为：

[135] 区块链上的节点 A 需要将一笔钱由交易发起方转账至节点 B 对应的交易接收方。在将转账以交易的形式请求写入区块链之前，节点 A 先确定该交易的交易数据中的需要隐藏的信息，例如：交易发起方和交易接收方的输入、输出，交易发起方和交易接收方的余额等。然后，计算出该交易的交易根，并基于交易根构建需要隐藏的信息的证明数据，以证明需要隐藏的信息的有效性、真实性等。然后，将交易根和证明数据发送至交易接收方，由交易接收方对交易根进行验证，若验证无误，则由交易接收方对交易根签名后，发起将证明数据和带有交易发起方、交易接收方签名的交易根写入区块链的交易请求。或者，交易接收方在对交易根签名后，将签名后的交易根+验证结果返回给交易发起方，以指示交易发起方发起将证明数据和带有交易发起方、交易接收方签名的交易根写入区块链的交易请求。

[136] 其中，在上述两个应用场景中，转账或者合并均是為了便于理解“交易”而做出的示例，但实际上，“交易”还可以为在节点 A 中记录一条信息、节点 A 将一条信

息发送给节点 B 等等，相应地，“需要隐藏的信息”也可自由设置，例如：交易双方的余额等，此处不做限定。

[137] 以下结合附图，详细说明本发明各实施例提供的技术方案。

[138] 实施例 1

5 [139] 图 2 为本说明书实施例 1 提供的一种数据处理方法的流程示意图，该方法可由区块链中的参与交易的节点来执行，具体可以包括如下步骤：

[140] 步骤 22、交易发起方确定交易数据中需要隐藏的信息；

[141] 需要说明的是，步骤 22 的一种实现方式可以为：

10 [142] 节点获取交易发起方（用户）完成的交易清单，交易清单中记载有选项以及选项对应的内容，例如：收款人、付款人、收款人交易前后余额、付款人交易前后余额等。然后，基于预定的隐藏规则，从中选取出对应的信息。

[143] 其中，隐藏规则可以为：基于预设置的隐藏选项，确定交易清单中与隐藏选项对应的选项及其内容，并作为需要隐藏的信息。隐藏选项举例为：收款人交易前后余额、付款人交易前后余额。

15 [144] 隐藏规则还可以为：基于预设置的筛选规则，从交易清单中选出与特定关键词对应的数据，例如：特定关键词为“余额”或者“交易额”，则筛选出的对应的数字，并将筛选出的数据作为需要隐藏的信息。

[145] 需要说明的是，步骤 22 的另一种实现方式可以为：

20 [146] 交易发起方在完成交易清单的过程中，自定义该交易清单中需要隐藏的数据并进行标记。例如：标记收款人交易前后余额、付款人交易前后余额。

[147] 则节点在获取到交易发起方完成交易清单后，基于标记确定交易数据中需要隐藏的信息。

[148] 步骤 24、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；

25 [149] 需要说明的是，步骤 24 中构建交易根的一种实现方式可以为：

[150] 首先，节点基于交易数据对应的交易清单，对交易数据进行解析，以确定其中的交易前的数据和交易后的数据。例如：收款人交易前后余额、付款人交易前后余额。

[151] 然后, 将交易前的数据作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; 将交易后的数据作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。其中, 第一预定单向函数和第二预定单向函数可以为同一单向函数。

5 [152] 其中, 单向函数可以为单向函数树, 相应地, 构建输入交易根/输出交易根的步骤可以具体为: 根据交易前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入交易根/输出交易根。例如: 通过在交易前后的余额后面添加固定长度的随机数, 比如定义一个 128bit 的数字, 前 10bit 表示余额, 后面的 bit 为随机数。

10 [153] 不难理解的是, 输入交易根和输出交易根的数量为至少一个。例如: (rootA (叶节点为 A 的账户余额 100), rootB (叶节点为 B 的账户余额 800), rootA' (叶节点为 A 的账户余额 50), rootB' (叶节点为 B 的账户余额 950)。其中, rootA 和 rootB 为输入交易根, rootA' 和 rootB' 未输出交易根。另外, 在构建交易根的过程中, 添加随机数的作用是为了区分每个输入交易根和输出交易根, 以在后续共识节点对其进行验证时,
15 以防止碰撞。

