基于区块链的云制造信息数据记录技术

董 蓉,苑明海,周 灼
(河海大学 机电工程学院,江苏 常州 213000)

摘 要:为了增强云制造服务交易信息记录的安全性,优化资源配置,提高资源共享率,提出了区块链技术与云制造平台相结合的方法,将区块链技术与云平台中资源提供者和需求者紧密联系。利用区块链技术对云平台中的交易进行记录、存储及共享,提出了交易区块链体系结构,分析了交易区块链基础架构模型,提出了记账节点的基本组成,设计了云制造服务平台中信息数据记录的方法与过程,并将信息记录与共享方法应用在企业的设备资源中。建立了制造资源属性信息模型,分为公有域和私有域两部分,对公有域部分进行合理共享,私有域部分进行私密保护。应用结果证明,区块链技术与云服务平台的结合,可提高资源的共享率和利用率,保证了云服务平台中信息的安全性与可靠性。

关键词:区块链;云制造;记录存储;架构模型
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2019)05-0097-05
doi:10.3969/j.issn.1673-629X.2019.05.021

Cloud Manufacturing Service Transaction Information Recording Technology Based on Block Chain

DONG Rong, YUAN Ming-hai, ZHOU Zhuo
(School of Mechanical and Electronic Engineering, Hohai University, Changzhou 213000, China)

Abstract: In order to enhance the security of cloud manufacturing service transaction information record and optimize resource allocation and increase resource sharing rate, we put forward the combination of block chain technology and cloud manufacturing platform and link block chain technology to resource providers and demanders. Using block chain technology to record, store and share transactions in cloud platform, we propose the architecture of transaction block chain, analyze the infrastructure model of transaction block chain, present the basic composition of the accounting node, and design the method and process of information data recording in cloud manufacturing service platform. At the same time the sharing methods are applied to enterprise equipment resources. The attribute information model of manufacturing resources is established, which is divided into two parts: public domain and private domain. The part of the public domain is shared reasonably, and the private domain part is privately-protected. The application results show that the combination of block chain technology and cloud service platform can improve the sharing rate and utilization ratio of resources and ensure the security and reliability of information in cloud service platform.

Key words: block chain; cloud manufacturing; record storage; architecture model

0 引 言

随着信息技术的飞速发展,云制造平台的应用日益广泛。在云制造服务平台中,数据信息的记录和存储十分重要,信息的共享和信息的隐私保护对于云制造服务具有重要意义。

现阶段云制造平台中的数据记录主要依靠中心化的网络。曹佳硕[1]对资源描述框架数据的存储方法进行研究,提出了基于 Hbase 的存储方案,对资源描述框架查询语言进行研究,提出了语义扩展的查询方法,实现了基于语义与基于关键字相结合的查询;赵淳等[2]针对云制造环境中的企业交易过程,设计并实现了一个仿真平台,该平台采用服务智能体对企业行为进行描述,通过定义不同规则实现了不同交易模式的仿真。以上研究均对云平台中交易的记录与存储起到了极大的推动作用。

然而在上述研究中,云服务平台主要依赖于传统的中心化网络记录和存储信息,这使得数据信息的保护存在部分潜在漏洞,若网络中心遭到威胁,平台中的

收稿日期:2018-06-19 **修回日期**:2018-10-11 **网络出版时间**:2018-12-21
基金项目:教育部人文社科规划基金项目(17YJA630127)
作者简介:董 蓉(1992-),女,硕士,研究方向为先进制造系统;苑明海,博士,副教授,研究方向为先进制造系统建模及优化设计。

所有数据信息将面临被篡改或者丢失的风险。并且传统的数据中心控制全网,使得信息资源难以达到高度共享,存在资源浪费、效率低下等问题。

针对上述问题,文中提出一种基于区块链的云制造服务数据记录与存储方法。首先,利用区块链技术的去中心化、不可篡改性、透明化和匿名性等特点[3-6],将区块链技术与云平台相结合,提出了交易区块链体系结构,为区块链技术在云制造平台中的应用奠定基础。然后,提出了云制造平台中数据记录的方法,并将该方法应用于设备资源信息记录中,以提高数据记录的安全性。

