(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 111131211 A
(43)申请公布日 2020.05.08

(21)申请号 201911302266.0

(22)申请日 2019.12.17

(71)申请人 杭州甘道智能科技有限公司
地址 310012 浙江省杭州市滨江区西兴街道丹枫路399号2号楼A楼1602室

(72)发明人 宋学武 林炀平 柯叶翔

(74)专利代理机构 杭州求是专利事务所有限公司 33200
代理人 贾玉霞

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
G07F 17/20(2006.01)

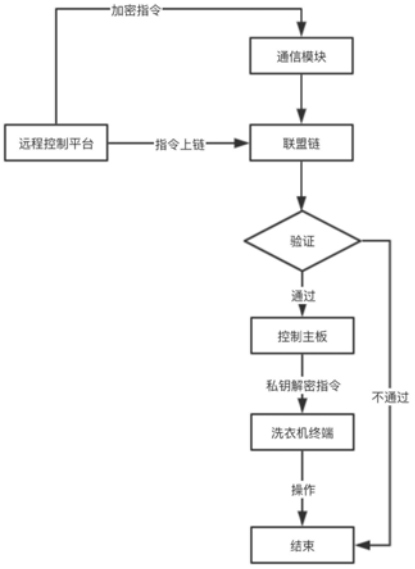
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种面向共享洗衣机安全的防篡改方法

(57)摘要

本发明公开一种面向共享洗衣机安全的防篡改方法，洗衣机包括通信模块和控制模块，洗衣机的控制指令程序集成在控制模块中，洗衣机受远程控制中心的控制，远程控制中心对洗衣机所有的控制指令均采用非对称加密算法进行加密，公钥保存于远程控制中心，私钥保存在通信模块和控制模块中，且洗衣机控制指令的访问控制策略和哈希地址均保存在由远程控制中心、洗衣机组成的联盟链上；当终端向远程控制中心发送控制请求时，远程控制中心将控制指令对应的加密指令发送给洗衣机，通信模块将控制指令上传到联盟链进行共识，通过后发送给控制模块；控制模块通过对应私钥解密指令后控制洗衣机执行相关操作。该方法保障了共享服务生态的设备安全与数据安全。



CN 111131211 A

1.一种面向共享洗衣机安全的防篡改方法,其特征在于,所述的共享洗衣机包括通信模块和控制模块,共享洗衣机的控制指令程序集成在所述的控制模块中,所述的共享洗衣机受远程控制中心的控制,所述的远程控制中心对所述的共享洗衣机所有的控制指令均采用非对称加密算法进行加密,公钥保存于远程控制中心,私钥分别保存在洗衣机的通信模块和控制模块中,且所述的共享洗衣机控制指令的访问控制策略和哈希地址均保存在由远程控制中心、洗衣机组成的联盟链上。

当终端向远程控制中心发送控制请求时,所述的远程控制中心将所述的控制指令对应的加密指令发送给所述的共享洗衣机的通信模块,通信模块将所述的控制指令上传到联盟链中进行共识,通过后发送给所述的控制模块;所述的控制模块通过对应的私钥解密指令后控制洗衣机执行相关操作。

2.根据权利要求1所述的面向共享洗衣机安全的防篡改方法,其特征在于,所述的通信模块支持2G/3G/4G/5G多种通信方式。

3.根据权利要求1所述的面向共享洗衣机安全的防篡改方法,其特征在于,所述的控制模块为MCU控制主板。

4.根据权利要求1所述的面向共享洗衣机安全的防篡改方法,其特征在于,所述的控制中心包括区块链信息交互模块和设备信息交互模块,分别实现与区块链服务器的信息交互和与洗衣机通信模块的信息交互。

5.根据权利要求1所述的面向共享洗衣机安全的防篡改方法,其特征在于,所述的控制中心模块与通信模块通过预先编写好的智能合约与区块链节点服务器进行信息交互。

一种面向共享洗衣机安全的防篡改方法

技术领域

[0001] 本发明涉及区块链技术领域,尤其涉及一种面向共享洗衣机安全的防篡改方法。

背景技术

[0002] 区块链技术,区块链是一种新型去中心化分布式账本技术,能安全地存储数字货币交易或其他数据,特点是存储在区块链上的信息不可伪造和篡改,区块链共识算法驱动区块链上的每个节点都参与到交易的验证过程中,保证区块链上交易都是经过确认可信的,区块链上每个节点都维护一个公共的账本,用于存储区块链网络上所有用户的余额和智能合约数据,任何一个节点对自己所维护的账本的修改都将不被其他节点所承认,从而保证公共账本不可被伪造和篡改。

[0003] 非对称加密算法是一种密钥的保密方法。非对称加密算法需要两个密钥:公开密钥(publickey:简称公钥)和私有密钥(privatekey:简称私钥)。公钥与私钥是一对,如果用公钥对数据进行加密,只有用对应的私钥才能解密。因为加密和解密使用的是两个不同的密钥,所以这种算法叫作非对称加密算法。