[154] 步骤 24 中构建证明数据的一种实现方式可以为:

[155] 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。

20 [156] 需要说明的是, 预定的逻辑运算可以为根据需要证明的内容而自定义的特定函数。例如: 当需要证明交易发起方的第一账户与第二账户之间发生了交易时, 则特定函数可以具体为以交易根和需要隐藏的信息为输入, 计算交易前的第一账户、第二账户的余额和交易后的第一账户、第二账户的余额是否相同, 或者, 交易前的余额与交易后的余额差值不超过 n 元, 交易后第二账户的利息发生了增长了等等。然后, 将整个函数运算过程用零知识证明的方式输出一个证明, 即证明隐藏的信息可以用来计算特定函数。

25 [157] 步骤 26、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。

[158] 可见, 本实施例首先通过单向函数保证交易数据的真实性和不可篡改, 然后, 通过构建证明数据来证明需要隐藏的信息的合法性, 而又不会向非交易参与方透露任何

需要隐藏的信息。与现有技术相比，能有效防止由于任意一个节点的数据被泄露而影响整个区块链数据的隐私，达到提高区块链数据安全性的目的。

[159] 实施例 2

[160] 图 3 为本说明书实施例 2 提供的一种数据处理方法的流程示意图，该方法可由
5 区块链中的共识节点执行，具体可以包括如下步骤：

[161] 步骤 32、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；

[162] 需要说明的是，步骤 32 可以为在实施例 1 的基础上进行的步骤，其中的交易请求、交易根和证明数据等在实施例 1 中均有相关描述，故，此处不再对其进行赘述。
10

[163] 步骤 34、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；

[164] 步骤 34 中验证交易根的一种实现方式可以为：

[165] 验证所述交易根是否有合法的签名，若是，则第一验证结果为通过，若否，则
15 第一验证结果为未通过。

[166] 具体地，首先，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。

[167] 不难理解的是，每个输出交易根均对应一个地址 hash(pk)，基于该地址可判定此
20 交易的参与方有哪些，然后，验证交易根是否有所有参与方的签名且合法。例如：地址只有 1 个，则可以认为是同一用户的不同账户之间的交易。进而若验证出该用户的签名无误，则第一验证结果为通过。

[168] 另外，对于签名的验证涉及区块链的数字签名机制，此处不做限定。

[169] 步骤 34 中验证交易根的另一实现方式可以为：

[170] 在步骤 34 中验证交易根的上一种实现方式的基础上，本实现方式还进一步地：
25

[171] 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，若是，则确定第一验证结果为未通过，若否，且有合法签名，则确定第一验证结果为通过。

[172] 具体的，验证输出交易根的目的是避免出现“碰撞”。此处的碰撞可以理解为：存在与该输出交易根具有同一（用户）签名且相同的输入交易根或输出交易根，导致的无法判定交易根对应的“钱”是用户未“花”的“钱”，还是该用户之前已经“花”了的“钱”。

- 5 [173] 而由于在构建输出交易根时，向交易后的数据中添加了随机数，因此，得出的输出交易根具有唯一性。进而，可对比处该输出交易根与已经上链的输出交易根和输出交易根是否重复，并基于对比结果判定是否发生碰撞。

[174] 步骤 34 中验证交易根的另一种实现方式可以为：

- 10 [175] 在上一实现方式的基础上，进一步地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。

[176] 本实现方式中，验证输入交易根的目的旨在避免“双花”。此处的“双花”可以理解为：用户将输入交易根对应的“钱”同时交易给其他两个用户。由于其避免方式与验证输出交易根的方式相似，故，此处不再赘述。

- 15 [177] 对于步骤 34 的后两种实现方式，节点区分输入交易根和输出交易根的方式可以为：存在未花费的交易输出(Unspent Transaction Outputs, UTXO)的交易根为输入交易根，其余则为输出交易根。

