(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 111586125 A
(43)申请公布日 2020.08.25

(21)申请号 202010349585.3

(22)申请日 2020.04.28

(71)申请人 济南浪潮高新科技投资发展有限公司
地址 250104 山东省济南市高新区孙村镇科航路2877号研发楼一楼

(72)发明人 薛长青 高明 金长新

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 刘新雷

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)

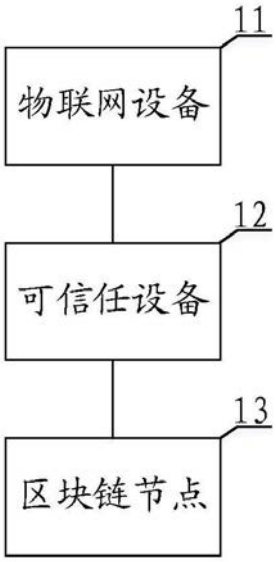
权利要求书1页 说明书6页 附图2页

(54)发明名称

一种物联网系统

(57)摘要

本申请公开了一种物联网系统，包括：物联网设备，用于采集原始采集数据，接收控制指令；可信任设备，用于接收原始采集数据，对原始采集数据进行处理，得到处理后的采集数据，利用密钥对采集数据进行加密，得到加密采集数据，接收加密指令，利用密钥对加密指令进行解密，得到控制指令，发送控制指令至物联网设备；区块链节点，用于接收加密采集数据并广播，接收用户终端发送的加密指令并广播；本申请增设预先存储有被授权的各物联网设备的密钥的可信任设备，未被授权的物联网设备和用户终端所发出的数据均会被截断在可信任设备，因此，提高了物联网系统的安全度，同时，区块链的应用，确保了数据不会被修改，确保了数据的安全性。



CN 111586125 A

1.一种物联网系统，其特征在于，包括：物联网设备、可信任设备和区块链节点；所述区块链节点为区块链网络中的一个节点；

所述物联网设备，用于发送采集到的原始采集数据至所述可信任设备，接收所述可信任设备发送的控制指令；

所述可信任设备，用于接收所述物联网设备发送的所述原始采集数据，对所述原始采集数据进行处理，得到处理后的采集数据，利用与所述物联网设备对应的密钥对所述采集数据进行加密，得到加密后的加密采集数据，发送所述加密采集数据至所述区块链节点，接收加密指令，利用与所述物联网设备对应的密钥对所述加密指令进行解密，得到控制指令，发送所述控制指令至所述物联网设备；

所述区块链节点，用于接收所述加密采集数据并广播所述加密采集数据至所述区块链网络中的各节点存储，接收用户终端发送的所述加密指令并广播所述加密指令至各节点存储，将所述加密指令发送至所述可信任设备。

2.根据权利要求1所述的物联网系统，其特征在于，所述区块链节点，还用于对所述加密采集数据进行解密，得到所述采集数据，利用智能合约对所述采集数据进行分析，判断是否需要告警，如果需要告警，广播告警信息至各节点和所述用户终端。

3.根据权利要求2所述的物联网系统，其特征在于，所述可信任设备，包括：数据采集通道、数据处理模块、硬件加密模块、数据交换模块和设备控制通道；

所述数据采集通道，用于接收所述物联网设备发送的所述原始采集数据；

所述数据处理模块，用于对所述原始采集数据进行处理，得到处理后的所述采集数据，发送所述采集数据至所述硬件加密模块，转发所述控制指令至所述设备控制通道；

所述硬件加密模块，用于利用与所述物联网设备对应的密钥对所述采集数据进行加密，得到加密后的加密采集数据，接收加密指令，利用与所述物联网设备对应的密钥对所述加密指令进行解密，得到控制指令；

所述数据交换模块，用于发送所述加密采集数据至所述区块链节点，接收加密指令；

所述设备控制通道，用于发送所述控制指令至所述物联网设备。

4.根据权利要求3所述的物联网系统，其特征在于，所述数据处理模块，具体用于对所述原始采集数据进行整合格式化，并将与所述原始采集数据对应的告警阈值合并，得到包括所述原始采集数据和所述告警阈值的处理后的所述采集数据。

5.根据权利要求4所述的物联网系统，其特征在于，所述区块链节点，具体用于调用初始智能合约，从所述初始智能合约中调用与所述物联网设备对应的所述智能合约，利用所述智能合约和所述采集数据中的所述告警阈值，判断是否需要告警。