[0004] 现有的共享洗衣机行业,共享洗衣机终端主要是由集成控制主板及通信控制模块来控制洗衣机的相关操作,用户通过手机软件终端向远程控制平台发送操作请求,远程控制平台授权后向相应的洗衣机终端发送指令,洗衣机的通信模块接收后传达给控制主板,再由集成程序解析指令进行洗衣机相应操作。但由于洗衣机的通信模块暴露,易被非法替换,直接通过篡改后的通信控制模块向洗衣机发送操作指令的现象比较普遍,严重影响了共享洗衣机行业的公平和安全。

发明内容

[0005] 针对现有技术的不足,本发明公开一种面向共享洗衣机安全的防篡改方法,能够有效保护共享洗衣机的设备安全与数据安全。

[0006] 本发明的目的通过如下的技术方案来实现:

[0007] 一种面向共享洗衣机安全的防篡改方法,其特征在于,所述的共享洗衣机包括通信模块和控制模块,共享洗衣机的控制指令程序集成在所述的控制模块中,所述的共享洗衣机受远程控制中心的控制,所述的远程控制中心对所述的共享洗衣机所有的控制指令均采用非对称加密算法进行加密,公钥保存于远程控制中心,私钥分别保存在洗衣机的通信模块和控制模块中,且所述的共享洗衣机控制指令的访问控制策略和哈希地址均保存在由远程控制中心、洗衣机组成的联盟链上;

[0008] 当终端向远程控制中心发送控制请求时,所述的远程控制中心将所述的控制指令对应的加密指令发送给所述的共享洗衣机的通信模块,通信模块将所述的控制指令上传到联盟链中进行共识,通过后发送给所述的控制模块;所述的控制模块通过对应的私钥解密指令后控制洗衣机执行相关操作。

[0009] 进一步地,所述的通信模块支持2G/3G/4G/5G多种通信方式。

[0010] 进一步地，所述的控制模块为MCU控制主板。

[0011] 进一步地，所述的控制中心包括区块链信息交互模块和设备信息交互模块，分别实现与区块链服务器的信息交互和与洗衣机通信模块的信息交互。

[0012] 进一步地，所述的控制中心模块与通信模块通过预先编写好的智能合约与区块链节点服务器进行信息交互。

[0013] 本发明的有益效果具体如下：

[0014] 本发明公开的面向共享洗衣机安全的防篡改方法，通过区块链+物联网技术，消除共享洗衣机在投入使用时遭遇人为恶意篡改问题，降低合作成本，同时保障共享服务生态的设备安全与数据安全。

[0015] (1)远程控制模块向通信模块发送的指令采用非对称加密算法加密，所生成的加密指令对应区块链上的唯一且不可篡改的交易哈希，非法指令无效；

[0016] (2)通信模块接收远程控制模块的加密指令后，会进一步与区块链进行交互，而只有存储了有效私钥的通信模块才能通过区块链节点的身份验证后，才能正常访问查询区块链上的交易信息，加强了身份验证保障；

[0017] (3)身份认证通过后的通信模块在区块链上验证加密指令的交易哈希是否有效，加强了指令的真实有效；

[0018] (4)洗衣机控制模块用保存的私钥解析出正确的控制指令，才能控制洗衣机操作，保证了控制模块的唯一性，也保证了指令的合法有效性。

附图说明

[0019] 图1为本发明的面向共享洗衣机安全的防篡改方法的流程图。

具体实施方式

[0020] 下面根据附图和优选实施例详细描述本发明，本发明的目的和效果将变得更加明白。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0021] 如图1所示，本发明的面向共享洗衣机安全的防篡改方法，首先要搭建一条联盟链，部署相关业务节点，这里的业务节点包括远程控制中心、洗衣机节点，远程控制中心模块发送的加密指令在联盟链上存证。

[0022] 共享洗衣机包括通信模块和控制模块，共享洗衣机的控制指令程序集成在所述的控制模块中，所述的共享洗衣机受远程控制中心的控制，所述的远程控制中心对所述的共享洗衣机所有的控制指令均采用非对称加密算法进行加密，公钥保存在远程控制中心，私钥分别保存在洗衣机的通信模块和控制模块中，且所述的共享洗衣机控制指令的访问控制策略和哈希地址均保存在联盟链上；

[0023] 当终端向远程控制中心发送控制请求时，所述的远程控制中心将所述的控制指令对应的加密指令发送给所述的共享洗衣机的通信模块，通信模块将所述的控制指令上传到联盟链中，验证加密指令是否存在于联盟链上，验证通过后后通过串口协议发送给洗衣机的控制模块，控制模块通过对应的私钥解密指令后控制洗衣机执行相关操作。

[0024] 洗衣机的控制指令程序烧录至洗衣机控制主板中，洗衣机控制主板内置于洗衣机内部，不向外暴露，通过控制主板可控制洗衣机的相关操作，主要包括洗涤、脱水、设置洗涤

