(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 109711836 A
(43)申请公布日 2019.05.03

(21)申请号 201811361122.8

(22)申请日 2018.11.15

(71)申请人 远光软件股份有限公司
地址 519000 广东省珠海市港湾大道科技一路3号

(72)发明人 鲁静 宋斌 程晗蕾 向万红 陈利浩

(74)专利代理机构 深圳市威世博知识产权代理事务所(普通合伙) 44280
代理人 何倚雯

(51)Int.Cl.
G06Q 20/38(2012.01)

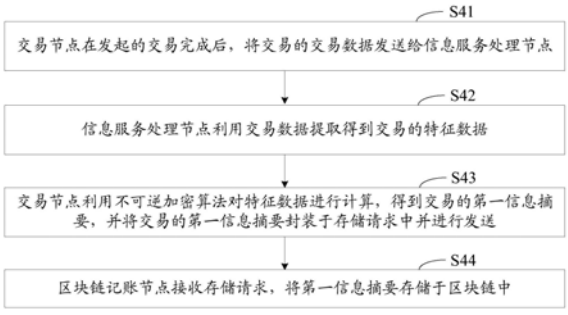
权利要求书2页 说明书10页 附图6页

(54)发明名称

一种交易的存储方法、存储网络和电子设备

(57)摘要

本申请公开了一种交易存储方法、存储网络和电子设备，交易存储方法包括：交易节点在发起的交易完成后，将交易的交易数据发送给信息服务处理节点；信息服务处理节点利用交易数据提取得到交易的特征数据；交易节点利用不可逆加密算法对特征数据进行计算，得到交易的第一信息摘要，并将交易的第一信息摘要封装于存储请求中并进行发送；区块链记账节点接收存储请求，将第一信息摘要存储于区块链中。通过上述方案，能够避免交易被恶意篡改，保证交易的可靠性。



CN 109711836 A

1.一种交易的存储方法,其特征在于,所述存储方法包括:

交易节点在发起的交易完成后,将所述交易的交易数据发送给信息服务处理节点;

所述信息服务处理节点利用所述交易数据提取得到所述交易的特征数据;

所述交易节点利用不可逆加密算法对所述特征数据进行计算,得到所述交易的第一信息摘要,并将所述交易的第一信息摘要封装于存储请求中并进行发送;

区块链记账节点接收所述存储请求,将所述第一信息摘要存储于区块链中。

2.根据权利要求1所述的存储方法,其特征在于,所述信息服务处理节点利用所述交易数据提取得到所述交易的特征数据,包括:

将所述交易数据进行筛选得到所述交易的关键数据;

将所述关键数据编码得到所述特征数据。

3.根据权利要求1所述的存储方法,其特征在于,所述区块链记账节点接收所述存储请求之后,所述方法还包括:

利用所述不可逆加密算法对设定时间段内接收到的存储请求中的第一信息摘要进行计算,得到第二信息摘要;

将所述第二信息摘要存储于所述区块链中。

4.根据权利要求3所述的存储方法,其特征在于,所述存储方法还包括:

利用智能合约对所述第一信息摘要的有效性进行检测;

若检测结果为有效则将所述第一信息摘要和第二信息摘要存储于区块链中;

若检测结果为无效,则通过报警节点进行警报。

5.根据权利要求1所述的存储方法,其特征在于,所述存储方法还包括:所述信息服务处理节点保存所述交易的特征数据与所述第一信息摘要之间的映射关系;

查询节点从所述区块链中获取待查询交易节点的交易的第一信息摘要;

根据所述第一信息摘要与对应的特征数据的映射关系从所述信息服务处理节点中查询到对应的交易的所述特征数据。

6.根据权利要求1所述的存储方法,其特征在于,所述存储方法还包括:

验证节点通过存储的所述第一信息摘要验证一特定时间内是否存在待验证交易。

7.根据权利要求6所述的存储方法,其特征在于,所述验证节点通过存储的所述第一信息摘要验证一特定时间内是否存在待验证交易包括:

所述验证节点根据待验证特征数据生成第一信息摘要或第二信息摘要,将生成的所述第一信息摘要或第二信息摘要与所述区块链中在特定时间内存储的相应第一信息摘要或相应第二信息摘要进行对比,在对比结果为相同则判断所述特定时间内存在所述待验证交易对应的记录。

8.根据权利要求1或3所述的方法,其特征在于,所述不可逆加密算法为哈希算法,所述第一信息摘要为利用所述哈希算法对所述交易数据进行计算得到的哈希值,所述第二信息摘要是利用所述哈希算法对所述哈希值进行计算得到;

其中,所述交易包括红包交易、积分交易以及企业内的商城交易,所述交易数据包括交易双方的信息、交易数额以及交易时间,所述交易数额以法定货币或积分的形式体现。

9.一种存储网络,其特征在于,包括相互连接的交易节点、信息服务处理节点和区块链记账节点;其中,

所述交易节点、信息服务处理节点和区块链记账节点分别用于执行权利要求1至8任一项所述的存储方法中的相应步骤。

10.一种电子设备，其特征在于，所述电子设备为权利要求9所述的交易节点、信息服务处理节点和区块链记账节点。

一种交易的存储方法、存储网络和电子设备

技术领域

[0001] 本申请涉及存储领域，特别是涉及一种交易的存储方法、存储网络和电子设备。

背景技术

[0002] 目前，针对交易信息的存储形式存在两种：一种是纸质形式，该形式不易存储，纸质文件容易丢失或损毁；另一种是电子化形式，其存储较为便利，且不易丢失。基于电子化文件的明显优势，文件电子化是日渐广泛使用的一种形式。

[0003] 如今，电子文件主要采用中心化存储方式，即将文件集中存储在一台或多台服务器中。然而，此中心化存储方式会使得文件容易被恶意修改，这会给文件带来较大的不安全性，特别对于一些准确性、安全性要求较高的交易文件。如果这些交易文件被不法分子通过入侵该服务器进行恶意修改，而文件相关人员却无法获知该修改，则容易造成交易双方的利益损害。

发明内容

[0004] 本申请主要解决的技术问题是提供一种交易的存储方法、存储网络和电子设备，能够避免交易数据被恶意篡改，保证交易信息的可靠性。

[0005] 为了解决上述问题，本申请第一方面提供了一种交易的存储方法，其特征在于，所述存储方法包括：

[0006] 交易节点在发起的交易完成后，将所述交易的交易数据发送给信息服务处理节点；

[0007] 所述信息服务处理节点利用所述交易数据提取得到所述交易的特征数据；

[0008] 所述交易节点利用不可逆加密算法对所述特征数据进行计算，得到所述交易的第一信息摘要，并将所述交易的第一信息摘要封装于存储请求中并进行发送；

[0009] 区块链记账节点接收所述存储请求，将所述第一信息摘要存储于区块链中。

[0010] 为了解决上述问题，本申请第二方面提供了一种存储网络，包括相互连接的交易节点、信息服务处理节点和区块链记账节点；其中，交易节点、信息服务处理节点和区块链记账节点分别用于执行上述的存储方法中的相应步骤。

[0011] 为了解决上述问题，本申请第三方面提供了一种电子设备，所述电子设备为上述网络中的交易节点、信息服务处理节点和区块链记账节点。

[0012] 上述方案中，交易数据对应的第一信息摘要可由区块链记账节点保存在区块链中，由于区块链具有高安全性、能够有效防止数据篡改，故提高了交易数据的第一信息摘要的存储可靠性，进而利用高可靠性的第一信息摘要能够对交易进行验证，可避免第一信息摘要被恶意篡改，保证第一信息摘要的可靠性，提高该交易的安全度和可信度。

