(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111435240 B
(45)授权公告日 2025.05.06

(21)申请号 202010040206.2

(22)申请日 2020.01.15

(65)同一申请的已公布的文献号
申请公布号 CN 111435240 A

(43)申请公布日 2020.07.21

(30)优先权数据
16/248,367 2019.01.15 US

(73)专利权人 费希尔-罗斯蒙特系统公司
地址 美国德克萨斯州

(72)发明人 J·S·卡希尔

(74)专利代理机构 永新专利商标代理有限公司 72002
专利代理师 戚英豪 丁燕

(51)Int.Cl.
G05B 19/418(2006.01)

(56)对比文件
CN 108830447 A,2018.11.16

审查员 代云飞

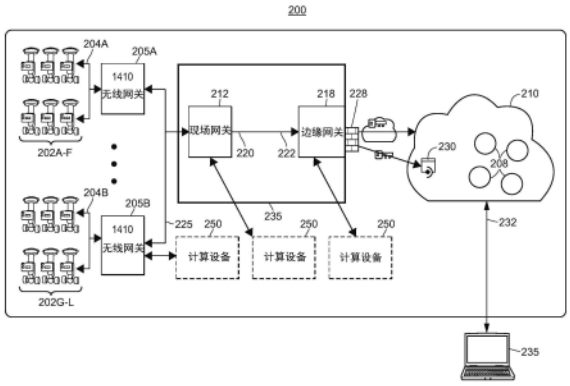
权利要求书3页 说明书41页 附图19页

(54)发明名称

过程控制系统中记录质量控制、生产或监管数据的方法和系统

(57)摘要

为了在过程工厂内提供可信、安全、且不变的交易记录,描述了在过程控制系统中利用分布式账本的技术。分布式账本可以由接收从现场设备、控制器、操作员工作站、或在过程工厂内运行的其他设备广播的交易的节点维护。交易可以包括过程工厂数据,例如过程参数数据、产品参数数据、配置数据、用户交互数据、维护数据、调试数据、工厂网络数据、和产品跟踪数据。分布式账本还可用于执行智能合约,以允许诸如现场设备之类的机器自行交易,而无需人工干预。以这种方式,可以获取记录的过程参数值和产品参数值以验证产品的质量。此外,可以响应于触发事件而记录监管数据,以便监管机构可以审查数据。



CN 111435240 B

1.一种用于使用由多个参与者维护的分布式账本在过程控制系统中记录质量控制、生产或监管数据的方法,所述方法包括:

经由各自执行物理功能以控制工业过程的一个或多个现场设备检测与过程工厂内的质量控制有关的触发事件;

从所述触发事件获得事件数据,包括以下中的至少一个:所述触发事件的时间、所述触发事件的持续时间、与所述触发事件有关的产品参数数据、或与所述触发事件有关的过程参数数据;

生成包括所述事件数据的交易,其中,所述交易被存储在所述分布式账本中,所述交易还包括所述触发事件的唯一标识符;

将所述交易传送给维护所述分布式账本的参与者的分布式账本网络中的至少一个其他参与者;以及

将包括所述触发事件的唯一标识符的所检测到的触发事件的指示传送到所述过程工厂中的一个或多个其他过程控制元件,以用于所述其他过程控制元件生成包括与所述触发事件有关的附加事件数据的交易。

2.根据权利要求1所述的方法,其中,所述触发事件是以下中的至少一个:警报、错误、泄漏、维修事件、过程重大事件、或纠正措施。

3.根据权利要求1所述的方法,还包括:

接收对来自特定触发事件的事件数据的请求;

从所述分布式账本中获得所述事件数据;以及

在用户界面上呈现来自所述特定触发事件的所述事件数据。

4.根据权利要求1所述的方法,其中,生成包括所述事件数据的交易包括:生成包括与所述事件数据中的至少一些相对应的加密哈希值的交易。

5.根据权利要求4所述的方法,还包括:

将所述事件数据存储在数据库中;以及

响应于对认证所述事件数据的请求,提供与来自所述分布式账本的所述事件数据中的至少一些相对应的所述加密哈希值以及来自所述数据库的所述事件数据,以验证所述事件数据的真实性。

6.根据权利要求1所述的方法,其中,所述触发事件是安全阀中的打开,并且来自所述触发事件的所述事件数据包括以下中的至少一个:

打开所述安全阀的时间,

打开所述安全阀的持续时间,

打开所述安全阀时的压力值,或

打开所述安全阀时排出的流体量。

7.根据权利要求1所述的方法,其中,所述分布式账本是能够由所述过程工厂和监管机构访问的私有区块链。

8.根据权利要求1所述的方法,其中,所述分布式账本是公有区块链。

9.一种用于使用由多个参与者维护的分布式账本在过程控制系统中记录质量控制、生产或监管数据的系统,包括:

设置在过程工厂中的一个或多个设备,所述一个或多个设备各自执行物理功能以控制

工业过程;以及

在所述过程工厂中执行的计算设备,所述计算设备包括:

一个或多个处理器;

通信单元;以及

非暂时性计算机可读介质,其耦合到所述一个或多个处理器和所述通信单元,并且在其上存储指令,所述指令在由所述一个或多个处理器执行时使所述计算设备执行以下操作:

经由所述一个或多个设备检测与所述过程工厂内的质量控制有关的触发事件;

从所述触发事件获得事件数据,包括以下中的至少一个:所述触发事件的时间、所述触发事件的持续时间、与所述触发事件有关的产品参数数据、或与所述触发事件有关的过程参数数据;

生成包括所述事件数据的交易,其中,所述交易被存储在所述分布式账本中,所述交易还包括所述触发事件的唯一标识符;

将所述交易传送给维护所述分布式账本的参与者的分布式账本网络的至少一个其他参与者,以便验证所述交易并在所述分布式账本中记录所述交易;以及

将包括所述触发事件的所述唯一标识符的所检测到的触发事件的指示传送到所述过程工厂中的所述一个或多个设备,以用于所述一个或多个设备生成包括与所述触发事件有关的附加事件数据的交易。

10.根据权利要求9所述的系统,其中,所述触发事件是以下中的至少一个:警报、错误、泄漏、维修事件、过程重大事件、或纠正措施。

11.根据权利要求9所述的系统,其中,所述指令还使所述计算设备执行以下操作:

接收对来自特定触发事件的事件数据的请求;

从所述分布式账本中获得所述事件数据;以及

在用户界面上呈现来自所述特定触发事件的所述事件数据。

12.根据权利要求9所述的系统,其中,所述交易包括与所述事件数据中的至少一些相对应的加密哈希值。

13.根据权利要求12所述的系统,其中,所述指令还使所述计算设备执行以下操作:

将所述事件数据存储在数据库中;以及

响应于对认证所述事件数据的请求,提供与来自所述分布式账本的所述事件数据中的至少一些相对应的加密哈希值以及来自所述数据库的所述事件数据,以验证所述事件数据的真实性。

14.根据权利要求9所述的系统,其中,所述触发事件是安全阀中的打开,并且来自所述触发事件的所述事件数据包括以下中的至少一个:

打开所述安全阀的时间,

打开所述安全阀的持续时间,

打开所述安全阀时的压力值,或

打开所述安全阀时排出的流体量。

15.根据权利要求9所述的系统,其中,所述分布式账本是能够由所述过程工厂和监管机构访问的私有区块链。

16.根据权利要求9所述的系统,其中,所述分布式账本是公有区块链。

过程控制系统中记录质量控制、生产或监管数据的方法和系统

技术领域

[0001] 本公开内容总体上涉及过程工厂和过程控制系统，具体而言，涉及在过程控制系统中使用分布式账本来记录数据和事件。

背景技术

[0002] 如用于化学、石油或其他过程工厂的分布式过程控制系统通常包括经由模拟、数字或组合模拟/数字总线或经由无线通信链路或网络通信地耦合到一个或多个现场设备的一个或多个过程控制器。现场设备，可以是例如阀、阀定位器、开关和变送器(例如，温度、压力、液位和流量传感器)，位于工厂环境内并通常执行物理或过程控制功能，例如打开或关闭阀，测量过程参数(例如压力、温度等)，以控制在过程工厂或系统中执行的一个或多个过程。智能现场设备，例如符合公知的现场总线协议的现场设备，还可以执行控制计算、报警功能以及通常在控制器内实现的其他控制功能。通常也位于工厂环境内的过程控制器接收指示由现场设备获得的过程测量结果的信号和/或与现场设备有关的其他信息，并执行运行例如不同控制模块的控制器应用，控制模块基于接收到的信息制定过程控制决策、生成控制信号，并与现场设备(例如HART®、WirelessHART®和FOUNDATION® Fieldbus现场设备)中执行的控制模块或块协调。控制器内的控制模块通过通信线路或链路将控制信号发送到现场设备，从而控制过程工厂或系统的至少一部分的操作。如本文所用的，现场设备和控制器通常被称为“过程控制设备”。

[0003] 来自现场设备和控制器的信息通常通过数据高速通道可由一个或多个其他硬件设备获得，例如操作员工作站、个人计算机或计算设备、数据历史记录、报告生成器、中心化数据库或其他中心化管理计算设备，它们通常放置在控制室中或远离严酷的工厂环境的其他位置。这些硬件设备中的每一个通常跨整个过程工厂或过程工厂的一部分集中。这些硬件设备运行应用，这些应用例如可以使操作员能够执行关于控制过程和/或操作过程工厂的功能，例如改变过程控制例程的设置，修改控制器或现场设备内的控制模块的操作，查看过程的当前状态，查看现场设备和控制器生成的警报，为培训人员或测试过程控制软件而模拟过程的操作，保留和更新配置数据库等。硬件设备、控制器和现场设备所利用的数据高速通道可以包括有线通信路径、无线通信路径或有线和无线通信路径的组合。

[0004] 作为示例，由艾默生过程管理公司(EMERSON PROCESS MANAGEMENT)销售的DeltaV™控制系统包括存储在位于过程工厂内的不同位置处的不同设备内并由不同设备执行的多个应用。驻留在一个或多个工作站或计算设备中的配置应用使用户能够创建或更改过程控制模块，并经由数据高速通道将这些过程控制模块下载到专用分布式控制器。通常，这些控制模块由通信互连的功能块组成，这些功能块是面向对象的编程协议中的对象，其基于其输入执行控制方案内的功能，并向控制方案内的其他功能块提供输出。配置应用还可以允许设计者创建或改变操作员界面，操作员界面由查看应用使用以向操作员显示数据并使操作员能够改变过程控制例程内的设置，例如设定点。每个专用控制器以及在某些情

况下的一个或多个现场设备存储并执行各自的控制器应用,该控制器应用运行分配和下载到其上的控制模块以实现实际过程控制功能。可以在一个或多个操作员工作站(或与操作员工作站和数据高速通道通信连接的一个或多个远程计算设备)上执行的查看应用经由数据高速通道从控制器应用接收数据,并使用用户界面向过程控制系统设计者、操作员或用户显示该数据,并且可以提供许多不同的视图中的任何一个,例如操作员视图、工程师视图、技术人员视图等。数据历史记录应用通常存储在数据历史记录设备中并由其执行,该数据历史记录设备收集并存储通过数据高速通道提供的一些或全部数据,而配置数据库应用可在连接到数据高速通道的另一计算机中运行以存储与之相关的当前过程控制例程配置和数据。可替换地,配置数据库可以位于与配置应用相同的工作站中。

[0005] 一般而言,过程工厂的过程控制系统包括现场设备、控制器、工作站以及通过一组分层网络和总线互连的其他设备。过程控制系统又可以与各种业务和外部网络连接,例如,以降低制造和运营成本,提高生产率和效率,提供对过程控制和/或过程工厂信息的及时访问等。另一方面,过程工厂和/或过程控制系统与企业和/或外部网络和系统的互连会增加可能由于商业系统和应用(例如企业和/或外部网络中所使用的)中的预期漏洞而引起的网络入侵和/或恶意网络攻击的风险。过程工厂、网络、和/或控制系统的网络入侵和恶意网络攻击可能会不利地影响信息资产的机密性、完整性和/或可用性,通常来说,这些漏洞类似于通用计算网络的漏洞。但是,与通用计算机网络不同,过程工厂、网络和/或控制系统的网络入侵还可能不仅导致工厂装备、产品、和其他有形资产的损坏、破坏和/或损失,而且还导致失去生命。例如,网络入侵可能会使过程变得不受控制,从而导致爆炸、火灾、水灾、暴露于有害物质等。因此,确保与过程控制工厂和系统有关的通信至关重要。

发明内容

[0006] 公开了用于在过程控制系统中利用分布式账本或区块链的技术、系统、装置、部件、设备和方法。所述技术、系统、装置、部件、设备和方法可以应用于工业过程控制系统、环境和/或工厂,在本文中可互换地称为“工业控制”、“过程控制”或“过程”系统、环境和/或工厂。通常,这样的系统和工厂以分布的方式提供对一个或多个过程的控制,这些过程操作以制造、精炼、转化、产生或生产物理材料或产品。

[0007] 例如,在过程控制系统中,分布式账本可以由本文称为“边缘网关”的节点维护。节点接收从现场设备、控制器、操作员工作站、或在过程工厂内运行的其他设备广播到分布式账本网络的交易。在某些情况下,交易包括与过程工厂实体相对应的过程参数的过程参数值。过程工厂实体可包括过程工厂中用于过程的一部分的设备,这些设备包含、转化、产生、或转移物理材料,例如阀、罐、混合器、泵、热交换器等。交易还可以包括产品参数值,例如由过程工厂生产的物理材料或产品的属性,包括产品的温度、产品的体积、产品的质量、产品的密度、产品的压力等。

[0008] 然后可以获取所记录的过程参数值和产品参数值以验证产品的质量。例如,第一过程工厂可以制造、精炼、转化、产生、或生产产品,然后将其运送到第二过程工厂。第二过程工厂可以通过从分布式账本中获取所记录的过程参数值和产品参数值来确定产品符合某些质量标准。另外,监管数据可以记录在分布式账本中。例如,响应于诸如警报、错误、泄漏、维修事件、过程重大事件、纠正措施等触发事件,诸如现场设备或控制器之类的过程控

制元件可以产生包括来自触发事件的数据的交易,例如事件发生的时间,事件的持续时间,事件所涉及的过程工厂实体的过程参数值,事件中所涉及的产品的产品参数值等。然后将监管数据记录在分布式账本中,以便监管机构可以查看数据。

[0009] 更进一步地,分布式账本可以被用于执行智能合约,这将在下面更详细地描述。过程控制系统可以将智能合约部署到分布式账本中以交换值,例如在收到完好的产品后。智能合约也可以部署到分布式账本,以允许诸如现场设备之类的机器自行进行交易,而无需人工干预。例如,根据智能合约的条款,第一过程工厂中的计算设备可以在从第一过程工厂中的一个或多个现场设备接收到产品已从第二过程工厂交付并且该产品符合一定质量标准的指示后,自动向第二过程工厂中的计算设备提供预定数量的通证(token)。智能合约还可在过程工厂中用于大量其他应用,下面将对此进行更详细的描述。

[0010] 通过利用分布式账本和在某些情况下的过程工厂中的智能合约,每个过程工厂或过程工厂的网络可以在过程工厂中提供可信、安全、且不变的交易记录。分布式账本的安全、不变、和免信任的性质在过程控制系统中尤其重要,在过程控制系统中,网络入侵不仅可能导致工厂装备、产品、和其他有形资产的损坏、破坏和/或损失,而且还导致失去生命。此外,分布式账本允许过程工厂跟踪从原材料到成品的产品沿袭,并在产品制造后进一步跟踪产品。而且,当竞争实体利用或转移公共资源时,可以使用分布式账本来确定实体之一所利用的资源量,并公平补偿竞争实体对资源的使用。例如,炼油厂可以生产经由石油管道提供给几个实体或过程工厂的石油。每个过程工厂负责向炼油厂补偿过程工厂从输油管道接收的油量。分布式账本可用于记录从在供油时从测量油量的设备接收的每个过程工厂的油量。由于难以更改分布式账本中的记录数据,因此竞争实体不必相信数据是可靠的。

附图说明

[0011] 图1是示例过程工厂或过程控制系统的框图,其尤其示出了过程控制系统的各个示例部件、过程控制系统本身、以及其他示例系统和/或网络之间的互连;

[0012] 图2是用于过程工厂或过程控制系统的示例安全架构的框图;

[0013] 图3是用于在过程控制系统中记录交易并执行智能合约的示例性分布式账本系统;

[0014] 图4示出了过程控制系统中的分布式账本网络上的示例性验证网络节点和示例性交易流;

[0015] 图5示出了过程控制系统中的分布式账本网络上的网络节点的示例性部件;

[0016] 图6A示出了示例分布式账本,其包括过程控制系统中的具有交易块的区块链。

[0017] 图6B示出了另一示例分布式账本,其包括由不同过程工厂维护的多个侧区块链或侧链以及合并了来自侧链的交易数据的由多个过程工厂维护的主区块链;

[0018] 图7A示出了又一示例分布式账本,其包括各自由不同过程工厂维护的多个本地区块链;

[0019] 图7B示出了由多个过程工厂维护的并合并了来自本地区块链的区块的过程工厂的全局区块链;

[0020] 图7C示出了由几个过程工厂维护的合并了每个过程工厂的每个全局区块链的区块的超级区块链。

[0021] 图8示出了用于在过程工厂中执行安全写操作以将过程参数写至安全仪表系统(SIS)设备的分布式账本网络中的示例性智能合约状态;

[0022] 图9示出了表示由作为报告从输油管道接收的油量的现场设备的证据谕示产生的证据交易的示例性交易。

[0023] 图10示出了表示由作为报告软件或固件更新的计算设备的证据谕示产生的证据交易的示例性交易。

[0024] 图11示出了表示由作为报告过程参数或产品参数数据的过程工厂实体的证据谕示产生的证据交易的示例性交易。

[0025] 图12示出了表示用于使用分布式账本在过程控制系统中记录数据的示例性方法的流程图;

[0026] 图13示出了表示用于使用分布式账本在过程控制系统中安全计量不可信数据的示例性方法的流程图;

[0027] 图14示出了表示用于使用分布式账本在过程控制系统中记录质量控制、生产、或监管数据的示例性方法的流程图;

[0028] 图15示出了表示用于使用分布式账本记录过程控制系统和所连接的仪器中的软件或固件的状态的示例性方法的流程图;

[0029] 图16示出了表示用于使用分布式账本在过程控制系统中创建智能合约的示例性方法的流程图;以及

[0030] 图17示出了表示用于使用分布式账本在过程控制系统中与智能合约进行交互的示例性方法的流程图。

具体实施方式

[0031] 分布式账本是由若干参与者维护的用于数据、事件、交易等的存储机制。具体而言,分布式账本是一种就分布式账本中记录的信息的有效性或无效性达成分布式共识的方法。即,分布式账本向参与者和观察者提供去中心化的信任。与依赖中央权力机构相反,分布式账本是一个去中心化的数据库,其中对账本的更改的交易记录由对等网络的每个节点维护和验证。一种类型的分布式账本,即区块链,由一起组织成“区块”并按顺序排序的交易的分组组成(因此称为“区块链”)。尽管在区块链的上下文中引用了本文所讨论的分布式账本,但这仅是分布式账本的一个示例。分布式账本还可以包括tangle、区块晶格(block lattice)或其他有向无环图(DAG)。无论如何,随着时间的流逝,节点可以加入并离开区块链网络,并且可以从节点离开时传播的对等节点获得区块。节点可以维护其他节点的地址,并彼此交换已知节点的地址,以促进新信息以去中心化的、对等方式在网络中传播。

[0032] 共享账本的节点形成本文所谓的分布式账本网络。分布式账本网络中的节点根据一组共识规则验证对区块链的更改(例如,当创建新交易和/或区块时)。共识规则取决于正在由区块链跟踪的信息,并且可以包括有关链本身的规则。例如,共识规则可以包括更改的发起者提供身份证明,以使得只有批准的实体才可以发起对链的更改。共识规则可以要求区块和交易遵守格式要求,并提供有关更改的某些元信息(例如,区块必须低于大小限制,交易必须包含多个字段,等等)。共识规则可以包括用于确定将新区块添加到链中的顺序(例如,通过工作量证明系统、权益证明等)的机制。

[0033] 满足共识规则的对区块链的添加从已经验证该添加的节点传播到验证节点所知道的其他节点。如果接收到对区块链的更改的所有节点都验证了新区块，则分布式账本反映存储在所有节点上的新的更改，并且可以说已经就新区块和其中包含的信息达成了分布式共识。接收到该更改的验证节点会忽略任何不符合共识规则的更改，并且该更改不会传播到其他节点。因此，与使用中央权力机构的传统系统不同，单方不能单方面改变分布式账本，除非单方可以以符合共识规则的方式进行改变。无法修改过去的交易导致区块链通常被描述为可信的、安全且不可变的。

[0034] 在区块链网络上应用共识规则的节点的验证活动可以采取各种形式。在一种实施方式中，区块链可以被视为跟踪诸如资产所有权之类的数据的共享电子表格。在另一种实施方式中，验证节点执行“智能合约”中包含的代码，并且分布式共识表示为网络节点同意所执行的代码的输出。

[0035] 智能合约是一种计算机协议，其能够自动执行和/或实施不同各方之间的协议。特别地，智能合约可以是位于区块链上特定地址的计算机代码。在某些情况下，智能合约可以响应于区块链中的参与者将资金(例如比特币、以太币或其他数字/虚拟货币之类的加密货币)发送到存储智能合约的地址而自动运行。此外，智能合约可以保持其地址中存储的资金量的余额。在某些情况下，当此余额达到零时，智能合约可能不再可用。

[0036] 智能合约可以包括一个或多个触发条件，当满足时，其对应于一个或多个动作。对于一些智能合约，可以基于一个或多个决策条件来确定所执行的(多个)动作。在一些情况下，数据流可以被路由到智能合约，使得智能合约可以检测到触发条件已经发生和/或分析决策条件。

[0037] 可以以公开、去中心化、和非许可的方式部署区块链，这意味着任何一方都可以查看分布式账本，提交要添加到账本的新信息、或作为验证节点加入网络。其他区块链是私有的(例如，许可的账本)，它们在一组有权参与区块链网络的实体之间将链数据保持私有。其他区块链实施方式可以是许可的和非许可的，因此可能需要验证参与者，但只有网络中的参与者希望公开的信息才会公开。

[0038] 在一些实施方式中，分布式账本包括诸如主区块链和独立于主区块链而操作的几个侧链的多个区块链。侧链然后与主区块链交互以将一些交易数据从侧链提供给主区块链。通过这种方式，侧链可以是私有的，而主区块链是公共的，或者可以供比侧链更多的实体使用。来自侧链的非敏感信息可以在主区块链上共享。同样在一些实施方式中，分布式账本包括由相同的验证节点维护的并行执行的多层或单独的区块链。可以将来自第一层的区块链的一些交易数据提供给第二层的区块链，反之亦然。

[0039] 在一个示例中，可以由本文称为“边缘网关”的验证节点来维护过程控制系统中的分布式账本，所述验证节点使用一个或多个公共和/或私有网络(例如私有企业网络、互联网、蜂窝路由器、回程互联网或其他类型的回程连接)将数据传输到诸如其他过程工厂之类的远程系统。边缘网关接收由例如过程控制设备(例如现场设备或在过程工厂中运行的控制器)广播到分布式账本网络的交易。过程工厂中的其他计算设备(例如操作员工作站、服务器设备、或其他用户接口设备)也可以将交易广播到分布式账本网络。然后，边缘网关验证广播的交易。

[0040] 在另一个示例中，边缘网关执行“智能合约”中包含的代码，而现场设备充当“证据

谕示”,其将与质量控制、法规遵从、产品的交付或接收以及交付/接收的数量等有关的证据提供给区块链。

[0041] 图1是可以利用本文描述的新颖分布式账本技术中的任何一个或多个的示例过程工厂10的框图。过程工厂10(在本文中也可互换地称为过程控制系统10或过程控制环境10)包括一个或多个过程控制器,该过程控制器接收指示现场设备获得的过程测量结果的信号,处理该信息以实施控制例程,并生成通过有线或无线过程控制通信链路或网络发送到其他现场设备的控制信号,以控制工厂10中过程的操作。通常,至少一个现场设备执行物理功能(例如,打开或关闭阀,升高或降低温度,进行测量,感测条件等)以控制过程的操作。某些类型的现场设备通过使用I/O设备与控制器进行通信。过程控制器、现场设备、和I/O设备可以是有线或无线的,并且过程工厂环境或系统10中可以包括任何数量的有线和无线过程控制器、现场设备和I/O设备及其组合。

[0042] 例如,图1示出了过程控制器11,该过程控制器11经由输入/输出(I/O)卡26和28通信地连接到有线现场设备15-22,并且经由无线网关35和过程控制数据高速通道或主干105通信地连接到无线现场设备40-46。过程控制数据高速通道105可以包括一个或多个有线和/或无线通信链路,并且可以使用任何期望的或合适的或通信协议(例如,以太网协议)来实现。在一些配置(未示出)中,控制器11可以使用除主干105之外的一个或多个通信网络通信地连接到无线网关35,例如通过使用支持一个或多个通信协议(例如,Wi-Fi或其他符合IEEE 802.11的无线局域网协议、移动通信协议(例如WiMAX、LTE或其他符合ITU-R的协议)、Bluetooth®、HART®、WirelessHART®、Profibus、FOUNDATION®现场总线等)的任何数量的其他有线或无线通信链路。

[0043] 控制器11可以是例如艾默生过程管理公司(Emerson Process Management)销售的DeltaV™控制器,它可以使用现场设备15-22和40-46中的至少一些进行操作以实现批量过程或连续过程。在一个实施例中,除了被通信地连接到过程控制数据高速通道105之外,控制器11还使用与例如标准4-20mA设备,I/O卡26、28和/或任何智能通信协议(例如FOUNDATION®Fieldbus协议,HART®协议,WirelessHART®协议等)相关联的任何期望的硬件和软件通信地连接到现场设备15-22和40-46中的至少一些。在图1中,控制器11、现场设备15-22和I/O卡26、28是有线设备,并且现场设备40-46是无线现场设备。当然,有线现场设备15-22和无线现场设备40-46可以符合任何其他期望的(多个)标准或协议,例如任何有线或无线协议,包括将来开发的任何标准或协议。

[0044] 图1的过程控制器11包括处理器30,该处理器30实施或监督一个或多个过程控制例程38(例如,存储在存储器32中的例程)。处理器30被配置为与现场设备15-22和40-46以及与通信地连接至控制器11的其他节点进行通信。应当注意,本文描述的任何控制例程或模块可以具有由不同控制器或其他设备(如果需要)实现或执行的其部分。同样地,将在过程控制系统10内实现的本文所述的控制例程或模块38可以采用任何形式,包括软件、固件、硬件等。控制例程可以以任何期望的软件格式来实现,例如使用面向对象的编程、梯形逻辑、顺序功能图、功能框图,或使用任何其他软件编程语言或设计范例。控制例程38可以存储在任何期望类型的存储器32中,例如随机存取存储器(RAM)或只读存储器(ROM)。同样,控制例程38可以被硬编码到例如一个或多个EPROM、EEPROM、专用集成电路(ASIC)或任何其他

硬件或固件元件中。因此,控制器11可以被配置为以任何期望的方式实现控制策略或控制例程。

[0045] 控制器11使用通常所谓的功能块来实现控制策略,其中每个功能块是整个控制例程的对象或其他部分(例如,子例程),并结合其他功能块(通过称为链路的通信)操作来实现过程控制系统10中的过程控制回路。基于控制的功能块通常执行输入功能(例如与变送器、传感器或其他过程参数测量设备相关联的)、控制功能(例如与执行PID、模糊逻辑等控制的控制例程相关联的)、或输出功能(控制某个设备(例如阀)的操作以在过程控制系统10内执行某个物理功能)中的一个。当然,存在混合和其他类型的功能块。功能块可以存储在控制器11中并由控制器11执行,这通常是当这些功能块用于或关联于标准4-20mA设备和某些类型的智能现场设备(例如HART®设备)的情况,或者可以存储在现场设备自身中并由现场设备自身实现,这可以是FOUNDATION®Fieldbus设备的情况。控制器11可以包括一个或多个控制例程38,其可以实现一个或多个控制回路,该控制回路通过执行一个或多个功能块来执行。

