(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 113409144 A
(43)申请公布日 2021.09.17

(21)申请号 202110676998.7

(22)申请日 2021.06.18

(71)申请人 东北大学
地址 110819 辽宁省沈阳市和平区文化路3号巷11号

(72)发明人 于汪源 田萌萌 刘园

(74)专利代理机构 沈阳东大知识产权代理有限公司 21109
代理人 李珉

(51)Int.Cl.
G06Q 40/04(2012.01)
G06F 21/62(2013.01)
G06F 21/64(2013.01)

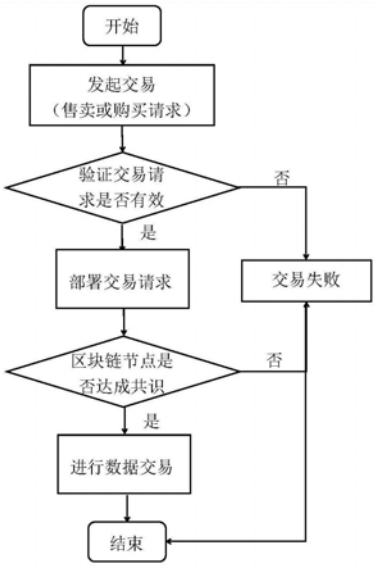
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种具有隐私保护的区块链数据交易方法

(57)摘要

本发明提供一种具有隐私保护的区块链数据交易方法，涉及区块链技术领域。参与交易得到卖方用户将原始数据经过公钥内积加密后存储到星际文件系统中，并在区块链中发起一个创建卖方智能合约的交易请求；买方用户在区块链中发起一个创建买方智能合约的交易请求；区块链上的共识节点对参与交易用户发起的交易请求进行有效性查验的，若查验通过，则区块链上的所有共识节点将交易请求记录在链，卖方用户与买方用户基于区块链进行数据交易；若检查无效，则驳回该交易申请。该方法基于区块链，保障了数据交易过程的可追溯性，保障了买卖双方的权益。数据交易过程使用密钥加密，保证了交易平台自身无法查看和保存易中的数据。



CN 113409144 A

1.一种具有隐私保护的区块链数据交易方法,其特征在于:

参与交易的用户在区块链中发起数据交易申请;

区块链上的共识节点对参与交易用户发起的交易请求进行有效性查验,若查验通过,则区块链上的所有共识节点将交易请求记录在链,卖方用户与买方用户基于区块链进行数据交易;若检查无效,则驳回该交易申请。

2.根据权利要求1所述的一种具有隐私保护的区块链数据交易方法,其特征在于:所述参与交易的用户分为卖方用户和买方用户;卖方用户是数据拥有者,发起售卖数据请求;买方用户是数据需求者,发起购买数据请求;所述卖方用户将原始数据经过公钥内积加密后存储到星际文件系统中。

3.根据权利要求2所述的一种具有隐私保护的区块链数据交易方法,其特征在于:所述参与交易的用户向区块链发起数据交易申请的具体方法为:

参与交易的卖方用户发布售卖数据请求,即卖方用户在区块链中发起一个创建卖方智能合约的交易请求,该智能合约用于售卖数据,合约内容包括数据摘要、数据存储地址、用于内积加密的公钥内容及售卖操作;买方用户发布购买数据请求,即买方用户在区块链中发起一个创建买方智能合约的交易请求,该智能合约用于购买数据,合约内容包括出价以及购买操作。

4.根据权利要求3所述的一种具有隐私保护的区块链数据交易方法,其特征在于:所述区块链上的共识节点对参与交易用户发起的交易请求进行有效性查验的具体方法为:

区块链上的共识节点接收用户的交易请求,检查交易格式是否正正确,交易签名是否合法,交易发起者地址是否存在,并检查发起交易请求的用户账户余额是否满足最大交易费用,如验证不通过,则返回错误,驳回交易请求;若验证通过,则将交易请求放入区块链上的交易池中,并向其他共识节点转发,区块链上的其他共识节点收到交易请求后,重复上述验证过程,直至该交易请求被获得出块权的共识节点打包到区块中,并全网广播。

