(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112822016 B
(45)授权公告日 2023.04.28

(21)申请号 202110098715.5
(22)申请日 2021.01.25
(65)同一申请的已公布的文献号
申请公布号 CN 112822016 A
(43)申请公布日 2021.05.18
(73)专利权人 厦门市易联众易惠科技有限公司
地址 361000 福建省厦门市软件园二期观日路18号504之一
(72)发明人 施建安 关涛 庄一波 赵友平 陈俊海 孙志伟
(74)专利代理机构 厦门智慧呈睿知识产权代理事务所(普通合伙) 35222
专利代理师 陈晓思
(51)Int.Cl.
H04L 9/14(2006.01)
H04L 9/08(2006.01)
H04L 9/40(2022.01)
(56)对比文件
CN 102017578 A,2011.04.13
CN 111404950 A,2020.07.10
CN 111431713 A,2020.07.17
CN 112116472 A,2020.12.22
US 2012257757 A1,2012.10.11
WO 2018076365 A1,2018.05.03
审查员 游润

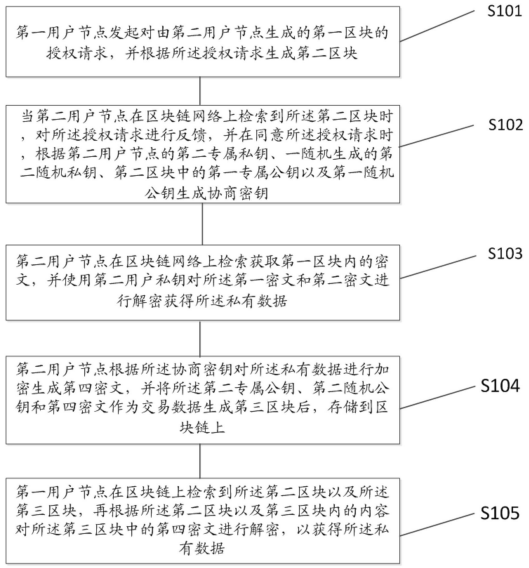
权利要求书3页 说明书8页 附图2页

(54)发明名称

在区块链上进行数据授权的方法及区块链网络

(57)摘要

本发明提供了一种在区块链上进行数据授权的方法及区块链网络，方法包括：第一用户节点发起对第二用户节点的第一区块的授权请求，生成第二区块；当第二用户节点检索到第二区块时，在同意授权请求时，根据第二用户节点的第二专属私钥、第二随机私钥、第一专属公钥以及第一随机公钥生成协商密钥；第二用户节点获取第一区块内的密文，解密获得私有数据；第二用户节点使用协商密钥对私有数据加密生成第四密文，将第二专属公钥、第二随机公钥和第四密文生成第三区块；第一用户节点在区块链上检索到第二区块以及第三区块，根据第二区块以及第三区块内的内容对第四密文进行解密，以获得私有数据。本发明实现了两个用户节点之间可靠安全的数据授权。



CN 112822016 B

1.一种在区块链上进行数据授权的方法,其特征在于,包括:

第一用户节点发起对由第二用户节点生成的第一区块的授权请求,并根据所述授权请求生成第二区块;其中,所述第一区块内包含有第一密文和第二密文,所述第一密文由第二用户节点的第二专属公钥对一随机生成的密钥进行加密生成;所述第二密文由所述密钥对第二用户节点的私有数据进行加密生成;所述第二区块包括第一区块的编号、第一用户节点的第一专属公钥、随机生成的第一随机公钥以及第三密文;所述第三密文由第一专属公钥对与所述第一随机公钥对应的第一随机私钥进行加密获得;

当第二用户节点在区块链网络上检索到所述第二区块时,对所述授权请求进行反馈,并在同意所述授权请求时,根据第二用户节点的第二专属私钥、一随机生成的第二随机私钥、第二区块中的第一专属公钥以及第一随机公钥生成协商密钥;

第二用户节点在区块链网络上检索获取第一区块内的密文,并使用第二用户私钥对所述第一密文和第二密文进行解密获得所述私有数据;

第二用户节点根据所述协商密钥对所述私有数据进行加密生成第四密文,并将所述第二专属公钥、第二随机公钥和第四密文作为交易数据生成第三区块后,存储到区块链上;

第一用户节点在区块链上检索到所述第二区块以及所述第三区块,再根据所述第二区块以及第三区块内的内容对所述第三区块中的第四密文进行解密,以获得所述私有数据。

2.根据权利要求1所述的在区块链上进行数据授权的方法,其特征在于,所述第一密文由所述第二专属公钥对所述密钥进行SM2加密生成;所述第二密文由所述密钥对第二用户节点的私有数据进行SM4加密生成。

