(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 111131229 B
(45)授权公告日 2022.03.01

(21)申请号 201911333042.6
(22)申请日 2019.12.26
(65)同一申请的已公布的文献号
申请公布号 CN 111131229 A
(43)申请公布日 2020.05.08
(73)专利权人 湖南天河国云科技有限公司
地址 410100 湖南省长沙市长沙经济技术开发区星沙产业基地开元东路1318号综合楼308
(72)发明人 谭林 尹海波 李旷 陈昕 杨征
(74)专利代理机构 长沙德恒三权知识产权代理事务所(普通合伙) 43229
代理人 徐仰贵
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/12(2022.01)
(56)对比文件
CN 109087409 A,2018.12.25
CN 110474865 A,2019.11.19
CN 108537489 A,2018.09.14
CN 110049111 A,2019.07.23
审查员 肖丽金

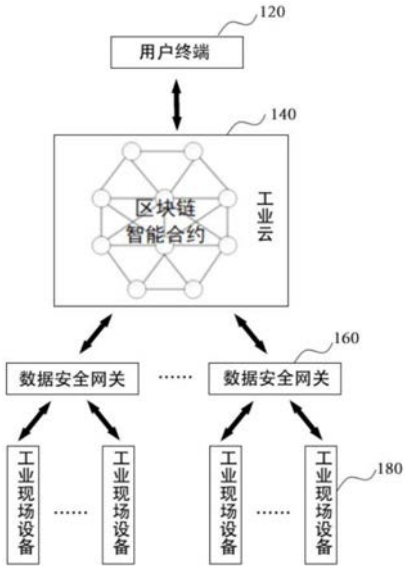
权利要求书2页 说明书12页 附图6页

(54)发明名称

一种基于区块链的工业互联网可信控制方法、装置和系统

(57)摘要

本发明公开了一种基于区块链的工业互联网可信控制方法、装置和系统，所述方法包括：定义和编写工业控制系统的智能合约代码；向区块链网络发送所述智能合约；设置数据安全网关的设备权限以及允许控制及查询的用户账户信息；所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制。本发明通过区块链智能合约的流程、参数定义能力，访问控制能力实现了工业互联网控制系统的安全、可信，解决目前工业互联网控制系统对于安全、可信方面的顾虑，通过一个安全、可信的方式实现工业互联网控制安全，可以促进工业互联网从烟囱式格局走向更加开发之路。



CN 111131229 B

1.一种基于区块链的工业互联网可信控制方法,其特征在于,用于数据安全网关中,所述方法包括:

定义和编写工业控制系统的智能合约代码;

设置所述工业现场设备的访问权限、修改权限、撤销权限、延期权限、可调参数,以及可调参数允许值范围;

向区块链网络发送所述智能合约,设置数据安全网关的设备权限以及允许控制及查询的用户账户信息;

数据安全网关检查区块链网络智能合约状态,并实现本地控制逻辑的更新;

所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制;

其中,所述的撤销权限/延期权限方法包括:将用户控制命令定义为C_i,产生区块链事件E_i,区块链安全系统通过发现E_i,进行警示;

区块链安全系统通过特有权限向区块链发起对C_i撤销/延期指令,执行cancelAction(C_i)或者延期执行:hangUpAction(C_i);

区块链智能合约对执行目标和来源执行权限验证,并产生新事件E_i^{cancel};

数据安全网关一旦检测到事件E_i^{cancel},就会停止对C_i的执行,等待区块确认过程中,数据安全网关可以继续等待其他C_i命令;

数据安全网关一旦检测到事件E_i^{delay},就会停止对C_i的执行,并继续等待E_i^{delay}中的演示后,继续等待区块确认后,实施对工业控制设备的控制。

2.根据权利要求1所述的基于区块链的工业互联网可信控制方法,其特征在于,在向区块链网络发送所述智能合约的步骤之后,所述方法还包括:

订阅或查询区块链网络的智能合约事件日志,所述智能合约事件日志用于触发所述工业控制系统在检测出智能合约事件日志的合约状态发生变更时,在一定时间后依据合约状态变更后的智能合约所定义的流程和参数对工业现场设备进行控制;

所述智能合约事件日志还用于触发预警系统在检测出关键控制命令后进行预警提醒。

3.一种基于区块链的工业互联网可信控制装置,其特征在于,用于数据安全网关中,所述装置包括:

合约创建模块,用于定义和编写工业控制系统的智能合约代码;

发送模块,用于向区块链网络发送所述智能合约;

安全网关权限模块,用于设置数据安全网关的设备权限以及允许控制及查询的用户账户信息;

设备权限模块,用于设置所述工业现场设备的访问权限、修改权限、撤销权限、延期权限、可调参数,以及可调参数允许值范围;

数据安全网关检查区块链网络智能合约状态,并实现本地控制逻辑的更新;

所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制;

其中,设备权限模块中,所述的撤销权限/延期权限方法包括:将用户控制命令定义为

C_i，产生区块链事件E_i，区块链安全系统通过发现E_i，进行警示；区块链安全系统通过特有权限向区块链发起对C_i撤销/延期指令，执行cancelAction(C_i)或者延期执行：hangUpAction(C_i)；

区块链智能合约对执行目标和来源执行权限验证，并产生新事件E_i^{cancel}；

数据安全网关一旦检测到事件E_i^{cancel}，就会停止对C_i的执行，等待区块确认过程中，数据安全网关可以继续等待其他C_i命令；

数据安全网关一旦检测到事件E_i^{delay}，就会停止对C_i的执行，并继续等待E_i^{delay}中的演示后，继续等待区块确认后，实施对工业控制设备的控制。

4.根据权利要求3所述的基于区块链的工业互联网可信控制装置，其特征在于，所述装置还包括：

操作变更模块，用于订阅或查询区块链网络的智能合约事件日志，所述智能合约事件日志用于触发所述工业控制系统在检测出智能合约事件日志的合约状态发生变更时，在一定时间后依据合约状态变更后的智能合约所定义的流程和参数对工业现场设备进行控制；

所述智能合约事件日志还用于触发预警系统在检测出关键控制命令后进行预警提醒。

5.一种基于区块链的工业互联网可信控制系统，其特征在于，包括：

数据安全网关，与工业控制系统连接，用于定义和编写工业控制系统的智能合约代码，设置数据安全网关的设备权限以及允许控制及查询的用户账户信息，所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制；

区块链网络，分别与用户终端和数据安全网关连接，用于接收来自数据安全网关的智能合约代码并初始化数据安全网关的设备权限和控制状态；

其中，所述的数据安全网关用于执行如权利要求1-2任一所述的方法步骤。

6.一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行如权利要求1-2任一所述的方法步骤。

一种基于区块链的工业互联网可信控制方法、装置和系统

技术领域

[0001] 本发明涉及工业控制系统安全领域，具体涉及一种基于区块链的工业互联网可信控制方法、装置和系统。

背景技术

[0002] 工业互联网要求实现产业上下游、跨领域的广泛互联互通，打破“信息孤岛”，促进集成共享。目前工业互联网系统还处于企业内部工业互联阶段，无法实现真正意义上的工业互联网。制造业及周边产业之间还是依赖于传统沟通方法实现信息交流和沟通，无法实现制造协同。现有的工业互联网控制系统存在以下缺点：