6.根据权利要求3所述的物联网系统，其特征在于，所述硬件加密模块，具体用于利用所述物联网设备的私钥对所述采集数据添加数字签名，得到加密后的所述加密采集数据，接收加密指令，利用所述物联网设备的公钥对所述加密指令进行解密，得到控制指令。

一种物联网系统

技术领域

[0001] 本发明涉及区块链和物联网领域，特别涉及一种物联网系统。

背景技术

[0002] 云计算、大数据、新一代移动通信技术与智能感知、行业应用相互交织，激荡融合，不断激发创新活力，成为物联网发展的新动力。区块链技术作为当前国内外的焦点技术之一，可能会对未来技术创新和产业变革产生重要影响。在物联网中如何定位和应用区块链技术值得进一步思考和探讨。

[0003] 区块链是分布式数字存储、点对点传输、共识机制、加密算法等技术的集成应用。从狭义上讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义而言，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问安全、利用智能化合约来编程和操作数据的一种全新的分布式基础架构与计算范式。与传统的数据库技术相比，区块链具备3个特点：一是数据的不可篡改性；二是系统集体维护；三是信息的公开透明。同时，相对传统数据库技术，现阶段的区块链技术数据吞吐量小，读写时延较大，更适合低频率、小数据的可靠存储和处理。

[0004] 现有技术中，由于物联网系统中，物联网设备很多，难以管理，容易出现非授权的物联网设备接入物联网系统中，影响物联网系统安全，为此，需要一种能够提高物联网系统安全度的物联网系统。

发明内容

[0005] 有鉴于此，本发明的目的在于提供一种物联网系统，提高安全度。其具体方案如下：

[0006] 一种物联网系统，包括：物联网设备、可信任设备和区块链节点；所述区块链节点为区块链网络中的一个节点；

[0007] 所述物联网设备，用于发送采集到的原始采集数据至所述可信任设备，接收所述可信任设备发送的控制指令；

[0008] 所述可信任设备，用于接收所述物联网设备发送的所述原始采集数据，对所述原始采集数据进行处理，得到处理后的采集数据，利用与所述物联网设备对应的密钥对所述采集数据进行加密，得到加密后的加密采集数据，发送所述加密采集数据至所述区块链节点，接收加密指令，利用与所述物联网设备对应的密钥对所述加密指令进行解密，得到控制指令，发送所述控制指令至所述物联网设备；

[0009] 所述区块链节点，用于接收所述加密采集数据并广播所述加密采集数据至所述区块链网络中的各节点存储，接收用户终端发送的所述加密指令并广播所述加密指令至各节点存储，将所述加密指令发送至所述可信任设备。

[0010] 可选的，所述区块链节点，还用于对所述加密采集数据进行解密，得到所述采集数据，利用智能合约对所述采集数据进行分析，判断是否需要告警，如果需要告警，广播告警信息至各节点和所述用户终端。

[0011] 可选的，所述可信任设备，包括：数据采集通道、数据处理模块、硬件加密模块、数据交换模块和设备控制通道；

[0012] 所述数据采集通道，用于接收所述物联网设备发送的所述原始采集数据；

[0013] 所述数据处理模块，用于对所述原始采集数据进行处理，得到处理后的所述采集数据，发送所述采集数据至所述硬件加密模块，转发所述控制指令至所述设备控制通道；

[0014] 所述硬件加密模块，用于利用与所述物联网设备对应的密钥对所述采集数据进行加密，得到加密后的加密采集数据，接收加密指令，利用与所述物联网设备对应的密钥对所述加密指令进行解密，得到控制指令；

[0015] 所述数据交换模块，用于发送所述加密采集数据至所述区块链节点，接收加密指令；

[0016] 所述设备控制通道，用于发送所述控制指令至所述物联网设备。

[0017] 可选的，所述数据处理模块，具体用于对所述原始采集数据进行整合格式化，并将与所述原始采集数据对应的告警阈值合并，得到包括所述原始采集数据和所述告警阈值的处理后的所述采集数据。

[0018] 可选的，所述区块链节点，具体用于调用初始智能合约，从所述初始智能合约中调用与所述物联网设备对应的所述智能合约，利用所述智能合约和所述采集数据中的所述告警阈值，判断是否需要告警。