[0046] 有线现场设备15-22可以是任何类型的设备,例如传感器、阀、变送器、定位器等,而I/O卡26和28可以是符合任何期望通信或控制器协议的任何类型的I/O设备。在图1中,现场设备15-18是标准4-20mA设备或通过模拟线路或组合的模拟和数字线路与I/O卡26通信的HART®设备,而现场设备19-22是智能设备,例如FOUNDATION®Fieldbus现场设备,它们使用FOUNDATION®Fieldbus通信协议通过数字总线与I/O卡28通信。然而,在一些实施例中,有线现场设备15、16和18-21中的至少一些和/或I/O卡26、28中的至少一些另外或可替代地使用过程控制数据高速通道105和/或通过使用其他合适的控制系统协议(例如Profibus、DeviceNet、Foundation® Fieldbus、ControlNet、Modbus、HART等)与控制器11通信。

[0047] 在图1中,无线现场设备40-46使用诸如WirelessHART®协议的无线协议经由无线过程控制通信网络70进行通信。这样的无线现场设备40-46可以与无线网络70的一个或多个其他设备或节点直接通信,这些设备或节点也被配置为进行无线通信(例如,使用该无线协议或另一无线协议)。为了与未配置为进行无线通信的一个或多个其他节点进行通信,无线现场设备40-46可以利用连接到过程控制数据高速通道105或另一过程控制通信网络的无线网关35。无线网关35提供对无线通信网络70的各种无线设备40-58的访问。特别地,无线网关35提供无线设备40-58、有线设备15-28、和/或过程控制工厂10的其他节点或设备之间的通信耦合。例如,无线网关35可以通过使用过程控制数据高速通道105和/或通过使用过程工厂10的一个或多个其他通信网络来提供通信耦合。

[0048] 与有线现场设备15-22相似,无线网络70的无线现场设备40-16在过程工厂10中执行物理控制功能,例如打开或关闭阀,或获得过程参数的测量结果。然而,无线现场设备40-46被配置为使用网络70的无线协议进行通信。因而,无线现场设备40-46、无线网关35、和无线网络70的其他无线节点52-58是无线通信分组的生产者和消费者。

[0049] 在过程工厂10的某些配置中,无线网络70包括非无线设备。例如,在图1中,图1的现场设备48是传统的4-20mA设备,而现场设备50是有线HART®设备。为了在网络70内通

信,现场设备48和50经由无线适配器52A、52B连接到无线通信网络70。无线适配器52A、52B支持无线协议,例如WirelessHART,并且还可以支持一种或多种其他通信协议,例如FOUNDATION®Fieldbus、PROFIBUS、DeviceNet等。另外,在一些配置中,无线网络70包括一个或多个网络接入点55A、55B,其可以是与无线网关35进行有线通信的分离的物理设备,或者可以作为整体设备与无线网关35一起提供。无线网络70还可以包括一个或多个路由器58,以将分组从一个无线设备转发到无线通信网络70内的另一无线设备。在图1中,无线设备40-46和52-58通过无线通信网络70的无线链路60和/或经由过程控制数据高速通道105彼此通信并且与无线网关35通信。

[0050] 在图1中,过程控制系统10包括通信地连接到数据高速通道105的一个或多个操作员工作站或用户接口设备8。经由操作员工作站8,操作员可以查看和监控过程工厂10的运行时操作,以及采取可能需要的任何诊断、纠正、维护、和/或其他措施。至少一些操作员工作站8可以位于工厂10内或附近的各种受保护区域,并且在某些情况下,至少一些操作员工作站8可以远程定位,但是仍然与工厂10通信连接。操作员工作站8可以是有线或无线计算设备。

[0051] 示例过程控制系统10可以进一步包括配置应用(未示出)和配置数据库(未示出),它们中的每一个也通信地连接到数据高速通道105。如上所述,配置应用的各种实例(未示出)可以在一个或多个用户接口设备8上执行,以使用户能够创建或改变过程控制模块,并经由数据高速通道105将这些模块下载到控制器11,以及使用户能够创建或改变操作员界面,操作员经由操作员界面能够在过程控制例程中查看数据并更改数据设置。配置数据库(未示出)存储所创建的(例如,已配置的)模块和/或操作员界面。

[0052] 在某些配置中,过程控制系统10包括一个或多个其他无线接入点7a,这些无线接入点7a使用其他无线协议(例如Wi-Fi或其他符合IEEE 802.11的无线局域网协议,移动通信协议(例如WiMAX(全球微波访问互操作性)),LTE(长期演进)或其他符合ITU-R(国际电信联盟无线电通信部门)的协议,短波无线电通信(例如近场通信(NFC)和蓝牙)或其他无线通信协议)与其他设备进行通信。通常,这样的无线接入点7a允许手持式设备或其他便携式计算设备在与无线网络70不同并且支持与无线网络70不同的无线协议的相应无线过程控制通信网络上进行通信。例如,无线或便携式用户接口设备8可以是过程工厂10中的操作员使用的移动工作站或诊断测试装备。在某些情况下,除了便携式计算设备之外,一个或多个过程控制设备(例如,控制器11、现场设备15-22、或无线设备35、40-58)也使用接入点7a支持的无线协议进行通信。

[0053] 在一些配置中,过程控制系统10包括到当前过程控制系统10外部的系统的一个或多个网关7b、7c(在本文中也称为“边缘网关”,并且在下面进行更详细的描述)。通常,这样的系统是由过程控制系统10生成或操作的信息的客户或供应者。例如,过程控制工厂10可以包括网关节点7b,以将当前过程工厂10与另一过程工厂通信地连接。另外或可替代地,过程控制工厂10可以包括网关节点7c,以将当前过程工厂10与外部公共或私有系统(例如实验室系统(例如,实验室信息管理系统或LIMS)、操作员巡视数据库、物料处理系统、维护管理系统、产品库存控制系统、生产调度系统、天气数据系统、运输和处理系统、包装系统、互联网、其他供应商的过程控制系统或其他外部系统)进行通信连接。

[0054] 注意,尽管图1仅示出了单个控制器11,其具有包括在示例过程工厂10中的有限数

量的现场设备15-22和40-46、无线网关35、无线适配器52、接入点55、路由器58、和无线过程控制通信网络70,这仅是示例性而非限制性的实施例。可以在过程控制工厂或系统10中包括任意数量的控制器11,并且控制器11中的任意一个可以与任意数量的有线或无线设备和网络15-22、40-46、35、52、55、58和70通信以控制工厂10中的过程。

[0055] 此外,应注意,图1的过程设备或控制系统10可以包括通过数据高速通道105通信连接的现场环境(例如,“过程工厂车间”)和后端环境(例如,服务器12)。如图1所示,现场环境包括物理部件(例如,过程控制设备、网络、网络元件等),该物理部件在其中设置、安装、和互连以在运行时进行操作以控制过程。例如,控制器11,I/O卡26、28,现场设备15-22和其他设备以及网络部件40-46、35、52、55、58和70定位、设置、或以其他方式包括在过程工厂10的现场环境中。一般而言,在过程工厂10的现场环境中,使用设置在其中的物理部件来接收和处理原材料,以产生一个或多个产品。

[0056] 过程工厂10的后端环境包括各种部件,例如服务器计算设备12、操作员工作站8、数据库或数据存储库等,它们被屏蔽和/或保护免受现场环境的严酷条件和材料的侵害。参考图1,后端环境包括例如操作员工作站8、服务器计算设备12、和/或支持过程工厂10的运行时操作的功能。在一些配置中,过程工厂10的后端环境中所包括的各种计算设备、数据库和其他部件和装备可以物理上位于不同的物理位置,其中一些对于过程工厂10可以是本地的,而其中一些可以是远程的。

[0057] 图2包括用于过程工厂10的示例安全架构200的框图。如图2所示,一个或多个设备202通信地连接到一个或多个无线网关205A、205B,其例如可以是图1的无线网关35的实例。网关205A、205B与设备202之间的通信连接由附图标记204A、204B表示。

[0058] 设备集202被示出为包括有限数量的无线现场设备。然而,应理解,本文关于设备202描述的概念和特征可以容易地应用于过程工厂10的任何数量的现场设备,以及任何类型的现场设备。例如,现场设备202可以包括一个或多个有线现场设备15-22,其经由过程工厂10的一个或多个有线通信网络通信地连接到无线网关205A、205B,和/或现场设备202可以包括耦合到无线适配器52A、52B的有线现场设备48、50。

[0059] 此外,应理解,设备集202不仅限于现场设备,而是可以附加地或替代地包括过程工厂10内的任何设备或部件,该设备或部件作为过程工厂10控制在线过程的结果而生成数据。例如,设备集202可以包括生成诊断数据的诊断设备或部件,在过程工厂10的各个部件之间传输信息的网络路由设备或部件,等等。实际上,图1中所示的任何部件(例如,部件7a-7c、8、11、12、15-22、26、28、35、40-46、52、55、58、60和70)和其他未示出的部件可以是生成数据以传送到远程系统210的设备。因此,设备集202在本文中可互换地称为“数据源202”或“数据源设备202”。

[0060] 图2进一步示出了可以用于过程工厂10和/或过程工厂10利用的远程应用或服务集合208。远程应用或服务集合208可以在一个或多个远程系统210上执行或托管。当由过程工厂10生成实时数据并且应用或服务208接收实时数据时,至少一些应用或服务208对实时数据进行实时操作。其他应用或服务208可以在时序要求不太严格的情况下对过程工厂生成的数据进行操作或执行。可以在远程系统210处执行或托管并且作为由过程工厂10生成的数据的消费者的应用/服务208的示例包括监控和/或感测在过程工厂10处发生的条件和/或事件的应用、以及在线过程在过程工厂10上执行时监控在线过程本身的至少一部分

的应用或服务。应用/服务208的其他示例包括描述性和/或规定性分析,其可以对过程工厂10生成的数据进行操作,并且在某些情况下,可以对从分析过程工厂生成的数据中收集或发现的知识以及其他过程工厂生成的数据或从其他过程工厂接收的数据进行操作。应用/服务208的其他示例包括一个或多个例程,这些例程实现规定的功能和/或改变,例如,作为另一服务或应用的结果,这些功能和/或改变将被实施回过程工厂10中。应用和服务208的其他示例对从分析过程工厂和/或其他过程工厂生成的历史数据或从将过程工厂实体的数据与相同或相似类型的数据过程工厂实体进行比较到而收集的知识进行操作。

[0061] 可以以任何期望的方式来实现一个或多个远程系统210,例如通过联网服务器的远程存储库、一个或多个云计算系统、一个或多个网络等来实现。为了便于讨论,本文使用单数形式指代一个或多个远程系统210,即“远程系统210”,但应理解,所述术语可以指一个系统、多于一个系统、或任何数量的系统。在一些情况下,分析过程工厂数据的计算设备250可以被包括在远程系统210内。

[0062] 一般而言,安全架构200提供端到端的安全性,从其中安装并操作设备202的过程工厂10的现场环境到提供使用和操作由过程工厂10生成的数据的应用和/或服务208的远程系统210。因而,由设备202和过程工厂10的其他部件生成的数据能够被安全地传输到远程系统210,以供远程应用/服务208使用,同时保护工厂10免受网络攻击、入侵、和/或其他恶意事件的侵害。特别地,安全架构200包括现场网关212、和设置在过程工厂10(例如,在过程工厂10的无线网关205A、205B之间)和远程系统210之间的边缘网关218。

[0063] 从过程工厂10发出并从输入端口220传输到输出端口222的数据可以进一步通过加密来保护。在示例中,现场网关212加密数据并将加密的数据传递到输入端口220。加密和传输的数据业务在一个示例中可以是UDP(用户数据报协议)数据业务,并且在另一个示例中可以是JSON数据业务或是某个其他通用通信格式。

[0064] 现场网关212通信地连接到过程控制工厂10。如图2所示,现场网关212通信地连接到无线网关205A、205B,无线网关205A、205B设置在过程工厂10的现场环境内并通信地连接到一个或多个设备或数据源202。如前所述,设备或数据源202和无线网关205A、205B可以使用WirelessHART工业协议或其他合适的无线协议进行通信,该协议被构造为经由一个或多个安全机制来提供安全的通信。例如,WirelessHART工业协议提供128位AES加密,并且可以相应地保护通信路径204A、204B。

[0065] 另外,分别使用与通信连接204A、204B所使用的相同或不同的安全机制保护无线网关205A、205B与现场网关212之间的通信连接225。在示例中,通信连接225由TLS(传输层安全性)包装器保护。例如,无线网关205A、205B生成HART-IP格式的数据分组,该数据分组由TLS包装器保护,以传输到现场网关212。

[0066] 因此,如上所述,在一个实施例中,由设备202生成的数据或分组可以使用第一安全机制来保护以用于到无线网关205A、205B的传输204A、204B,并且随后使用第二安全机制来保护以用于从无线网关205A、205B到现场网关212的传输225,再随后使用第三安全机制来保护以用于传输到边缘网关218。另外或替代地,并且如图2所示,边缘网关218可以由防火墙228保护。

[0067] 可以使用诸如私有企业网络、互联网、蜂窝路由器、回程互联网或其他类型的回程连接之类的一个或多个公共和/或私有网络来传递从边缘网关218传送到远程系统210的数

据。重要地,通过使用第四安全机制或通过使用以上先前讨论的安全机制之一来保护从边缘网关218到远程系统210传送的数据的安全。图2示出了经由SAS(共享访问签名)令牌保护的从边缘网关218传送到远程系统210的数据业务,该SAS令牌可以通过在远程系统210处提供的令牌服务230来管理。边缘网关218向令牌服务230进行认证,并请求SAS令牌,该SAS令牌仅在有限的时间段内有效,例如两分钟,五分钟,三十分钟,不超过一个小时等。边缘网关218接收并使用SAS令牌,用于保护和认证到远程系统210的AMQP(高级消息队列协议)连接,内容数据经由该连接从边缘网关218传送到远程系统210。

[0068] 在远程系统210处,经由域认证服务232提供安全性。因此,只有经由域认证服务232认证和授权的用户接口设备235才能访问远程系统210处“可用”的至少一些数据,其包括设备202生成的数据等。

[0069] 因此,如上所述,安全架构200为由设备或数据源202生成的数据提供端到端的安全性,同时在过程工厂10中进行操作以控制过程,例如从数据源202的数据开始端通过其到远程系统210的传输而被一个或多个远程应用或服务208所操作。重要的是,安全架构200提供了这种端到端的安全性,同时防止了在过程工厂10招致恶意攻击。

[0070] 注意,尽管图2将无线网关205A、205B示出为将设备或数据源202通信地连接到现场网关212,但在一些布置中,省略了无线网关205A、205B中的一个或多个,并且源数据从数据源202直接传输到现场网关212。例如,数据源202可以经由过程工厂10的大数据网络将源数据直接传输到现场网关212。一般而言,过程工厂10的大数据网络不是主干工厂网络105,大数据网络也不是用于使用工业通信协议(例如Profibus、DeviceNet、Foundation Fieldbus、ControlNet、Modbus、HART等)在设备之间传输控制信号的工业协议网络。而是,过程工厂10的大数据网络可以是为过程工厂10实现的覆盖网络,该网络可以在节点之间流传输数据,例如用于数据处理和分析目的。大数据网络的节点可以包括例如,数据源202、无线网关205A、205B和现场网关212,以及图1所示的部件7a-7c、8、11、12、15-22、26、28、35、40-46、52、55、58、60和70中的任何一个或多个和其他部件。因此,例如,对于过程工厂数据网络的许多节点,分别包括用于通常利用工业通信协议的过程工厂操作的指定接口,以及用于可以利用流传输协议的数据处理/分析操作的另一指定接口。

[0071] 相对于图2进一步指出,在一些实施例中,可以使用有线网关(未示出)代替无线网关205A、205B之一。更进一步,现场网关212和边缘网关218可以在物理上位于同一位置,例如图2中的框235所示,或者部件212和218可以物理上位于多个位置。例如,现场网关212或边缘网关218中的一个或多个可设置在过程工厂10处。另外或可替代地,现场网关212或边缘网关218中的一个或多个可远离过程工厂10设置。

[0072] 如果需要,过程工厂10可以由多于一个的现场网关212服务,并且任何数量的现场网关210可以由单个边缘网关218服务。在一些实施例中,如果需要,远程系统210可以由多于一个的边缘网关218服务。

[0073] 尽管以上示例涉及用于分析过程工厂数据的计算设备250作为远程系统210的部件,但是计算设备250可以通过以安全的方式与任何合适的通信部件进行通信来接收过程工厂数据。例如,计算设备250可以通信地连接到无线网关205A、205B、现场网关212、或边缘网关218。可以经由加密技术、防火墙、数据二极管、或任何其他合适的安全机制来保护从设备202到计算设备250的通信路径。

[0074] 一旦在计算设备250处接收到过程工厂数据,计算设备就分析过程工厂数据以识别相应过程工厂实体中的状况。然后,例如经由域认证服务将状况的指示发送到用户接口设备235。以这种方式,操作员可以查看在过程工厂内的各过程工厂实体处发生的状况。然后,操作员可以采取适当的措施来解决由这些状况造成的问题。

[0075] 过程控制系统中的分布式账本架构

[0076] 尽管在图2中将过程工厂10示出为包括单个边缘网关218,但过程工厂10可以包括几个边缘网关,每个边缘网关都充当分布式账本网络中的验证节点。图3示出了用于记录过程工厂数据的示例性分布式账本系统300。过程工厂数据可以包括过程参数数据、产品参数数据、配置数据、用户交互数据、维护数据、调试数据、工厂网络数据、产品跟踪数据、与过程工厂10中的事件相关的事件数据,例如警报、泄漏、故障、错误等,或在一个或多个过程工厂中生成或与之相关的任何其他合适的数据。

[0077] 系统300包括分布式账本312和多个节点302、304、306、308和310,这些节点可以是过程工厂10中的边缘网关,例如边缘网关218,可以是现场设备,或者可以是在过程工厂10或其他过程工厂中运行的任何合适的计算设备。每个节点维护分布式账本312的副本。当对分布式账本312进行更改时,每个节点经由网络314接收该更改并更新其分布式账本312的各自副本。分布式账本系统300中的节点302-310可以使用共识机制来决定是否适合对分布式账本312进行接收的更改。

[0078] 因此,系统中的每个节点具有其自己的分布式账本312副本,该副本与其他节点存储的分布式账本312的每个其他副本相同。由于分布式账本的去中心化性质,分布式账本系统300可以比中央权力机构数据库系统更稳健。这样,在分布式账本系统300上不存在像中心化系统中那样的单点故障。

[0079] 图4示出了分布式账本网络上用于解决交易的示例性验证网络节点和示例性交易流400。图4包括分别由虚线的左侧和右侧表示的两个时间帧420和422,节点A402和节点B404(其可以是过程工厂10中的两个边缘网关,可以是两个不同过程工厂中的两个边缘网关,可以是相同或不同过程工厂中的两个现场设备等),交易集合408A-408D,交易区块集合409A-409D,分布式账本410和区块链418。

[0080] 块传播流400可以从节点A 402在时间420接收交易406开始。当节点A402确认交易406有效时,节点A 402可以将交易添加到新生成的区块408。作为将交易406添加到区块408的部分,节点A 402可以求解密码难题并将该解包括在新生成的区块408中,作为完成生成区块408的工作的证明。可替代地,可以使用权益证明算法来生成区块408,其中节点A 402“保留”网络上使用的一定数量的数字通证,但是,网络本身确定将创造新区块的节点。在其他实施例中,可以将交易406添加到交易池中,直到池中存在足够数量的交易以形成区块为止。节点A 402可以在时间412将新创建的区块408传输到网络。在传播区块408之前或之后,节点A 402可以将区块408添加到其区块链418的副本中。

[0081] 虽然本文将工作证明和权益证明描述为用于选择节点以创造新区块的共识算法,但是这些仅是一些示例共识算法,并非旨在进行限制。可以利用其他共识算法,例如委托的权益证明,其中节点选择节点的子集(称为委托)来执行验证,而委托则轮流创造新区块。共识算法还可以包括权限证明,权重证明,拜占庭容错,tangle共识算法,区块晶格共识算法等。

[0082] 在任何情况下,交易409A-409D可以包括对状态数据库416的更新。状态数据库416可以包含由部署在区块链418上的智能合约创建的变量的当前值。诸如区块408之类的经验证区块可以包括影响状态数据库416中的状态变量的交易。在时间422,节点B 404可以在412处经由网络接收新创建的区块408。节点B 404可以通过检查对在区块408中提供的密码难题的解来验证交易块408是有效的。如果该解是准确的,则节点B 404可以将区块408添加到其区块链418中,并且对状态数据库416进行任何更新,如区块408中的交易所拒绝的。节点B 404然后可以在时间314将区块408发送到网络的其余部分。

[0083] 图5示出了在用于记录过程工厂数据的分布式账本网络上验证网络节点500的示例性部件。节点500可以包括至少一个处理器502、存储器504、通信模块506、应用集合508、外部端口510、区块链管理器514、智能合约516、和操作系统518。在一些实施例中,节点500可以通过使用区块链管理器514生成新的交易块,或者可以将交易广播到其他网络节点。类似地,节点500可以结合存储在存储器504中的智能合约516一起使用区块链管理器514来执行本文公开的功能。存储器504可以进一步包括链数据524,链数据524包括例如用于存储部署在其上的智能合约的状态的区块链的状态数据库。

[0084] 在其他实施例中,智能合约516独立于区块链管理器514或其他应用而操作。在一些实施例中,节点500不具有存储在该节点处的区块链管理器514或智能合约516。在一些实施例中,节点500可以具有比所描述的更多或更少的部件。节点500的部件在下面更详细地描述。

[0085] 节点500,作为去中心化账本系统300或另一个去中心化或中心化网络的部分,可以用作与和一个或若干过程工厂中发生的数据或事件关联的交易进行交互和/或操纵该交易的系统的部分。

[0086] 图6A示出了示例性分布式账本600,其包括在过程控制系统中具有交易的区块602-608的区块链。在一些实施例中,区块链600包括连接在一起以形成交易的区块602-608的链的若干区块602-608。为了将区块和交易加密地链接在一起,区块链600中的每个区块将其交易组织成默克尔树(Merkle Tree)。在默克尔树中,根据加密哈希算法(例如,SHA-256)对每个交易进行哈希处理,然后将所得的输出哈希值与另一交易的哈希值组合。然后,还根据加密哈希算法对组合结果进行哈希处理。然后,将此输出与其他两个交易的哈希值组合,并重复此过程,直到将区块中的所有交易组合并进行哈希处理以生成默克尔根(Merkle root)为止,该默克尔根在块602-608的头部中使用。如果该区块中的任何单个交易被篡改,则将生成不同的默克尔根,因为默克尔根是该区块中所有交易的哈希值的组合。

[0087] 即,可以使用诸如上面讨论的算法的加密哈希算法来对交易进行哈希处理,并且可以将每个交易的哈希值存储在树中。随着树的构建,可以将同一级别的每个相邻节点的哈希值哈希在一起,以创建存在于树中更高级别的新节点。因此,树顶部或默克尔根的节点取决于树中下方存储的每个交易的哈希值。每个交易可以包括数据集。数据集可以包括交易的识别数据,以及标识交易的性质和交易需要的交易数据(例如,输入和输出地址、交易值、文档哈希值、时间戳、交易费用值等)。

[0088] 为了验证区块是有效的,节点可以将区块的默克尔根与包含在区块链的其他节点的副本中的同一区块的默克尔根进行比较。因此,如果默克尔根在区块的每个节点的副本中均相同,则默克尔根可用作块中包含的交易的证据,也可用作未篡改区块内容的证据。

[0089] 在一种实施方式中,存储在区块链“上”的文档是已经根据加密哈希算法(例如,SHA-256)进行哈希处理的文档,并且所得到的输出哈希值已经被包括在被网络节点接受为满足区块链的共识规则的区块中的交易中。这样,可以稍后通过将文档的哈希值与存储在区块链上的哈希值进行比较来验证或确认文档。例如,如果文档集合导致在某个日期记录在区块链上的SHA-256哈希值,则区块链提供该文档在该日期存在的加密证据。

[0090] 将文档存储在区块链上的一种方式是向网络广播包括文档的哈希值的交易,如果交易满足网络的所有共识规则,则该交易将包括在区块中。在一些实施方式中,区块链是许可的账本,这意味着仅授权的网络参与者可以广播交易。在其他实施方式中,仅一些授权的网络参与者可以进行某些交易。例如,当现场设备确定产品的属性(例如,产品的温度、产品的体积、产品的质量、产品的密度、产品的压力等)时,指示过程工厂10中生成的产品的属性的产品参数数据可以由现场设备上传到区块链600。区块链600中可以仅包括数据的加密哈希值,从而即使通过链外方获得数据,也可以使用区块链来验证数据。

[0091] 验证网络节点可以验证签名的交易或签名的消息是由与收集测量结果的现场设备所拥有的已发布的公共密钥相对应的私有密钥签名的。在至少一种实施方式中,有效的身份证明可以被区块链网络用作共识规则。这样,任何试图添加新产品参数数据而没有与授权添加新产品参数数据的身份相匹配的加密身份证明的交易都将被网络拒绝,因为它不符合共识规则。可以为过程工厂10中的每个现场设备分配公钥/私钥对,该公钥/私钥对在区块链网络中被标识为与该现场设备相对应。另外,每个现场设备可以被授权收集某些类型的测量结果。例如,第一现场设备可以被授权收集产品的温度测量结果,而第二现场设备可以被授权收集指示制造的产品的体积的体积测量结果。如果验证网络节点接收到不是来自授权的现场设备的有关产品参数数据的交易,或者包括现场设备未被授权收集的类型的测量结果的交易,则验证网络节点将拒绝交易。

[0092] 图6B示出了包括与图6A中描述的架构不同的架构的另一示例性分布式账本650。与图6A中的分布式账本600类似,图6B中的分布式账本650包括在过程控制系统中具有交易的区块662-668的区块链660。区块链660可以被称为分布式账本650中的主区块链。除了主区块链660之外,分布式账本650还包括多个侧区块链670、680或由具有交易的区块672-676、682-686的不同过程工厂维护的侧链。例如,侧链670可以由两个过程工厂维护:工厂A和工厂B,以记录与在两个过程工厂之内或之间发生的事件有关的交易。这些交易可以包括:当工厂A将产品运送到工厂B时,工厂B以通证值的形式向工厂A发送付款。侧链680也可以由两个过程工厂维护:工厂C和工厂D,以记录与在工厂C和工厂D之内或之间发生的事件有关的交易。这些交易可以包括工厂D记录在特定时间段内从工厂C收到的油量。

[0093] 在一些实施例中,主区块链660由包括工厂A-D的若干过程工厂以及若干其他过程工厂维护。同样在一些实施例中,侧链670、680与主区块链660交互,以将它们各自的区块672-676、682-686中的至少一些交易提供给主区块链660。以这种方式,侧链670、680可以包括来自与维护它们的过程工厂有关的交易的数据。主区块链660可以包括来自与每个过程工厂有关的交易的数据。另外,侧链670、680可以包括私有或敏感数据,其不意味着在维护特定侧链的过程工厂外部共享。来自侧链670的非私有或敏感的数据可以提供给主区块链660,而私有或敏感数据不提供给主区块链660。例如,侧链670可以在工厂A和工厂B之间执行智能合约,该智能合约在工厂A从工厂B收到满足某些质量标准的产品时将通证值从工厂