[0003] 控制系统安全问题：目前，制造系统的主要问题是工业制造控制系统是企业核心生产系统，对安全等级要求高，对于接入工业互联网使得控制系统存在安全隐患；另外，控制系统的安全审计主要依赖控制系统自身安全审计功能，无法有效实现控制主体、来源安全审计和识别，同时，对控制流程调整依赖于内部系统本身，如果接入工业互联网，无法保证其流程的可信度。

[0004] 控制系统网络安全问题：现有系统基于内部局域网络构建，无法经受开放工业互联网的安全冲击，通过传统的系统间软件接口无法确保控制系统在可靠、安全、可信方面得到有效保障，成为阻碍工业互联网发展的绊脚石。

[0005] 针对上述的问题，目前尚未提出有效的解决方案。

发明内容

[0006] 有鉴于此，本发明的目的在于提供一种基于区块链的工业互联网可信控制方法、装置和系统，能够实现工业互联网控制系统控制流程的安全、可信。

[0007] 本发明实施例的第一方面提供了一种基于区块链的工业互联网可信控制方法，用于数据安全网关中，所述方法包括：

[0008] 定义和编写工业控制系统的智能合约代码；

[0009] 向区块链网络发送所述智能合约；

[0010] 设置数据安全网关的设备权限以及允许控制及查询的用户账户信息；

[0011] 所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制。

[0012] 进一步地，在向区块链网络发送所述智能合约的步骤之后，所述方法还包括：

[0013] 设置所述工业现场设备的访问权限、修改权限、可调参数，以及可调参数允许值范围；

[0014] 订阅或查询区块链网络的智能合约事件日志，所述智能合约事件日志用于触发所述工业控制系统在检测出智能合约事件日志的合约状态发生变更时，在一定时间后依据合约状态变更后的智能合约所定义的流程和参数对工业现场设备进行控制；

[0015] 所述智能合约事件日志还用于触发预警系统在检测出关键控制命令后进行预警

提醒。

[0016] 本发明实施例的第二方面提供了一种基于区块链的工业互联网可信控制方法，用于区块链网络中，所述方法包括：

[0017] 接收来自数据安全网关的智能合约代码，所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制；

[0018] 初始化数据安全网关的设备权限和控制状态。

[0019] 进一步地，在接收来自数据安全网关的智能合约代码的步骤之后，所述方法还包括：

[0020] 接收用户对智能合约的操作请求信息；

[0021] 验证所述用户操作请求信息所对应的操作权限，当验证成功时，区块链网络根据用户操作请求信息，修改智能合约，并更新智能合约日志的合约状态；

[0022] 所述操作请求信息包括修改、取消或延期当前指定待确认指令的一种或多种。

[0023] 本发明实施例的第三方面提供了一种基于区块链的工业互联网可信控制装置，用于数据安全网关中，所述装置包括：

[0024] 合约创建模块，用于定义和编写工业控制系统的智能合约代码；

[0025] 发送模块，用于向区块链网络发送所述智能合约；

[0026] 安全网关权限模块，用于设置数据安全网关的设备权限以及允许控制及查询的用户账户信息；

[0027] 所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制。

[0028] 进一步地，所述装置还包括：

[0029] 设备权限模块，用于设置所述工业现场设备的访问权限、修改权限、可调参数，以及可调参数允许值范围；

[0030] 操作变更模块，用于订阅或查询区块链网络的智能合约事件日志，所述智能合约事件日志用于触发所述工业控制系统在检测出智能合约事件日志的合约状态发生变更时，在一定时间后依据合约状态变更后的智能合约所定义的流程和参数对工业现场设备进行控制；

[0031] 所述智能合约事件日志还用于触发预警系统在检测出关键控制命令后进行预警提醒。

[0032] 本发明实施例的第四方面提供了一种基于区块链的工业互联网可信控制装置，用于区块链网络中，所述装置包括：

[0033] 合约接收模块，用于接收来自数据安全网关的智能合约代码，所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制；

[0034] 初始化模块，用于初始化数据安全网关的设备权限和控制状态。

[0035] 进一步地，所述装置还包括：

[0036] 请求接收模块，用于接收用户对智能合约的操作请求信息；

[0037] 合约更新模块，用于验证所述用户操作请求信息所对应的操作权限，当验证成功时，区块链网络根据用户操作请求信息，修改智能合约，并更新智能合约日志的合约状态；

[0038] 所述操作请求信息包括修改智能合约、取消当前智能合约控制指令或延期当前智能合约控制指令中的一种或多种。

[0039] 本发明实施例的第五方面提供了一种基于区块链的工业互联网可信控制系统，所述系统包括：

[0040] 数据安全网关，与工业控制系统连接，用于定义和编写工业控制系统的智能合约代码，设置数据安全网关的设备权限以及允许控制及查询的用户账户信息，所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制；

[0041] 区块链网络，分别与用户终端和数据安全网关连接，用于接收来自数据安全网关的智能合约代码并初始化数据安全网关的设备权限和控制状态。

[0042] 本发明实施例的第六方面提供了一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行如下方法步骤：

[0043] 定义和编写工业控制系统的智能合约代码；

[0044] 向区块链网络发送所述智能合约；

[0045] 设置数据安全网关的设备权限以及允许控制及查询的用户账户信息；

[0046] 所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制。

[0047] 在本发明实施例中，数据安全网关定义和编写工业控制系统的智能合约代码，并将智能合约代码发送给区块链网络，区块链网络初始化数据安全网关的设备权限以及允许控制和查询的用户账户信息，通过区块链智能合约的流程、参数定义能力，安全审计能力，访问控制能力实现了工业互联网控制系统的安全、可信，解决目前工业互联网控制系统对于安全、可信方面的顾虑，通过一个安全、可信的方式实现工业互联网控制安全，可以促进工业互联网从烟囱式格局走向更加开发之路。

附图说明

[0048] 为了更清楚地说明本发明实施例中的技术方案，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一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0049] 图1是本发明各个实施例所涉及的工业互联网的一种实施环境的结构示意图；

[0050] 图2是本发明一个实施例提供的一种基于区块链的工业互联网可信控制方法的流程图；

[0051] 图3是本发明另一个实施例提供的一种基于区块链的工业互联网可信控制方法的流程图；

[0052] 图4是本发明实施例提供的一种基于区块链的工业互联网可信控制方法与用户交互过程的一种时序图；

[0053] 图5是本发明实施例提供的一种基于区块链的工业互联网可信控制方法关于取消或延期操作过程的时序图；

[0054] 图6是本发明一个实施例提供的一种基于区块链的工业互联网可信控制装置的结

构示意图；

[0055] 图7是本发明另一个实施例提供的一种基于区块链的工业互联网可信控制装置的结构示意图；

[0056] 图8是本发明实施例提供的终端设备的示意图。

具体实施方式

[0057] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本发明实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本发明。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本发明的描述。

[0058] 为了说明本发明所述的技术方案，下面通过具体实施例来进行说明。

[0059] 请参阅图1，其示出了本发明各个实施例所涉及的工业互联网的一种实施环境的结构示意图。该实施环境包括：用户终端120、区块链网络140、数据安全网关160和工业现场设备180。

