(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 113435891 B
(45)授权公告日 2021.11.26

(21)申请号 202110978049.4

(22)申请日 2021.08.25

(65)同一申请的已公布的文献号
申请公布号 CN 113435891 A

(43)申请公布日 2021.09.24

(73)专利权人 环球数科集团有限公司
地址 518063 广东省深圳市南山区粤海街道高新南九道10号深圳湾科技生态园10栋B座17层01-03号

(72)发明人 张卫平 丁烨 张浩宇 黄筱雨

(74)专利代理机构 北京清控智云知识产权代理事务所(特殊普通合伙) 11919
代理人 马肃

(51)Int.Cl.
*G06Q 20/38*(2012.01)
*G06Q 20/40*(2012.01)
*G06F 21/60*(2013.01)
*G06F 21/64*(2013.01)

(56)对比文件
CN 112487443 A,2021.03.12
CN 104917793 A,2015.09.16
CN 109493009 A,2019.03.19
CN 111046427 A,2020.04.21
CN 111767559 A,2020.10.13
AU 2021100984 A4,2021.04.29

审查员 余汉鸣

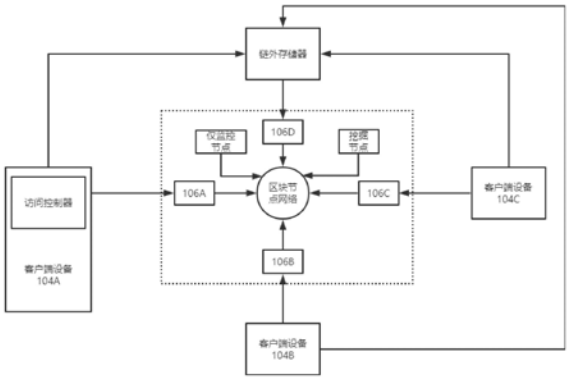
权利要求书2页 说明书8页 附图4页

(54)发明名称

一种基于区块链的可信数据颗粒化共享系统

(57)摘要

本发明提供了一种基于区块链的可信数据颗粒化共享系统,其特征在于,包括客户端设备、区块链节点和链外存储器,所述链外存储器用于保存需要共享的数据,所述区块链节点用于广播和记录对共享数据的操作,所述客户端设备用于接入区块链节点并对数据进行本地处理,所述客户端设备包括访问控制器、加密组件和上传组件,所述访问控制器对申请访问数据的交易进行处理,所述加密组件对上传的共享数据进行加密处理,所述上传组件与所述链外存储器连接并将加密后的数据上传到所述链外存储器;本系统将数据本体与数据操作分开记录,而数据操作采用区块链记录,保证了数据的可信化,而访问控制器能够实现对共享数据的颗粒化授权。




CN 113435891 B

1.一种基于区块链的可信数据颗粒化共享系统,其特征在于,包括客户端设备、区块链节点和链外存储器,所述链外存储器用于保存需要共享的数据,所述区块链节点用于广播和记录对共享数据的操作,所述客户端设备用于接入区块链节点并对数据进行本地处理;

所述区块链节点包括广播和监控节点、挖掘节点和仅监控节点,所述广播和监控节点用于连接客户端设备和链外存储器,并对客户端设备和/或链外存储器上传的交易进行广播及监控,所述挖掘节点对完成的交易进行挖掘生成块并将块记录在区块链中,所述监控节点对节点网络中广播的交易进行监控;

所述客户端设备包括访问控制器、加密组件、上传组件和连接组件,所述访问控制器对申请访问数据的交易进行处理,所述加密组件对上传的共享数据进行加密处理,所述上传组件与所述链外存储器连接并将加密后的数据上传到所述链外存储器,所述连接组件与所述广播和监控节点连接用于传递交易;

所述访问控制器能够对被申请访问的数据内容进行颗粒度批准及撤销,所述访问控制器获取到保存在链外存储器中的部分数据的首尾地址,并分别将首尾地址处理得到哈希值$H_1$和$H_2$,若有n段数据,则按顺序处理得到哈希值序列{$H_1$、$H_2$、...、$H_{2n}$};

这些哈希值的获取公式为:

$H_1$=Hash(Ad||ID);

$H_i$=Hash(Ad||ID||$H_{i-1}$),1<i<=2n;

其中,Ad为数据段的首地址或尾地址,ID为申请方的用户ID;

当含有所述哈希值序列的交易被广播并被链外存储器获取后,所述链外存储器根据所述哈希值序列批准或撤销部分数据的授权。

2.如权利要求1所述的一种基于区块链的可信数据颗粒化共享系统,其特征在于,所述广播和监控节点保存有与其连接的客户端或链外存储器的ID并构成维护列表,所述广播和监控节点通过所述列表中的ID识别在节点网络中需要获取的交易。

3.如权利要求2所述的一种基于区块链的可信数据颗粒化共享系统,其特征在于,在节点网络中广播的交易类型包括数据上传、数据访问请求、数据访问授权、数据访问确认,所述数据上传是在客户端设备往链外存储器上传共享数据后在节点网络中广播的交易,所述数据访问请求是接收到数据上传交易的任意第三方客户端向数据所有者客户端申请访问数据的交易,所述数据访问授权是数据所有者客户端在接收到数据访问请求后的答复交易,所述数据访问确认是由链外存储器在解密并提供数据后发起,由第三方客户端接收数据后进行签收的交易。

