基于区块链的ICS数据安全策略研究

刘 俊,陈 慧,王 军
(沈阳化工大学,辽宁 沈阳 110000)

摘 要:随着“中国制造2025”规划的推进,工业控制系统(industrial control system,ICS)日益增长,工控网络安全性和可靠性得到普遍关注。区块链思想和技术的出现,为数据安全性和可靠性提供了新的思路。针对工业控制网络中的数据安全问题,将区块链技术应用于工业控制网络中,再结合区块链的关键技术,以及区块链不可篡改、分布式记账和不可伪造的去中心化特点,提出了在工控区块链网络环境下的共识控制模型。在模型中记录一旦被输入就永远不会被更改或删除,想通过干预个别节点而篡改数据是不可能的,除非对全网信息进行干预,保证了模型中节点之间的数据的一致性。通过OPNET网络仿真软件对工控区块链网络进行仿真,其网络延时和吞吐量都说明了区块链技术能实现工业控制系统的网络安全、数据安全,使工业控制网络可靠、安全、高效、低成本。

关键词:区块链;工业控制系统;网络安全;数据安全;共识机制;OPNET
中图分类号:TP39 **文献标识码**:A **文章编号**:1673-629X(2021)01-0149-06
doi:10.3969/j.issn.1673-629X.2021.01.027

Research on Data Security Strategy of ICS Based on Blockchain

LIU Jun,CHEN Hui,WANG Jun
(Shenyang University of Chemical Technology,Shenyang 110000,China)

Abstract:With the promotion of “Made in China 2025” plan,the industrial control system (ICS) in China is growing day by day,and the safety and reliability of industrial control network are paid more and more attention. The emergence of blockchain idea and technology provides a new idea for data security and reliability. Aiming at the problem of data security in the industrial control network,applying the block chain technology to the industrial control network and combining the key technologies of the block chain,as well as the characteristics of the block chain that can not be tampered with,distributed accounting and non forgeable decentralization,we put forward the consensus control model in the industrial control block chain network environment. In this model,once the records are input,they will never be changed or deleted. It is impossible to tamper with data by intervening individual nodes,unless the whole network information is intervened to ensure the consistency of data between nodes in the model. Through OPNET Network simulation software to simulate the industrial control blockchain network,its network delay result graph and throughput graph can show that blockchain technology can realize the network security,data security of industrial control system,and make the industrial control network reliable,safe,efficient and low-cost.

Key words:blockchain;industrial control system;network security;data security;consensus mechanism;OPNET

0 引 言

工业控制系统(industrial control system,ICS)是指由计算机与工业过程控制部件组成的自动控制系统,它由控制器、传感器、传送器、执行器和输入/输出接口等部分组成。工业控制系统的子系统或功能组件包括但不限于数据采集与监视控制(SCADA)系统、分布式控制系统(DCS)、可编程逻辑控制器(PLC)、远程测控单元(RTU)等相关信息系统,如图1所示。这些组成部分通过工业通信线路,按照一定的通信协议进行连接,形成一个具有自动控制能力的工业生产制造或加工系统。工业控制网络就是工业控制系统中的网络部分,是一种把工厂中各个生产流程和自动化控制系统通过各种通信设备组织起来的通信网络。这些网络节点是指分散在各个生产现场,具有相应数字通信能力的测量控制仪器。它采用规范、公开的通信协议,把现场总线当作通信连接的纽带,从而使现场控制设备可以相互沟通,共同完成相应的生产任务。

目前来说,随着信息化和智能化融合的不断推进,

收稿日期:2020-02-28 **修回日期**:2020-06-30
基金项目:辽宁省自然基金项目(20190200828)
作者简介:刘 俊(1971-),男,副教授,研究方向为网络安全;通讯作者:王 军(1978-),男,教授,研究方向为物联网与网络安全。

由于集成电路的种类繁多,潜在的风险和影响程度也不尽相同。工业控制系统的信息安全隐患分布于工业控制系统架构的所有层级,攻击者可能通过嗅探、欺骗、物理攻击及病毒传播的方式,进行未授权或非法操作,影响企业正常生产。近年来的工业控制网络安全事件显示出稳步增长的趋势,工控系统频频发生的网络安全事件引发了各国关注,专家、研究人员和工程师致力于解决工业控制系统网络安全问题。