[0060] 用户终端120可以是手机、平板电脑、电子书阅读器、便携式计算机和台式计算机等。

[0061] 多个工业现场设备180组成工业控制系统，工业控制系统可以控制机床、机器臂，机器人等智能设备进行工业生产，控制系统安全可以保障设备正常、可信运转。

[0062] 区块链网络140基于分布式账本技术构建的数据库技术，采用分布式点对点技术构建区块链网络140，具有不可篡改、安全、可信的特点，基于区块链技术构建的工业互联网控制系统，可以从网络层面实现网络攻击的防御，有效抵御外部系统的恶意攻击。

[0063] 区块链网络140与用户终端120进行数据交互，显示工业现场各种系统、设备的参数状态，对工业现场设备180所连接智能设备进行控制；所述区块链网络140，利用虚拟化技术构建分布式的多个区块链节点，各个区块链节点均连接云端服务器数据库，各个节点之间通过构建小世界网络进行相互验证，保证各个节点的可信。其中，所述区块链节点通过共识机制生成区块，对区块进行验证，并对通过验证的数据包采用区块链无中心化存储方式并加密存储至所述云端服务器数据库，以执行智能合约的方式实现数据共享。

[0064] 其中，智能合约是以控制(control)作为基本元素来构建的，控制是工业控制系统网络的基本控制单位，表示控制者对工业现场设备180的控制。一个控制过程通常由一组相互关联的控制组成。

[0065] 具体地，控制是一个五元组C(p,e,c,r,tc)，含义是人p(person)向工业现场设备180(equipment)发出指令，如果指令c(command)达成，就产生结果r(result)。其中，指令c和结果r的值是布尔值。值为true表示指令已达成(或结果已完成)，值为false表示指令未达成(或结果未完成)；而tc(time-constraints)表示该控制的有效期，tc为true，控制才会有效。

[0066] 其中，一个控制的生命周期内可能有5种不同的状态。

[0067] (一)激活(activation)：指令c和结果r都为false，时间未超出控制的有效期。表示控制有效，在等待指令c的达成和结果r的完成；

[0068] (二)就绪(ready)：指令c为true，结果r为false，时间未超出控制的有效期，表示

控制已生效且指令c已经达成,在等待结果r的完成;

[0069] (三)满足(satisfy):指令c和结果r都为true,表示指令c已达成,结果r也已完成,控制已被履行;

[0070] (四)过期(expire):指令c和结果r都为false,时间已超出控制的有效期。表示在控制失效时,指令c未能达成而结果r也未能完成;

[0071] (五)违约(violate):指令c为true,但结果r为false,时间已超出控制的有效期。表示当控制失效时,尽管已达成了指令c,但仍然未履行其控制完成结果r,已经违约。

[0072] 其中,控制有效期是一个二元组tc:=(cact,cbas),式中cact表示控制进入激活(activation)状态之后,对指令c的完成时间限制;cbas表示控制进入就绪(ready)状态之后,对结果r的完成时间限制。若这两个限制满足,tc为true;否则,tc为false。

[0073] 其中,一个动作可以表示为action:=actionname(executor,object,input,output),式中:actionname是动作的名称,executor是动作的执行者,object是动作的作用对象,input是输入参数,output是输出参数(act,exectuor是必需的(required),而object,input和output都是可选的(optional))。动作的值是一个布尔值,action=fasle表示没有完成该动作,action=true表示该动作已完成。动作的默认值为false。

[0074] 工业互联网智能合约就是定义在一组控制之上的有限自动机SC:=(CC,A,S,s_0,δ,F),其中,CC=$\{C_1,C_2,...,C_n\}$是一个有限的控制集合;

[0075] A是这些控制涉及到的动作的集合(包括超时动作,也就是时间超出了控制的有效期);S=$\{s_0,s_1,s_2,...,s_m\}$是一个有限的状态集合。状态si由CC中所有控制的状态共同决定;

[0076] s0是初始状态,其中,CC中所有控制或者处于激活状态(有条件控制),或者就绪状态(无条件控制);

[0077] δ:S×A→S是状态变迁函数A中的动作会促使CC中承诺的状态发生变化,从而引起智能合约的状态发生变化;

[0078] F∈S是一个有限的终止状态集合。

[0079] 所述数据安全网关160,用于连接并采集至少一个工业现场设备180的数据,并通过互联网将所采集的数据传输至所述区块链网络140,数据安全网关160中创建虚拟机,在虚拟机中运行虚拟化的数据加密程序。

[0080] 每个区块链节点管理N个数据安全网关160,每个数据安全网关160由M个区块链节点管理,其中N≥1,M≥2;当某个区块链节点因故障失效时,其余区块链节点同时完成与用户终端120和数据安全网关160的通信;在一个数据安全网关160对应M个区块链节点中,选择距离数据安全网关最近的1个区块链节点作为目标区块链节点,负责该数据安全网关160与用户终端120的通信,以提高通信效率。

[0081] 所述区块链节点与数据安全网关160之间采用非对称加密算法对数据生成数字签名并进行数据加密;其中,数字签名用以验证数据的本真性以及数据是否被篡改,数据加密使数据只能被确定的接收方接收。

[0082] 所述非对称加密算法由私钥和公钥组成,使用公钥加密时,使用对应的私钥进行解密,使用私钥加密时,使用对应的公钥进行解密;

[0083] 数据加密过程是:数据经过双SHA256运算后生成32位的唯一哈希值,再使用私钥

加密哈希值生成数字签名，将数字签名和数据使用接收方的公钥进行加密得到加密数据。

[0084] 其中，私钥生产过程依赖于数据安全网关160内部处理器的芯片ID和加密算法，确保设备私钥的唯一性和不可篡改特性。私钥由设备存储，不允许离开存储装置，公钥作为区块链对设备唯一管理标识。计算机程序只接受区块链已经确认的状态，对工业现场设备180进行控制。

[0085] 区块链节点之间通过工作量证明的共识机制达成共识，最先完成工作量证明运算的区块链节点获得生成新区块的权利并成为此次共识过程的主节点，其余区块链节点为区块链从节点，区块链从节点进行验证统一存储区块链主节点生成的区块，保证数据的一致性，下次最先完成工作量证明运算的区块链节点成为新的区块链主节点；

[0086] 区块链主节点将生成的新区块广播给区块链从节点，区块链从节点对新区块进行验证，并回复验证结果和数据签名至区块链主节点，区块链主节点收集回复结果，根据少数服从多数的原则，如果多数区块链节点赞成该区块，区块链主节点将新区块和验证结果重新广播，区块链从节点存储新区块。

[0087] 区块链节点执行智能合约实现工业现场设备180之间数据共享，智能合约规定了数据共享的条件，所述条件由数据提供者制定，目标区块链节点执行智能合约，根据约束条件输出结果，对数据进行加密后发送至某数据安全网关160，该数据安全网关160接收后进行解密，完成相应的任务。

[0088] 其中，本发明基于区块链智能合约技术和内置区块链智能合约Dapp的数据安全网关160，实现工业互联网控制系统网络进行的安全保护，以及工业互联网控制系统的控制可信安全。

