(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107273759 A
(43)申请公布日 2017.10.20

(21)申请号 201710318981.8

(22)申请日 2017.05.08

(71)申请人 上海点融信息科技有限责任公司
地址 200023 上海市黄浦区局门路457号八号桥四期3楼

(72)发明人 陈曦

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 酆迅 潘聪

(51)Int.Cl.
G06F 21/62(2013.01)
H04L 29/06(2006.01)

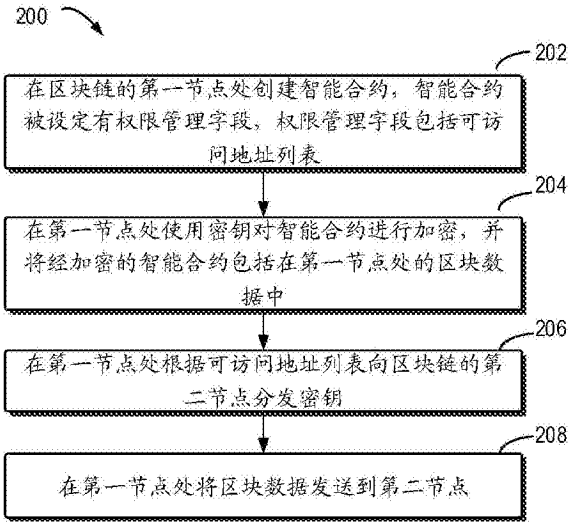
权利要求书2页 说明书9页 附图3页

(54)发明名称

用于保护区块链数据的方法、设备以及计算机可读存储介质

(57)摘要

本公开涉及用于保护区块链数据的方法、设备以及计算机可读存储介质。该用于保护区块链数据的方法包括：在区块链的第一节点处创建智能合约，智能合约被设定有权限管理字段，权限管理字段包括可访问地址列表；在第一节点处使用密钥对智能合约进行加密，并将经加密的智能合约包括在第一节点处的区块数据中；在第一节点处根据可访问地址列表向区块链的第二节点分发密钥；以及在第一节点处将区块数据发送到第二节点。



CN 107273759 A

1.一种用于保护区块链数据的方法,包括:

在所述区块链的第一节点处创建智能合约,所述智能合约被设定有权限管理字段,所述权限管理字段包括可访问地址列表;

在所述第一节点处使用密钥对所述智能合约进行加密,并将经加密的所述智能合约包括在所述第一节点处的区块数据中;

在所述第一节点处根据所述可访问地址列表向所述区块链的第二节点分发所述密钥;以及

在所述第一节点处将所述区块数据发送到所述第二节点。

2.根据权利要求1所述的方法,其中,所述权限管理字段还包括所述第二节点对所述智能合约的访问权限,所述访问权限包括设定读写权限的读写访问权限。

3.根据权利要求1或2所述的方法,其中,所述在所述第一节点处根据所述可访问地址列表向所述第二节点分发所述密钥包括:

以点对点通信进行密钥分发,所述密钥包括对称密钥。

4.根据权利要求1或2所述的方法,其中,在所述第二节点处接收所述密钥和所述区块数据,并使用所述密钥从所述区块数据中解密经加密的所述智能合约,以创建经解密的所述智能合约。

5.根据权利要求4所述的方法,其中,在所述第二节点处根据经解密的所述智能合约来执行交易。

6.根据权利要求1或2所述的方法,其中,所述区块数据还包括区块号、交易数据、签名、以及随机数。

7.根据权利要求6所述的方法,其中,所述智能合约的历史交易数据和当前状态被逻辑隔离地存储在数据库中,所述智能合约的当前状态根据所述数据库中存储的所述区块号和所述智能合约的智能合约号进行查询。

8.根据权利要求6所述的方法,其中,所述第一节点与所述第二节点之间通过点对点通信来进行数据共识。

9.根据权利要求8所述的方法,其中,所述数据共识根据所述区块号、所述智能合约的智能合约号、以及所述智能合约的历史交易数据形成的交易数据摘要来进行。

10.根据权利要求1或2所述的方法,还包括:

在所述第一节点处将所述区块数据发送到所述区块链的第三节点,而不向所述第三节点分发所述密钥。

11.一种用于保护区块链数据的设备,包括:

处理器;

存储器,耦合至所述处理器并且存储有指令,所述指令在由所述处理器执行时使得所述设备执行以下动作:

在所述区块链的第一节点处创建智能合约,所述智能合约被设定有权限管理字段,所述权限管理字段包括可访问地址列表;

在所述第一节点处使用密钥对所述智能合约进行加密,并将经加密的所述智能合约包括在所述第一节点处的区块数据中;

在所述第一节点处根据所述可访问地址列表向所述区块链的第二节点分发所述密钥;

以及

在所述第一节点处将所述区块数据发送到所述第二节点。

12.根据权利要求11所述的设备，其中，所述权限管理字段还包括所述第二节点对所述智能合约的访问权限，所述访问权限包括设定读写权限的读写访问权限。

13.根据权利要求11或12所述的设备，其中，所述在所述第一节点处根据所述可访问地址列表向所述第二节点分发所述密钥包括：

以点对点通信进行密钥分发，所述密钥包括对称密钥。

14.根据权利要求11或12所述的设备，其中，在所述第二节点处接收所述密钥和所述区块数据，并使用所述密钥从所述区块数据中解密经加密的所述智能合约，以创建经解密的所述智能合约。