[0019] 可选的，所述硬件加密模块，具体用于利用所述物联网设备的私钥对所述采集数据添加数字签名，得到加密后的所述加密采集数据，接收加密指令，利用所述物联网设备的公钥对所述加密指令进行解密，得到控制指令。

[0020] 本发明中，物联网系统，包括：物联网设备、可信任设备和区块链节点；区块链节点为区块链网络中的一个节点；物联网设备，用于发送采集到的原始采集数据至可信任设备，接收可信任设备发送的控制指令；可信任设备，用于接收物联网设备发送的原始采集数据，对原始采集数据进行处理，得到处理后的采集数据，利用与物联网设备对应的密钥对采集数据进行加密，得到加密后的加密采集数据，发送加密采集数据至区块链节点，接收加密指令，利用与物联网设备对应的密钥对加密指令进行解密，得到控制指令，发送控制指令至物联网设备；区块链节点，用于接收加密采集数据并广播加密采集数据至区块链网络中的各节点存储，接收用户终端发送的加密指令并广播加密指令至各节点存储，将加密指令发送至可信任设备。

[0021] 本发明增设预先存储有被授权的各物联网设备的密钥的可信任设备，未被授权的物联网设备和用户终端所发出的数据均会被截断在可信任设备，而无法到达另一端，因此，提高了物联网系统的安全度，同时，区块链的应用，确保了物联网设备上传的数据不会被修改，确保了数据的安全性。

附图说明

[0022] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现

有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

[0023] 图1为本发明实施例公开的一种物联网系统结构示意图；

[0024] 图2为本发明实施例公开的另一种物联网系统结构示意图。

具体实施方式

[0025] 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。

[0026] 本发明实施例公开了一种物联网系统，参见图1所示，该系统包括：物联网设备11、可信任设备12和区块链节点13；区块链节点13为区块链网络中的一个节点；

[0027] 物联网设备11，用于发送采集到的原始采集数据至可信任设备12，接收可信任设备12发送的控制指令；

[0028] 可信任设备12，用于接收物联网设备11发送的原始采集数据，对原始采集数据进行处理，得到处理后的采集数据，利用与物联网设备11对应的密钥对采集数据进行加密，得到加密后的加密采集数据，发送加密采集数据至区块链节点13，接收加密指令，利用与物联网设备11对应的密钥对加密指令进行解密，得到控制指令，发送控制指令至物联网设备11；

[0029] 区块链节点13，用于接收加密采集数据并广播加密采集数据至区块链网络中的各节点存储，接收用户终端发送的加密指令并广播加密指令至各节点存储，将加密指令发送至可信任设备12。

[0030] 具体的，物联网设备11可以包括共享单车、共享充电宝、无人机和监控设备等可以接入物联网系统的设备，这些设备，可以通过GPS、传感器和摄像头等数据采集设备采集原始采集数据，以供物联网系统利用这些原始采集数据确认各物联网设备11的工作状态，并可以进行远程控制。

[0031] 具体的，为了有效管理接入物联网系统中的物联网设备11，避免未被授权的物联网设备11接入系统中，造成安全隐患，在区块链节点13与物联网设备11之间增设可信任设备12，可信任设备12中预先存储有被授权的各物联网设备11的密钥，在物联网设备11的原始采集数据发送至区块链中存储前，由可信任设备12对原始采集数据进行加密，加密后的加密采集数据，才能够发送至区块链进行存储，因此，如果未授权的物联网设备11接入到物联网系统中，想要将原始采集数据发送至区块链中，首先要将原始采集数据发送至可信任设备12中，此时，由于可信任设备12中没有存储未授权的物联网设备11的密钥，无法对未授权的物联网设备11的原始采集数据进行加密，所以未授权的物联网设备11的原始采集数据无法发送至区块链中，形成了第一道防护，确保了未授权的物联网设备11完全接入到物联网系统中，提高了物联网的安全度。

[0032] 具体的，基于区块链网络的特性，区块链节点13在接收到加密采集数据后，进行全网广播，将加密采集数据广播到每一个区块链节点13中进行存储，确保加密采集数据在区块链中无法被修改，保证了数据本身的安全性。