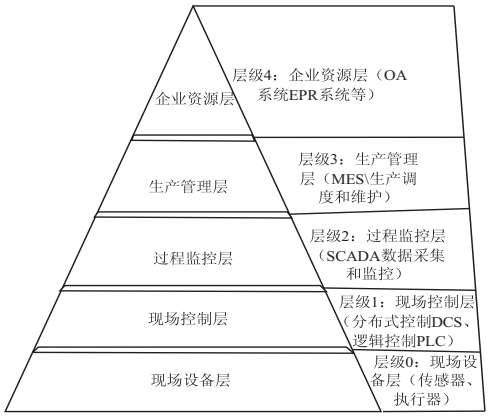

图 1 工业控制系统典型架构

1 相关研究成果

现有的工业安全防护系统都是针对过程监控层及以上的信息技术网络部分,以及从信息网络到工控网络之间的边界部分[1]。林枫[2]提出工业控制是一项具有综合性、技术复杂性的体系工程,工业控制系统本身在设计或操作中容易出现安全隐患。工业控制的网络化设计与应用,让工业控制系统部分暴露在公共信息交流中,使得病毒和木马攻击工业控制系统。其实,工业控制系统从现场设备采集数据到现场控制层 PLC 中及现场设备中存在着不安全的连接或者非法认证等不安全事件,网络系统中的数据可能会遭到复制、篡改,丢失,最终导致系统出现异常或故障。因此有必要加强防护工控网络中的数据安全。

部分研究人员将区块链技术应用到物联网安全上[3-5],解决了物联网的通信安全模式;柏亮[6]从区块链和工业物联网的体系架构角度出发,分析了区块链在工业物联网中的应用可能性,并提出了一种区块链结合工业物联网的架构,使用区块链分布式系统替代传统工业物联网中信息传输和数据管理部分。

在工业控制系统和工业互联网上还是有待研究。因此将结合区块链技术的特点,在过程监控层和现场控制层做安全模型来保护工业控制网络的安全。防止从监控中心向 PLC 下发逻辑组态工程文件在编译成功后,运行过程中不被篡改或者替换。利用区块链技术的去信任、去中心化、集体维护、可靠数据库等特点,构建基于区块链的 ICS 共识控制模型,使区块链网络取代工业控制系统的现场网络,解决 ICS 网络数据安全问题,保证了数据的可用性、保密性、完整性,并且在工业控制网络中传输和交换的数据不会发生增加、修改、丢失和泄露等。

2 区块链技术

2.1 区块链的概念

区块链,也称为共享账本,是一个记录的追加列表,使用加密技术链接和保护记录。著名的区块链实现包括比特币[7]和以太坊[8]。区块链由私有或公共对等网络管理,该网络共同验证并生成新区块。因此,区块链网络由多个节点组成,每个节点都有区块链的本地副本。一些节点参与一个领导选举过程(即工作证明),该过程确定哪个节点获得将下一个块附加到链的权限。这些正在积极竞争成为下一轮领导人的节点被称为矿工。在每轮领导人选举开始时,所有矿工都开始研究一个新的计算问题(例如产生散列),这个问题取决于三个数据:新的交易块、区块链上的最后一个块和一个随机数。这统称为当前块的块头。每次矿工用一个新的随机数对块头执行散列函数时,他们都会得到一个新的结果。为了赢得选举,矿工必须找到一个以一定数量的零开头的散列,需要多少个零是一个未知的参数,由网络上连接了多少矿工和多少计算能力决定。解决此问题的第一个挖掘者获得了使用尚未包含在任何块中的挂起事务编写新块的权限。参加和赢得选举的动机是一种金钱奖励。赢家可以发行一定数量的开采货币,他们可以收取所有交易费用。为了优先处理他们的事务,用户可以提出支付更高的费用。因此,区块链形成了一个系统,可以在不需要任何中央机构的情况下实现分散共识。

区块链的分布式账本可以安全地存储数据,而信息不能伪造和篡改位于区块链上的智能合约脚本,允许多步骤流程。区块链技术是由节点组成的分布式数据库系统。各节点是一个账户,记录事务数据,并使用加密方法来形成这些块,组成数据块,这些数据块的内容是基于时间戳、分散的列值、工作证明和其他确保数据安全的技术。区块链技术的本质是数据的存储、传输和非对称性分布式结构的数据加密方法,用区块链中的数据块代替对中心依赖的服务器,提供底层技术支持,实现信息交流,工业自动化基础设施与环境的安全可靠结构。

