(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 110851865 A
(43)申请公布日 2020.02.28

(21)申请号 201911097688.9

(22)申请日 2019.11.12

(71)申请人 北京海益同展信息科技有限公司
地址 100176 北京市大兴区北京经济技术开发区科创十一街18号院2号楼6层601

(72)发明人 苟喜霞

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李昊 刘剑波

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)

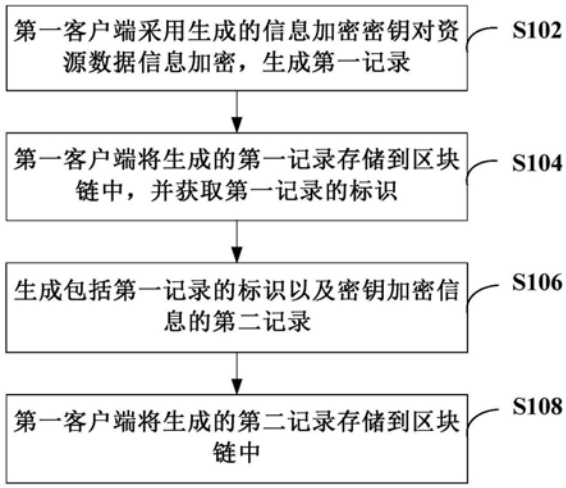
权利要求书2页 说明书9页 附图6页

(54)发明名称

资源数据的处理方法、装置、系统和存储介质

(57)摘要

本发明公开了一种资源数据的处理方法、装置、系统和存储介质，涉及数据处理技术。资源数据的处理方法包括：第一客户端采用生成的信息加密密钥对资源数据信息加密，生成第一记录；第一客户端将生成的第一记录存储到区块链中，并获取第一记录的标识；第一客户端采用第二客户端的用户的公钥加密信息加密密钥、以获得密钥加密信息，生成包括第一记录的标识以及密钥加密信息的第二记录，其中，第二客户端的用户对资源数据具有查询权限；第一客户端将生成的第二记录存储到区块链中，以便第二客户端的用户从区块链中读取第一记录或第二记录。从而在实现资源数据信息可追溯、不可篡改的前提下，提高了资源数据的隐私性。



CN 110851865 A

1.一种资源数据的处理方法,包括:

第一客户端采用生成的信息加密密钥对资源数据信息加密,生成第一记录;

第一客户端将生成的第一记录存储到区块链中,并获取所述第一记录的标识;

第一客户端采用第二客户端的用户的公钥加密所述信息加密密钥、以获得密钥加密信息,生成包括所述第一记录的标识以及所述密钥加密信息的第二记录,其中,第二客户端的用户对所述资源数据具有查询权限;

第一客户端将生成的第二记录存储到区块链中,以便第二客户端的用户从区块链中读取所述第一记录或所述第二记录。

2.根据权利要求1所述的资源数据的处理方法,还包括:

第一客户端将所述第一记录的标识、所述第二记录的标识与第二客户端的用户的账户进行绑定,以便第二客户端向用户显示绑定的第一记录和第二记录。

3.根据权利要求1所述的资源数据的处理方法,还包括:

第二客户端采用第二客户端的用户的私钥对所述第二记录中的密钥加密信息进行解密,获得第一记录的标识和信息加密密钥;

第二客户端采用所述信息加密密钥对所述第一记录进行解密,获得资源数据信息。

4.根据权利要求3所述的资源数据的处理方法,其中,所述资源数据信息是资源转移执行信息;

所述资源数据的处理方法还包括:

响应于获得资源转移数据信息,第二客户端调用智能合约,以便通过智能合约验证预先获得的资源转移结果与所述资源转移执行信息的一致性。

5.根据权利要求4所述的资源数据的处理方法,其中,所述第一客户端的用户为资源转移执行机构用户、第二客户端的用户为组织机构用户或个人用户。

6.根据权利要求3所述的资源数据的处理方法,其中,第一客户端的用户为组织机构用户、第二客户端的用户为资源转移执行机构用户或个人用户,所述资源数据信息是资源转移明细信息,以便资源转移执行机构用户根据所述资源转移明细信息执行资源转移。

7.根据权利要求3所述的资源数据的处理方法,其中,第一客户端的用户为组织机构用户、第二客户端的用户为资源获取机构用户,所述资源数据信息是资源扣除信息;

所述资源数据的处理方法还包括:

资源获取机构用户的客户端响应于获得资源扣除信息,调用资源转移智能合约,以便根据所述资源扣除信息将资源从组织机构用户转移到资源获取机构用户。

8.根据权利要求1所述的资源数据的处理方法,还包括:

客户端计算客户端的用户信息的哈希值;

客户端采用对所述用户信息具有查询权限的用户的公钥,对所述客户端的用户的公钥进行加密;

客户端将包括用户信息的哈希值以及对所述客户端的用户的公钥进行加密的结果的初始化信息记录存储到区块链中;

其中,所述客户端为第一客户端或第二客户端。

9.一种资源数据的处理装置,包括:

第一记录生成模块,被配置为采用生成的信息加密密钥对资源数据信息加密,生成第

一记录；

第一记录存储模块，被配置为将生成的第一记录存储到区块链中，并获取所述第一记录的标识；

第二记录生成模块，被配置为采用对所述资源数据具有查询权限的用户的公钥加密所述信息加密密钥、以获得密钥加密信息，生成包括所述第一记录的标识以及所述密钥加密信息的第二记录；

第二记录存储模块，被配置为将生成的第二记录存储到区块链中，以便对所述资源数据具有查询权限的用户从区块链中读取所述第一记录或所述第二记录。

10.根据权利要求9所述的资源数据的处理装置，还包括：

第一解密模块，被配置为采用自身的私钥对区块链中的第二记录中的密钥加密信息进行解密，获得第一记录的标识和信息加密密钥；

第二解密模块，被配置为采用所述信息加密密钥对区块链中的第一记录进行解密，获得资源数据信息。

11.一种资源数据的处理系统，包括：

多个权利要求9或10所述的资源数据的处理装置；以及

区块链系统。

12.一种资源数据的处理装置，包括：

存储器；以及

耦接至所述存储器的处理器，所述处理器被配置为基于存储在所述存储器中的指令，执行如权利要求1～8中任一项所述的资源数据的处理方法。

13.一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现权利要求1～8中任一项所述的资源数据的处理方法。