时间、停止洗涤、复位等。

[0025] 进一步地，洗衣机的控制模块为MCU控制主板。

[0026] 进一步地，所述的控制中心模块与通信模块通过预先编写好的智能合约与区块链节点服务器进行信息交互。

[0027] 进一步地，远程控制中心模块包括区块链信息交互模块和设备信息交互模块，分别实现与区块链服务器的信息交互和与洗衣机通信模块的信息交互，远程控制中心通过设备信息交互模块获取到来自用户的操作请求，通过解析请求类型用公钥生成相应的加密指令，再通过区块链信息交互模块在所述联盟链上生成相应的哈希地址，继而将加密指令通过设备信息交互模块指令发送给洗衣机通信模块。

[0028] 进一步地，远程控制中心模块节点和洗衣机数据节点通过智能合约分别存储和验证加密指令。

[0029] 进一步地，远程控制中心模块向通信模组发送加密指令，通信模组接收到加密指令后，与区块链洗衣机数据节点服务器通信，首先，区块链节点会对通信模组的私钥进行身份验证，验证通过后，通信模组可对区块链节点的交易信息进行查询操作，验证该指令密文的哈希地址的真实性，如果验证通过，则将指令通过串口协议发送给洗衣机控制主板；如果验证不通过，则操作无效，指令终止。

[0030] 进一步地，洗衣机控制主板通过自己保存的密钥来解密通信模组发出的加密指令，获取到指令信息原文后，通过控制程序控制洗衣机执行相关操作。

[0031] 所述的通信模块支持2G/3G/4G/5G多种通信方式。

[0032] 本领域普通技术人员可以理解，以上所述仅为发明的优选实例而已，并不用于限制发明，尽管参照前述实例对发明进行了详细的说明，对于本领域的技术人员来说，其依然可以对前述各实例记载的技术方案进行修改，或者对其中部分技术特征进行等同替换。凡在发明的精神和原则之内，所做的修改、等同替换等均应包含在发明的保护范围之内。

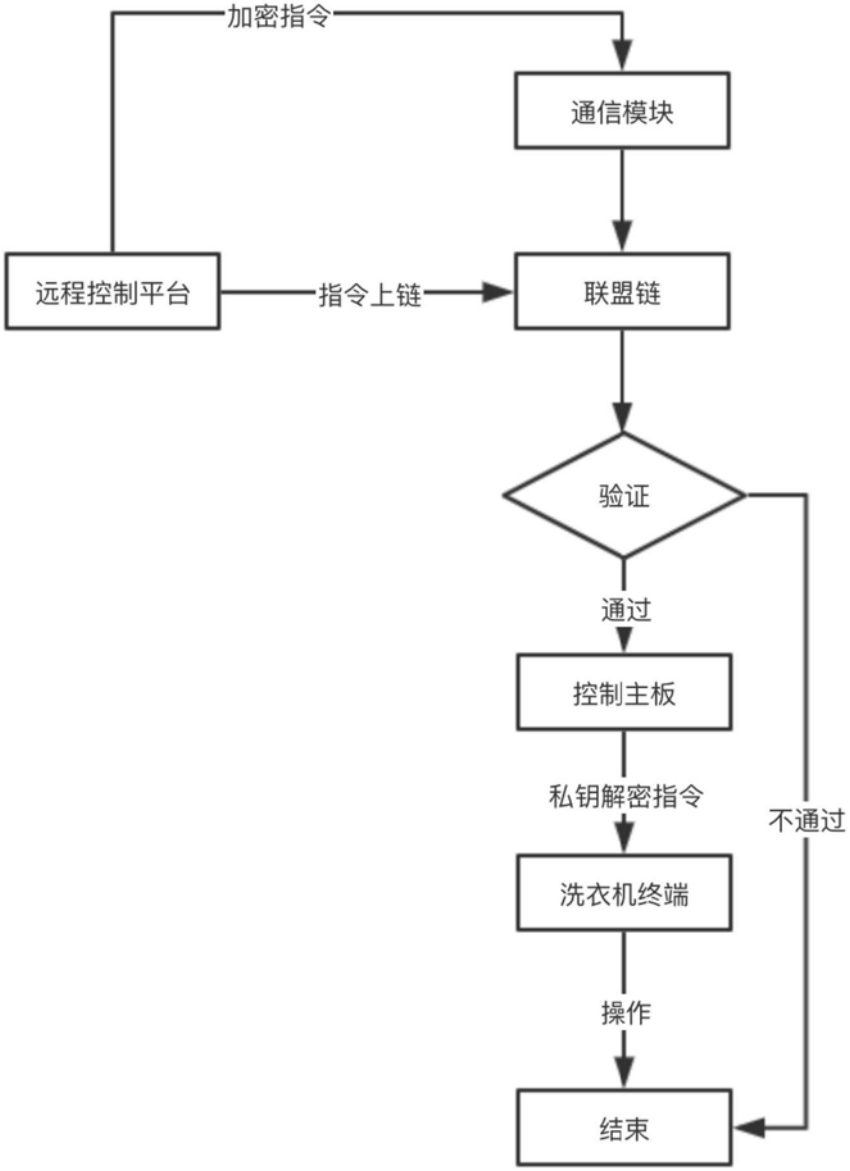


图1