[0089] 下面通过几个具体的实施例对本发明实施便提供的工业互联网可信控制方案进行详细介绍和说明。

[0090] 请参阅图2，本发明实施例的第一方面提供了一种基于区块链的工业互联网可信控制方法，用于数据安全网关中，所述方法包括：

[0091] 步骤S102，定义和编写工业控制系统的智能合约代码；

[0092] 步骤S104，向区块链网络发送所述智能合约；

[0093] 步骤S106，设置数据安全网关的设备权限以及允许控制及查询的用户账户信息；

[0094] 所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制。

[0095] 其中，智能合约为运行在基于分布式账本技术的区块链网络140平台上面的软件代码，可以在区块链上执行，是图灵机完备的，可以在区块链之上保持状态，执行的业务逻辑。

[0096] 本发明采用区块链智能合约技术来定义工业控制系统的控制流程，参数、权限，安全审计、日志记录，在此基础上，实现安全、可信的远程控制系统。智能合约通过代码定义控制系统的执行流程，由区块链数据安全网关160实现智能合约的控制流程执行。控制流程通过智能合约代码进行定义，智能合约的代码可以经过审核、安全审计后发布到区块链，后面所有智能合约的操作都需要经过区块链授权才可以操作或者修改控制流程或者参数。

[0097] 系统控制参数同样由智能合约的状态定义，对智能合约状态的修改均通过智能合约来记录，确保只有在智能合约内经过授权的用户才有权限修改参数。

[0098] 区块链数据安全网关160是基于区块链的智能控制单元，属于具有Dapp功能的数据安全网关160装置，它通过和区块链网络140交互，获取该设备的流程和状态信息，按智能合约的程序过程进行控制工作，属于受区块链智能合约控制的控制单元。

[0099] 进一步地，在向区块链网络发送所述智能合约的步骤之后，所述方法还包括：

[0100] 设置所述工业现场设备的访问权限、修改权限、可调参数，以及可调参数允许值范围；

[0101] 订阅或查询区块链网络的智能合约事件日志，所述智能合约事件日志用于触发所述工业控制系统在检测出智能合约事件日志的合约状态发生变更时，在一定时间后依据合约状态变更后的智能合约所定义的流程和参数对工业现场设备进行控制。

[0102] 预警系统检测智能合约事件日志，并对关键控制命令具有预警提醒，并通过特有取消或延期权限，对控制操作予以取消或延期。

[0103] 具体的，基于智能合约的控制单元工作流程如下：

[0104] a)基于控制系统的特殊性，定义和编写控制系统的智能合约(Smart Contract)；

[0105] b)设计控制系统可调参数($Params_i$)，及其允许值范围($Range_{start}^{end}$)、访问权限($Permission_{access}$)、修改权限($Permission_{mondify}$)、撤销权限($Permission_{cancel}$)、延期权限($Permission_{delay}$)，权限采用基于角色($Role_i$)和用户组($UserGroup_i$)和设备组($DeviceGroup_i$)结合的方式进行授权；权限包括：只读、可写、可调、可取消、可延期，角色可以任意组合上述部分权限列表，并赋予特定用户组；用户组可以关联设备组进行资源分配；

[0106] c)在区块链网络中发布智能合约(deployContract)，初始化(initialize)并设置允许控制(addControlPermission)、查询的账户信息(addAccessPermission())，设置数据安全网关160设备权限(addAllowedDevice(device,deviceGroup))；

[0107] d)现场安装数据安全网关160，并接入区块链网络140，数据安全网关160开始依据智能合约定义的流程和参数开始工作；

[0108] e)如果希望调整工业控制流程，通过相应的软件和账户私钥key修改智能合约参数，达到修改工业控制流程的目的；修改记录、安全均由区块链及智能合约来保障；

[0109] f)数据安全网关160检查区块链网络140智能合约状态，并实现本地控制逻辑的更新，实现由区块链完成系统的控制修改流程。

[0110] 本发明的方法应用于基于区块链的工业互联网可信控制系统的数据安全网关，图4和图5显示了发明实施例提供的方法与用户交互过程的时序图，由时序图可知，本发明实施例在实施环境下总体控制流程如下：

[0111] 1)定义工业控制逻辑及允许暴露的控制接口，抽象为控制状态和对状态的访问，状态定义为Si，对状态的操作函数为$F_{read}(S_i)$，$F_{write}(S_i)$；

[0112] 2)设计访问(读)权限RP_i，控制(写)权限组WP_i，对控制接口定义访问权限Ai；

[0113] 3)定制智能合约策略C，实现合约功能编码，绑定相关用户权限C(S_i,RP_i,WP_i,F_{read}(Si),$F_{write}(S_i)$)；

[0114] 4)在区块链部署智能合约deploy(C)，初始化相关权限配置C.init(S_i,RP_i,WP_i)，设定安全网关公钥地址C.initDevices($address_{device}$,S_i)；

[0115] 5)初始化安全网关智能合约地址addr，安全网关按智能合约初始化控制逻辑C.readParams()，进入区块链控制状态；

[0116] 6)外部用户如果有控制策略需要调整(生产计划调整、产品参数调整等),通过智能合约执行参数调整工作C.writeParam(address$_{device}$,S_i),如图4所示用户向区块链提交控制请求;

[0117] 7)智能合约检查用户操作权限onlyReadPermission(address$_{sender}$,address$_{device}$),onlyWritePermission(address$_{sender}$,address$_{device}$),执行动作是否被允许,参数范围是否具有调整权限allowedRange(address$_{sender}$,address$_{device}$,value),一切权限和参数检查通过后,智能合约修改智能合约状态,记录响应日志,如图4所示智能合约和区块链的验证过程;

[0118] 8)数据安全网关通过订阅/查询智能合约日志subscribeEvent(address$_{device}$),发现状态变更readControlStatus(address$_{sender}$),并等待一定时间后(区块稳定时间周期),依据新控制指令工作readRunParams(address$_{sender}$),如图4所示数据安全网关读取合约日志流程,并等待区块确认,最后对工业现场设备进行控制逻辑调整,实时安全可信控制。

[0119] 其中,数据安全网关160通过区块链日志记录实现对过程的记录,控制参数和权限由智能合约管理,数据安全网关确保实体对应,并利用区块链不可篡改能力,实现可信控制。工控装置对于状态读取,执行,控制反馈通过区块链来执行,实现可信记录。用户操作必须经过合约授权,并在合约中记录,实现用户侧的可信控制。

[0120] 控制系统存在误操作或者攻击发现,可以紧急取消/延期当前操作。本发明提供如图5所示控制撤销流程。本发明实施例在实施环境下对控制命令的撤销制流程如下:

[0121] 1)当系统检测到异常控制逻辑提交到区块链,并在数据安全网关等待确认期间,可以执行撤销或延期执行,确保工业控制系统的高度安全。将用户控制命令定义为C_i,产生区块链事件E_i,安全系统通过发现E_i,进行警示。

[0122] 2)安全系统警示系统通过特有权限向区块链发起对C_i取消/延期指令,执行cancelAction(C_i)或者延期执行:hangUpAction(C_i);

[0123] 3)区块链智能合约对执行目标和来源执行权限验证,并产生新事件E_i^{cancel};

