(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 108038184 A
(43)申请公布日 2018.05.15

(21)申请号 201711297767.5

(22)申请日 2017.12.08

(71)申请人 横琴密达科技有限责任公司
地址 519031 广东省珠海市横琴新区环岛东路1889号创意谷18栋110室-119(集中办公区)

(72)发明人 韩永飞

(74)专利代理机构 杭州千克知识产权代理有限公司 33246
代理人 郭扬部

(51)Int.Cl.
G06F 17/30(2006.01)
G06Q 20/06(2012.01)

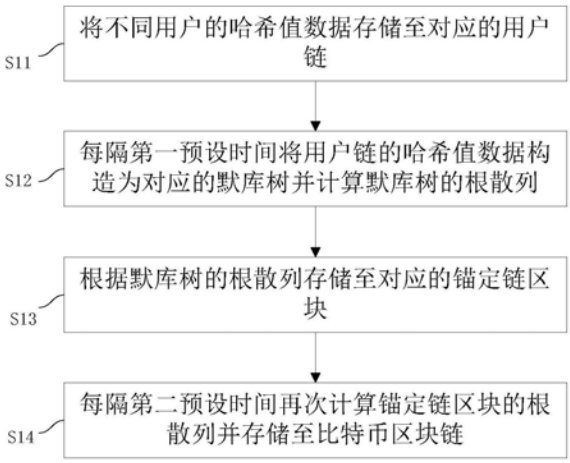
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种基于区块链的数据存储方法及系统、一种智能区块链

(57)摘要

本发明公开了一种基于区块链的数据存储方法及系统、一种智能区块链，用以解决现有的区块链存储方式消耗成本并且存储有限的问题。该方法包括：将不同用户的哈希值数据存储至对应的用户链；每隔第一预设时间将所述用户链的哈希值数据构造为对应的默库树并计算所述默库树的根散列；根据所述默库树的根散列存储至对应的锚定链区块；每隔第二预设时间再次计算锚定链区块的根散列并存储至比特币区块链。本发明通过构建基于区块链的分层数据存储体系对电子数据进行固化，大大减轻了网络的数据传输负荷和用户的存储压力。



CN 108038184 A

1.一种基于区块链的数据存储方法,其特征在于,包括步骤:

将不同用户的哈希值数据存储至对应的用户链;

每隔第一预设时间将所述用户链的哈希值数据构造为对应的默库树并计算所述默库树的根散列;

根据所述默库树的根散列存储至对应的锚定链区块;

每隔第二预设时间再次计算锚定链区块的根散列并存储至比特币区块链。

2.根据权利要求1所述的一种基于区块链的数据存储方法,其特征在于,所述用户链和所述锚定链的数据都存储于区块链的节点中。

3.根据权利要求2所述的一种基于区块链的数据存储方法,其特征在于,所述区块链的节点根据用户的设置部署。

4.一种基于区块链的数据存储系统,其特征在于,包括:

第一存储模块,用于将不同用户的哈希值数据存储至对应的用户链;

构造模块,用于每隔第一预设时间将所述用户链的哈希值数据构造为对应的默库树并计算所述默库树的根散列;

第二存储模块,用于根据所述默库树的根散列存储至对应的锚定链区块;

第三存储模块,用于每隔第二预设时间再次计算锚定链区块的根散列并存储至比特币区块链。

5.根据权利要求4所述的一种基于区块链的数据存储系统,其特征在于,所述第一存储模块的用户链和所述第二存储模块的锚定链的数据都存储于区块链的节点中。

6.根据权利要求5所述的一种基于区块链的数据存储系统,其特征在于,所述第三存储模块中,所述区块链的节点根据用户的设置部署。

7.一种智能区块链,其特征在于,包括:

用户链,用于存储不同用户的哈希值数据并根据所述哈希值数据构造默库树;

锚定链,用于计算所述用户链的默库树的根散列并存储计算后的默库树的根散列;

