区块链安全存储方法

申请号：201610823105.6
申请日：2016-09-13

申请(专利权)人　中国电子科技集团公司第三十二研究所
地址　200233 上海市嘉定区嘉罗路1485号
发明(设计)人　刘银平　李龙　姚洪　何杰

主分类号　G06F21/62(2013.01)I
分类号　G06F21/62(2013.01)I　G06F17/30(2006.01)I
公开(公告)号　106503574A
公开(公告)日　2017-03-15
专利代理机构　上海汉声知识产权代理有限公司 31236
代理人　郭国中

(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 106503574 A
(43)申请公布日 2017.03.15

(21)申请号 201610823105.6

(22)申请日 2016.09.13

(71)申请人 中国电子科技集团公司第三十二研究所
地址 200233 上海市嘉定区嘉罗路1485号

(72)发明人 刘银平 李龙 姚洪 何杰

(74)专利代理机构 上海汉声知识产权代理有限公司 31236
代理人 郭国中

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 17/30(2006.01)

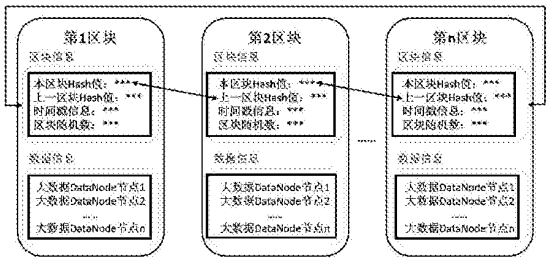
权利要求书1页 说明书5页 附图1页

(54)发明名称

区块链安全存储方法

(57)摘要

本发明提供了一种区块链安全存储方法，令每一个客户端Client都具有名称节点NameNode，大大提高了大数据平台存储数据的安全性，通过去中心化的设计有效避免了集中化服务器带来的压力，将中心服务器的功能，通过整个私有区块链网络进行共同分摊；并对Hadoop的每一个数据块的DataNode，进行加密，充分保障了大数据中每一个数据的安全性；还改进了大数据平台存储与管理数据的机制，从依托于中心节点的单一方式，转化成由所有参与者共同维护的网络环境，真正实现了去中心设计。通过PKI和用户权限的设定，突破了对重要数据简单粗放明文存储的弊端，深化安全加密存储的流程和方法。



CN 106503574 A

1.一种区块链安全存储方法,其特征在于,包括:

令每一个客户端Client都具有名称节点NameNode,其中,所述名称节点NameNode用于写入数据到区块链中的数据节点DataNode的数据块Block中。

2.根据权利要求1所述的区块链安全存储方法,其特征在于,包括:

当客户端Client提交写入数据的请求时,由区块链中所有区块的节点竞争获得将待写入数据写入到新的数据块的写入权限,得到具有写入权限的区块节点,该具有写入权限的区块节点通过密钥管理中心生成公钥和私钥,公钥用于加密待写入的数据块,私钥有具有写入权限的区块节点自己保存。

3.根据权利要求2所述的区块链安全存储方法,其特征在于,包括:

当该具有写入权限的区块节点自身需要读取本节点的数据块时,使用自己的私钥直接解密获得明文数据;当其他节点需要读取该具有写入权限的区块节点的数据时,由该具有写入权限的区块节点通过私钥对数据块进行解密后,使用其他节点的公钥进行加密后发送给其他节点。

4.根据权利要求1所述的区块链安全存储方法,其特征在于,包括:

客户端的名称节点NameNode获取到向数据节点DataNode写入数据的权限后,通过非对称加密算法,对每一个写入数据节点DataNode的数据块Block结合发起写入数据块Block的节点的公钥进行加密;对于客户端读取数据节点DataNode的数据时,通过与加密时生成的公钥的对应私钥进行解密,实现数据块Block中区链块数据的获取操作。

5.根据权利要求1所述的区块链安全存储方法,其特征在于,包括:

将多个密钥管理中心,分别设置在异地,形成分布式密钥管理中心;分布式密钥管理中心用于管理和生成公私密钥对,根据每一个客户端对公私钥的密钥对进行管理,公私钥与用户端进行匹配。

6.根据权利要求1所述的区块链安全存储方法,其特征在于,包括:

建立分布式的用户管理中心;分布式的用户管理中心用于对客户端的权限和属性进行管理,管理区块链节点上的客户端,按照客户端分配对应的公私钥,当客户端获取不同节点上区块数据信息时,先检查对应区块的客户端的权限,得到认可后由所在区块链的节点,辨识每一个原始写入数据的客户端,从而发起向原始写入加密数据的客户端,咨询获取加密数据的环节。

7.根据权利要求1所述的区块链安全存储方法,其特征在于,包括:

令客户端Client在写入数据的时候打开Hadoop分布式文件系统HDFS,通过名称节点NameNode创建文件或打开已存在文件,将文件写入数据节点DataNode的数据块Block中,并进行确认字符ACK包确认,在确认成功后关闭Hadoop分布式文件系统HDFS,客户端Client通知名称节点NameNode完成了对数据块Block的写入保存;若确认未成功则提示确认失败。

8.根据权利要求2所述的区块链安全存储方法,其特征在于,包括:

每一个客户端的名称节点NameNode通过网络同步机制,在网络中计算Hash值进行竞争获得写入新的数据块Block的权限。

区块链安全存储方法

技术领域

[0001] 本发明涉及云计算、大数据领域，具体地，涉及区块链技术与大数据安全存储的区块链安全存储方法。

背景技术

[0002] 现有Hadoop大数据中的技术方案，都是基于HDFS分布式文件系统存储数据，中心节点都是集中NameNode等几台服务器上，中心节点的控制严格限制了数据的安全性；具体每一个数据块的DataNode的存储，没有进行加密处理；传统的存储方案流程简易，只侧重数据的存储，没有充分考虑数据的安全性。

[0003] 经检索，发现如下相关检索结果：

[0004] 相关检索结果1：

[0005] 申请(专利)号：201510955506.2；名称：一种区块链溯源追踪方法

[0006] 该专利文献涉及互联网上的溯源追踪方法，提供一种区块链溯源追踪方法，所述方法包括如下步骤：区块链系统收到某一待溯源追踪的区块链地址后，从当前区块开始，按照区块产生的次序遍历整个区块链；所述区块链系统根据遍历结果，构建所述待溯源追踪的区块链地址的收入生成树和支出生成树，获得该待溯源追踪的区块链地址的资产转移历史记录。该专利文献称将有助于追踪区块链系统的非法使用行为及非法使用者，避免区块链系统成为被不法分子利用的工具，为区块链技术的更广泛应用提供基础，主要应用可用于审计功能。

[0007] 技术要点比较：

[0008] 1.区块链追踪技术：该专利文献主要是通过将待追踪的区块链地址收入生成树和支出生成树。本发明主要是通过用户进行匹配查询。

[0009] 2.用户管理中心技术：本发明通过设计用户管理中心，首先管理每个节点用户，其次深入详尽的管理每个用户对应的公私钥。该专利文献没有考虑到这个方法。

[0010] 相关检索结果2：

[0011] 申请(专利)号：201610100747.3；名称：区块链的打包存储方法

[0012] 该专利文献提供一种区块链的打包存储方法，一个公钥地址有多笔支出时，必须依次验证余额是否足够，这里将支出地址按地址的区间分类，可用不同的线程或进程来分别校验交易，可确保同一支出地址不超过余额，每个地址区间收款增加的余额再传送到相应的地址区间所在的服务器，再一次统计最后的余额。存储数据时，为克服写盘速度的限制，可循环依次向多台服务器写盘，可以将区块链区块高度和服务器的个数做除法取模映射，或将区块高度与服务器的对应关系作为元数据，交给专门的元数据服务器来管理，访问数据时，首先访问元数据服务器，获得区块高度对应的服务器，设置每次写盘的数据量，可以使每次写盘结束的时刻不大于下次轮到写盘的时刻。