资源数据的处理方法、装置、系统和存储介质

技术领域

[0001] 本发明涉及数据处理技术，特别涉及一种资源数据的处理方法、装置、系统和存储介质。

背景技术

[0002] 目前，在资源发放和转移的过程中，可能涉及到多方的参与。例如，组织机构将所拥有的带宽分配给下一层级的用户，例如个人用户，带宽分配的实现过程由运营商执行；又例如，企业将薪水发放给员工，而转账过程需要由银行来执行。

发明内容

[0003] 发明人经过分析后发现，部分资源数据涉及隐私。如果将其公开，则用户的隐私难以得到保障；如果进行保密处理，又难以对其进行监督和管理，与资源数据相关的用户也难以对其准确性进行核实。

[0004] 本发明实施例所要解决的一个技术问题是：如何提高资源数据处理的隐私性和准确性。

[0005] 根据本发明一些实施例的第一个方面，提供一种资源数据的处理方法，包括：第一客户端采用生成的信息加密密钥对资源数据信息加密，生成第一记录；第一客户端将生成的第一记录存储到区块链中，并获取第一记录的标识；第一客户端采用第二客户端的用户的公钥加密信息加密密钥、以获得密钥加密信息，生成包括第一记录的标识以及密钥加密信息的第二记录，其中，第二客户端的用户对资源数据具有查询权限；第一客户端将生成的第二记录存储到区块链中，以便第二客户端的用户从区块链中读取第一记录或第二记录。

[0006] 在一些实施例中，资源数据的处理方法还包括：第一客户端将第一记录的标识、第二记录的标识与第二客户端的用户的账户进行绑定，以便第二客户端向用户显示绑定的第一记录和第二记录。

[0007] 在一些实施例中，资源数据的处理方法还包括：第二客户端采用第二客户端的用户的私钥对第二记录中的密钥加密信息进行解密，获得第一记录的标识和信息加密密钥；第二客户端采用信息加密密钥对第一记录进行解密，获得资源数据信息。

[0008] 在一些实施例中，资源数据信息是资源转移执行信息；资源数据的处理方法还包括：响应于获得资源转移数据信息，第二客户端调用智能合约，以便通过智能合约验证预先获得的资源转移结果与资源转移执行信息的一致性。

[0009] 在一些实施例中，第一客户端的用户为资源转移执行机构用户、第二客户端的用户为组织机构用户或个人用户。

[0010] 在一些实施例中，第一客户端的用户为组织机构用户、第二客户端的用户为资源转移执行机构用户或个人用户，资源数据信息是资源转移明细信息，以便资源转移执行机构用户根据资源转移明细信息执行资源转移。

[0011] 在一些实施例中，第一客户端的用户为组织机构用户、第二客户端的用户为资源

获取机构用户，资源数据信息是资源扣除信息；资源数据的处理方法还包括：资源获取机构用户的客户端响应于获得资源扣除信息，调用资源转移智能合约，以便根据资源扣除信息将资源从组织机构用户转移到资源获取机构用户。

[0012] 在一些实施例中，资源数据的处理方法还包括：客户端计算客户端的用户信息的哈希值；客户端采用对用户信息具有查询权限的用户的公钥，对客户端的用户的公钥进行加密；客户端将包括用户信息的哈希值以及对客户端的用户的公钥进行加密的结果的初始化信息记录存储到区块链中；其中，客户端为第一客户端或第二客户端。

[0013] 根据本发明一些实施例的第二个方面，提供一种资源数据的处理装置，包括：第一记录生成模块，被配置为采用生成的信息加密密钥对资源数据信息加密，生成第一记录；第一记录存储模块，被配置为将生成的第一记录存储到区块链中，并获取第一记录的标识；第二记录生成模块，被配置为采用对资源数据具有查询权限的用户的公钥加密信息加密密钥、以获得密钥加密信息，生成包括第一记录的标识以及密钥加密信息的第二记录；第二记录存储模块，被配置为将生成的第二记录存储到区块链中，以便对资源数据具有查询权限的用户从区块链中读取第一记录或第二记录。

[0014] 在一些实施例中，资源数据的处理装置还包括：第一解密模块，被配置为采用自身的私钥对区块链中的第二记录中的密钥加密信息进行解密，获得第一记录的标识和信息加密密钥；第二解密模块，被配置为采用信息加密密钥对区块链中的第一记录进行解密，获得资源数据信息。

[0015] 根据本发明一些实施例的第三个方面，提供一种资源数据的处理系统，包括：一个或多个前述资源数据的处理装置；以及区块链系统。

[0016] 根据本发明一些实施例的第四个方面，提供一种资源数据的处理装置，包括：存储器；以及耦接至存储器的处理器，处理器被配置为基于存储在存储器中的指令，执行前述任意一种资源数据的处理方法。

[0017] 根据本发明一些实施例的第五个方面，提供一种计算机可读存储介质，其上存储有计算机程序，其中，该程序被处理器执行时实现前述任意一种资源数据的处理方法。

[0018] 上述发明中的一些实施例具有如下优点或有益效果：资源数据信息以密文的形式存储在区块链中，并且仅有具有查询权限的用户可以从区块链中获取信息，从而在实现资源数据信息可追溯、不可篡改的前提下，使得用户仅能查看自身具备的权限范围内的数据，提高了资源数据的隐私性。

[0019] 通过以下参照附图对本发明的示例性实施例的详细描述，本发明的其它特征及其优点将会变得清楚。

附图说明

[0020] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0021] 图1A示出了根据本发明一些实施例的资源数据的处理方法的流程示意图。

[0022] 图1B示出了根据本发明另一些实施例的资源数据的处理方法的流程示意图。

[0023] 图2为根据本发明一些实施例的资源转移执行方法的流程示意图。

[0024] 图3为根据本发明一些实施例的资源转移明细信息处理方法的流程示意图。

[0025] 图4为根据本发明一些实施例的资源扣除方法的流程示意图。

[0026] 图5为根据本发明一些实施例的信息初始化方法的流程示意图。

[0027] 图6为根据本发明一些实施例的资源数据的处理装置的结构示意图。

[0028] 图7为根据本发明一些实施例的资源数据的处理系统的结构示意图。

[0029] 图8示出了根据本发明另一些实施例的资源数据的处理装置的结构示意图。

[0030] 图9示出了根据本发明又一些实施例的资源数据的处理装置的结构示意图。

具体实施方式

[0031] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。以下对至少一个示例性实施例的描述实际上仅仅是说明性的，决不作为对本发明及其应用或使用的任何限制。基于本发明中的实施例，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例，都属于本发明保护的范围。