15.根据权利要求14所述的设备，其中，在所述第二节点处根据经解密的所述智能合约来执行交易。

16.根据权利要求11或12所述的设备，其中，所述区块数据还包括区块号、交易数据、签名、以及随机数。

17.根据权利要求16所述的设备，其中，所述智能合约的历史交易数据和当前状态被逻辑隔离地存储在数据库中，所述智能合约的当前状态根据所述数据库中存储的所述区块号和所述智能合约的智能合约号进行查询。

18.根据权利要求16所述的设备，其中，所述第一节点与所述第二节点之间通过点对点通信来进行数据共识。

19.根据权利要求18所述的设备，其中，所述数据共识根据所述区块号、所述智能合约的智能合约号、以及所述智能合约的历史交易数据形成的交易数据摘要来进行。

20.根据权利要求11或12所述的设备，所述指令在由所述处理器执行时使得所述设备还执行以下动作：

在所述第一节点处将所述区块数据发送到所述区块链的第三节点，而不向所述第三节点分发所述密钥。

21.一种计算机可读存储介质，具有存储在其上的计算机可读程序指令，所述计算机可读程序指令用于执行根据权利要求1-10中任一项所述的方法。

用于保护区块链数据的方法、设备以及计算机可读存储介质

技术领域

[0001] 本公开的实施例总体上涉及区块链技术，并且更具体地，涉及用于保护区块链数据的方法、设备以及计算机可读存储介质。

背景技术

[0002] 区块链作为一种新型的去中心化的记录技术而受到广泛关注。由于区块链本身不支持数据保护，因此，数据保护成为区块链应用(例如商用)的重点技术之一。

[0003] 目前已有的解决方案包括：1)多链+明文数据，即每个区块链节点需要维护多条区块链；2)同态算法或零知识证明。这两种解决方案中，第一种解决方案存在因单一区块链上节点数有限而产生的备份风险及共识风险；而第二种解决方案存在算法复杂度高，执行效率低的问题。

发明内容

[0004] 本公开的各实施例提供了用于保护区块链数据的方法、设备以及计算机可读存储介质以至少部分地解决现有技术的上述以及其它潜在问题。

[0005] 在本公开的第一方面，提供了一种用于保护区块链数据的方法。该方法包括：在区块链的第一节点处创建智能合约，智能合约被设定有权限管理字段，权限管理字段包括可访问地址列表；在第一节点处使用密钥对智能合约进行加密，并将经加密的智能合约包括在第一节点处的区块数据中；在第一节点处根据可访问地址列表向区块链的第二节点分发密钥；以及在第一节点处将区块数据发送到第二节点，

[0006] 在本公开的第二方面，提供了一种用于保护区块链数据的设备。该设备包括：处理器；存储器，耦合至处理器并且存储有指令，该指令在由处理器执行时使得设备执行以下动作：在区块链的第一节点处创建智能合约，智能合约被设定有权限管理字段，权限管理字段包括可访问地址列表；在第一节点处使用密钥对智能合约进行加密，并将经加密的智能合约包括在第一节点处的区块数据中；在第一节点处根据可访问地址列表向区块链的第二节点分发密钥；以及在第一节点处将区块数据发送到第二节点。

[0007] 在本公开的第三方面，提供了一种计算机可读存储介质。该计算机可读存储介质具有存储在其上的计算机可读程序指令，该计算机可读程序指令用于执行根据以上在本公开的第一方面中所描述的方法。

附图说明

[0008] 现将仅通过示例的方式，参考所附附图对本公开的实施例进行描述，在附图中，相同或相似的附图标注表示相同或相似的元素，其中：

[0009] 图1示出了区块链技术的示意图；

[0010] 图2示出了根据本公开的实施例的用于保护区块链数据的方法的流程示意图；

[0011] 图3示出了根据本公开的实施例的用于保护区块链数据的方法的示例实现方式；

以及

[0012] 图4示出了根据本公开的实施例的用于保护区块链数据的设备的示意图。

具体实施方式

[0013] 下面将参照附图更详细地描述本公开的实施例。虽然附图中显示了本公开的某些实施例，然而应当理解的是，本公开可以通过各种形式来实现，而且不应该被解释为限于这里阐述的实施例，相反提供这些实施例是为了更加透彻和完整地理解本公开。应当理解的是，本公开的附图及实施例仅用于示例性作用，并非用于限制本公开的保护范围。

[0014] 本文使用的术语“包括”及其变形是开放性包括，即“包括但不限于”。术语“基于”是“至少部分地基于”。术语“一个实施例”表示“至少一个实施例”；术语“另一实施例”表示“至少一个另外的实施例”。其他术语的相关定义将在下文描述中给出。

[0015] 图1示出了区块链技术的示意图，本公开的示例实施例中的方法、设备以及计算机可读存储介质可以实现于这样的场景(例如区块链网络)中。应当理解的是，区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。其中，所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。由于区块链是一种新型的去中心化的记录技术，因此受到了广泛的关注，其应用领域也日益广泛。

[0016] 关于智能合约的理念，密码学家尼克·萨博(Nick Szabo)给出的定义是“一个智能合约是一套以数字形式定义的承诺(promises)，包括合约参与方可以在上面执行这些承诺的协议”。从本质上讲，这些自动合约的工作原理类似于其它计算机程序的if-then语句。智能合约只是以这种方式与真实世界的资产进行交互。当一个预先编好的条件被触发时，智能合约执行相应的合同条款。

[0017] 传统地，由于区块链本身不支持数据保护，因此，数据保护成为区块链商用的重点技术之一。以区块链的典型应用场景——供应链管理为例，供应链的上下游企业形成了区块链上的各个节点。这一场景并不适合采用传统的多链形式进行数据交易。而且，对链上的任一企业而言，由于交易仅限于链上的部分企业，因此，不必要的交易信息共享将会导致商业机密的泄露。