3.根据权利要求1所述的在区块链上进行数据授权的方法,其特征在于,所述第三密文由第一专属公钥对所述第一随机私钥进行SM2加密生成;所述第一随机公钥与所述第一随机私钥、所述第二随机公钥与所述第二随机私钥均为由SM2算法随机生成的一对密钥对;且在每次授权请求中均不同。

4.根据权利要求1所述的在区块链上进行数据授权的方法,其特征在于,所述协商密钥由第二专属私钥和第二随机私钥,以及第三区块中的第一专属公钥和第一随机公钥,使用SM2算法的密钥交换协议进行密钥交换计算,再使用KDF函数生成。

5.根据权利要求1所述的在区块链上进行数据授权的方法,其特征在于,第二用户节点在区块链网络上检索获取第一区块内的密文,并使用第二用户私钥对所述第一密文和第二密文进行解密获得所述私有数据具体为:

第二用户节点在区块链上检索到第一区块,并获取第一区块内的第一密文以及第二密文的数据;

第二用户节点使用第二专属私钥对第一密文进行SM2解密,获得所述密钥;

第二用户节点使用所述密钥对第二密文进行SM4解密,获得所述私有数据。

6.根据权利要求1所述的在区块链上进行数据授权的方法,其特征在于,所述第四密文由第二用户节点使用所述协商密钥对所述私有数据进行SM4加密生成。

7.根据权利要求1所述的在区块链上进行数据授权的方法,其特征在于,第一用户节点在区块链上检索到所述第二区块以及所述第三区块,再根据所述第二区块以及第三区块内的内容对所述第三区块中的第四密文进行解密,以获得所述私有数据,具体包括:

第一用户节点在区块链上检索到第二区块和第三区块,并获取两个区块内的数据;

第一用户节点使用第一专属私钥对第二区块中的第三密文进行SM2解密，获得第一随机私钥；

第一用户节点使用第一专属私钥和第一随机私钥，以及第三区块中的第二专属公钥和第二随机公钥，使用SM2算法的密钥交换协议进行密钥交换计算，使用KDF函数生成所述协商密钥；

第一用户节点使用所述协商密钥对第三区块中的第四密文进行SM4解密，获得所述私有数据。

8.一种区块链网络，其特征在于，包括通过点对点网络实现通信的多个用户节点，所述用户节点包括第一用户节点以及第二用户节点；其中：

所述第一用户节点，用于发起对由第二用户节点生成的第一区块的授权请求，并根据所述授权请求生成第二区块；其中，所述第一区块内包含有第一密文和第二密文，所述第一密文由第二用户节点的第二专属公钥对一随机生成的密钥进行加密生成；所述第二密文由所述密钥对第二用户节点的私有数据进行加密生成；所述第二区块包括第一区块的编号、第一用户节点的第一专属公钥、随机生成的第一随机公钥以及第三密文；所述第三密文由第一专属公钥对与所述第一随机公钥对应的第一随机私钥进行加密获得；

所述第二用户节点，用于当在区块链网络上检索到所述第二区块时，对所述授权请求进行反馈，并在同意所述授权请求时，根据第二用户节点的第二专属私钥、一随机生成的第二随机私钥、第二区块中的第一专属公钥以及第一随机公钥生成协商密钥；