分布式数据存储的区块链技术维护一个可靠的数据库,能够适应工控系统网络信息安全,并采用区块链密码技术保证数据不被篡改和伪造,为工业控制系统的全过程提供安全可靠的支持。分布式存储和分块链

技术满足了工业控制系统网络的安全要求。区块链技术与分布式存储技术相结合,在集成电路中构建一个 p2p 网络,从而将工业设备交易数据安全地存储在区块链中,通过复杂的验证机制,区块链能够保持完整性和一致性,实现高效可靠的传输和数据交换。区块链技术可以使工业设备交易和数据交换过程简单,节省成本。区块链还可以通过存储,在不丧失数据机密性的前提下,对工业装置交易数据进行验证和分析,通过区块链技术提高 ICS 效率,未来智能设备可以在分布式物联网,利用区块链记录监控和管理智能设备,智能化契约可以规范智能设备的行为,解决工业控制系统的网络安全问题。

2.2　块链结构

区块链中的第一个区块是比较特别的,称为“起源”,它是将区块链网络所有的用户端变成通用的。为了保证块之间的完整性,最重要的组成单元就是时间戳机构,这些“块”上都是带有 HASH 函数序列的时间戳。每个块都引用它前面一个块中的记录,这将在块之间建立链接,形成的整个结构就被称为区块链。

即使使用多个技术服务协议来提高可靠性和减少漏洞,作为一方的信任服务提供商也无法完全避免对信息的操纵。因此,使用这些时间戳意味着对发行机构的信任。任何能够访问这个有序的、后向链接的块列表的设备节点都可以读取它,并找出 ICS 网络上正在交换的数据的全部状态,这样就可以监测到 ICS 网络中的错误,并避免网络被攻击。

块链的组织如图 2 所示:区块是每个设备节点传输的数据集合,包括了交易过程中产生的相关信息和记录,这是形成块链的基本单位。为了确保块链的可追溯性,每个块都有一个时间戳作为唯一标记。该块由两部分组成:

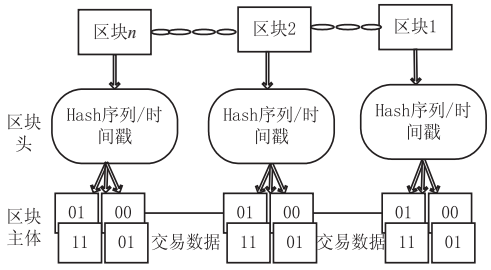

图 2　块链结构

块头,链接到前面块,并为块链提供完整性。其中包含上一个地址的哈希地址摘要、带有哈希序列的 merkle 树、区块创建时间戳;

块体,在每个终端中记录更新的数据信息,包括当前区块经过验证的、区块创建过程中生成的所有交易记录或者是其他信息,可以理解为一个分布式的账本,此账本中的数据可以长久保存和查询,保证了信息存在冗余备份。

3　基于区块链的 ICS 数据安全策略研究

区块链技术是一种在网络成员之间复制和共享的分布式数据账本,运行一致性算法,在不占用大量计算资源的情况下,保证 ICS 中设备交易数据的安全。更高的系统和需要建立一个较短的更新间隔技术系统。区块链技术是一种集成电路网络安全的方法,它包含了大量的数据处理、实时性要求等内容,再利用数据库技术更大的吞吐量、更快的数据通信技术、更高效的一致性机制来保证工控网络的安全性。

为了提高工业控制网络的安全性,在工控网络中的各级服务器、交换机、PLC 甚至底层设备都可以作为参与节点接入区块链网络。区块链网络本质上是一组非信任节点与其他没有信任节点的共享数据库交互,每个设备节点包含整个数据库事务信息,称为一个块和一个分类账,ICS 中的所有设备节点形成区块链和分布式分类账。为了帮助工控网络和区块链达成共识,各自区块链网络需要建立每个设备节点事务和工控网络连接,并且它们应遵循的某些规则。这些规则被编程到每个区块链的客户端节点上,然后使用它们来决定传入的事务是否有效,从而决定它是否应该被中继到网络中。

