基于区块链技术的内容存储方法

申请号：201610823156.9
申请日：2016-09-14

申请(专利权)人　中国银联股份有限公司
地址　200135 上海市浦东新区含笑路36号银联大厦
发明(设计)人　于镳

主分类号　G06F21/62(2013.01)I
分类号　G06F21/62(2013.01)I　G06F3/06(2006.01)I
公开(公告)号　106372533A
公开(公告)日　2017-02-01
专利代理机构　中国专利代理(香港)有限公司 72001
代理人　王星　付曼

(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 106372533 A
(43)申请公布日 2017.02.01

(21)申请号 201610823156.9

(22)申请日 2016.09.14

(71)申请人 中国银联股份有限公司
地址 200135 上海市浦东新区含笑路36号银联大厦

(72)发明人 于镳

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 王星 付曼

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 3/06(2006.01)

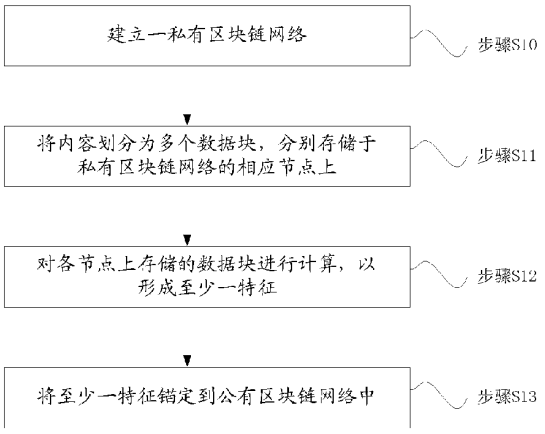
权利要求书1页 说明书4页 附图1页

(54)发明名称

基于区块链技术的内容存储方法

(57)摘要

本发明涉及一种基于区块链技术的内容存储方法，包括如下步骤：建立一私有区块链网络；将内容划分为多个数据块，分别存储于私有区块链网络的相应节点上；对各节点上存储的数据块进行计算，以形成至少一特征；将至少一特征锚定到公有区块链网络中。该存储方法能够以低成本来实施，也能够进一步提升内容或数据的安全性、可靠性。



CN 106372533 A

1.一种基于区块链技术的内容存储方法,包括如下步骤:

a)、建立一私有区块链网络;

b)、将内容划分为多个数据块,分别存储于所述私有区块链网络的相应节点上;

c)、对各所述节点上存储的所述数据块进行计算,以形成至少一特征;

d)、将所述至少一特征锚定到公有区块链网络中。

2.根据权利要求1所述的方法,其特征在于,所述步骤a)包括:

根据用户业务规模和/或所述内容的量来确定所述私有区块链网络的节点数量。

3.根据权利要求2所述的方法,其特征在于,所述步骤a)还包括:

确定所述私有区块链网络中的哪些节点需要进行共识;

采用工作量证明共识算法来建立和/或优化所述私有区块链网络。

4.根据权利要求1所述的方法,其特征在于,所述特征为哈希值。

5.根据权利要求1所述的方法,其特征在于,所述步骤d)具体包括:

周期性地将所述至少一特征锚定到所述公有区块链网络中。

6.根据权利要求1至5中任一项所述的方法,其特征在于,其还包括步骤e):

将所述私有区块链网络的各所述节点上存储的所述数据块与所述公有区块链网络中所锚定的相应特征相结合,分别对各所述数据块进行验证。

7.根据权利要求6所述的方法,其特征在于,其还包括步骤f):

基于所述私有区块链网络的各所述节点上存储的所述数据块分别通过验证后,向所述私有区块链网络增加节点。

基于区块链技术的内容存储方法

技术领域

[0001] 本发明涉及数据存储技术领域。

背景技术

[0002] 现有技术中，进行内容存储与验证，通常会采用数据库技术来实现。然而，不管是传统的关系型数据库还是非关系型数据库，抑或是现有的分布式数据库，都存在很大的局限性。

[0003] 首先，数据库是中心化的，即使是分布式数据库也存在“中心化”的问题，这就导致了一旦中心被攻破，那么所有存储在数据库中的内容将不再安全，很多情况下甚至是不可再恢复的。

[0004] 其次，数据库的存储方式使得内容变更极为容易，只要拥有数据库的管理权限，就能够对存储内容进行篡改，甚至能够做到不被发现。

[0005] 再次，数据库的维护是由一群专业的数据库维护人员进行的。结合到实际应用中，数据库的维护者还必须对业务非常熟悉，这等于是将风险落在了少数的维护人员身上。