[0032] 除非另外具体说明，否则在这些实施例中阐述的部件和步骤的相对布置、数字表达式和数值不限制本发明的范围。

[0033] 同时，应当明白，为了便于描述，附图中所示出的各个部分的尺寸并不是按照实际的比例关系绘制的。

[0034] 对于相关领域普通技术人员已知的技术、方法和设备可能不作详细讨论，但在适当情况下，所述技术、方法和设备应当被视为授权说明书的一部分。

[0035] 在这里示出和讨论的所有示例中，任何具体值应被解释为仅仅是示例性的，而不是作为限制。因此，示例性实施例的其它示例可以具有不同的值。

[0036] 应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步讨论。

[0037] 图1A示出了根据本发明一些实施例的资源数据的处理方法的流程示意图。如图1A所示，该实施例的资源数据的处理方法包括步骤S102～S108。

[0038] 在步骤S102中，第一客户端采用生成的信息加密密钥对资源数据信息加密，生成第一记录。

[0039] 在一些实施例中，信息加密密钥可以是第一客户端在欲对资源数据信息加密之前新生成的，从而可以提高数据的安全性。

[0040] 在步骤S104中，第一客户端将生成的第一记录存储到区块链中，并获取第一记录的标识。

[0041] 在步骤S106中，第一客户端采用第二客户端的用户的公钥加密信息加密密钥以获得密钥加密信息，生成包括第一记录的标识以及密钥加密信息的第二记录，其中，第二客户端的用户对资源数据具有查询权限。

[0042] 第一记录和第二记录即区块链中的“交易记录”。“交易记录”代表区块链的区块中的一条数据，其中记载的可以是任意信息、而并不一定记载交易信息。

[0043] 在一些实施例中，第二记录中的第一记录的标识以及密钥加密信息可以以键值对

的方式存储，例如<key:第一记录的标识,value:密钥加密信息>。

[0044] 例如，信息加密密钥为K1，第二客户端的用户的公钥为PK1，资源数据信息为Text1。采用K1对Text1的加密结果为Text1'，采用PK1对K1的加密结果为K1'。则第一记录的内容为Text1'、ID为TX1，则第二记录的内容为<TX1,K1'>。

[0045] 每个公钥都有对应其他机构的公钥信息，公钥信息的传递可以采用CA(Certificate Authority,证书授权)或其他方式、以保证其安全性。

[0046] 在步骤S108中，第一客户端将生成的第二记录存储到区块链中，以便第二客户端的用户从区块链中读取第一记录或第二记录。

[0047] 在一些实施例中，第一客户端将第一记录的标识、第二记录的标识与第二客户端的用户的账户进行绑定，以便第二客户端向用户显示绑定的第一记录和第二记录。从而，用户的客户端中仅能够显示与自己相关的记录。

[0048] 通过上述实施例的方法，资源数据信息以密文的形式存储在区块链中，并且仅有具有查询权限的用户可以从区块链中获取信息，从而在实现资源数据信息可追溯、不可篡改的前提下，使得用户仅能查看自身具备的权限范围内的数据，提高了资源数据的隐私性。

[0049] 在一些实施例中，除了步骤S102～S108以外，还可以包括步骤S110和步骤S112，如图1B所示。

[0050] 在步骤S110中，第二客户端采用第二客户端的用户的私钥对第二记录中的密钥加密信息进行解密，获得第一记录的标识和信息加密密钥。

[0051] 在步骤S112中，第二客户端采用信息加密密钥对第一记录进行解密，获得资源数据信息。

[0052] 通过上述实施例的方法，用户可以通过私钥获取密钥加密信息中的信息加密密钥。在通过第一记录的标识定位到第一记录后，可以采用信息加密密钥获取解密后的资源数据信息。从而，提高了资源数据的隐私性。

[0053] 在上述实施例中，第一客户端和第二客户端中的“第一”、“第二”用来分别指代一次将信息上传到区块链过程中的上传者和查看者。当客户端的身份转变时，其称呼可以由第一客户端变为第二客户端、或者由第二客户端变为第一客户端。例如，当客户端A上传信息a、客户端B查看信息a时，客户端A为第一客户端、客户端B为第二客户端；当客户端B上传信息b、而客户端A查看信息b时，客户端B为第一客户端、客户端A为第二客户端。

[0054] 在一些实施例中，当资源数据信息是资源转移执行信息时，查询方在获得该信息后，可以调用智能合约核对执行结果。下面以第一客户端的用户为资源转移执行机构用户、第二客户端的用户为组织机构用户或个人用户为例，描述资源转移执行过程。

[0055] 图2为根据本发明一些实施例的资源转移执行方法的流程示意图。如图2所示，该实施例的资源转移执行方法包括步骤S202～S230。

[0056] 在步骤S202中，资源转移执行机构用户的客户端采用生成的第一信息加密密钥对资源转移执行信息加密，生成第一记录。资源转移执行信息表示将组织机构用户的资源转移给个人用户，因此个人用户和组织机构用户具有对资源转移执行信息的查询权限。

[0057] 资源转移执行信息例如可以是组织机构用户通过资源转移执行机构转移的资源的名称、数量、时间等等。例如，企业通过银行向员工下发薪酬，网络平台通过运营商向个人用户分配带宽等等。

[0058] 在步骤S204中，资源转移执行机构用户的客户端将生成的第一记录存储到区块链中，并获取第一记录的标识。

[0059] 在步骤S206中，资源转移执行机构用户的客户端采用组织机构用户的公钥加密该信息加密密钥、以获得第一密钥加密信息，生成包括第一记录的标识以及第一密钥加密信息的、组织机构用户的第二记录。

[0060] 在步骤S208中，资源转移执行机构用户的客户端采用个人用户的公钥加密该信息加密密钥、以获得第二密钥加密信息，生成包括第一记录的标识以及第二密钥加密信息的、个人用户的第二记录。

[0061] 在步骤S210中，资源转移执行机构用户的客户端将生成的、组织机构用户的第二记录和个人用户的第二记录存储到区块链中。

[0062] 在步骤S212中，组织机构用户的客户端从区块链中获取组织机构用户的第二记录。

[0063] 在步骤S214中，组织机构用户的客户端采用组织机构用户的私钥对组织机构用户的第二记录中的第一密钥加密信息进行解密，获得第一记录的标识和信息加密密钥。

[0064] 在步骤S216中，组织机构用户的客户端根据第一记录的标识，从区块链中获取第一记录。

[0065] 在步骤S218中，组织机构用户的客户端采用信息加密密钥对第一记录进行解密，获得资源转移执行信息。

[0066] 在步骤S220中，响应于获得资源转移数据信息，组织机构用户的客户端调用智能合约，以便通过智能合约验证预先获得的资源转移结果与资源转移执行信息的一致性。