比特币区块链,用于再次计算所述默库树的根散列并存储再次计算后的根散列。

一种基于区块链的数据存储方法及系统、一种智能区块链

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种基于区块链的数据存储方法及系统、一种智能区块链。

背景技术

[0002] 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，本质上是一个去中心化的数据库，同时为比特币的底层技术，被广泛应用与证券交易、电子商务、智能合约、物联网、社交通讯以及文件存储等众多领域。

[0003] 当前的区块链技术是由一串使用密码学方法产生的数据块组成的，每一个区块都包含了上一个区块的哈希值，并且确保按照时间顺序在上一个区块之后产生，从创始区块开始连接到当前区块，形成块链。区块链的前期数据结构基本是为了实现比特币转账交易而设计的，存在优点和缺点。

[0004] 现有的区块链技术存在以下缺点：

[0005] (1)若应用区块链技术的方式将数据存储在币基交易中，缺点只有该区块的创建者才能把数据写入币基，也就是说只有通过消耗相当成本的算力并挖得区块的基础上才能够获得存储机会；

[0006] (2)若应用区块链技术的方式为将数据散列并编码为比特币输出，然后设置输出脚本的第一个操作为“操作返回”，并构造一笔交易广播到比特币网络上，缺点是存储的数据极其有限，且过于频繁地发送容易导致网络阻塞。

发明内容

[0007] 本发明要解决的技术问题目的在于提供一种基于区块链的数据存储方法及系统、一种智能区块链，用以解决现有的区块链存储方式消耗成本并且存储有限的问题。

[0008] 为了实现上述目的，本发明采用的技术方案为：

[0009] 一种基于区块链的数据存储方法，包括步骤：

[0010] 将不同用户的哈希值数据存储至对应的用户链；

[0011] 每隔第一预设时间将所述用户链的哈希值数据构造为对应的默库树并计算所述默库树的根散列；

[0012] 根据所述默库树的根散列存储至对应的锚定链区块；

[0013] 每隔第二预设时间再次计算锚定链区块的根散列并存储至比特币区块链。

[0014] 进一步地，所述用户链和所述锚定链的数据都存储于区块链的节点中。

[0015] 进一步地，所述区块链的节点根据用户的设置部署。

[0016] 一种基于区块链的数据存储系统，包括：

[0017] 第一存储模块，用于将不同用户的哈希值数据存储至对应的用户链；

[0018] 构造模块，用于每隔第一预设时间将所述用户链的哈希值数据构造为对应的默库树并计算所述默库树的根散列；

[0019] 第二存储模块，用于根据所述默库树的根散列存储至对应的锚定链区块；

[0020] 第三存储模块，用于每隔第二预设时间再次计算锚定链区块的根散列并存储至比特币区块链。

[0021] 进一步地，所述第一存储模块的用户链和所述第二存储模块的锚定链的数据都存储于区块链的节点中。

[0022] 进一步地，所述第三存储模块中，所述区块链的节点根据用户的设置部署。

[0023] 一种智能区块链，包括：

[0024] 用户链，用于存储不同用户的哈希值数据并根据所述哈希值数据构造默库树；

[0025] 锚定链，用于计算所述用户链的默库树的根散列并存储计算后的默库树根散列；

[0026] 比特币区块链，用于再次计算所述默库树的根散列并存储再次计算后的根散列。

[0027] 本发明与传统的技术相比，有如下优点：

[0028] 本发明通过构建基于区块链的分层数据存储体系对电子数据进行固化，大大减轻了网络的数据传输负荷和用户的存储压力。

附图说明

[0029] 图1是实施例一提供的一种基于区块链的数据存储方法流程图；

[0030] 图2是实施例二提供的一种基于区块链的数据存储系统结构图；

[0031] 图3是实施例三提供的一种智能区块链的结构图。

具体实施方式

[0032] 以下是本发明的具体实施例并结合附图，对本发明的技术方案作进一步的描述，但本发明并不限于这些实施例。

[0033] 实施例一

[0034] 本实施例提供了一种基于区块链的数据存储方法，如图1所示，包括步骤：

[0035] S11:将不同用户的哈希值数据存储至对应的用户链；

[0036] S12:每隔第一预设时间将用户链的哈希值数据构造为对应的默库树并计算默库树的根散列；

[0037] S13:根据默库树的根散列存储之对应的锚定链区块；

[0038] S14:每隔第二预设时间再次计算锚定链区块的根散列并存储之比特币区块链。

[0039] 本实施例构建了分层数据存储体系解决现有的区块链存储成本高，空间有限的问题。本实施例的区块链为智能区块链，包括了三层，用户链、锚定链及比特币区块链。通过分层数据存储体系，使数据安全性更高，并且不会造成网络堵塞。