A传输到工厂B。工厂A和B可能不希望通过在主区块链660上部署智能合约来向公众或一大批过程工厂公开智能合约的所有条款,或者可能不希望将对产品属性的每次测量结果都被提供给公众或一大批过程工厂。另外,随着更多的交易被添加到主区块链660,对主区块链660的存储器存储需求增加。因此,它可以减少用于验证分布式账本网络中的节点的存储器需求以在主区块链660之外存储一些交易。无论如何,当智能合约确定工厂A已经从工厂B接收了满足必需质量标准的产品时,可以将把通证值从工厂A传输到工厂B的交易提供给主区块链660。

[0094] 在一些实施例中,主区块链660是公有区块链,这意味着任何一方都可以查看分布式账本,提交要添加到账本中的新信息,或作为验证节点加入网络。侧链670、680是私有的或被许可的区块链,其在被授权参与侧区块链网络的一组实体中保持链数据私有(例如,侧链670可以是工厂A和工厂B之间私有的)。在其他实施例中,主区块链660也是被许可的区块链,但是与侧链670、680相比,主区块链具有更多数量的被授权参与区块链网络的实体。例如,主区块链660可以是包括工厂A-D和若干其他过程工厂的大量过程工厂之间私有的,而侧链670是工厂A和工厂B之间私有的。

[0095] 作为侧链的补充或替代,分布式账本650可以包括链外发生的其他形式的交易,这些交易不是主区块链660的部分。例如,诸如工厂A和工厂B之类的两方可以打开支付通道,其中在工厂A和工厂B之间交换阈值量的通证的初始交易被提供给主区块链660。然后工厂A和工厂B可以彼此交易而不在主区块链660上记录任何东西,只要它们彼此来回发送阈值量的部分,并且没有任何交易导致其中一个过程工厂具有大于阈值量。当两个过程工厂完成彼此的交易后,它们可以关闭支付通道并为主区块链660中的每个过程工厂提供最终通证量。例如,工厂A和工厂B可以在工厂A将两个通证发送到工厂B时打开支付通道。然后工厂B可以将一个通证发送回工厂A,以便每个过程工厂都具有一个通证,工厂B可以将0.5个通证发送回工厂A,依此类推,只要这两个过程工厂都没有超过两个通证。在其他实施例中,分布式账本650可以包括多个区块链层,该区块链层包括彼此独立地操作的单独的区块链。例如,第一区块链层可以记录与供应链有关的交易,而第二区块链层可以记录与通证交换有关的交易。第一区块链层可以是公有的,而第二区块链层可以是私有的,反之亦然。

[0096] 除了经由侧链或链外交易保护隐私之外,在一些实施例中,可以在公有区块链上,例如在图6A所示的区块链600上保留隐私。例如,区块链600中的交易可以通过各种加密技术来混淆交易各方的身份和交易量。

[0097] 图7A-7C示出了包括与图6A中所描述的架构不同的架构的另一示例性分布式账本700。图7A-7C中的分布式账本700包括多个本地区块链710、720,其中每个本地区块链710、720由不同方或过程工厂维护。每个本地区块链710、720包括过程控制系统中交易的区块712-716、722-726。例如,多个过程工厂可以共享资源,例如来自输油管道的油,来自发电系统的电力,通过铁路、汽车、海上或空中运输的产品,通过液体、气体、蒸汽、燃料或材料管道的产品,或来自配水系统中的水。工厂A中的现场设备可以收集有关共享资源的测量结果,例如从管道中获得的油量,并将交易中的测量数据广播到工厂A的本地区块链。类似地,工厂B中的现场设备可以收集有关共享资源的测量结果,并将交易中的测量数据广播到工厂B的本地区块链。

[0098] 如图7B所示,将来自每个本地区块链710、720的交易提供给用于各自的当事方或

过程工厂的全局区块链730,其中该全局区块链730由多个过程工厂和/或经由具有多个云计算系统的云服务来维护。例如,将来自用于工厂A的本地区块链710的区块提供给用于工厂A的全局区块链730,将来自用于工厂B的本地区块链720的区块提供给用于工厂B的全局区块链,等等。在阈值时间段或时期后,将交易的区块从本地区块链提供给相应的全局区块链。以这种方式,维护每个本地区块链的特定过程工厂内的验证节点可以从本地区块链中删除或修剪除最近区块之外已提供给全局区块链的区块,以减少存储需求。

[0099] 如图7B所示,在时期E(附图标记740)期间,将区块N(附图标记742)、区块N+1(附图标记746)和区块N+2(附图标记748)添加到用于工厂A的本地区块链710。在时期E的阈值时间段到期后,维护用于工厂A的本地区块链710的验证节点将区块N-N+2(附图标记742-746)提供给用于工厂A的全局区块链730。然后,维护用于工厂A的本地区块链710的验证节点从本地区块链710删除或修剪区块N(附图标记742)和区块N+1(附图标记744)以减少存储需求。此时的本地区块链710仅包括最近的区块,区块N+2(附图标记746)。然后在时期E+1(附图标记750)期间,将区块N+3(附图标记752)和区块N+4(附图标记754)添加到本地区块链710。在时期E+1的阈值时间段到期后,维护用于工厂A的本地区块链710的验证节点将区块N+3-N+4(附图标记752-754)提供给用于工厂A的全局区块链730。维护用于工厂A的本地区块链710的验证节点从本地区块链710删除或修剪区块N+2-N+3(附图标记746、752)。此时的本地区块链710仅包括最近的区块,N+4区块(附图标记754)。

[0100] 如图7C所示,维护全局区块链(诸如用于工厂A的全局区块链730和用于工厂B的全局区块链770)的验证节点结合了全局区块链730、770以创建具有状态区块762、764的超级区块链760。每个状态区块762、764包括特定时间段内来自全局区块链730、770的每个区块。例如,状态区块K(附图标记762)包括来自每个全局区块链730、770的相应区块N、区块N+1和区块N+2。状态区块K+1(附图标记764)包括来自每个全局区块链730、770的相应区块N+3、区块N+4和区块N+5。

[0101] 为了将区块和交易以密码方式链接在一起,超级区块链760中的每个状态区块762、764将其交易组织成Merkle树。如果状态区块中的任何单个交易被篡改,则将生成不同的Merkle根,因为Merkle根是该区块中所有交易的哈希值的组合。每个状态区块762、764的Merkle根包括在状态区块762、764的头部中。

[0102] 图7A-7C中描述的具有本地区块链、全局区块链和超级区块链的分布式账本架构700允许竞争实体验证测量数据的准确性。例如,如果工厂A向工厂B报告工厂A从两个实体之间共享的输油管道中获取了30,000加仑油,则工厂B可以从超级区块链中获取测量数据以验证此测量的准确性。还可以通过为包括测量数据的状态区块的头部计算预期Merkle根,并将状态区块的头部中的实际Merkle根与预期Merkle根进行比较,来在超级区块链760内以密码方式验证测量数据。这允许竞争实体分析超级区块链760以验证超级区块链760中的状态块762、764未被篡改。

[0103] 过程控制系统中的智能合约

[0104] 如上所述,过程控制系统可以例如在接收到处于良好状态的产品时将智能合约部署到分布式账本以交换值。智能合约也可以部署到分布式账本以允许诸如现场设备之类的机器自行进行交易,而无需人工干预。

[0105] 图8示出了过程控制系统内的分布式账本网络中的示例性智能合约状态806。图8

包括区块链802、交易的区块804和安全写请求智能合约状态806。智能合约可由分布式账本网络或区块链网络中的任何参与者(例如,工厂操作员、配置工程师、过程系统设计者等)部署,以便例如为安全写请求建立合约状态806。部署的智能合约可以向区块链网络中的其他参与者暴露方法和数据。智能合约状态中的某些数据可以是私有数据,只能通过调用智能合约的方法进行更改,或仅由授权的区块链参与者进行更改。更改智能合约状态的一种方法是将交易广播到分布式账本网络。如果广播的交易满足共识规则,则网络验证器可以将交易包括在区块中。将向智能合约发送数据的交易包含在区块链中可以导致验证节点更新智能合约的状态数据库,从而允许网络参与者访问丰富的状态机制来管理安全写请求,并最终将参数数据写到安全仪表系统(SIS)设备。

[0106] 安全写请求智能合约状态806可以包括用于识别提交安全写请求的操作员、操作员用于提交安全写请求的计算设备和/或作为安全写请求的目标的SIS设备的多条数据。在某些实施例中,可以通过分配给操作员的电子钱包的加密公钥来识别操作员。如果操作员的电子钱包在操作员的计算设备上进行操作,则可以通过与操作员相同的加密公钥来识别操作员的计算设备。在其他实施例中,操作员的计算设备可以通过其他网络参与者已知属于操作员的计算设备的其他加密公钥来识别。

[0107] 在一些实施例中,合约所有者可以为SIS设备选择唯一的ID,使得发送到智能合约的后续交易和数据可以通过ID号识别SIS设备。例如,每个SIS设备在智能合约中可以具有不同的唯一标识符。合约所有者还可以指定被授权执行安全写操作的操作员和/或计算设备的标识符。发送到智能合约的后续数据可以包括由与识别智能合约中的操作员和/或计算设备的公钥相对应的私钥签名的消息,从而提供加密证明:交易是由授权的操作员和/或授权的计算设备发起的。私钥和公钥可以仅操作员/计算设备单独管理,以将可能尝试伪造交易的任何攻击者的攻击面减到最小(例如,操作员/计算设备离线生成公钥/私钥对,并且仅将公钥提供给其他网络参与者)。可以根据安全地存储的种子值(例如,在一张物理纸上或一张纸的多个副本上)来生成操作员和/或计算设备的私钥,使得在数据丢失的情况可以恢复私钥。

[0108] 为了将参数数据写入SIS设备,安全写请求智能合约状态806可以获取安全写请求的证据。用于安全写请求的证据可以包括要在SIS设备中改变的参数的名称和/或该参数的路径信息。证据还可以包括新的参数值,并且在一些实施例中,证据可以包括循环冗余校验(CRC)值或其他错误校验值以及新的参数值,以确保参数信息完整无损,未被破坏。在一些实施例中,响应于接收到参数信息,智能合约可以向操作员的计算设备提供确认对话框,该确认对话框包括SIS设备的名称、要在SIS设备中改变的参数的名称和/或路径、新的参数值以及操作员确认安全写请求的确认按钮。在这种情况下,证据可以包括操作员是否选择了确认按钮的指示。

[0109] 操作员和/或操作员的计算设备可以将包括证据的交易广播到区块链802。可以对证据进行加密签名以提供加密身份证明,即证据来自被授权执行安全写请求的操作员和/或操作员的计算设备。因此,智能合约可以将所提供的身份与被授权执行安全写请求的操作员和/或计算设备的列表进行比较。在一些实施例中,智能合约可以将所提供的身份与被授权对作为安全写请求的目标的特定SIS设备执行安全写请求的操作员和/或计算设备的列表进行比较。

[0110] 安全写请求智能合约状态806的另一方面是智能合约数据。可以将智能合约数据认为是根据面向对象编程范例创建的对象中的私有和公有数据,因为可以直接从对象外部更新智能合约数据,或者可以仅以有限的方式更新智能合约数据,例如通过调用智能合约的方法。智能合约数据可以包括要在SIS设备中改变的参数的名称和/或路径,以及新的参数值。在一些实施例中,智能合约数据可以包括参数信息是否已经被完整接收的指示。例如,包括要改变的参数和参数信息的交易也可以包括CRC值或其他错误校验值。智能合约可以基于要改变的参数和参数信息生成预期CRC值,并且将预期CRC值与接收到的CRC值进行比较。如果预期CRC值与接收到的CRC值匹配,则智能合约可以确定参数信息已经被完整接收。同样在一些实施例中,智能合约数据可以包括是否确认了安全写请求的指示。例如,如果智能合约通过操作员和/或操作员的计算设备接收到指示操作员选择了确认按钮的交易,则智能合约可以确定安全写请求已被确认。

[0111] 例如,如图8所示,智能合约数据可以包括锁定/解锁SIS设备的参数,指示设置锁定SIS设备的参数的参数值“1”或“锁定”,指示已确认安全写请求的确认值“1”、“是”或“真”,以及指示参数信息未损坏的接收到的数据完整值“1”、“是”或“真”。因此,智能合约可以确定应该将新参数值提供给SIS设备。然后,智能合约可以将参数信息提供给SIS设备或通信耦合到SIS设备的控制器,以执行安全数据写入。

[0112] 在一些实施例中,当发送安全写请求的操作员和/或计算设备被授权执行对目标SIS设备的安全数据写入,参数信息未损坏,并且确认了安全写请求时,安全写请求智能合约可以向目标SIS设备或通信耦合到目标SIS设备的控制器提供参数信息。在其他实施例中,安全写请求智能合约不确定参数信息是否被完整接收。作为替代,响应于接收到安全写请求,安全写请求智能合约将包括参数名称和/或参数路径、新参数值和CRC值的参数信息的第一实例提供给目标SIS设备或控制器。响应于接收到对安全写请求的确认,安全写请求智能合约还将参数信息的第二实例提供给目标SIS设备或控制器。然后,控制器或目标SIS设备确定两个实例中的参数信息是否相同以及参数信息是否已被完整接收。当两个实例中的参数信息相同并且参数信息已被完整接收时,控制器或目标SIS设备会将参数的新参数值写入目标SIS设备。

[0113] 虽然图8示出了用于安全写请求的智能合约状态806,这仅是为了便于说明的一个示例智能合约。分布式账本网络中的参与者(例如,工厂操作员、配置工程师、过程控制系统设计者等)可以部署与过程控制相关的任何合适的智能合约。

[0114] 在另一个示例中,可以部署智能合约,该智能合约获取过程工厂10内经历故障的设备的设备信息,并响应于接收到共享设备信息的请求,将设备信息提供给设备供应商。具体而言,当过程工厂10内的设备经历故障时,例如过程工厂实体,该设备可以将交易发送到存储在分布式账本上的智能合约的地址。可以对该交易进行加密签名以提供该交易来自设备的加密身份证明。在其他实施例中,过程工厂实体可以将故障的指示发送到控制器、现场设备或其他过程控制设备,该控制器、现场设备或其他过程控制设备充当证据谕示并生成交易。无论如何,交易可以包括设备的设备信息,例如设备的标识信息,设备的品牌、型号和年份,设备的维护历史,故障的类型,设备内的损坏部件等。

[0115] 在一些实施例中,智能合约将设备信息传输到过程工厂10中的维护人员的计算设备,以供维护人员审查设备信息。在审查设备信息后,维护人员可以确定设备供应商需要审

查设备信息,以进一步调查故障和/或提供替换设备或替换部件。因此,维护人员的计算设备可以生成交易,该交易请求智能合约将设备信息提供给设备供应商。可以对该交易进行加密签名,以提供该交易来自维护人员的加密身份证明。响应于确定向设备供应商提供设备信息的请求来自授权的维护人员,智能合约可以将设备信息提供给设备供应商的计算设备。

[0116] 另一示例智能合约是一种智能合约,其从第一过程工厂获得通证值,确定符合某些质量标准的产品从第二过程工厂转移至第一过程工厂,并将该通证值提供给第二过程工厂。在一些实施例中,智能合约可以从诸如第一过程工厂中的现场设备之类的证据谕示接收到已经在第一过程工厂处接收到产品的指示。现场设备还可以提供与产品相关的参数数据,智能合约将其与质量指标集进行比较以确定产品是否符合质量标准。如果产品符合质量标准,则智能合约将通证值提供给第二过程工厂。否则,智能合约可以将通证值返回给第一过程工厂。

[0117] 过程控制系统中分布式账本中记录的交易类型

[0118] 过程控制系统分布式账本可以包括与过程控制有关的许多不同类型的交易。这些交易可以包括:1)与在过程工厂10处的产品的交付或接收以及所交付/接收的数量有关的交易;2)与过程工厂10内的设备(例如操作员工作站、服务器设备、控制器、I/O设备、网络设备、现场设备等)处的软件或固件更新有关的交易;3)与过程工厂10中的质量控制、生产或监管报告有关的交易;4)记录过程工厂数据的交易;5)通过产品跟踪数据记录产销监管链的交易。

[0119] 在某些场景中,例如,将交易提供给智能合约以改变智能合约状态。在其他场景中,不将交易提供给智能合约,而只是作为与一个或多个过程工厂有关的信息的安全、不变和免信任记录而记录在分布式账本中。

[0120] 与产品交付或接收以及已交付/已接收的数量有关的交易

[0121] 图9示出了表示报告在过程工厂10处从输油管道接收的油量的证据交易的示例性交易906。虽然在图9中的示例性交易906报告了来自输油管道的油量,但这仅是出于易于说明的目的的一个示例。也可以报告其他来源的其他材料或产品,例如来自发电系统的电力,通过铁路、汽车、海上或空中运输的产品,通过液体、气体、蒸汽、燃料或材料管道的产品,或来自配水系统的水。无论如何,交易906可以由充当证据谕示的现场设备生成。当现场设备检测到流过阀的油时,现场设备将交易906广播到区块链902以包括在诸如区块904之类的区块中。

[0122] 交易906可以包括交易ID和诸如工厂A中的现场设备456之类的发起者(通过加密身份证明来识别)。交易906还可以包括与产品有关的识别信息,产品的提供者(例如,油生产商)以及与所接收的产品的数量有关的信息。例如,现场设备可以是流速传感器,其确定在特定时间段(例如,一个小时、一天等)上在工厂A处获得的油的体积,并且将体积包括在交易中。在其他实施例中,现场设备可以在一系列交易中包括各个时间段的多个流速,并且作为时间的函数的流速可以用于确定在工厂A处接收的油量。此外,交易906可以包括关于事件、产品标识符和产品提供者标识符的信息的加密哈希值。在另一实施方式中,关于事件、产品标识符和产品提供者标识符的信息不存储为加密哈希值,而是可由观察者或其他网络参与者在区块904中直接访问。

[0123] 尽管在该示例中,接收产品的过程工厂10的现场设备生成交易,但是提供产品的过程工厂10的现场设备或其他实体可以生成交易。该交易可以附加于或替代由接收产品的过程工厂10的现场设备进行的交易而生成。与过程工厂内的设备处的软件或固件更新有关的交易

[0124] 为了防止将未经授权的软件或固件引入到过程工厂10中,可以将对过程工厂10中的设备的软件和固件更新以数字方式记录在分布式账本中,例如上述分布式账本中。分布式账本可以维护对过程工厂10中的设备的每个软件和固件更新的记录,包括更新的时间和日期,执行更新的用户的身份(通过加密身份证明),改变到软件的先前版本和/或软件的新版本。过程工厂10内的服务器设备12或其他计算设备可以连续或周期性地(例如每秒一次、每分钟一次、每小时一次、每天一次等)获取在过程工厂10中的设备中运行的软件和固件的当前版本。服务器设备12还可以从分布式账本中获取交易,并将设备中的当前软件或固件与分布式账本中记录的软件或固件的最新版本进行比较。在一些实施例中,分布式账本存储软件或固件的新版本的加密哈希值,并且将在设备中执行的当前软件或固件与加密哈希值进行比较以验证该软件或固件未被篡改。

[0125] 如果设备中的当前软件或固件与分布式账本中记录的软件或固件的最新版本不匹配,则服务器设备12可以阻止设备执行当前软件或固件。在一些实施例中,服务器设备12可以例如通过将先前版本下载到设备来使该设备中的软件或固件恢复到先前版本。以这种方式,未经授权的用户不能篡改在过程工厂10中执行的软件或固件。

[0126] 图10示出了表示报告过程工厂10内的设备中的软件或固件更新的证据交易的示例性交易1006。交易1006可以由接收更新的设备(诸如操作员工作站、另一用户接口设备8、服务器设备12、控制器11、I/O设备26、28、网络设备、现场设备15-22、40-46等)生成。过程工厂10中的网络设备可以包括例如无线网关35、路由器58、无线接入点7a、55、边缘网关、无线适配器52等。

[0127] 交易1006可以包括交易ID和修改软件或固件的发起者,例如John Doe(通过加密身份证明来识别)。交易1006还可包括用于执行软件或固件的设备的标识信息(操作员工作站1234)(通过加密身份证明来识别),包括版本号以及更新时间和日期的描述(“更新为版本10.3.1.4,于2019年1月15日上午6:02”)。此外,交易1006可以包括用于软件的新版本的软件指令的加密哈希值。在另一实施方式中,该软件的新版本不存储为加密哈希值,而是可由观察者或其他网络参与者在区块1004中直接访问。在一些实施例中,共识规则指示仅授权用户可以在分布式账本上记录软件或固件更新。因此,在将交易1006广播到分布式账本时,如果发起者是授权用户,则验证节点验证交易1006。如果发起者不是授权用户,则不将交易1006包括在分布式账本中,并且对该软件的更新将与分布式账本中记录的软件的最新版本不匹配。

[0128] 在示例性场景中,在2019年1月15日上午6:03,过程工厂10中的服务器设备12获得在操作员工作站1234中执行的软件的状态,并例如通过对在操作员工作站1234中执行的软件指令执行加密哈希处理来将该软件与分布式账本中的用于软件的新版本的软件指令的加密哈希值进行比较。如果加密哈希值相同,则服务器设备12确定软件未被篡改。另一方面,如果加密哈希值不同,则服务器设备确定软件已被篡改,并阻止操作员工作站1234以其当前状态执行软件。然后,服务器设备12将软件的先前状态下载到操作员工作站1234,并且

操作员工作站1234恢复以其先前状态执行软件。

[0129] 与过程工厂中的质量控制、生产或监管报告相关的交易

[0130] 过程工厂具有报告和记录保存要求,以遵从诸如环境保护局(EPA)之类的监管机构。例如,EPA颁布了泄漏检测和维修(LDAR)法规,以使来自例如泄漏的设备(如过程工厂中的阀、泵和连接器)的泄漏的挥发性有机化合物和有害空气污染物的排放最小化。为了遵从法规并提供安全、不变和免信任的记录,可以将监管数据记录在分布式账本中。例如,响应于诸如警报、错误、泄漏、维修事件、过程重大事件、纠正措施等触发事件,诸如现场设备、控制器或过程工厂实体之类的过程控制元件可以生成交易,包括来自触发事件的数据,例如事件发生的时间、事件的持续时间、事件所涉及的过程工厂实体的过程参数值、事件所涉及的产品的产品参数值等。然后将监管数据记录在分布式账本中,以便监管机构可以审查数据。

[0131] 在一些实施例中,当触发事件发生时,过程控制元件之一检测到触发事件。然后,过程控制元件向其他过程控制元件通知触发事件,并将唯一的标识符分配给触发事件。以这种方式,每个过程控制元件可以收集与触发事件有关的测量结果,并且将交易广播到分布式账本,其中每个交易包括用于触发事件的相同唯一标识符。

[0132] 在一些实施例中,将监管数据记录在公有区块链中,使得任何人可以查看来自过程工厂10的监管数据。在其他实施例中,将监管数据记录在过程工厂10和监管机构可访问的私有或许可的区块链中。在其他实施例中,将监管数据记录在过程工厂网络中的多个过程工厂以及监管机构可访问的私有或许可的区块链中。

[0133] 图11示出了表示报告过程参数或产品参数数据的证据交易的示例性交易1106。交易1106可以由过程工厂实体生成,该过程工厂实体可以是过程工厂10内用于包含、转化、产生或转移物理材料的过程的一部分中的设备,诸如阀、罐、混合器、泵、加热器等。

[0134] 交易1106可以包括交易ID和收集产品或过程参数测量结果的发起者(加热器Y-001)(通过加密身份证明来识别)。交易1106还可以包括与产品有关的标识信息、产品参数数据(例如,产品的温度已在100℃下保持2小时)以及过程参数数据(例如,加热器Y-001中的温度为120℃)。当响应于触发事件而生成交易1106时,交易1106还可包括用于触发事件的标识信息和来自触发事件的事件数据,例如触发事件的时间、触发事件的持续时间、和/或触发事件的描述。在某些场景中,多个过程工厂实体响应于同一触发事件而生成交易,并且彼此通信来为该触发事件分配唯一的标识符。以这种方式,诸如审查分布式账本的监管机构之类的当事方可以查看与同一触发事件相关联的每个交易。

[0135] 此外,交易1106可以包括产品和/或过程参数数据以及与触发事件有关的数据的加密哈希值。在另一个实施方式中,产品参数数据、过程参数数据以及与触发事件有关的其他数据不存储为加密哈希值,而是可由观察者或其他网络参与者在区块1104中直接访问。

[0136] 如上所述,触发事件可以包括警报、错误、泄漏、维修事件、纠正措施等。在示例场景中,触发事件可以是由安全阀的打开引起的过程工厂10中的泄漏。当过程控制系统中的压力超过阈值压力量时,安全阀可以打开,或者安全阀可以与在阀处检测到的压力成比例地打开。当安全阀打开时,安全阀或一个或多个其他现场设备可以检测到打开的时间、打开的持续时间、打开的大小、安全阀打开时安全阀中的压力、从安全阀泄漏出的流体的流速、和/或流体的属性,例如流体的温度、流体的类型等。在一些实施例中,从安全阀泄漏出的流

体的量也可以基于安全阀的流速,打开的大小和打开的持续时间来确定。然后,安全阀和/或一个或几个其他现场设备可以生成交易,类似于交易1106,包括针对由安全阀的打开引起的泄漏的触发事件的相同的唯一标识符,和/或针对触发事件的相同描述。每个交易还可以包括过程参数数据,例如打开的时间、打开的大小、安全阀中的压力、从安全阀泄漏出的流体的流速等。交易还可以包括产品参数数据,诸如流体的属性。然后,生成交易的设备将交易广播到分布式账本网络,以供验证节点(例如边缘网关)确认交易有效并将交易包括在分布式账本中。

[0137] 审查事件的监管机构可以从包括在具有触发事件标识符的交易中的分布式账本中请求并获得事件数据。然后,监管机构的计算设备(例如,如图2所示的计算设备235)可以在用户界面上呈现事件数据。在其他实施例中,分布式账本包括事件数据的加密哈希值,其响应于对认证事件数据的请求而被提供给监管机构的计算设备235。事件数据是从其他数据源(例如通信连接到过程工厂10中的服务器设备12的数据库)获得的。监管机构的计算设备235然后计算获得的事件数据的加密哈希值,并将获得的事件数据的加密哈希值与来自分布式账本的事件数据的加密哈希值进行比较。如果加密哈希值相同,则监管机构的计算设备235确定来自数据库的事件数据未被篡改。否则,监管机构的计算设备235确定来自数据库的事件数据不可靠。

[0138] 记录过程工厂数据的交易

[0139] 除了将过程参数数据和产品参数数据记录在与触发事件有关的交易中之外,过程和产品参数数据还可以包括在与触发事件不相关的交易中,例如,用于维护过程工厂10的操作的准确记录。其他类型的过程工厂数据也可以包括在交易中,例如配置数据、用户交互数据、维护数据、调试数据、工厂网络数据、产品跟踪数据、或在一个或多个过程工厂中生成或与一个或多个过程工厂相关的任何其他合适的数据。用户交互数据可以包括由操作员或配置工程师在例如操作员工作站处执行的操作。操作员可以通过操作员工作站处的用户控件调整设置点、响应警报等,其可以作为用户交互数据包括在交易中。以这种方式,当竞争实体质疑在过程工厂10中制造的产品的质量时,过程工厂10可从与该产品有关的分布式账本中获取过程工厂数据。然后,过程工厂10可以审查制造产品所涉及的每个过程工厂实体的记录,制造产品时过程工厂实体的参数值,在制造过程中各个阶段的产品的参数值,在产品的制造期间发生的触发事件等。因此,过程工厂10可以确定是否适当地制造产品以符合某些质量标准,或者在生产期间是否发生了导致产品不符合质量标准的异常。