附图说明

[0013] 图1是本申请一实施例中所采用的区块链技术架构示意图；

[0014] 图2是本申请一实施例中的所采用的区块链的区块的结构示意图；

[0015] 图3是本申请交易网络一实施例的结构示意图；

[0016] 图4是本申请交易的存储方法一实施例的流程示意图；

[0017] 图5是本申请交易的存储方法另一实施例的流程示意图；

[0018] 图6是本申请交易的存储方法又一实施例的流程示意图；

[0019] 图7是本申请交易的存储方法又一实施例的流程示意图；

[0020] 图8是本申请电子设备一实施例的结构示意图；

[0021] 图9是本申请非易失性存储介质一实施例的结构示意图。

具体实施方式

[0022] 下面结合说明书附图，对本申请实施例的方案进行详细说明。

[0023] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、接口、技术之类的具体细节，以便透彻理解本申请。

[0024] 本文中术语“系统”和“网络”在本文中常被可互换使用。本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在 B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0025] 区块链技术是通过去中心化的方式集体维护一个可靠的数据的技术方案。该技术方案主要让区块(Block)通过密码学方法相关联起来，每个数据块包含一定时间内的系统全部数据信息，并且生产数字签名以验证信息的有效性并链接到下一个数据块形成一条主链(Chain)。该技术自身所具有的中心化、分布式、去信任化、透明、可追踪、不可篡改、数据安全及信用的自我建立等的特征，使其在金融领域中应用有极大优势，尤其是支付清结算服务。

[0026] 为便于理解本申请区块链网络，先对本申请采用的区块链技术进行举例说明。在一具体应用中，电子设备运行该区块链技术以成为该区块链网络的节点，该区块链技术架构如图1所示，包括区块链基础层11、技术层12、服务层13以及用户层14。

[0027] 区块链基础层(又称区块链数据层)11用于封装底层数据区块，并在当前数据区块头中加盖时间戳等技术以获取数据区块的写入时间。将区块按时序链接到当前最长的主区块链上，形成最新的区块链式结构。并且，可利用不可逆加密算法(如SHA256算法)对基础数据(本申请中的记账节点接收到的基础数据是交易数据的哈希值)进行至少一次 (如两次)计算，生成唯一的区块链ID，即哈希(Hash)值。具体地，针对交易的管理，该区块链可为区块联盟链，以保证该区块链并非完全公开，只有注册的会员节点才可访问。

[0028] 技术层12，包括网络层和共识层。搭建以太坊私有链，由P2P对等网和PoW(工作量证明)共识机制构成了一个分布式账本，用于记录经过共识确认后的交易信息。其中，网络层封装了区块链网络系统的P2P 组网方式、消息传播机制和数据验证机制等要素，使各节点地位对等且以扁平式拓扑结构相互连通和相互拥有分布式、自治性、开放可自由进出等特性。区块链网络中每一个节点都能参与区块数据的校验和记账过程，仅当区块数据通过全网大部分节点验证后，才能记入区块链。区块链这种去中心化设计保证文件数据不可篡改、不可伪造。

[0029] 服务层13包括合约层和应用层。在应用层上为企业员工和各部门、分公司提供会员制服务，实现账户管理服务、分布式记账服务、身份认证服务、各种交易服务(例如红包交易、积分交易等)。在合约层上针对企业的交易定制个性化的BaaS(Blockchain as a Service)服务，在区块链底层平台上撰写交易(例如发红包、抢红包、收红包、红包消费、余额查询)、信用评分、审计预警等智能合约代码。

[0030] 用户层14，用于通过调用区块链智能合约服务实现交易的各项功能。例如用户注册、交易生成等。以红包交易的应用为例，该应用层为发红包、抢红包、收红包、红包消费等交易行为提供数据交互接口。

[0031] 区块链网络用一种去中心化的方式来收集，打包且安全保护交易数据，并把交易数据的第一信息摘要(经过至少一次哈希运算后形成的信息摘要)锚定到区块链上。具体，区块链可以采用区块联盟链的网络来实现。区块链的节点不断变换在网络系统中所承担的责任，永远不会只有一个节点在控制整个网络系统，即不会只有一个记账节点进行记账。每个节点都只是网络系统中的一部分。区块链的节点定时如每十分钟变换一次角色，没有节点会永久控制网络系统的任何一部分。

[0032] 在一具体实施例中，区块链的区块封装可如图2所示。该区块链的区块20包括区块头(Header)21和区块体(Body)22。该区块体22可存储有至少一条对基础数据(例如本申请中是对交易数据或交易数据的哈希值)进行设定哈希运算得到的哈希值(Hash)221。并通过哈希值数生成相应的密钥阵列222，再利用随机数223经过“挖矿”记入区块头21。区块头21可封装父区块(前一区块)哈希值211、时间戳212、随机数213、当前区块的目标哈希值214以及Merkle根215等信息。

[0033] 其中，该父区块哈希值211，通过该值才可将每个区块首尾相连组成了区块链；该随机数213为记录解密该区块相关数学题的答案的值；该Merkle根215是由区块体22中所有基础数据的哈希值再逐级两两哈希计算出来的，用于检验交易数据的哈希值是否存在于该区块中；该时间戳212用于记录该区块20产生的时间。可以理解的是，该区块的结构可根据采用的区块链技术的不同进行调整，例如不采用Pow共识机制，则不存在上述的随机数。

[0034] 请参阅图3，图3是本申请交易网络一实施例的结构示意图。本实施例中，该交易网络30用于完成企业内的交易，以及交易过程中产生的交易数据的存储。考虑到在区块链技术下交易的吞吐量和交易的响应时间要求，本实施例的交易网络30采用即时通讯网络32和区块链网络 31并行的方式部署。仅将关键的业务流程放入区块链服务，而一般工作流则在即时通讯网络32完成。

[0035] 企业内的交易可包括企业内的红包交易、积分交易以及电子商城的交易。其中，红包交易可包括发红包、抢红包、收红包以及提现等。

[0036] 企业内的红包交易作为目前最常见且涉及巨大现金流的电子红包种类，一直备受瞩目。它广义上是指企业在各种社交或支付平台(如支付宝、微信、QQ等)出于提高企业知名度和扩大企业影响力的目的向不特定的公众发放红包；狭义上是指企业通过自有的即时通讯软件(相当于即时通讯网络32)，将现金预付给第三方支付平台，由第三方支付平台给具有领取资格的内部员工。员工在收到红包后，可以存在自己账户零钱包中，也可以直接提现或转至自己的网银、支付宝等银行账户，用于个人消费。

[0037] 现有的企业内的红包交易可以作为企业奖励手段，随时随地发放的特性能够调动

员工工作积极性和活跃职场氛围，同时也可以与企业薪酬机制挂钩，用来实时衡量企业对员工工作的满意度。其次，企业内的红包交易可以作为企业经营手段，对资源分配和风险管控上具有相当大的灵活性。更延伸地，它的隐秘性能够避免员工之间相互比较，从一定程度上缓解企业与员工之间的矛盾，达到人才有效管理。

[0038] 积分交易包括积分的提现和充值等。该积分可为企业内部流通的虚拟积分，也就是说其仅在企业内部使用，例如可用于企业自有电子商城的消费等。

[0039] 积分还可以与红包交易的余额进行一定比例的转换。红包交易的余额通常是以法定货币的形式体现，其中，其类型可包括人民币，美元、英镑等。

[0040] 以法定货币为人民币举例，为了实现人民币与虚拟积分等价值兑换，双币都需要在区块链上锚定，用户间的红包发送使用虚拟积分实时结算，账户中的虚拟积分余额实时更新；用户在充值、提现时，经由即时通讯网络32向第三方支付平台或银行发出支付指令，并在区块链上实时记账并自动结算。