第二用户节点，还用于在区块链网络上检索获取第一区块内的密文，并使用第二用户私钥对所述第一密文和第二密文进行解密获得所述私有数据；

第二用户节点，还用于使用所述协商密钥对所述私有数据进行加密生成第四密文，并将所述第二专属公钥、第二随机公钥和第四密文作为交易数据生成第三区块后，存储到区块链上；

第一用户节点，还用于在区块链上检索到所述第二区块以及所述第三区块，再根据所述第二区块以及第三区块内的内容对所述第三区块中的第四密文进行解密，以获得所述私有数据。

9.根据权利要求8所述的区块链网络，其特征在于，第二用户节点具体用于：

使用第二专属私钥和第二随机私钥，以及第二区块中的第一专属公钥和第一随机公钥，使用SM2算法的密钥交换协议进行密钥交换计算，使用KDF函数生成所述协商密钥；

在区块链上检索到第一区块，并获取第一区块内的第一密文以及第二密文的数据；

使用第二专属私钥对第一密文进行SM2解密，获得所述密钥；

使用所述密钥对第二密文进行SM4解密，获得所述私有数据；

使用所述协商密钥对所述私有数据进行SM4加密，生成第四密文，并将所述第二专属公钥、第二随机公钥和第四密文作为交易数据生成第三区块后，存储到区块链上。

10.根据权利要求8所述的区块链网络，其特征在于，所述第一用户节点具体用于：

在区块链上检索到第二区块和第三区块，并获取两个区块内的数据；

使用第一专属私钥对第二区块中的第三密文进行SM2解密，获得第一随机私钥；

使用第一专属私钥和第一随机私钥，以及第三区块中的第二专属公钥和第二随机公钥，使用SM2算法的密钥交换协议进行密钥交换计算，使用KDF函数生成所述协商密钥；

使用所述协商密钥对第三区块中的第四密文进行SM4解密,获得所述私有数据。

在区块链上进行数据授权的方法及区块链网络

技术领域

[0001] 本发明涉及计算机技术领域，特别涉及一种在区块链上进行数据授权的方法及区块链网络。

背景技术

[0002] 区块链具有分布式、去中心化、防篡改等特性。由于区块链构建的特性，每个节点都存储有全部的区块数据，理论上用户可以查看到所有的区块数据。当使用区块链对敏感数据进行数据存储和数据交换时，需要对用户查看数据的权限进行验证和授权，用户只能查看被授权的数据。同时，因为区块链特有的防篡改性质，将授权请求和数据授权的过程记录在区块链上，可以实现对用户请求授权、授权操作、数据查询等操作的留痕和追溯。因此，如何在区块链上构建数据授权和交换的方法是具体应用区块链时必不可少的需求。

发明内容

[0003] 有鉴于此，本发明的目的在于提供一种在区块链上进行数据授权的方法及区块链网络，以满足上述需求。

[0004] 本发明第一实施例提供了一种在区块链上进行数据授权的方法，其包括：

[0005] 第一用户节点发起对由第二用户节点生成的第一区块的授权请求，并根据所述授权请求生成第二区块；其中，所述第一区块内包含有第一密文和第二密文，所述第一密文由第二用户节点的第二专属公钥对一随机生成的密钥进行加密生成；所述第二密文由所述密钥对第二用户节点的私有数据进行加密生成；所述第二区块包括第一区块的编号、第一用户节点的第一专属公钥、随机生成的第一随机公钥以及第三密文；所述第三密文由第一专属公钥对与所述第一随机公钥对应的第一随机私钥进行加密获得；

[0006] 当第二用户节点在区块链网络上检索到所述第二区块时，对所述授权请求进行反馈，并在同意所述授权请求时，根据第二用户节点的第二专属私钥、一随机生成的第二随机私钥、第二区块中的第一专属公钥以及第一随机公钥生成协商密钥；

[0007] 第二用户节点在区块链网络上检索获取第一区块内的密文，并使用第二用户私钥对所述第一密文和第二密文进行解密获得所述私有数据；

[0008] 第二用户节点使用所述协商密钥对所述私有数据进行加密生成第四密文，并将所述第二专属公钥、第二随机公钥和第四密文作为交易数据生成第三区块后，存储到区块链上；

[0009] 第一用户节点在区块链上检索到所述第二区块以及所述第三区块，再根据所述第二区块以及第三区块内的内容对所述第三区块中的第四密文进行解密，以获得所述私有数据。

[0010] 优选地，所述第一密文由所述第二专属公钥对所述密钥进行SM2加密生成；所述第二密文由所述密钥对第二用户节点的私有数据进行SM4加密生成。

[0011] 优选地，所述第三密文由第一专属公钥对所述第一随机私钥进行SM2加密生成；所

述第一随机公钥与所述第一随机私钥、所述第二随机公钥与所述第二随机私钥均为由SM2算法随机生成的一对密钥对;且在每次授权请求中均不同。

[0012] 优选地,所述协商密钥由第二专属私钥和第二随机私钥,以及第三区块中的第一专属公钥和第一随机公钥,使用SM2算法的密钥交换协议进行密钥交换计算,再使用KDF函数生成。

[0013] 优选地,第二用户节点在区块链网络上检索获取第一区块内的密文,并使用第二用户私钥对所述第一密文和第二密文进行解密获得所述私有数据具体为:

[0014] 第二用户节点在区块链上检索到第一区块,并获取第一区块内的第一密文以及第二密文的数据;

[0015] 第二用户节点使用第二专属私钥对第一密文进行进行SM2解密,获得所述密钥;

[0016] 第二用户节点使用所述密钥对第二密文进行SM4解密,获得所述私有数据。

[0017] 优选地,所述第四密文由第二用户节点使用所述协商密钥对所述私有数据进行SM4加密生成。

[0018] 优选地,第一用户节点在区块链上检索到所述第二区块以及所述第三区块,再根据所述第二区块以及第三区块内的内容对所述第三区块中的第四密文进行解密,以获得所述私有数据,具体包括:

[0019] 第一用户节点在区块链上检索到第二区块和第三区块,并获取两个区块内的数据;

[0020] 第一用户节点使用第一专属私钥对第二区块中的第三密文进行SM2解密,获得第一随机私钥;

[0021] 第一用户节点使用第一专属私钥和第一随机私钥,以及第三区块中的第二专属公钥和第二随机公钥,使用SM2算法的密钥交换协议进行密钥交换计算,使用KDF函数生成所述协商密钥;

[0022] 第一用户节点使用所述协商密钥对第三区块中的第四密文进行SM4解密,获得所述私有数据。

[0023] 优选地,还包括:

[0024] 当所述第二用户节点不同意所述授权请求时,则结束本次授权流程。

[0025] 本发明实施例还提供了一种区块链网络,其包括通过点对点网络实现通信的多个用户节点,所述用户节点包括第一用户节点以及第二用户节点;其中:

[0026] 所述第一用户节点,用于发起对由第二用户节点生成的第一区块的授权请求,并根据所述授权请求生成第二区块;其中,所述第一区块内包含有第一密文和第二密文,所述第一密文由第二用户节点的第二专属公钥对一随机生成的密钥进行加密生成;所述第二密文由所述密钥对第二用户节点的私有数据进行加密生成;所述第二区块包括第一区块的编号、第一用户节点的第一专属公钥、随机生成的第一随机公钥以及第三密文;所述第三密文由第一专属公钥对与所述第一随机公钥对应的第一随机私钥进行加密获得;

[0027] 所述第二用户节点,用于当在区块链网络上检索到所述第二区块时,对所述授权请求进行反馈,并在同意所述授权请求时,根据第二用户节点的第二专属私钥、一随机生成的第二随机私钥、第二区块中的第一专属公钥以及第一随机公钥生成协商密钥;

[0028] 第二用户节点,还用于在区块链网络上检索获取第一区块内的密文,并使用第二

用户私钥对所述第一密文和第二密文进行解密获得所述私有数据；

[0029] 第二用户节点，还用于根据所述协商密钥对所述私有数据进行加密生成第四密文，并将所述第二专属公钥、第二随机公钥和第四密文作为交易数据生成第三区块后，存储到区块链上；

[0030] 第一用户节点，还用于在区块链上检索到所述第二区块以及所述第三区块，再根据所述第二区块以及第三区块内的内容对所述第三区块中的第四密文进行解密，以获得所述私有数据。

[0031] 优选地，第二用户节点具体用于：

[0032] 使用第二专属私钥和第二随机私钥，以及第二区块中的第一专属公钥和第一随机公钥，使用SM2算法的密钥交换协议进行密钥交换计算，使用KDF函数生成所述协商密钥；

[0033] 在区块链上检索到第一区块，并获取第一区块内的第一密文以及第二密文的数据；

[0034] 使用第二专属私钥对第一密文进行进行SM2解密，获得所述密钥；

[0035] 使用所述密钥对第二密文进行SM4解密，获得所述私有数据；

[0036] 使用所述协商密钥对所述私有数据进行SM4加密，生成第四密文，并将所述第二专属公钥、第二随机公钥和第四密文作为交易数据生成第三区块后，存储到区块链上。

[0037] 优选地，所述第一用户节点具体用于：

[0038] 在区块链上检索到第二区块和第三区块，并获取两个区块内的数据；

[0039] 使用第一专属私钥对第二区块中的第三密文进行SM2解密，获得第一随机私钥；

[0040] 使用第一专属私钥和第一随机私钥，以及第三区块中的第二专属公钥和第二随机公钥，使用SM2算法的密钥交换协议进行密钥交换计算，使用KDF函数生成所述协商密钥；

[0041] 使用所述协商密钥对第三区块中的第四密文进行SM4解密，获得所述私有数据。

[0042] 上述一个实施例中，实现了第一用户节点与第二用户节点之间通过密钥交换机制将私有数据D从第二用户共享给第一用户节点的过程。只要第一用户节点与第二用户节点各自的专属私钥未泄露，在数据交换过程中，即使第三方节点取得了所有区块的密文，也无法获得所述私有数据D的明文。同时，因为整个数据交换过程都储存在区块链上，因此，可以对数据交换过程进行追溯和取证。

[0043] 更进一步的，本实施例中同时采用三个方法提高SM4密钥的安全性：

[0044] (1)SM4密钥采用一次一密的方式随机产生。当需要加密数据时，随机产生此次加密的密钥，这样即使是相同的数据，重复加密的密文也是不同的，增加了破解密钥的难度；

[0045] (2)对于用户的私有数据，当需要将SM4密钥存储在区块链上时，使用用户自己的专属公钥使用SM2算法对SM4密钥进行加密，这样保证只有使用用户自己的私钥才能解密；

[0046] (3)对于需要进行数据交换的数据，使用数据交换双方用户的私有密钥进行密钥交换而产生的协商密钥K作为SM4密钥，如此可实现SM4密钥和各种私钥不存储在区块链上，也不在网络中传输，在网络中存储和传输的都是各种公钥。

附图说明

[0047] 为了更清楚地说明本发明实施方式的技术方案，下面将对实施方式中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本发明的某些实施例，因此不应被看作