[0067] 在步骤S222中，个人用户的客户端从区块链中获取个人用户的第二记录。

[0068] 在步骤S224中，个人用户的客户端采用个人用户的私钥对个人用户的第二记录中的第二密钥加密信息进行解密，获得第一记录的标识和信息加密密钥。

[0069] 在步骤S226中，个人用户的客户端根据第一记录的标识，从区块链中获取第一记录。

[0070] 在步骤S228中，个人用户的客户端采用信息加密密钥对第一记录进行解密，获得资源转移执行信息。

[0071] 在步骤S230中，响应于获得资源转移数据信息，个人用户的客户端调用智能合约，以便通过智能合约验证预先获得的资源转移结果与资源转移执行信息的一致性。

[0072] 通过上述实施例的方法，可以在解密获得资源转移执行信息后，自动调用智能合约验证资源转移结果是否正确，从而可以及时发现错误数据，提高了资源数据处理的效率。

[0073] 在一些实施例中，第一客户端的用户为组织机构用户、第二客户端的用户为资源转移执行机构用户或个人用户。资源数据信息是资源转移明细信息，以便资源转移执行机构用户根据资源转移明细信息执行资源转移，例如执行图2实施例中的资源转移过程。下面参考图3描述资源转移明细信息的处理方法的实施例。

[0074] 图3为根据本发明一些实施例的资源转移明细信息处理方法的流程示意图。如图3所示，该实施例的资源转移明细信息处理方法包括步骤S302～S310。

[0075] 在步骤S302中，组织机构用户的客户端采用生成的信息加密密钥对资源转移明细信息加密，生成第一记录。

[0076] 在步骤S304中，组织机构用户的客户端将生成的第一记录存储到区块链中，并获取第一记录的标识。

[0077] 在步骤S306中，组织机构用户的客户端采用资源转移执行机构用户或个人用户的客户端的用户的公钥加密信息加密密钥、以获得密钥加密信息，生成包括第一记录的标识以及密钥加密信息的第二记录，其中，资源转移执行机构用户或个人用户对资源数据具有查询权限。

[0078] 在步骤S308中，组织机构用户的客户端将生成的第二记录存储到区块链中。

[0079] 在步骤S310中，资源转移执行机构用户或个人用户从区块链中读取第一记录或第二记录。

[0080] 通过上述实施例的方法，资源转移执行机构用户或个人用户可以查询资源转移明细信息，并且仅有与资源转移明细信息相关的用户可以查看，提高了资源转移明细信息的隐私性。

[0081] 在一些实施例中，第一客户端的用户为组织机构用户、第二客户端的用户为资源获取机构用户，资源数据信息是资源扣除信息。从而，资源获取机构用户在获得了资源扣除信息后，可以发起资源扣除。下面参考图4描述本发明资源扣除方法的实施例。

[0082] 图4为根据本发明一些实施例的资源扣除方法的流程示意图。如图4所示，该实施例的资源扣除方法包括步骤S402～S418。

[0083] 在步骤S402中，组织机构用户的客户端采用生成的信息加密密钥对资源扣除信息加密，生成第一记录。

[0084] 资源获取机构可以为保险机构、税务机构、社保机构等等。例如，企业在计算员工的薪酬后，可以进一步计算五险一金等信息，并生成资源扣除信息。

[0085] 在步骤S404中，组织机构用户的客户端将生成的第一记录存储到区块链中，并获取第一记录的标识。

[0086] 在步骤S406中，组织机构用户的客户端采用资源获取机构用户的公钥加密信息加密密钥、以获得密钥加密信息，生成包括第一记录的标识以及密钥加密信息的第二记录，其中，资源获取机构用户对资源数据具有查询权限。

[0087] 在步骤S408中，组织机构用户的客户端将生成的第二记录存储到区块链中。

[0088] 在步骤S410中，资源获取机构用户的客户端从区块链中获取第二记录。

[0089] 在步骤S412中，资源获取机构用户的客户端采用自己的私钥对第二记录中的密钥加密信息进行解密，获得第一记录的标识和信息加密密钥。

[0090] 在步骤S414中，资源获取机构用户的客户端根据第一记录的标识，从区块链中获取第一记录。

[0091] 在步骤S416中，资源获取机构用户的客户端采用信息加密密钥对第一记录进行解密，获得资源扣除信息。

[0092] 在步骤S418中，资源获取机构用户的客户端响应于获得资源扣除信息，调用资源转移智能合约，以便根据资源扣除信息将资源从组织机构用户转移到资源获取机构用户。

[0093] 通过上述实施例的方法，资源获取机构在获取了资源扣除信息之后，可以自动调用智能合约，完成资源扣除的过程。提高了资源数据的处理效率和自动化程度。

[0094] 用户的相关信息可以预先存储在区块链中。下面参考图5描述本发明信息初始化

方法的实施例。

[0095] 图5为根据本发明一些实施例的信息初始化方法的流程示意图。如图5所示，该实施例的信息初始化方法包括步骤S502～S506。

[0096] 在步骤S502中，客户端计算客户端的用户信息的哈希值。

[0097] 例如，对于个人用户，用户信息可以是姓名、个人资源账户等等；对于企业，用户信息可以是企业名称、企业标识、企业资源账号等等。

[0098] 在步骤S504中，客户端采用对用户信息具有查询权限的用户的公钥，对客户端的用户的公钥进行加密。

[0099] 在步骤S506中，客户端将包括用户信息的哈希值以及对客户端的用户的公钥进行加密的结果的初始化信息记录存储到区块链中。

[0100] 从而，具有查询权限的用户在需要使用该客户端用户的公钥加密时，可以从区块链中获取初始化信息，并采用自身的私钥进行解密，提高了信息的安全性和隐私性。

[0101] 当进行资源数据处理的参与方包括多个时，各方通过上述各个实施例组织在一起形成一个联盟，即，可以形成一个联盟链系统。各参与方在系统中的身份平等，共同参与区块链的共识机制，提高了流程的可靠性、准确性。通过密码学、智能合约等技术，使得整个资源数据的处理过程透明，并且在一定的权限内是公开的。

[0102] 下面参考图6描述本发明资源数据的处理装置的实施例。

[0103] 图6为根据本发明一些实施例的资源数据的处理装置的结构示意图。如图6所示，该实施例的资源数据的处理装置600包括：第一记录生成模块6100，被配置为采用生成的信息加密密钥对资源数据信息加密，生成第一记录；第一记录存储模块6200，被配置为将生成的第一记录存储到区块链中，并获取第一记录的标识；第二记录生成模块6300，被配置为采用对资源数据具有查询权限的用户的公钥加密信息加密密钥、以获得密钥加密信息，生成包括第一记录的标识以及密钥加密信息的第二记录；第二记录存储模块6400，被配置为将生成的第二记录存储到区块链中，以便对资源数据具有查询权限的用户从区块链中读取第一记录或第二记录。