在工控网络的现场设备层[9-11],分析其数据来源,对采集后的数据进行数据审计,将其存在区块链中,流程如图 3 所示,分为三个部分。

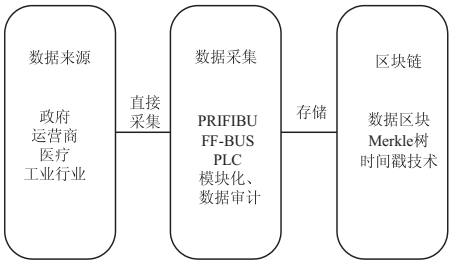

图 3　工控网络区块链步骤

(1)现场总线控制网络利用诸如 PRIFIBUS(过程现场总线)、FF-BUS(基金会现场总线)等现场总线技术将传感器、继电器等现场设备与一些 PLC 控制器或者 RTU 等现场控制设备相连。

(2)在各类系统设备接口上添加适配层,实时采集系统设备接口数据到区块链中,实现监控工业控制网络与区块链各类交易数据的实时状态。

(3)采集的数据经过数据审计,通过区块链中的哈希算法形成加密信息摘要,也就是带有哈希序列的一条条数据,最后被编写在 merkle 树中存储。区块链所具有的时间戳技术可以使得数据信息具有不可篡改、不可伪造和可追溯的重要特征。

当区块链技术应用于由现场总线连接的设备节点组成的 ICS 网络时,交易模式如图 4 所示:区块链链中的每个区块都包含了 Hash 序列加时间戳的组合密钥,构成的“块”链接到下一个区块中,这些“块”中还包含了 ICS 网络中设备之间的交易数据,多个“块”形成一个线性序列。由于“块”是通过哈希密码序列进行标识的,每个块还引用前一个块的信息,那么,通过区块链中的这些区块,就可以检查发送方和接收方的数据是否经过验证和篡改。用户在 ICS 网络中进行数据交易时,只需要在设备节点之间进行交易。因为每个设备节点都在执行智能合约并记录交易数据,而且区块链在 ICS 的设备节点之间自我复制,更加一步说明 ICS 网络中的任何设备节点都可以记录所有的事务数据。结果,ICS 网络上的设备节点附加到块链上,只有经过验证、相互同意的事务才会被写入区块链的底层存储,最终保证了数据交换的安全性。

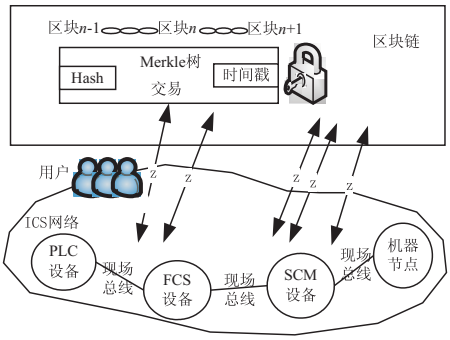

图 4 区块链交易模式

3.1 共识机制

区块链的核心组成部分,可以在没有中央权威或实体的情况下运行:共识机制[12]。为了理解共识机制的概念,首先看看区块链和传统系统之间的区别,如图 5 所示。

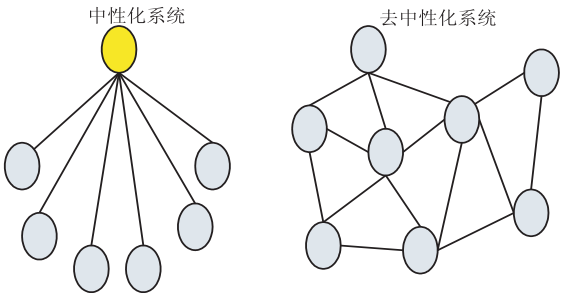

图 5 中心化系统 vs 去中心化系统

中心化系统:即集中式系统,在进行各项信息交流服务时需要一个“领导”(中心节点)来进行转达,只有“领导”才有权保护和更新数据库的权限。一切信息流由中心节点机构控制和管理,它决定了数据库中的数据类型。在网络中仅与授权中心相关联的其他节点(设备),才能对数据的一部分进行访问。

去中心化系统:区块链技术使用分散的网络体系结构。任何人都可以成为一个节点,每个节点都可以成为服务器。意味着在系统网络中传输数据后会有无数个节点来记录,不再是单一的权威集中式服务,每个节点在层次中都是平等的,将会获得更多的访问权限,自己的信息掌握在自己手中。

共识机制是指以去中心化的方式就网络的状态达成统一协议的过程。也被称为共识算法,有助于验证和已核实的信息添加到分布式账本中,保证其事务被存储在块链上。因此,共识机制负责安全地更新分布式网络中的数据状态。它一直是硬编码规则,以确保该协议总是能够找到全球计算机网络和协议数据的唯一来源。实现无需信任的网络,而无需中心数据或“领导”。