是对范围的限定，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他相关的附图。

[0048] 图1是本发明第一实施例提供的在区块链上进行数据授权的方法的流程示意图。

[0049] 图2是本发明第二实施例提供的区块链网络的示意图。

具体实施方式

[0050] 为使本发明实施方式的目的、技术方案和优点更加清楚，下面将结合本发明实施方式中的附图，对本发明实施方式中的技术方案进行清楚、完整地描述，显然，所描述的实施方式是本发明一部分实施方式，而不是全部的实施方式。基于本发明中的实施方式，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施方式，都属于本发明保护的范围。因此，以下对在附图中提供的本发明的实施方式的详细描述并非旨在限制要求保护的本发明的范围，而是仅仅表示本发明的选定实施方式。基于本发明中的实施方式，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施方式，都属于本发明保护的范围。

[0051] 请参阅图1，本发明第一实施例提供了一种在区块链上进行数据授权的方法，其包括：

[0052] S101，第一用户节点发起对由第二用户节点生成的第一区块的授权请求，并根据所述授权请求生成第二区块。

[0053] 在本实施例中，所述第一用户节点以及所述第二用户节点位于区块链网络中，区块链网络一般都包括多个以点对点网络实现通信连接的节点，这些节点均是对等节点，从而实现去中心化。

[0054] 在本实施例中，特别的，当第一用户节点想要查看第二用户节点的私有数据时，所述第二用户节点先将所述私有数据加密成第一区块并上传至区块链网络中。

[0055] 具体地，第二用户节点通过如下步骤来生成所述第一区块：

[0056] 首先，第二用户节点随机生成一个128bit的密钥KA，作为本次使用的SM4算法密钥；

[0057] 然后，第二用户节点使用自身的第二专属公钥对所述密钥KA进行SM2加密，生成第一密文C10。

[0058] 其中，SM2算法全称为SM2椭圆曲线公钥密码算法，是我国自主设计的公钥密码算法。SM2算法与RSA算法不同的是，SM2算法是基于椭圆曲线上点群离散对数难题，相对于RSA算法，256位的SM2密码强度已经比2048位的RSA密码强度要高。

[0059] 接着，第二用户节点使用所述密钥KA对私有数据D进行SM4加密，生成密文第二密文C11。

[0060] 其中，SM4算法全称为SM4分组密码算法，是我国自主设计的分组对称密码算法。要保证一个对称密码算法的安全性的基本条件是其具备足够的密钥长度，SM4算法与AES算法具有相同的密钥长度和分组长度都是128比特，因此在安全性上高于3DES算法。

[0061] 最后，所述第二用户节点将第一密文C10和第二密文C11作为交易数据生成第一区块，并存储到区块链上，其中，第一区块编号记为H1。

[0062] 在本实施例中，需要说明的是，对于区块链网络中的每个节点，其均具有一对专属

的非对称的密钥对，即具有一个专属公钥和一个专属私钥，其中，专属公钥一般是公开的，而专属私钥则仅所属用户节点可见。

[0063] 在本实施例中，第一用户节点在发起授权请求时，将生成对应的第二区块H2，其中，所述第二区块H2包括第一区块的编号H1、第一用户节点自身的第一专属公钥、随机生成的第一随机公钥以及第三密文C20；所述第三密文C20由使用第一专属公钥对与所述第一随机公钥对应的第一随机私钥进行SM2加密获得。

[0064] 其中，所述第一随机公钥与所述第一随机私钥均为由SM2算法随机生成的一对密钥对，且在每次授权请求中均不同。

[0065] S102，当第二用户节点在区块链网络上检索到所述第二区块时，对所述授权请求进行反馈，并在同意所述授权请求时，根据第二用户节点的第二专属私钥、一随机生成的第二随机私钥、第二区块中的第一专属公钥以及第一随机公钥生成协商密钥。

[0066] 在本实施例中，如果第二用户节点在区块链网络中检索到所述第二区块H2时，其可以对所述第二区块H2进行响应，如同意授权或者不同意授权。如果第二用户节点不同意授权，则结束本次的授权流程。如果第二用户节点同意本次授权，则其根据第二用户节点自身的第二专属私钥、一随机生成的第二随机私钥、第二区块H2中的第一专属公钥以及第一随机公钥生成协商密钥K。

[0067] 其中，所述协商密钥K由第二专属私钥和第二随机私钥，以及第二区块H2中的第一专属公钥和第一随机公钥，使用SM2算法的密钥交换协议进行密钥交换计算，再使用KDF函数生成。

[0068] 其中，密钥生成函数KDF按GMT0003.3-2012 5.4.3给出的算法生成协商密钥K。

[0069] S103，第二用户节点在区块链网络上检索获取第一区块内的密文，并使用第二用户私钥对所述第一密文和第二密文进行解密获得所述私有数据。

[0070] 具体地，第二用户节点首先在区块链上检索到第一区块H1，并获取第一区块H1内的第一密文以及第二密文，然后使用第二专属私钥对第一密文C10进行进行SM2解密，获得所述密钥KA，最后使用所述密钥KA对第二密文C11进行SM4解密，获得所述私有数据D。