[0104] 在一些实施例中，资源数据的处理装置600还包括：绑定模块6500，被配置为将第一记录的标识、第二记录的标识与对资源数据具有查询权限的用户的账户进行绑定，以便对资源数据具有查询权限的用户的客户端向用户显示绑定的第一记录和第二记录。

[0105] 在一些实施例中，资源数据的处理装置600还包括：第一解密模块6600，被配置为采用自身的私钥对区块链中的第二记录中的密钥加密信息进行解密，获得第一记录的标识和信息加密密钥；第二解密模块6700，被配置为采用信息加密密钥对区块链中的第一记录进行解密，获得资源数据信息。

[0106] 在一些实施例中，资源数据信息是资源转移执行信息；资源数据的处理装置600还包括：智能合约调用模块6800，被配置为响应于获得资源转移数据信息调用智能合约，以便通过智能合约验证预先获得的资源转移结果与资源转移执行信息的一致性。

[0107] 在一些实施例中，资源数据信息是资源转移执行信息；资源数据的处理装置600还包括：智能合约调用模块6800，被配置为响应于获得资源扣除信息，调用资源转移智能合约，以便根据资源扣除信息将资源从组织机构用户转移到资源获取机构用户。

[0108] 在一些实施例中，资源数据的处理装置600还包括：初始化模块6900，被配置为计

算客户端的用户信息的哈希值;对用户的公钥进行加密;将包括用户信息的哈希值以及对用户的公钥进行加密的结果的初始化信息记录存储到区块链中。

[0109] 下面参考图7描述本发明资源数据的处理系统的实施例。

[0110] 图7为根据本发明一些实施例的资源数据的处理系统的结构示意图。如图7所示,该实施例的资源数据的处理系统70包括一个或多个资源数据的处理装置710以及区块链系统720。

[0111] 图8示出了根据本发明另一些实施例的资源数据的处理装置的结构示意图。如图8所示,该实施例的资源数据的处理装置80包括:存储器810以及耦接至该存储器810的处理器820,处理器820被配置为基于存储在存储器810中的指令,执行前述任意一个实施例中的资源数据的处理方法。

[0112] 其中,存储器810例如可以包括系统存储器、固定非易失性存储介质等。系统存储器例如存储有操作系统、应用程序、引导装载程序(Boot Loader)以及其他程序等。

[0113] 图9示出了根据本发明又一些实施例的资源数据的处理装置的结构示意图。如图9所示,该实施例的资源数据的处理装置90包括:存储器910以及处理器920,还可以包括输入输出接口930、网络接口940、存储接口950等。这些接口930,940,950以及存储器910和处理器920之间例如可以通过总线960连接。其中,输入输出接口930为显示器、鼠标、键盘、触摸屏等输入输出设备提供连接接口。网络接口940为各种联网设备提供连接接口。存储接口950为SD卡、U盘等外置存储设备提供连接接口。

[0114] 本发明的实施例还提供一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现前述任意一种资源数据的处理方法。

[0115] 本领域内的技术人员应当明白,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非瞬时性存储介质(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。

[0116] 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。应理解为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。

[0117] 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。

[0118] 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。

[0119] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，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。

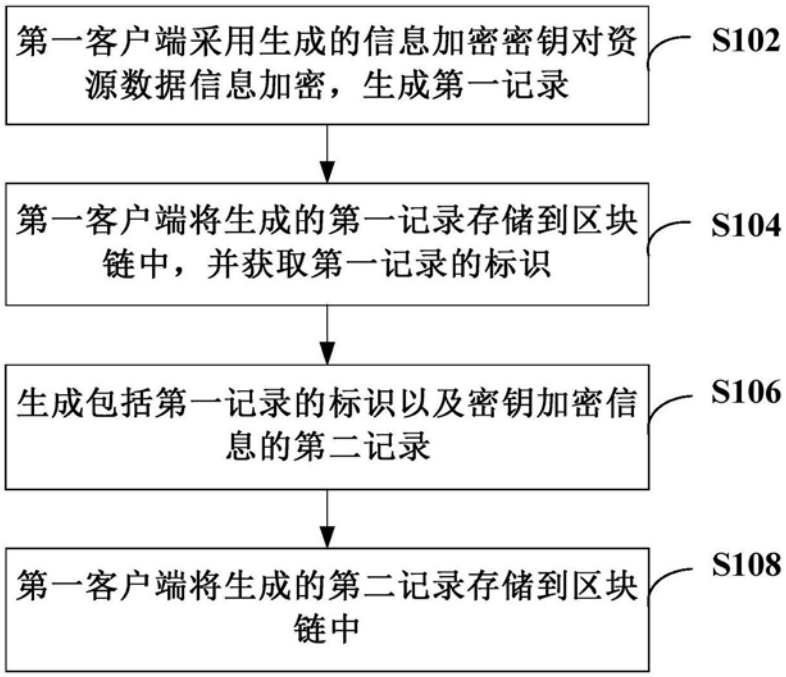

第一客户端采用生成的信息加密密钥对资源数据信息加密，生成第一记录
S102
第一客户端将生成的第一记录存储到区块链中，并获取第一记录的标识
S104
生成包括第一记录的标识以及密钥加密信息的第二记录
S106
第一客户端将生成的第二记录存储到区块链中
S108