区块链的共识算法在工控网络中能够解决的问题有:

(1)在工控网络中做出决策,达成信息数据传输一致;

(2)确认每个人的数据库中只有一种方案确定数据的存储;

(3)能确保工控网络的交易真实可信,每个用户能够自我监控。

3.2 共识控制模型(consensus control model)

区块链是一个去中心化的时间戳服务器技术[13-15],可以自动创建分散的、为每个提交的文件提供防篡改和可公开验证的时间戳,将此技术加上共识机制与工控网络的监控/控制层结合,搭建一个如图 6 所示的模型,此模型称为共识控制模型(consensus control model)。

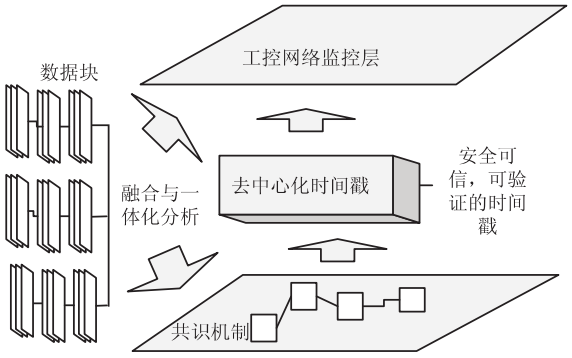

图 6 共识控制模型

首先,在工业资源平台服务器上搭建区块链平台,设置准入机制,配置不同的组织关系,并为各个组织配置相应的通道,完成底层基础网络的搭建。在搭建好的工控区块链网络的环境下将模型分为三层:

第一层将底层区块链中的数据分成片打包上传到服务器中;

第二层中共识机制负责安全地更新分布式网络中的数据状态;

第三层去中心化时间戳服务技术,为每次共识机制更新的数据状态提供可公开验证的时间戳;

最后,在控制层采用一定选择机制,诸如监控中心,对这些带有哈希序列的数据节点进行打包形成区块,同时利用大数据分析平台对工业资产进行评估,对评估良好的工业资源配给一定数量的通证奖励,在后续的交易中通常可以作为手续费附加在智能合约中被优先打包成区块,由此对工业生态的健康成长和运行进行一定程度的引导。区块链上的每个组织都会有记账节点来进行分布式记账,并维护全网的一个公共的账本;同时,对于工业资产数据的读写操作均会被记录到区块链中,以实现全方位的安全可信管控,以便随时监控来自底层的数据是否安全,确保信息层的管理员拿到的数据是最安全的。

在工控网络中的部分数据之前是由管理员或者企业总部管理和保存,用户无法便利获得自己的记录和历史数据。通过此模型的相关技术进行用户隐私数据保存,用户自己可以真正地掌握,而不是企业或管理员操控。这不仅有助于保护用户隐私,也增强了用户使用数据的自主性,实现了信息的共享性和工控网络的去中心化性。

4　仿真与验证

为了解区块链网络的运行方式以及共识控制模型,设计安全机制验证:在同一个区块链上操作一组客户端节点保存事务数据的副本;假设 ICS 中的设备节点可以看作是区块链网络节点,每个设备节点都在区块链网络上进行交易;利用区块链技术的分布式账本、共识机制,智能联系,非对称加密等特点应用于工业控制系统以解决网络安全问题。

4.1　实验模型与结果

使用 opnet14.5 版本的网络仿真软件对工业区块链网络进行仿真,并对仿真结果进行分析验证。

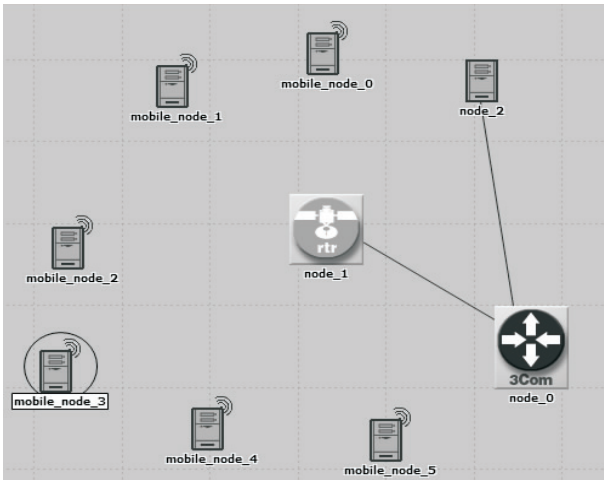

图 7　OPNET 分布式网络拓扑模型

由于工业区块链网络去中心化的分布式系统,则在全分布式非结构化拓扑结构中,每一个节点既可以作为客户机又可以作为服务器,还可以作为对等实体,在网络中也扮演着多重角色,其地位是完全平等的,并且它们与相邻的有相同的能力。因此可以建立如图 7 所示的网络模型。