[0018] 为了解决上述以及其他潜在的缺陷和问题，本公开的实施例提供了用于保护区块链数据的方法、设备以及计算机可读存储介质。下面将参考附图描述本公开的若干示例实施例。

[0019] 图2示出了根据本公开的实施例的用于保护区块链数据的方法200的流程示意图。其中，该方法200能够应用于图1所示的区块链网络中。

[0020] 在202处，在区块链的第一节点处创建智能合约，智能合约可以被设定有权限管理字段，权限管理字段包括可访问地址列表。

[0021] 在一些示例实现中，权限管理字段还可以包括第二节点对智能合约的访问权限，访问权限可以包括设定读写权限的读写访问权限。

[0022] 以三个区块链节点为例，如图3所示，其中示出了用于保护区块链数据的方法的示例实现方式。该区块链网络中包括例如三个区块链节点，分别为区块链节点1(称为“第一节点”)、区块链节点2(称为“第二节点”)和区块链节点3(称为“第三节点”)。其中，在区块链节点1处创建智能合约，在提交时，可以增加额外的权限管理字段，该权限管理字段可包含可

访问地址列表(例如可访问地址哈希值列表)。以此方式,私密数据可以通过智能合约进行管理,配置相应的访问权限。

[0023] 附加地,在区块链节点1处创建智能合约时,权限管理字段除了可包含可访问地址列表之外,还可以包含区块链节点2对智能合约的访问权限。此外,权限管理字段还可以包含区块链节点3对智能合约的访问权限。该访问权限例如可以包括设定具体读写或特定数据接口访问的读写访问权限。应当理解的是,这里对"访问权限"的限定仅仅是示例性的,无意以任何方式限制本公开的范围。

[0024] 例如,如图3所示,可以在区块链的区块链节点1处创建智能合约X,并设定权限管理字段,权限管理字段的内容为区块链节点2和3的地址的哈希值(即"3C344bQYPsL5FXAbv67kGksNLR1urufnE"和"3GFHwAZFDtPuBDS396PirD5jzHRDv9ni1n"),以及区块链节点2和3对智能合约X的访问权限。

[0025] 作为示例,具体实现的权限管理字段的内容如下所示。

[0026]

```
{
    "3C344bQYPsL5FXAbv67kGksNLR1urufnE5", // 区块链节
```

[0027]

```
点2的地址的哈希值
        "3GFHwAZFDtPuBDS396PirD5jzHRDv9ni1n"    // 区块链
节点3的地址的哈希值
    }
```

[0028] 通过以上的示例,可以设置针对智能合约X的权限管理字段。而且,根据以上权限管理字段中的可访问地址列表,区块链上的区块链节点2和区块链节点3可以访问在区块链节点1处创建的智能合约X。附加地,由于权限管理字段中还可以设置有区块链节点2和区块链节点3对智能合约的访问权限,因此,根据这样的访问权限,区块链节点2和区块链节点3对于智能合约X可以分别具有不同的访问权限。

[0029] 在一些示例实现中,如果智能合约未设定有权限管理字段,则该智能合约将以公开智能合约(如图3所示的公开智能合约)处理,即智能合约的创建和交易信息将以明文形式存在。

[0030] 在204处,在第一节点处使用密钥对智能合约进行加密,并将经加密的智能合约包括在第一节点处的区块数据中。

[0031] 例如,区块数据为区块链间通信使用,其中在第一节点处经加密的智能合约可以包括在区块数据中,而该区块数据随后可以被发送到区块链上的其它节点(例如图3中的区块链节点2和区块链节点3)。比如,智能合约的所有交易数据可以以密文形式添加到区块数据中,随后可以发送给区块链上的其它节点。

[0032] 以此方式,可以保证私密数据(例如第一节点处的智能合约Y)以密文形式保存在区块链上,所有节点均可备份,不存在因节点数的限制(例如传统的多链+明文数据技术中存在的节点数的限制)带来的备份风险。而且,由于具体实现时仅依赖于常用的加密算法,不存在高时延(例如传统的同态算法技术中存在算法复杂度高带来的高时延)而带来的效

率问题。

[0033] 在一些示例实现中，区块数据还包括区块号、交易数据、签名、以及随机数(Nonce)。

[0034] 例如，区块数据是链上数据的一部分，且用于区块链节点之间的数据通信，而智能合约数据可以包含在区块数据中。在保存数据时，区块原始数据可以单独保存，与智能合约的执行状态数据可以是分离的。由于区块数据可被全网共享，因此，可以从根本上保证区块链上的数据的一致性。

[0035] 在206处，在第一节点处根据可访问地址列表向区块链的第二节点分发密钥。

[0036] 在一些示例实现中，在第一节点处根据可访问地址列表向第二节点分发密钥包括：以点对点通信进行密钥分发，密钥包括对称密钥。

[0037] 如图3所示，区块链节点1创建了智能合约Y，并在可访问地址列表中指定仅区块链节点2可访问(例如图3中S1——创建智能合约Y，设置区块链节点2可访问)。相应地，区块链节点1可以以点对点通信仅向区块链节点2分发密钥(例如图3中S2——发送智能合约Y密钥给区块链节点2)。