[0006] 最后，数据库的灾备问题，一个企业为了保证自己数据的高安全、高可用性，往往会建立多个异地中心，采用数据库同步备份的方式实时的进行同步而，这将会极大地增加运维成本。

[0007] 因此，本领域技术人员一直期望获得更加安全可靠、且实现成本低的内容存储方式。

[0008] 另一方面，区块链是一种账本数据存储方式，是以多份拷贝形式存在于点对点网络上的只可追加的总账数据库。它具有集体维护、去中心化、信任共识机制、数据不可篡改等特性。

[0009] 在数据存储方面，区块链采用了链式账本结构，相较传统二维数据库表结构，其将一定数量的数据记录打包成数据块，再将数据块之间通过摘要信息链接，使得对数据库的改动可以通过数学算法迅速甄别，能有效防止对数据信息的篡改。在网络层面，区块链采用了P2P组网方式，根据业务种类不同，有五到上千个不等的能独立承担业务流量和数据存储的业务节点，相较传统灾备网络结构中最成熟的两地三中心架构，有更多节点参与到核心网络的组建和账本数据的保存中，提高了系统的可用性和可靠性。

[0010] 此外，区块链采用哈希算法和各类对称、非对称加密算法，可以对节点进行身份管理和访问控制，保证记账行为和数据内容的不可否认特性，对账户信息、记账数据的机密性进行保护。

发明内容

[0011] 本发明的目的在于提供一种结合区块链技术、更加安全可靠、且实现成本低的内容存储方式。

[0012] 为实现上述目的，本发明提供一种技术方案如下：

一种基于区块链技术的内容存储方法，包括如下步骤：a)、建立一私有区块链网络；b)、将内容划分为多个数据块，分别存储于私有区块链网络的相应节点上；c)、对各节点上存储的数据块进行计算，以形成至少一特征；d)、将至少一特征锚定到公有区块链网络中。

[0013] 优选地，步骤a)包括：根据用户业务规模和/或内容的量来确定私有区块链网络的节点数量。

[0014] 优选地，步骤a)还包括：确定私有区块链网络中的哪些节点需要进行共识；采用工作量证明共识算法来建立和/或优化私有区块链网络。

[0015] 优选地，步骤d)具体包括：周期性地将至少一特征锚定到公有区块链网络中。

[0016] 优选地，其还包括步骤e)：将私有区块链网络的各节点上存储的数据块与公有区块链网络中所锚定的相应特征相结合，分别对各数据块进行验证。

[0017] 优选地，其还包括步骤f)：基于私有区块链网络的各节点上存储的数据块分别通过验证后，向私有区块链网络增加节点。

[0018] 本发明所提供的内容存储方法，由于基于区块链技术来实现，相比于现有的基于数据库的数据存储方式，其能够引入去中心化、信任共识机制、数据不可篡改等特性，从而使得数据或内容更加安全可靠。此外，通过结合私有区块链网络、公有区块链网络，该存储方法能够以低成本来实施；通过这种结合来对数据或内容进行验证，也能够进一步提升内容或数据的安全性。

附图说明

[0019] 图1示出根据本发明一实施例的、基于区块链技术的内容存储方法的流程图。

[0020] 图2示出根据本发明另一实施例的、基于区块链技术的内容存储方法的流程图。

具体实施方式

[0021] 如图1所示，本发明第一实施例提供一种基于区块链技术的内容存储方法，其包括如下各步骤：

步骤S10、建立一私有区块链网络。

[0022] 具体地，首先，可以根据用户业务规模和/或需要存储的内容的量来确定私有区块链网络的规模或是其节点数量。

[0023] 优选情况下，在该步骤中，还确定私有区块链网络中的哪些节点需要进行共识；以及，采用工作量证明(POW)共识算法来建立和/或优化私有区块链网络。

[0024] 可以理解，为了让这些节点达成一致，需要设计节点共识算法，以便于选定记账(存储)节点以及对每个数据块的合法性和有效性达成一致。用户可以根据其业务逻辑来自定义共识算法，节点个数最优控制在5-8个。

[0025] 此外，还可以根据不同的区块链技术来修正或优化节点的数量。

[0026] 步骤S11、将内容划分为多个数据块，分别存储于私有区块链网络的相应节点上。

[0027] 具体地，在存储于相应节点上之后，这多个数据块之间能够通过摘要信息相互链接，这多个数据块、连同它们之间的链接关系，共同组成需要存储的内容，从而使得对内容的任何更改将会被迅速甄别。