5.根据权利要求4所述的一种具有隐私保护的区块链数据交易方法,其特征在于:所述区块链上的所有共识节点将交易请求记录在链的具体方法为:

区块链上的所有共识节点接收到包含卖方或买方交易请求的区块后,对区块进行验证,如果验证通过,共识节点将该区块同步到自己的区块链中,并从交易池中删除该交易请求,完成区块链同步,卖方智能合约或买方智能合约成功部署到区块链中。

6.根据权利要求5所述的一种具有隐私保护的区块链数据交易方法,其特征在于:所述卖方用户与买方用户基于区块链进行数据交易的具体方法为:

步骤1、买方用户调用智能合约请求卖方用户的数据;

买方用户在区块链上发起一个购买数据的交易请求,该交易请求明确标记接收账户地址,即卖方用户部署智能合约的地址;该交易请求包含买方公钥、交易出价这些基础信息;

步骤2、卖方用户响应买方用户交易请求,并发送加密数据;

卖方用户接到买方用户的数据购买请求后,将分布式存储在星际文件系统中的加密数据的hash值发送给买方用户;

步骤3、买方用户接收卖方发来的数据,并发起验证请求;

买方用户收到卖方用户发来的hash值后,从星际文件系统中获得hash值对应的加密数据,然后,随机选择一个加密数据子集,请求卖方发送对应的原始数据,以验证加密数据的

有效性；

步骤4、卖方用户向买方用户发送买方请求的原始数据；

卖方用户收到验证请求后，将待验证的原始数据用买方节点的公钥加密并发送给买方用户进行验证；

步骤5、买方用户根据卖方用户发来的待验证原始数据及卖方内积操作的公钥完成验证，买卖双方进行数据买卖交易。

7.根据权利要求5所述的一种具有隐私保护的区块链数据交易方法，其特征在于：所述买方用户完成验证，买卖双方进行数据买卖交易的具体方法为：

买方用户接收到卖方用户发来的待验证原始数据后，用卖方内积操作的公钥进行加密得到验证集，将验证集与所选择验证的加密数据子集进行对比，如果不符合，则认为收到虚假数据集，终止交易；如果符合，则验证通过，认定接收到的加密数据集为有效数据集；买方将按照事先约定好的价格向卖方转账；卖方将用于解密加密数据集的密钥发送给买方用户，完成整个交易过程。

一种具有隐私保护的区块链数据交易方法

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种具有隐私保护的区块链数据交易方法。

背景技术

[0002] 2011年至2014年这四年间，我国大数据处于起步发展阶段，大数据的市场规模增速稳定，每年均保持在20％以上。2015年，大数据市场规模已达到98.9亿元，同比增长30.7％。2016年，大数据市场规模增速迎来高潮，达到45％，市场规模继续扩大，超过160亿元。预计未来十年，大数据的市场增速稳定。

[0003] 随着大数据市场的稳定发展，数据驱动的智能应用日益普及，数据本身的价值也日益彰显，对于数据分析公司以及大数据研究人员来说，收集足够数量的数据俨然成为训练精准模型的关键。然而，有价值的数据资源分散各处，有效的数据交易可以实现数据资源的高效利用，增加数据价值。因此，一个有效的数据交易方案具有社会实用价值。当前数据交易形式主要有以下几类：

[0004] 一、数据卖方与数据买方间的私下交易。数据卖方整理、包装数据，通过一定的营销手段，将数据信息推送给可能的数据购买者。数据买方通过发现、筛选等过程寻找可信的数据所有者。双方私下通信，谈判，协商价格，最终达成数据交易。

[0005] 二、数据交易平台。自大数据概念兴起后，就受到政府以及企业界的高度关注，在此背景下，很多大数据交易平台应运而生。数据卖方和数据买方在数据交易平台注册身份，在平台上进行买卖行为。三、基于区块链的数据交易系统。随着区块链技术的出现，其去中心化和防篡改优势被应用到数据交易系统中。“李姝，赵培培，于金刚，王海汀.基于区块链的数据交易平台的研究与设计[J].小型微型计算机系统，2021，42(05)：1109-1114.”提出了一种基于区块链的数据交易模式，卖方发布一个包含数据信息的智能合约，买方通过查询区块链浏览产品目录，选中符合数据后，通过智能合约支付，卖方将数据解密秘钥通过会话通道发送给买方，买方验证数据，如果数据信息属实则双方达成交易，如验证未通过，则驳回交易。