图1A

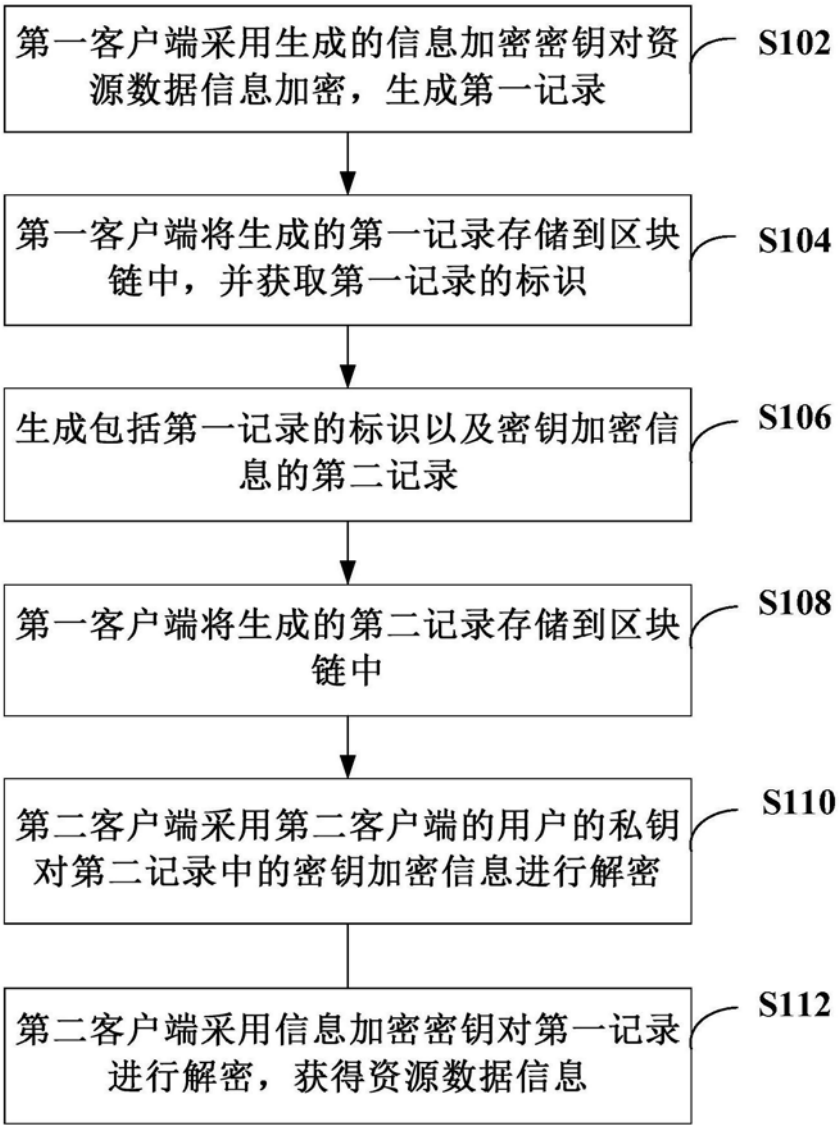

第一客户端采用生成的信息加密密钥对资源数据信息加密，生成第一记录
S102
第一客户端将生成的第一记录存储到区块链中，并获取第一记录的标识
S104
生成包括第一记录的标识以及密钥加密信息的第二记录
S106
第一客户端将生成的第二记录存储到区块链中
S108
第二客户端采用第二客户端的用户的私钥对第二记录中的密钥加密信息进行解密
S110
第二客户端采用信息加密密钥对第一记录进行解密，获得资源数据信息
S112

图1B

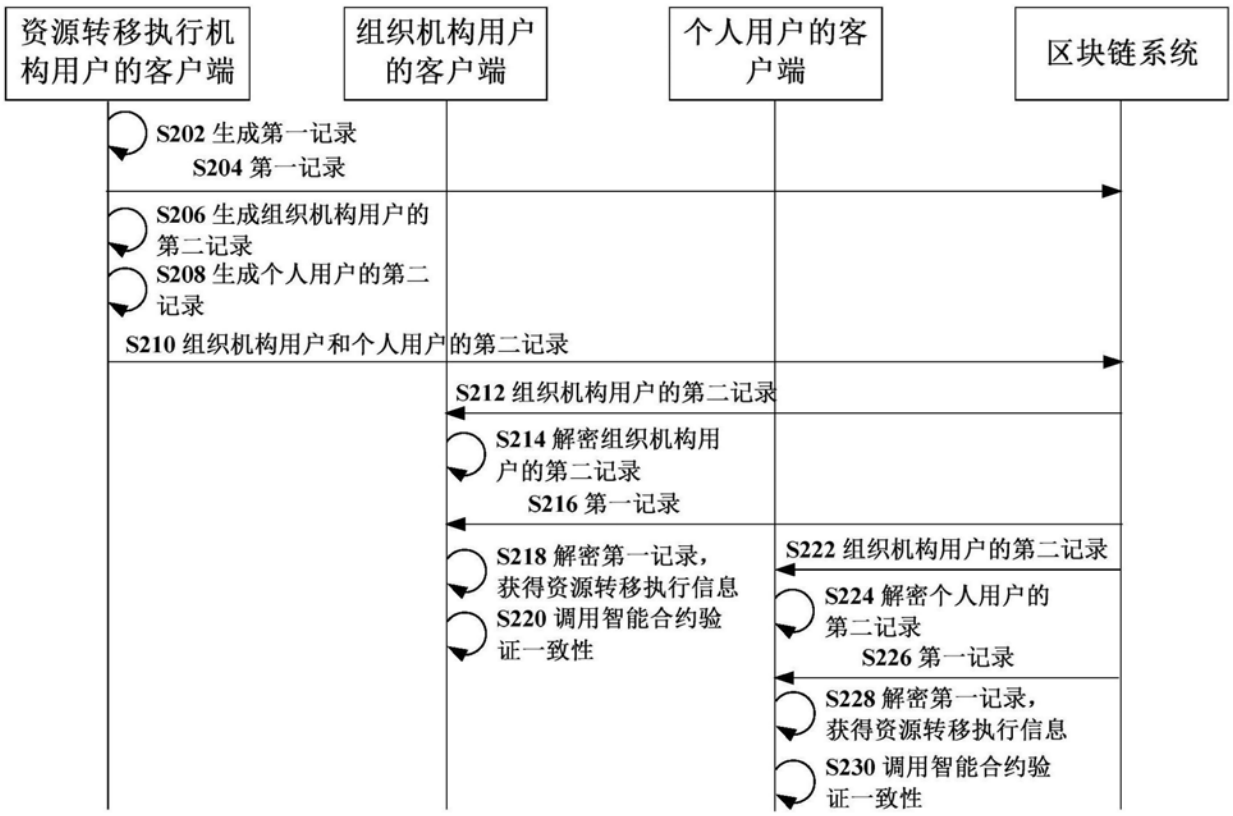

资源转移执行机构用户的客户端
组织机构用户的客户端
个人用户的客户端
区块链系统
S202 生成第一记录
S204 第一记录
S206 生成组织机构用户的第二记录
S208 生成个人用户的第二记录
S210 组织机构用户和个人用户的第二记录
S212 组织机构用户的第二记录
S214 解密组织机构用户的第二记录
S216 第一记录
S218 解密第一记录，获得资源转移执行信息
S220 调用智能合约验证一致性
S222 组织机构用户的第二记录
S224 解密个人用户的第二记录
S226 第一记录
S228 解密第一记录，获得资源转移执行信息
S230 调用智能合约验证一致性

