

区块链技术综述：在下一代智能制造中的应用

林知微 张嵩川 王成吉 周亦炜

A survey on application of block chain in next generation intelligent manufacturing

LIN Zhiwei, ZHANG Songchuan, WANG Chengji, ZHOU Yiwei

引用本文：

林知微, 张嵩川, 王成吉, 等. 区块链技术综述：在下一代智能制造中的应用[J]. 智能科学与技术学报, 2023, 5(2): 200-211.

Zhiwei LIN, Songchuan ZHANG, Chengji WANG, et al. A survey on application of block chain in next generation intelligent manufacturing[J]. Chinese Journal of Intelligent Science and Technology, 2023, 5(2): 200-211.

您可能感兴趣的其他文章

面向元宇宙的数字公民身份认证方案

A metaverse-oriented digital citizen authentication scheme

智能科学与技术学报. 2022. 4(3): 396-409

知识驱动的冶金企业原料供应链订单分配方法

Knowledge-driven order allocation method for raw material supply chain in metallurgical enterprises

智能科学与技术学报. 2022. 4(3): 355-370

基于联邦学习的分布式农业组织

Distributed agricultural organization based on federated learning

智能科学与技术学报. 2022. 4(2): 288-297

智能优化算法在供应链网络中的应用

Application of intelligent optimization algorithms in supply chain network

智能科学与技术学报. 2022. 4(2): 174-183

加密管理：一种基于区块链的新型组织管理模式

Crypto management: a novel organizational management model based on blockchain

智能科学与技术学报. 2022. 4(2): 145-156

NFT：基于区块链的非同质化通证及其应用

NFT: blockchain-based non-fungible token and applicationss

智能科学与技术学报. 2021. 3(2): 234-242

区块链技术综述：在下一代智能制造中的应用

林知微^{1,2}, 张嵩川¹, 王成吉¹, 周亦炜¹

(1. 北京理工大学自动化学院, 北京 100081;

2. 复杂系统智能控制与决策国家重点实验室, 北京 100081)

摘要: 在我国制造业企业推进数字化转型的进程中, 区块链技术引起了研究人员的广泛关注。总结了区块链技术国内外整体研究进展, 给出了区块链技术在食品、军工产品供应链追踪和质量管理以及云制造等智能制造领域的应用案例。就区块链的存储问题、可扩展性问题、算力消耗问题和安全隐私问题提出了区块链与智能制造融合应用的建议, 以期为后续的研究者提供有价值的研究思路。

关键词: 智能制造; 区块链; 供应链; 共识机制

中图分类号: TP393

文献标志码: A

doi: 10.11959/j.issn.2096-6652.202248

A survey on application of block chain in next generation intelligent manufacturing

LIN Zhiwei^{1,2}, ZHANG Songchuan¹, WANG Chengji¹, ZHOU Yiwei¹

1. School of Automation, Beijing Institute of Technology, Beijing 100081, China

2. Key Laboratory of Complex System Intelligent Control and Decision, Beijing 100081, China

Abstract: In the process of promoting digital transformation of Chinese manufacturing enterprises, block chain technology has attracted extensive attention of researchers. The overall research progress domestically and abroad in the field of block chain technology was concluded. The recent researches on block chain technology in manufacturing process of food and military products, cloud manufacturing and other fields were summarized. The future path of combining block chain technology with intelligent manufacturing was predicted from 4 aspects: storage problem, scalability problem, computational power waste problem, security and privacy problem, aiming to provide valuable research ideas for further researchers.

Key words: intelligent manufacturing, block chain, supply chain, consensus mechanism

0 引言

数字经济时代巨大的计算量带来的能源消耗问题始终是各界关注的问题之一。根据我国碳排放产业的分布情况, 碳排放大部分来自发电和工业端, 实现碳中和的路径可以拆分为两个部分: 可避免的排放和不可避免的排放。在我国制造业企业推进数字化转型的进程中, 智能制造相关产业需要兼顾效率、便捷、绿色节能等方面。

智能制造发展初期, 智能化主要体现在生产过程中的各种设备通过物联网等技术互通, 工业大数据仅在单一生产场景内部流转。随着互联网技术的发展, 智能制造逐步迈入新时代。下一代智能制造是以产品的整个生命周期为对象, 通过现代传感器、互联网、大数据、人工智能等手段实现的信息化生产制造过程。产品的生命周期包含原材料获取、生产流程、物流运输、市场营销以及售后服务等。