[0006] 数据所有者与数据买方间的私下交易往往需要双方私下谈判达成交易，没有三方保障以及可追溯的交易行为，交易的安全性和可靠性无法得到保障。此外，交易双方间的连通关系很难建立，买方需要调用各种资源联系可靠地数据卖方，卖方需要额外的精力进行数据销售，增加了双方的交易成本。

[0007] 数据交易平台虽然解决了上述买卖双方间通信以及交易见证问题，但数据交易平台均为集中式平台，数据交易的安全性和公平性均依赖于数据平台，平台标准是唯一的评判标准，一旦数据平台采取非法访问等恶意行为，平台用户的权益将受到侵害。

[0008] 基于区块链的数据交易系统解决了三方交易平台的问题，保障了数据交易过程中的安全性和防篡改性，但是最终完成交易的数据信息完全裸露，数据买方可以低成本复制卖方数据并进行二次转卖，损害了数据卖方的权益，侵犯数据卖方的隐私。

发明内容

[0009] 本发明要解决的技术问题是针对上述现有技术的不足，提供一种具有隐私保护的区块链数据交易方法，针对数据交易的使用场景，利用内积加密技术以及区块链系统，提出一种去中心化的数据交易方法，规范交易过程以及参与数据交易者的行为，以此保障数据交易过程中的安全性、公平性以及透明性。克服了现有数据交易模式中，交易不可追溯，服务中心化，内容可复制的缺陷。

[0010] 为解决上述技术问题，本发明所采取的技术方案是：一种具有隐私保护的区块链数据交易方法，具体包括：

[0011] 参与交易的用户在区块链中发起数据交易申请；

[0012] 区块链上的共识节点对参与交易用户发起的交易请求进行有效性查验，若查验通过，则区块链上的所有共识节点将交易请求记录在链，卖方用户与买方用户基于区块链进行数据交易；若检查无效，则驳回该交易申请。

[0013] 进一步地，所述参与交易的用户分为卖方用户和买方用户；卖方用户是数据拥有者，发起售卖数据请求；买方用户是数据需求者，发起购买数据请求；所述卖方用户将原始数据经过公钥内积加密后存储到星际文件系统中。

[0014] 进一步地，所述参与交易的用户向区块链发起数据交易申请的具体方法为：

[0015] 参与交易的卖方用户发布售卖数据请求，即卖方用户在区块链中发起一个创建卖方智能合约的交易请求，该智能合约用于售卖数据，合约内容包括数据摘要、数据存储地址、用于内积加密的公钥内容及售卖操作；买方用户发布购买数据请求，即买方用户在区块链中发起一个创建买方智能合约的交易请求，该智能合约用于购买数据，合约内容包括出价以及购买操作。

[0016] 进一步地，所述区块链上的共识节点对参与交易用户发起的交易请求进行有效性查验的具体方法为：

[0017] 区块链上的共识节点接收用户的交易请求，检查交易格式是否正正确，交易签名是否合法，交易发起者地址是否存在，并检查发起交易请求的用户账户余额是否满足最大交易费用，如验证不通过，则返回错误，驳回交易请求；若验证通过，则将交易请求放入区块链上的交易池中，并向其他共识节点转发，区块链上的其他共识节点收到交易请求后，重复上述验证过程，直至该交易请求被获得出块权的共识节点打包到区块中，并全网广播。

[0018] 进一步地，所述区块链上的所有共识节点将交易请求记录在链的具体方法为：

[0019] 区块链上的所有共识节点接收到包含卖方或买方交易请求的区块后，对区块进行验证，如果验证通过，共识节点将该区块同步到自己的区块链中，并从交易池中删除该交易请求，完成区块链同步，卖方智能合约或买方智能合约成功部署到区块链中。