[0041] 电子商城的交易包括通过红包或积分在电子商城购买物品等。

[0042] 基于企业的交易，该区块链网络31用于存储交易数据以及交易数据对应的信息摘要(例如前文所述的哈希值)。该即时通讯网络32用于提供给用户完成企业内的交易。例如用户可在即时通讯网络32完成企业内的交易，例如可将现金预付给第三方支付平台(如支付宝、微信或 QQ等)，由第三方支付给具有领取资格的其他用户。该其他用户在收到该现金后，可以存在自己账户中，也可以直接提现或转至自己的网银、支付宝等银行账户，用于个人消费。

[0043] 即时通讯网络32可包括服务器321，用于存储用户在其上完成的一些与交易无关的数据，例如参与交易的用户之间的通话记录等，还可以用于将用户在交易过程中产生的交易数据发送到区块链网络31中，使得区块链网络31对交易数据进行存储。该区块链网络31即为利用区块链技术组成的多节点网络系统。本实施例中，该区块链网络31包括多个运行区块链技术而参与同一区块链的记账节点311(也称为区块链记账节点)。该区块链网络31用于存储交易对应的信息，例如交易数据以及交易数据的摘要信息(包括第一摘要信息和第二摘要信息)。具体地，该区块链网络31中的每个记账节点311为具有竞争记账能力的节点，以将交易记录的信息摘要存储于该区块链网络31中的每个记账节点311 的本地区块链的区块(可如图2所示)中，故每个记账节点311均保存该交易记录的信息摘要，实现交易记录的信息摘要的分布式存储。

[0044] 区块链网络31还可包括交易管理节点312、信息服务处理节点313、查询节点314、验证节点315、报警节点316以及交易节点317。以交易为红包交易为例，该交易节点317可包括红包发起节点、红包接收节点等；该交易管理节点312可对其他节点的身份信息进行管理，例如，交易节点中的用户进行实名认证、登录认证等；信息服务处理节点313可对交易过程中产生的交易数据进行处理，例如筛选处理，编码处理得到特征数据；该查询节点314可用于查询第三方交易节点的交易数据。验证节点315用于验证区块链中的交易是否真实存在；报警节点316用于在交易信息存在不符合预设规定时发出警报。

[0045] 上述节点311-317具体可以为任意电子设备，例如服务器、手机、计算机、平板电脑等，在一实施例，该记账节点311为区块链服务器。可以理解的是，上述节点312-317均可与节点311可通信，本实施例中的节点312-317作为区块链节点，例如为区块链的轻量记账节

点，但在其他实施例中，节点312-317不限定为区块链节点，即该节点312-317 的至少部分未必参与区块链。另外，上述节点的区分均是根据通过该节点当时所执行的任务，也就是当时的功能而确定的，在实际应用当中，多个不同功能的节点可为同一个主体，例如查询节点、记账节点以及报警节点可均为企业内部的审计部门对应的账户。上述节点的相应主体都需要事先在区块链平台上完成注册(在一应用中，该区块链为区块联盟链，故事先在区块联盟链平台上完成会员制注册)，并获取公私钥，确定其身份可信后，允许开展如下所述的交易存储业务。

[0046] 在一实施例中，该交易管理节点312用于对节点用户进行身份管理和身份认证。其中，该身份认证用于新节点用户注册进入区块链网络中。具体如，新节点311、313-317向交易管理节点312发送账户注册请求，具体可通过在即时通讯网络32向交易管理节点312发送账户注册请求。其中，该账户注册信息包括请求注册的账户名(提供于注册成功后用户登录该区块链网络)以及该节点用户的身份信息，例如姓名、学位、工作经历、国家身份证信息。其中，该注册信息也可仅包含用户身份信息。交易管理节点312将账户注册请求中的身份信息与预设身份数据库(如：人力资源信息管理系统)中的身份信息进行比对；若预设身份数据库不存在匹配的身份信息，则认证不通过，并返回包含失败原因的注册失败消息；若预设身份数据库存在匹配的身份信息，则认证通过，发送注册成功消息，并通过哈希算法生成唯一的用户区块链ID。并且运行区块链技术中的相关算法如设定哈希运算生成一组公钥和私钥作为注册的账户的公钥和私钥。然后，新节点将该公钥广播于该区块链网络，以使网络中的其他节点均接收并保存该用户注册的账户公钥。并且，该新节点将其私钥和区块链地址保存于本地，或者该私钥还可发送于设定的可信任的节点进行存储，以作备份。此时，账户注册完成。用户拥有这些身份证明才能在授权区块链网络上进行交易。对于用户节点账号可以分多个类别角色：普通员工用户、各部门用户、分公司用户。进一步地，交易管理节点312还可将注册请求中的身份信息保存至设定管理数据库，以统一管理参与该区块链的用户身份。

[0047] 注册所采取的哈希算法主要采用双SHA3-256哈希函数运算，即将任意长度的原始数据经过两次SHA256哈希运算后转换为长度为256位 (32字节)的二进制数字来统一存储和识别。

[0048] 可以理解的是，上述区块链网络的交易节点317在发起的交易完成后发起存储请求，以请求记账节点311进行交易数据的信息摘要的存储。

[0049] 因此，本实施例的区块链仅保存具有价值的即时消息。区块链网络上的每一个记账节点都保存着过去所有的交易数据，并且是在授权下公开透明，相关利益方通过授权机制保护下浏览关于自己权限内的交易数据，并且区块链上存储的数据是不可篡改的。

[0050] 上述区块链网络对交易进行管理的具体方式如下面实施例所述。

[0051] 请参阅图4，图4是本申请交易的存储方法一实施例的流程示意图。本实施例中，该方法由作为上述区块链网络的相关节点执行，具体包括：

[0052] S41：交易节点在发起的交易完成后，将交易的交易数据发送给信息服务处理节点。进一步的，交易节点还可将该交易数据进行存储。

[0053] 交易节点可在即时通讯网络上完成交易。在完成该交易后，可通过即时通讯网络或交易节点将该交易的交易数据发送给信息处理节点。

[0054] 例如,交易节点A可在企业内部的即时通讯网络上发送一红包给交易节点B,则在交易节点A完成该红包的发送,且交易节点B接收该红包后,交易节点A或即时通讯网络将该红包交易的交易数据发送给信息服务处理节点。

[0055] 交易数据可包括交易数额,交易双方的信息,交易方式,交易时间等信息。交易金额可以法定货币或积分的形式体现。例如,交易双方的信息可为交易节点A和交易节点B,交易方式可为交易节点A向交易节点B发送红包。

[0056] S42:信息服务处理节点利用交易数据提取得到交易的特征数据。

[0057] 具体而言,信息服务处理节点可将交易数据进行筛选得到交易的关键数据,进一步将关键数据编码得到特征数据。

[0058] 其中,筛选的规则可预先设置,根据筛选的规则将交易数据的关键数据进行筛选出来。例如在交易节点A向交易节点B发送一个金额为 10元人民币的红包时,信息服务处理节点可通过筛选的规则筛选出:A、B、10该三个关键数据。

[0059] 进一步的可对筛选出来的关键数据进行编码得到交易的特征数据。

[0060] 通过筛选和编码可将交易的原始数据进行简化,从进一步节省了存储的空间。

[0061] S43:交易节点利用不可逆加密算法对特征数据进行计算,得到交易的第一信息摘要,并将交易的第一信息摘要封装于存储请求中并进行发送。

[0062] 其中,不可逆加密算法可为前文所述的哈希算法。

[0063] 交易节点接收信息服务处理节点发送的特征数据后,可将该特征数据进行存储,并采用SHA256方法对特征数据进行计算,得到交易的哈希值,该哈希值可记为第一信息摘要。然后将该第一信息摘要封装于存储请求中后向区块链网络进行全网公布。以由区块链网络中的记账节点竞争记账权,并由竞争得到记账权的记账节点来实现对该第一信息摘要进行存储。