[0140] 过程工厂数据还可以用于对产品进行根本原因分析。例如,产品可能具有预测的保存期,例如汽油,其半寿命期可能小于一个月。在一些实施例中,计算设备可以基于产品的特性来预测产品的保存期,产品的特性包括在制造产品时记录在分布式账本中的过程参数数据和产品参数数据。计算设备还可基于具有相似组成部分的相似产品的历史数据和/或制造期间的过程参数数据和产品参数数据来预测产品的保存期。具体而言,计算设备可以基于相同类型的产品(例如,汽油)的平均保存期来预测产品的保存期。

[0141] 计算设备然后可以基于产品中组成部分的质量从平均保存期增加或减少预测的保存期。例如,可以将组成部分分类为高于平均值、平均值或低于平均值。组成部分的指示可以与相关联的等级或质量分数一起存储在数据库中。可以将具有质量分数低于第一阈值分数或排名低于第一阈值排名的组成部分分类为低于平均值。可以将具有质量分数高于第

一阈值分数且低于第二阈值分数或排名高于第一阈值排名且低于第二阈值排名的组成部分分类为平均值。可以将具有质量分数高于第二阈值分数或排名高于第二阈值排名的组成部分分类为高于平均值。

[0142] 计算设备还可以根据产品的属性(例如产品的温度、产品的体积、产品的质量、产品的密度、产品的压力、产品的粘度、产品的化学组成等)增加或减少预测的保存期。例如,计算设备可以为每个属性分配质量分数,并基于每个质量分数调整预测的保存期。

[0143] 在一些实施例中,计算设备可以基于先前产品的实际保存期、先前产品中的组成部分以及先前产品的属性来生成机器学习模型以预测产品的保存期。

[0144] 此外,当产品的实际保存期与预测的保存期不同时,计算设备可以从分布式账本中获取与该产品相关的过程工厂数据以识别原因。例如,由于产品中质量较差的组成部分,实际保存期可能低于预期的保存期。在另一个示例中,由于过程工厂10中的加热器将产品加热到不期望的温度,因此实际保存期可能低于预期的保存期。

[0145] 通过产品跟踪数据记录产销监管链的交易

[0146] 为了提供供应链中产品的产销监管链的准确记录,可以生成交易,其中交易包括产品的来源或供应商以及处理产品的实体(例如制造商、分销商、分销设施、零售商和购买产品的客户)的标识信息。具体而言,交易可以包括具有产品的标识信息、产品供应商/制造商的标识信息、产品每个组成部分的制造商/供应商的标识信息、供应链中接收和处理产品的实体的标识信息、销售产品的零售商的标识信息、和/或购买产品的客户的标识信息的产品跟踪数据。当产品从一个实体(例如,过程工厂)交付到另一实体(例如,仓库)时,交付实体可以生成交易,该交易包括交付实体的标识信息、接收实体的标识信息以及产品在被转移到接收实体的指示。

[0147] 因此,诸如顾客之类的用户可以经由用户接口设备使用产品的标识信息从分布式账本中获取涉及特定产品的每个交易。然后,用户接口设备可以通过用户界面显示产品的供应商或来源以及处理产品的实体(例如制造商、分销商、分销设施、零售商和购买产品的客户)的指示。用户接口设备还可以通过用户界面显示产品组成部分的指示。然后,用户可以使用组成部分的标识信息从分布式账本中检索涉及产品特定组成部分的每个交易。然后,用户接口设备可以通过用户界面显示组成部分的供应商或来源以及处理组成部分的实体(例如制造商、分销商、分销设施等)的指示。

[0148] 在一些实施例中,产品包装可包括产品标识符,例如条形码或射频识别(RFID)标签,其在被扫描时为产品提供来自分布式账本的数据。例如,用户可以通过移动设备扫描条形码或RFID标签,然后在移动设备上呈现产品的供应商或来源以及处理该产品的实体的指示。

[0149] 图12示出了表示用于使用分布式账本在过程控制系统中记录数据的示例性方法1200的流程图。方法1200可以由过程工厂10内的现场设备15-22、40-46、过程工厂10内的控制器11或过程工厂10内的另一计算设备(例如,操作员工作站、服务器设备12、用户接口设备8、I/O设备26、28、网络设备35等)执行。

[0150] 在框1202处,从现场设备获得与过程控制元件有关的数据。过程控制元件可以是现场设备、控制器或过程工厂实体,例如阀、罐、混合器、泵、热交换器等。数据可以包括过程工厂数据,例如用于过程控制元件的参数的过程参数数据(例如,罐填充液位、泵速、热交换

器中的温度),以及用于进入、离开过程控制元件、在过程控制元件内和/或由过程控制元件控制的产品的产品参数数据(例如,罐中流体的温度,离开阀的流体流速)。然后,在框1204处,生成交易,该交易包括与过程控制元件有关的过程工厂数据。生成交易的实体(例如,现场设备)利用对于该实体唯一的加密签名对交易进行签名(框1206),并利用该实体的身份数据(例如该实体拥有的公共加密密钥)扩充交易(框1208)。例如,交易可以由对应于实体拥有的公共加密密钥的私有加密密钥签名。

[0151] 在框1210处,将交易传送到分布式账本网络中的参与者。例如,现场设备可以将交易广播到分布式账本网络。然后,诸如边缘网关之类的验证节点可以确认交易有效,将交易添加到交易的区块中,求解密码难题,并将解包括在新生成的区块中,以作为完成生成区块的工作的证明。然后,验证节点可以将新生成的区块提供给分布式账本网络中的每个其他验证节点,以将新生成的区块包括在它们各自的分布式账本的副本中。

[0152] 在一些实施例中,验证节点根据共识规则集来确认交易,并且当交易满足每个共识规则时,将交易添加到区块。例如,共识规则可以包括交易的发起者提供身份证明,使得只有批准的实体才可以向分布式账本发起交易。共识规则可以要求区块和交易遵守格式要求,并提供有关交易的某些元信息(例如,区块必须小于大小限制,交易必须包含多个字段,等等)。接收到该交易的验证节点会忽略任何不满足共识规则的交易,并且该交易不会传播到其他节点。

[0153] 验证节点包括收发器,用以与广播具有分布式账本数据(例如过程工厂数据)的交易的现场设备、控制器或过程工厂10中的其他计算设备进行通信。另外,验证节点可以包括用于存储分布式账本的副本的存储器,该存储器包括用于存储部署在分布式账本上的智能合约的状态的状态数据库。此外,验证节点可以包括应用,例如过程数据验证器,该过程数据验证器将共识规则集应用于分布式账本数据,并且如果分布式账本数据满足共识规则,则将分布式账本数据附加到验证节点的分布式账本副本。

[0154] 图13示出了表示用于使用分布式账本在过程控制系统中安全计量不可信数据的示例性方法1300的流程图。方法1300可以由过程工厂10内的现场设备15-22、40-46、过程工厂10内的控制器11或过程工厂10内的另一计算设备(例如,操作员工作站、服务器设备12、用户接口设备8、I/O设备26、28、网络设备35等)执行。方法1300还可以由诸如边缘网关之类的验证节点或现场设备和验证节点的组合来执行。

[0155] 在框1302处,从现场设备获得与过程控制元件有关的数据。过程控制元件可以是现场设备、控制器或过程工厂实体,例如阀、罐、混合器、泵、热交换器等。数据可以包括过程工厂数据,例如用于过程控制元件的参数的过程参数数据(例如,罐填充液位、泵速、热交换器中的温度),以及用于进入、离开过程控制元件、在过程控制元件内和/或由过程控制元件控制的产品的产品参数数据(例如,罐中流体的温度,离开阀的流体流速)。然后,在框1304处,生成交易,该交易包括与过程控制元件有关的过程工厂数据。生成交易的实体(例如,现场设备)利用对于该实体唯一的加密签名对交易进行签名,并利用该实体的身份数据(例如该实体拥有的公共加密密钥)扩充交易。例如,交易可以由对应于实体拥有的公共加密密钥的私有加密密钥签名。

[0156] 在框1306处,将交易传送到分布式账本网络中的参与者。可能有多个本地分布式账本,其中每个本地分布式账本由不同的当事方或过程工厂维护。例如,工厂A的本地分布

式账本网络可以由工厂A内的边缘网关组成。边缘网关可以记录交易,该交易包括与工厂A内的事件和设备相关的过程工厂数据。然后,将交易添加到本地分布式账本网络达阈值时间段或时期。在阈值时间段到期之后(框1308),维护本地分布式账本的验证节点将在阈值时间段期间生成的交易或交易的区块提供给全局分布式账本网络(框1310)。全局分布式账本网络可以包括跨多个过程工厂的验证节点,例如具有多个云计算系统的云服务。验证节点可以为每个过程工厂维护全局分布式账本(例如,全局区块链)。然后,本地分布式账本网络中的验证节点可以从本地分布式账本中删除或修剪除最近区块之外已提供给全局分布式账本的区块。本地分布式账本的验证节点可以继续生成区块,在每个时期到期后将区块广播到全局分布式账本网络,并在区块已添加到全局区块链后删除区块的本地副本。

[0157] 同样在一些实施例中,组合用于各个实体或过程工厂的每个全局区块链以创建具有状态区块的超级区块链。每个状态区块包括来自全局区块链的对应于特定时间段或时期的每个区块。

[0158] 图14示出了表示用于使用分布式账本在过程控制系统中记录质量控制、生产或监管数据的示例性方法1400的流程图。方法1400可以由过程工厂10内的现场设备15-22、40-46、过程工厂10内的控制器11或过程工厂10内的另一计算设备(例如,操作员工作站、服务器设备12、用户接口设备8、I/O设备26、28、网络设备35等)执行。

[0159] 在框1402处,由过程控制元件检测与质量控制有关的触发事件。触发事件可以是警报、错误、泄漏、维修事件、过程重大事件、纠正措施等。在一些实施例中,将触发事件的指示提供给现场设备、控制器或过程工厂10内的其他计算设备。在其他实施例中,现场设备、控制器或其他计算设备检测触发事件。

[0160] 在任何情况下,在框1404处,获得触发事件的事件数据。事件数据可包括触发事件的唯一标识符、触发事件的时间、触发事件的持续时间、触发事件的描述、触发事件中涉及的过程控制元件的标识信息、触发事件期间由过程控制元件制造的产品的标识信息等。然后,在框1406处,生成交易,该交易包括触发事件的事件数据和/或事件数据的加密哈希值。交易还可以包括交易发起者的标识信息、发生触发事件时产品的产品参数数据、触发事件期间过程控制元件的过程参数数据、或任何其他合适的信息。在一些实施例中,过程工厂10内的多个现场设备、控制器或其他计算设备可以生成与触发事件有关的交易。例如,第一现场设备可以生成包括触发事件时加热器中的温度的交易,而第二现场设备可以生成包括触发事件时泵的速度的交易。

[0161] 在框1408处,将交易传送到分布式账本网络中的参与者。例如,现场设备可以将交易广播到分布式账本网络。然后,诸如边缘网关之类的验证节点可以确认交易有效,将交易添加到交易区块中,求解密码难题,并将解包括在新生成的区块中,以作为完成生成区块的工作的证明。然后,验证节点可以将新生成的区块提供给分布式账本网络中的每个其他验证节点,以将新生成的区块包括在它们各自的分布式账本的副本中。

[0162] 如上所述,交易可以包括触发事件的事件数据的加密哈希值、和/或触发事件的事件数据和与该触发事件有关的其他过程工厂数据的组合。除了生成交易之外,现场设备还可以将事件数据或与触发事件有关的其他过程工厂数据提供给服务器设备12以存储在例如数据库中(框1410)。

[0163] 然后,为了认证事件数据,将数据库中存储的事件数据与分布式账本中包括的加

密哈希值进行比较(框1412)。如果存在匹配,则事件数据未被篡改。例如,审查事件的监管机构可以从分布式账本中请求并获得事件数据的加密哈希值,其包括在具有触发事件标识符的交易中。从其他数据源(例如通信耦合到过程工厂10中的服务器设备12的数据库)获得事件数据。监管机构的计算设备然后计算获得的事件数据的加密哈希值,并将所获得的事件数据的加密哈希值与来自分布式账本的事件数据的加密哈希值进行比较。如果加密哈希值相同,则监管机构的计算设备确定来自数据库的事件数据未被篡改。否则,监管机构的计算设备确定来自数据库的事件数据不可靠。在其他实施例中,过程工厂10内的计算设备获取存储在数据库中的事件数据以及来自分布式账本的事件数据的加密哈希值,并将事件数据与加密哈希值进行比较以认证事件数据。

[0164] 图15示出了表示用于使用分布式账本记录过程控制系统和所连接的仪器中的软件或固件的状态的示例性方法1500的流程图。方法1500可以由过程工厂10内的现场设备15-22、40-46,过程工厂10内的控制器11或过程工厂10内的另一计算设备(例如,操作员工作站、服务器设备12、用户接口设备8、I/O设备26、28、网络设备35等)执行。

[0165] 在框1502处,获得在过程工厂10的设备上执行的软件或固件的当前状态。例如,在过程工厂10内的接收软件或固件更新的设备可以获得软件或固件的新版本。该设备可以是操作员工作站、另一用户接口设备8、服务器设备12、控制器11、I/O设备26、28、网络设备35、现场设备15-22、40-46等。然后在框1504处,设备可以生成交易,该交易包括对软件或固件的当前状态的指示。例如,指示可以是用于软件的新版本的软件指令的加密哈希值。交易还可以包括通过加密身份证明所识别的修改软件或固件的发起者、执行软件或固件的设备的标识信息、更新的描述、更新的时间和日期等。

[0166] 在框1506处,将交易传送到分布式账本网络中的参与者。例如,计算设备可以将交易广播到分布式账本网络。然后,诸如边缘网关之类的验证节点可以确认交易有效,将交易添加到交易的区块中,求解密码难题,并将解包括在新生成的区块中,以作为完成生成区块的工作的证明。然后,验证节点可以将新生成的区块提供给分布式账本网络中的每个其他验证节点,以将新生成的区块包括在它们各自的分布式账本的副本中。

[0167] 在一些实施例中,验证节点根据共识规则集来确认交易,并且当交易满足每个共识规则时,将交易添加到区块。此外在一些实施例中,共识规则指示仅授权用户可以在分布式账本上记录软件或固件更新。因此,在将交易广播到分布式账本时,如果发起者是授权用户,则验证节点确认交易有效。如果发起者不是授权用户,则不将该交易包括在分布式账本中,并且对软件的更新将与分布式账本中记录的软件的最新版本不匹配。

[0168] 无论如何,在框1508中,获得在过程工厂10中的设备上执行的软件或固件的状态。例如,过程工厂10内的服务器设备12或其他计算设备可以连续或周期性地(例如每秒一次、每分钟一次、每小时一次、每天一次等)获得在过程工厂10中的设备中运行的软件和固件的当前版本。然后,将在服务器设备12处获得的软件或固件的状态与分布式账本中存储的软件或固件的加密哈希值进行比较,以验证该软件或固件未被篡改(框1510)。如果软件或固件的状态与存储在分布式账本中的软件或固件的加密哈希值匹配,则软件或固件继续在设备上执行(框1514)。否则,服务器设备12确定该软件已被篡改,并阻止该设备以其当前状态执行该软件(框1512)。在一些实施例中,服务器设备12然后将软件的先前状态下载到设备,并且设备以其先前状态恢复执行软件。

[0169] 图16示出了表示用于使用分布式账本在过程控制系统中创建智能合约的示例性方法1600的流程图。方法1600可以由过程工厂10内的现场设备15-22、40-46、过程工厂10内的控制器11或过程工厂10内的另一计算设备(例如,操作员工作站、服务器设备12、用户接口设备8、I/O设备26、28、网络设备35等)执行。

[0170] 在框1602处,生成与一个或多个过程工厂有关的智能合约。例如,当工厂A从工厂B接收到符合某些质量标准的产品时,智能合约可以将通证值从工厂A传输到工厂B。过程控制系统中的另一个示例智能合约可以包括安全写请求智能合约,该安全写请求智能合约允许工厂人员将参数数据写入过程工厂10中的SIS设备。过程控制系统中的又一个示例智能合约可以包括设备信息智能合约,该设备信息智能合约从经历故障的设备获得设备信息,并响应于接收到共享设备信息的请求而将设备信息提供给设备供应商。

[0171] 在框1604处,将智能合约部署到存储在分布式账本上的地址。部署的智能合约可以向分布式账本网络中的其他参与者暴露方法和数据。智能合约状态中的某些数据可以是私有数据,其只可以通过调用智能合约的方法进行更改,或仅由授权的区块链参与者进行更改。更改智能合约状态的一种方法是将交易广播到分布式账本网络。如果广播的交易满足共识规则,则网络验证器可以将交易包括在分布式账本中。

[0172] 在一些实施例中,诸如边缘网关之类的验证节点执行包含在智能合约中的代码,并且现场设备充当证据谕示并提供更改智能合约状态的证据交易。

[0173] 图17示出了表示用于使用分布式账本在过程控制系统中与智能合约进行交互的示例性方法1700的流程图。方法1700可以由过程工厂10内的现场设备15-22、40-46、过程工厂10内的控制器11或过程工厂10内的另一计算设备(例如,操作员工作站、服务器设备12、用户接口设备8、I/O设备26、28、网络设备35等)执行。

[0174] 在框1702处,从过程工厂10内发生的事件获得事件数据。事件可以是过程工厂10交付或在过程工厂10处接收的产品,在过程工厂10处制造的产品的完成,产品属性的改变,过程参数值的改变,触发事件(例如警报、错误、泄漏、维修事件、纠正措施、用户交互(例如对SIS设备的写请求、向设备供应商提供设备信息的请求、或在接收到特定产品时请求传输通证值的请求)),或过程工厂10中发生的任何其他合适的事件。事件数据可以包括过程参数数据、产品参数数据、配置数据、用户交互数据、维护数据、调试数据、工厂网络数据、产品跟踪数据、或与事件相关的任何其他合适的数据,例如事件的日期和时间、事件的持续时间、事件的描述等。

[0175] 然后在框1704处,生成交易,该交易包括事件数据和生成交易的实体的标识信息,例如分配给该实体的加密公钥。可以对交易进行加密签名以提供生成交易的实体的加密身份证明。在框1706处,将交易传送到部署智能合约的分布式账本上的地址。以这种方式,诸如边缘网关之类的验证节点根据交易中包括的事件数据来更改智能合约状态。

[0176] 例如,当工厂A从工厂B接收到符合某些质量标准的产品时,智能合约可以将通证值从工厂A传输到工厂B。工厂A中的现场设备可以生成交易,该交易包括与产品质量相关的事件数据,例如工厂A的标识信息,产品的标识信息,从工厂B接收到产品的指示、以及描述产品属性的产品参数数据(例如,产品的温度、产品的体积、产品的密度、产品的粘度或产品的化学组成)。现场设备可以将交易提供给智能合约的地址,并且验证节点可以改变智能合约状态以包括产品参数数据。在一些实施例中,智能合约将产品参数数据中包括的产品属

性与产品的最小阈值要求集合进行比较,以满足适当的质量标准。如果产品满足质量标准,则智能合约可以将通证值传输到工厂B。在一些实施例中,工厂B中的现场设备可以生成交易,该交易包括与产品质量相关的事件数据,例如过程参数数据,其描述涉及制造产品的工厂B中的过程工厂实体的参数值,其中在制造产品时收集参数值。

[0177] 本公开内容中描述的技术的实施例可以单独地或组合地包括任意数量的以下方面:

[0178] 1.一种在分布式账本网络上的过程工厂中的验证网络节点,包括:收发器,其被配置为与各自执行物理功能以控制过程工厂中的工业过程的一个或多个现场设备进行通信,以及与对等网络节点交换分布式账本数据,分布式账本数据包括具有过程工厂数据的交易;存储介质,其被配置为存储分布式账本的副本;以及过程数据验证器,其被配置为将共识规则集应用于从对等网络节点接收的分布式账本数据,过程数据验证器还被配置为:如果分布式账本数据满足共识规则,则将从对等网络节点接收的分布式账本数据附加到分布式账本的副本。

[0179] 2.根据方面1所述的验证网络节点,其中,从对等节点接收的分布式账本数据包括生成具有过程工厂数据的交易的实体的身份证明。

[0180] 3.根据前述方面中任一项所述的验证网络节点,其中,为了附加从对等节点接收的分布式账本数据,交易验证器被配置为:基于交易区块来求解密码难题;以及将密码难题的解添加到交易区块;将交易区块附加到分布式账本的副本;以及将交易区块传送到分布式账本网络中的对等网络节点中的至少一个。

[0181] 4.根据前述方面中任一项所述的验证网络节点,其中,共识规则集包括以下中的至少一个:交易或交易区块的格式化要求;用于确定对等网络节点中的哪一个将把下一个交易或交易区块添加到分布式账本的机制;或用于对每个交易中包括的过程工厂数据进行哈希处理的加密哈希算法。

[0182] 5.根据前述方面中任一项所述的验证网络节点,其中,过程数据验证器还被配置为执行智能合约中的代码并更新用于智能合约的状态数据库。

[0183] 6.根据前述方面中任一项所述的验证网络节点,其中,过程数据验证器还被配置为:如果分布式账本数据不满足共识规则,则忽略从对等网络节点接收的分布式账本数据。

[0184] 7.根据前述方面中任一项所述的验证网络节点,其中,验证网络节点和对等网络节点是相同过程工厂内的设备。

[0185] 8.根据前述方面中任一项所述的验证网络节点,其中,验证网络节点和对等网络节点是多个过程工厂内的设备。

[0186] 9.一种用于使用由多个参与者维护的分布式账本在过程控制系统中记录数据的方法,该方法包括:由计算设备获得与过程工厂内的过程控制元件有关的过程工厂数据;生成包括过程工厂数据的交易,其中,交易被存储在分布式账本中;将交易传送给维护分布式账本的参与者的分布式账本网络的至少一个其他参与者。

[0187] 10.根据方面9所述的方法,其中,生成交易包括:基于交易生成加密签名;以及利用加密签名扩充交易。

[0188] 11.根据方面9或方面10中任一项所述的方法,其中,数据是从过程工厂内的现场设备获得的,并且生成所述交易还包括:获得现场设备的身份数据;并利用身份数据扩充交

易。

[0189] 12.根据方面9-11中任一项所述的方法,还包括:将交易添加到交易区块;以及根据交易区块求解密码难题;将密码难题的解添加到交易区块;以及将交易区块传送给分布式账本网络中的至少一个其他参与者。

[0190] 13.根据方面9-12中任一项所述的方法,其中,数据是产品跟踪数据,并且生成交易包括生成指示产品已经从过程工厂转移到另一实体的交易。

[0191] 14.根据方面9-13中任一项所述的方法,其中,数据是产品参数数据,包括以下中的至少一个:产品的温度、产品的体积或产品的化学组成,并且其中,产品参数数据被存储在分布式账本中,以在产品被提供给另一实体时验证产品的参数数据的真实性。

[0192] 15.根据方面9-14中任一项所述的方法,其中,分布式账本网络包括多个层,并且还包括:在第一实例中,生成要存储在分布式账本的第一层中的交易;以及在第二实例中,生成要存储在分布式账本的第二层中的交易。

[0193] 16.根据方面9-15中任一项所述的方法,其中,分布式账本的第一层是公有的,而分布式层的第二层是私有的。

[0194] 17.根据方面9-16中任一项所述的方法,其中,分布式账本是以下中的至少一个:区块链、tangle、区块晶格或其他有向无环图。

[0195] 18.根据方面9-17中任一项所述的方法,其中,过程工厂数据包括以下中的至少一个:产品参数数据、配置数据、产品跟踪数据或过程参数数据。

[0196] 19.根据方面9-18中任一项所述的方法,其中,生成交易包括生成包括与过程工厂数据相对应的加密哈希值的交易。

[0197] 20.一种用于使用由多个参与者维护的分布式账本在过程控制系统中记录数据的系统,包括:设置在过程工厂中的一个或多个设备,该一个或多个设备各自执行物理功能以控制工业过程;以及在过程工厂中执行的计算设备,该计算设备包括:一个或多个处理器;通信单元;以及非暂时性计算机可读介质,其耦合到一个或多个处理器和通信单元,并在其上存储指令,所述指令在由一个或多个处理器执行时使计算设备执行以下操作:获得与过程工厂内的一个或多个设备有关的过程工厂数据;生成包括过程工厂数据的交易;并将交易传送给维护分布式账本的参与者的分布式账本网络的至少一个其他参与者,以便验证交易并在分布式账本中记录交易。

[0198] 21.根据方面20所述的系统,其中,为了生成交易,所述指令使计算设备执行以下操作:基于交易生成加密签名;并利用加密签名扩充交易。

[0199] 22.根据方面20或方面21中任一项所述的系统,其中,数据是从过程工厂内的现场设备获得的,并且,为了生成交易,所述指令使计算设备执行以下操作:获得现场设备的身份数据;并利用身份数据扩充交易。

[0200] 23.根据方面20-22中任一项所述的系统,所述指令还使计算设备执行以下操作:将交易添加到交易区块;以及基于交易区块求解密码难题;将密码难题的解添加到交易区块;以及将交易区块传送给分布式账本网络中的至少一个其他参与者。

[0201] 24.根据方面20-23中任一项所述的系统,其中,分布式账本网络包括多个层,并且所述指令还使计算设备执行以下操作:在第一实例中,生成要存储在分布式账本的第一层中的交易;以及在第二实例中,生成要存储在分布式账本的第二层中的交易。

[0202] 25.根据方面20-24中任一项所述的系统,其中,分布式账本的第一层是公有区块链,并且分布式层的第二层是私有区块链。

[0203] 26.根据方面20-25中任一项所述的系统,其中,分布式账本是以下中的至少一个:区块链、tangle、区块晶格或其他有向无环图。

[0204] 27.根据方面20-26中任一项所述的系统,其中,过程工厂数据包括以下中的至少一个:产品参数数据、配置数据、产品跟踪数据或过程参数数据。

[0205] 28.根据方面20-26中任一项所述的系统,其中,生成交易包括生成包括与过程工厂数据相对应的加密哈希值的交易。

[0206] 29.一种非暂时性计算机可读存储器,其耦合到一个或多个处理器,并在其上存储指令,所述指令在由一个或多个处理器执行时使一个或多个处理器执行以下操作:接收包括由一个或多个现场设备生成的过程工厂数据的交易,该一个或多个现场设备各自执行物理功能以控制过程工厂中的工业过程;存储分布式账本的副本;将共识规则集应用于所接收的交易;如果所接收的交易满足共识规则,则将所接收的交易中的一个附加到分布式账本的副本;将所附加的交易传送到存储分布式账本的副本的至少一个对等网络节点。

[0207] 30.根据方面29所述的计算机可读存储器,其中,所接收的交易包括生成交易的实体的身份证明。

[0208] 31.根据方面29或方面30中任一项所述的计算机可读存储器,其中,为了附加所接收的交易中的一个,所述指令使一个或多个处理器执行以下操作:基于包括所接收的交易的交易区块来求解密码难题;将密码难题的解添加到交易区块;将交易区块附加到分布式账本的副本;以及将交易区块传送到对等网络节点。

[0209] 32.根据方面29-31中任一项所述的计算机可读存储器,其中,共识规则集包括以下中的至少一个:交易或交易区块的格式化要求;用于确定对等网络节点中的哪一个将把下一个交易或交易区块添加到分布式账本的机制;或用于对每个交易中包括的过程工厂数据进行哈希处理的加密哈希算法。

[0210] 33.根据方面29-32中任一项所述的计算机可读存储器,其中,所述指令还使一个或多个处理器执行以下操作:如果分布式账本数据不满足共识规则,则忽略从对等网络节点接收的分布式账本数据。