1 云制造服务平台中交易信息数据的记录与存储方法

利用区块链技术和云服务平台实现云制造服务交易信息的记录与存储,提出了交易区块链,具体如图 1 所示。

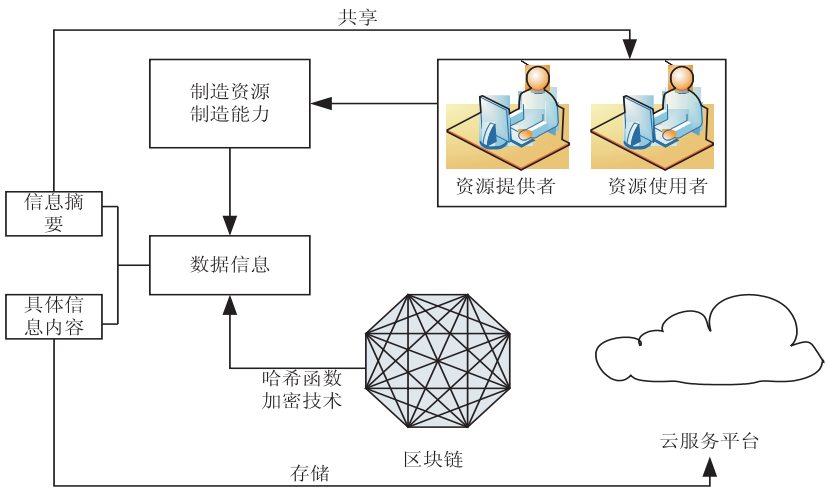

图 1 交易区块链体系结构

在交易区块链中主要有资源提供者和资源使用者两大主体,资源提供者可以是不同的企业或个人,负责给相应的使用者提供制造资源及能力,当交易完成时,双方均可记录此交易。区块链中的信息记录均是公开的,但私有的信息可进行加密保护,即可以通过相关技术进行隐藏,只有拥有其对应的密码,才可访问到该记录。在交易区块链的公共账本中,只出现相应的交易记录概要,以及为实现价值流通的基本功能,并且由于区块链的存储空间有限,详细的交易记录都存储在云服务平台中。

图 2 为交易区块链各层的具体设计。

交易区块链的数据层存储着各资源信息交易摘要及其详细数据在云服务平台中的存储位置,哈希函数保证了数据的不可篡改性,时间戳保证了数据的可追溯性。在数据存储中,资源信息的数据 D、元数据 data 等记入到区块链里,如 $\{D;data;Sig(D;data)\}$。资源提供者对自身资源信息数据的使用具有决定权,在访问控制交易中,资源提供者将主体对资源信息的权限写入区块链,主体用资源使用者的公钥 pku 表示,用访问对象公钥 pku 对资源信息数据解密密钥 key 加密,再加上签名。