[0064] 进一步地,该存储请求可经加密之后再进行全网公布。例如,采用非对称加密算法进行加密。或者仅对存储请求中第一信息摘要进行加密。在一具体场景中,交易节点可采用指定的记账节点的账户公钥进行加密,以使相应的记账节点根据自身账户私钥进行解密得到解密后的存储请求,此时,只有可进行解密的记账节点可竞争该第一信息摘要的记账权。或者由可进行解密的记账节点重新广播于各记账节点,以使各记账节点共同竞争该记账权。当然,交易节点也可采用该区块链网络中所有记账节点均可解密的加密方式对该存储请求进行加密,以使记账节点接收到该存储请求之后,均可进行正确解密并竞争记账权。例如交易节点可首先将自身的公钥全网公布到各记账节点当中,在交易完成后,将获取的第一信息摘要用自身的私钥进行加密,然后全网公布,则保存有该交易节点的公钥的记账节点均可对该第一信息摘要解密,从而竞争记账权。

[0065] 进一步的,交易节点还可将该第一信息摘要与特征数据进行相互锚定,形成第一信息摘要与特征数据之间的映射关系,该映射关系可封装于存储请求中,向信息服务处理节点广播,也可以单独向信息服务处理节点进行广播,使得信息服务处理节点保存,便于后续通过该映射关系查询到对应的交易的特征数据。

[0066] S44:区块链记账节点接收存储请求,将第一信息摘要存储于区块链中。

[0067] 区块链记账节点接收到交易节点广播的存储请求后,从存储请求中获取第一信息摘要,并将该第一信息摘要存储在区块链中。其中该第一信息摘要将成为记账节点的基础

数据而进行不可逆加密算法，得到第二信息摘要，并在不可逆加密算法后争夺记账权，在获得记账权后将第二信息摘要同样存储于区块链中。

[0068] 下面对记账节点实现存储交易的具体过程进行举例说：区块链网路中的多个记账节点将当前时间段获取的第一信息摘要封装于本地如图2 所示的区块中，并通过共识机制如Pow共识机制来竞争该区块的记账权。当某个记账节点获得记账权时，向区块链网络广播该区块。区块链网络的其他区块链节点对该区块的有效性进行验证，在该区块链网络不认同区块有效性时，该区块链网络的所有区块链节点将其区块丢弃，并重新如上述竞争记账权并生成新区块；在该区块链网络认同区块有效性时，该区块链网络的所有区块链节点将所述区块或者区块头同步到自身区块链上。其中，若该节点为轻量节点，则将区块头同步于其当前区块链上，若该节点为全节点，则将整个区块同步于其当前区块链上。此时，即实现将第一信息摘要和第二信息摘要存储于所述区块链网络的区块链中。在完成存储之后，区块链网络中的各个记账节点可利用区块标识及相应第二摘要信息查找得到对应区块中存储的第一摘要信息，进而可利用该来验证该交易是否发生篡改，进而可保证该交易的安全性。

[0069] 请参阅图5，图5是本申请交易的存储方法另一实施例的部分流程示意图。本实施例主要介绍对交易的相关数据的查询。除图4所示的步骤外，还包括以下步骤：

[0070] S51：信息服务处理节点保存交易的特征数据与第一信息摘要之间的映射关系。

[0071] 在前文的步骤S43，交易节点利用不可逆加密算法对特征数据进行计算后，交易节点还可将该第一信息摘要与特征数据进行相互锚定，形成第一信息摘要与特征数据之间的映射关系，该映射关系可封装于存储请求中，向所有节点广播，也可以单独向信息服务处理节点进行广播，使得信息服务处理节点保存，便于后续通过该映射关系查询到对应的交易的特征数据。

[0072] S52：查询节点从区块链中获取待查询交易节点的交易的第一信息摘要。

[0073] 本步骤中的查询节点可为仅具有查询功能的节点，也可以为记账节点或其他节点。其中，若为仅具有查询功能的节点，其可在任一记账节点存储的区块链中获取待查询交易节点的第一摘要信息。若为记账节点，其可在自身存储的区块链中获取该带查询交易节点的第一摘要信息。

[0074] 查询节点对应的实体可为公司的审计部门。

[0075] S53：根据第一信息摘要与对应的特征数据的映射关系从信息服务处理节点中查询到对应的交易的特征数据。

[0076] 在步骤S52获取到待查询交易节点的第一摘要信息后，将其发送到信息服务处理节点中，由信息服务处理节点根据第一摘要信息和对应的特征数据的映射关系查询到交易的特征数据。

[0077] 进一步的，还可以根据特征数据的编码和筛选规则获取原始的交易数据。

[0078] 值得注意的是，上述方法查询的是第三方待查询交易节点的交易信息(例如特征数据或原始数据等)。

[0079] 在一实施例中，每个交易节点还可以将参与交易时产生的交易信息 (例如特征数据或原始数据等)进行存储，得到自身的交易信息。在一实际场景应用中，交易节点在发生交易完成后，获取得到交易的交易数据并进行存储。并进一步执行前文的步骤S41。由此在

需要查询自身的交易数据时可在存储自身交易数据的数据库中进行查询。

[0080] 综上，若交易节点仅为区块链中的普通节点，即不参与记账，则其可仅设置一个数据库用来存储自身交易产生的交易数据。若交易节点为区块链中的记账节点，则其可包括两个数据库，一个用来存储自身交易产生的交易数据，另一个用来存储所有交易节点产生的交易数据对应的区块链。

[0081] 请参阅图6，图6是本申请交易的存储方法另一实施例的部分流程示意图。本实施例主要介绍对交易的相关数据的验证。具体是通过验证节点通过存储的第一信息摘要验证一特定时间内是否存在待验证交易。更具体的，除图4所示的步骤外，还包括以下步骤：

[0082] 步骤S61：验证节点根据待验证特征数据生成第一信息摘要或第二信息摘要。

[0083] 本实施例的验证节点可为记账节点，其自身存储有所有交易节点的特征数据对应的第一信息摘要和第二信息摘要。

[0084] 待验证特征数据可以为需验证的节点自身交易产生的，也可以为其他交易节点交易产生的。例如交易节点A需要验证在特定时间段内其是否向交易节点B发起一红包交易，则该待验证特征数据则为交易节点A 自身交易产生，其可将该待验证特征数据发送给验证节点；又如审计部门对应的审计节点需要验证在特定时间段内交易节点A是否向交易节点B发起一红包交易，则该待验证特征数据则为交易节点A交易产生，审计节点可将向交易节点A发送验证请求，请求交易节点A将待验证特征数据发送给验证节点。

[0085] 验证节点在接受到待验证交易数据后可根据待验证交易数据生成第一信息摘要或第二信息摘要，以方便后续的对比。

[0086] 步骤S62：将生成的第一信息摘要或第二信息摘要与区块链中在特定时间内存储的相应第一信息摘要或相应第二信息摘要进行对比。

[0087] 本步骤中，若验证节点接根据待验证交易数据生成第一信息摘要，则将该生成的第一信息摘要和自身存储在区块链中的在特定时间内的相应第一信息摘要进行对比。例如将根据交易节点A的特征数据生成的第一信息摘要和存储在区块链中的特定时间的交易节点A对应的第一信息摘要进行比对；同理的，若验证节点接根据待验证交易数据生成第二信息摘要，则将该生成的第二信息摘要和自身存储在区块链中的在特定时间内的相应第二信息摘要进行对比。