[0020] 进一步地，所述卖方用户与买方用户基于区块链进行数据交易的具体方法为：

[0021] 步骤1、买方用户调用智能合约请求卖方用户的数据；

[0022] 买方用户在区块链上发起一个购买数据的交易请求，该交易请求明确标记接收账户地址，即卖方用户部署智能合约的地址；该交易请求包含买方公钥、交易出价这些基础信息；

[0023] 步骤2、卖方用户响应买方用户交易请求，并发送加密数据；

[0024] 卖方用户接到买方用户的数据购买请求后，将分布式存储在星际文件系统中的加

密数据的hash值发送给买方用户；

[0025] 步骤3、买方用户接收卖方发来的数据，并发起验证请求；

[0026] 买方用户收到卖方用户发来的hash值后，从星际文件系统中获得hash值对应的加密数据，然后，随机选择一个加密数据子集，请求卖方发送对应的原始数据，以验证加密数据的有效性；

[0027] 步骤4、卖方用户向买方用户发送买方请求的原始数据；

[0028] 卖方用户收到验证请求后，将待验证的原始数据用买方节点的公钥加密并发送给买方用户进行验证；

[0029] 步骤5、买方用户根据卖方用户发来的待验证原始数据及卖方内积操作的公钥完成验证，买卖双方进行数据买卖交易。

[0030] 进一步地，所述买方用户完成验证，买卖双方进行数据买卖交易的具体方法为：

[0031] 买方用户接收到卖方用户发来的待验证原始数据后，用卖方内积操作的公钥进行加密得到验证集，将验证集与所选择验证的加密数据子集进行对比，如果不符合，则认为收到虚假数据集，终止交易；如果符合，则验证通过，认定接收到的加密数据集为有效数据集；买方将按照事先约定好的价格向卖方转账；卖方将用于解密加密数据集的密钥发送给买方用户，完成整个交易过程。

[0032] 采用上述技术方案所产生的有益效果在于：本发明提供的一种具有隐私保护的区块链数据交易方法，基于区块链，无需第三方信任机构就能实现数据的交易。买卖双方的交易行为在链上记载，由所有共识节点共识，保障了数据交易过程的可追溯性，保障买卖双方的权益。买卖过程使用密钥加密，保证了交易平台自身无法查看和保存交易中的数据。采用内积加密方式对卖方数据进行加密，使得数据买方无法获得数据的原始内容，不能进行复制转卖，保障了卖方的隐私并防止数据二次转卖。买方得到的最终数据是内积加密后的结果，数据原始信息得以隐藏，保障数据卖方的隐私性。内积加密后的数据对数据买方具有可用性，满足买方数据分析的需求。在此机制下，避免了数据低成本复制并转卖的行为。

附图说明

[0033] 图1为本发明实施例提供的一种具有隐私保护的区块链数据交易方法的流程图；

[0034] 图2为本发明实施例提供的公钥内积加密方法的流程图；

[0035] 图3为本发明实施例提供的卖方用户与买方用户基于以太坊进行数据交易的框架图；

[0036] 图4为本发明实施例提供的卖方用户与买方用户基于以太坊进行数据交易的流程图。

具体实施方式

[0037] 下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述。以下实施例用于说明本发明，但不用来限制本发明的范围。

[0038] 以太坊是一个可编程区块链，核心是以太坊虚拟机(EVM)。EVM是一个图灵完备的虚拟机，可以实现各种复杂逻辑，执行用户在以太坊网络中发布或调用的智能合约。智能合约实际上就是EVM可执行的代码。本实施例在以太坊上完成买卖双方的数据交易。

[0039] 本实施例中，一种具有隐私保护的区块链数据交易方法，如图1所示，具体包括以下步骤：

[0040] 步骤1、参与交易的用户在区块链中发起数据交易申请；

[0041] 参与交易的用户分为两类：卖方用户和买方用户；卖方用户是数据拥有者，发起售卖数据请求；买方用户是数据需求者，发起购买数据请求；交易过程依托于区块链进行。本实施例中，卖方用户发布售卖数据请求，即卖方用户在以太坊中发起一个创建卖方智能合约的交易请求，该智能合约用于售卖数据，合约内容包括数据摘要、数据存储地址、用于内积加密的公钥内容及售卖操作；买方用户发布购买数据请求，即买方用户在以太坊中发起一个创建买方智能合约的交易请求，该智能合约用于购买数据，合约内容包括出价以及购买操作。