收稿日期: 2022-08-01; 修回日期: 2022-08-26

通信作者: 林知微, linzhiwei@bit.edu.cn

智能制造的发展过程中产生了大量需要在产业链中不同企业或个人之间流转和处理的数据，而中心化存储、简单的网络通信等传统处理方法难以确保数据快速、有效、安全地传输。为了解决上述问题，将区块链技术引入智能制造是有效的技术路径。区块链是一种具有去中心化、公开性、安全性、匿名性、不可修改等特性的分布式数据账本^[1]，近年来逐渐受到研究人员的关注。

区块链具有快速匿名交易、不可修改等优势，能够解决制造业中信息不对等、资源难以共享、交易费用高等问题。使用区块链技术搭建可信化平台，可以打通产业链上下游信息壁垒；使用区块链技术实现供应链追踪，能够提高信息的安全性和公开性；区块链技术的应用能够确保工业大数据快速安全地流转。

1 区块链研究背景及技术介绍

1.1 区块链研究历史

区块链技术起源于2008年Nakamoto S^[2]发表的《比特币：一种点对点的电子现金系统》(Bitcoin: a peer-to-peer electronic cash system)，文中提出了一种完全不依赖中心机构的点对点的电子现金系统。这种现金系统基于密码学而不是第三方信用中介，所以其不需要中转即可实现点对点支付。文中提出了区块链早期的共识机制——工作量证明(proof of work, PoW)。除非重新完成想要修改的区块及其之后所有区块的工作量证明，否则记录将不可修改。这种共识机制的问题在于如果要对区块链进行延长，需要投入大量的算力。这一时期被称为区块链1.0时代。

2014年，Vitalik B^[3]提出的以太坊概念标志着区块链技术正式进入区块链2.0时代，其突出特点是加入了智能合约。智能合约是一套以数字形式定义的承诺，合约参与方可以在区块链上执行这些承诺的协议，该概念最早出现于1995年，但当时的技术手段难以保障智能合约的安全性^[4]。区块链技术的发展解决了这一问题，并使其成为以太坊的核心。智能合约能减少合约以外的其他成本，使以太坊能够推广到更多金融领域。

此后区块链技术开始逐渐应用于物联网、农业生产、智能制造、医疗保健等领域。这也标志着区块链技术逐渐进入区块链3.0时代^[5]。区块链技术能够在金融以外的其他领域应用的一个关键节点是Hyperledger项目^[6]。Hyperledger Fabric是开源的企

业级许可制分布式账本技术平台，该平台具有高度可定制性，为企业级开发提供便利^[7]。Hyperledger Fabric采用许可制，与完全公开的区块链不同，网络的参与者已经对对方有了一定的了解，在牺牲一定去中心化特性的同时，增加了对有争议的网络协议或框架修改的可能性。

目前，区块链技术仍处于区块链3.0时代，区块链技术正在快速融入社会的各个领域。

1.2 区块链研究意义

区块链在金融领域已经取得了瞩目的研究成果。近来提出了Web3.0概念，Web3.0的突出特点是去中心化，将互联网由原本的平台管理变为用户管理，所产生的利益也由用户享有，通过固定的协议进行利益分配。以区块链为基础的网络金融迅速崛起，并以此为核心向诸多传统行业领域辐射^[8]。但是由于区块链本身的发展还未完全成熟，区块链技术的应用仍存在一些亟待解决的问题。

(1) 存储问题。区块链需要每个节点保存完整的链条以验证交易的合法性，而区块链会在交易中不断延长，所占用的存储空间也会不断增大^[9]。区块链的响应速度和可扩展性难以满足智能制造供应链的需求。

(2) 安全问题。区块链具备比传统网络更高的安全性，但这并不代表区块链不会被攻击，相反，区块链一直存在隐私保护的问题。区块链具有公开性，每个节点都保存整个链条，这导致了现有的加密方式仍难以做到完全按权限限制信息访问。

(3) 部署问题。区块链在金融领域的部署已经趋于完善，但是区块链在其他领域的应用仍处于探索阶段。区块链在广义制造业中的作用基本停留在供应链管理层面而没有真正融入生产过程，其作用没有得到充分发挥。

(4) 能源问题。区块链的延长往往需要大量的计算。目前，算力消耗过大带来的算力浪费和能源消耗将直接影响传统制造业的数字化转型。区块链技术的算力消耗与其采用的共识机制有关，这将在后面的内容中进行说明。

1.3 区块链技术介绍

成熟的区块链算法一般包括控制区块链延长规则的共识机制和实现所需功能的智能合约。目前主流的区块链平台有以太坊区块链、EOS区块链、Hyperledger区块链、Gochain区块链等，其中以以太坊区块链更为常见。