4.如权利要求3所述的一种基于区块链的可信数据颗粒化共享系统,其特征在于,在节点网络中广播的交易类型还包括撤销数据授权,所述撤销数据授权由数据所有者客户端发起,链外存储器接收的交易,当链外存储其接收撤销数据授权后,对应的第三方客户端将无法从所述链外存储器中获取到撤销授权的部分数据。

5.如权利要求4所述的一种基于区块链的可信数据颗粒化共享系统,其特征在于,所述链外存储器在接收到哈希值序列时,根据所述哈希值序列确定初步检索地址范围[a%,b%]:

$$a\% = H'_{i-1}\%;$$

$$b\% = H_i\% = H'_{i-1}\% + (1 - H'_{i-1}\%) \bullet \frac{i}{2n};$$

其中，$H_0'\%=0$，$H_i'\%$表示已经搜索到的哈希值$H_i$的对应地址在整个申请数据中的百分比位置，$H_i\%$表示预估的哈希值$H_i$的对应地址在整个申请数据中的百分比位置；

在初步检索地址范围内[a%,b%]采用首尾交替方式检索，若未在[a%,b%]范围内检索到对应的地址，继续在[b%,100%]范围内采用按序检索。

# 一种基于区块链的可信数据颗粒化共享系统

## 技术领域

[0001] 本发明涉及数据管理技术领域，尤其涉及一种基于区块链的可信数据颗粒化共享系统。

## 背景技术

[0002] 实现数据共享，可以使更多的人更充分地使用已有数据资源，减少资料收集、数据采集等重复劳动和相应费用，而把精力重点放在开发新的应用程序及系统集成上。由于不同用户提供的数据可能来自不同的途径，其数据内容、数据格式和数据质量千差万别，因而给数据共享带来了很大困难，有时甚至会遇到数据格式不能转换或数据转换格式后丢失信息的棘手问题，严重地阻碍了数据在各部门和各软件系统中的流动与共享。

[0003] 现在已经开发出了很多数据共享系统，经过我们大量的检索与参考，发现现有的共享系统有如公开号为KR101500118B1，KR101818004B1、CN103369050B和KR101528376B1所公开的系统，其包括管理服务器及分别与管理服务器连接的数个门户服务器，所述管理服务器具有依次连接的权限配置模块、调用模块、存储模块及信息整理模块；本发明中管理服务器提供信息时，可以直接通过调用模块调用本身存储在存储模块中的数据信息，若存储模块没有相关信息，则调用模块调用指定门户服务器中的数据信息并存储在存储模块中，然后通过信息整理模块组装Portlet信息，最后通过请求门户服务器展现数据信息。但该系统中共享的数据存在被篡改的可能，而且对共享数据的数据无法实现高颗粒度性。

## 发明内容

[0004] 本发明的目的在于，针对所存在的不足，提出了一种基于区块链的可信数据颗粒化共享系统，

[0005] 本发明采用如下技术方案：

[0006] 一种基于区块链的可信数据颗粒化共享系统，包括客户端设备、区块链节点和链外存储器，所述链外存储器用于保存需要共享的数据，所述区块链节点用于广播和记录对共享数据的操作，所述客户端设备用于接入区块链节点并对数据进行本地处理；

[0007] 所述区块链节点包括广播和监控节点、挖掘节点和仅监控节点，所述广播和监控节点用于连接客户端设备和链外存储器，并对客户端设备和/或链外存储器上传的交易进行广播及监控，所述挖掘节点对完成的交易进行挖掘生成块并将块记录在区块链中，所述仅监控节点对节点网络中广播的交易进行监控；

[0008] 所述客户端设备包括访问控制器、加密组件、上传组件和连接组件，所述访问控制器对申请访问数据的交易进行处理，所述加密组件对上传的共享数据进行加密处理，所述上传组件与所述链外存储器连接并将加密后的数据上传到所述链外存储器，所述连接组件与所述广播和监控节点连接用于传递交易；

[0009] 所述访问控制器能够对被申请访问的数据内容进行颗粒度批准及撤销，所述访问控制器获取到保存在链外存储器中的部分数据的首尾地址，并分别将首尾地址处理得到哈

希值$H_1$和$H_2$，若有n段数据，则按顺序处理得到哈希值序列{$H_1$、$H_2$、...、$H_{2n}$}；

[0010] 这些哈希值的获取公式为：

[0011] $H_1$=Hash(Ad||ID)；

[0012] $H_i$=Hash(Ad||ID||$H_{i-1}$)，1<i<=2n；

[0013] 其中，Ad为数据段的首地址或尾地址，ID为申请方的用户ID；

[0014] 当含有所述哈希值序列的交易被广播并被链外存储器获取后，所述链外存储器根据所述哈希值序列批准或撤销部分数据的授权；

[0015] 进一步的，所述广播和监控节点保存有与其连接的客户端或链外存储器的ID并构成维护列表，所述所述广播和监控节点通过所述列表中的ID识别在节点网络中需要获取的交易；

[0016] 进一步的，在节点网络中广播的交易类型包括数据上传、数据访问请求、数据访问授权、数据访问确认，所述数据上传是在客户端设备往链外存储器上传共享数据后在节点网络中广播的交易，所述数据访问请求是接收到数据上传交易的任意第三方客户端向数据所有者客户端申请访问数据的交易，所述数据访问授权是数据所有者客户端在接收到数据访问请求后的答复交易，所述数据访问确认是由链外存储器在解密并提供数据后发起，由第三方客户端接收数据后进行签收的交易；

[0017] 进一步的，在节点网络中广播的交易类型还包括撤销数据授权，所述撤销数据授权由数据所有者客户端发起，链外存储器接收的交易，当链外存储其接收撤销数据授权后，对应的第三方客户端将无法从所述链外存储器中获取到撤销授权的部分数据；