[0088] 若对比结果为相同，则跳转到步骤S63；若对比的结果为不同，则跳转到步骤S64。

[0089] 步骤S63：判断特定时间内存在待验证红包交易对应的记录。

[0090] 步骤S64：判断特定时间内不存在待验证红包交易对应的记录。

[0091] 通过本实施例的验证方法可验证每一笔交易的真实性，有效防止不承认交易的行为以及修改交易的行为。

[0092] 应理解，通过本实施例的验证方法还可以帮助审计部门或有查询需求的用户查询和核实在特定时间段是否存在交易特定的交易记录，也就是可以查询特定时间段的多个交易记录。

[0093] 请参阅图7，图7是本申请交易的存储方法另一实施例的部分流程示意图。本实施例主要介绍对交易的相关数据的预警。值得注意的是，该预警步骤是在前文步骤S43之前执行的，因此结合前文图4的步骤得到本实施例的方法包括以下步骤：

[0094] S71：交易节点在发起的交易完成后，将交易的交易数据发送给信息服务处理节

点。

[0095] S72:信息服务处理节点利用交易数据提取得到交易的特征数据。

[0096] 步骤S71和步骤S72分别与前文所述的步骤S41和S42相同。

[0097] 步骤S73:利用智能合约对第一信息摘要的有效性进行检测。

[0098] 本步骤之前事先编写智能合约。事前资金预付、事中清结算交易、事后用户资金管理与交易记录管理等业务的智能合约编写。编写智能合约时,将审计规则统一为判断、循环两种语句,并用代码替代。记账节点在对交易的相关信息,例如第一信息摘要进行记账的同时,触发审计规则判断交易的合法性。例如,可通过判断第一信息摘要来判断该交易是否超出了预设的规则,如交易金额是否超过预设的金额阈值,交易对象是否为企业内的员工,交易时间是否合理等判断。“记账即审计”,所有审计过程无需人工干预,可利用计算机语言实现自动监管。

[0099] 区块链能够帮助企业提高红包资金流水的审计效率和增强其公信力的同时,还能优化审计预警机制。传统审计预警机制是依赖于内置在审计数据采集模块中的事件触发器,逻辑流程是:数据记录—事件触发—发送提醒—等待处理。区块链技术能够对数据丢失、更改、销毁等异常情况自动判断和处理,进而实现审计的高效无偏差监督。由于每个记账节点的账簿都是同步、实时更新的,审计人员可以利用审计终端直接访问区块链上记录的信息,实现了脱离审计数据采集模块的远程审计模式。

[0100] 本步骤可为审计部门对应的节点对第一信息摘要进行验证。

[0101] 若检测的结果为有效,则跳转到步骤S74;若检测的结果为无效,则跳转到步骤S75。

[0102] 步骤S72:将第一信息摘要和第二信息摘要存储于区块链中。具体可如前文所述,在此不再赘述。

[0103] 步骤S75:则通过报警节点进行警报。

[0104] 进一步的,智能合约根据员工的消费情况,利用事先写入的规则进行信用评分,并对异常交易进行审计预警。员工可通过即时通讯网络查询自己的历史交易记录、积分变动记录和信用分,接收异常交易预警推送。

[0105] 请参阅图8,图8是本申请电子设备一实施例的结构示意图。本实施例中,该电子设备90为图3所示存储网络中的节点311-317。该电子设备90包括存储器91、处理器92以及通信电路93。其中,电子设备 90的各个组件可通过总线耦合在一起,或者处理器分别与其他组件一一连接。

[0106] 通信电路93用于与其他电子设备如存储网络中的其他节点实现通信,具体可包括发送器和接收器。

[0107] 存储器91用于存储处理器92执行的计算机指令、处理器92在处理过程中的数据以及本地区块链,其中,该存储器91包括非易失性存储部分,用于存储上述计算机指令。

[0108] 处理器92控制该电子设备90的操作,处理器92还可以称为CPU (Central Processing Unit,中央处理单元)。处理器92可能是一种集成电路芯片,具有信号的处理能力。处理器92还可以是通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现成可编程门阵列(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。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。

[0109] 在本实施例中，处理器92通过调用存储器91存储的计算机指令，用以执行上述方法实施例中任一节点所执行的步骤。

[0110] 本申请还提供一种存储网络或区块链网络的实施例，该存储网络或区块链网络可包括图3所示中的至少部分节点，以用于实现上述任一方法实施例。例如，存储网络包括上述交易节点、信息服务处理节点和区块链记账节点，该交易节点在发起的交易完成后，将交易的交易数据发送给信息服务处理节点；信息服务处理节点利用交易数据提取得到所述交易的特征数据；交易节点利用不可逆加密算法对特征数据进行计算，得到交易的第一信息摘要，并将交易的第一信息摘要封装于存储请求中并进行发送；区块链记账节点接收存储请求，将第一信息摘要存储于区块链中。

[0111] 本申请还提供一种非易失性存储介质的实施例，如图9所示，该非易失性存储介质10存储有处理器可运行的计算机指令101，该计算机指令101用于执行上述实施例中的方法。具体地，该存储介质10具体可如图8所示的存储器91。

[0112] 上述方案可实现以下有益效果：

[0113] (1)大幅提高企业交易资金流水审计效率，缩短财务对账时间。

[0114] 传统的集团审计往往滞后于交易的发生，对审计部门而言，繁重的审计工作量也导致审计时间周期漫长，而区块链模式下，所有交易资金流入或流出动态自动记账，审计的规则自动在各分公司执行，“交易即结算”的同时，也是审计工作的开始，实现实时审计，提高其时效。数据一旦上链，便不可篡改，交易记录的绝对真实，极大缩短了财务对账时间。

[0115] (2)根源性固化会计凭证，降低财务信息真伪辨别成本。交易从发起、共识、结算、到保全等整个生命周期的数据以密码学方式被打包放入区块中，同时所有公私钥均由企业集团产生，财务数据真实透明、不可篡改，会计凭证真实性、合规性获得高度保证，减少审计结果偏离的可能性。

[0116] (3)保障记账凭证的完整性，降低审计检查风险。在区块链模式下，任何交易数据的变更同步至所有参与记账节点的本地存储账本，即使某一区块遭受故障和攻击，也不会发生数据丢失、无法恢复的情况，因此保障了审计数据的完整性，减少审计人员漏报的可能性。

[0117] (4)授权式数据跨部门、跨分公司安全共享，提升获取审计证据的工作效率。基于会员注册方式，区块链网络上的任何拥有对应密钥的节点都可以查询整个区块链上的数据记录，包括交易金额、交易对象、积分余额、积分消费明细等信息。通过“时间戳”可以知道交易何时发生、信息何时写入，数据不间断地时序排列帮助审计人员追根溯源、一笔笔验证，精准分析财务数据是否被篡改，降低了审计调查取证的难度。

[0118] (5)利用智能合约的预置规则，实现自动、实时地审计预警。

[0119] 以上描述中，为了说明而不是为了限定，提出了诸如特定系统结构、接口、技术之类的具体细节，以便透彻理解本申请。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施方式中也可以实现本申请。在其它情况中，省略对众所周知的装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