[0211] 34.根据方面29-33中任一项所述的计算机可读存储器,其中,对等网络节点是相同过程工厂内的设备。

[0212] 35.根据方面29-34中的任一项所述的计算机可读存储器,其中,对等网络节点是多个过程工厂内的设备。

[0213] 36.一种用于使用由多个参与者维护的分布式账本在过程控制系统中安全计量不可信数据的方法,该方法包括:由执行物理功能以控制过程中的工业过程的现场设备收集过程工厂内的参数的测量结果;由计算设备获得参数的测量结果;生成包括测量结果的交易;以及将交易传送给维护本地分布式账本的参与者的本地分布式账本网络中的至少一个其他参与者;在阈值时间段之后,将在阈值时间段期间生成的多个交易传送给维护全局分布式账本的参与者的全局分布式账本网络中的至少一个参与者。

[0214] 37.根据方面36所述的方法,还包括:将交易添加到交易的本地区块中;基于交易的本地区块求解密码难题;将密码难题的解添加到交易的本地区块中;以及将交易的本地

区块传送给本地分布式账本网络中的至少一个其他参与者。

[0215] 38.根据方面36或方面37中任一项所述的方法,还包括:在阈值时间段之后,将在阈值时间段期间生成的一个或多个交易的本地区块传送给全局分布式账本网络中的至少一个参与者。

[0216] 39.根据方面36-38中任一项所述的方法,还包括:在阈值时间段之后,从本地分布式账本网络中减少在阈值时间段期间生成的多个交易中的至少一些交易。

[0217] 40.根据方面36-39中任一项所述的方法,其中,全局分布式账本是可由操作多个过程工厂的多个实体查看的经许可的区块链。

[0218] 41.根据方面36-40中任一项所述的方法,其中,参数与操作多个过程工厂的多个实体之间的共享资源有关。

[0219] 42.根据方面36-41中任一项所述的方法,其中,全局分布式账本包括与多个实体相对应的多个全局分布式账本,每个全局分布式账本包括存储在用于与全局分布式账本相同的相应实体的本地分布式账本中的交易。

[0220] 43.根据方面36-42中任一项所述的方法,还包括:对于在阈值时间段期间生成的交易,将来自多个全局分布式账本中的每个的交易添加到交易的状态区块中;基于交易的状态区块求解密码难题;将密码难题的解添加到交易的状态区块中;以及将交易的状态区块传送给维护超级区块链的参与者的超级区块链网络中的至少一个其他参与者。

[0221] 44.根据方面36-43中任一项所述的方法,其中,本地分布式账本是可由操作过程工厂的实体查看的私有区块链。

[0222] 45.根据方面36-44中任一项所述的方法,其中,生成包括测量结果的交易包括生成包括与测量结果相对应的加密哈希值的交易。

[0223] 46.根据方面36-45中任一项所述的方法,其中,操作多个过程工厂的多个实体之间的共享资源是流体管道中的流体,并且参数的测量结果是由多个实体之一从流体管道所获得的流体量。

[0224] 47.一种用于使用由多个参与者维护的分布式账本对过程控制系统中的不可信数据进行安全计量的系统,包括:一个或多个现场设备,设置在过程工厂中,每个现场设备执行物理功能以控制工业过程,一个或多个现场设备被配置为收集过程工厂内的参数的测量结果并将参数的测量结果提供给一个或多个边缘网关设备;以及在过程工厂中执行的一个或多个边缘网关设备,每个边缘网关设备都包括:一个或多个处理器;通信单元;以及非暂时性计算机可读介质,其耦合到一个或多个处理器和通信单元并在其上存储指令,指令在被一个或多个处理器执行时,使边缘网关设备执行以下操作:获得参数的测量结果中的至少一个;生成包括测量结果的交易;以及将交易传送给维护本地分布式账本的边缘网关的本地分布式账本网络中的至少一个其他边缘网关;以及在阈值时间段之后,将在阈值时间段期间生成的多个交易传送给维护全局分布式账本的参与者的全局分布式账本网络中的至少一个参与者。

[0225] 48.根据方面47所述的系统,其中,指令还使边缘网关执行以下操作:将交易添加到交易的本地区块;基于交易的本地区块求解密码难题;将密码难题的解添加到交易的本地区块中;以及将交易的本地区块传送给本地分布式账本网络中的至少一个其他边缘网关。

[0226] 49.根据方面47或方面48中任一项所述的系统,其中,指令还使边缘网关执行以下操作:在阈值时间段之后,将在阈值时间段期间生成的一个或多个交易的本地区块传送给全局分布式账本网络中的至少一个参与者。

[0227] 50.根据方面47-49中任一项所述的系统,其中,指令还使边缘网关执行以下操作:在阈值时间段之后,从本地分布式账本网络中减少在阈值时间段期间生成的多个交易中的至少一些交易。

[0228] 51.根据方面47-50中任一项所述的系统,其中,全局分布式账本是可由操作多个过程工厂的多个实体查看的经许可的区块链。

[0229] 52.根据方面47-51中任一项所述的系统,其中,参数与操作多个过程工厂的多个实体之间的共享资源有关。

[0230] 53.根据方面47-52中任一项所述的系统,其中,全局分布式账本包括与多个实体相对应的多个全局分布式账本,每个全局分布式账本包括存储在用于与全局分布式账本相同的相应实体的本地分布式账本中的交易。

[0231] 54.根据方面47-53中任一项所述的系统,还包括:计算设备,其位于维护全局分布式账本的全局分布式账本网络中,包括:一个或多个处理器;通信单元;以及非暂时性计算机可读介质,其耦合到一个或多个处理器和通信单元并在其上存储指令,指令在被一个或多个处理器执行时,使计算设备执行以下操作:对于在阈值时间段期间生成的交易,将来自多个全局分布式账本中的每个的交易添加到交易的状态区块中;基于交易的状态区块求解密码难题;将密码难题的解添加到交易的状态区块中;以及将交易的状态区块传送给维护超级区块链的参与者的超级区块链网络中的至少一个其他参与者。

[0232] 55.根据方面47-54中任一项所述的系统,其中,本地分布式账本是可由操作过程工厂的实体查看的私有区块链。

[0233] 56.根据方面47-55中任一项所述的系统,其中,交易包括与测量结果相对应的加密哈希值。

[0234] 57.根据方面47-56中任一项所述的系统,其中,操作多个过程工厂的多个实体之间的共享资源是流体管道中的流体,并且参数的测量结果是由多个实体之一从流体管道所获得的流体量。

[0235] 58.一种本地分布式账本网络上的过程工厂中的验证网络节点,包括:收发器,被配置为(i)与一个或多个现场设备进行通信,每个现场设备执行物理功能以控制过程工厂中的工业过程并收集过程工厂内的参数的测量结果,以及(ii)与对等网络节点交换本地分布式账本数据,该本地分布式账本数据包括具有参数的测量结果的交易;存储介质,被配置为存储本地分布式账本的副本;以及过程数据验证器,被配置为将共识规则集应用于从对等网络节点接收到的分布式账本数据,过程数据验证器还被配置为:如果分布式账本数据满足共识规则,则将从对等网络节点接收到的分布式账本数据附加到分布式账本的副本,其中,在阈值时间段之后,收发器被配置为将在阈值时间段期间生成的多个交易传送给维护全局分布式账本的参与者的全局分布式账本网络中的至少一个参与者。

[0236] 59.根据方面58所述的验证网络节点,其中,在阈值时间段之后,验证网络节点被配置为从本地分布式账本的副本中减少在阈值时间段期间生成的多个交易中的至少一些交易。

[0237] 60.根据方面58或方面59中任一项所述的验证网络节点,其中,全局分布式账本是可由操作多个过程工厂的多个实体查看的经许可的区块链。

[0238] 61.根据方面58-60中的任一项所述的验证网络节点,其中,参数中的至少一个参数与操作多个过程工厂的多个实体之间的共享资源有关。

[0239] 62.根据方面58-61中的任一项所述的验证网络节点,其中,全局分布式账本包括与多个实体相对应的多个全局分布式账本,每个全局分布式账本包括存储在用于与全局分布式账本相同的相应实体的本地分布式账本中的交易。

[0240] 63.根据方面58-62中的任一项所述的验证网络节点,其中,本地分布式账本是可由操作过程工厂的实体查看的私有区块链。

[0241] 64.根据方面58-63中的任一项所述的验证网络节点,其中,交易包括与参数的测量结果相对应的加密哈希值。

[0242] 65.一种用于使用由多个参与者维护的分布式账本在过程控制系统中记录质量控制、生产或监管数据的方法,该方法包括:经由各自执行物理功能以控制工业过程的一个或多个现场设备检测与过程工厂内的质量控制有关的触发事件;从触发事件获得事件数据,包括以下中的至少一个:触发事件的时间、触发事件的持续时间、与触发事件有关的产品参数数据、或与触发事件有关的过程参数数据;生成包括事件数据的交易,其中,交易被存储在分布式账本中;以及将交易传送给维护分布式账本的参与者的分布式账本网络的至少一个其他参与者。

[0243] 66.根据方面65所述的方法,其中,所述触发事件是以下中的至少一个:警报、错误、泄漏、维修事件、过程重大事件、或纠正措施。

[0244] 67.根据方面65或方面66中任一项所述的方法,还包括:接收对来自特定触发事件的事件数据的请求;从分布式账本中获得事件数据;以及在用户界面上呈现来自特定触发事件的事件数据。

[0245] 68.根据方面65-67中任一项所述的方法,其中,生成包括事件数据的交易包括:生成包括与事件数据中的至少一些相对应的加密哈希值的交易。

[0246] 69.根据方面65-68中任一项所述的方法,还包括:将事件数据存储在数据库中;以及响应于对认证事件数据的请求,提供与来自分布式账本的事件数据中的至少一些相对应的加密哈希值以及来自数据库的事件数据,以验证事件数据的真实性。

[0247] 70.根据方面65-69中任一项所述的方法,其中,触发事件是安全阀中的打开,并且来自触发事件的事件数据包括以下中的至少一个:打开安全阀的时间、打开安全阀的持续时间、打开安全阀时的压力值、或打开安全阀时排出的流体量。

[0248] 71.根据方面65-70中任一项所述的方法,其中,分布式账本是可由过程工厂和监管机构访问的私有区块链。

[0249] 72.根据方面65-71中任一项所述的方法,其中,分布式账本是公有区块链。

[0250] 73.根据方面65-72中任一项所述的方法,其中,交易还包括用于触发事件的唯一标识符。

[0251] 74.根据方面65-73中任一项所述的方法,还包括:将包括触发事件的唯一标识符的所检测到的触发事件的指示传送到过程工厂中的一个或多个其他过程控制元件,以用于其他过程控制元件生成包括与触发事件有关的附加事件数据的交易。

[0252] 75.一种用于使用由多个参与者维护的分布式账本在过程控制系统中记录质量控制、生产或监管数据的系统,包括:设置在过程工厂中的一个或多个设备,该一个或多个设备各自执行物理功能以控制工业过程;以及在过程工厂中执行的计算设备,所述计算设备包括:一个或多个处理器;通信单元;以及非暂时性计算机可读介质,其耦合到一个或多个处理器和通信单元,并在其上存储指令,所述指令在由一个或多个处理器执行时使计算设备执行以下操作:经由一个或多个设备检测与过程工厂内的质量控制有关的触发事件;从触发事件获得事件数据,包括以下中的至少一个:触发事件的时间、触发事件的持续时间、与触发事件有关的产品参数数据、或与触发事件有关的过程参数数据;生成包括事件数据的交易,其中,交易被存储在分布式账本中;以及将交易传送给维护分布式账本的参与者的分布式账本网络的至少一个其他参与者,以便验证交易并在分布式账本中记录交易。

[0253] 76.根据方面75所述的系统,其中,触发事件是以下中的至少一个:警报、错误、泄漏、维修事件、过程重大事件或纠正措施。

[0254] 77.根据方面75或方面76中的任一项所述的系统,其中,所述指令还使得计算设备执行以下操作:接收对来自特定触发事件的事件数据的请求;从分布式账本中获得事件数据;以及在用户界面上呈现来自特定触发事件的事件数据。

[0255] 78.根据方面75-77中任一项所述的系统,其中,交易包括与事件数据中的至少一些相对应的加密哈希值。

[0256] 79.根据方面75-78中任一项所述的系统,其中,所述指令还使计算设备执行以下操作:将事件数据存储在数据库中;以及响应于对认证事件数据的请求,提供与来自分布式账本的事件数据中的至少一些相对应的加密哈希值以及来自数据库的事件数据,以验证事件数据的真实性。

[0257] 80.根据方面75-79中任一项所述的系统,其中,触发事件是安全阀中的打开,并且来自触发事件的事件数据包括以下中的至少一个:打开安全阀的时间、打开安全阀的持续时间、打开安全阀时的压力值、或打开安全阀时排出的流体量。

[0258] 81.根据方面75-80中任一项所述的系统,其中,分布式账本是可由过程工厂和监管机构访问的私有区块链。

[0259] 82.根据方面75-81中任一项所述的系统,其中,分布式账本是公有区块链。

[0260] 83.根据方面75-82中任一项所述的系统,其中,交易还包括用于触发事件的唯一标识符。

[0261] 84.根据方面75-83中的任一项所述的系统,其中,所述指令还使计算设备执行以下操作:将包括触发事件的唯一标识符的所检测到的触发事件的指示传送到过程工厂中的一个或多个设备,以用于该一个或多个设备生成包括与触发事件有关的附加事件数据的交易。

[0262] 85.一种在分布式账本网络上的过程工厂中的验证网络节点,包括:收发器,其被配置为与各自执行物理功能以控制过程工厂中的工业过程的一个或多个现场设备进行通信,以及与对等网络节点交换分布式账本数据,分布式账本数据包括具有来自触发事件的事件数据的交易;存储介质,其被配置为存储分布式账本的副本;以及过程数据验证器,其被配置为将共识规则集应用于从对等网络节点接收的分布式账本数据,过程数据验证器还被配置为:如果分布式账本数据满足共识规则,则将从对等网络节点接收的分布式账本数

据附加到分布式账本的副本。

[0263] 86.根据方面85所述的验证网络节点,其中,事件数据包括以下中的至少一个:触发事件的时间、触发事件的持续时间、与触发事件有关的产品参数数据、或与触发事件有关的过程参数数据。

[0264] 87.根据方面85或方面86中任一项所述的验证网络节点,其中,触发事件是以下中的至少一个:警报、错误、泄漏、维修事件或纠正措施。

[0265] 88.根据方面85-87中任一项所述的验证网络节点,其中,从对等节点接收的分布式账本数据包括:生成具有事件数据的交易的一个或多个现场设备中的一个现场设备的身份证明。

[0266] 89.根据方面85-88中任一项所述的验证网络节点,其中,为了附加从对等节点接收的分布式账本数据,所述交易验证器被配置为:基于交易区块来求解密码难题;以及将密码难题的解添加到交易区块;将交易区块附加到分布式账本的副本;并将交易区块传送到分布式账本网络中的对等网络节点中的至少一个。

[0267] 90.根据方面85-89中任一项所述的验证网络节点,其中,所述共识规则集包括以下中的至少一个:交易或交易区块的格式化要求;用于确定对等网络节点中的哪一个将把下一个交易或交易区块添加到分布式账本的机制;或用于对每个交易中包括的过程控制数据进行哈希处理的加密哈希算法。

[0268] 91.根据方面85-90中任一项所述的验证网络节点,其中,分布式账本是可由过程工厂和监管机构访问的私有区块链。

[0269] 92.根据方面85-91中任一项所述的验证网络节点,其中,分布式账本是公有区块链。

[0270] 93.根据方面85-92中任一项所述的验证网络节点,其中,交易还包括触发事件的唯一标识符。

[0271] 94.一种用于使用由多个参与者维护的分布式账本在过程控制系统和所连接的仪器中记录软件或固件的状态的方法,该方法包括:由计算设备获得在具有一个或多个现场设备的过程工厂内执行的软件或固件的当前状态,该一个或多个现场设备各自执行物理功能以控制工业过程,软件或固件在过程工厂内的网络或过程控制设备中执行;生成包括在过程工厂内执行的软件或固件的当前状态的交易,其中,交易被存储在分布式账本中;以及将交易传送给维护分布式账本的参与者的分布式账本网络中的至少一个其他参与者。

[0272] 95.根据方面94所述的方法,其中,在过程工厂内执行的软件或固件的当前状态是从更新了当前状态的用户的计算设备获得的,并且生成交易还包括:获得用户的身份数据;在一个或多个处理器处,利用用户的身份数据来扩充交易;在一个或多个处理器处,基于交易生成加密签名;以及在一个或多个处理器处,利用加密签名来扩充交易。

[0273] 96.根据方面94或方面95中任一项所述的方法,其中,生成包括在过程工厂内执行的软件或固件的当前状态的交易包括:生成包括与在过程工厂内执行的软件或固件的当前状态相对应的加密哈希值的交易。

[0274] 97.根据方面94-96中任一项所述的方法,还包括:从执行软件或固件的网络或过程控制设备获得在过程工厂内执行的软件或固件的状态;以及将在过程工厂内执行的软件或固件的状态与分布式账本中的加密哈希值进行比较,以验证软件或固件未被篡改。

[0275] 98.根据方面94-97中任一项所述的方法,还包括:响应于根据加密哈希值确定在过程工厂内执行的软件或固件的状态与存储在分布式账本中的软件或固件的当前状态不匹配,阻止在过程工厂内执行软件或固件。

[0276] 99.根据方面94-98中任一项所述的方法,还包括:使软件或固件恢复到先前状态。

[0277] 100.根据方面94-99中任一项所述的方法,还包括:响应于根据加密哈希值确定在过程工厂内执行的软件或固件的状态与存储在分布式账本中的软件或固件的当前状态相匹配,使网络或过程控制设备执行软件或固件。

[0278] 101.根据方面94-100中任一项所述的方法,还包括:将交易添加到交易区块;以及根据交易区块求解密码难题;将密码难题的解添加到交易区块;以及将交易区块传送给分布式账本网络中的至少一个其他参与者。

[0279] 102.根据方面94-101中任一项所述的方法,还包括:将交易中的身份数据与对应于被授权更新在过程工厂中执行的软件或固件的状态的用户的多个身份数据集进行比较;以及当身份数据包括在多个身份数据集中时,将交易添加到交易区块。

[0280] 103.根据方面94-102中任一项所述的方法,其中,分布式账本是经许可的区块链。

[0281] 104.一种用于使用由多个参与者维护的分布式账本在过程控制系统和所连接的仪器中记录软件或固件的状态的系统,包括:设置在过程工厂中的一个或多个设备,该一个或多个设备各自执行物理功能以控制工业过程;在过程工厂中执行的计算设备,所述计算设备包括:一个或多个处理器;通信单元;以及非暂时性计算机可读介质,其耦合到一个或多个处理器和通信单元,并在其上存储指令,所述指令在由一个或多个处理器执行时使计算设备执行以下操作:获得在过程工厂内执行的软件或固件的当前状态,软件或固件在设置在过程工厂中的一个或多个设备或过程工厂内的网络设备中的至少一个中执行;生成包括在过程工厂内执行的软件或固件的当前状态的交易,其中,交易被存储在分布式账本中;以及将交易传送给维护分布式账本的参与者的分布式账本网络中的至少一个其他参与者,以便验证交易并将交易记录在分布式账本中。

[0282] 105.根据方面104所述的系统,其中,在过程工厂内执行的软件或固件的当前状态是从更新了当前状态的用户的计算设备获得的,并且为了生成交易,所述指令使计算设备执行以下操作:获得用户的身份数据;利用用户的身份数据来扩充交易;基于交易生成加密签名;以及利用加密签名来扩充交易。

[0283] 106.根据方面104或方面105中任一项所述的系统,其中,利用对应于在过程工厂内执行的软件或固件的当前状态的加密哈希值来生成交易。

[0284] 107.根据方面104-106中任一项所述的系统,还包括:服务器设备,服务器设备包括:一个或多个处理器;通信单元;以及非暂时性计算机可读介质,其耦合到一个或多个处理器和通信单元,并在其上存储指令,所述指令在由一个或多个处理器执行时使服务器设备执行以下操作:从执行软件或固件的网络或过程控制设备获得在过程工厂内执行的软件或固件的状态;以及将在过程工厂内执行的软件或固件的状态与分布式账本中的加密哈希值进行比较,以验证软件或固件未被篡改。

[0285] 108.根据方面104-107中任一项所述的系统,其中,所述指令还使服务器设备执行以下操作:响应于根据加密哈希值确定在过程工厂内执行的软件或固件的状态与存储在分布式账本中的软件或固件的当前状态不匹配,阻止在过程工厂内执行软件或固件。

[0286] 109.根据方面104-108中的任一项所述的系统,其中,所述指令还使服务器设备执行以下操作:使软件或固件恢复到先前状态。

[0287] 110.根据方面104-109中任一项所述的系统,其中,所述指令还使服务器设备执行以下操作:响应于根据加密哈希值确定在过程工厂内执行的软件或固件的状态与存储在分布式账本中的软件或固件的当前状态相匹配,使网络或过程控制设备执行软件或固件。

[0288] 111.根据方面104-110中任一项所述的系统,其中,所述指令还使计算设备执行以下操作:将交易添加到交易区块;以及基于交易区块求解密码难题;将密码难题的解添加到交易区块;以及将交易区块传送给分布式账本网络中的至少一个其他参与者。

[0289] 112.根据方面104-111中任一项所述的系统,其中,所述指令还使计算设备执行以下操作:将交易中的身份数据与对应于被授权更新在过程工厂内执行的软件或固件的状态的用户的多个身份数据集进行比较;以及当身份数据包括在多个身份数据集中时,将交易添加到交易区块。

[0290] 113.根据方面104-112中任一项所述的系统,其中,分布式账本是经许可的区块链。

[0291] 114.一种在分布式账本网络上的过程工厂中的验证网络节点,包括:收发器,其被配置为与各自执行物理功能以控制过程工厂中的工业过程的一个或多个现场设备进行通信,以及与对等网络节点交换分布式账本数据,分布式账本数据包括具有指示在过程工厂内执行的软件或固件的当前状态的数据的交易;存储介质,其被配置为存储分布式账本的副本;以及过程数据验证器,其被配置为将共识规则集应用于从对等网络节点接收的分布式账本数据,过程数据验证器还被配置为:如果分布式账本数据满足共识规则,则将从对等网络节点接收的分布式账本数据附加到分布式账本的副本。

[0292] 115.根据方面114所述的验证网络节点,其中,为了附加从对等节点接收的分布式账本数据,交易验证器被配置为:基于交易区块来求解密码难题;以及将密码难题的解添加到交易区块;将交易区块附加到分布式账本的副本;并将交易区块传送到分布式账本网络中的对等网络节点中的至少一个。

[0293] 116.根据方面114或方面115中任一项所述的验证网络节点,其中,所述共识规则集包括以下至少中的一个:交易或交易区块的格式化要求;用于确定对等网络节点中的哪一个将把下一个交易或交易区块添加到分布式账本的机制;或用于对每个交易中包括的软件或固件状态数据进行哈希处理的加密哈希算法。

[0294] 117.根据方面114-116中任一项所述的验证网络节点,其中,从对等节点接收的分布式账本数据包括生成交易的设备的用户的身份证明,该交易具有指示在过程工厂中执行的软件或固件的当前状态的数据。

[0295] 118.一种用于使用由多个参与者维护的分布式账本在过程控制系统中创建智能合约的方法,该方法包括:由一个或多个处理器生成与具有一个或多个现场设备的过程工厂有关的智能合约,每个现场设备执行物理功能以控制工业过程;以及由一个或多个处理器将智能合约部署到存储在由分布式账本网络的多个参与者维护的分布式账本上的地址。

[0296] 119.根据方面118所述的方法,其中,智能合约根据在过程工厂内发生的事件来接收或提供通证值。

[0297] 120.根据方面118或方面119中任一项所述的方法,其中,生成与过程工厂有关的

智能合约包括:生成智能合约,该智能合约从第一过程工厂获得通证值,确定产品从第二过程工厂转移到第一过程工厂,并将通证值提供给第二过程工厂。

[0298] 121.根据方面118-120中任一项所述的方法,其中,智能合约通过从证据谕示接收指示在第一过程工厂处接收到产品的交易,来确定产品从第二过程工厂转移到第一过程工厂。

[0299] 122.根据方面118-121中任一项所述的方法,其中,生成与过程工厂有关的智能合约还包括:生成智能合约,该智能合约确定产品符合或超过一个或多个质量指标,并响应于确定产品符合或超过一个或多个质量指标,将通证值提供给第二过程工厂。

[0300] 123.根据方面118-122中任一项所述的方法,其中,智能合约通过从证据谕示接收各自包括产品参数值或过程参数值的一个或多个交易,并将产品参数值或过程参数值与一个或多个质量指标中包含的产品参数阈值或过程参数阈值进行比较,来确定产品符合或超过一个或多个质量指标。

[0301] 124.根据方面118-123中任一项所述的方法,其中,生成与过程工厂有关的智能合约包括:生成智能合约,该智能合约获得过程工厂中经历故障的设备的设备信息,并响应于接收到共享设备信息的请求,将设备信息提供给设备供应商。

[0302] 125.根据方面118-124中任一项所述的方法,其中,智能合约通过从证据谕示接收包括设备信息的交易来获得设备信息。

[0303] 126.根据方面118-125中任一项所述的方法,其中,智能合约通过接收包括该请求连同发出该请求的用户的身份数据的交易来接收该请求,并且,智能合约将交易中的身份数据与对应于被授权请求分布式账本网络共享设备信息的用户的多个身份数据集进行比较,并当多个身份数据集内包括该身份数据时,将设备信息提供给设备供应商。

[0304] 127.根据方面118-126中任一项所述的方法,其中,生成与过程工厂有关的智能合约包括:生成智能合约,该智能合约接收与安全仪表系统(SIS)设备相关联的参数,并响应于确定提供该参数的操作员是经授权的操作员,将该参数将参数写入SIS设备。

[0305] 128.根据方面118-127中任一项所述的方法,其中,智能合约通过接收包括该参数连同提供交易的操作员的身份数据的交易,来接收与SIS设备相关联的参数,并且其中,确定提供参数的操作员是经授权的操作员包括:将交易中的身份数据与对应于被授权调整与SIS设备相关联的参数的操作员的多个身份数据集进行比较。

[0306] 129.根据方面118-128中任一项所述的方法,其中,与SIS设备相关联的参数是锁定SIS设备的请求。

[0307] 130.一种用于使用由多个参与者维护的分布式账本在过程控制系统中与智能合约进行交互的方法,该方法包括:从在具有一个或多个现场设备的过程工厂内发生的事件获得事件数据,每个现场设备执行物理功能以控制工业过程;响应于智能合约被部署到存储在分布式账本上的地址,由计算设备生成包括事件数据的交易;以及将交易传送到存储在由分布式账本网络中的多个参与者维护的分布式账本上的智能合约。

[0308] 131.根据方面130所述的方法,还包括:获得计算设备的身份数据;在一个或多个处理器处利用计算设备的身份数据扩充交易;在一个或多个处理器处基于交易生成加密签名;以及在一个或多个处理器处利用加密签名扩充交易。

[0309] 132.根据方面130或方面131中任一项所述的方法,还包括:将交易添加到交易区

块中;基于交易区块求解密码难题;将密码难题的解添加到交易区块中;以及将交易区块传送给分布式账本网络中的至少一个其他参与者。

[0310] 133.根据方面130-132中任一项所述的方法,其中,智能合约从第一过程工厂获得通证值,确定产品从第二过程工厂转移到第一过程工厂,并将通证值提供给第二过程工厂,并且其中,从在过程工厂内发生的事件获得事件数据包括:获得在第一过程工厂处接收到产品的指示;以及生成包括第一过程工厂的标识信息、产品的标识信息、以及在第一过程工厂处从第二过程工厂接收到产品的指示的交易。