[0018] 进一步的，所述链外存储器在接收到哈希值序列时，根据所述哈希值序列确定初步检索地址范围[a%,b%]：

[0019] $$a\% = H'_{i-1}\%$$ ；

[0020] $$b\% = H_i\% = H'_{i-1}\% + (1 - H'_{i-1}\%) \bullet \frac{i}{2n}$$ ；

[0021] 特别的，$H_0$'%=0，其中，$H_i$'%表示已经搜索到的哈希值$H_i$的对应地址在整个申请数据中的百分比位置，$H_i$%表示预估的哈希值$H_i$的对应地址在整个申请数据中的百分比位置；

[0022] 在初步检索地址范围内[a%,b%]采用首尾交替方式检索，若未在[a%,b%]范围内检索到对应的地址，继续在[b%,100%]范围内采用按序检索。

[0023] 本发明所取得的有益效果是：

[0024] 本系统中的区块链用于记录数据上传、数据访问请求、数据访问授权、数据访问确认、数据更新操作的证据，保证共享数据的完整性和真实性，以及操作的可追溯性和可审计性，此外，对数据的操作记录也可用于评估某一方的行为，以建立信任，由于区块链中只记录了数据的哈希值，而不是真实的共享数据，因此与链上数据共享解决方案相比，可以保证良好的可扩展性，本系统中的访问控制器能够实现以段落为基础单位的颗粒度授权，实现授权数据的高度灵活性。

## 附图说明

[0025] 从以下结合附图的描述可以进一步理解本发明。图中的部件不一定按比例绘制，

而是将重点放在示出实施例的原理上。在不同的视图中，相同的附图标记指定对应的部分。

[0026] 图1为整体结构框架示意图；

[0027] 图2为交易处理流程示意图；

[0028] 图3为交易数据内容示意图；

[0029] 图4为访问控制器的控制包内容示意图；

[0030] 图5为数据段地址检索示意图。

## 具体实施方式

[0031] 为了使得本发明的目的、技术方案及优点更加清楚明白，以下结合其实施例，对本发明进行进一步详细说明；应当理解，此处所描述的具体实施例仅用于解释本发明，并不用于限定本发明。对于本领域技术人员而言，在查阅以下详细描述之后，本实施例的其它系统、方法和/或特征将变得显而易见。旨在所有此类附加的系统、方法、特征和优点都包括在本说明书内，包括在本发明的范围内，并且受所附权利要求书的保护。在以下详细描述描述了所公开的实施例的另外的特征，并且这些特征根据以下将详细描述将是显而易见的。

[0032] 本发明实施例的附图中相同或相似的标号对应相同或相似的部件；在本发明的描述中，需要理解的是，若有术语“上”、“下”、“左”、“右”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或组件必须具有特定的方位，以特定的方位构造和操作，因此附图中描述位置关系的用语仅用于示例性说明，不能理解为对本专利的限制，对于本领域的普通技术人员而言，可以根据具体情况理解上述术语的具体含义。

[0033] 实施例一。

[0034] 本实施例提供了一种基于区块链的可信数据颗粒化共享系统，包括客户端设备、区块链节点和链外存储器，所述链外存储器用于保存需要共享的数据，所述区块链节点用于广播和记录对共享数据的操作，所述客户端设备用于接入区块链节点并对数据进行本地处理；

[0035] 所述区块链节点包括广播和监控节点、挖掘节点和仅监控节点，所述广播和监控节点用于连接客户端设备和链外存储器，并对客户端设备和/或链外存储器上传的交易进行广播及监控，所述挖掘节点对完成的交易进行挖掘生成块并将块记录在区块链中，所述仅监控节点对节点网络中广播的交易进行监控；

[0036] 所述客户端设备包括访问控制器、加密组件、上传组件和连接组件，所述访问控制器对申请访问数据的交易进行处理，所述加密组件对上传的共享数据进行加密处理，所述上传组件与所述链外存储器连接并将加密后的数据上传到所述链外存储器，所述连接组件与所述广播和监控节点连接用于传递交易；

[0037] 所述访问控制器能够对被申请访问的数据内容进行颗粒度批准及撤销，所述访问控制器获取到保存在链外存储器中的部分数据的首尾地址，并分别将首尾地址处理得到哈希值$H_1$和$H_2$，若有n段数据，则按顺序处理得到哈希值序列$\{H_1、H_2、...、H_{2n}\}$；

[0038] 这些哈希值的获取公式为：

[0039] $H_1=Hash(Ad||ID)$；

[0040] $H_i=Hash(Ad||ID||H_{i-1})$，$1<i<=2n$；

[0041] 其中，Ad为数据段的首地址或尾地址，ID为申请方的用户ID；

[0042] 当含有所述哈希值序列的交易被广播并被链外存储器获取后，所述链外存储器根据所述哈希值序列批准或撤销部分数据的授权；

[0043] 所述广播和监控节点保存有与其连接的客户端或链外存储器的ID并构成维护列表，所述所述广播和监控节点通过所述列表中的ID识别在节点网络中需要获取的交易；

[0044] 在节点网络中广播的交易类型包括数据上传、数据访问请求、数据访问授权、数据访问确认，所述数据上传是在客户端设备往链外存储器上传共享数据后在节点网络中广播的交易，所述数据访问请求是接收到数据上传交易的任意第三方客户端向数据所有者客户端申请访问数据的交易，所述数据访问授权是数据所有者客户端在接收到数据访问请求后的答复交易，所述数据访问确认是由链外存储器在解密并提供数据后发起，由第三方客户端接收数据后进行签收的交易；