[0124] 4)数据安全网关一旦检测到事件E_i^{cancel},就会停止对C_i的执行,等待区块确认过程中,数据安全网关可以继续等待其他C_i命令;

[0125] 5)数据安全网关一旦检测到事件E_i^{delay},就会停止对C_i的执行,并继续等待E_i^{delay}中的演示后,继续等待区块确认后,实施对工业控制设备的控制。

[0126] 在本发明实施例中,数据安全网关定义和编写工业控制系统的智能合约代码,并将智能合约代码发送给区块链网络,区块链网络初始化数据安全网关的设备权限以及允许控制和查询的用户账户信息,通过区块链智能合约的流程、参数定义能力,安全审计能力,访问控制能力实现了工业互联网控制系统的安全、可信,解决目前工业互联网控制系统对于安全、可信方面的顾虑,通过一个安全、可信的方式实现工业互联网控制安全,可以促进工业互联网从烟囱式格局走向更加开发之路。

[0127] 请参阅图3,本发明实施例的第二方面提供了一种基于区块链的工业互联网可信控制方法,用于区块链网络中,所述方法包括:

[0128] 步骤S202,接收来自数据安全网关的智能合约代码;

[0129] 步骤S204,初始化数据安全网关的设备权限和控制状态。

[0130] 进一步地，在接收来自数据安全网关的智能合约代码的步骤之后，所述方法还包括：

[0131] 接收用户对智能合约的操作请求信息；

[0132] 验证所述用户操作请求信息所对应的操作权限，当验证成功时，区块链网络根据用户操作请求信息，修改智能合约，并更新智能合约日志的合约状态；

[0133] 所述操作请求信息包括修改智能合约、取消当前智能合约控制指令或延期当前智能合约控制指令中的一种或多种。

[0134] 请参阅图6，本发明实施例的第三方面提供了一种基于区块链的工业互联网可信控制装置20，用于数据安全网关160中，所述装置包括：

[0135] 合约创建模块202，用于定义和编写工业控制系统的智能合约代码；

[0136] 发送模块204，用于向区块链网络发送所述智能合约；

[0137] 盒子权限模块206，用于设置数据安全网关的设备权限以及允许控制及查询的用户账户信息；

[0138] 所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制。

[0139] 进一步地，所述装置还包括：

[0140] 设备权限模块，用于设置所述工业现场设备的访问权限、修改权限、可调参数，以及可调参数允许值范围；

[0141] 操作变更模块，用于订阅或查询区块链网络的智能合约事件日志，所述智能合约事件日志用于触发所述工业控制系统在检测出智能合约事件日志的合约状态发生变更时，在一定时间后依据合约状态变更后的智能合约所定义的流程和参数对工业现场设备进行控制；

[0142] 所述智能合约事件日志还用于触发预警系统在检测出关键控制命令后进行预警提醒。

[0143] 请参阅图7，本发明实施例的第四方面提供了一种基于区块链的工业互联网可信控制装置30，用于区块链网络中140，所述装置包括：

[0144] 合约接收模块302，用于用于接收来自数据安全网关的智能合约代码，所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制；

[0145] 初始化模块304，用于初始化数据安全网关的设备权限和控制状态。

[0146] 进一步地，所述装置还包括：

[0147] 请求接收模块，用于接收用户对智能合约的操作请求信息；

[0148] 合约更新模块，用于验证所述用户操作请求信息所对应的操作权限，当验证成功时，区块链网络根据用户操作请求信息，修改智能合约，并更新智能合约日志的合约状态；

[0149] 所述操作请求信息包括修改智能合约、取消当前智能合约控制指令或延期当前智能合约控制指令中的一种或多种。

[0150] 本发明实施例的第五方面提供了一种基于区块链的工业互联网可信控制系统，所述系统包括：

[0151] 数据安全网关160，与工业控制系统连接，用于定义和编写工业控制系统的智能合

约代码，设置数据安全网关的设备权限和允许控制及查询的用户账户信息，所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制，其中工业控制系统由多个工业现场设备180组成。

[0152] 区块链网络140，分别与用户终端120和数据安全网关140连接，用于接收来自数据安全网关160的智能合约代码并初始化数据安全网关160的设备权限和控制状态。

[0153] 在本发明实施例中，数据安全网关定义和编写工业控制系统的智能合约代码，并将智能合约代码发送给区块链网络，区块链网络初始化数据安全网关的设备权限以及允许控制和查询的用户账户信息，通过区块链智能合约的流程、参数定义能力，安全审计能力，访问控制能力实现了工业互联网控制系统的安全、可信，解决目前工业互联网控制系统对于安全、可信方面的顾虑，通过一个安全、可信的方式实现工业互联网控制安全，可以促进工业互联网从烟囱式格局走向更加开发之路。

[0154] 图7是本发明一实施例提供的终端设备的示意图。如图7所示，该实施例的终端设备10包括：处理器100、存储器101以及存储在所述存储器101中并可在所述处理器100上运行的计算机程序102，例如进行基于区块链的工业互联网可信控制方法的程序。所述处理器100执行所述计算机程序102时实现上述方法实施例中的步骤，例如，图1所示的S102、S104和S106的步骤。或者，所述处理器100执行所述计算机程序102时实现上述各装置实施例中各模块/单元的功能，例如图4所示的合约创建模块202、发送模块204、安全网关权限模块206的功能。

[0155] 示例性的，所述计算机程序102可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器101中，并由所述处理器100执行，以完成本发明。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述所述计算机程序102在终端设备10中的执行过程。例如，所述计算机程序102可以被分割成合约创建模块202、发送模块204和安全网关权限模块206(虚拟装置中的模块)，各模块具体功能如下：

[0156] 合约创建模块202，用于定义和编写工业控制系统的智能合约代码；

[0157] 发送模块204，用于向区块链网络发送所述智能合约；

[0158] 盒子权限模块206，用于设置数据安全网关的设备权限以及允许控制及查询的用户账户信息；

[0159] 所述智能合约用于触发所述工业控制系统依据所述智能合约代码定义的流程和参数对工业现场设备进行控制。

[0160] 所述终端设备10可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。终端设备10可包括，但不仅限于，处理器100、存储器101。本领域技术人员可以理解，图4仅仅是终端设备10的示例，并不构成对终端设备10的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述终端设备还可以包括输入输出设备、网络接入设备、总线等。

[0161] 所述处理器100可以是中央处理单元(Central Processing Unit,CPU)，还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、

分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0162] 所述存储器101可以是终端设备10的内部存储单元，例如终端设备10的硬盘或内存。所述存储器101也可以是终端设备10的外部存储设备，例如所述终端设备10上配备的插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)等。进一步地，所述存储器101还可以既包括终端设备10的内部存储单元也包括外部存储设备。所述存储器101用于存储所述计算机程序以及终端设备10所需的其他程序和数据。所述存储器101还可以用于暂时地存储已经输出或者将要输出的数据。

[0163] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中，上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。另外，各功能单元、模块的具体名称也只是为了便于相互区分，并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0164] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述或记载的部分，可以参见其它实施例的相关描述。

[0165] 本领域普通技术人员可以意识到，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、或者计算机软件和电子硬件的结合来实现。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。