[0028] 步骤S12、对各节点上存储的数据块进行计算，以形成至少一特征。

[0029] 该步骤中，可以对私有区块链网络中的各数据块按一定的算法(如默克尔树哈希算法)进行计算，得出一个或一组特征，诸如哈希值、或其他的数据统计特征。特征可以与数据块一一对应，从而该一个特征能够反映对应数据块的特性；或者，也可以基于多个数据块形成单个特征，从而使得该特征能够表征所存储内容的特性。

[0030] 步骤S13、将上述至少一特征锚定到公有区块链网络中。

[0031] 具体地，可以将步骤S12中计算得到的一个或多个特征锚定到公有区块链(例如，比特币公有区块链、以太坊公有区块链等)网络上，从而可以利用公有区块链网络的公正性来验证私有区块链网络中的各数据块的合法性和有效性。

[0032] 优选情况下，可以按一定频率、周期性地将各特征锚定到公有区块链网络中，以利于数据或内容的更新及安全。

[0033] 例如，某票据业务进行票据的存储和验证，那么票据业务系统可以根据票据量来设定锚定的机制，如设定每10万条票据进行一次公链锚定。那么在业务系统中可以设置一个定时任务，每当票据数量增加到10万的时候，将这10万条数据进行打包并存储到私有区块链网络中，同时根据每一条记录的哈希值进行默克尔树计算，最终计算出一个root值(默克尔树的根)，并将这个root值发送到公有区块链网络上进行记录。

[0034] 该内容存储方法基于区块链技术来实现，相比于现有的基于数据库的数据存储方式，其能够使得数据或内容更加安全可靠。此外，正是由于利用了区块链技术，其不需要设置大型数据库而可方便地实现数据的存储、查询及验证，从而实施及维护成本低，利于在行业内推广应用。

[0035] 如图2所示，本发明第二实施例提供另一种基于区块链技术的内容存储方法，其能够在上述第一实施例的基础上进行改进而得到。

[0036] 具体地，其包括：步骤S10、建立一私有区块链网络；步骤S11、将内容划分为多个数据块，分别存储于私有区块链网络的相应节点上；步骤S12、对各节点上存储的数据块进行计算，以形成至少一特征；以及步骤S13、将上述至少一特征锚定到公有区块链网络中。

[0037] 与上述第一实施例不同的是，其还包括步骤S14：将私有区块链网络的各节点上存储的数据块与公有区块链网络中所锚定的相应特征相结合，分别对各数据块进行验证。这种验证可以按照用户的指示来进行，也可以定期进行。

[0038] 经上述验证后，能够确保所存储内容的高可用性和高可靠性。

[0039] 作为该第二实施例的优选实施方式，在步骤S14之后，还可以进行如下步骤：基于私有区块链网络的各节点上存储的数据块分别通过上述验证后，向该私有区块链网络增加节点。所增加的新节点能够用于存储新的数据块，从而实现内容的更新或扩充。

[0040] 与上述第一实施例相比，该第二实施例进一步利于为私有区块链网络的各节点上存储的数据块提供公信力，还可以进一步增加可信的新节点来实现所存储内容的更新或扩充。

[0041] 可以理解，在与具体的应用场景相结合时，可以定义并实现多个应用程序接口(API)。

[0042] API是用户业务系统与私有区块链之间的桥梁，同时也是私有区块链与公有区块链之间的桥梁。通过API的调用，业务系统的开发人员可以快速而方便地使用区块链技术来实现内容的存储、检索与验证，而无需再去学习区块链技术本身。为了适用大多数内容存储

与验证的场景，可以提出六类API接口。

[0043] 1)、内容存储API。业务系统通过调用该接口能够迅速地将需要存储的内容保存到私有区块链网络中。

[0044] 2)、内容查询API。业务系统通过调用该接口能够快速检索到存储在私有区块链网络中的内容。

[0045] 3)、公链锚定参数设置API。如上所述，增加了公链锚定的功能是为了保证私有区块链网络的公正性。公链锚定的参数设置由业务系统调用，例如，业务系统根据业务规则和需求可以设置锚定公链的频率，如每隔100条内容锚定一次或每72个小时锚定一次，也可以根据用户指示来进行。设置合适的锚定参数，使得既可以节约使用公链的成本，又能够保证内容的安全。

[0046] 4)、公链锚定参数查询API。对应于公链锚定参数的设置，业务系统可以随时查询设置过的公链锚定参数。随着业务功能或需求的变更，可能会对曾经设置过的锚定参数做修正，此时就需要通过该接口来查询参数后，再调用参数设置API来进行修改。