[0311] 134.根据方面130-133中任一项所述的方法,其中,获得在第一过程工厂处接收到产品的指示还包括:获得产品的一个或多个产品参数值或在制造产品时涉及的过程工厂实体的一个或多个过程参数值;以及生成包括一个或多个产品参数值或一个或多个过程参数值的交易。

[0312] 135.根据方面130-134中任一项所述的方法,其中,智能合约获得过程工厂内经历故障的设备的设备信息,并响应于接收到共享设备信息的请求,将设备信息提供给设备供应商,并且其中,从过程工厂内发生的事件获得事件数据包括:获得设备的设备信息;以及生成包括设备的标识信息和设备信息的交易。

[0313] 136.根据方面130-135中任一项所述的方法,其中,智能合约接收与安全仪表系统(SIS)设备相关联的参数,并且响应于确定提供参数的操作员是经授权的操作员而将参数写入SIS设备,并且其中,从过程工厂内发生的事件获得事件数据包括:获得改变与SIS设备相关联的参数的请求;以及生成包括SIS设备的标识信息、所改变的参数、以及所改变的参数的新参数值的交易。

[0314] 137.一种用于使用由多个参与者维护的分布式账本在过程控制系统中创建智能合约的计算设备,包括:一个或多个处理器;通信单元;以及非暂时性计算机可读介质,其耦合到一个或多个处理器和通信单元并在其上存储指令,指令在被一个或多个处理器执行时使计算设备执行以下操作:生成与具有一个或多个现场设备的过程工厂有关的智能合约,每个现场设备执行物理功能以控制工业过程;以及将智能合约部署到存储在由分布式账本网络中的多个参与者维护的分布式账本上的地址。

[0315] 138.根据方面137所述的计算设备,其中,智能合约根据过程工厂内发生的事件来接收或提供通证值。

[0316] 139.根据方面137或方面138中的任一项所述的计算设备,其中,智能合约从第一过程工厂获得通证值,确定产品从第二过程工厂转移到第一过程工厂,并将通证值提供给第二过程工厂。

[0317] 140.根据方面137-139中任一项所述的计算设备,其中,智能合约通过从证据谕示接收指示在第一过程工厂处接收到产品的交易来确定产品从第二过程工厂转移到第一过程工厂。

[0318] 141.根据方面137-140中任一项所述的计算设备,其中,智能合约确定产品符合或超过一个或多个质量指标,并且响应于确定产品符合或超过一个或多个质量指标来将通证值提供给第二过程工厂。

[0319] 142.根据方面137-141中任一项所述的计算设备,其中,智能合约通过从证据谕示接收各自包括产品参数值或过程参数值的一个或多个交易,并将产品参数值或过程参数值

与一个或多个质量指标中包括的产品参数阈值或过程参数阈值进行比较,来确定产品符合或超过一个或多个质量指标。

[0320] 143.根据方面137-142中任一项所述的计算设备,其中,智能合约获得过程工厂内经历故障的设备的设备信息,并响应于接收到共享设备信息的请求,将设备信息提供给设备供应商。

[0321] 144.根据方面137-143中任一项所述的计算设备,其中,智能合约通过从证据谕示接收包括设备信息的交易来获得设备信息。

[0322] 145.根据方面137至144中任一项所述的计算设备,其中,智能合约通过接收包括该请求连同发出请求的用户的身份数据的交易来接收共享设备信息的请求,并且,智能合约将交易中的身份数据与对应于被授权请求分布式账本网络共享设备信息的用户的多个身份数据集进行比较,并当多个身份数据集内包括该身份数据时,将设备信息提供给设备供应商。

[0323] 146.根据方面137-145中任一项所述的计算设备,其中,智能合约接收与安全仪表系统(SIS)设备相关联的参数,并且响应于确定提供参数的操作员是经授权的操作员,将该参数将参数写入SIS设备。

[0324] 147.根据方面137-146中任一项所述的计算设备,其中,智能合约通过接收包括该参数连同提供交易的操作员的身份数据的交易来接收与SIS设备相关联的参数,并且其中,确定提供参数的操作员是经授权的操作员包括:将交易中的身份数据与对应于被授权调整与SIS设备相关联的参数的操作员的多个身份数据集进行比较。

[0325] 148.根据方面137-147中任一项所述的计算设备,其中,与SIS设备相关联的参数是锁定SIS设备的请求。

[0326] 149.一种用于使用由多个参与者维护的分布式账本在过程控制系统中的智能合约进行交互的系统,包括:一个或多个设备,其设置在过程工厂中,每个设备执行物理功能以控制工业过程;以及机身设备,其在过程工厂中执行,包括:一个或多个处理器;通信单元;以及非暂时性计算机可读介质,其耦合到一个或多个处理器和通信单元并在其上存储指令,指令在被一个或多个处理器执行时使计算设备执行以下操作:经由一个或多个设备从在过程工厂内发生的事件获得事件数据;响应于智能合约被部署到存储在分布式账本上的地址,生成包括事件数据的交易;以及将交易传送到存储在由分布式账本网络中的多个参与者维护的分布式账本上的智能合约。

[0327] 150.根据方面149所述的系统,其中,所述指令还使所述计算设备:获得计算设备的身份数据;利用计算设备的身份数据扩充交易;基于交易生成加密签名;以及利用加密签名扩充交易。

[0328] 151.根据方面149或方面150中任一项所述的系统,其中,指令还使计算设备执行以下操作:将交易添加到交易区块中;以及基于交易区块求解密码难题;将密码难题的解添加到交易区块中;以及将交易区块传送给分布式账本网络中的至少一个其他参与者。

[0329] 152.根据方面149-151中任一项所述的系统,其中,智能合约从第一过程工厂获得通证值,确定产品从第二过程工厂转移到第一过程工厂,并将通证值提供给第二过程工厂,并且其中,为了从在过程工厂内发生的事件获得事件数据,指令使计算设备执行以下操作:获得在第一过程工厂处接收到产品的指示;以及生成包括第一过程工厂的标识信息、产品

的标识信息、以及在第一过程工厂处从第二过程工厂接收到产品的指示的交易。

[0330] 153.根据方面149-152中任一项所述的系统,其中,为了获得在第一过程工厂处接收到产品的指示,指令使计算设备执行以下操作:获得产品的一个或多个产品参数值或在制造产品时涉及的过程工厂实体的一个或多个过程参数值;以及生成包括一个或多个产品参数值或一个或多个过程参数值的交易。

[0331] 154.根据方面149-153中任一项所述的系统,其中,智能合约获得过程工厂内经历故障的设备的设备信息,并响应于接收到共享设备信息的请求,将设备信息提供给设备供应商,并且其中,为了从过程工厂内发生的事件获得事件数据,指令使计算设备执行以下操作:获得设备的设备信息;以及生成包括设备的标识信息和设备信息的交易。

[0332] 155.根据方面149-154中任一项所述的系统,其中,智能合约接收与安全仪表系统(SIS)设备相关联的参数,并且响应于确定提供参数的操作员是经授权的操作员而将参数写入SIS设备,并且其中,为了从过程工厂内发生的事件获得事件数据,指令使计算设备执行以下操作:获得改变与SIS设备相关联的参数的请求;以及生成包括SIS设备的标识信息、所改变的参数、以及所改变的参数的新参数值的交易。

[0333] 当以软件实现时,本文描述的任何应用、服务和引擎可以存储在任何有形的、非暂时性的计算机可读存储器中,例如存储在磁盘、激光盘、固态存储器设备、分子存储器存储设备或其他存储介质上、存储在计算机或处理器的RAM或ROM中,等等。尽管将本文所公开的示例系统公开为包括在硬件上执行的软件和/或固件以及其他部件,但应注意的是,这种系统仅仅是说明性的,不应被认为是限制性的。例如,可以预期,这些硬件、软件和固件部件中的任何一个或全部可以仅以硬件、仅以软件或以硬件和软件的任何组合来体现。因此,尽管将本文所描述的示例系统描述为以在一个或多个计算机设备的处理器上执行的软件来实现,但是本领域普通技术人员将容易理解,所提供的示例不是实现这种系统的唯一方式。

[0334] 因此,尽管已经参照特定示例描述了本发明,但是这些特定示例仅旨在用于说明而不是限制本发明,对于本领域普通技术人员而言将显而易见的是,在不脱离本发明的精神和范围的情况下,可以对所公开的实施例进行改变、添加或删除。

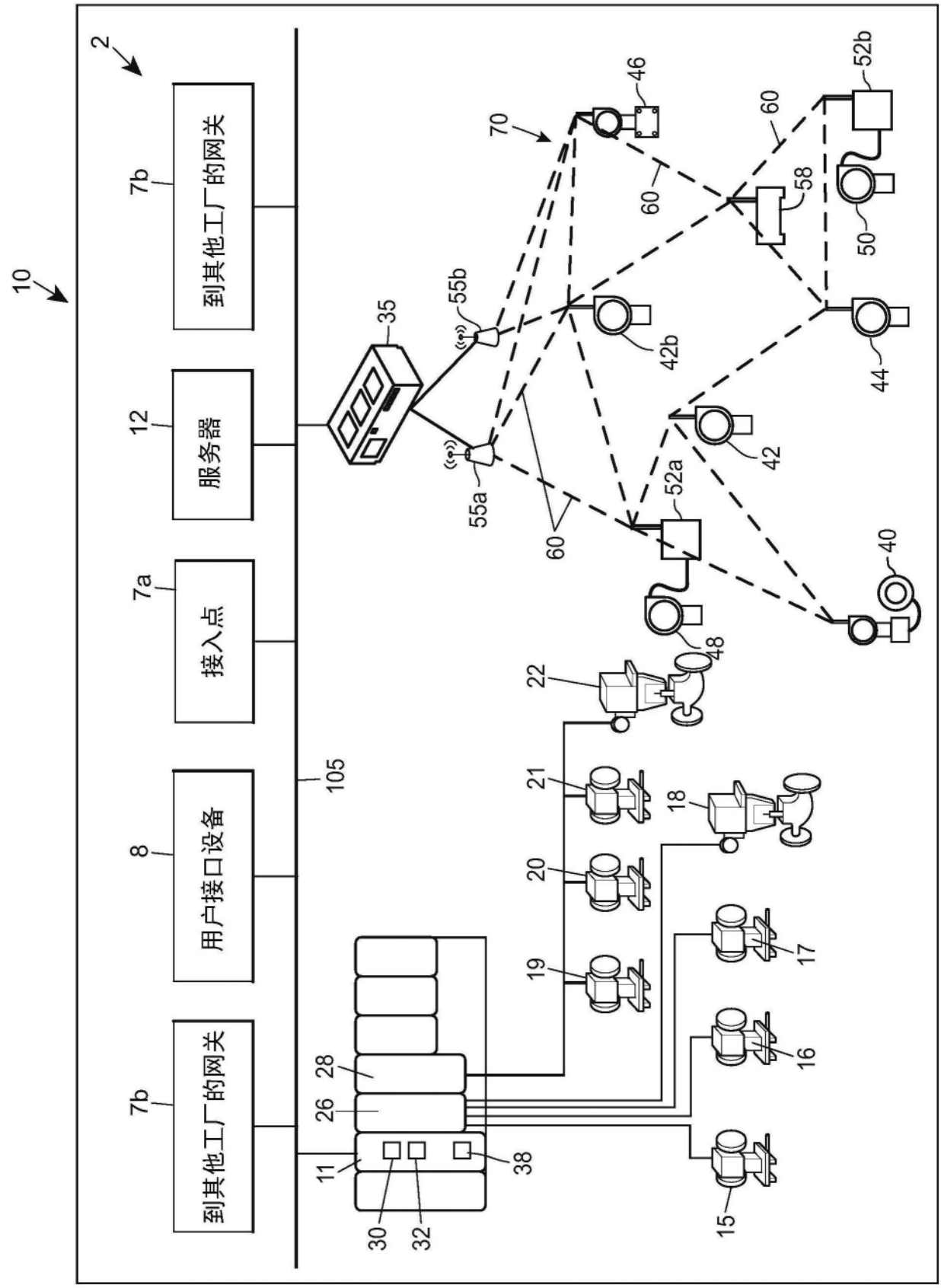

10
2
7b
到其他工厂的网关
12
服务器
7a
接入点
8
用户接口设备
7b
到其他工厂的网关
105
35
55b
55a
70
46
60
58
52b
50
42b
44
42
52a
40
48
22
21
18
20
19
17
16
15
28
26
11
38
30
32

图1

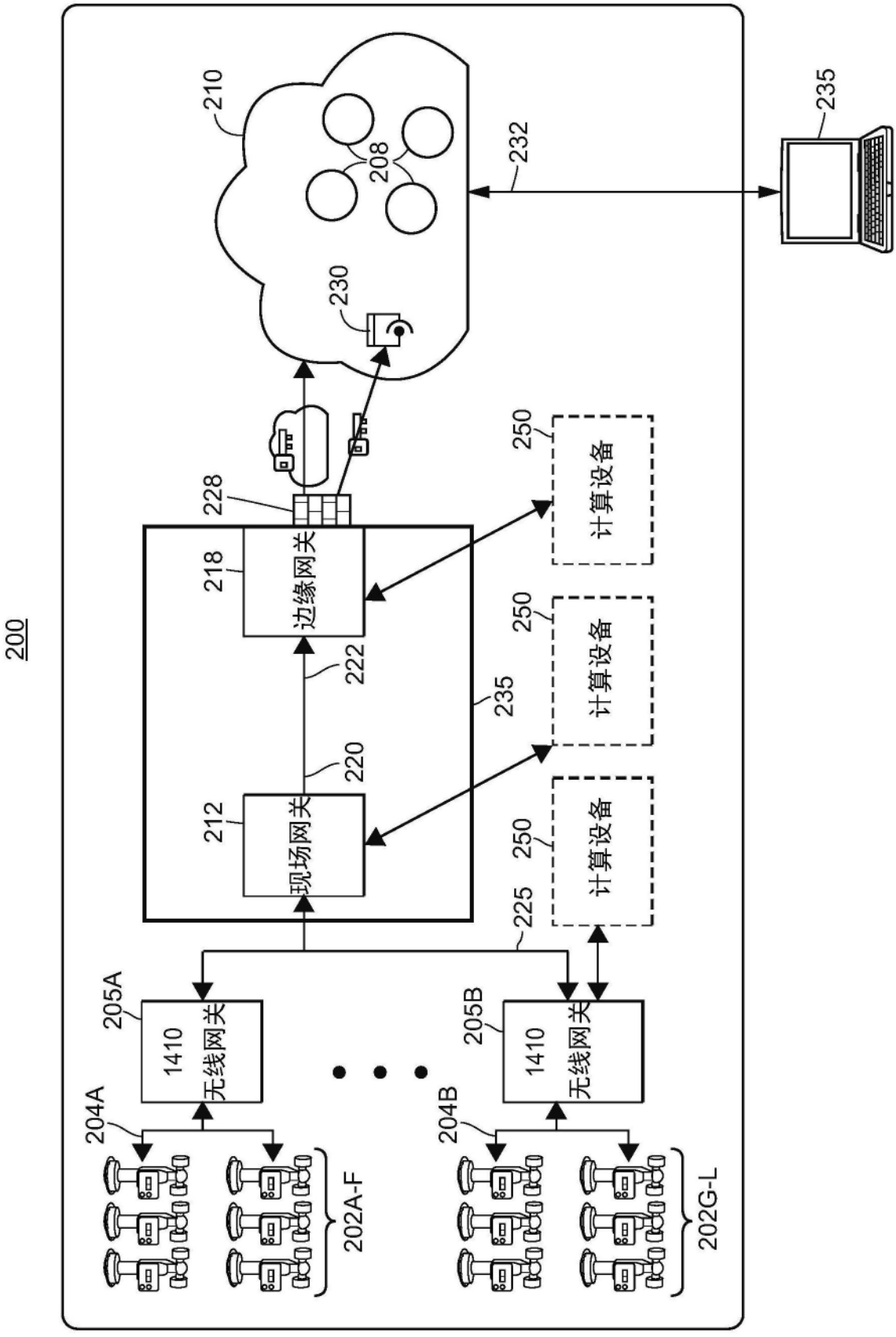

200
210
208
232
235
230
228
218
边缘网关
250
计算设备
222
235
250
计算设备
220
212
现场网关
250
计算设备
225
205A
1410
无线网关
205B
1410
无线网关
204A
204B
202A-F
202G-L

图2

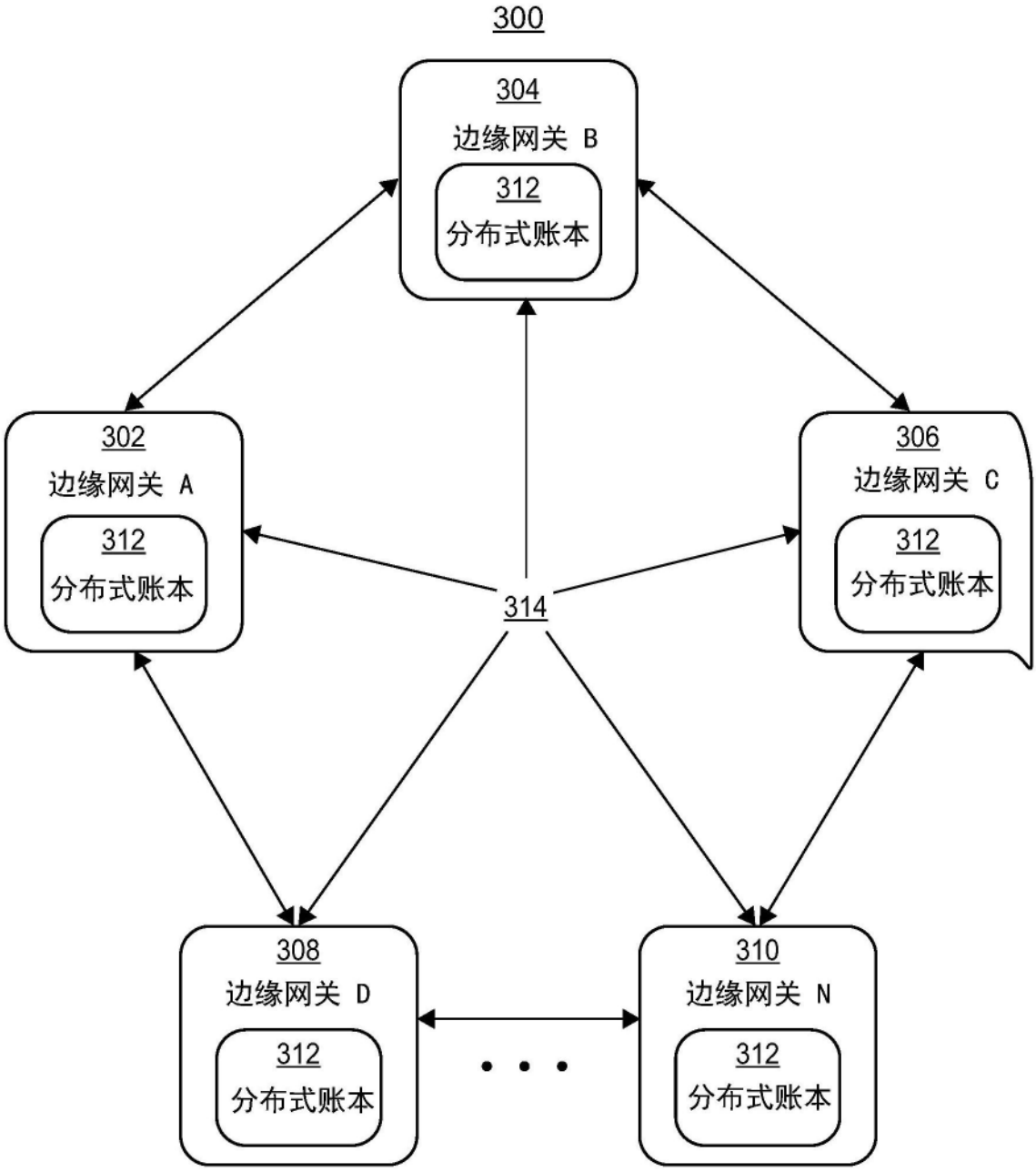

300
304
边缘网关 B
312
分布式账本
302
边缘网关 A
312
分布式账本
306
边缘网关 C
312
分布式账本
314
308
边缘网关 D
312
分布式账本
310
边缘网关 N
312
分布式账本

图3

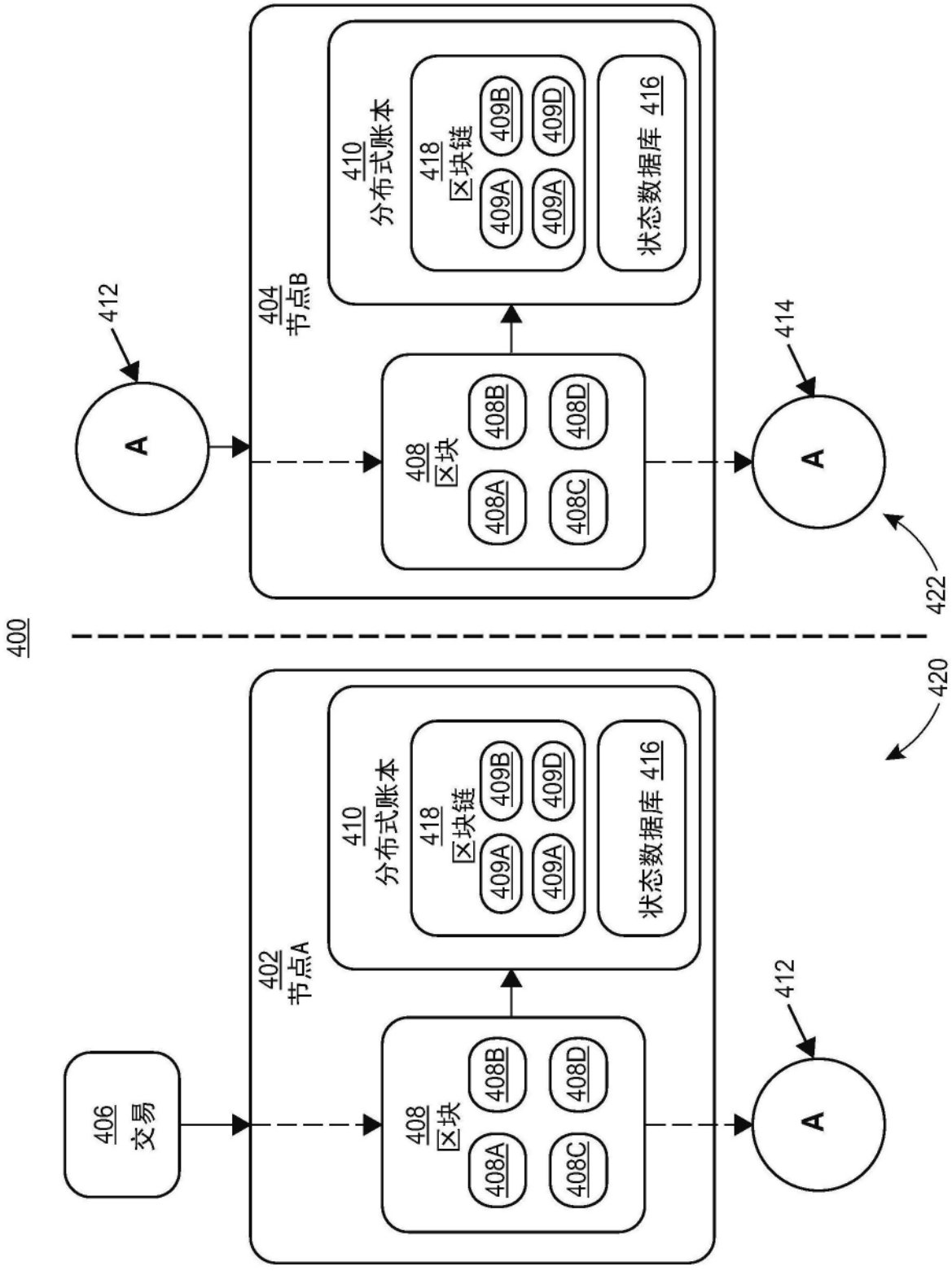

400
406 交易
402 节点A
404 节点B
408 区块
408A
408B
408C
408D
410 分布式账本
418 区块链
409A
409B
409D
状态数据库 416
412
414
A
420
422

图4

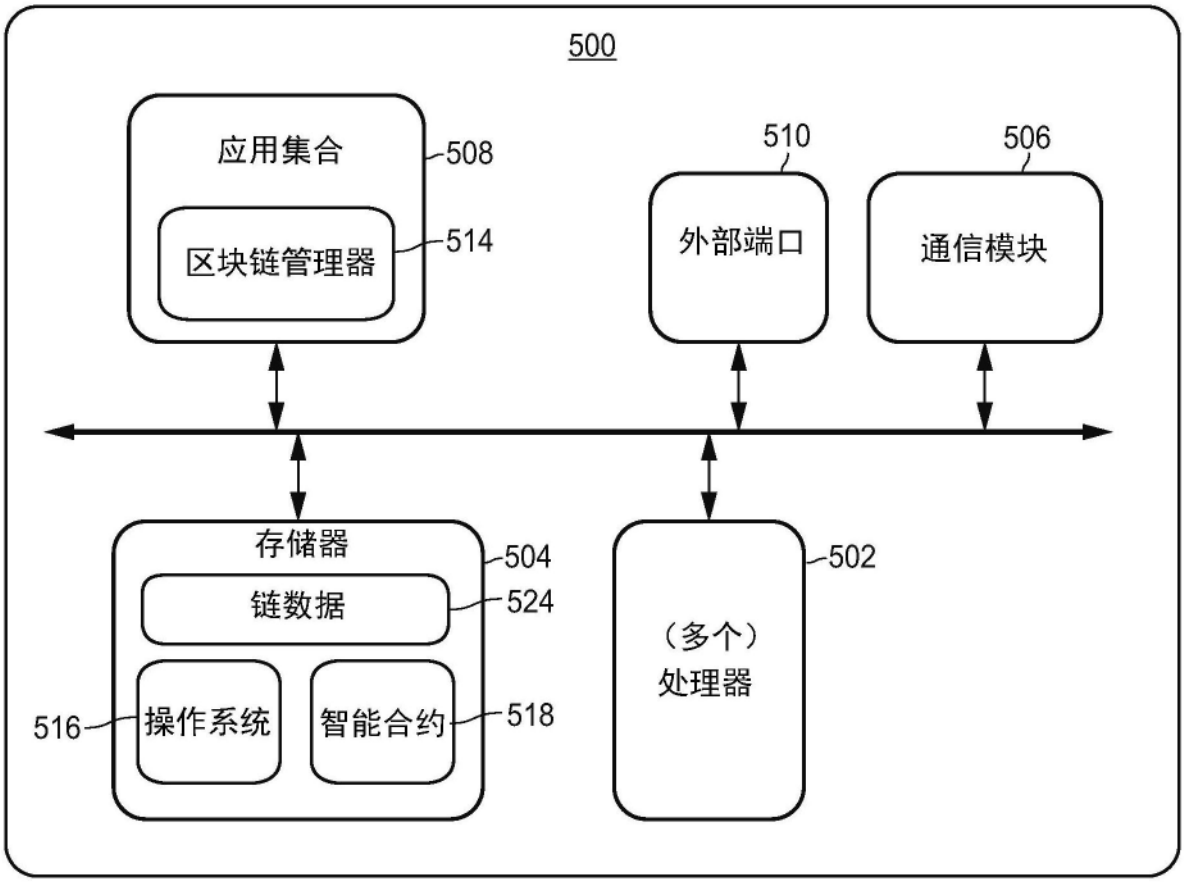

500
应用集合
508
区块链管理器
514
510
外部端口
506
通信模块
存储器
504
链数据
524
516
操作系统
智能合约
518
（多个）
处理器
502