[0013] 技术要点比较：

[0014] 1.合并数据包写入账单：该专利文献侧重于对多个区块链账单数据进行合并写

入，使用多线程并发。本发明侧重区块链技术和大数据技术结合，达到去中心化，以及安全加密存储的目的。

[0015] 2.增量数据写入Map和Reduce过程：该专利文献重点的出发点主要在于通过计算区块高度做除法取模映射去写入数据。而本发明主要是通过利用Map和Reduce的映射机制，将同样数据进行提取，减少写入相同数据。

[0016] 相关检索结果3：

[0017] 现有技术文献：名称《区块链：新经济蓝图及导读》，出版自新星出版社，ISBN：9787513319720。

[0018] 技术要点比较：

[0019] 1.大数据存储技术：该现有技术文献中没有详细描述大数据技术在区块链设计思想中如果体现和运用。

[0020] 2.密钥管理中心设计技术：该现有技术文献中主要的案例背景，是以区块链技术与电子货币的管理，以及区块链技术与市场、经济、货币的结合应用，没有深入讲解区块链技术中加密方案、密钥管理中心如何设计等技术方案。

发明内容

[0021] 针对现有技术中的缺陷，本发明的目的是提供一种区块链安全存储方法。本发明主要解决的技术问题体现在如下任一点：

[0022] 1)解决大数据Hadoop通过中心节点控制的数据存储方案，避免了因个别单位数据中心的崩溃，而影响整体业务的继续进行，发明去中心化的存储方案，代替使用Hadoop的基于中心节点NameNode进行统一控制；

[0023] 2)大数据平台由于融合了海量各类敏感数据信息，数据存储通过Map和Reduce进行切块存储而且是明文存储，数据的内在安全不能进行安全保护和脱敏，使用本发明对每一DataNode数据块，进行基于PKI的非对称算法，主要使用SHA256加密算法，对每一块数据块进行加密脱敏后存储，保证了只有拥有私钥的本人，才能有获取数据内容的权限；

[0024] 3)通过对区块链技术和大数据技术深度理解，本发明在大数据领域，实现基于区块链技术的去中心话的存储方案，改进传统数据存储，大数据存储的流程和设计思路，充分考虑到数据存储的安全性。

[0025] 根据本发明提供的一种区块链安全存储方法，包括：

[0026] 令每一个客户端Client都具有名称节点NameNode，其中，所述名称节点NameNode用于写入数据到区块链中的数据节点DataNode的数据块Block中。

[0027] 优选地，包括：

[0028] 当客户端Client提交写入数据的请求时，由区块链中所有区块的节点竞争获得将待写入数据写入到新的数据块的写入权限，得到具有写入权限的区块节点，该具有写入权限的区块节点通过密钥管理中心生成公钥和私钥，公钥用于加密待写入的数据块，私钥有具有写入权限的区块节点自己保存。

[0029] 优选地，包括：

[0030] 当该具有写入权限的区块节点自身需要读取本节点的数据块时，使用自己的私钥直接解密获得明文数据；当其他节点需要读取该具有写入权限的区块节点的数据时，由该

具有写入权限的区块节点通过私钥对数据块进行解密后，使用其他节点的公钥进行加密后发送给其他节点。

[0031] 优选地，包括：

[0032] 客户端的名称节点NameNode获取到向数据节点DataNode写入数据的权限后，通过非对称加密算法，对每一个写入数据节点DataNode的数据块Block结合发起写入数据块Block的节点的公钥进行加密；对于客户端读取数据节点DataNode的数据时，通过与加密时生成的公钥的对应私钥进行解密，实现数据块Block中区链块数据的获取操作。

[0033] 优选地，包括：

[0034] 将多个密钥管理中心，分别设置在异地，形成分布式密钥管理中心；分布式密钥管理中心用于管理和生成公私密钥对，根据每一个客户端对公私钥的密钥对进行管理，公私钥与用户端进行匹配。