[0042] 考虑到大量数据存储到区块链上会影响交易速度和调用智能合约的成本，所述卖方用户将原始数据经过公钥内积加密后存储到星际文件系统(IPFS)中，提高数据存储效率同时保障数据的防伪性以及防篡改性，卖方智能合约中的数据内容是以一系列hash值的形式表示。

[0043] 为保护数据交易内容的隐私性，卖方用户在IPFS中存储的数据并非原始数据，而是经过公钥内积加密的数据集；公钥内积加密也叫非对称密钥加密，指的是由对应的一对唯一性密钥(即公开密钥和私有密钥)组成的加密方法，具体加密方式如图2所示。

[0044] 步骤2、以太坊上的共识节点对参与交易用户发起的交易请求进行有效性查验，若查验通过，则执行步骤3，若检查无效，则驳回该交易申请；

[0045] 以太坊上的共识节点接收用户的交易请求，检查交易格式是否正正确，交易签名是否合法，交易发起者地址是否存在，并检查发起交易请求的用户账户余额是否满足最大交易费用，如验证不通过，则返回错误，驳回交易请求；若验证通过，则将交易请求放入以太坊上的交易池中，并向其他共识节点转发，以太坊上的其他共识节点收到交易请求后，重复上述验证过程，直至该交易请求被获得出块权的共识节点打包到区块中，并全网广播；所述交易池也称作内存池，用来暂存尚未被加入到区块的交易记录；同时共识节点还要将交易广播到网络中，其他共识节点对交易进行验证，验证通过以后也将该交易加入到自己的交易池里；

[0046] 步骤3、以太坊上的所有共识节点将交易请求记录在链；

[0047] 以太坊上的所有共识节点接收到包含卖方或买方交易请求的区块后，对区块进行验证，如果验证通过，共识节点将该区块同步到自己的区块链中，并从交易池中删除将该交易请求，完成区块链同步，卖方智能合约或买方智能合约成功部署到区块链中；

[0048] 步骤4、卖方用户与买方用户基于以太坊进行数据交易，如图3、4所示，整个交易过程在区块链中的共识均按步骤2和步骤3的方法完成；

[0049] 步骤4.1、买方用户调用智能合约请求卖方用户的数据；

[0050] 买方用户在以太坊上发起一个购买数据的交易请求，该交易请求明确标记接收账户地址，即卖方用户部署智能合约的地址；该交易请求包含买方公钥、交易出价这些基础信息；

[0051] 步骤4.2、卖方用户响应买方用户交易请求，并发送加密数据；

[0052] 卖方用户接到买方用户的数据购买请求后，将分布式存储在星际文件系统(IPFS)

中的加密数据的hash值发送给买方用户;(图3中卖方用户智能合约中的函数“set_ipfs_hash()”实现此功能)

[0053] 步骤4.3、买方用户接收卖方发来的数据,并发起验证请求;

[0054] 买方用户收到卖方用户发来的hash值后,从星际文件系统中获得hash值对应的加密数据,然后,随机选择一个加密数据子集,向卖方索要对应的原始数据,以验证加密数据的有效性;(图3中买方用户智能合约合约中的函数“choose_dataset()”实现此功能)

[0055] 步骤4.4、卖方用户向买方用户发送买方请求的原始数据;

[0056] 卖方用户收到验证请求后,将待验证的原始数据用买方节点的公钥加密并发送给买方用户进行验证(图3中卖方用户智能合约中的函数“send_dataset()”实现此功能)

[0057] 步骤4.5、买方用户根据卖方用户发来的待验证原始数据及卖方内积操作的公钥完成验证,买卖双方进行数据买卖交易;