[0038] 在208处，在第一节点处将区块数据发送到第二节点。

[0039] 在一些示例实现中，图2所示的方法200还可以包括：在第一节点处将区块数据发送到区块链的第三节点，而不向第三节点分发密钥。

[0040] 在一些示例实现中，在第二节点处接收密钥和区块数据，并使用密钥从区块数据中解密经加密的智能合约，以创建经解密的智能合约。附加地，在第二节点处还可以根据经解密的智能合约来执行交易。

[0041] 如图3所示，区块链节点1在将经加密的智能合约Y包括在第一节点(即区块链节点1)处的区块数据中之后，可以以广播的方式将区块数据发送到包括第二节点(即区块链节点2)和第三节点(即区块链节点3)的所有区块链节点上(例如，图3中S3——加密智能合约Y，以及图3中S4——发送经加密的智能合约Y(其被包含在区块数据中))。

[0042] 此时，由于区块链节点2接收到从第一节点发送的智能合约Y的密钥，而区块链节点3没有接收到这样的密钥，因此，区块链节点2可以在接收到区块数据后采用这样的密钥进行解密(例如图3中S5——解密智能合约Y)，以便在区块链节点2处创建经解密的智能合约Y(例如图3中S6——建立智能合约Y的逻辑数据分片)，而区块链节点3由于没有接收到这样的密钥，因此将无法在区块链节点3处创建经解密的智能合约Y(例如图3中S5——解密智能合约Y失败)。

[0043] 以此方式，在第一节点处创建智能合约并将经加密的智能合约包括在第一节点处的区块数据中之后，区块链上的其它节点都可接收区块数据(即实现所有节点均可备份)，但只有拥有该智能合约的密钥的节点才能进行解密，执行相应的交易，从而实现对区块链上数据的保护功能(例如，在交易仅限于供应链上的部分企业时，避免不必要的交易信息共享所导致的商业机密泄露的问题)。

[0044] 根据本公开的实施例，方法200还可以包括附加的数据共识过程。例如，在208之后，第一节点与第二节点之间可以通过点对点通信来进行数据共识。

[0045] 这里的数据共识例如是指采用已有共识算法(例如raft/pbft)来确认区块链上多个节点之间的数据一致性。以此方式，本公开能够在保证数据私密性的同时可达成数据共

识。

[0046] 在一些示例实现中，数据共识可以根据区块号、智能合约的智能合约号、以及智能合约的历史交易数据形成的交易数据摘要来进行。

[0047] 这里，数据共识(例如私密数据(如智能合约Y)的共识)可以具有唯一标识，即区块号及智能合约号(例如可以是智能合约地址或唯一指定的ID)。并且，可以采用现有共识算法来达成局部共识。

[0048] 为获得区块号及智能合约号，每个智能合约的历史交易数据及当前状态在存储时可以逻辑隔离。例如，底层可采用相同的物理数据库，也可采用不同的物理数据库。在存储时，执行完任一交易后，可以在智能合约的逻辑数据库中插入一条以区块号及智能合约号作为键值的记录，以便用于后续完成数据共识。

[0049] 相应地，在一些示例实现中，智能合约的历史交易数据和当前状态可以被逻辑隔离地存储在数据库中，智能合约的当前状态根据数据库中存储的区块号和智能合约的智能合约号进行查询。

[0050] 进一步地，数据共识可以通过点对点通信完成，部署同一智能合约的节点(例如图3中部署有同一智能合约Y的区块链节点1和区块链节点2)可参与共识(例如图3中S7——完成智能合约Y的交易的区块的共识)。而且，数据共识可由提交智能合约的节点(例如图3中创建智能合约的区块链节点1)发起，通过点对点通信，发送等待共识的数据，例如：

[0051]

```
{
    "blockhash" :
"000000000000000051d2e759c63a26e247f185ecb7926ed7a6624bc31c2
a717b",
    "contract" :
"0xb9bc498e7711aca691c86db8a4369eb60949e922",
    "merkleroot" :
"9891747e37903016c3b77c7a0ef10acf467c530de52d84735bd55538719
f9916"
}
```

[0052] 其中，以上等待共识的数据包括区块号(blockhash)，智能合约号(contract)以及根据所有该智能合约历史数据形成的交易数据摘要(如上面提到的merkleroot值)。具体来说，merkleroot可以基于该智能合约的历史交易数据来生成，对每次交易生成一个摘要(这里是哈希值)，插入作为merkle数的底层节点，同时更新根节点值。这里的等待共识的数据仅仅是示例性的，无意以任何方式限制本公开的范围。

[0053] 由此可见，由于私密数据(例如智能合约Y)以密文形式保存在区块数据中，区块链上所有节点均可备份，而且还可以对区块数据达成数据共识，因此不存在因节点数的限制(例如传统的多链+明文数据技术中存在节点数的限制)带来的备份风险和共识风险。

[0054] 图4示出了根据本公开的实施例的用于保护区块链数据的设备400。该设备400包括处理器402和存储器404。该存储器404耦合至处理器402并且存储有指令，该指令在由处理器执行时使得设备执行以下动作：在区块链的第一节点处创建智能合约，智能合约被设定有权限管理字段，权限管理字段包括可访问地址列表；在第一节点处使用密钥对智能合约进行加密，并将经加密的智能合约包括在第一节点处的区块数据中；在第一节点处根据可访问地址列表向区块链的第二节点分发密钥；以及在第一节点处将区块数据发送到第二节点。

[0055] 在一些示例实现中，用于保护区块链数据的设备400可以对应于区块链上的任意节点。作为示例，每个区块链节点可以包含相应的处理器402和存储器404，其中处理器402可以包括数据管理模块406和密钥管理模块408。