[0045] 在节点网络中广播的交易类型还包括撤销数据授权，所述撤销数据授权由数据所有者客户端发起，链外存储器接收的交易，当链外存储其接收撤销数据授权后，对应的第三方客户端将无法从所述链外存储器中获取到撤销授权的部分数据；

[0046] 所述链外存储器在接收到哈希值序列时，根据所述哈希值序列确定初步检索地址范围[a%,b%]：

[0047] $$a\% = H'_{i-1}\% ;$$

[0048] $$b\% = H_i\% = H'_{i-1}\% + (1 - H'_{i-1}\%) \bullet \frac{i}{2n} ;$$

[0049] 其中，$H_0'\%=0$，$H_i'\%$表示已经搜索到的哈希值$H_i$的对应地址在整个申请数据中的百分比位置，$H_i\%$表示预估的哈希值$H_i$的对应地址在整个申请数据中的百分比位置；

[0050] 在初步检索地址范围内[a%,b%]采用首尾交替方式检索，若未在[a%,b%]范围内检索到对应的地址，继续在[b%,100%]范围内采用按序检索。

[0051] 实施例二。

[0052] 本实施例包含实施例一的全部内容，本实施例的区块链节点包括多个广播和监控节点，所述广播和监控节点能够在区块链上生成和广播交易，这些节点能够接收区块链中广播的所有交易，进而监控交易的广播；

[0053] 参与共享数据的客户端以及链外存储器需要连接到其中一个广播和监控节点，如图1所示，公司A的客户端连接到广播和监控节点106A，公司B的客户端连接到广播和监控节点106B，公司C的客户端连接到广播和监控节点106C，链外存储器连接到广播和监控节点106D，每个广播和监控节点存储被允许经由其访问区块链的用户的标识符列表；

[0054] 一对客户端设备之间的每个数据传输事件由客户端设备和链外存储器作为中介，使得一个或多个数据交易消息经由它们与之通信的相应广播和监控节点被发布到区块链，所述数据交易消息不包括要在客户端设备之间共享的实际数据，实际数据由一个客户端设备上传到链外存储器并将数据上传交易发布到区块链，所述数据上传交易仅包含实际数据的散列，使得来自链外存储器的实际数据的下载者可以验证数据未被篡改；

[0055] 一旦数据被上传到链外存储器，系统中的其他客户端设备就可以请求访问它，例如，客户端设备104B访问客户端104A上传的数据具体包括下述流程：

[0056] S1、客户端设备104B向区块链发布数据访问请求交易；

[0057] S2、所述数据访问请求交易被广播和监控节点106A检测并传递到与客户端设备104A通信的访问控制器，如果访问被批准，所述客户端设备104A向区块链发布数据访问授权交易；

[0058] S3、所述数据访问授权交易被与链外存储器连接的广播和检测节点106D检测到，所述链外存储器通过广播和监控节点106D生成数据访问确认交易并发布到区块链；

[0059] S4、所述数据访问确认交易被广播和监控节点106B检测到，客户端设备104B访问存储在链外存储器处的数据，并将完成的交易发布并记录在区块链中；

[0060] 所述区块链节点还包括一个或多个挖掘节点，所述挖掘节点能够通过收集在给定时间窗口内广播的一定数量的有效交易来生成块；

[0061] 所述区块链节点还包括一个或多个监控节点，所述监控节点能够监控区块链广播的区块和交易，但不能在区块链上生成和广播交易或区块，所述监控节点配置为允许通过资源有限的设备访问区块链，因此能够访问区块链的公司或个人能够通过轻量级设备访问链上数据，所述监控节点能够访问区块链并检测以该监控节点所连接到的设备为目标的交易；

[0062] 系统中的所有共享数据都被加密并保存在所述链外存储器中，部署在公司A、B中的访问控制器接收公司间访问请求并基于访问控制策略对保存在链外存储器中的加密数据执行访问控制；

[0063] 对共享数据的所有操作都记录在区块链中，区块链中可以记录四种不同的与数据传输事件相关的操作，如下详述，每种操作对应一种区块链交易：

[0064] 数据上传：共享数据的所有者首先使用基于属性的加密算法对数据进行加密。然后，部署在数据所有者系统中的客户端设备将加密数据上传到链外存储器，一旦数据所有者将数据上传到链外存储器中，其连接的广播和监控节点就生成数据上传交易并将其发布到区块链中，明文数据的哈希值包含在数据上传交易中，每次数据所有者更新存储的数据时，需要发布包含更新后的数据哈希的相应数据上传交易，这确保了数据所有者无法在不被检测到的情况下篡改存储的数据；

[0065] 数据访问请求：部署在拥有数据的公司中的访问控制器对保存在链外存储器中的加密数据执行访问控制，一旦一家公司需要另一家公司的数据，通过其连接的广播和监控节点在区块链上生成和发布数据访问请求交易，然后，连接到数据所有者公司的广播和监控节点将接收数据访问请求交易并将访问请求发送到数据所有者的访问控制器，访问控制器基于访问控制策略决定是批准还是拒绝该请求；

[0066] 数据访问授权：如果数据访问请求被批准，访问控制器为请求公司生成代理密钥，代理密钥被加密并发送到与数据所有者连接的广播和监控节点，所述广播和监控节点生成包含加密代理密钥的数据访问授权交易并将该交易发布到区块链中，代理密钥可以由链外存储器和数据所有者之间的共享密钥加密，或者由链外存储器的公钥加密，在使用链外存储器的公钥加密代理密钥的情况下，公钥可以是链外存储器的区块链交易公钥、链外存储器的云数据部分解密公钥，也可以是链外存储器中专用于代理密钥加密的密钥对；