[0071] S104，第二用户节点根据所述协商密钥对所述私有数据进行加密生成第四密文，并将所述第二专属公钥、第二随机公钥和第四密文作为交易数据生成第三区块后，存储到区块链上。

[0072] 具体地，第二用户节点首先使用所述协商密钥K对所述私有数据D进行SM4加密生成第四密文C30，然后将所述第二专属公钥、第二随机公钥和第四密文C30作为交易数据生成第三区块H3后，存储到区块链上。

[0073] S105，第一用户节点在区块链上检索到所述第二区块以及所述第三区块，再根据所述第二区块以及第三区块内的内容对所述第三区块中的第四密文进行解密，以获得所述私有数据。

[0074] 具体地：

[0075] 首先，第一用户节点在区块链上检索到第二区块H2和第三区块H3，并获取两个区块内的数据；

[0076] 然后，第一用户节点使用第一专属私钥对第二区块H2中的第三密文C20进行SM2解密，获得第一随机私钥。

[0077] 接着,第一用户节点使用第一专属私钥和第一随机私钥,以及第三区块H3中的第二专属公钥和第二随机公钥,使用SM2算法的密钥交换协议进行密钥交换计算,使用KDF函数生成所述协商密钥K。

[0078] 最后,第一用户节点使用所述协商密钥K对第三区块H3中的第四密文C30进行SM4解密,获得所述私有数据D。

[0079] 至此,第一用户节点与第二用户节点之间完成了通过密钥交换机制将私有数据D从第二用户节点共享给第一用户节点的过程。只要第一用户节点与第二用户节点各自的专属私钥未泄露,在数据交换过程中,即使第三方节点取得了所有区块的密文,也无法获得所述私有数据D的明文。同时,因为整个数据交换过程都储存在区块链上,因此,可以对数据交换过程进行追溯和取证。

[0080] 更进一步的,由于对称加密算法只需要一个密钥,加密和解密使用同一个密钥。因此交易数据的安全性依赖于密钥是否被泄露。为此在本实施例中同时采用三个方法提高SM4密钥的安全性:

[0081] (1)SM4密钥采用一次一密的方式随机产生。当需要加密数据时,随机产生此次加密的密钥,这样即使是相同的数据,重复加密的密文也是不同的,增加了破解密钥的难度;

[0082] (2)对于用户的私有数据,当需要将SM4密钥存储在区块链上时,使用用户自己的专属公钥使用SM2算法对SM4密钥进行加密,这样保证只有使用用户自己的私钥才能解密;

[0083] (3)对于需要进行数据交换的数据,使用数据交换双方用户的私有密钥进行密钥交换而产生的协商密钥K作为SM4密钥,如此可实现SM4密钥和各种私钥不存储在区块链上,也不在网络中传输,在网络中存储和传输的都是各种公钥。

[0084] 本发明第二实施例还提供了一种区块链网络,其包括通过点对点网络实现通信的多个用户节点,所述用户节点包括第一用户节点A以及第二用户节点B;其中:

[0085] 所述第一用户节点A,用于发起对由第二用户节点B生成的第一区块的授权请求,并根据所述授权请求生成第二区块;其中,所述第一区块内包含有第一密文和第二密文,所述第一密文由第二用户节点的第二专属公钥对一随机生成的密钥进行加密生成;所述第二密文由所述密钥对第二用户节点的私有数据进行加密生成;所述第二区块包括第一区块的编号、第一用户节点的第一专属公钥、随机生成的第一随机公钥以及第三密文;所述第三密文由第一专属公钥对与所述第一随机公钥对应的第一随机私钥进行加密获得;

[0086] 所述第二用户节点B,用于当在区块链网络上检索到所述第二区块时,对所述授权请求进行反馈,并在同意所述授权请求时,根据第二用户节点的第二专属私钥、一随机生成的第二随机私钥、第二区块中的第一专属公钥以及第一随机公钥生成协商密钥;

[0087] 第二用户节点B,还用于在区块链网络上检索获取第一区块内的密文,并使用第二专属私钥对所述第一密文和第二密文进行解密获得所述私有数据;

[0088] 第二用户节点B,还用于根据所述协商密钥对所述私有数据进行加密生成第四密文,并将所述第二专属公钥、第二随机公钥和第四密文作为交易数据生成第三区块后,存储到区块链上;

[0089] 第一用户节点A,还用于在区块链上检索到所述第二区块以及所述第三区块,再根据所述第二区块以及第三区块内的内容对所述第三区块中的第四密文进行解密,以获得所述私有数据。

[0090] 优选地，第二用户节点B具体用于：

[0091] 使用第二专属私钥和第二随机私钥，以及第二区块中的第一专属公钥和第一随机公钥，使用SM2算法的密钥交换协议进行密钥交换计算，使用KDF函数生成所述协商密钥；