[0047] 5)、公链锚定结果查询API。业务系统在设定好公链锚定参数之后，私有区块链会按照规则和设定的算法在满足条件之时定期地向公链锚定内容，业务系统可以根据锚定参数配置查询到某一时间段内向公链锚定的结果。

[0048] 6)、公链锚定结果验证API。当私有区块链网络中需要增加新的节点的时候，出于安全考虑，新增加的节点必须要验证整个私有区块链网络的公正性，以防被整个私有区块链所欺诈。具体地，新增加节点可以随机同步私有区块链网络中的一些内容，然后通过该接口来获取到锚定到公有区块链的哈希值，然后通过设定的锚定规则和算法可以验证哈希值的正确性。

[0049] 上述说明仅针对于本发明的优选实施例，并不在于限制本发明的保护范围。本领域技术人员可作出各种变形设计，而不脱离本发明的思想及附随的权利要求。

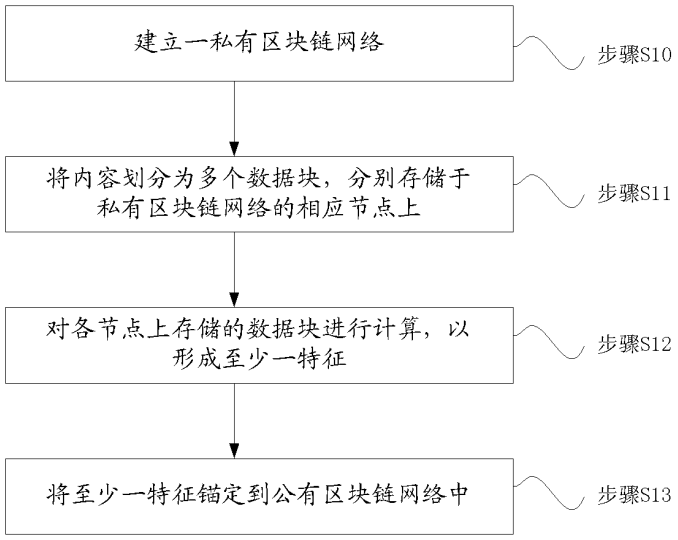

建立一私有区块链网络
步骤S10
将内容划分为多个数据块，分别存储于私有区块链网络的相应节点上
步骤S11
对各节点上存储的数据块进行计算，以形成至少一特征
步骤S12
将至少一特征锚定到公有区块链网络中
步骤S13

图 1

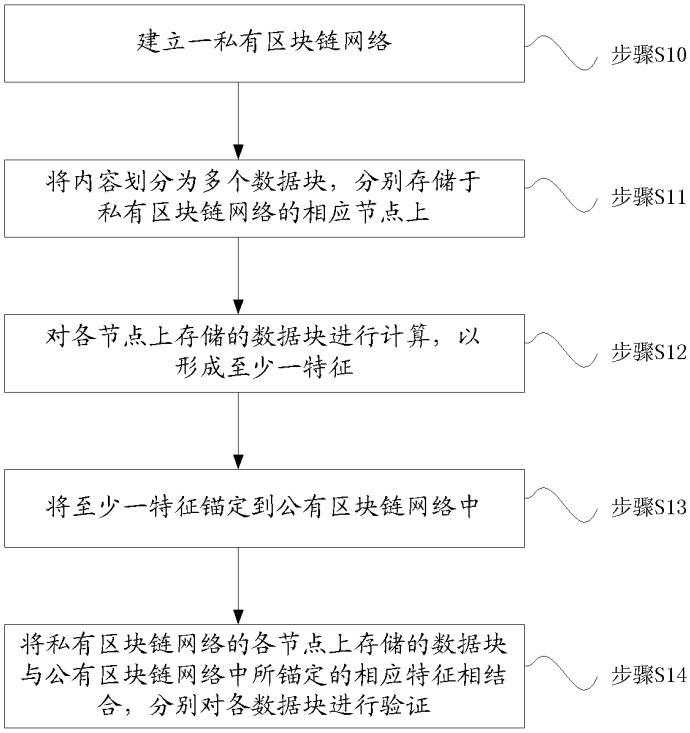

建立一私有区块链网络
步骤S10
将内容划分为多个数据块，分别存储于私有区块链网络的相应节点上
步骤S11
对各节点上存储的数据块进行计算，以形成至少一特征
步骤S12
将至少一特征锚定到公有区块链网络中
步骤S13
将私有区块链网络的各节点上存储的数据块与公有区块链网络中所锚定的相应特征相结合，分别对各数据块进行验证
步骤S14

图 2