[0067] 数据访问确认：在接收和解密代理密钥后，链外存储器使用代理密钥和链外存储器的私钥对加密数据进行部分解密，作为由链外存储器执行的解密的结果，将生成中间数

据，授权数据请求者通过用其私钥解密中间数据来获得数据的明文，生成中间数据后，连接到链外存储器的广播和监控节点生成需要数据请求者签名的数据访问确认交易，并将该交易发布到区块链，在解密中间数据时，数据请求者签署数据访问确认交易；

[0068] 结合图3，交易数据的字段可以包括以下内容：

[0069] 交易ID：第一个字段是交易的标识符，所述交易ID可以是通过散列交易信息生成的交易散列ID；

[0070] 发送者的先前交易ID：第二个字段是指向发送方先前交易的指针，该子字段的功能是将发送者创建的所有交易链接在一起，链式记录可用于审计和跟踪发送者的行为；

[0071] 发送者的公钥：这个子字段包含发送者的公钥，可以用来验证下一个子字段发送者的签名，交易的发送方是发起交易的一方；

[0072] 发送者签名：该子字段是发送方在交易上的签名，用于保证交易的完整性和真实性，每个发送方生成自己的公私钥对，公钥记录在前一个子字段发送方的公钥中，发送方使用私钥交易生成签名；

[0073] 元数据：该子字段包含与交易对应的操作特定信息，所述元数据包含四个字段：数据标识符、交易类型、接收方的用户ID和操作信息；

[0074] 数据标识符是对与交易相关的数据的引用；

[0075] 交易类型表示与交易相关的操作类型，所述交易类型取以下值之一：数据上传、数据访问请求、数据访问授权、数据访问确认；

[0076] 接收方的用户ID：每个客户端设备和链外存储器具有其自己的用户ID作为唯一身份，该用户ID在该方加入系统后立即被其他方广播和记录，每个广播和监控节点维护一个列表，该列表记录其连接的客户端设备或链外存储器的用户ID，一旦交易广播到整个区块链网络，每个广播和监控节点都会检查接收到的交易中接收方的用户ID，如果广播和监控节点将接收方与连接的客户端设备或链外存储器匹配，则广播和监控节点将交易转发给接收方以进行进一步处理；

[0077] 操作信息是与该交易相关联的操作相关的信息；

[0078] 接收者的公钥：这个子字段包含了接收者的公钥，用于验证下一个子字段接收者的签名，交易的接收者是交易的发送方需要与之通信的一方；

[0079] 接收方签名：该子字段是接收方在交易上的签名，用于保证交易的完整性和真实性，接收方使用公私钥对在交易上生成签名，公钥记录在前一个子字段接收方的公钥中；

[0080] 输出：该子字段由交易的接收者填充，指示与该交易相关的数据上传/访问操作的结果；

[0081] 结合图2，下面以数据上传交易为例对处理交易的流程进行说明，具体包括如下步骤：

[0082] S201、发送者发起交易，并且这可以包括执行一个或多个链外操作；

[0083] 在数据上传交易中，发送者是上传数据对象的客户端设备，而接收者是数据对象将被上传到的链外存储器，客户端设备中的加密组件对数据对象进行加密，上传组件将加密的数据对象上传到链外存储器，数据对象的数据标识符此时也由发送方生成；

[0084] S202、发送者签署交易；

[0085] S203、发送者可以将交易发送到它所连接的广播和监控节点，在数据上传交易操

作中，发送者的客户端设备签署数据上传交易并将其传输到与其连接的广播和监控节点，数据上传交易包括图3所示的字段，交易类型是“数据上传交易”，操作信息包括数据对象的散列，需要注意的是，交易不包括数据对象本身，而仅包括数据对象的哈希值；

[0086] S204、与发送者客户端设备连接的广播和监控节点向网络广播交易；

[0087] S205、与接收者连接的广播和监控节点根据交易元数据中的接收者的用户ID检测到存在针对接收者的交易，在数据上传交易中，接受者为链外存储器；

[0088] S206、连接到链外存储器的广播和监控节点将交易转发给链外存储器；

[0089] S207、链外存储器基于交易的内容采取行动，具体地，基于从数据所有者上传加密数据的结果，链外存储器填充交易的输出，对于数据上传交易，输出可以包括上传标签和时间戳，上传标签表示数据上传操作的结果，如果加密数据已成功上传到云端，则链外存储器将标签值设置为1，否则，如果上传不成功，标签值设置为0，时间戳用于记录链外存储器签署交易的时间；

[0090] S208、链外存储器在输出上签名；

[0091] S209、链外存储器将完成的交易发送到与其连接的广播和监控节点；

[0092] S210、其链外存储器连接的广播和监控节点广播要记录在区块链中完成的交易；

[0093] S211、交易被验证并添加到区块链；

[0094] 所述访问控制器能够对被申请访问的数据内容进行颗粒度批准及撤销，所述访问控制器获取到保存在链外存储器中的部分数据的首尾地址，并分别将首尾地址处理得到哈希值$H_1$和$H_2$，若有n段数据，则按顺序处理得到哈希值$H_1$、$H_2$、...、$H_{2n}$；