[0035] 优选地，包括：

[0036] 建立分布式的用户管理中心；分布式的用户管理中心用于对客户端的权限和属性进行管理，管理区块链节点上的客户端，按照客户端分配对应的公私钥，当客户端获取不同节点上区块数据信息时，先检查对应区块的客户端的权限，得到认可后由所在区块链的节点，辨识每一个原始写入数据的客户端，从而发起向原始写入加密数据的客户端，咨询获取加密数据的环节。

[0037] 优选地，包括：

[0038] 令客户端Client在写入数据的时候打开Hadoop分布式文件系统HDFS，通过名称节点NameNode创建文件或打开已存在文件，将文件写入数据节点DataNode的数据块Block中，并进行确认字符ACK包确认，在确认成功后关闭Hadoop分布式文件系统HDFS，客户端Client通知名称节点NameNode完成了对数据块Block的写入保存；若确认未成功则提示确认失败。

[0039] 优选地，包括：

[0040] 每一个客户端的名称节点NameNode通过网络同步机制，在网络中计算Hash值进行竞争获得写入新的数据块Block的权限。

[0041] 与现有技术相比，本发明具有如下的有益效果：

[0042] 1、大大提高了大数据平台存储数据的安全性，通过去中心化的设计有效避免了集中化服务器带来的压力，将中心服务器的功能，通过整个私有区块链网络进行共同分摊。

[0043] 2、对Hadoop的每一个数据块的DataNode，进行基于SHA256安全哈希散列算法加密，使用基于PKI机制非对称加密方案，充分保障了大数据中每一个数据的安全性。

[0044] 3、改进了大数据平台存储与管理数据的机制，从依托于中心节点的单一方式，转化成由所有参与者共同维护的网络环境，真正实现了去中心设计。通过PKI和用户权限的设定，突破了对重要数据简单粗放明文存储的弊端，深化安全加密存储的流程和方法。

附图说明

[0045] 通过阅读参照以下附图对非限制性实施例所作的详细描述，本发明的其它特征、目的和优点将会变得更明显：

[0046] 图1为去中心化的大数据区块链存储方法图。

[0047] 图2为大数据存储节点的区块安全加密存储方法图。

具体实施方式

[0048] 下面结合具体实施例对本发明进行详细说明。以下实施例将有助于本领域的技术人员进一步理解本发明，但不以任何形式限制本发明。应当指出的是，对本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变化和改进。这些都属于本发明的保护范围。

[0049] 根据本发明提供的区块链安全存储方法，包括：

[0050] 基于区块链技术的去中心化存储方法，每一个客户端使用一个独立的程序，例如以比特币为例，用户维护自己的钱包和交易记录。另外需要一个挖矿程序的终端，通过实时竞争计算获得10分钟的交易账单数据，生成一个区块，进行全网广播，之后再将这个区块按照Hash值，写入到区块链的链表中。

[0051] 大数据Hadoop通过HDFS分布式文件系统存储用户数据，客户端Client在写入数据的时候打开Hadoop分布式文件系统HDFS，通过NameNode创建文件或打开已存在文件，之后找到具体写入数据的DataNode节点，写入数据块Block，进行ACK包确认，确认成功后关闭HDFS，客户端最后通知NameNode完成了对数据块Block的写入保存。

[0052] 将大数据Hadoop大数据中心节点服务处理程序NameNode模块，进行程序改进，修改成基于区块链技术方案的客户端程序，达到去中心化的目的，从而每一个客户端都有一套NameNode处理程序。

[0053] 基于区块链技术的大数据NameNode客户端程序，在互联网的每一个客户节点上被平等对待，当写入数据时，每一个NameNode客户端节点通过网络同步机制，在网络中计算Hash值进行竞争获得写入新的DataNode的权利。

[0054] 客户端的NameNode节点汇聚向DataNode写入数据的权限后，通过PKI非对称加密算法SHA256(256位安全哈希散列算法)，对每一个写入DataNode的Block结合公钥进行加密，对于客户读取DataNode节点数据的时候，通过与加密时生成的公钥的对应私钥进行解密，实现Block区链块数据的获取操作。