[0040] 具体的，哈希值是一段数据唯一且极其紧凑的数值表示形式。如果散列一段明文而且哪怕只更改该段落的一个字母，随后的哈希都将产生不同的值。要找到散列为同一个值的两个不同的输入，在计算上来说基本上是不可能的。消息身份验证代码(MAC)哈希函数通常与数字签名一起用于对数据进行签名，而消息检测代码(MDC)哈希函数则用于数据完整性。

[0041] 每个用户的哈希值数据都存放在自己的用户链上，每隔第一预设时间将用户链上的哈希值数据构造成一颗默库树，并计算该默库树的根散列，将根散列存放至锚定链区块

中。

[0042] 默库树，即Merkle可信树，是为了解决多重一次签名中的认证问题而产生的，Merkle可信树结构具有一次签名大量认证的优点，在认证方面具有显著的优势。如今，Merkle可信树的树形结构已经被广泛应用到了信息安全的各个领域，比如证书撤销、源组播认证、群密钥协商等等。并且基于Merkle可信树的数字签名方案在安全性上仅仅依赖于哈希函数的安全性，且不需要太多的理论假设，这使得基于Merkle可信树的数字签名更加安全、实用。

[0043] 每隔第二预设时间再次计算锚定链区块的默库树的根散列，将其保存至比特币区块链，整个过程称之为锚定。

[0044] 其中，用户链和锚定链的数据都存储于区块链的节点中，区块链节点间组成类似于比特币的点对点网络。

[0045] 对于有条件部署区块链节点的用户，区块链鼓励自行部署节点。由于区块链节点越多，整个网络的数据安全性就越高。而对于没有条件部署区块链节点的用户，一方面可以信任区块链自身不会篡改节点中的数据，另一方面，只要有其他的用户部署了区块链的节点，区块链自身篡改数据的可能性就越低，因为区块链的节点越多，自身就越难篡改数据。

[0046] 因此，本实施例通过分层数据存储体系，使数据更为安全，成本更低，存储空间越大，避免了网络阻塞的问题。

[0047] 实施例二

[0048] 本实施例提供了一种基于区块链的数据存储系统，如图2所示，包括：

[0049] 第一存储模块21，用于将不同用户的哈希值数据存储至对应的用户链；

[0050] 构造模块22，用于每隔第一预设时间将用户链的哈希值数据构造为对应的默库树并计算默库树的根散列；

[0051] 第二存储模块23，用于根据默库树的根散列存储之对应的锚定链区块；

[0052] 第三存储模块24，用于每隔第二预设时间再次计算锚定链区块的根散列并存储之比特币区块链。

[0053] 本实施例构建了分层数据存储体系解决现有的区块链存储成本高，空间有限的问题。本实施例的区块链为智能区块链，包括了三层，用户链、锚定链及比特币区块链。通过分层数据存储体系，使数据安全性更高，并且不会造成网络堵塞。

[0054] 具体的，哈希值是一段数据唯一且极其紧凑的数值表示形式。如果散列一段明文而且哪怕只更改该段落的一个字母，随后的哈希都将产生不同的值。要找到散列为同一个值的两个不同的输入，在计算上来说基本上是不可能的。消息身份验证代码(MAC)哈希函数通常与数字签名一起用于对数据进行签名，而消息检测代码(MDC)哈希函数则用于数据完整性。

[0055] 每个用户的哈希值数据都存放在自己的用户链上，每隔第一预设时间将用户链上的哈希值数据构造成一颗默库树，并计算该默库树的根散列，将根散列存放至锚定链区块中。