[0056] 数据管理模块406例如可以负责管理区块数据和智能合约数据。其中，区块数据是链上数据的一部分，且用于节点间数据通信，而智能合约数据是包含在区块数据中。在保存数据时，区块原始数据单独保存，与智能合约的执行状态数据是分离的。区块数据为全网共享，从根本上保证了链上数据的一致性。这里，管理私密数据的智能合约可以保存在独立的逻辑数据分片中(例如管理私密数据的智能合约，其原始合约和交易数据均加密后保存在唯一的区块链上，每个智能合约对应一个独立的数据分片)，按区块号及智能合约号(例如智能合约地址或唯一指定的ID)查询当前状态。

[0057] 密钥管理模块408例如可以负责维护智能合约的密钥的生成、分发、使用、存储和备份等。密钥管理模块408还可以引入密钥维护算法，如前向安全性或密钥旋转以提升安全性。此外，密钥管理模块408还可以根据数据管理模块406给出的权限管理字段(例如权限列表)来分发密钥，同时向数据管理模块406提供数据的加密和解密的接口。

[0058] 本公开可以被实现为一种计算机可读存储介质，具有存储在其上的计算机可读程序指令，计算机可读程序指令可以用于执行根据图1中的示例实施例所描述的用于保护区块链数据的方法。

[0059] 取决于具体的需求和应用场景，本公开可以被具体实现为一种系统、方法和/或计算机程序产品。计算机程序产品可以包括计算机可读存储介质，其上载有用于执行本公开的各个方面的计算机可读程序指令。

[0060] 本公开中所描述的方法和功能可以至少部分地由一个或多个硬件逻辑组件来执行。例如但不限于，可以使用的硬件逻辑组件的示意性类型包括现场可编程门阵列(FPGA)、专用集成电路(ASIC)、专用标准产品(ASSP)、片上系统(SOC)、复杂可编程逻辑器件(CPLD)等。

[0061] 计算机可读存储介质可以是可以保持和存储由指令执行设备使用的指令的有形设备。计算机可读存储介质例如可以是——但不限于——电存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或者上述的任意合适的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括：便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、静态随机存取存储器(SRAM)、便携式压缩盘只读存储器(CD-ROM)、数字多功能盘(DVD)、记忆棒、软盘、机械编码设备、例如其上存储有指令的打孔卡或凹槽内凸起结构、以及上述的任意合适的组合。这里所使用的计算机可读存储介质不被解释为瞬时信号本身，诸如无线电波或者其它自由传播的电磁波、通

过波导或其它传输媒介传播的电磁波(例如,通过光纤电缆的光脉冲)、或者通过电线传输的电信号。

[0062] 这里所描述的计算机可读程序指令可以从计算机可读存储介质下载到各个计算/处理设备,或者通过网络、例如因特网、局域网、广域网和/或无线网下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光纤传输、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配卡或者网络接口从网络接收计算机可读程序指令,并转发该计算机可读程序指令,以供存储在各个计算/处理设备中的计算机可读存储介质中。

[0063] 用于执行本公开操作的计算机程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、或者以一种或多种编程语言的任意组合编写的源代码或目标代码,所述编程语言包括面向对象的编程语言—诸如Smalltalk、C++等,以及常规的过程式编程语言—诸如“C”语言或类似的编程语言。计算机可读程序指令可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中,远程计算机可以通过任意种类的网络—包括局域网(LAN)或广域网(WAN)—连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。在一些实施例中,通过利用计算机可读程序指令的状态信息来个性化定制电子电路,例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA),该电子电路可以执行计算机可读程序指令,从而实现本公开的各个方面。

[0064] 这里参照根据本公开实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述了本公开的各个方面。应当理解,流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合,都可以由计算机可读程序指令实现。

[0065] 这些计算机可读程序指令可以提供给通用计算机、专用计算机或其它可编程数据处理装置的处理器,从而生产出一种机器,使得这些指令在通过计算机或其它可编程数据处理装置的处理器执行时,产生了实现流程图和/或框图中的一个或多个方框中规定的功能/动作的装置。也可以把这些计算机可读程序指令存储在计算机可读存储介质中,这些指令使得计算机、可编程数据处理装置和/或其它设备以特定方式工作,从而,存储有指令的计算机可读介质则包括一个制造品,其包括实现流程图和/或框图中的一个或多个方框中规定的功能/动作的各个方面的指令。

[0066] 也可以把计算机可读程序指令加载到计算机、其它可编程数据处理装置、或其它设备上,使得在计算机、其它可编程数据处理装置或其它设备上执行一系列操作步骤,以产生计算机实现的过程,从而使得在计算机、其它可编程数据处理装置、或其它设备上执行的指令实现流程图和/或框图中的一个或多个方框中规定的功能/动作。

[0067] 附图中的流程图和框图显示了根据本公开的多个实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段或指令的一部分,所述模块、程序段或指令的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个连续的方框实际上可以基本并行地执

行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0068] 此外，虽然采用特定次序描绘了各操作，但是这应当理解为要求这样操作以所示出的特定次序或以顺序次序执行，或者要求所有图示的操作应被执行以取得期望的结果。在一定环境下，多任务和并行处理可能是有利的。同样地，虽然在上面论述中包含了若干具体实现细节，但是这些不应当被解释为对本公开的范围的限制。在单独的实现的上下文中描述的某些特征还可以组合地实现在单个实现中。相反地，在单个实现的上下文中描述的各种特征也可以单独地或以任何合适的子组合的方式实现在多个实现中。