[178] 步骤 34 中验证证明数据的一种实现方式可以为：

- 20 [179] 共识节点基于交易根用零知识证明算法验证证明数据，若验证通过，则确定证明无误。

[180] 步骤 36、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 [181] 需要说明的是，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。

[182] 可见，本实施例首先通过单向函数保证交易数据的真实性和不可篡改，然后，通过构建证明数据来证明需要隐藏的信息的合法性，而又不会向非交易参与方透露任何需要隐藏的信息。与现有技术相比，能有效防止由于任意一个节点的数据被泄露而影响

到整个区块链数据的隐私，达到提高区块链数据安全性的目的。

[183] 实施例 3

[184] 图 4 为本说明书实施例 3 提供的一种数据处理方法的流程示意图，参见图 4，该方法可以有区块链中的节点执行，具体包括如下

5 [185] 步骤 42、交易节点 A（交易发起方）确定交易数据中的需要隐藏的信息；

[186] 步骤 44、交易节点 A 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；

[187] 步骤 46、交易节点 A 向交易节点 B（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
10 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。

[188] 步骤 48、交易节点 B 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；

[189] 步骤 410、交易节点 B 确定验证是否通过；

[190] 步骤 412、若验证结果为通过，则交易节点 B 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
15 请求。

[191] 步骤 414、共识节点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；

20 [192] 步骤 414 的一种实现方式可以为：

[193] 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。其中，预定阈值可以具体为 2。

25 [194] 不难理解的是，每个输出交易根均有对应的地址，基于地址确定参与交易的节点，进而验证参与交易的节点是否都有在交易根上签名，若是且签名合法，则第一验证结果为通过。

[195] 步骤 416、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。

[196] 可见，本实施例首先通过单向函数保证交易数据的真实性和不可篡改，然后，通过构建证明数据来证明需要隐藏的信息的合法性，而又不会向非交易参与方透露任何需要隐藏的信息。与现有技术相比，能有效防止由于任意一个节点的数据被泄露而影响
5 到整个区块链数据的隐私，达到提高区块链数据安全性的目的。

[197] 实施例 4

[198] 图 5 为本说明书实施例 4 提供的一种数据处理方法的流程示意图，参见图 5，该方法可以有区块链中的节点执行，具体包括如下

[199] 步骤 52、交易节点 A（交易发起方）确定交易数据中的需要隐藏的信息；

10 [200] 步骤 54、交易节点 A 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；

[201] 步骤 56、交易节点 A 向交易节点 B（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。

15 [202] 步骤 58、交易节点 B 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；

[203] 步骤 510、交易节点 B 确定验证是否通过；

[204] 步骤 512、若验证结果为通过，则交易节点 B 对交易根进行签名，并向交易节点 A 发送允许上链的指示信息；

20 [205] 步骤 514、交易节点 A 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。

[206] 步骤 516、共识节点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；

25 [207] 步骤 518、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。

[208] 可见，本实施例首先通过单向函数保证交易数据的真实性和不可篡改，然后，通过构建证明数据来证明需要隐藏的信息的合法性，而又不会向非交易参与方透露任何需要隐藏的信息。与现有技术相比，能有效防止由于任意一个节点的数据被泄露而影响

到整个区块链数据的隐私，达到提高区块链数据安全性的目的。

[209] 实施例 5

[210] 结合图 6a 和 6b，下面以实例的方式对本说明书进行详细说明，具体可以包括如下步骤：

5 [211] 步骤 S62、参见图 6a，在交易上链前，区块链中的交易组织为分层的单向函数结构，最底层采用的是交易的明文，交易发起方通过单向函数做成树状，最后形成一个交易根 root。其中，明文可以作为需要隐藏的信息。

[212] 不难理解的是，因为所有交易内容都通过单向函数来组织，所以把交易根上链不会泄露任何数据隐私。

10 [213] 当然，交易组织格式也可以是非树状的任何单向函数形式。

[214] 步骤 S64、参见图 6b，假如需要利用交易数据计算特定函数 f，f 需要同时输入作为隐藏信息的交易 1（交易根为 root）的数据 2、交易 2（交易根为 root'）的数据 3'、交易 3（交易根为 root''）的数据 1''，即