[0058] 买方用户接收到卖方用户发来的待验证原始数据后,用卖方内积操作的公钥进行加密得到验证集,将验证集与所选择验证的加密数据子集进行对比,如果不符合,则认为收到虚假数据集,终止交易;如果符合,则验证通过,买方认定接收到的加密数据集为有效数据集(图3中买方用户智能合约中的函数“data_verification()”实现此功能);买方将按照事先约定好的价格向卖方转账(图3中买方用户智能合约中的函数“value_transfer()”实现此功能)。卖方将用于解密加密数据集的密钥发送给买方用户(如图3中卖方用户智能合约中的函数“generate_sk()”实现此功能),完成整个交易过程。

[0059] 最后应说明的是:以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述实施例所记载的技术方案进行修改,或者对其中部分或者全部技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明权利要求所限定的范围。

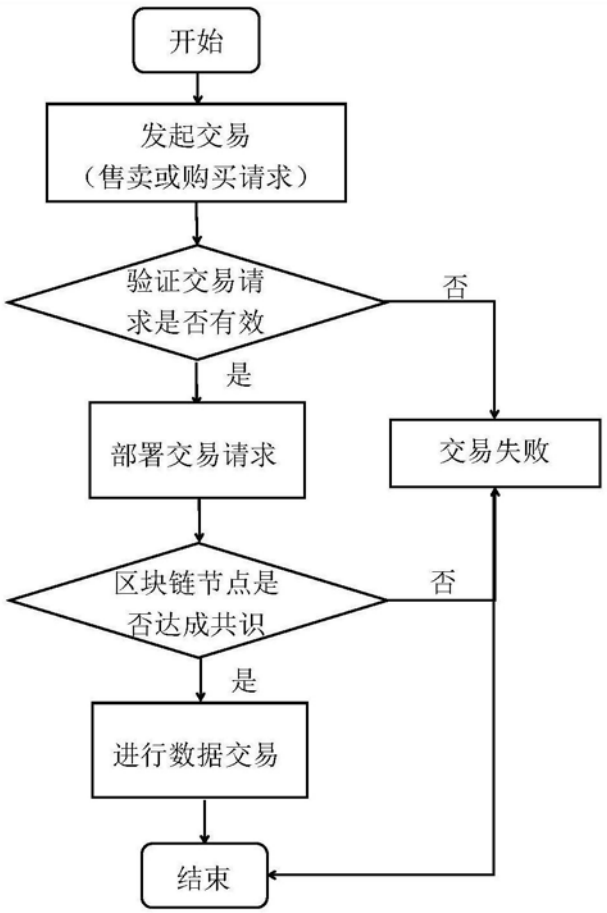

开始
发起交易
（售卖或购买请求）
验证交易请求是否有效
否
是
部署交易请求
交易失败
区块链节点是否达成共识
否
是
进行数据交易
结束

图1

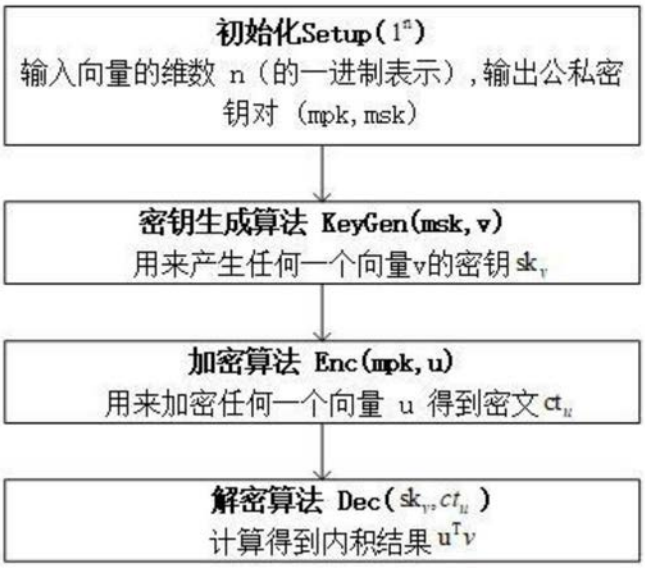

初始化Setup(1^n)
输入向量的维数 n（的一进制表示），输出公私密钥对（mpk, msk）
密钥生成算法 KeyGen(msk, v)
用来产生任何一个向量v的密钥 sk_v
加密算法 Enc(mpk, u)
用来加密任何一个向量 u 得到密文 ct_u
解密算法 Dec(sk_v, ct_u)
计算得到内积结果 $u^T v$