[0033] 可以理解的是,区块链节点13中存储有用于对加密采集数据进行解密的密钥。

[0034] 具体的,为了确保用户终端发送的控制指令的安全度,同样需要用户终端发送加密后的加密指令,加密指令通过区块链节点13发送至可信任设备12,如果用户终端发送的加密指令没有通过正确的密钥加密,则在可信任设备12中无法解密,物联网设备11就无法接收到该加密指令,从而在用户终端这一端,确保了加密指令的安全性。

[0035] 可见,本发明实施例增设预先存储有被授权的各物联网设备11的密钥的可信任设备12,未被授权的物联网设备11和用户终端所发出的数据均会被截断在可信任设备12,而无法到达另一端,因此,提高了物联网系统的安全度,同时,区块链的应用,确保了物联网设备11上传的数据不会被修改,确保了数据的安全性。

[0036] 需要说明的是,可信任设备12可以为本地服务器,一个可信任设备12可以对应多个物联网设备11,可信任设备12也可以集成在每个物联网设备11中,形成一对一的形式。

[0037] 本发明实施例公开了一种具体的分布式存储卷在线迁移方法,相对于上一实施例,本实施例对技术方案作了进一步的说明和优化。参见图2所示,具体的:

[0038] 具体的,上述区块链节点13,还可以用于对加密采集数据进行解密,得到采集数据,利用智能合约对采集数据进行分析,判断是否需要告警,如果需要告警,广播告警信息至各节点和用户终端。

[0039] 具体的,为了确保告警结果的准确性,在区块链节点13中进行告警判断,区块链节点13对加密采集数据进行解密后,得到采集数据,之后利用与采集数据对应的物联网设备11的智能合约对采集数据进行分析,判断是否需要告警,如果需要告警,广播告警信息至各节点保存告警结果,广播至用户终端已提醒用户出现告警。

[0040] 具体的,上述可信任设备12,可以包括:数据采集通道121、数据处理模块122、硬件加密模块123、数据交换模块124和设备控制通道125;其中,数据采集通道121,用于接收物联网设备11发送的原始采集数据;

[0041] 数据处理模块122,用于对原始采集数据进行处理,得到处理后的采集数据,发送采集数据至硬件加密模块123,转发控制指令至设备控制通道125;

[0042] 硬件加密模块123,用于利用与物联网设备11对应的密钥对采集数据进行加密,得到加密后的加密采集数据,接收加密指令,利用与物联网设备11对应的密钥对加密指令进行解密,得到控制指令;

[0043] 数据交换模块124,用于发送加密采集数据至区块链节点13,接收加密指令;

[0044] 设备控制通道125,用于发送控制指令至物联网设备11。

[0045] 具体的,数据交换模块124用以对接区块链主链的RPC(RPC,Remote Procedure Call,远程过程调用)和物联网设备11的API,实现区块链与物联网设备11之间的数据交换。

[0046] 进一步的,上述数据处理模块122,具体用于对原始采集数据进行整合格式化,并将与原始采集数据对应的告警阈值合并,得到包括原始采集数据和告警阈值的处理后的采集数据。

[0047] 具体的,智能合约进行告警判断所需的告警阈值,可以预先存储于可信任设备12中的数据处理模块122中,数据处理模块122在对原始采集数据进行整合格式化的同时,同时将告警阈值与原始采集数据进行结合,得到包括告警阈值和整合格式化的原始采集数据的采集数据,这样当区块链节点13解密加密采集数据后,便能够得到告警阈值和其中的数

据了。

[0048] 具体的，上述区块链节点13，可以具体用于调用初始智能合约，从初始智能合约中调用与物联网设备11对应的智能合约，利用智能合约和采集数据中的告警阈值，判断是否需要告警。

[0049] 具体的，初始智能合约包括大量的智能合约，每个智能合约相当于初始智能合约的子合约，每个智能合约对应不同的物联网设备11，因为不同的物联网设备11采集的数据可能不同，所对应的处理流程和判断方法不一样，及时同类型的物联网设备11也可能因各自应用场景不一样，智能合约不同，所以每个物联网设备11需要有各自对应的智能合约，并根据各自相应的智能合约结合告警阈值判断是否需要告警，如果不需要，则不用采取其它操作，继续正常运行。