[0166] 在本发明所提供的实施例中，应该理解到，所揭露的装置/终端设备和方法，可以通过其它的方式实现。例如，以上所描述的装置/终端设备实施例仅仅是示意性的，例如，所述模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通讯连接可以是通过一些接口，装置或单元的间接耦合或通讯连接，可以是电性，机械或其它的形式。

[0167] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0168] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0169] 所述集成的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实现上述实施例方法中的全部或部分流程，也可以通过计算机程序来指令相关的硬件来完成，所述的计

算机程序可存储于一计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机程序包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括：能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、电载波信号、电信信号以及软件分发介质等。需要说明的是，所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如在某些司法管辖区，根据立法和专利实践，计算机可读介质不包括电载波信号和电信信号。

[0170] 以上所述实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所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；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围，均应包含在本发明的保护范围之内。

[0171] 以上所述实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解，其依然可以对前述各实施例所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；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围，均应包含在本发明的保护范围之内。

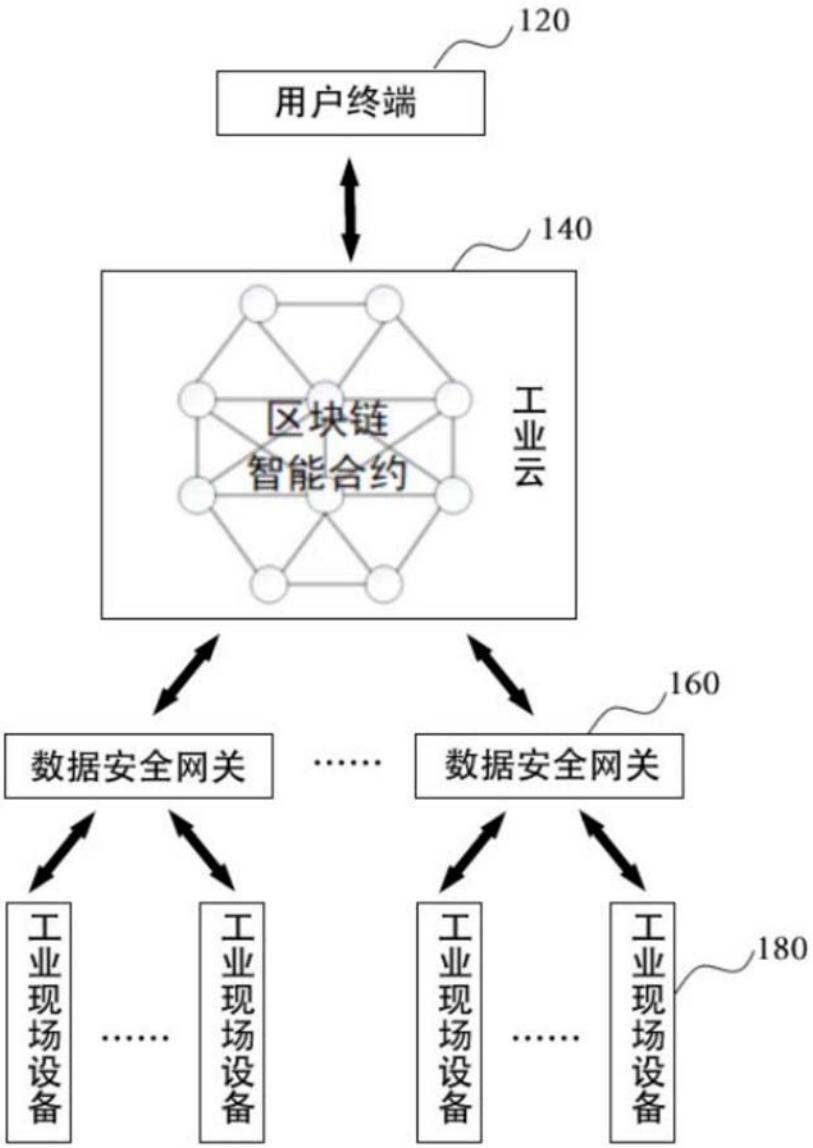

120
用户终端
140
区块链
智能合约
工业云
160
数据安全网关
……
数据安全网关
工业现场设备
……
工业现场设备
工业现场设备
……
工业现场设备
180

