(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 109413027 B
(45)授权公告日 2021.09.14

(21)申请号 201810993295.5

(22)申请日 2018.08.29

(65)同一申请的已公布的文献号
申请公布号 CN 109413027 A

(43)申请公布日 2019.03.01

(73)专利权人 上海麦士信息技术有限公司
地址 200435 上海市宝山区一二八纪念路968号1205室A区1007室

(72)发明人 李通越

(74)专利代理机构 上海海贝律师事务所 31301
代理人 范海燕

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04W 4/80(2018.01)
H04W 12/02(2009.01)

(56)对比文件
CN 104219678 A,2014.12.17
CN 108366362 A,2018.08.03
CN 108171068 A,2018.06.15
WO 2018093745 A1,2018.05.24
US 2017019788 A1,2017.01.19
姜威,姜泽睿."以区块链技术为核心的物联网安全解决对策研究".《通信技术》.2018,(第6期),全文.

审查员 刘叶

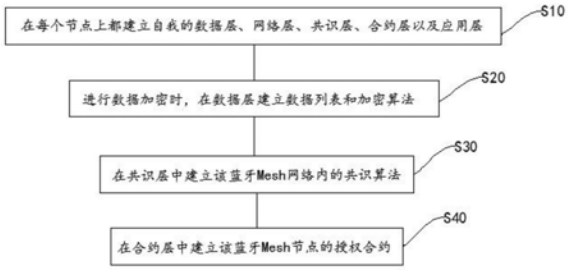
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种基于蓝牙Mesh分布式区块链数据授权加密方法

(57)摘要

本发明公开了一种基于蓝牙Mesh分布式区块链数据授权加密方法,包括以下步骤:在每个节点上都建立自我的数据层、网络层、共识层、合约层以及应用层;进行数据加密时,在数据层建立数据列表和加密算法;在共识层中建立该蓝牙Mesh网络内的共识算法;在合约层中建立该蓝牙Mesh节点的授权合约,以确定每个新节点在新添加入网络或者退出网络时的信息合约规则,本发明的整个网络通过使用分布式加密的方式,完成了网络去中心化,高安全性与稳定性的区块链式结构,保证了整个网络内的数据的可靠性和不可复制性,蓝牙Mesh目前大多应用于智能家居和智能城市等领域,利用分布式授权以及加密,可以保证每一个节点的不可复制性,以及提供统一的平台进行信息追溯。



CN 109413027 B

1.一种基于蓝牙Mesh分布式区块链数据授权加密方法,其特征在于包括以下步骤:

S10:在每个节点上都建立自我的数据层、网络层、共识层、合约层以及应用层;

S20:进行数据加密时,在数据层建立数据列表和加密算法,对各个节点的有效数据进行单点加密操作,实现各个节点的独立性,利用本地序号序列记录,形成链式结构;

S30:在共识层中建立该蓝牙Mesh网络内的共识算法;

S40:在合约层中建立该蓝牙Mesh节点的授权合约,以确定每个新节点在新添加入网络或者退出网络时的信息合约规则。

2.根据权利要求1所述的一种基于蓝牙Mesh分布式区块链数据授权加密方法,其特征在于:网络层为蓝牙Mesh的组网协议,该协议建立在网状连接结构上,进行数据双向通讯。

3.根据权利要求1所述的一种基于蓝牙Mesh分布式区块链数据授权加密方法,其特征在于:在应用层上每个蓝牙Mesh节点的数据做本地化的数据管理应用,以及整个蓝牙Mesh网络数据查询获取。

4.根据权利要求1所述的一种基于蓝牙Mesh分布式区块链数据授权加密方法,其特征在于:加密算法采用哈希算法,而数据签名则使用为非对称算法。

一种基于蓝牙Mesh分布式区块链数据授权加密方法

技术领域

[0001] 本发明涉及一种加密方法,具体为一种基于蓝牙Mesh分布式区块链数据授权加密方法。

背景技术

[0002] 从第一台计算机诞生起,经过几十年的高速发展,信息技术已经进入到我们的生活的方方面面,不断改变着我们的生活,我们已经进入了一个信息爆炸的信息化时代,大量的信息依靠传统的方式难以实现有效的储存和传输,因而以计算机技术和网络技术为基础的信息技术的发展显得尤为重要。