[0092] 在区块链上检索到第一区块，并获取第一区块内的第一密文以及第二密文的数据；

[0093] 使用第二专属私钥对第一密文进行进行SM2解密，获得所述密钥；

[0094] 使用所述密钥对第二密文进行SM4解密，获得所述私有数据；

[0095] 使用所述协商密钥对所述私有数据进行SM4加密，生成第四密文，并将所述第二专属公钥、第二随机公钥和第四密文作为交易数据生成第三区块后，存储到区块链上。

[0096] 优选地，所述第一用户节点A具体用于：

[0097] 在区块链上检索到第二区块和第三区块，并获取两个区块内的数据；

[0098] 使用第一专属私钥对第二区块中的第三密文进行SM2解密，获得第一随机私钥；

[0099] 使用第一专属私钥和第一随机私钥，以及第三区块中的第二专属公钥和第二随机公钥，使用SM2算法的密钥交换协议进行密钥交换计算，使用KDF函数生成所述协商密钥；

[0100] 使用所述协商密钥对第三区块中的第四密文进行SM4解密，获得所述私有数据。

[0101] 在本发明实施例所提供的几个实施例中，应该理解到，所揭露的装置和方法，也可以通过其它的方式实现。以上所描述的装置和方法实施例仅仅是示意性的，例如，附图中的流程图和框图显示了根据本发明的多个实施例的装置、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、程序段或代码的一部分，所述模块、程序段或代码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。也应当注意，在有些作为替换的实现方式中，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。

[0102] 另外，在本发明各个实施例中的各功能模块可以集成在一起形成一个独立的部分，也可以是各个模块单独存在，也可以两个或两个以上模块集成形成一个独立的部分。

[0103] 所述功能如果以软件功能模块的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，电子设备或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。需要说明的是，在本文中，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、物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、物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、物品或者设备中还存在另外的相同要素。