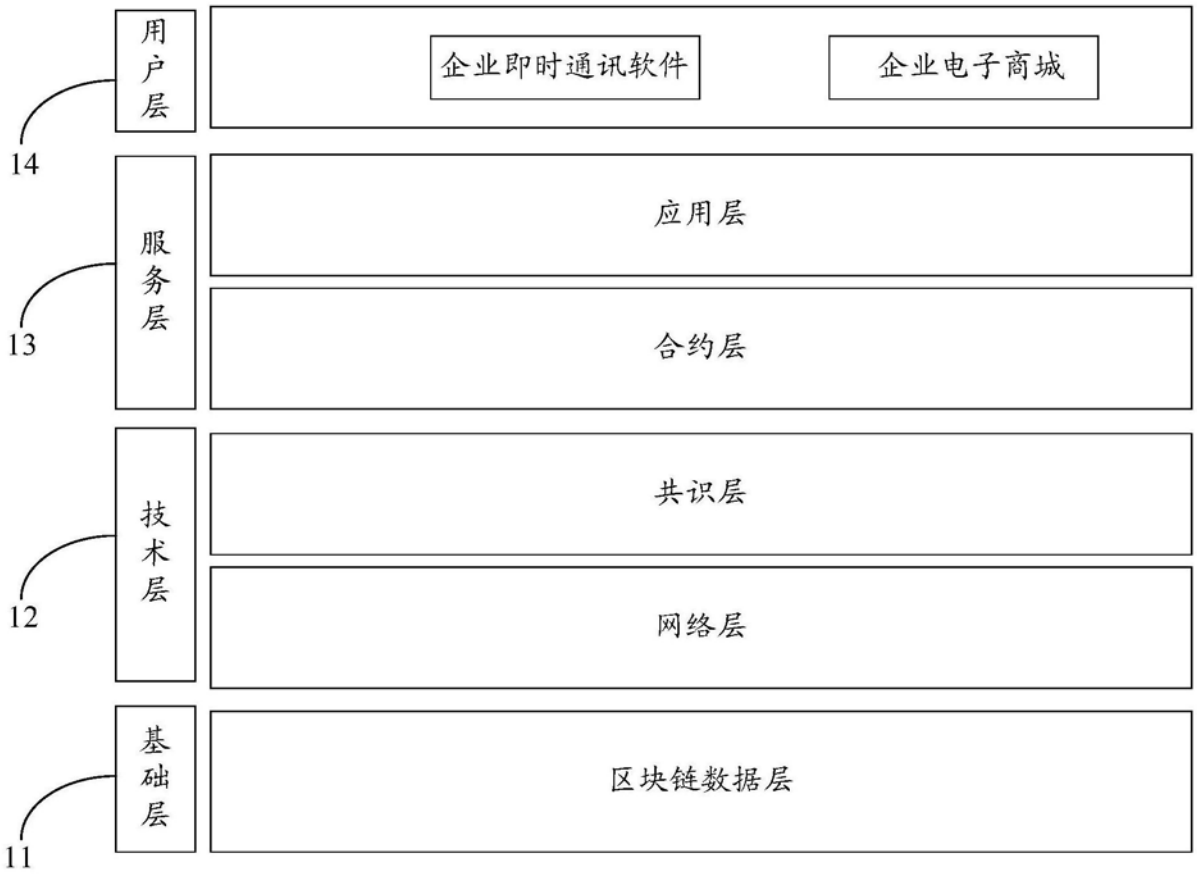

用户层
企业即时通讯软件
企业电子商城
14
服务层
应用层
合约层
13
技术层
共识层
网络层
12
基础层
区块链数据层
11

图1

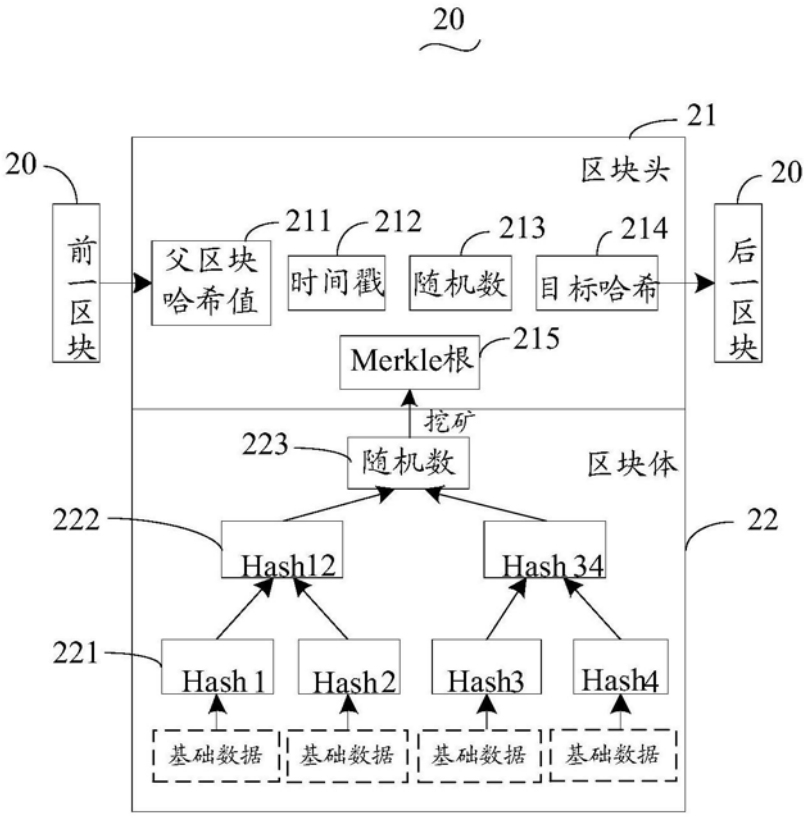

20
21
区块头
20
前一区块
父区块哈希值
211
时间戳
212
随机数
213
目标哈希
214
后一区块
20
Merkle根
215
挖矿
223
随机数
区块体
22
222
Hash12
Hash34
221
Hash 1
Hash2
Hash3
Hash4
基础数据
基础数据
基础数据
基础数据