[0003] 蓝牙作为一种短距离无线数据与语音通信的开放性规范,它工作在2.4GHz ISM的免费频段,采用快速跳频扩频技术,具有通信速度快、功耗小、成本低、抗干扰强等优势,因此被广泛应用于生活中各个领域,然而由于该技术采用无线传输的方式,这就可能导致用户数据在传输中被非法用户所盗取,蓝牙所采用的快速跳频技术只能解决系统内部及外界设备引起的相关干扰问题,不能够有效地发现及及非法用户的访问,在使用蓝牙Mesh的过程中,对于每个节点的安全性和私密性都提出了较高的要求,而基于Mesh分布式的特点,可以利用区块链技术,对于系统数据进行加密处理。

发明内容

[0004] 本发明的目的在于提供一种基于蓝牙Mesh分布式区块链数据授权加密方法,以解决上述背景技术中提出的问题。

[0005] 为实现上述目的,本发明提供如下技术方案:一种基于蓝牙Mesh分布式区块链数据授权加密方法,包括以下步骤:

[0006] S10:在每个节点上都建立自我的数据层、网络层、共识层、合约层以及应用层;

[0007] S20:进行数据加密时,在数据层建立数据列表和加密算法,对各个节点的有效数据进行单点加密操作,实现各个节点的独立性,利用本地序号序列记录,形成链式结构;

[0008] S30:在共识层中建立该蓝牙Mesh网络内的共识算法;

[0009] S40:在合约层中建立该蓝牙Mesh节点的授权合约,以确定每个新节点在新添加入网络或者退出网络时的信息合约规则。

[0010] 作为本发明一种优选的技术方案,网络层为蓝牙Mesh的组网协议,该协议建立在网状连接结构上,进行数据双向通讯。

[0011] 作为本发明一种优选的技术方案,在应用层上每个蓝牙Mesh节点的数据做本地化的数据管理应用,以及整个蓝牙Mesh网络数据查询获取。

[0012] 作为本发明一种优选的技术方案,加密算法采用哈希算法,而数据签名则使用为非对称算法。

[0013] 与现有技术相比,本发明的有益效果是:本发明的整个网络通过使用分布式加密的方式,完成了网络去中心化,高安全性与稳定性的区块链式结构,保证了整个网络内的数

据的可靠性和不可复制性，蓝牙Mesh目前大多应用于智能家居和智能城市等领域，利用分布式授权以及加密，可以保证每一个节点的不可复制性，以及提供统一的平台进行信息追溯。

附图说明

[0014] 图1为本发明提供的一种基于蓝牙Mesh分布式区块链数据授权加密方法流程图；

[0015] 图2为本发明提供的一种基于蓝牙Mesh分布式区块链数据授权加密方法的系统示意图。

具体实施方式

[0016] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0017] 请参阅图1与图2，本发明提供一种基于蓝牙Mesh分布式区块链数据授权加密方法，包括以下步骤：

[0018] S10：在每个节点上都建立自我的数据层、网络层、共识层、合约层以及应用层；

[0019] S20：进行数据加密时，在数据层建立数据列表和加密算法，对各个节点的有效数据进行单点加密操作，实现各个节点的独立性，利用本地序号序列记录，形成链式结构；

[0020] 其中在进行数据加密时，对于蓝牙节点来说，一般对性能要求比较低，需要使用一些嵌入式数据库以及轻量级加密算法；在性能不足的情况下，可以直接使用数据列表；而为了安全性，需要对数据进行加密，加密算法多使用哈希算法，而签名则使用为非对称算法，如相对计算量小的RSA以及复杂性较强的ECC椭圆曲线算法。