图1

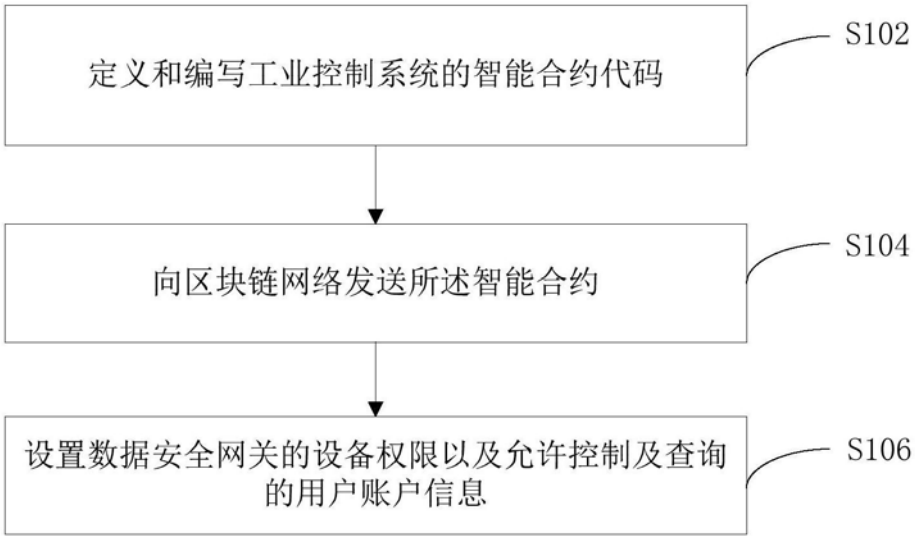

定义和编写工业控制系统的智能合约代码
S102
向区块链网络发送所述智能合约
S104
设置数据安全网关的设备权限以及允许控制及查询的用户账户信息
S106

图2

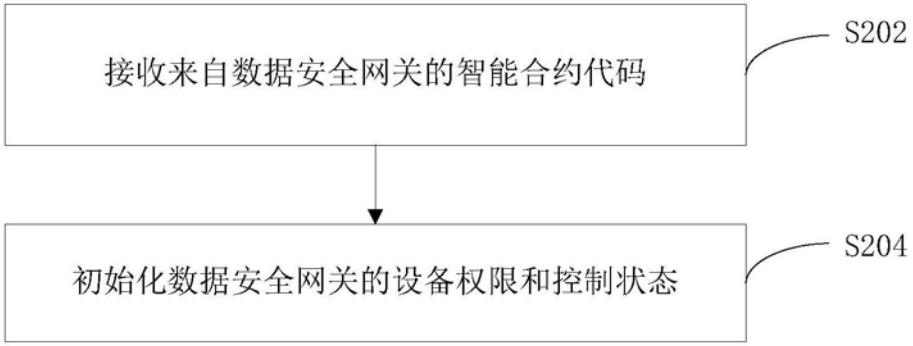

接收来自数据安全网关的智能合约代码
S202
初始化数据安全网关的设备权限和控制状态
S204

图3

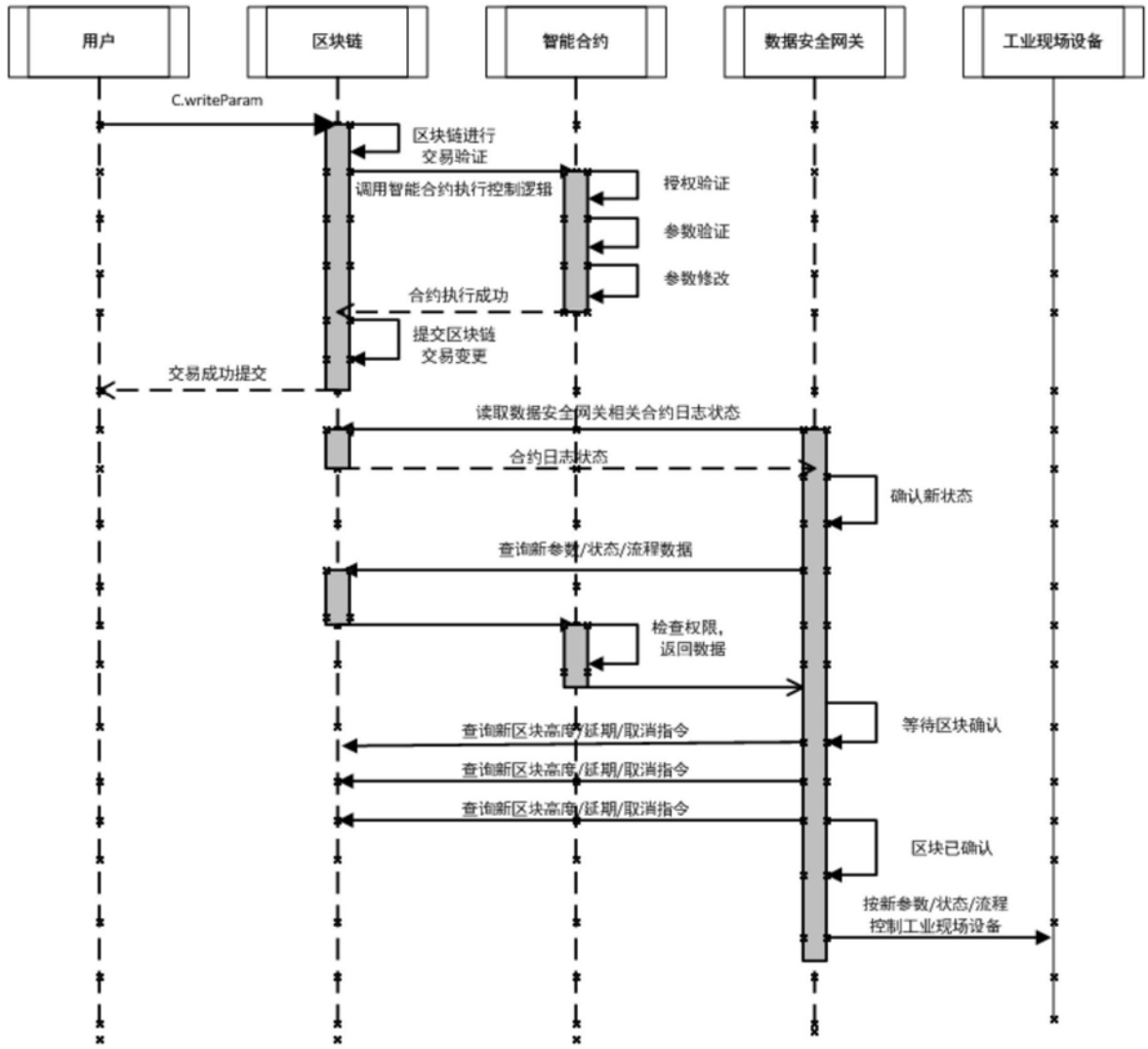

用户
区块链
智能合约
数据安全网关
工业现场设备
C.writeParam
区块链进行
交易验证
调用智能合约执行控制逻辑
授权验证
参数验证
参数修改
合约执行成功
提交区块链
交易变更
交易成功提交
读取数据安全网关相关合约日志状态
合约日志状态
确认新状态
查询新参数/状态/流程数据
检查权限,
返回数据
等待区块确认
查询新区块高度/证期/取消指令
查询新区块高度/证期/取消指令
查询新区块高度/证期/取消指令
区块已确认
按新参数/状态/流程
控制工业现场设备