[0069] 以下列出了本公开的一些示例实现方式。

[0070] 本公开可以被实现为一种用于保护区块链数据的方法，包括：在所述区块链的第一节点处创建智能合约，所述智能合约被设定有权限管理字段，所述权限管理字段包括可访问地址列表；在所述第一节点处使用密钥对所述智能合约进行加密，并将经加密的所述智能合约包括在所述第一节点处的区块数据中；在所述第一节点处根据所述可访问地址列表向所述区块链的第二节点分发所述密钥；以及在所述第一节点处将所述区块数据发送到所述第二节点。

[0071] 在一些实施例中，所述权限管理字段还包括所述第二节点对所述智能合约的访问权限，所述访问权限包括设定读写权限的读写访问权限。

[0072] 在一些实施例中，所述在所述第一节点处根据所述可访问地址列表向所述第二节点分发所述密钥包括：以点对点通信进行密钥分发，所述密钥包括对称密钥。

[0073] 在一些实施例中，在所述第二节点处接收所述密钥和所述区块数据，并使用所述密钥从所述区块数据中解密经加密的所述智能合约，以创建经解密的所述智能合约。

[0074] 在一些实施例中，在所述第二节点处根据经解密的所述智能合约来执行交易。

[0075] 在一些实施例中，所述区块数据还包括区块号、交易数据、签名、以及随机数。

[0076] 在一些实施例中，所述智能合约的历史交易数据和当前状态被逻辑隔离地存储在数据库中，所述智能合约的当前状态根据所述数据库中存储的所述区块号和所述智能合约的智能合约号进行查询。

[0077] 在一些实施例中，所述第一节点与所述第二节点之间通过点对点通信来进行数据共识。

[0078] 在一些实施例中，所述数据共识根据所述区块号、所述智能合约的智能合约号、以及所述智能合约的历史交易数据形成的交易数据摘要来进行。

[0079] 在一些实施例中，所述方法还包括：在所述第一节点处将所述区块数据发送到所述区块链的第三节点，而不向所述第三节点分发所述密钥。

[0080] 本公开可以被实现为一种用于保护区块链数据的设备，包括：处理器；存储器，耦合至所述处理器并且存储有指令，所述指令在由所述处理器执行时使得所述设备执行以下动作：在所述区块链的第一节点处创建智能合约，所述智能合约被设定有权限管理字段，所述权限管理字段包括可访问地址列表；在所述第一节点处使用密钥对所述智能合约进行加密，并将经加密的所述智能合约包括在所述第一节点处的区块数据中；在所述第一节点处根据所述可访问地址列表向所述区块链的第二节点分发所述密钥；以及在所述第一节点处

将所述区块数据发送到所述第二节点。

[0081] 在一些实施例中，所述权限管理字段还包括所述第二节点对所述智能合约的访问权限，所述访问权限包括设定读写权限的读写访问权限。

[0082] 在一些实施例中，所述在所述第一节点处根据所述可访问地址列表向所述第二节点分发所述密钥包括：以点对点通信进行密钥分发，所述密钥包括对称密钥。

[0083] 在一些实施例中，在所述第二节点处接收所述密钥和所述区块数据，并使用所述密钥从所述区块数据中解密经加密的所述智能合约，以创建经解密的所述智能合约。

[0084] 在一些实施例中，在所述第二节点处根据经解密的所述智能合约来执行交易。

[0085] 在一些实施例中，所述区块数据还包括区块号、交易数据、签名、以及随机数。

[0086] 在一些实施例中，所述智能合约的历史交易数据和当前状态被逻辑隔离地存储在数据库中，所述智能合约的当前状态根据所述数据库中存储的所述区块号和所述智能合约的智能合约号进行查询。

[0087] 在一些实施例中，所述第一节点与所述第二节点之间通过点对点通信来进行数据共识。

[0088] 在一些实施例中，所述数据共识根据所述区块号、所述智能合约的智能合约号、以及所述智能合约的历史交易数据形成的交易数据摘要来进行。

[0089] 在一些实施例中，所述指令在由所述处理器执行时使得所述设备还执行以下动作：在所述第一节点处将所述区块数据发送到所述区块链的第三节点，而不向所述第三节点分发所述密钥。

[0090] 本公开可以被实现为一种计算机可读存储介质，具有存储在其上的计算机可读程序指令，所述计算机可读程序指令用于执行根据以上所描述的用于保护区块链数据的方法。

[0091] 通过以上描述和相关附图中所给出的教导，这里所给出的本公开的许多修改形式和其它实施方式将被本公开相关领域的技术人员所意识到。因此，所要理解的是，本公开的实施方式并不局限于所公开的具体实施方式，并且修改形式和其它实施方式意在包括在本公开的范围之内。此外，虽然以上描述和相关附图在部件和/或功能的某些示例组合形式的背景下对示例实施方式进行了描述，但是应当意识到的是，可以由备选实施方式提供部件和/或功能的不同组合形式而并不背离本公开的范围。就这点而言，例如，与以上明确描述的有所不同的部件和/或功能的其它组合形式也被预期处于本公开的范围之内。虽然这里采用了具体术语，但是它们仅以一般且描述性的含义所使用而并非意在进行限制。