[0055] 密钥管理中心，建立分布式密钥管理中心，管理和生成公私密钥对，配合NameNode在新增区块链的block时，用公钥进行加密。

[0056] 用户管理中心，管理区块链节点上的用户，按照用户分配对应的私钥，让用户在获取某一个区块的数据时，首先根据用户自身的权限拿到自己对应的私钥，用自己的私钥解密对应公钥加密的DataNode数据块。

[0057] 下面对本发明进行更为具体的说明。

[0058] 通过修改区块链技术的客户端网络节点实现代码，实现对大数据平台中依赖几个名称节点NameNode写入数据到数据节点DataNode的方式进行改进。NameNode与区块链技术每个节点进行整合，使得NameNode由中心化方式写入DataNode的数据块，改变成每一个客户端节点都具有NameNode去写区块链中的DataNode的数据块了，从而实现了去中心化的设计。

[0059] 写入数据块DataNode加密保护方法的实现。当客户端Client提交写入数据的请求时，由区块链中所有的区块节点服务程序竞争获得写入新的数据块的权利，获得写入权限的节点，通过PKI密钥管理中心生成公钥和私钥，公钥用于加密待写入的数据块，私钥自己

保存。当自身需要读取本节点的数据块时候，使用自己的私钥直接解密获得明文数据；当其他节点的用户需要读取本节点的数据时，由本节点通过私钥对数据块进行解密后，使用请求者的公钥进行加密，之后发送给请求者。

[0060] 客户端的NameNode节点基于区块链技术，获取到向DataNode写入数据的权限后，通过PKI非对称加密算法SHA256(256位安全哈希散列算法)，对每一个写入DataNode的Block结合发起写入数据块的节点公钥进行加密；对于客户读取DataNode节点数据的时候，通过与加密时生成的公钥的对应私钥进行解密，实现Block区链块数据的获取操作。

[0061] 密钥管理中心的实现，基于kerbos技术部署多套具有主从备份功能的密钥管理中心，为了密钥服务的质量和安全性，将多个密钥管理中心，设置在异地进行。建立成功后的分布式密钥管理中心，管理和生成公私密钥对，根据每一个用户节点对公私钥的密钥对进行管理，公私钥必须与具体的用户进行匹配。

[0062] 用户(客户端)管理中心实现，建立分布式的用户管理中心，对用户的权限和用户属性进行管理，管理区块链节点上的用户，按照用户分配对应的公私钥，当用户获取不同节点上区块数据信息时，必须先检查对应区块的用户权限，得到认可后由所在区块链的节点，辨识每一个原始写入数据的用户，从而发起向原始写入加密数据的用户，咨询获取加密数据的环节。

[0063] 以上对本发明的具体实施例进行了描述。需要理解的是，本发明并不局限于上述特定实施方式，本领域技术人员可以在权利要求的范围内做出各种变化或修改，这并不影响本发明的实质内容。在不冲突的情况下，本申请的实施例和实施例中的特征可以任意相互组合。