图4

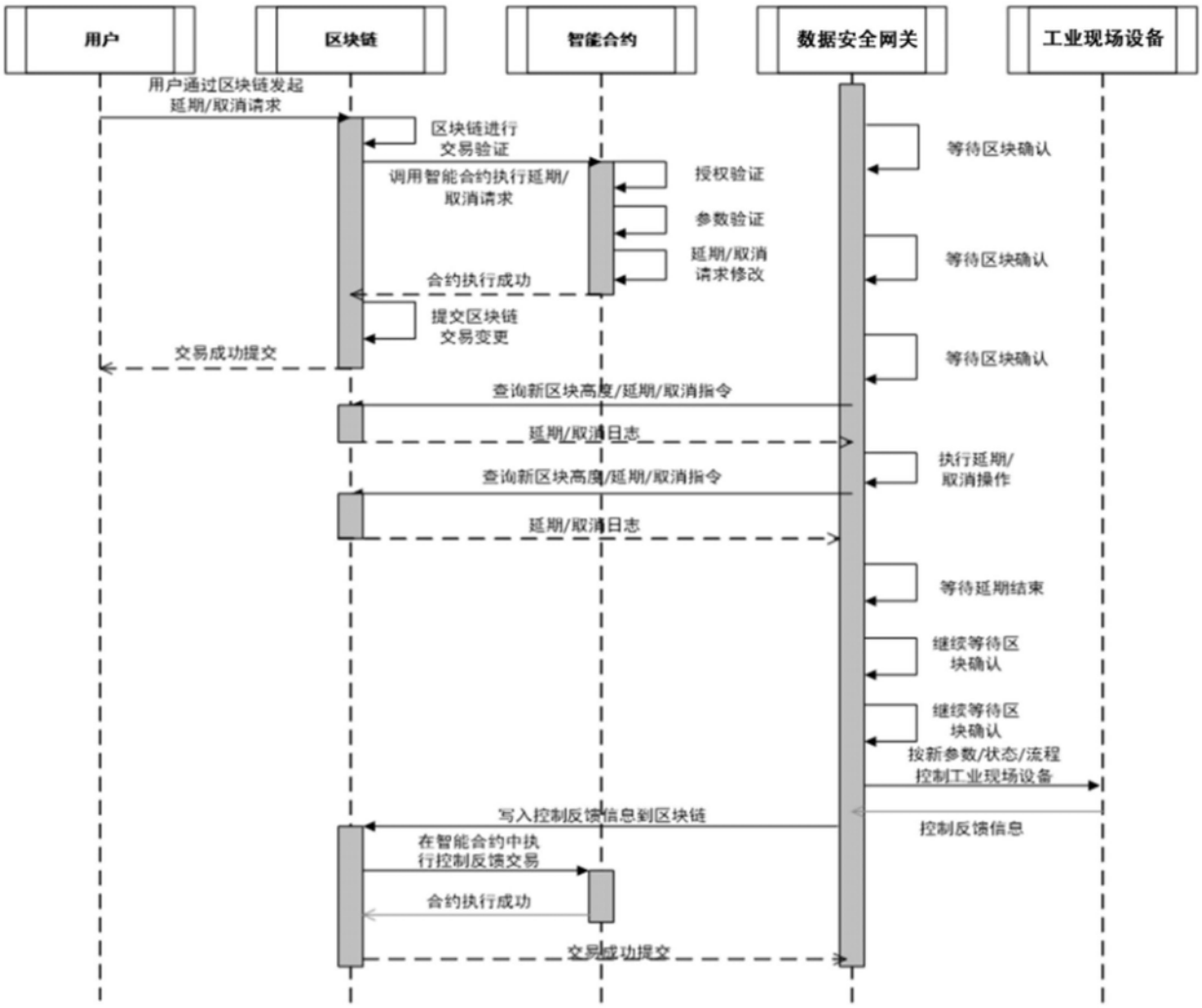

用户
区块链
智能合约
数据安全网关
工业现场设备
用户通过区块链发起
延期/取消请求
区块链进行
交易验证
调用智能合约执行延期/
取消请求
授权验证
参数验证
延期/取消
请求修改
合约执行成功
提交区块链
交易变更
交易成功提交
等待区块确认
等待区块确认
等待区块确认
查询新区块高度/延期/取消指令
延期/取消日志
执行延期/
取消操作
查询新区块高度/延期/取消指令
延期/取消日志
等待延期结束
继续等待区
块确认
继续等待区
块确认
按新参数/状态/流程
控制工业现场设备
写入控制反馈信息到区块链
控制反馈信息
在智能合约中执
行控制反馈交易
合约执行成功
交易成功提交

图5

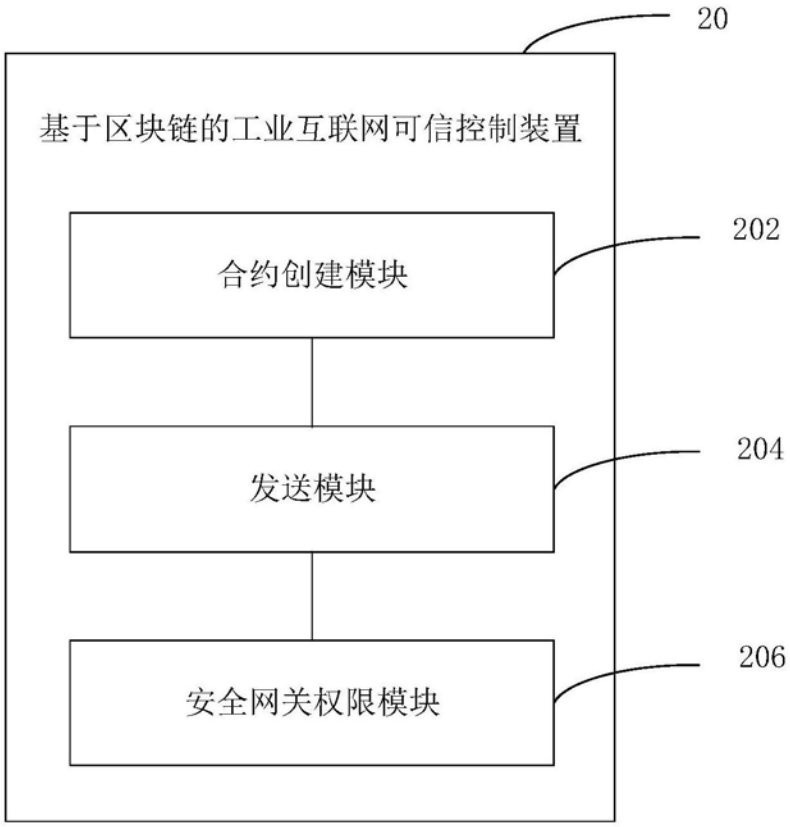

20
基于区块链的工业互联网可信控制装置
202
合约创建模块
204
发送模块
206
安全网关权限模块

图6

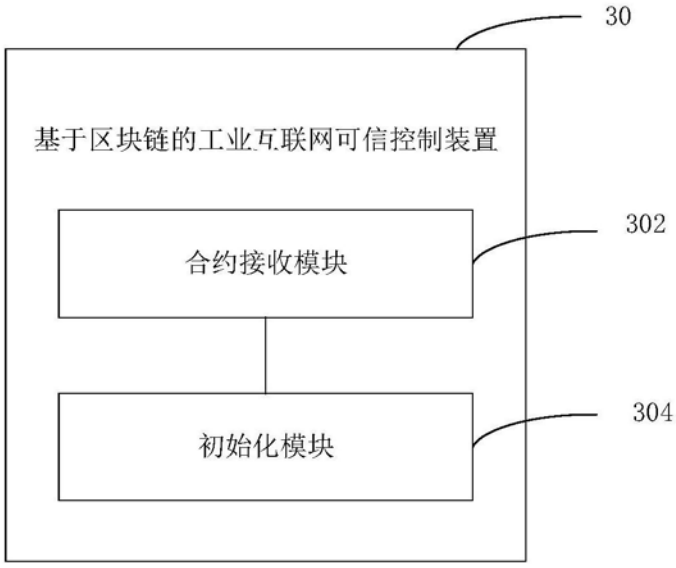

30
基于区块链的工业互联网可信控制装置
302
合约接收模块
304
初始化模块

图7

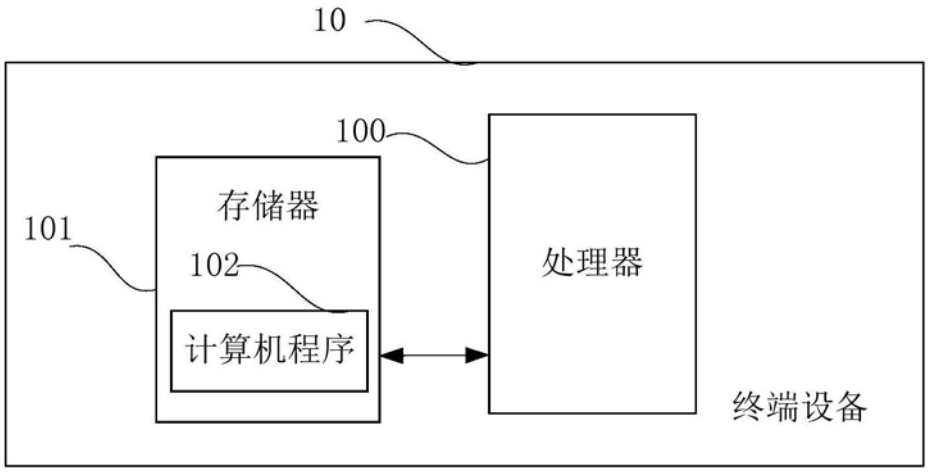


图8