[0050] 具体的，智能合约在告警时，告警信息将会作为新的事件生成，作为一个告警事件，在告警信息广播到区块链中时，该告警事件将会同时保存在区块链中。

[0051] 可以理解的是，因为区块链的特性，智能合约无法被更改，只能够终止全部合约后，重新发布新的合约。

[0052] 具体的，上述硬件加密模块123，可以具体用于利用物联网设备11的私钥对采集数据添加数字签名，得到加密后的加密采集数据，接收加密指令，利用物联网设备11的公钥对加密指令进行解密，得到控制指令。

[0053] 具体的，硬件加密模块123预先存储每个授权的物联网设备11的私钥和公钥，通过非对称加密确保物联网系统中数据的安全性。

[0054] 具体的，通过为采集数据添加数字签名，使加密采集数据在区块链网中数字签名也会广播到每个区块链节点13上，由于此时数据的签名指纹即数字签名已经记录在区块链上，任何人包括用户自己也不能对数据进行修改，其他用户在读取这些数据签名时就可以通过验证数据的完整性和真实性。

[0055] 具体的，可信任设备结合了区块链和物联网两大技术，充分利用了区块链的公开透明和不可篡改两大特性，结合硬件多重加密和数字指纹签名，可以实现双重设备认证，安全加密设备操作和可信签名数据采集。

[0056] 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0057] 专业人员还可以进一步意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0058] 以上对本发明所提供的技术内容进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

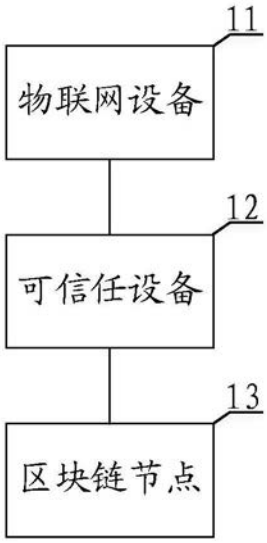


图1

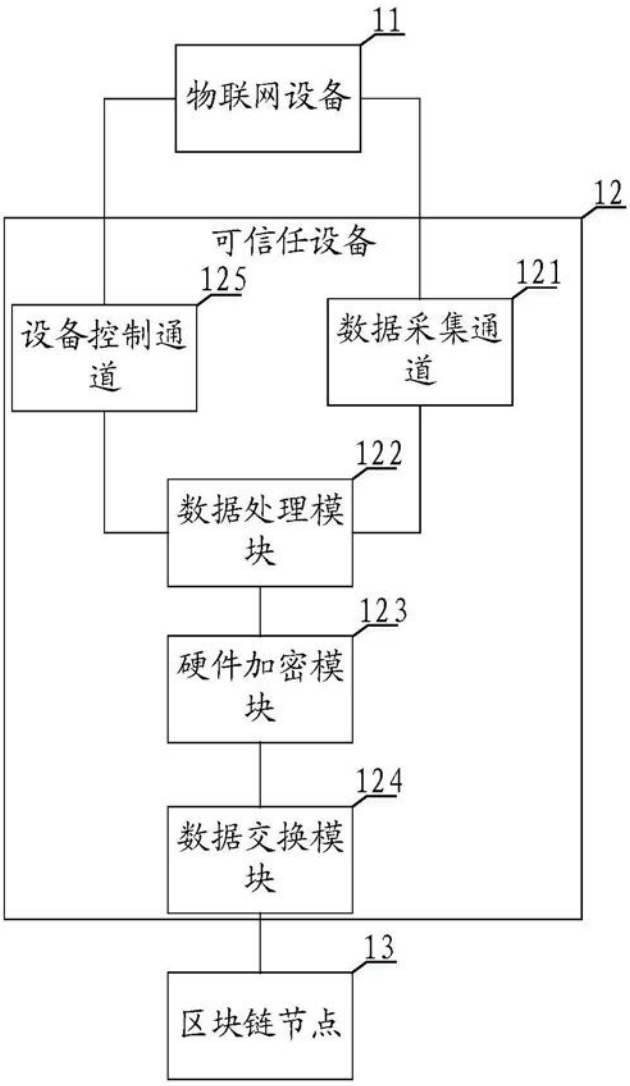

11
物联网设备
12
可信任设备
125
设备控制通道
121
数据采集通道
122
数据处理模块
123
硬件加密模块
124
数据交换模块
13
区块链节点

图2