[0021] S30：在共识层中建立该蓝牙Mesh网络内的共识算法；

[0022] 保证单独的节点数据在整个Mesh网络中都可以被识别为有效性，对于蓝牙Mesh的应用方向，使用PBFT实用拜占庭容错算法，在各个节点进行状态机的副本复制，两两节点互相进行响应交互判断，实现网络的共识性。

[0023] S40：在合约层中建立该蓝牙Mesh节点的授权合约，以确定每个新节点在新添加入网络或者退出网络时的信息合约规则；

[0024] 可以针对不同的应用场景设备修改不同的授权规则。

[0025] 作为本发明一种优选的技术方案，网络层为蓝牙Mesh的组网协议，该协议建立在网状连接结构上，进行数据双向通讯。

[0026] 作为本发明一种优选的技术方案，在应用层上每个蓝牙Mesh节点的数据做本地化的数据管理应用，以及整个蓝牙Mesh网络数据查询获取。

[0027] 基于上述，本发明具有的优点在于：本发明的整个网络通过使用分布式加密的方式，完成了网络去中心化，高安全性与稳定性的区块链式结构，保证了整个网络内的数据的可靠性和不可复制性，蓝牙Mesh目前大多应用于智能家居和智能城市等领域，利用分布式授权以及加密，可以保证每一个节点的不可复制性，以及提供统一的平台进行信息追溯。

[0028] 尽管已经示出和描述了本发明的实施例，对于本领域的普通技术人员而言，可以

理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由所附权利要求及其等同物限定。

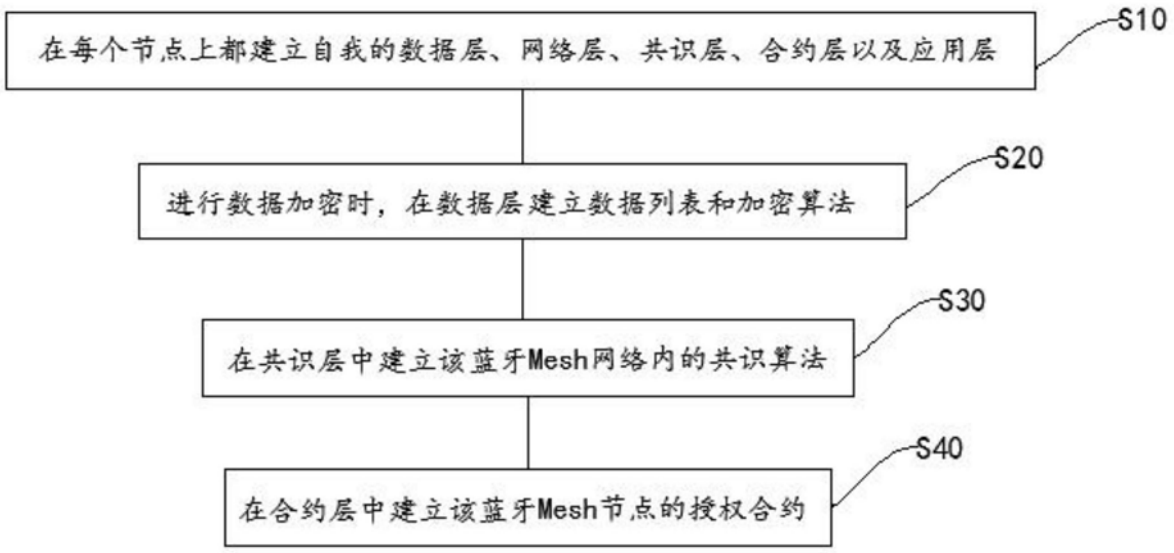

在每个节点上都建立自我的数据层、网络层、共识层、合约层以及应用层
S10
进行数据加密时，在数据层建立数据列表和加密算法
S20
在共识层中建立该蓝牙Mesh网络内的共识算法
S30
在合约层中建立该蓝牙Mesh节点的授权合约
S40

图1


应用层
数据查询
信息获取
合约层
授权规则
共识层
共识算法
网络层
BT Mesh
数据层
加密算法
数据列表

图2