图2

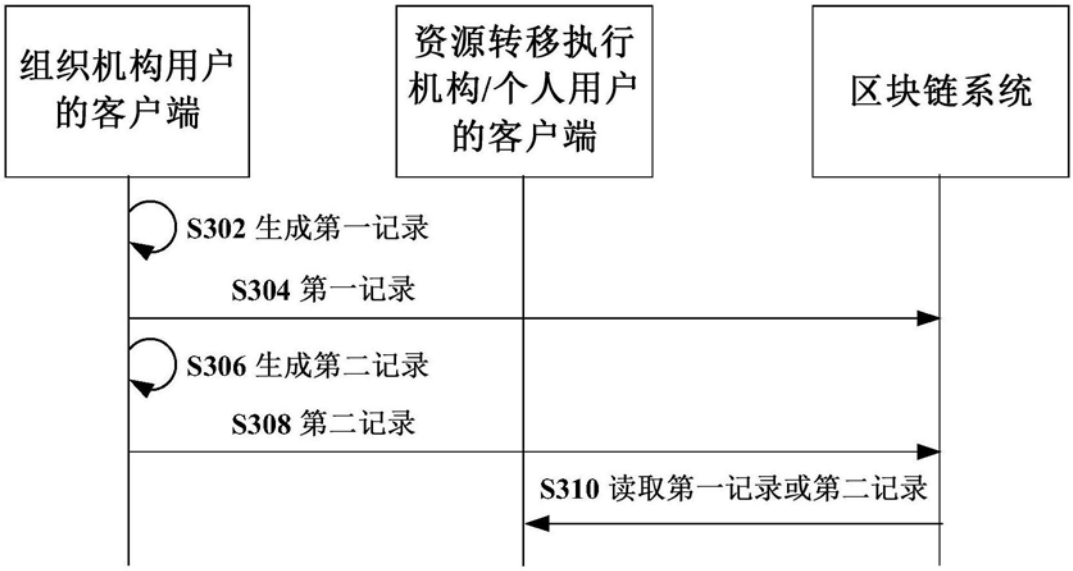

组织机构用户的客户端
资源转移执行机构/个人用户的客户端
区块链系统
S302 生成第一记录
S304 第一记录
S306 生成第二记录
S308 第二记录
S310 读取第一记录或第二记录

图3

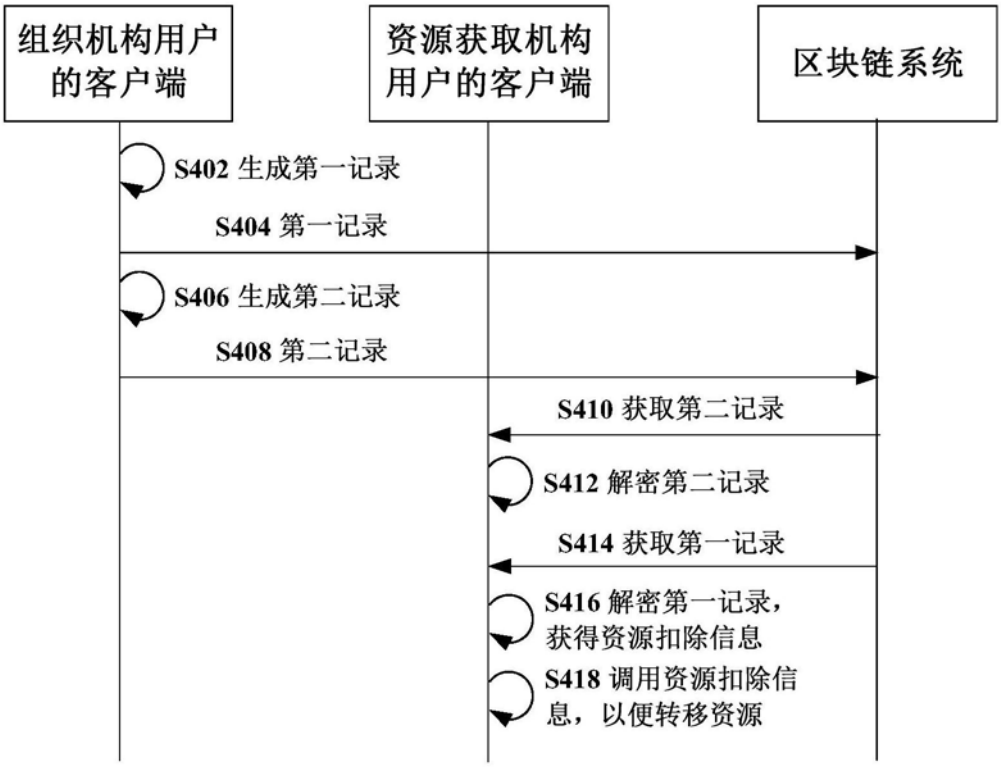

组织机构用户的客户端
资源获取机构用户的客户端
区块链系统
S402 生成第一记录
S404 第一记录
S406 生成第二记录
S408 第二记录
S410 获取第二记录
S412 解密第二记录
S414 获取第一记录
S416 解密第一记录，获得资源扣除信息
S418 调用资源扣除信息，以便转移资源

图4

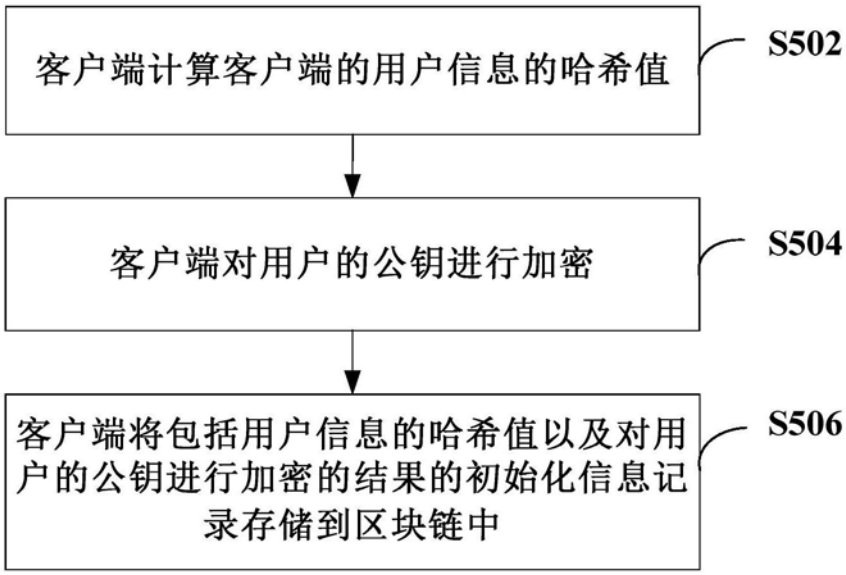

客户端计算客户端的用户信息的哈希值
S502
客户端对用户的公钥进行加密
S504
客户端将包括用户信息的哈希值以及对用户的公钥进行加密的结果的初始化信息记录存储到区块链中
S506