[215] 运算结果=f(数据 2， 数据 3'， 数据 1'')

15 [216] root= 交易根(数据 2)

[217] root'=交易根(数据 3')

[218] root''=交易根(数据 1'')

[219] 那么，可以通过零知识证明，交易发起方证明以上所有陈述的正确性，但是又不泄露数据 2、数据 3'、数据 1''。

20 [220] 需要说明的是，特定函数 f 为基于需要证明的隐藏的信息自定义的函数，以能起到证明为准，函数类型不限。例如：以交易双方的交易前的余额和交易后的余额为输入，计算两者的差值；或者，以交易发起方的交易前后的余额为输入，计算交易发起方的交易前后的余额差值不超过 m 等等。

25 [221] 步骤 S66、接收方（交易接收方或者区块链中的非交易参与节点）接收到证明后，利用零知识证明验证该证明的正确性，因而也确信了运算结果的正确性。

[222] 但是接收方只知道运算结果，假如运算函数本身不泄露除运算结果的信息，那么接收方不会知道函数的输入数据信息。

[223] 可见，本实施例可以用于一方向另外一方证明已上链交易的内容可以用来计算特定函数，但是该函数的运算又不暴露任何一方数据隐私。区块链通过单向函数保证数

据内容的真实性 and 不可篡改, 零知识证明保证数据运算过程满足双方实现约定的特定函数、以及该数据确实存在已经上链的交易。

[224] 对于上述方法实施方式, 为了简单描述, 故将其都表述为一系列的动作组合, 但是本领域技术人员应该知悉, 本发明实施方式并不受所描述的动作顺序的限制, 因为
5 依据本发明实施方式, 某些步骤可以采用其他顺序或者同时进行。其次, 本领域技术人员也应该知悉, 说明书中所描述的实施方式均属于优选实施方式, 所涉及的动作并不一定是本发明实施方式所必须的。

[225] 实施例 6

[226] 图 7 为本说明书实施例 6 提供的一种数据处理装置的结构示意图, 参见图 7, 该
10 装置具体可以包括: 确定单元 71、处理单元 72 和发起单元 73, 其中:

[227] 确定单元 71, 用于确定交易数据中需要隐藏的信息;

[228] 处理单元 72, 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;

[229] 发起单元 73, 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
15 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。

[230] 本实施例中, 确定单元 71, 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;

[231] 相应地, 所述处理单元 72, 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。
20

[232] 处理单元 72, 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。

[233] 处理单元 72, 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。
25

[234] 实施例 7

[235] 图 8 为本说明书实施例 7 提供的一种数据处理装置的结构示意图, 参见图 8, 该装置具体可以包括: 接收单元 81、验证单元 82 和响应单元 83, 其中:

[236] 接收单元 81, 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;

[237] 验证单元 82, 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;

[238] 响应单元 83, 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。

10 [239] 其中, 所述验证单元 82 的工作原理可以为:

[240] 验证所述交易根是否有合法的签名。具体地: 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。

15 [241] 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。

[242] 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。

[243] 响应单元 83 的工作原理可以为:

20 [244] 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。

[245] 实施例 8

[246] 图 9 为本说明书实施例 8 提供的一种数据处理装置的结构示意图, 参见图 9, 该装置具体可以包括: 确定单元 91、处理单元 92 和发送单元 93, 其中:

25 [247] 确定单元 91, 用于交易发起方确定交易数据中的需要隐藏的信息;

[248] 处理单元 92, 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;

[249] 发送单元 93, 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。

[250] 实施例 9

5 [251] 图 10 为本说明书实施例 9 提供的一种数据处理装置的结构示意图, 参见图 10, 该装置具体可以包括: 接收单元 101、验证单元 102 和发起单元 103, 其中:

[252] 接收单元 101, 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;

10 [253] 验证单元 102, 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;

[254] 发起单元 103, 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
15 求。

[255] 实施例 10

[256] 图 11 为本说明书实施例 10 提供的一种数据处理装置的结构示意图, 参见图 11, 该装置具体可以包括: 接收单元 111、验证单元 112 和响应单元 113, 其中:

[257] 接收单元 111, 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
20 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;

[258] 验证单元 112, 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;

[259] 响应单元 113, 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
25 所述交易请求。

[260] 其中, 验证单元 112, 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。

[261] 对于上述装置实施方式而言，由于其与方法实施方式基本相似，所以描述的比较简单，相关之处参见方法实施方式的部分说明即可。

5 [262] 应当注意的是，在本发明的装置的各个部件中，根据其要实现的功能而对其中的部件进行了逻辑划分，但是，本发明不受限于此，可以根据需要对各个部件进行重新划分或者组合。

[263] 实施例 11

10 [264] 图 12 为本说明书实施例 11 提供的一种电子设备的结构示意图，参见图 12，该电子设备包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成数据处理装置。当然，除了软件实现方式之外，本说明书并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限于各个逻辑单元，也可以是硬件或逻辑器件。

15 [265] 网络接口、处理器和存储器可以通过总线系统相互连接。总线可以是 ISA(Industry Standard Architecture，工业标准体系结构)总线、PCI(Peripheral Component Interconnect，外设部件互连标准)总线或 EISA(Extended Industry Standard Architecture，扩展工业标准结构)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 12 中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

20 [266] 存储器用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括只读存储器和随机存取存储器，并向处理器提供指令和数据。存储器可能包含高速随机存取存储器(Random-Access Memory，RAM)，也可能还包括非易失性存储器(non-volatile memory)，例如至少 1 个磁盘存储器。

[267] 处理器，用于执行所述存储器存放的程序，并具体执行：

25 [268] 确定交易数据中需要隐藏的信息；

[269] 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；

[270] 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。

[271] 还用于,

5 [272] 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;

[273] 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;

[274] 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。

10 [275] 还用于,

[276] 确定交易数据中的需要隐藏的信息;

[277] 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;

15 [278] 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。

[279] 还用于,

[280] 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;

20 [281] 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;

[282] 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。

[283] 还用于,

25 [284] 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;

[285] 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;

[286] 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。

[287] 上述如本说明书图 2-10 所示实施例揭示的数据处理装置或管理者 (Master) 节点执行的方法可以应用于处理器中, 或者由处理器实现。处理器可能是一种集成电路芯片, 具有信号的处理能力。在实现过程中, 上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器, 包括中央处理器 (Central Processing Unit, CPU)、网络处理器 (Network Processor, NP) 等; 还可以是数字信号处理器 (Digital Signal Processor, DSP)、专用集成电路 (Application Specific Integrated Circuit, ASIC)、现场可编程门阵列 (Field - Programmable Gate Array, FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本说明书实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本说明书实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成, 或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器, 闪存、只读存储器, 可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器, 处理器读取存储器中的信息, 结合其硬件完成上述方法的步骤。

[288] 数据处理装置还可执行图 2-图 5 的方法, 并实现管理者节点执行的方法。

[289] 实施例 12

[290] 基于相同的发明创造, 本说明书实施例还提供了一种计算机可读存储介质, 所述计算机可读存储介质存储一个或多个程序, 所述一个或多个程序当被包括多个应用程序的电子设备执行时, 使得所述电子设备执行实施例 1-5 提供的数据处理方法。

[291] 本说明书中的各个实施例均采用递进的方式描述, 各个实施例之间相同相似的部分互相参见即可, 每个实施例重点说明的都是与其他实施例的不同之处。尤其, 对于系统实施例而言, 由于其基本相似于方法实施例, 所以描述的比较简单, 相关之处参见方法实施例的部分说明即可。

[292] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下, 在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外, 在附图中描绘的过程不一定要求示出的特

定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[293] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[294] 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[295] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[296] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[297] 在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

[298] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

[299] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他

数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

[300] 还需要说明的是，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、商品或者设备不仅包括那些要素，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、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[301] 本领域技术人员应明白，本发明的实施例可提供为方法、系统或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[302] 以上所述仅为本发明的实施例而已，并不用于限制本发明。对于本领域技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本发明的权利要求范围之内。