网络层的作用是保证各个节点之间的相互通信,是一个 P2P 网络,在网络中每一个节点都是同等的,都具有生成数据和接收数据的能力。

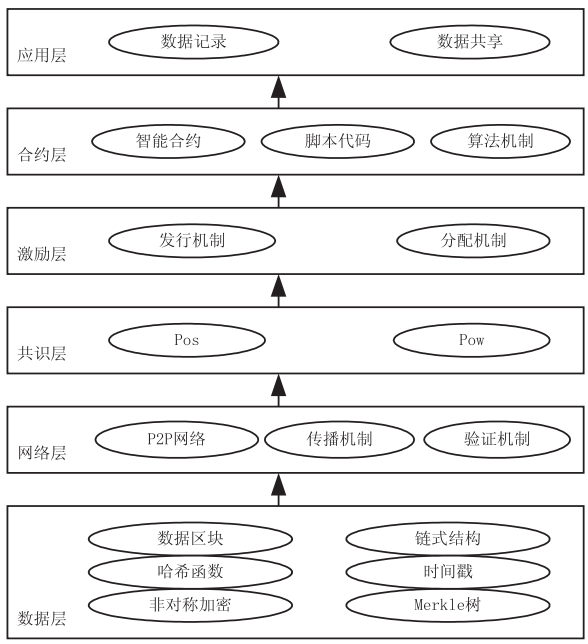

图 2 交易区块链基础架构模型

共识层主要通过一种共识机制,使得网络中的所有节点在平等的去中心化的情况下可以达成一致共识。

在激励层中,由一定的激励机制促进节点参与区块链的交易验证,区块链中许多节点共同工作参与保证了区块链中的安全。文中定义的交易区块链不是加密货币,因此原本区块链中由挖矿产生的货币机制不

适用,不能依赖原本的机制维护公共账本安全有效。在此交易链中,使用法币以代币的形式进行流通,进行支付交易,每次交易会产生相应交易费,在挖矿比赛中获胜方所得,作为挖矿奖励,在每个时间周期中都会产生新的区块。

合约层主要是对区块链中所有的脚本代码及算法进行封装。

应用层中主要包括制造资源及能力等信息在云平台中的保存记录及共享。交易信息的记录过程为:首先网络中某一个记账节点完成一个交易过程后形成一个交易记录并存储,生成一条交易信息摘要;接着,对该交易信息摘要进行私钥加密,并在全网公布,所有节点均可接收到加密后的交易信息摘要;在当前周期里,整个网络中新公开的交易信息摘要由具有记账权限的节点记录下来,并在网络中公开该记账节点,由此形成一个新的交易区块;再将新的交易区块与时间戳一起加入到原本的交易区块链,形成新的交易区块链,并在全网公布;最后,通过 P2P 技术,各记账节点将全网中所有新形成的交易区块链同步到自身节点中。

在云制造服务交易记录过程中,包括多个记账节点,每一个记账节点都具有独立记账能力。各记账节点中又包括交易信息数据存储库、交易区块链数据存储库、竞争记账权限模块、生成信息摘要模块、生成交易区块链模块和更新模块,如图 3 所示。

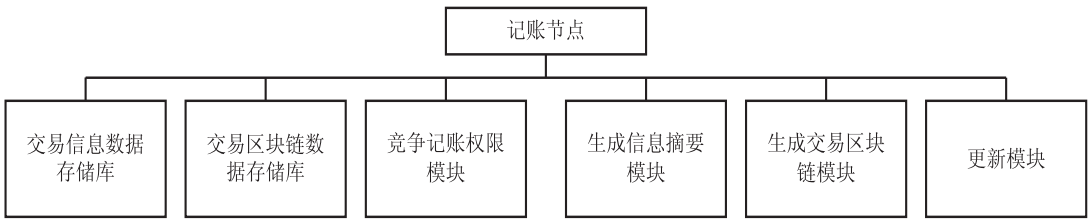

图 3　记账节点的基本组成

交易信息数据存储库主要用于存储记录自身的交易信息;交易区块链数据存储库用于存储交易区块链;竞争记账权限模块是通过竞争机制争夺记账权限;生成信息摘要模块主要包括交易完成后记录到记账信息数据库,根据交易记录形成交易信息摘要,对摘要进行加密后,在全网进行公布,全网中的其他节点均能接收到该交易信息摘要;生成交易区块链模块中包含当具有记账权限的节点记录所有新公开的交易信息摘要,形成一个新的区块,再将新的区块加上时间戳加入到自身原本的交易区块链,形成一个新的交易区块链并在全网公布;更新模块是通过 P2P 技术,将全网中新公开的所有新的交易区块链更新到自身节点中。

当云制造服务平台中某一企业完成一项交易后,需进行记录。信息交易的过程形成一个交易记录,记录中包含对象、名称、实际、数量及金额等内容。由区块链中的技术方法,即采用哈希方法形成交易记录摘要,再通过节点处的私钥进行加密,加密后在全网公开。网络中具有记账功能的节点通过竞争机制(PoW 或 PoS)获得记账权限,再将全网中所有没有记录过的新的交易信息摘要组合成一个新区块,加上时间戳,把新区块再加入到原来的交易区块链中,形成一个新的交易区块链。形成新的交易区块链之后,其他没有记账权限的节点将新形成的交易区块链更新到自身的数据库中。