[0095] 这些哈希值的获取公式为：

[0096] $H_1=Hash(Ad||ID)$；

[0097] $H_i=Hash(Ad||ID||H_{i-1})$，$1<i<=2n$；

[0098] 其中，Ad为数据段的首地址或为地址，ID为申请方的用户ID；

[0099] 需要注意的是，当i为奇数时，对应的Ad为数据段首地址，当i为偶数时，对应的Ad为数据段尾地址；

[0100] 所述访问控制器生成的控制包包括三个字段，结合图4，第一字段为授权类型，值为0,1或2，当值为0时，表示不允许访问，当值为1时，表示允许全部访问，当值为2时，表示允许部分访问，且第二字段或第三字段填充上述过程得到的哈希值序列；

[0101] 当第三方申请访问时，将部分允许访问的数据的哈希值序列填充进第二字段；

[0102] 当需要主动撤销第三方的部分访问权时，将需要禁止访问的数据的哈希值序列填充进第三字段；

[0103] 所述链外存储器在接收到哈希值序列时，根据所述哈希值序列确定初步检索地址范围[a%,b%]：

[0104] $$a\% = H'_{i-1}\%;$$

[0105] $$b\% = H_i\% = H'_{i-1}\% + (1 - H'_{i-1}\%) \bullet \frac{i}{2n};$$

[0106] 特别的，$H_0'\%=0$，其中，$H_i'\%$表示实际搜索到的哈希值$H_i$的对应地址在整个申请数据中的百分比位置，$H_i\%$表示预估的哈希值$H_i$的对应地址在整个申请数据中的百分比位置；

[0107] 在初步检索地址范围内[a%,b%]采用首尾交替方式检索,若未在[a%,b%]范围内检索到对应的地址,继续在[b%,100%]范围内采用按序检索;

[0108] 结合图5,链外存储器先计算得到$H_1\%$,在[0%,$H_1\%$]内交替检索地址并成功检索到$H_1'\%$,计算得到$H_2\%$,在[$H_1'\%$,$H_2\%$]交替检索地址并成功检索到$H_2'\%$,计算得到$H_3\%$,在[$H_2'\%$,$H_3\%$]内未检索到地址,在[$H_3\%$,100%]内按序检索到$H_3'\%$,计算得到$H_4\%$,在[$H_3'\%$,$H_4\%$]内交替检索到$H_4'\%$,[$H_1'\%$,$H_2'\%$]和[$H_3'\%$,$H_4'\%$]这两段数据为需要批准或撤销的数据段。

[0109] 虽然上面已经参考各种实施例描述了本发明,但是应当理解,在不脱离本发明的范围的情况下,可以进行许多改变和修改。也就是说上面讨论的方法,系统和设备是示例。各种配置可以适当地省略,替换或添加各种过程或组件。例如,在替代配置中,可以以与所描述的顺序不同的顺序执行方法,和/或可以添加,省略和/或组合各种部件。而且,关于某些配置描述的特征可以以各种其他配置组合,如可以以类似的方式组合配置的不同方面和元素。此外,随着技术发展其中的元素可以更新,即许多元素是示例,并不限制本公开或权利要求的范围。

[0110] 在说明书中给出了具体细节以提供对包括实现的示例性配置的透彻理解。然而,可以在没有这些具体细节的情况下实践配置例如,已经示出了众所周知的电路,过程,算法,结构和技术而没有不必要的细节,以避免模糊配置。该描述仅提供示例配置,并且不限制权利要求的范围,适用性或配置。相反,前面对配置的描述将为本领域技术人员提供用于实现所描述的技术的使能描述。在不脱离本公开的精神或范围的情况下,可以对元件的功能和布置进行各种改变。

[0111] 综上,其旨在上述详细描述被认为是例示性的而非限制性的,并且应当理解,以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后,技术人员可以对本发明作各种改动或修改,这些等效变化和修饰同样落入本发明权利要求所限定的范围。