区块链并不都是完全去中心化的，其基本构成

逻辑与其参与成员的权限有关。在确定区块链的构成逻辑后,依据共识机制将所需数据打包形成的第一个区块称为创世区块,之后的区块都要以这个区块为首进行添加。区块的添加规则及准入规则都是共识机制的一部分。在构建好区块链之后,可以将需要实现的功能通过智能合约写入区块链。最后,在所有互联网技术投入实际应用之前,都需要对其安全性进行验证,这也是保障上述功能实现的关键因素。

1.3.1 权限划分

按照成员加入区块链的权限,可以将区块链分为公有链和许可链^[10]。

公有链的特点是所有人都有访问区块链的权限,且能随时获取整条区块链的所有信息或进行去中心化的交易,因此公有链也被认为是完全去中心化的区块链^[11]。

许可链的特点是参加到区块链中的所有节点都是受到许可的,只有受许可的节点才能参与网络^[12]。在需要对内部信息进行保密的场景一般使用许可链。许可链并非完全去中心化,而是弱中心或多中心。许可链又可分为私有链和联盟链,二者区别为是否需要在网络建立之前确定节点的个数及身份。私有链并不允许所有人访问区块链,而是只允许区块链所有者或维护群体许可的节点加入^[13]。联盟链是由若干个组织或机构共同参与管理和维护的区块链,每个参与的机构掌握一个或多个节点,并且在区块链开始运行时,成员的数量和身份就已经确定^[14]。

1.3.2 共识机制

区块链的技术基础是一系列不需要第三方组织参与的共识机制算法。共识机制是指所有参与者全部认同并遵守的规则。在区块链上达成共识不需要第三方组织担保,而是以工作量或互相信任为前提^[15-16]。

目前区块链中使用的共识机制主要分为两种:基于工作量的共识机制和基于信任的共识机制。工作量证明、委托权益证明(delegated proof of stake, DPoS)等都属于基于工作量的共识机制。基于信任的区块链在牺牲一定的去中心化特性的前提下,大幅度降低了增加区块的难度。

(1) 基于工作量的共识机制

目前使用的基于工作量的共识机制均为PoW及其改进方案。PoW是所有共识机制中消耗算力和资源最多的共识机制^[2]。PoW机制中最重要的部

分是哈希运算,以SHA256算法为例,无论输入何种数据,最后都会返回大小为256 bit的哈希值。PoW机制主要用于公有链的搭建。

在这一共识机制下,区块链系统会给出一个目标哈希值,用户将想要记录的内容、时间戳、前一个区块的全部内容搭配一个随机数进行哈希运算,如果小于目标哈希值,便能成功将这些内容记录到区块链中,PoW区块链中单个区块的构建过程如图1所示。PoW机制最大的问题是需要消耗大量的时间和能源来完成记账,因此其难以在生产制造领域中推广。

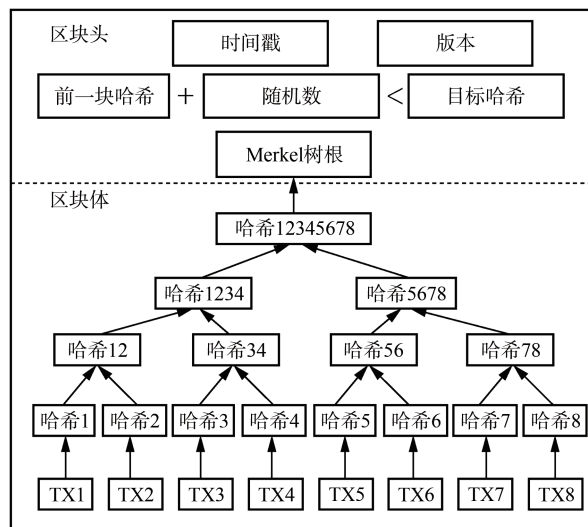


图1 PoW区块链中单个区块的构建过程

DPoS旨在降低PoW机制下的能源成本,其核心思想与企业的运营模式类似。在DPoS机制下,需要通过见证人认可才能参与区块链网络^[17]。经典的以DPoS为基础的EOS有21名见证人管理并进行记账^[18]。DPoS机制一定程度上解决了PoW机制需要投入大量能源成本的问题^[19]。在DPoS机制下只需要被选举的见证人进行哈希运算,符合企业级应用的管理逻辑,在生产制造过程中或与物联网结合的领域能够起到关键作用^[20]。

(2) 基于信任的共识机制

基于信任的共识机制主要是实用拜占庭容错(practical Byzantine fault tolerance, PBFT)算法及其改进算法,主要用于联盟链,在互相信任的企业联盟中有更好的应用。