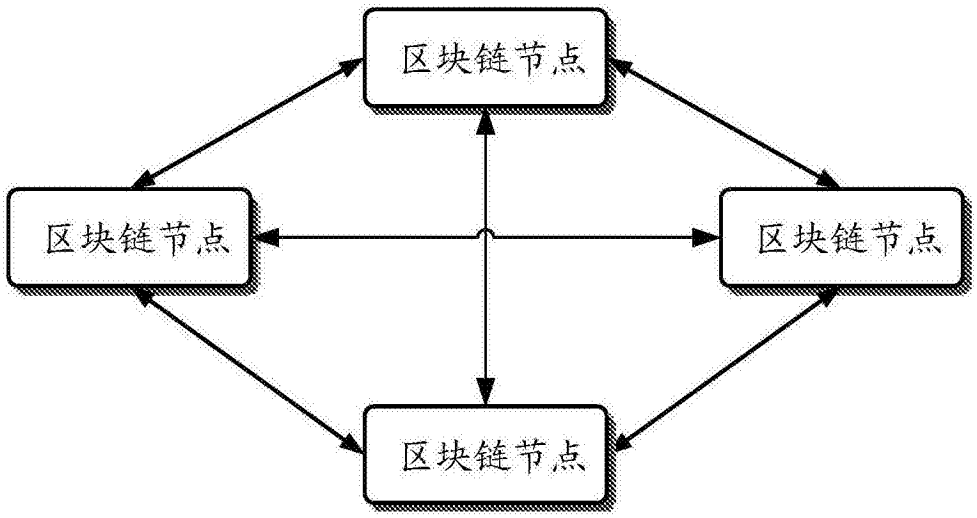

区块链节点
区块链节点
区块链节点
区块链节点

图1

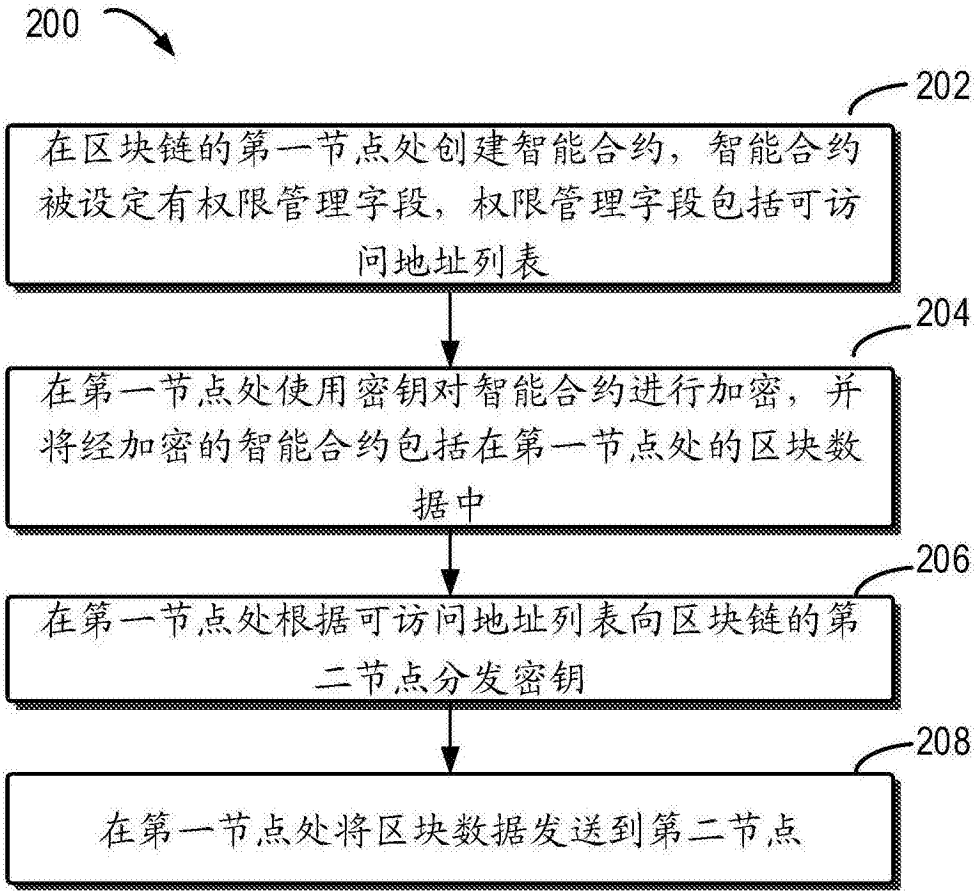

200
202
在区块链的第一节点处创建智能合约，智能合约被设定有权限管理字段，权限管理字段包括可访问地址列表
204
在第一节点处使用密钥对智能合约进行加密，并将经加密的智能合约包括在第一节点处的区块数据中
206
在第一节点处根据可访问地址列表向区块链的第二节点分发密钥
208
在第一节点处将区块数据发送到第二节点