2　某企业设备资源中的应用

为了更好地支持云制造资源的接入,实现制造资源的优化配置,以设备资源为例,将资源的属性信息分为四类,即基本信息、功能信息、评价信息和状态信息[7-11]。形式化描述为:

CMRI = {CMRBasI, CMRFunI, CMREvaI, CMRStaI}

其中,CMRI 表示云制造资源属性信息;CMRBasI 表示制造资源的基本信息;CMRFunI 表示制造资源的功能信息;CMREvaI 表示制造资源的评价信息;CMRStaI 表示制造资源的状态信息。

(1)基本信息。

基本信息是资源最基本的身份信息,包括设备信息即资源的编号、名称、型号及功率等,还包括企业信息即制造厂商以及购买日期及价格等。

(2)功能信息。

功能信息主要包括零件信息和能力信息,零件信息主要包括零件的类别、材料、尺寸、重量及生产类型,能力信息包括加工类型、精度、方法、尺寸及几何特征。

(3)评价信息。

评价信息主要包括质量合格率、故障率、操作人员等级、质量保证体系、质量管理水平、企业资源种类、同类资源数量等。

(4)状态信息。

状态信息主要包括闲置、使用中或维修中以及超负荷、满负荷或未满负荷。

根据上述属性模型划分,为了对公共信息进行合理的分享以及对私密信息进行保护,提出公有域和私有域,引入区块链技术,数据加密技术对信息进行匿名

保护,分布式网络使信息实现高效共享。公有域中的信息包含可以体现企业制造能力的一些信息但不包含核心技术,私有域中包含企业的机密核心信息。由此,建立制造资源的属性信息模型,如图 4 所示,基本信息和功能信息中的能力信息属于私有域,状态信息、评价信息和功能信息中的零件信息属于公有域[12-14]。

如上述企业作为资源提供者,首先将资源的属性信息进行分类,再按照区块链中的形式将属性信息分为公有域信息和私有域信息,将自己所具备的设备资源属性信息进行编排,形成一系列的资源属性信息数据(A)。信息数据生成后,资源提供者为资源信息数据生成哈希值,并将信息摘要(Summary)及其私钥(self key)签名后发布。网络中具有记账功能的节点通过竞争机制获得记账权限,再将全网中所有没有记录过的新的交易信息摘要组合成一个新区块,加上时间戳,把新区块再加入到原来的交易区块链中,形成一个新的交易区块链。公有域中的属性信息可直接发布,私有域中的资源信息用密钥(key)加密,以及将加密密钥用资源提供者的公钥(public key)加密后再发送给资源提供者,算法 1 如下:

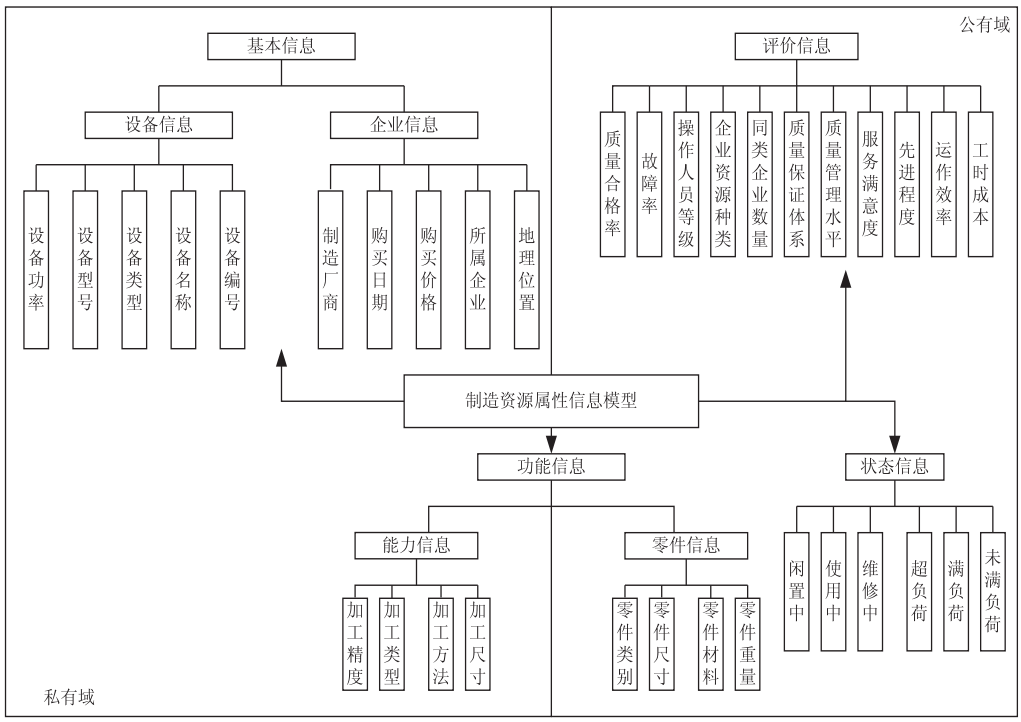

图 4 制造资源属性信息模型

算法 1:制造资源信息的发布。

Procedure Issuing(A)

Input:A

Output:制造资源属性信息

Begin

资源提供者产生资源属性信息 A;

生成数据 {Summary;H(A);Sig(Summary | H(A))} 并创建数据存储发布在全网;

将制造资源属性信息和经过哈希值签名后用密钥加密,将加密密钥用资源提供者的公钥加密,形成消息 $\{Enc_{key}(Summary | A | H(A) | Sig(Summary | A | H(A)));Enc(key)\}$ 后一起发送给资源提供者;

End

制造资源属性信息共享,该企业作为资源提供者可决定自身资源及能力的使用权限,通过访问控制交易授权资源使用者访问其制造资源信息数据。公有域中的信息在全网公开,不作权限设置,私有域中的信息需拥有解密密钥才能访问。授权时,将共享在云服务平台中的存储位置记录,以及资源属性信息的使用期限和权限通过资源使用者的公钥的解密密钥同时记入到区块链中,具体算法如下。

算法 2:制造资源属性信息共享。

Procedure Sharing(A)

Input:资源使用者的公钥和所需的资源属性信息

Output:生成一个访问控制交易

Begin

接收资源使用者请求,提取出资源使用者的公钥和资源属性信息需求;

根据资源使用者的资源属性信息请求,查找相关资源属性信息数据的存储位置 LCT 和其加密密钥 key;

创建访问控制交易,并写入交易

{LCT;permission;pku;expiration;Sig(LCT;permission;pku);Epko(key)} 向全网广播;

End

由上述方法,将企业的设备资源信息发布到云制造平台中,部分信息对全网公开,但部分私密信息并不

公开,这时需要提供对应的加密密钥才能看到私密信息具体内容,保证了信息数据的安全性,保护了资源提供者的隐私。在去中心化的特征下,保证了制造资源信息共享的同时,也保证了在某一节点可能存在数据丢失的情况下,对全网影响几乎微乎其微,使得云制造服务平台中的数据安全得到了保证。

3　结束语

提出一种基于区块链的云制造服务数据记录与存储方法。首先,将区块链技术与云平台相结合,提出交易区块链体系结构,对交易区块链中的数据层、网络层、共识层、激励层、合约层及应用层进行了分析。然后,对应用层中数据记录及存储进行研究,提出了云制造平台中数据记录的方法,并将该方法应用于设备资源信息记录中。结果表明,该方法明显增强了数据记录的安全性,提高了云制造平台中的资源共享效率。

参考文献:

[1] 曹佳硕. 基于 RDF 的云制造资源数据存储及检索方法的研究与实现[D]. 北京:北京交通大学,2013.