图2

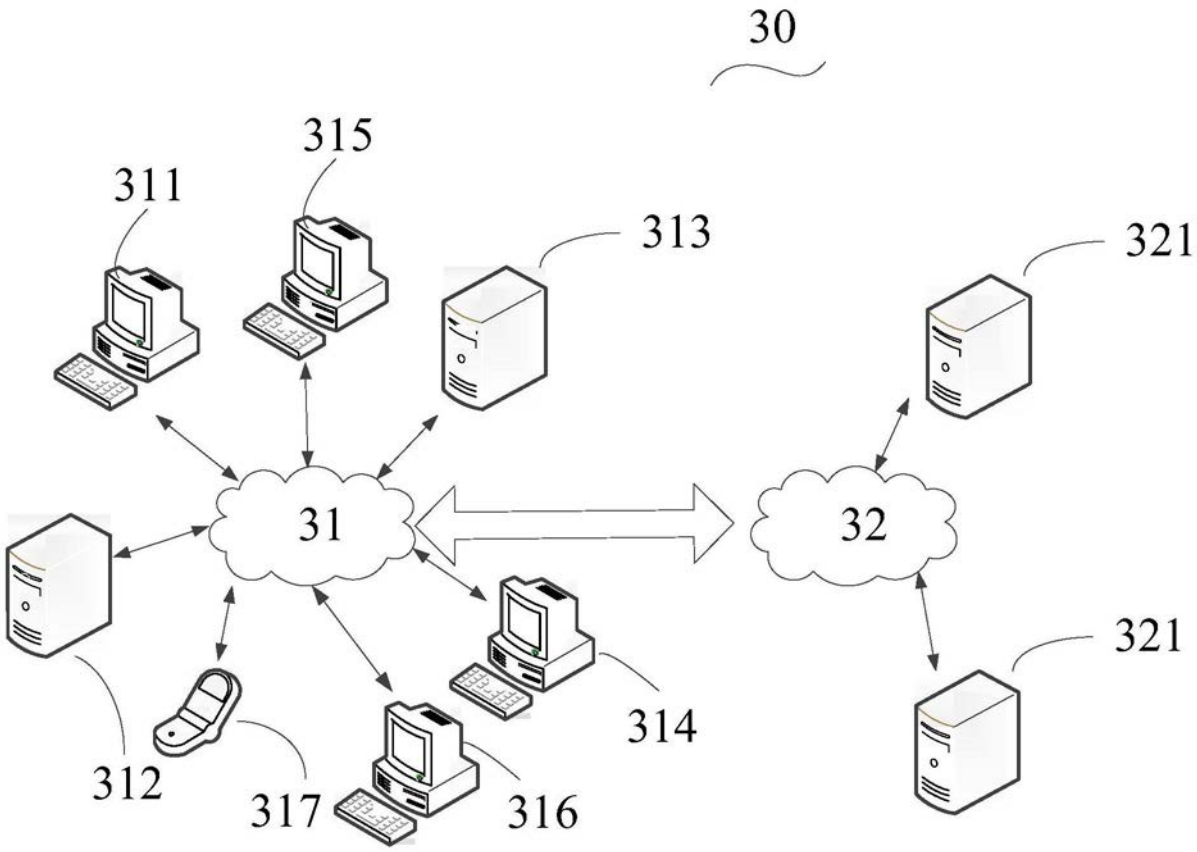

30
315
311
313
321
31
32
321
314
312
317
316

图3

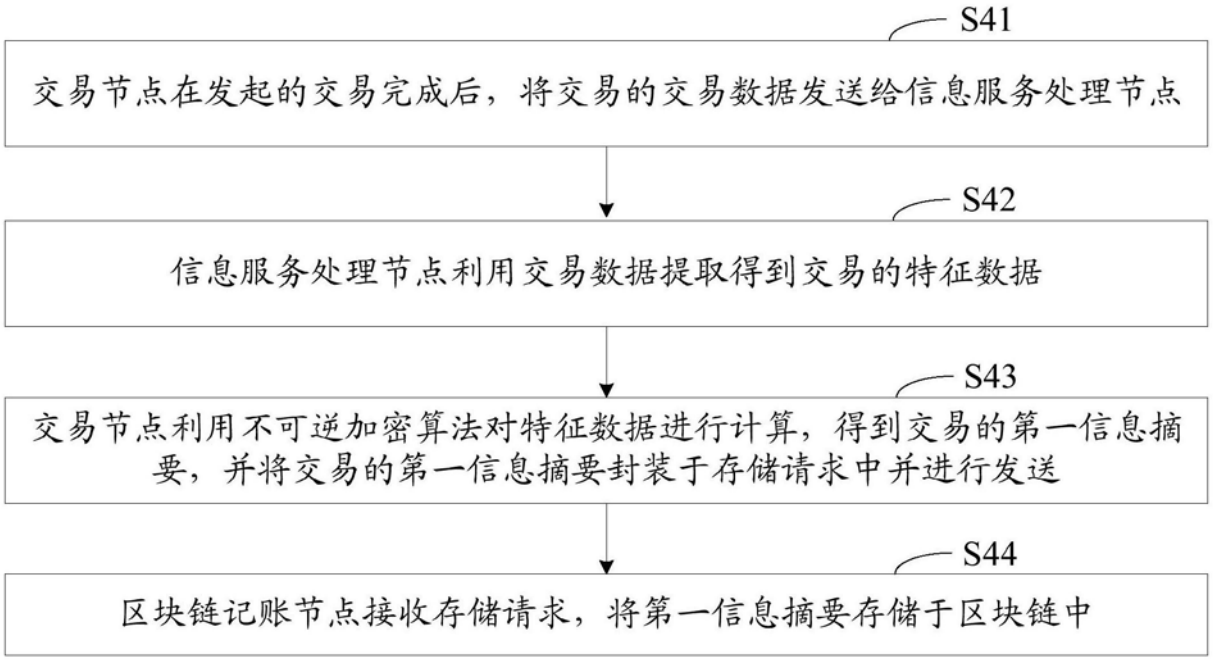

S41
交易节点在发起的交易完成后，将交易的交易数据发送给信息服务处理节点
S42
信息服务处理节点利用交易数据提取得到交易的特征数据
S43
交易节点利用不可逆加密算法对特征数据进行计算，得到交易的第一信息摘要，并将交易的第一信息摘要封装于存储请求中并进行发送
S44
区块链记账节点接收存储请求，将第一信息摘要存储于区块链中

图4

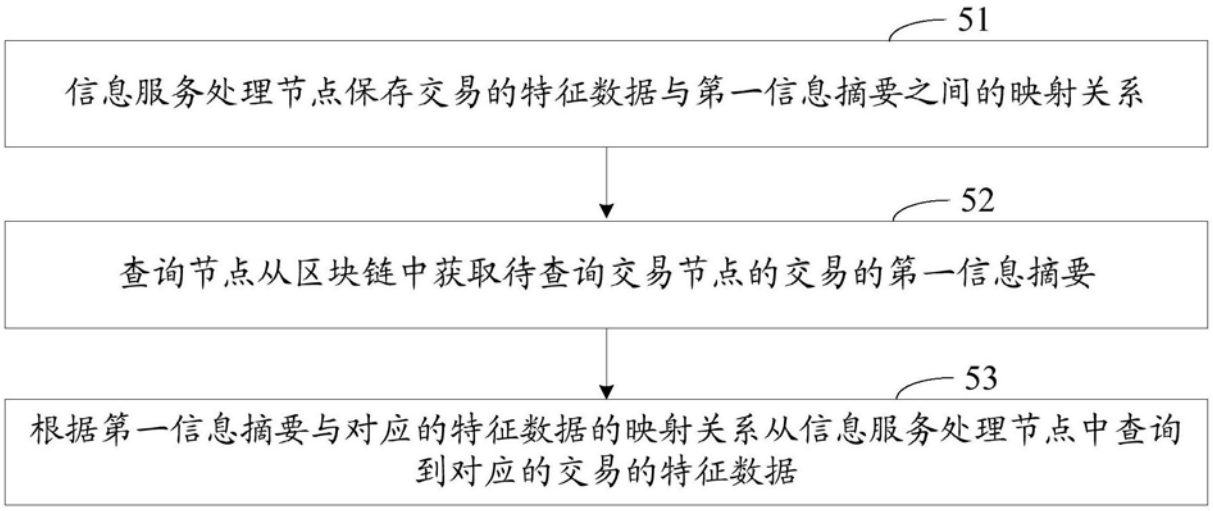

51
信息服务处理节点保存交易的特征数据与第一信息摘要之间的映射关系
52
查询节点从区块链中获取待查询交易节点的交易的第一信息摘要
53
根据第一信息摘要与对应的特征数据的映射关系从信息服务处理节点中查询到对应的交易的特征数据