[0056] 默库树，即Merkle可信树，是为了解决多重一次签名中的认证问题而产生的，Merkle可信树结构具有一次签名大量认证的优点，在认证方面具有显著的优势。如今，Merkle可信树的树形结构已经被广泛应用到了信息安全的各个领域，比如证书撤销、源组

播认证、群密钥协商等等。并且基于Merkle可信树的数字签名方案在安全性上仅仅依赖于哈希函数的安全性，且不需要太多的理论假设，这使得基于Merkle可信树的数字签名更加安全、实用。

[0057] 每隔第二预设时间再次计算锚定链区块的默库树的根散列，将其保存至比特币区块链，整个过程称之为锚定。

[0058] 其中，用户链和锚定链的数据都存储于区块链的节点中，区块链节点间组成类似于比特币的点对点网络。

[0059] 对于有条件部署区块链节点的用户，区块链鼓励自行部署节点。由于区块链节点越多，整个网络的数据安全性就越高。而对于没有条件部署区块链节点的用户，一方面可以信任区块链自身不会篡改节点中的数据，另一方面，只要有其他的用户部署了区块链的节点，区块链自身篡改数据的可能性就越低，因为区块链的节点越多，自身就越难篡改数据。

[0060] 因此，本实施例通过分层数据存储体系，使数据更为安全，成本更低，存储空间越大，避免了网络阻塞的问题。

[0061] 实施例三

[0062] 本实施例提供了一种智能区块链，如图3所示，包括：

[0063] 用户链31，用于存储不同用户的哈希值并根据哈希值数据构造默库树；

[0064] 锚定链32，用于计算用户链的默库树的根散列并存储计算后的默库树的根散列；

[0065] 比特币区块链33，用于再次计算默库树的根散列并存储再次计算后的根散列。

[0066] 本实施例提供了一种智能区块链，该智能区块链于传统的区块链相比，采用了分层数据存储体系，解决了现有的区块链存储数据有限并且消耗成本的问题。

[0067] 本实施例的智能区块链分为用户链31、锚定链32及比特币区块链33。

[0068] 具体的，每个用户的哈希值数据都存放在自己的用户链31上，每隔第一预设时间将用户链31上的哈希值数据构造成一颗默库树，并计算该默库树的根散列，将根散列存放至锚定链32的区块中。

[0069] 每隔第二预设时间再次计算锚定链32区块的默库树的根散列，将其保存至比特币区块链33，整个过程称之为锚定。

[0070] 其中，用户链31和锚定链32的数据都存储于区块链的节点中，区块链节点间组成类似于比特币的点对点网络。

[0071] 对于有条件部署区块链节点的用户，区块链鼓励自行部署节点。由于区块链节点越多，整个网络的数据安全性就越高。而对于没有条件部署区块链节点的用户，一方面可以信任区块链自身不会篡改节点中的数据，另一方面，只要有其他的用户部署了区块链的节点，区块链自身篡改数据的可能性就越低，因为区块链的节点越多，自身就越难篡改数据。

[0072] 本实施例提供构造智能区块链，通过分层存储体系，保证了数据的安全性，并且存储空间大大增加，同时不会造成网络的阻塞。

[0073] 本文中所描述的具体实施例仅仅是对本发明精神作举例说明。本发明所属技术领域的技术人员可以对所描述的具体实施例做各种各样的修改或补充或采用类似的方式替代，但并不会偏离本发明的精神或者超越所附权利要求书所定义的范围。