[2] 赵　淳,张　霖,任　磊,等. 面向云制造交易过程的仿真平台[J]. 计算机集成制造系统,2016,22(1):25-32.

[3] 林小驰,胡叶倩雯. 关于区块链技术的研究综述[J]. 金融市场研究,2016,45:97-109.

[4] 沈　鑫,裴庆祺,刘雪峰. 区块链技术综述[J]. 网络与信息安全学报,2016,2(11):11-20.

[5] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart con-tracts for the Internet of Things[J]. IEEE Access, 2016,4:2292-2303.

[6] SWAN M. Block chain thinking:the brain as a decentralized autonomous corporation[J]. IEEE Technology and Society Magazine,2015,34(4):41-52.

[7] 李伯虎. 云制造[M]. 北京:清华大学出版社,2015.

[8] 陈友玲,刘传彪,阳玮琦,等. 云制造环境下能力资源需求的评价与选择[J]. 计算机集成制造系统,2017,23(10):2304-2312.

[9] 黄　辉,王　哲,纪玉娇,等. 分布式网络化云制造模式分析[J]. 现代制造工程,2017(11):36-43.

[10] 朱李楠,王万良,沈国江. 基于改进差分进化算法的云制造资源优化组合方法[J]. 计算机集成制造系统,2017,23(1):203-214.

[11] 张　霖,罗永亮,范文慧,等. 云制造及相关先进制造模式分析[J]. 计算机集成制造系统,2011,17(3):458-468.

[12] XU Xun. From cloud computing to cloud manufacturing[J]. Robotics and Computer-Integrated Manufacturing,2012,28(1):75-86.

[13] 常瑞云,周井泉,许　斌,等. 基于离散人工群算法的云制造服务组合[J]. 计算机技术与发展,2016,26(7):177-182.

[14] 齐　轩,刘茜萍. 基于用户偏好的可信 QoS 服务选择方法[J]. 计算机技术与发展,2016,26(8):43-47.

(上接第 76 页)

[3] LIU Tianhua, YIN Shoulin. An improved particle swarm optimization algorithm used for BP neural network and multimedia course-ware evaluation[J]. Multimedia Tools and Applications,2017,76(9):11961-11974.

[4] SUN Aixi, JIN Xue, CHANG Yubo. Research on the process optimization model of micro-clearance electrolysis-assisted laser machining based on BP neural network and ant colony[J]. International Journal of Advanced Manufacturing Technology,2017,88(9-12):3485-3498.

[5] PENG J S. Multi-objective optimization of vibration characteristics of steering systems based on GA-BP neural networks[J]. Journal of Vibroengineering,2017,19(5):3216-3229.

[6] YANG Xinshe, KARAMANOGLU M, HE Xingshi. Flower pollination algorithm:a novel approach for multiobjective optimization[J]. Engineering Optimization,2013,46(9):1222-1237.

[7] 邓文杰. 基于聚粒子群算法的神经网络权值优化方法[J]. 计算机技术与发展,2017,27(10):16-18.

[8] 张　志,杨清海. 基于 BP 神经网络和改进 D-S 证据理论的目标识别方法[J]. 计算机应用与软件,2018,35(3):151-156.

[9] 付晓明,王福林,尚家杰. 基于多子代遗传算法优化 BP 神经网络[J]. 计算机仿真,2016,33(3):258-263.

[10] 沈夏炯,王　龙,韩道军. 人工蜂群优化的 BP 神经网络在入侵检测中的应用[J]. 计算机工程,2016,42(2):190-194.

[11] 吴文铁,宋日聪,李　敏. 蚁群优化神经网络的网络流量混沌预测[J]. 计算机工程与应用,2012,48(34):97-101.

[12] 严　旭,李思源,张　征. 基于遗传算法的 BP 神经网络在城市用水量预测中的应用[J]. 计算机科学,2016,43:547-550.

[13] 高　隽. 人工神经网络原理及仿真实例[M]. 北京:机械工业出版社,2007.

[14] 周志华,曹存根. 神经网络及其应用[M]. 北京:清华大学出版社,2004.