图5

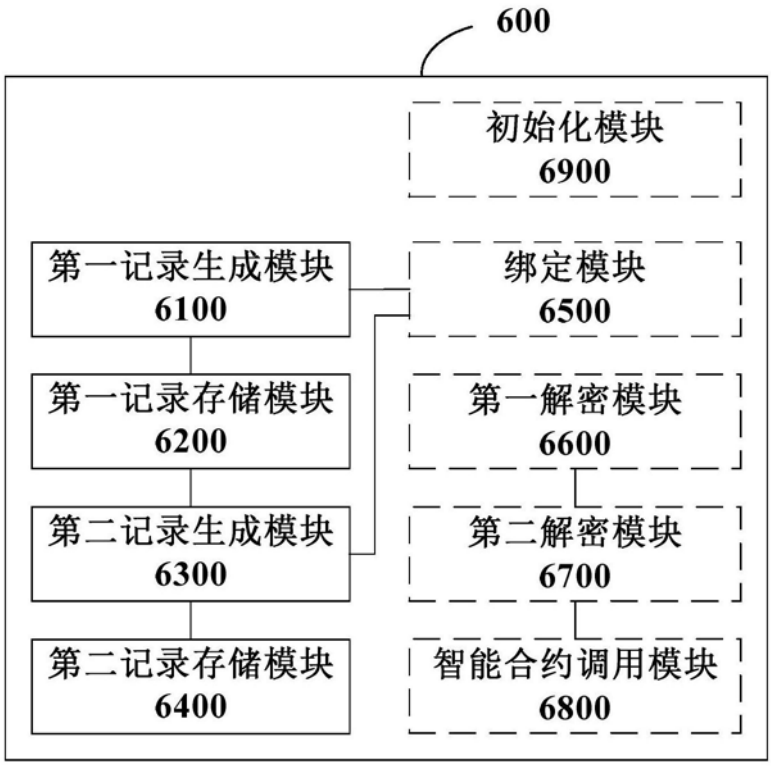

600
初始化模块
6900
第一记录生成模块
6100
绑定模块
6500
第一记录存储模块
6200
第一解密模块
6600
第二记录生成模块
6300
第二解密模块
6700
第二记录存储模块
6400
智能合约调用模块
6800

图6

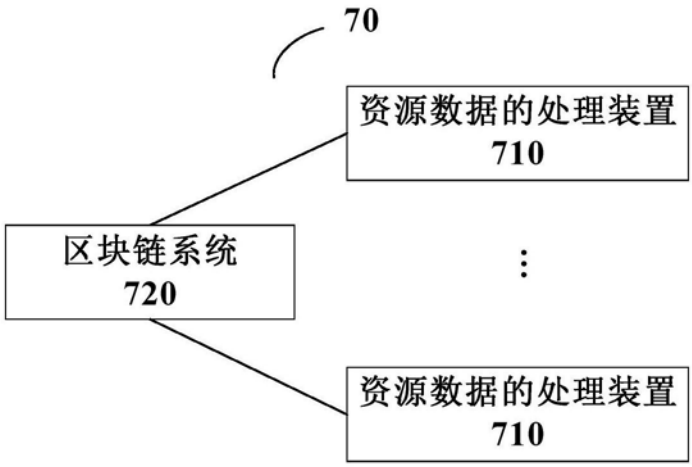

70
资源数据的处理装置
710
区块链系统
720
资源数据的处理装置
710

图7

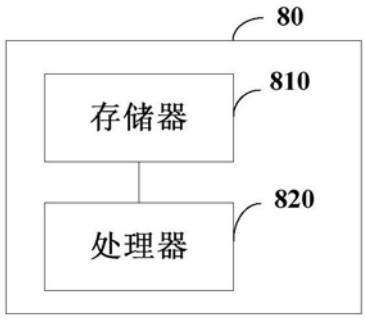

80
存储器
810
处理器
820

图8

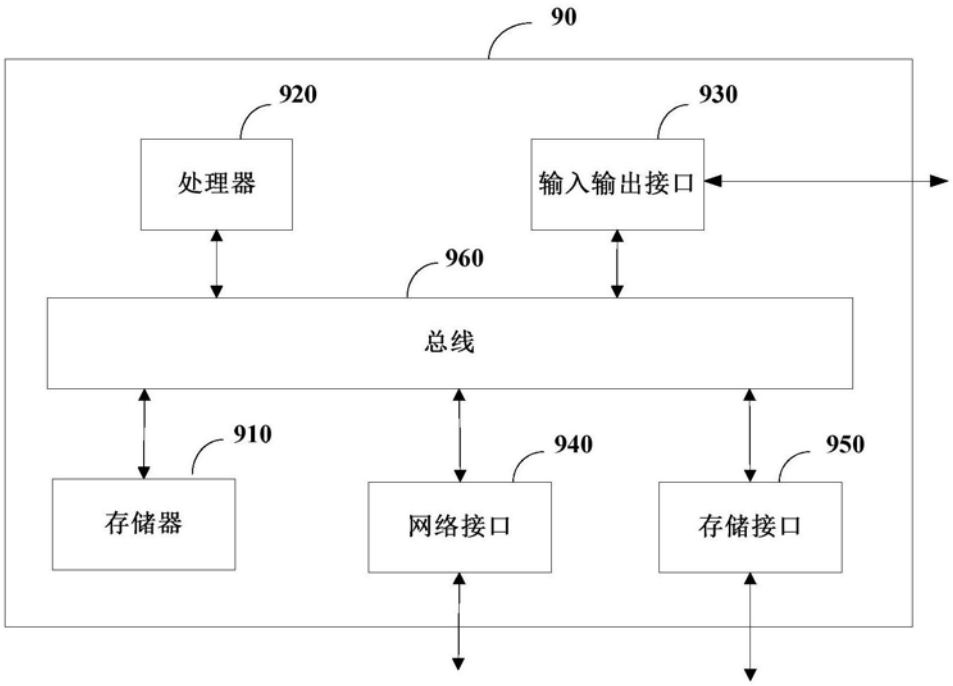

90
920
处理器
930
输入输出接口
960
总线
910
存储器
940
网络接口
950
存储接口

图9