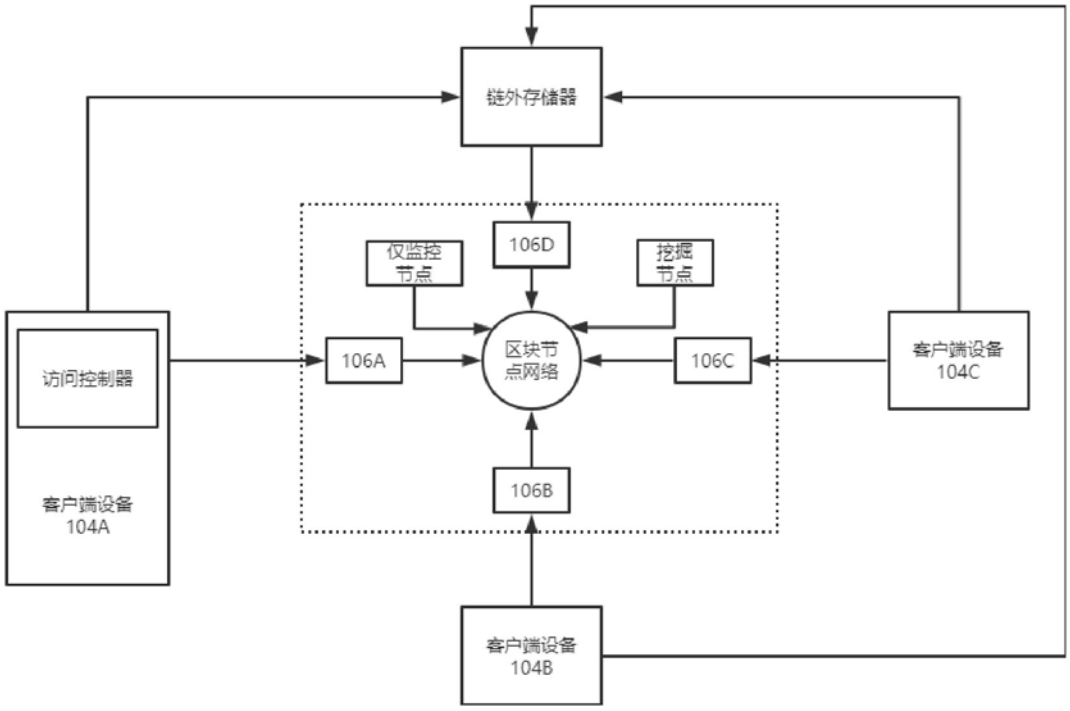

链外存储器
仅监控节点
106D
挖掘节点
访问控制器
106A
区块节点网络
106C
客户端设备104C
客户端设备104A
106B
客户端设备104B

图1

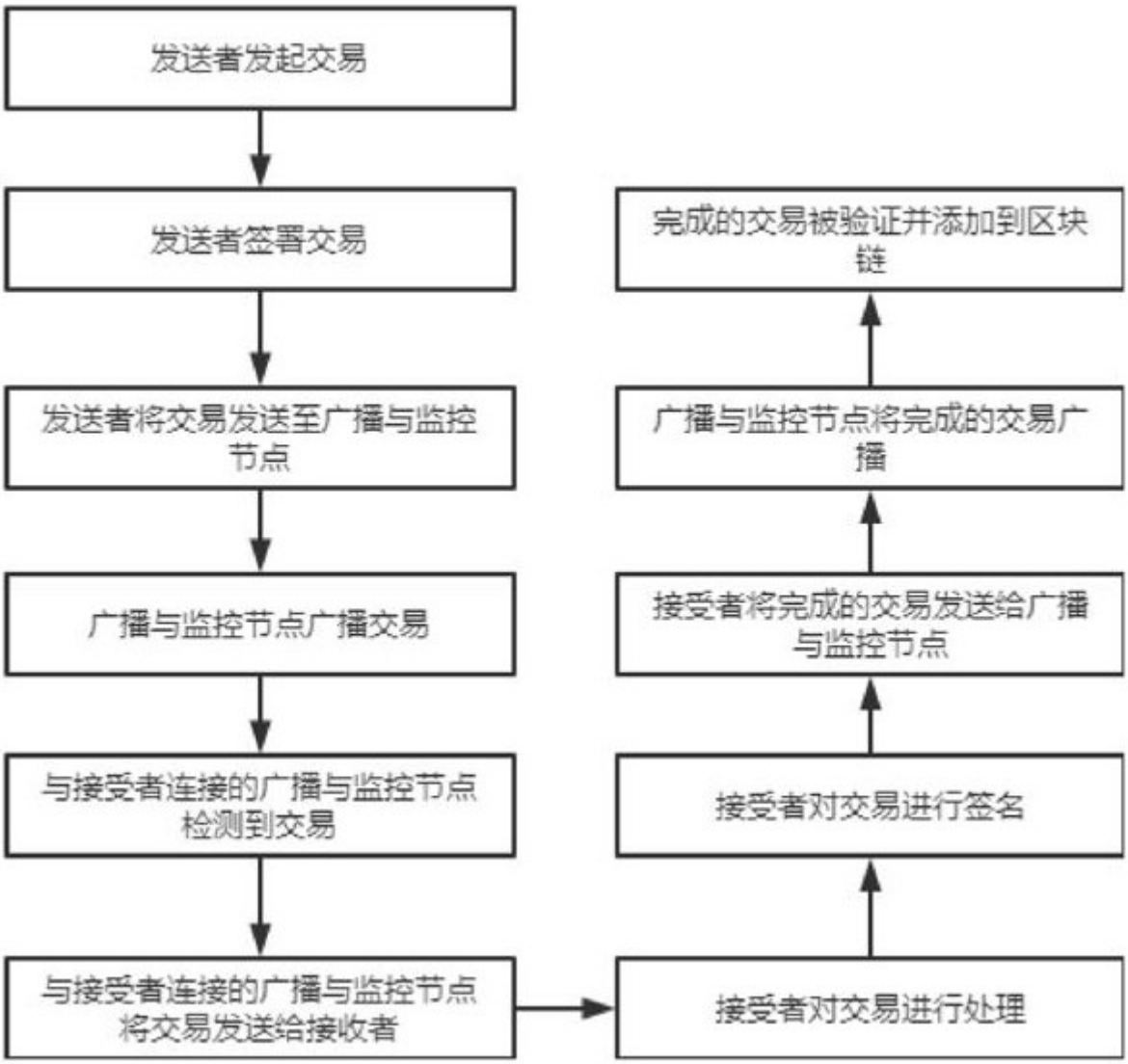

发送者发起交易
发送者签署交易
发送者将交易发送至广播与监控节点
广播与监控节点广播交易
与接受者连接的广播与监控节点检测到交易
与接受者连接的广播与监控节点将交易发送给接收者
接受者对交易进行处理
接受者对交易进行签名
接受者将完成的交易发送给广播与监控节点
广播与监控节点将完成的交易广播
完成的交易被验证并添加到区块链