图 8 中横坐标代表网络运行时间,纵坐标代表网络收敛延时时间。可以看出在工业区块链网络中进行数据传输 150 秒时的网络收敛的延时大约为 0.4 微秒,网络延时相对平稳,说明当工业控制系统和区块链技术结合时,可以防护数据被篡改,此时对网络的延时是最小的。

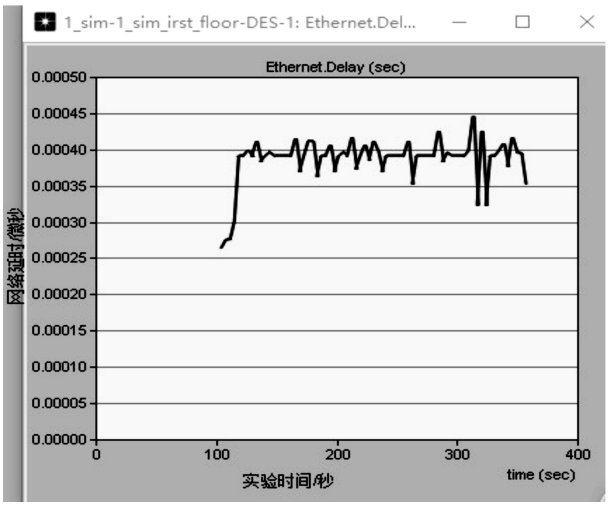

图 8　工业区块链网络的延时

图 9 中横坐标代表网络运行时间,纵坐标代表网络的吞吐量。可以看出在工业区块链网络中进行数据传输 400 秒时的网络吞吐量状态,从 20 秒时陡增,到 55 秒时吞吐量都趋于稳定,在 42 秒时网络吞吐量达到峰值 183 Mbps。以周期的形式达到峰值进而趋于稳定,说明在工业区块链网络中数据不易发生丢失或者出现其他网络问题。

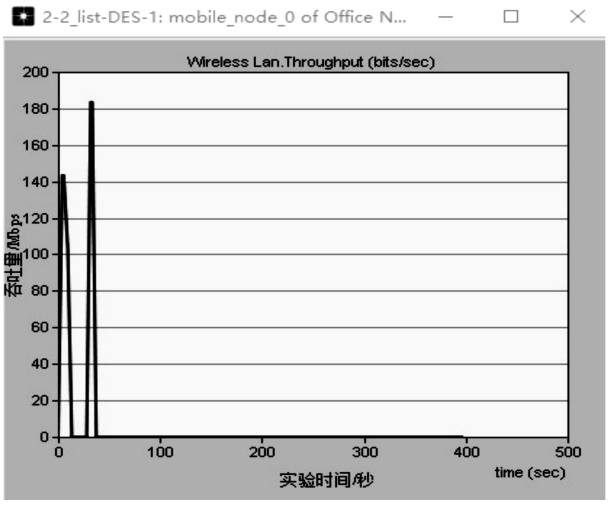

图 9　工业区块链网络的吞吐量

4.2 验证过程

(1)通过 ICS 区块链网络模块,让设备节点相互交换并相互传输数据,并让区块链存储。

(2)机器设备节点形成对等网络[16],其中一个机器设备节点与区块链上的另一个机器设备节点交互,节点之间通过一对私钥或公钥进行通信。它们使用自己的私钥签署自己的交易,并且可以通过它们的公钥在网络上寻址。非对称加密的使用将身份验证、完整性和不可否认性带入网络。每个签名的事务都由用户的节点广播到其相邻的对等节点。相邻的对等方在进一步传输之前确保该事务有效,无效和错误的事务被丢弃并拒绝,最终有效事务在整个 ICS 设备区块链网络中传播。