图5

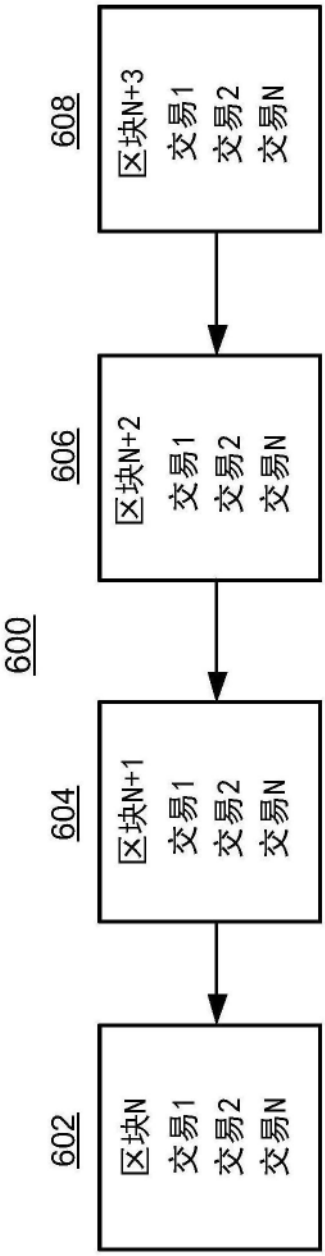

600
602
区块N
交易1
交易2
交易N
604
区块N+1
交易1
交易2
交易N
606
区块N+2
交易1
交易2
交易N
608
区块N+3
交易1
交易2
交易N

图6A

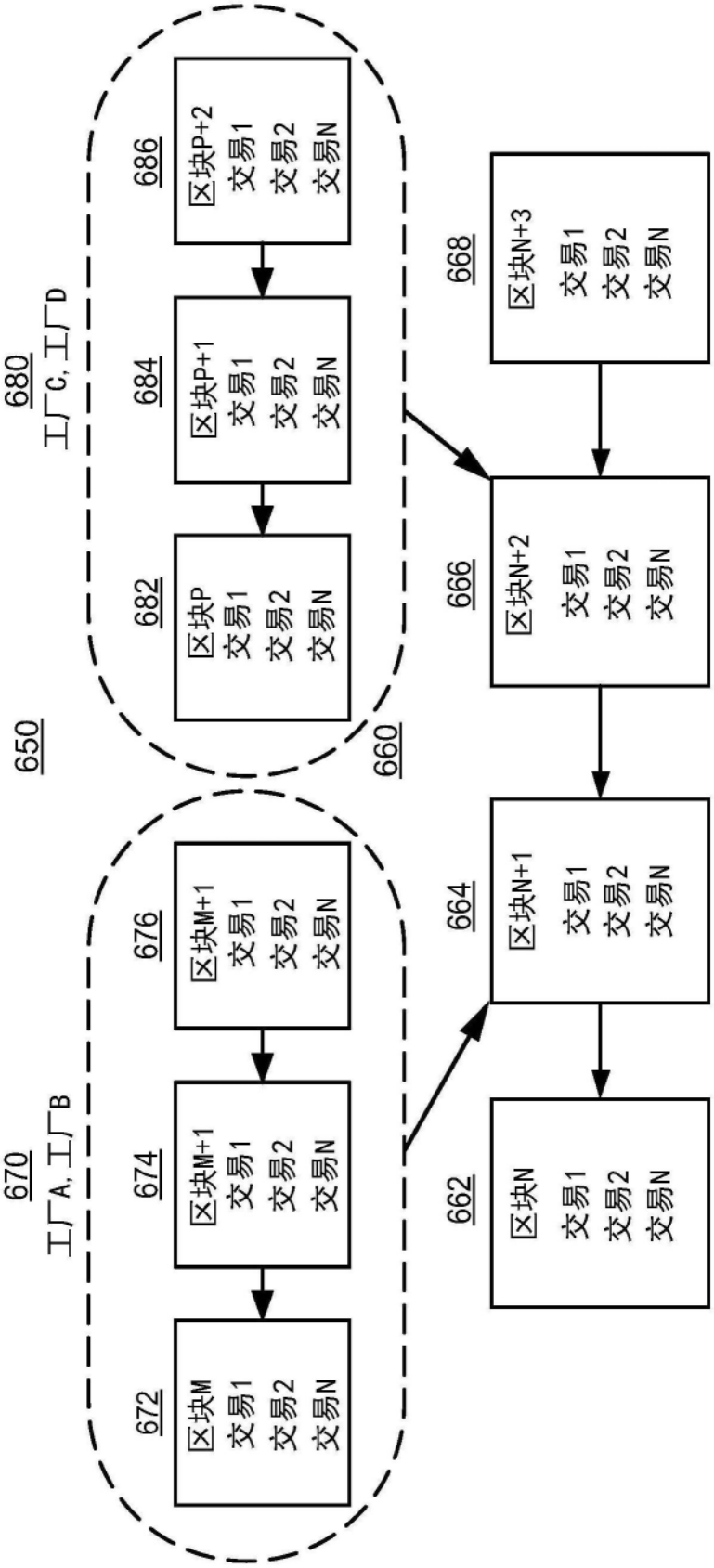

650
660
670
工厂A, 工厂B
672
区块M
交易1
交易2
交易N
674
区块M+1
交易1
交易2
交易N
676
区块M+1
交易1
交易2
交易N
680
工厂C, 工厂D
682
区块P
交易1
交易2
交易N
684
区块P+1
交易1
交易2
交易N
686
区块P+2
交易1
交易2
交易N
662
区块N
交易1
交易2
交易N
664
区块N+1
交易1
交易2
交易N
666
区块N+2
交易1
交易2
交易N
668
区块N+3
交易1
交易2
交易N

图6B

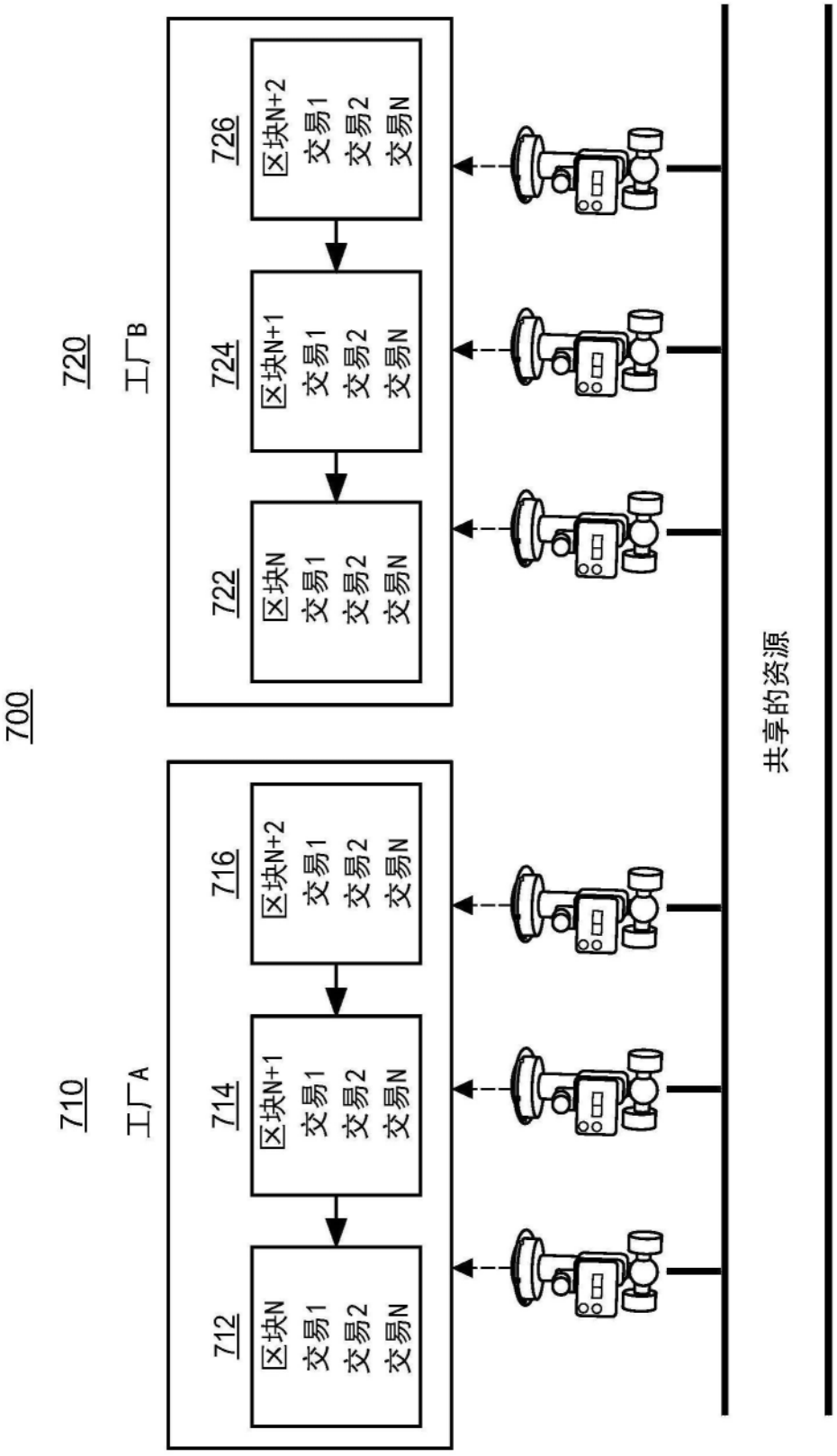

700
710
工厂A
712
区块N
交易1
交易2
交易N
714
区块N+1
交易1
交易2
交易N
716
区块N+2
交易1
交易2
交易N
720
工厂B
722
区块N
交易1
交易2
交易N
724
区块N+1
交易1
交易2
交易N
726
区块N+2
交易1
交易2
交易N
共享的资源

图7A

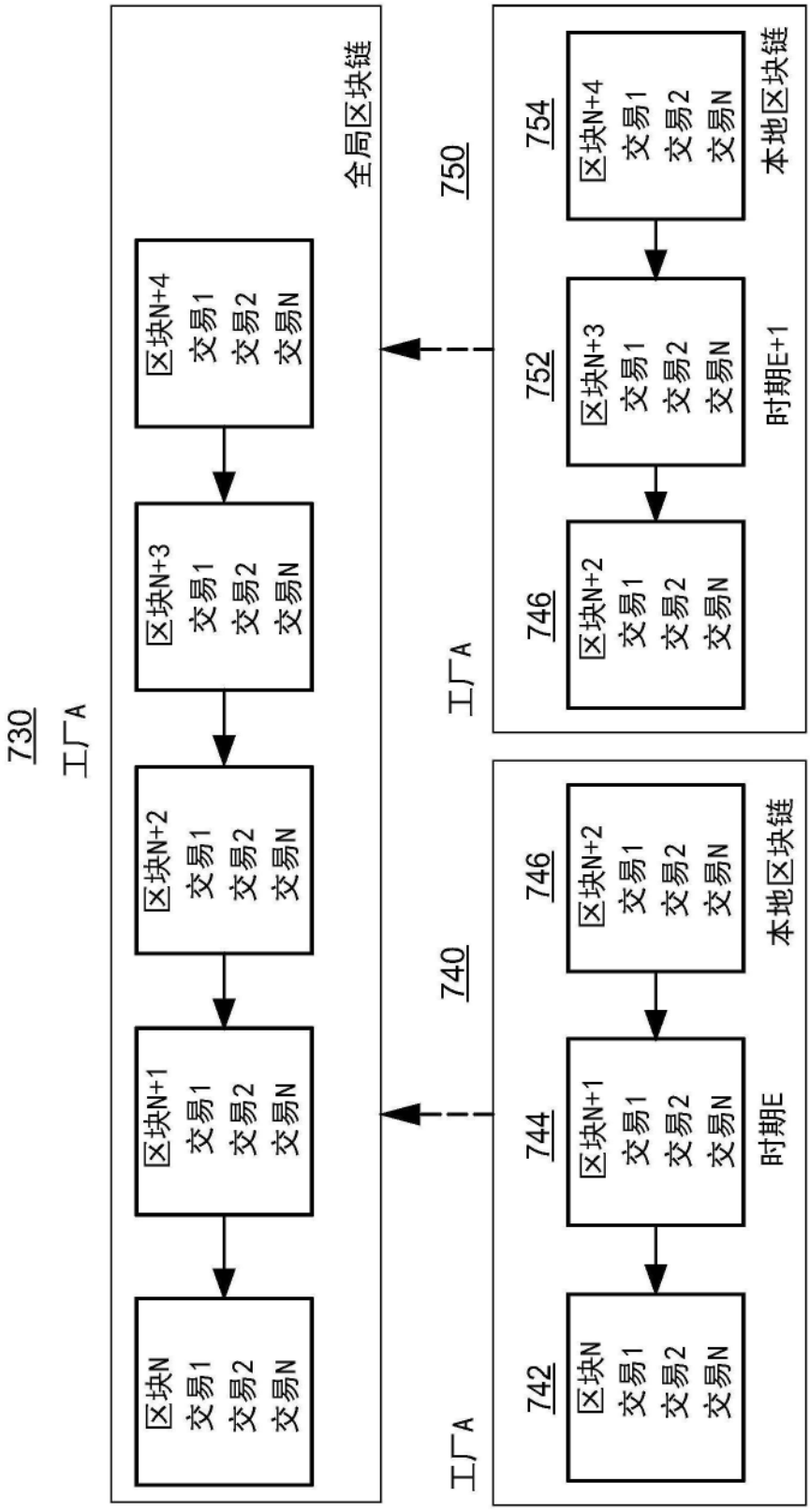

730
工厂A
全局区块链
区块N
交易1
交易2
交易N
区块N+1
交易1
交易2
交易N
区块N+2
交易1
交易2
交易N
区块N+3
交易1
交易2
交易N
区块N+4
交易1
交易2
交易N
740
742
744
746
750
752
754
746
本地区块链
时期E
本地区块链
时期E+1
工厂A
工厂A

图7B

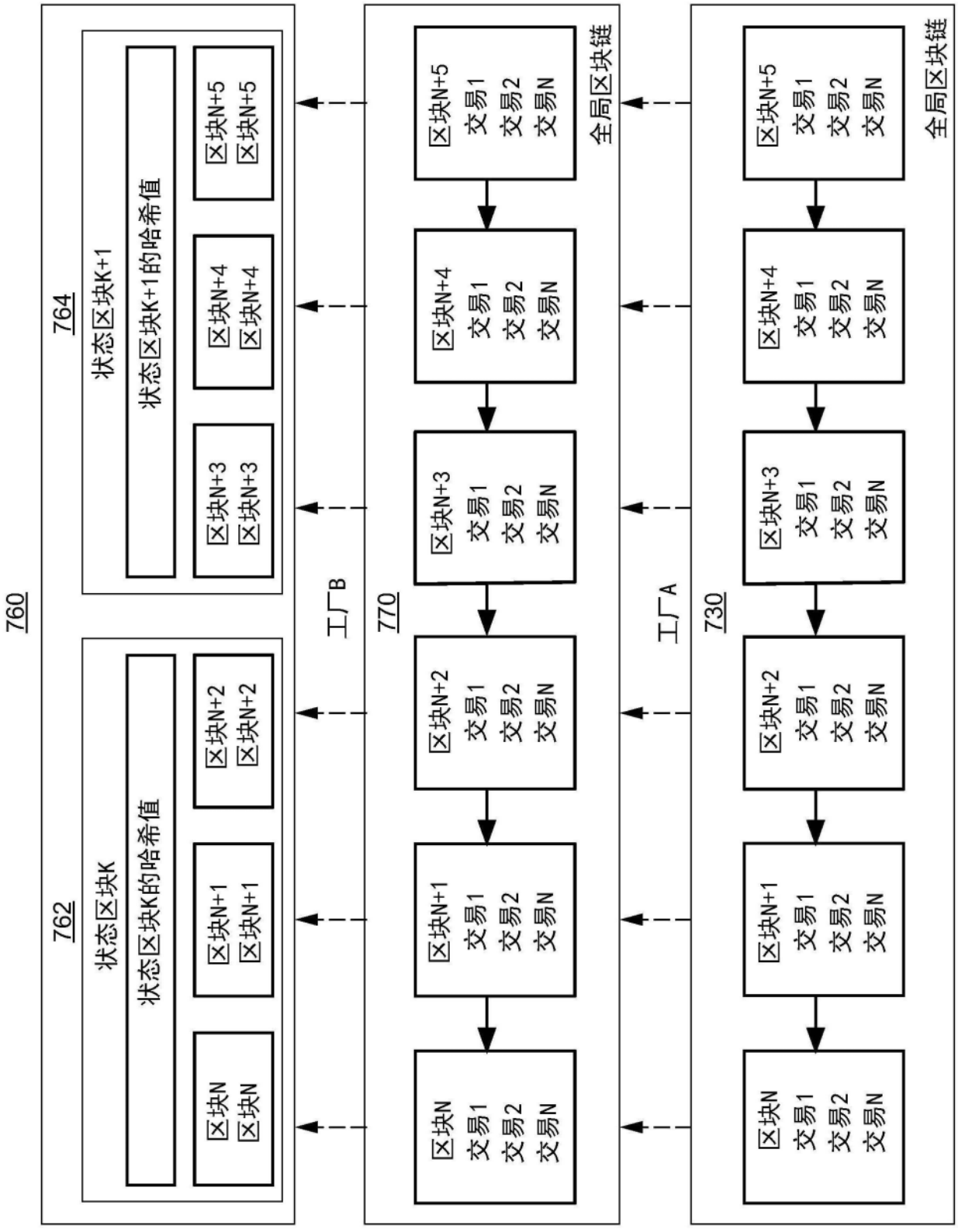

760
762
状态区块K
状态区块K的哈希值
区块N
区块N
区块N+1
区块N+1
区块N+2
区块N+2
764
状态区块K+1
状态区块K+1的哈希值
区块N+3
区块N+3
区块N+4
区块N+4
区块N+5
区块N+5
工厂B
770
全局区块链
区块N
交易1
交易2
交易N
区块N+1
交易1
交易2
交易N
区块N+2
交易1
交易2
交易N
区块N+3
交易1
交易2
交易N
区块N+4
交易1
交易2
交易N
区块N+5
交易1
交易2
交易N
工厂A
730
全局区块链
区块N
交易1
交易2
交易N
区块N+1
交易1
交易2
交易N
区块N+2
交易1
交易2
交易N
区块N+3
交易1
交易2
交易N
区块N+4
交易1
交易2
交易N
区块N+5
交易1
交易2
交易N

图7C

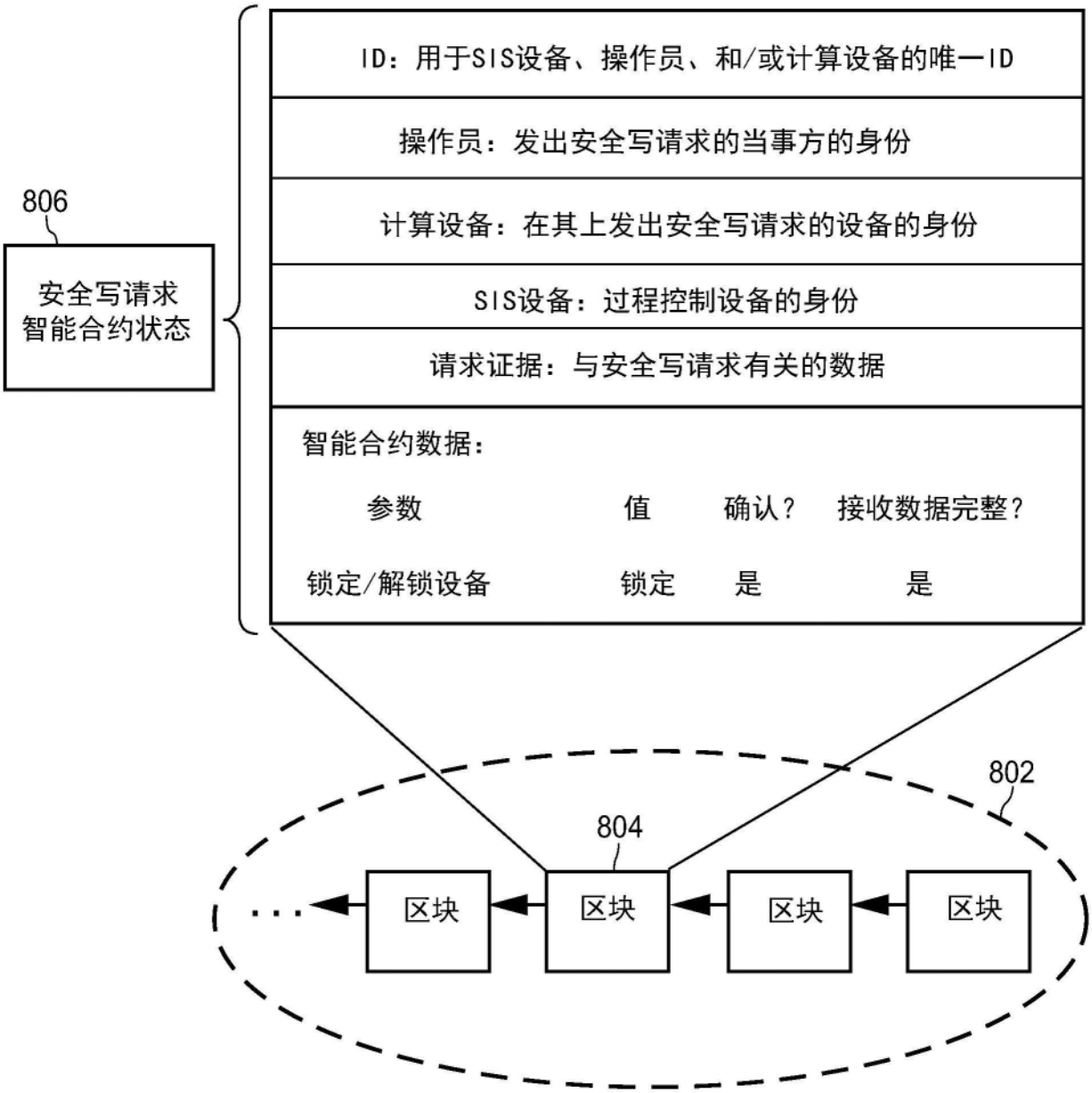

806
安全写请求
智能合约状态
ID：用于SIS设备、操作员、和/或计算设备的唯一ID
操作员：发出安全写请求的当事方的身份
计算设备：在其上发出安全写请求的设备的身份
SIS设备：过程控制设备的身份
请求证据：与安全写请求有关的数据
智能合约数据：
参数 值 确认？ 接收数据完整？
锁定/解锁设备 锁定 是 是
802
804
区块
区块
区块
区块

图8

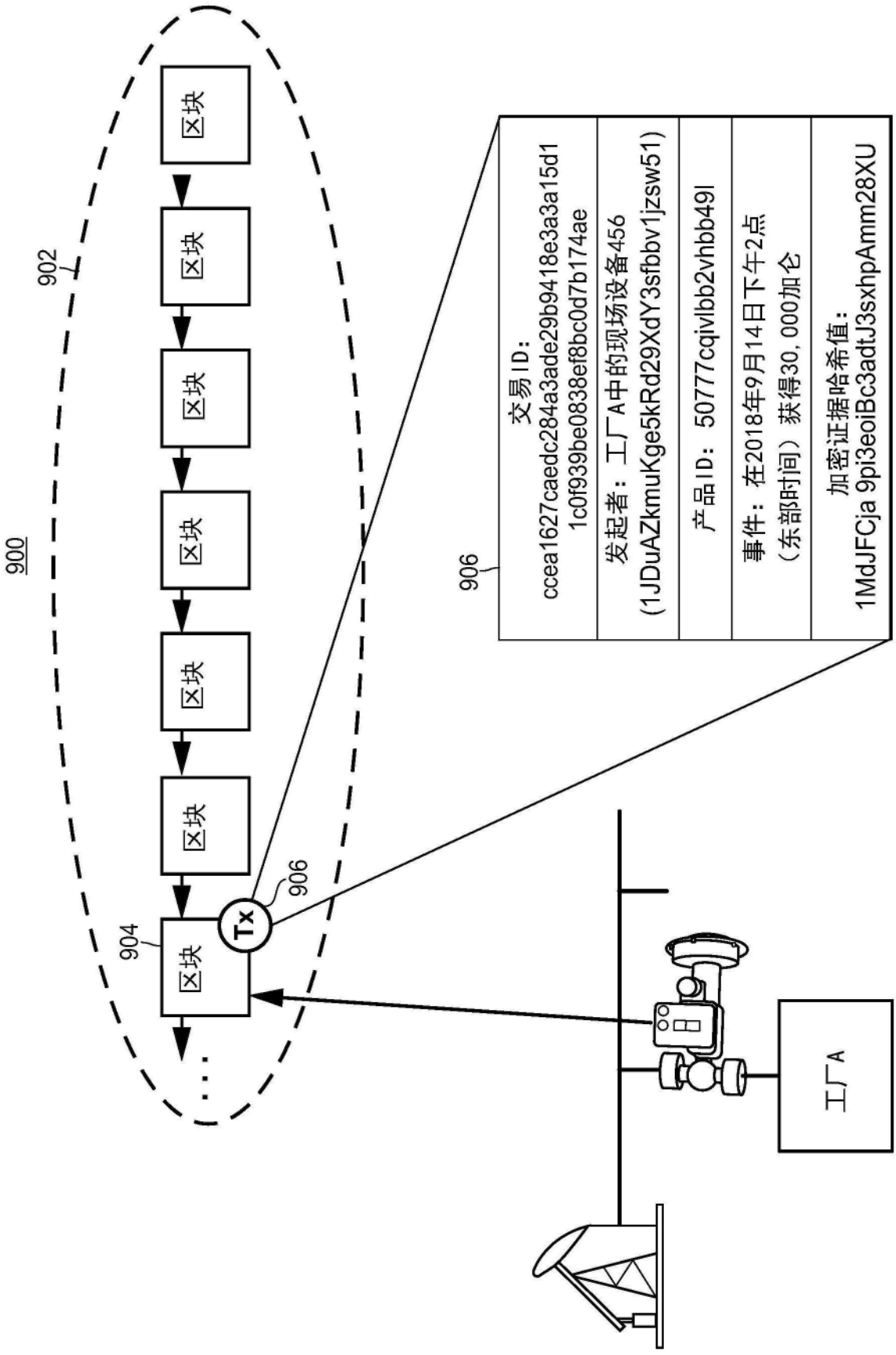

900
902
区块
区块
区块
区块
区块
区块
区块
904
Tx
906
906
交易ID:
ccea1627caedc284a3ade29b9418e3a3a15d1
1c0f939be0838ef8bc0d7b174ae
发起者：工厂A中的现场设备456
(1JDuAZkmuKge5kRd29XdY3sfbbv1jzsw51)
产品ID： 50777cqivlbb2vhbb49l
事件：在2018年9月14日下午2点
（东部时间）获得30,000加仑
加密证据哈希值:
1MdJFCja 9pi3eoiBc3adtJ3sxhpAmm28XU
工厂A