图2

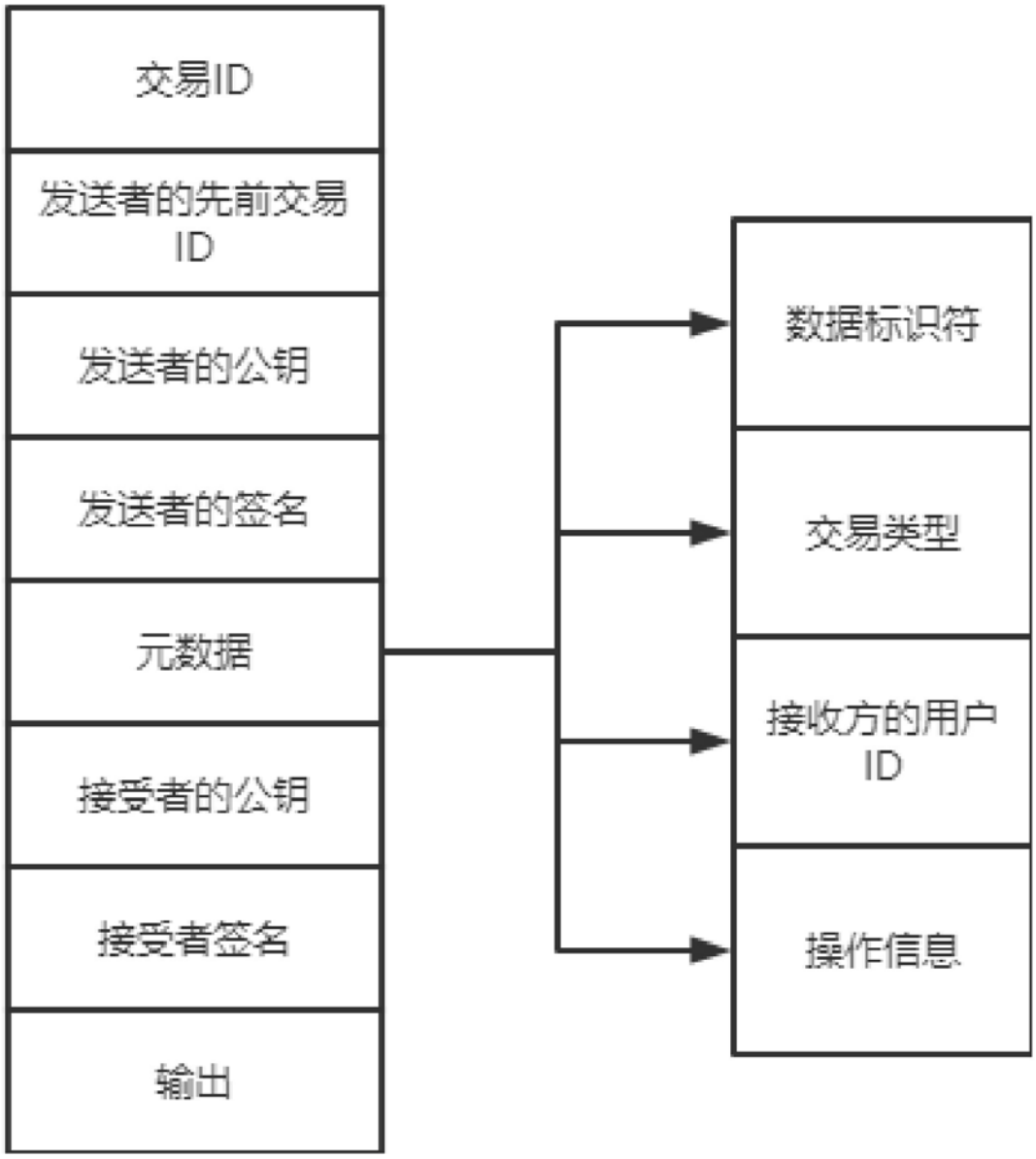

交易ID
发送者的先前交易ID
发送者的公钥
发送者的签名
元数据
接受者的公钥
接受者签名
输出
数据标识符
交易类型
接收方的用户ID
操作信息

图3


图4

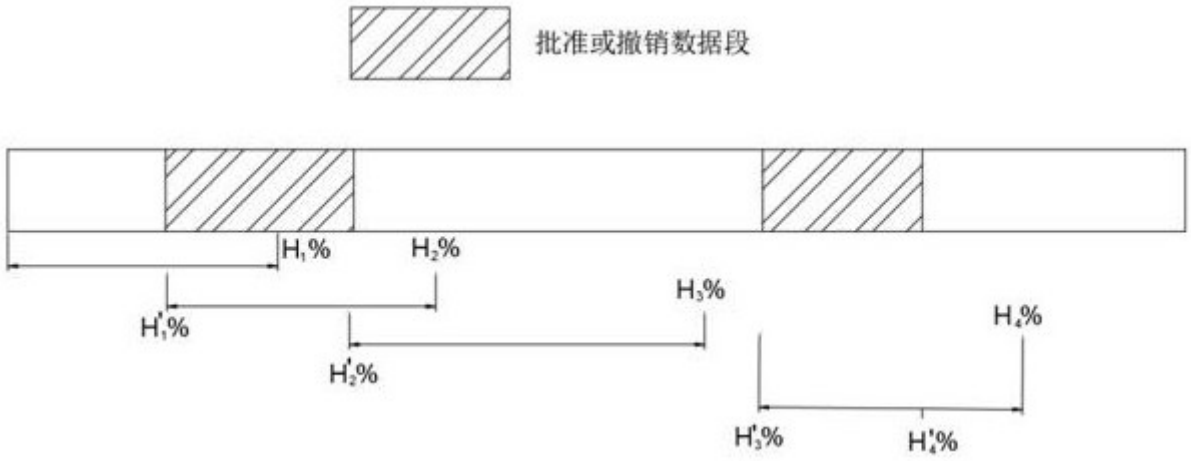



图5