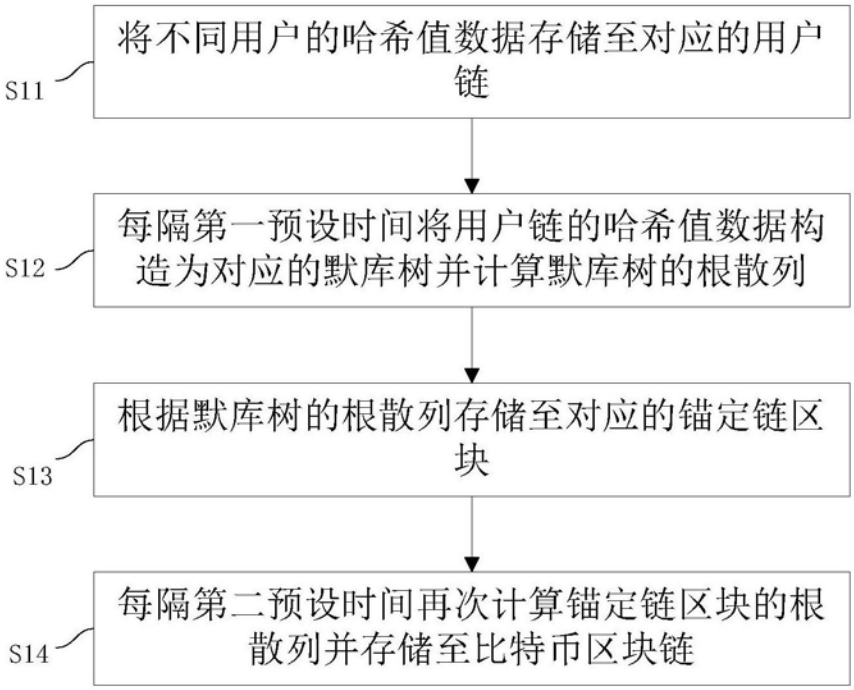

S11
将不同用户的哈希值数据存储至对应的用户链
S12
每隔第一预设时间将用户链的哈希值数据构造为对应的默库树并计算默库树的根散列
S13
根据默库树的根散列存储至对应的锚定链区块
S14
每隔第二预设时间再次计算锚定链区块的根散列并存储至比特币区块链

图1

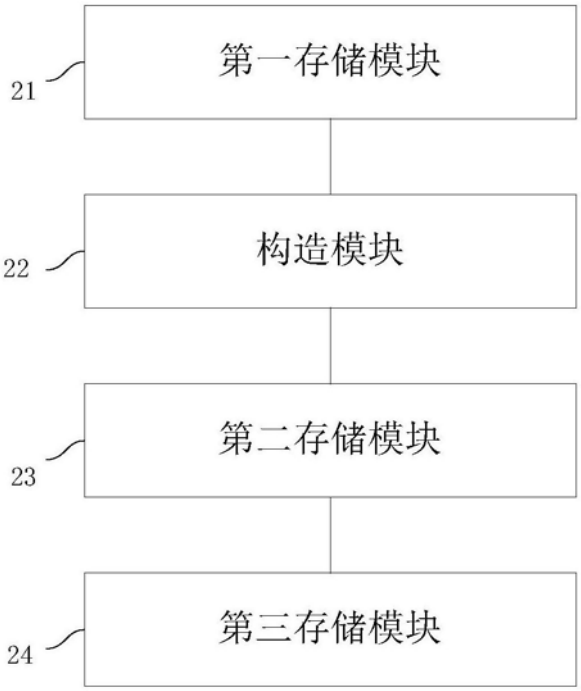

21
第一存储模块
22
构造模块
23
第二存储模块
24
第三存储模块

图2

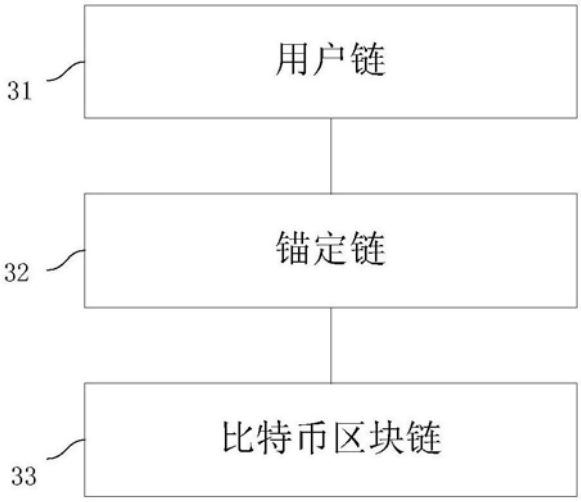


图3