[0104] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

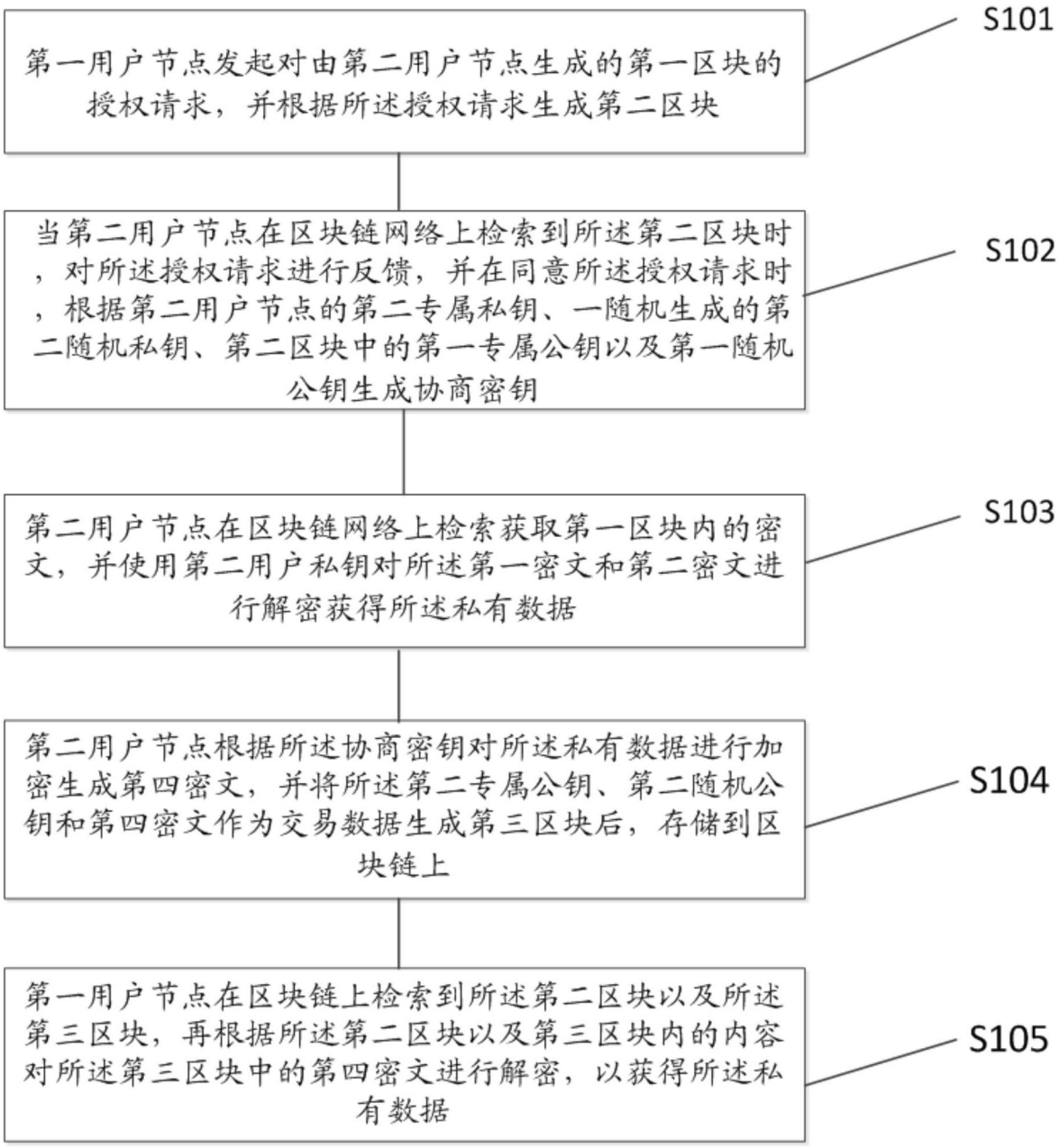

第一用户节点发起对由第二用户节点生成的第一区块的授权请求，并根据所述授权请求生成第二区块
S101
当第二用户节点在区块链网络上检索到所述第二区块时，对所述授权请求进行反馈，并在同意所述授权请求时，根据第二用户节点的第二专属私钥、一随机生成的第二随机私钥、第二区块中的第一专属公钥以及第一随机公钥生成协商密钥
S102
第二用户节点在区块链网络上检索获取第一区块内的密文，并使用第二用户私钥对所述第一密文和第二密文进行解密获得所述私有数据
S103
第二用户节点根据所述协商密钥对所述私有数据进行加密生成第四密文，并将所述第二专属公钥、第二随机公钥和第四密文作为交易数据生成第三区块后，存储到区块链上
S104
第一用户节点在区块链上检索到所述第二区块以及所述第三区块，再根据所述第二区块以及第三区块内的内容对所述第三区块中的第四密文进行解密，以获得所述私有数据
S105

图1

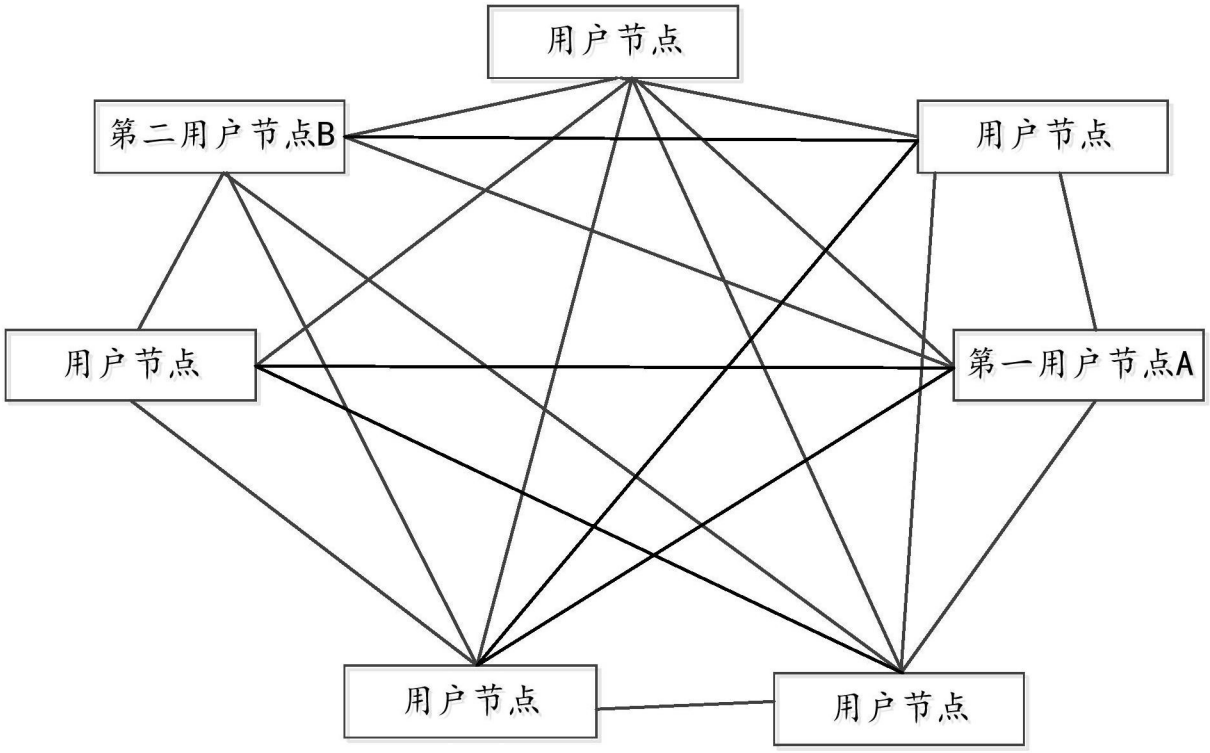


图2