图2

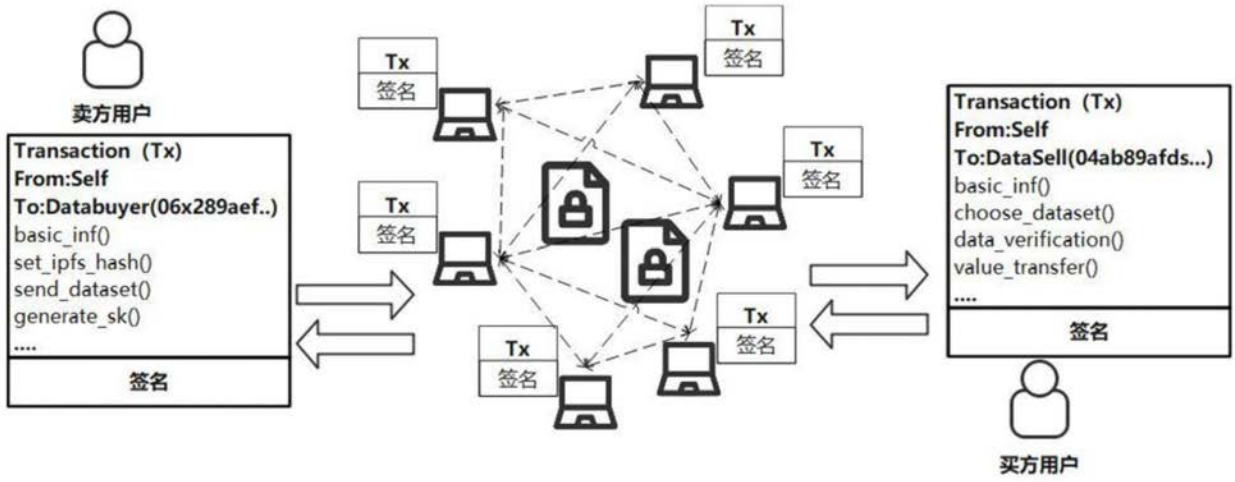

卖方用户
Transaction (Tx)
From:Self
To:Databuyer(06x289aef..)
basic_inf()
set_ipfs_hash()
send_dataset()
generate_sk()
....
签名
Tx
签名
Transaction (Tx)
From:Self
To:DataSell(04ab89afds...)
basic_inf()
choose_dataset()
data_verification()
value_transfer()
....
签名
买方用户

图3

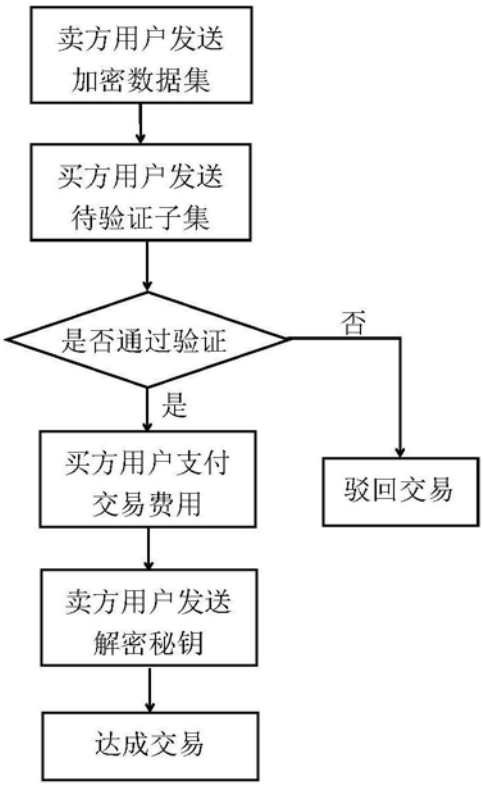

卖方用户发送加密数据集
买方用户发送待验证子集
是否通过验证
否
是
驳回交易
买方用户支付交易费用
卖方用户发送解密秘钥
达成交易

图4