图5

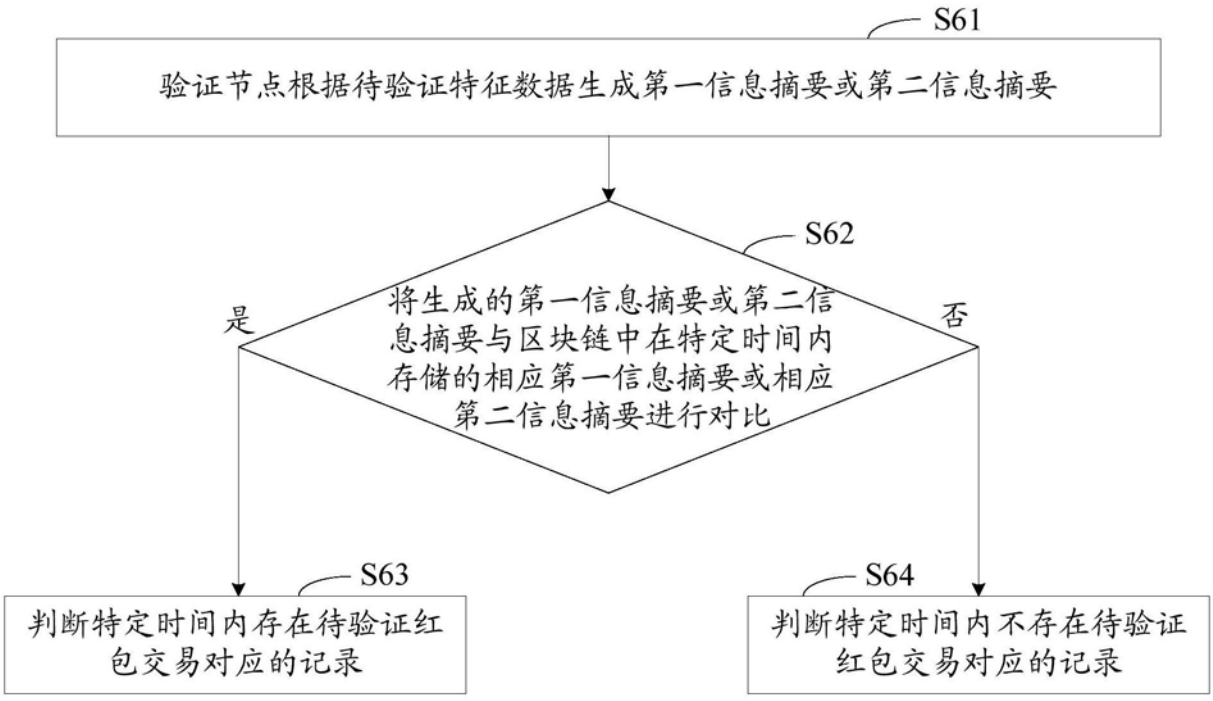

S61
验证节点根据待验证特征数据生成第一信息摘要或第二信息摘要
S62
将生成的第一信息摘要或第二信息摘要与区块链中在特定时间内存储的相应第一信息摘要或相应第二信息摘要进行对比
是
否
S63
判断特定时间内存在待验证红包交易对应的记录
S64
判断特定时间内不存在待验证红包交易对应的记录

图6

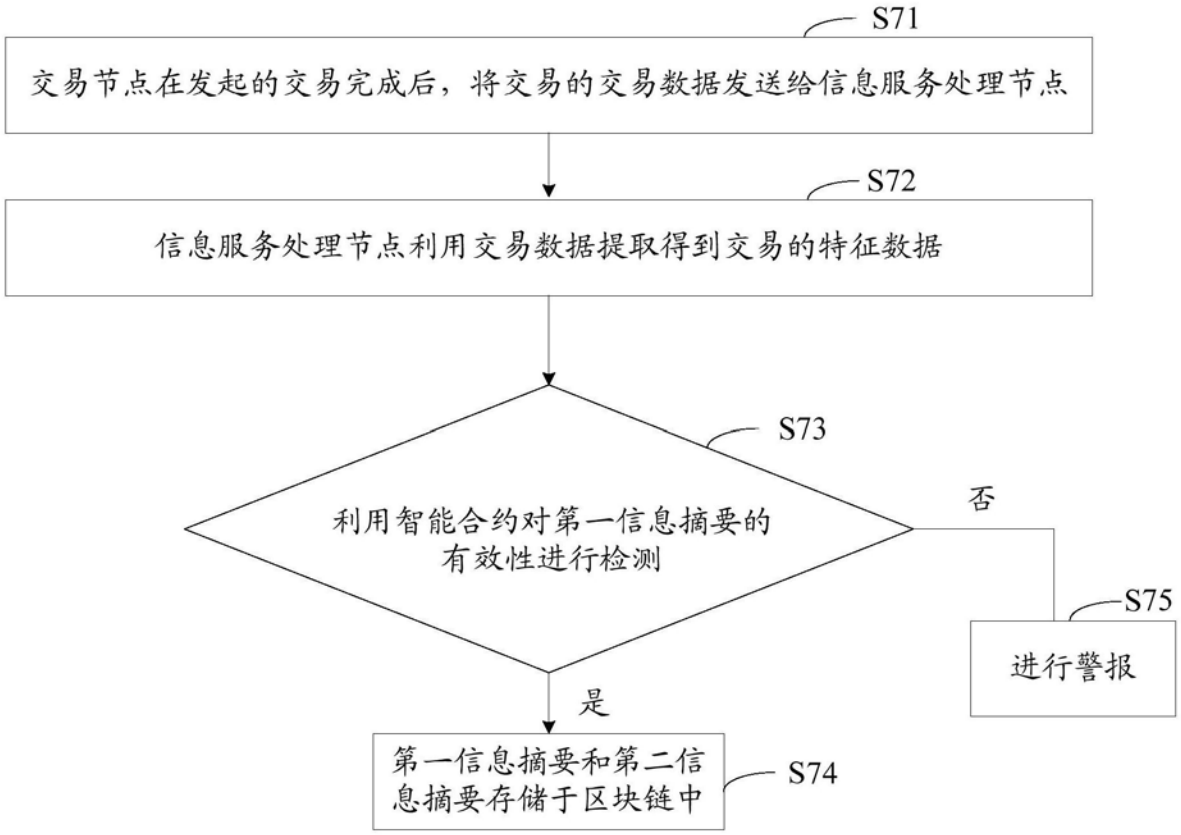

S71
交易节点在发起的交易完成后，将交易的交易数据发送给信息服务处理节点
S72
信息服务处理节点利用交易数据提取得到交易的特征数据
S73
利用智能合约对第一信息摘要的有效性进行检测
否
S75
进行警报
是
第一信息摘要和第二信息摘要存储于区块链中
S74

图7

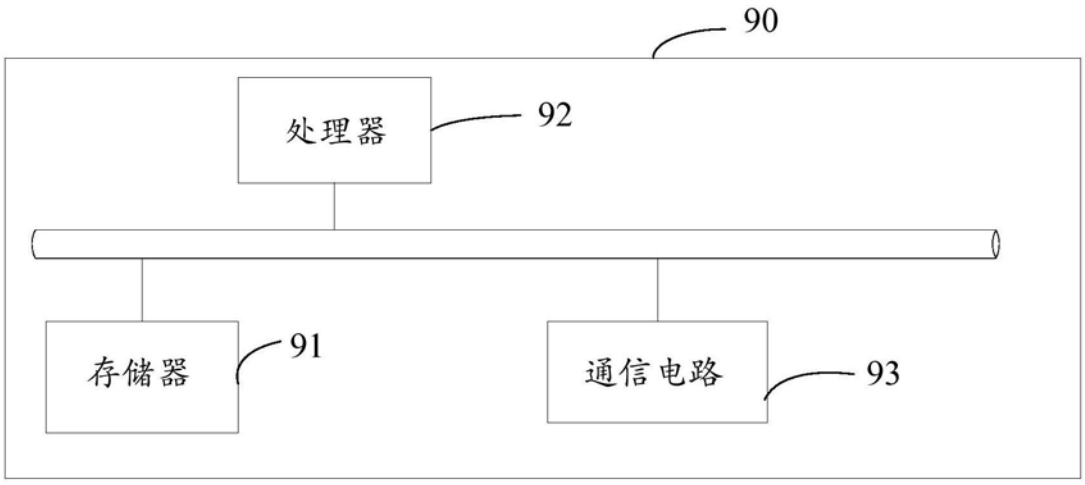

90
处理器
92
存储器
91
通信电路
93

图8

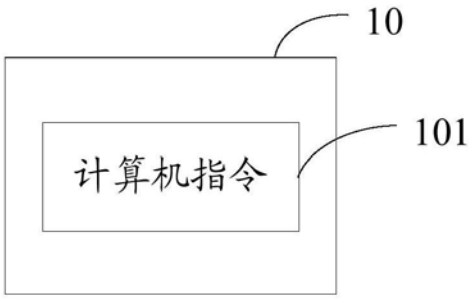


图9