图2

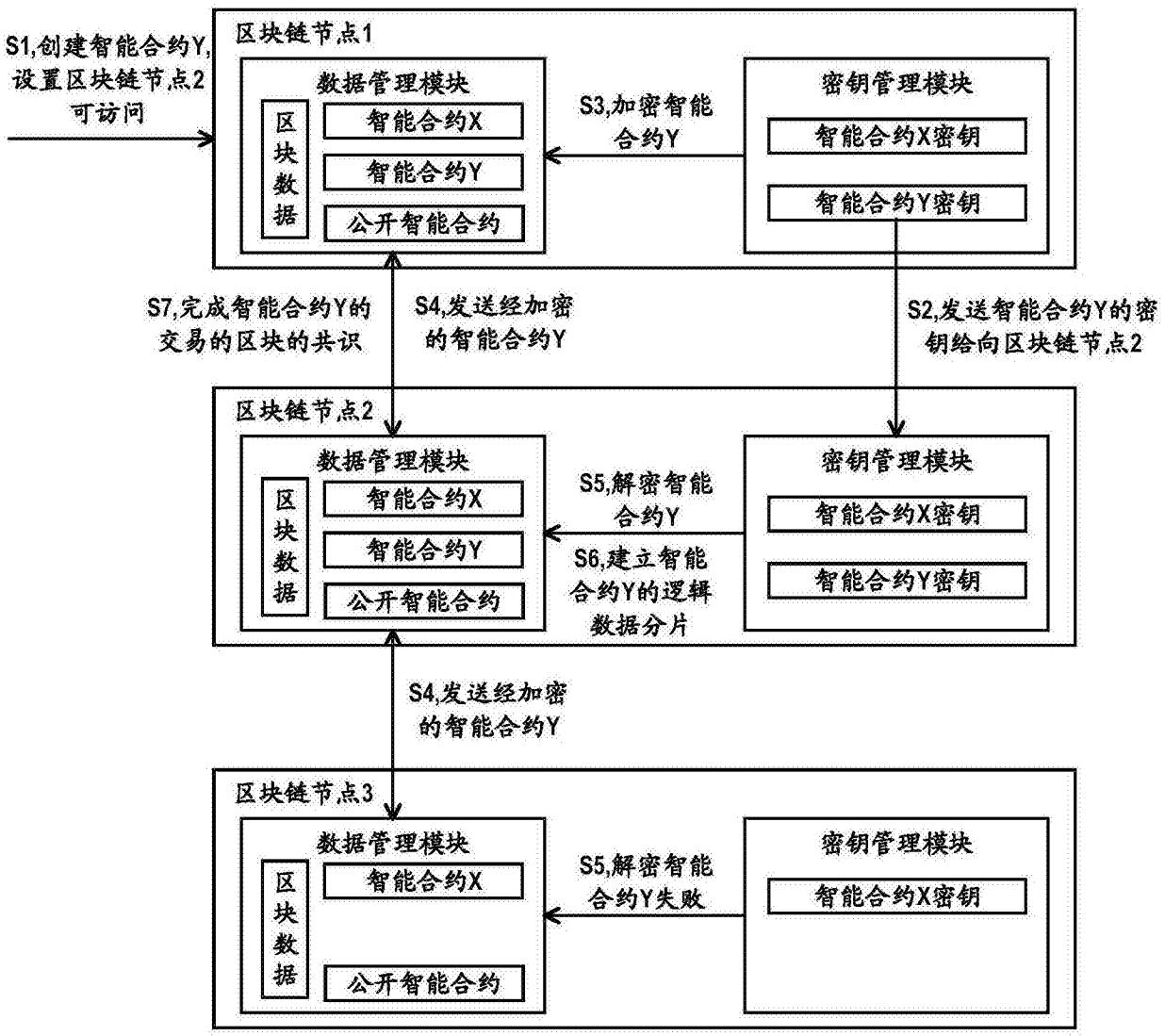

S1,创建智能合约Y,设置区块链节点2可访问
区块链节点1
数据管理模块
区块数据
智能合约X
智能合约Y
公开智能合约
S3,加密智能合约Y
密钥管理模块
智能合约X密钥
智能合约Y密钥
S7,完成智能合约Y的交易的区块的共识
S4,发送经加密的智能合约Y
S2,发送智能合约Y的密钥给向区块链节点2
区块链节点2
数据管理模块
区块数据
智能合约X
智能合约Y
公开智能合约
S5,解密智能合约Y
S6,建立智能合约Y的逻辑数据分片
密钥管理模块
智能合约X密钥
智能合约Y密钥
S4,发送经加密的智能合约Y
区块链节点3
数据管理模块
区块数据
智能合约X
公开智能合约
S5,解密智能合约Y失败
密钥管理模块
智能合约X密钥

图3

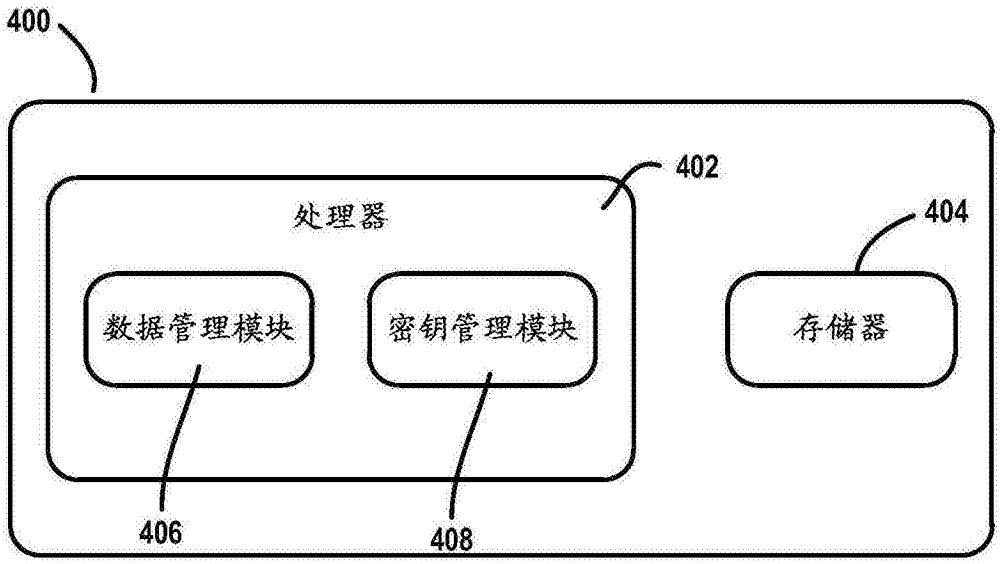


图4