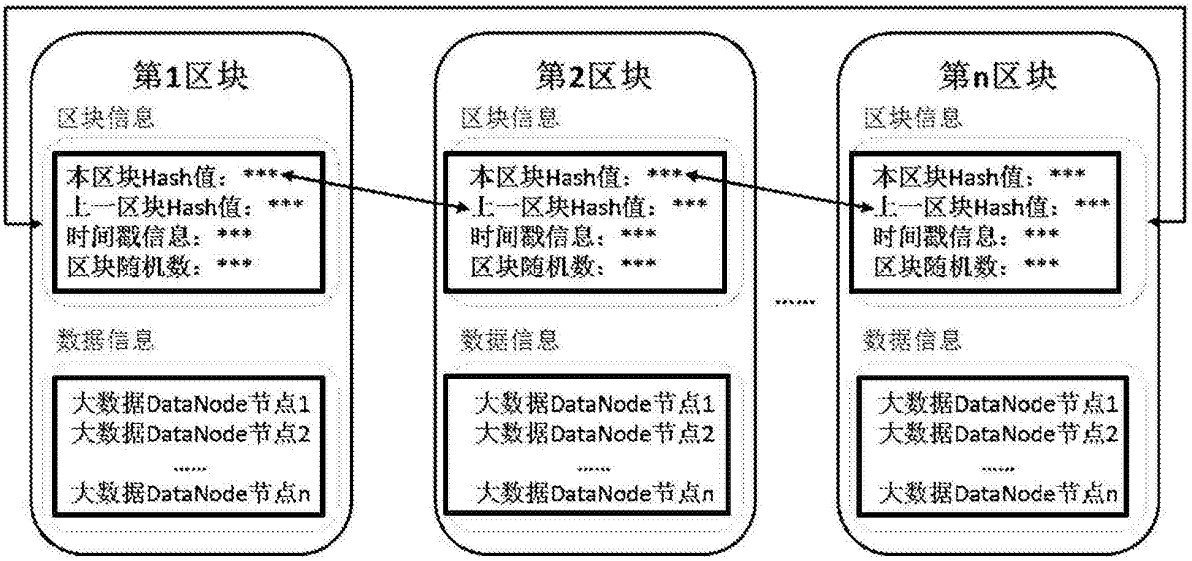

第1区块
区块信息
本区块Hash值：***
上一区块Hash值：***
时间戳信息：***
区块随机数：***
数据信息
大数据DataNode节点1
大数据DataNode节点2
.....
大数据DataNode节点n
第2区块
区块信息
本区块Hash值：***
上一区块Hash值：***
时间戳信息：***
区块随机数：***
数据信息
大数据DataNode节点1
大数据DataNode节点2
.....
大数据DataNode节点n
.....
第n区块
区块信息
本区块Hash值：***
上一区块Hash值：***
时间戳信息：***
区块随机数：***
数据信息
大数据DataNode节点1
大数据DataNode节点2
.....
大数据DataNode节点n

图1

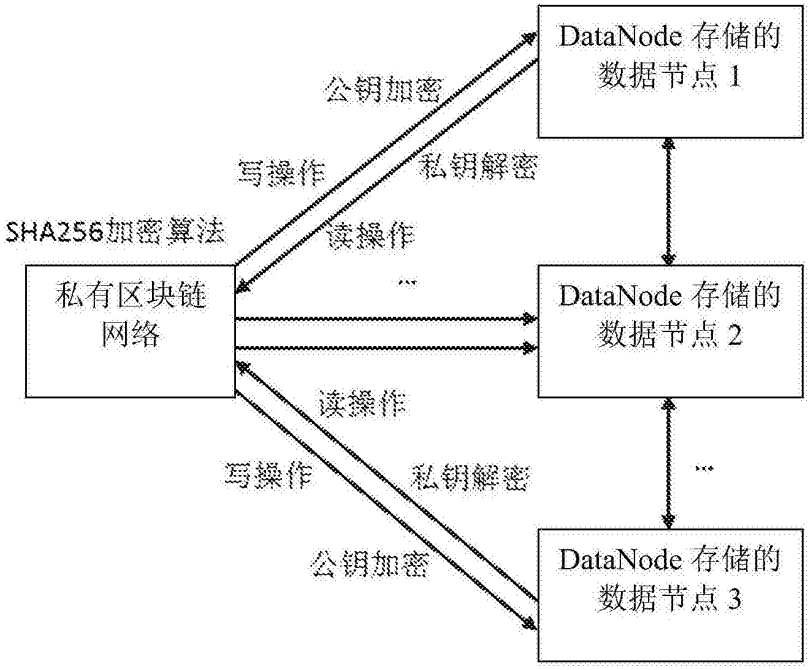

DataNode 存储的
数据节点 1
公钥加密
写操作
私钥解密
SHA256加密算法
读操作
...
私有区块链
网络
DataNode 存储的
数据节点 2
读操作
写操作
私钥解密
...
公钥加密
DataNode 存储的
数据节点 3

图2