(3)使用加密算法和区块链节点哈希值的方式记录机器设备的使用时间,检查区块的有效事务,验证区块链网络收集的机器设备事务数据和按时间戳排序的区块链节点事务数据,然后将正确的事务数据块链接到它们的子链中,如果设备之间有一个新的事务,它们会将这个新事务块添加到区块链中,并用它包含的新事务来更新其分类账。

(4)重复上面步骤,若验证的结果是所需要的正确数据时,步骤结束。

在隐含的共享数据库模型中,区块数据库的每一行都映射到与 ICS 设备节点对应的公钥或地址中,有效事务则是试图修改具有相应签名的行的事务数据。当网络中的每个节点遵循上述步骤时,其操作的共享区块链[17]将成为网络活动中的身份验证和时间戳记录。节点不必信任任何其他实体,由此产生了无信任环境这一术语,信任是由系统中不同参与者的交互作用而产生的一种紧急属性。

5 结束语

即使在工控网络数据安全上结合区块链技术有些重要的保留意见,但不应该低估这些非凡技术变革带来的有希望的社会经济效益。该文利用区块链技术的优点建立的共识控制模型,设计的工控区块链网络使工业控制网络的数据信息不被篡改,这种创新策略通过仿真结果得出能够高效率保证上层用户获得的数据的真实性、完整性。区块链和分散式分类账是一项基础和破坏性技术,将彻底改变工业控制系统的网络安全,使工业程序运算由程序-数据-验算-生产-回馈流程大力简化。但是,进一步在探究过程中发现工控网络中的攻击具有多样性,而最终基本的区块链问题归结到信任问题。后续将会研究区块链的安全、区块链能够解决工控网络攻击的类型、区块链用于资产的转移和跟踪等多个方面。

参考文献:

[1] 徐元清,卓 蔚. 区块链技术在烟草系统工控安全中的应用[J]. 微型电脑应用,2019,35(3):112-115.

[2] 林 枫. 工业控制系统网络安全防护体系的思考[J]. 信息通信,2017(5):123-124.

[3] 赵 阔,邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息网络安全,2017(5):1-6.

[4] 冯泽冰,方 琳. 区块链技术增强物联网安全应用前景分析[J]. 电信网技术,2018(2):1-5.

[5] BAHGA A,MADISETTI V K. Blockchain plat form for industrial internet of things[J]. Journal of Software Engineering and Applications,2016,9(10):533-546.

[6] 柏 亮. 区块链技术在工业物联网的应用研究[J]. 网络空间安全,2018,9(9):87-91.

[7] NAKAMOTO S. Bitcoin:a peer-to-peer electronic cash system[EB/OL]. 2008. http://www. bitcoin. org/bitcoin. pdf.

[8] WOOD G. Ethereum:a secure decentralised generalised transactionledger[EB/OL]. 2014. http://gavwood. com/Paper. pdf.

[9] 王禹贺. 工业控制网络安全评估方法研究[D]. 哈尔滨:哈尔滨理工大学,2019.

[10] 杨国泰. 工业控制系统安全网络防护分析[J]. 电子世界,2019(16):70-71.

[11] 孙柏林,刘哲鸣. 区块链技术在仪器仪表工业 4.0 中的应用[J]. 仪器仪表用户,2018,25(9):101-104.

[12] 趋势传媒. 共识算法指南:什么是共识机制?[EB/OL]. 2018-10-10. http://www. sohu. com/. 2018-10-10.

[13] HEPP T,WORTNER P,SCHÖNHALS A,et al. Securing physical assets on the blockchain:linking a novel object identification concept with distributed ledgers[C]//Proceedings of the 1st workshop on cryptocurrencies and blockchains for distributed systems. New York:ACM,2018:60-65.

[14] ESPOSITO C,DE SANTIS A,TORTORA G,et al. Blockchain:a panacea for healthcare cloud-based data security and privacy?[J]. IEEE Cloud Computing,2018,5(1):31-37.

[15] GIPP B,BREITINGER C,MEUSCHKE N,et al. Cryptsubmit:introducing securely timestamped manuscript submission and peer review feedback using the blockchain[C]//Proceedings of the 17th ACM/IEEE joint conference on digital libraries. Toronto:IEEE,2017:273-276.

[16] ZHI L,VATANKHAH B A,HUANG G Q. Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform[J]. Robotics and Computer-Integrated Manufacturing,2018,54:133-144.

[17] HUCKLE S,BHATTACHARYA R,WHITE M,et al. Internet of things,blockchain and shared economy applications[J]. Procedia Computer Science,2016,98:461-466.