图9

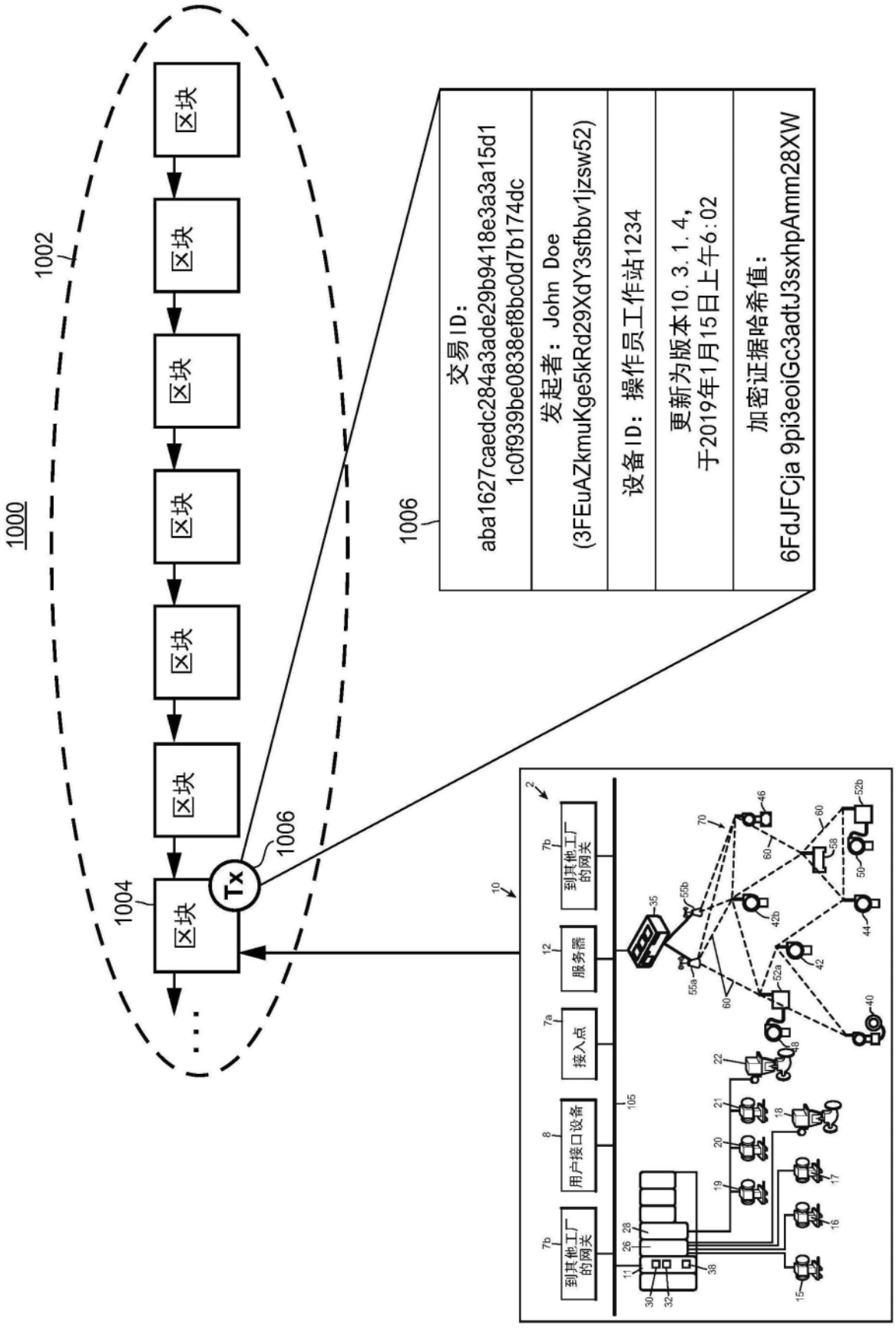

1000
1002
区块
区块
区块
区块
区块
区块
区块
1004
Tx
1006
交易ID:
aba1627caedc284a3ade29b9418e3a3a15d1
1c0f939be0838ef8bc0d7b174dc
发起者：John Doe
(3FEuAZkmuKge5kRd29XdY3sfbbv1jzsw52)
设备ID：操作员工作站1234
更新为版本10.3.1.4,
于2019年1月15日上午6:02
加密证据哈希值:
6FdJFCja 9pi3eoiGc3adtJ3sxhpAmm28XW
1006
到其他工厂的网关
用户接口设备
接入点
服务器
到其他工厂的网关

图10

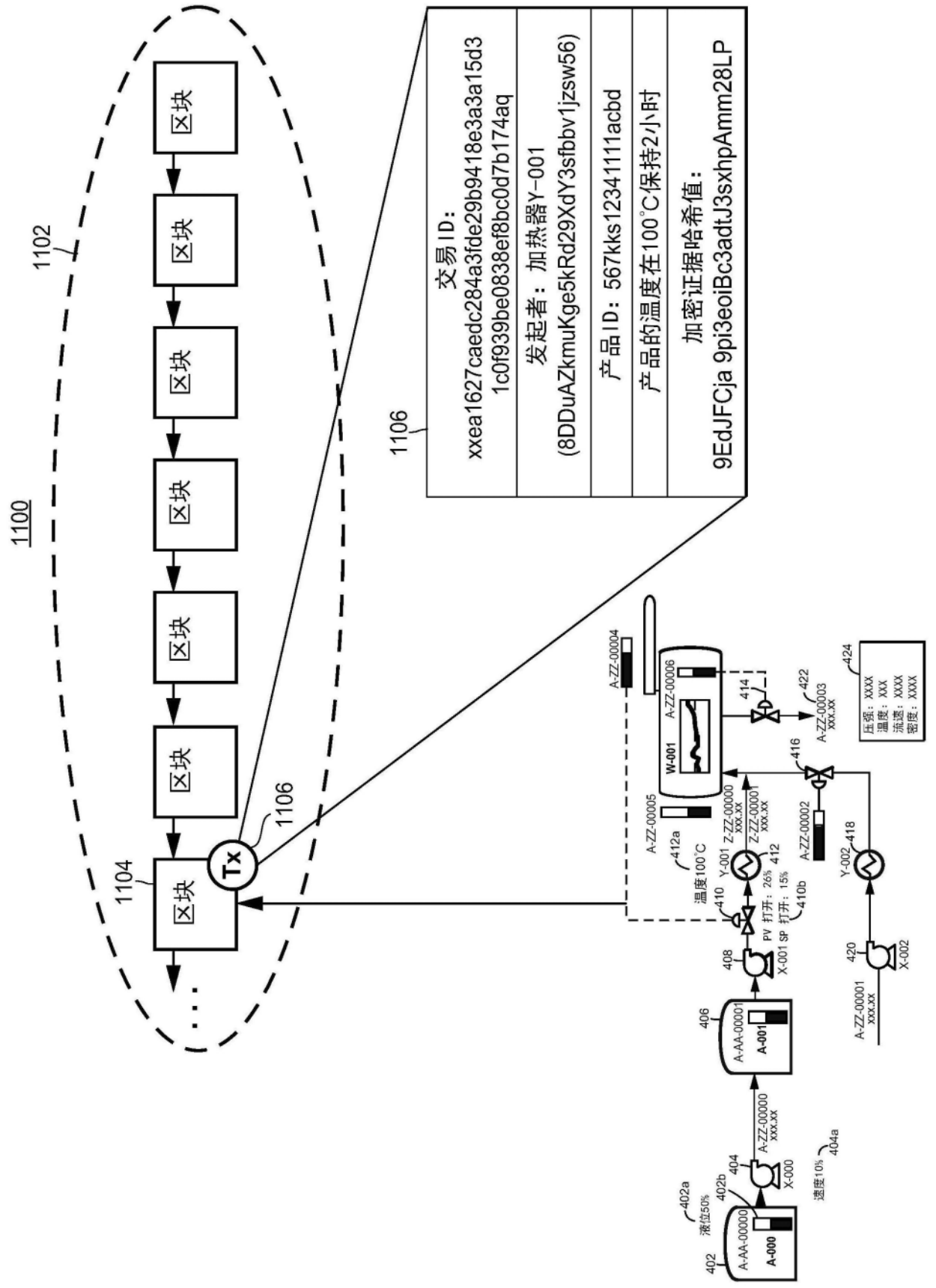

1100
1102
区块
区块
区块
区块
区块
区块
1104
Tx
1106
1106
交易ID:
xxea1627caedc284a3fde29b9418e3a3a15d3
1c0f939be0838ef8bc0d7b174aq
发起者：加热器Y-001
(8DDuAZkmuKge5kRd29XdY3sfbbv1jzsw56)
产品ID：567kks12341111acbd
产品的温度在100℃保持2小时
加密证据哈希值:
9EdJFCja 9pi3eoiBc3adtJ3sxhpAmm28LP
A-ZZ-00004
A-ZZ-00006
W-001
A-ZZ-00005
412a
温度100℃
410
Y-001
Z-ZZ-00000
xxx.xx
Z-ZZ-00001
xxx.xx
412
PV 打开：26%
X-001 SP 打开：15%
410b
414
422
A-ZZ-00003
xxx.xx
424
压强：XXXX
温度：XXX
流速：XXXX
密度：XXXX
416
A-ZZ-00002
Y-002
418
420
X-002
A-ZZ-00001
xxx.xx
408
406
A-AA-00001
A-001
A-ZZ-00000
xxx.xx
X-000
404
404a
速度10%
402a
液位50%
402b
A-AA-00000
A-000
402

图11

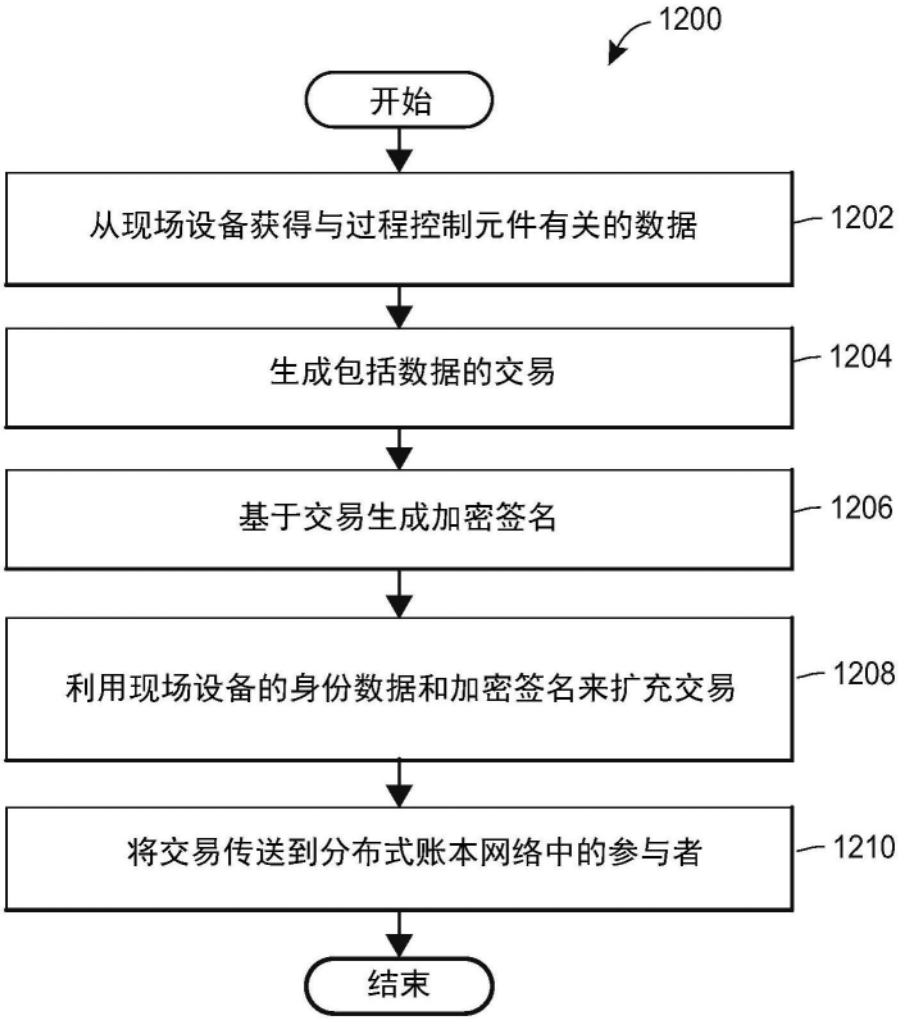

1200
开始
从现场设备获得与过程控制元件有关的数据
1202
生成包括数据的交易
1204
基于交易生成加密签名
1206
利用现场设备的身份数据和加密签名来扩充交易
1208
将交易传送到分布式账本网络中的参与者
1210
结束

图12

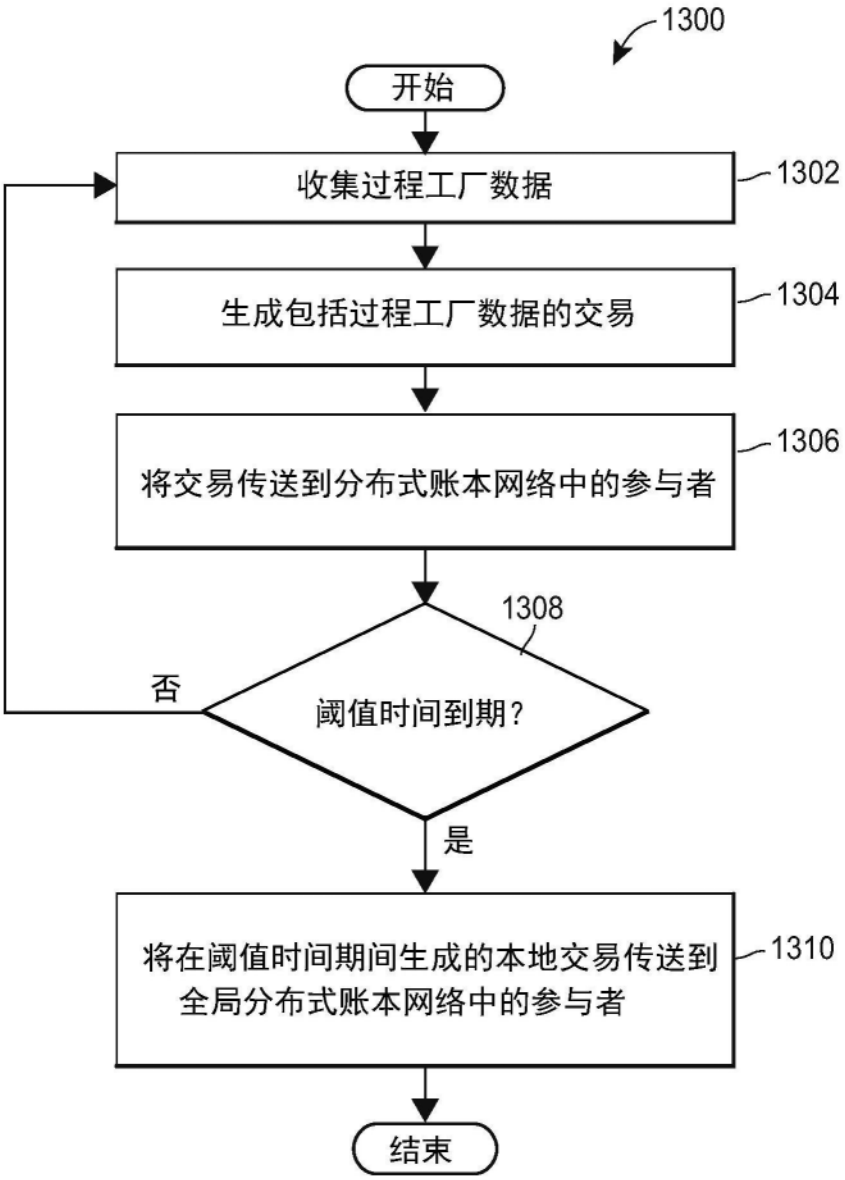

1300
开始
收集过程工厂数据
1302
生成包括过程工厂数据的交易
1304
将交易传送到分布式账本网络中的参与者
1306
1308
阈值时间到期?
否
是
将在阈值时间期间生成的本地交易传送到全局分布式账本网络中的参与者
1310
结束

图13

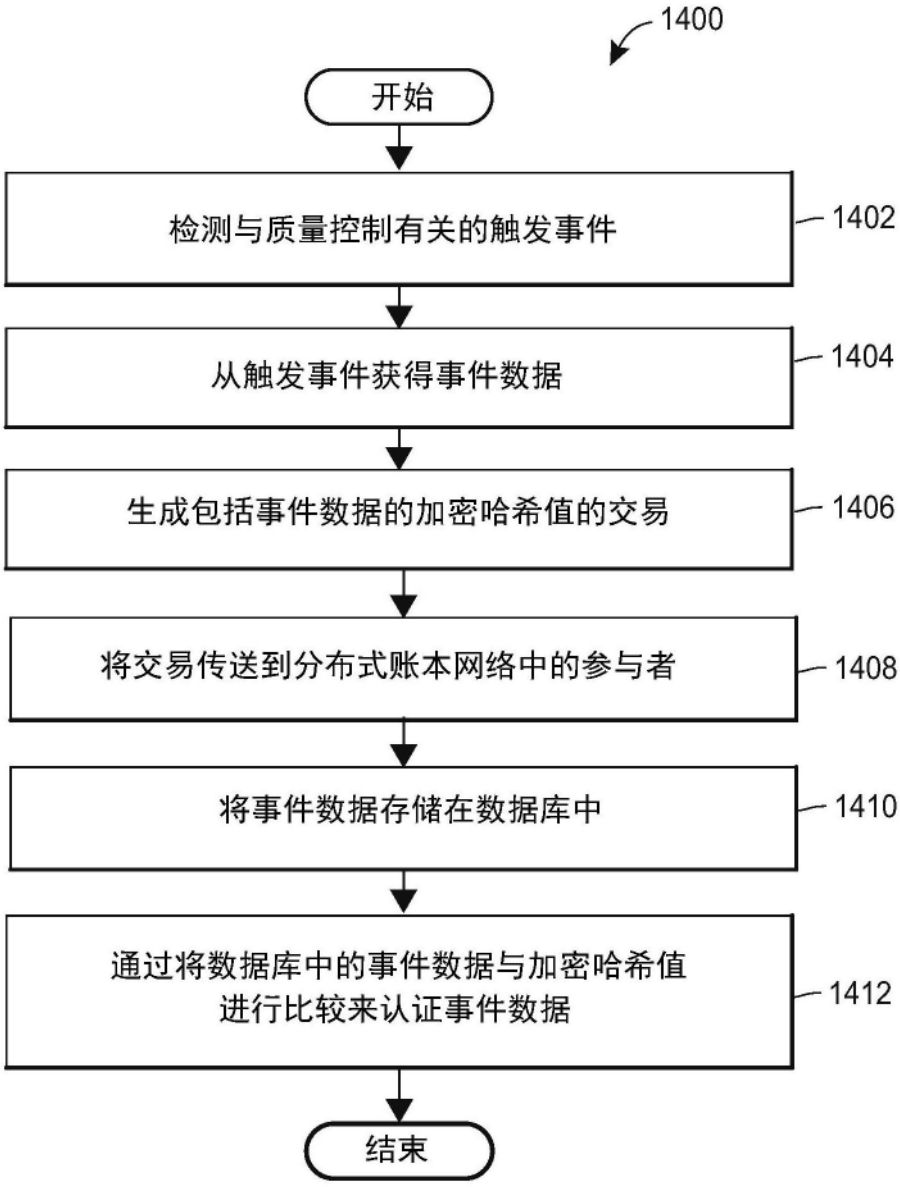

1400
开始
检测与质量控制有关的触发事件
1402
从触发事件获得事件数据
1404
生成包括事件数据的加密哈希值的交易
1406
将交易传送到分布式账本网络中的参与者
1408
将事件数据存储在数据库中
1410
通过将数据库中的事件数据与加密哈希值
进行比较来认证事件数据
1412
结束

图14

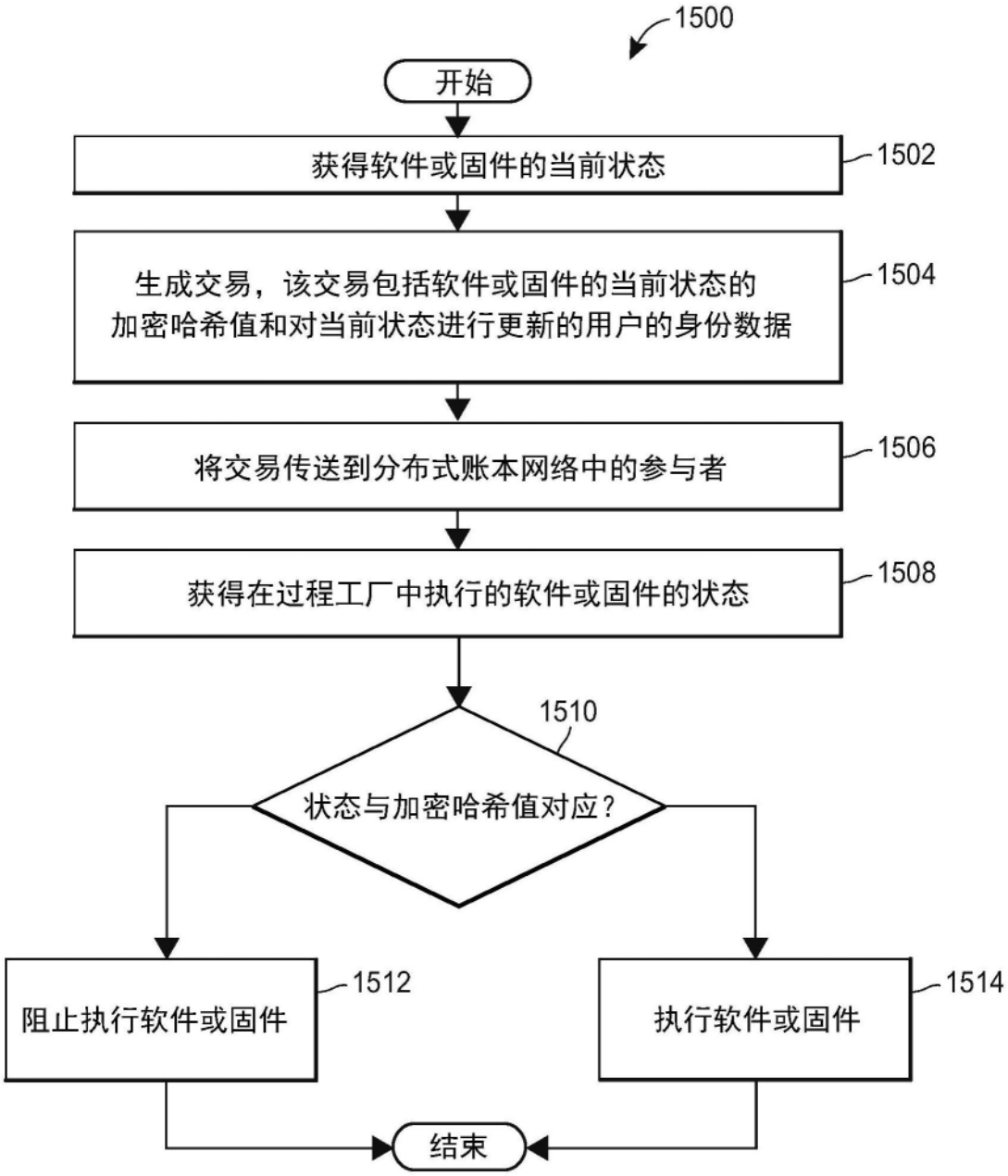

1500
开始
获得软件或固件的当前状态
1502
生成交易，该交易包括软件或固件的当前状态的加密哈希值和对当前状态进行更新的用户的身份数据
1504
将交易传送到分布式账本网络中的参与者
1506
获得在过程工厂中执行的软件或固件的状态
1508
1510
状态与加密哈希值对应？
阻止执行软件或固件
1512
执行软件或固件
1514
结束

图15

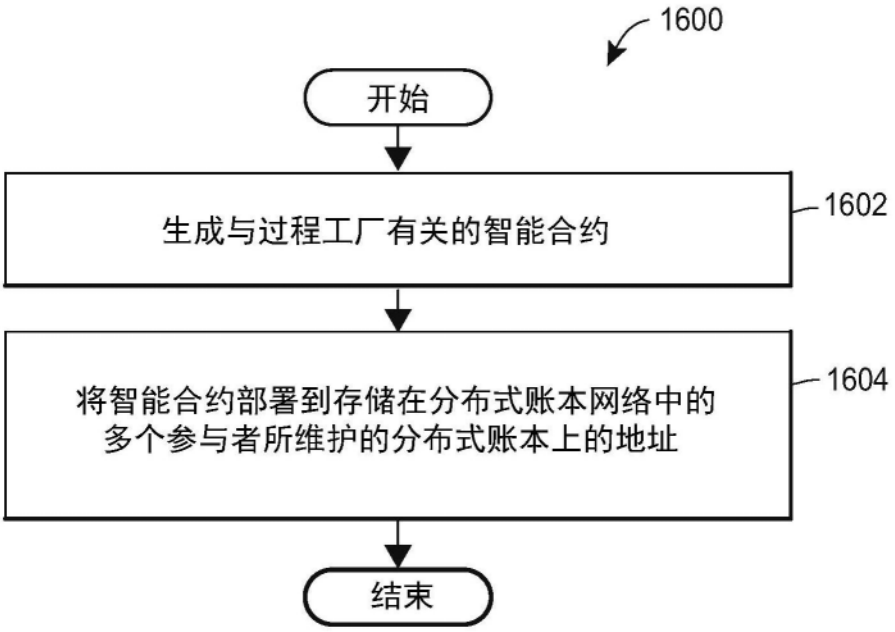

1600
开始
生成与过程工厂有关的智能合约
1602
将智能合约部署到存储在分布式账本网络中的
多个参与者所维护的分布式账本上的地址
1604
结束

图16

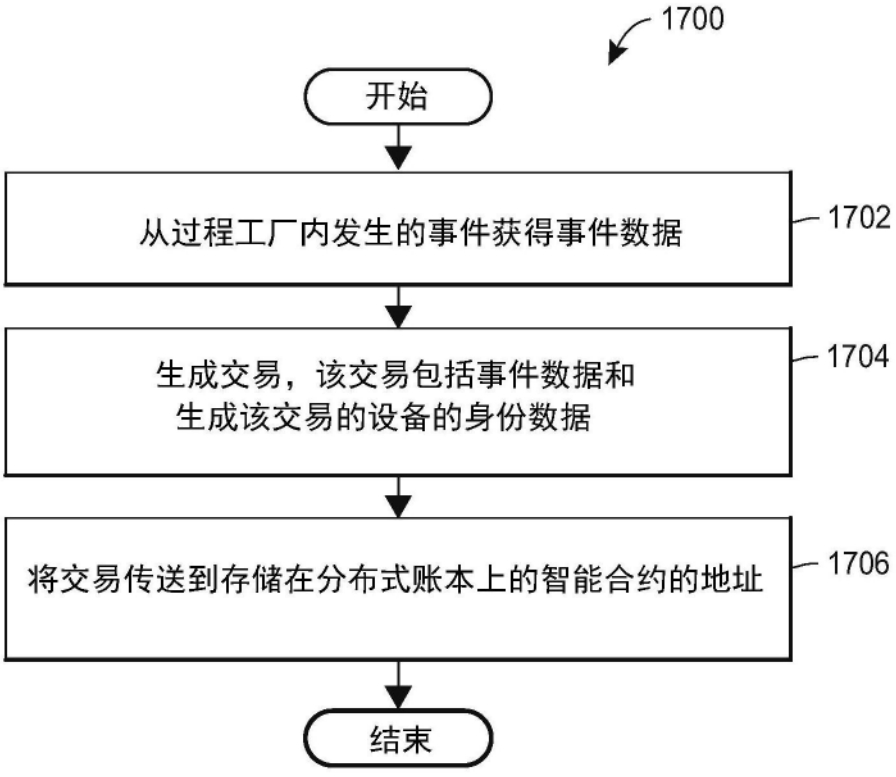

1700
开始
从过程工厂内发生的事件获得事件数据
1702
生成交易，该交易包括事件数据和
生成该交易的设备的身份数据
1704
将交易传送到存储在分布式账本上的智能合约的地址
1706
结束

图17