PBFT算法的内核是在不能确定所有的通信节点都可信的情况下,确保信息不会被修改^[21-22]。在PBFT算法下,如果恶意节点或故障节点数量少于

系统中所有节点数量的1/3，区块链当前状态便会达成一致，PBFT算法通信路径如图2所示^[23]。与之相较，raft容错算法虽然拥有1/2的容错率，但只能处理故障节点而无法处理被恶意破坏的节点^[24]。

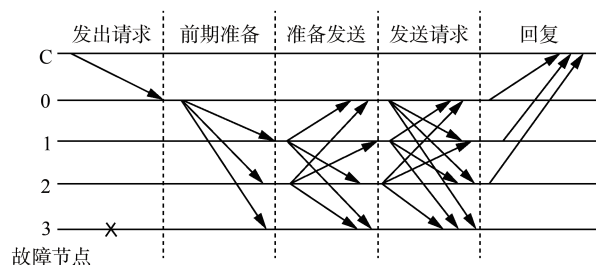


图2 PBFT算法通信路径

PBFT算法是Hyperledger Fabric在v0.6及之前版本使用的共识机制。基于PBFT算法的区块链不需要参与者进行大量的哈希运算就可以对区块链进行修改，没有额外的能源耗费。以PBFT算法搭建的区块链已经具有实用价值，可以用于管控供应链、按固定程序完成交易等场景。但是PBFT算法通信复杂度过高、可拓展性低，当节点个数达到100左右时，性能迅速下降，无法适应智能制造领域数据高速传输的需要^[1]。为了解决通信成本激增的问题，Hyperledger Fabric开发团队提出了简化拜占庭容错（simplified Byzantine fault tolerant, SBFT）算法。与上限是100个节点的PBFT算法相比，SBFT算法在206个节点的实际网络中仍有很好的表现^[25]。Hyperledger Fabric在v1.0版本后开始采用SBFT算法。

1.3.3 智能合约

以太坊概念的提出是区块链进入2.0时代的标志，其区别于以往区块链技术的最大特征是智能合约的引入。智能合约使区块链技术具备了向其他传统领域扩展的可能^[26]。在区块链1.0时代，由于底层语言不具备图灵完备性，难以实现智能合约。《以太坊：下一代智能合约和去中心化应用平台》（Ethereum: a next-generation smart contract and decentralized application platform）^[3]中首次提出将区块链与智能合约相结合。但以太坊需要开发者重新学习一门程序语言，这无疑增加了参与难度。之后，Hyperledger Fabric的出现解决了这一问题^[7]。Hyperledger Fabric具有高度可扩展性，可为以Java为代表的已有编程语言提供支持，降低了入门难度，其共识机制可插拔、模块高度可定制等特性使之非常适合企业级应用^[27]。

智能合约本质上是一种数字合约，除非交易双方达到智能合约上的条件，否则不会产生结果。智能合约与区块链技术融合后，增加了执行可追溯、交易不可逆等特性。智能合约作为一种嵌入式的程序化合约，可以嵌入任何区块链工程，应对合约中设定的情景^[28]。智能合约在供应链、物联网、医疗保健等领域均有应用^[29]。

1.3.4 安全保护

与传统网络组织结构相比，区块链本身已经具备更好的安全性。但其仍存在被攻击或自身软硬件发生错误的可能^[30]，这也是区块链真正投入使用的过程中遇到的一大难题。区块链存在的安全问题包括核心软件错误、钱包攻击、网络攻击、终端攻击等^[31]。下面将对如何解决区块链中可能存在的安全问题进行介绍^[32]。

（1）安全分析

区块链2.0时代以来，区块链的核心便包含了智能合约，而智能合约本身在程序设计阶段可能存在漏洞。在测试阶段或实际运行过程中对区块链进行安全分析，可以避免因智能合约漏洞而受到攻击的问题^[33]。

以Securify方案为例。Securify是一种用于以太坊的安全分析器，是一种可扩展的、完全自动化的安全分析程序^[34]。以往的智能合约安全自动化分析通常采用符号执行的方法（如Oyente符号执行工具）^[35]，这使算法的准确性受到严格限制。Securify采用特征匹配的方法检查智能合约能否实现预定功能，能够将漏洞和疑似漏洞分开，在确保准确性的同时节约了人工成本。

（2）隐私保护

在区块链投入智能制造的过程中，需要同时确保数据的公开性和安全性。账本和资金流动需要在区块链的成员中公开，受到所有参与者的监督^[36]。但在使用区块链进行交易时，需要对交易人的隐私、不能公布的内容进行保护。在去中心化的网络中，没有集中管理的第三方，而且网络中的每个参与者都能获得整个区块链的所有信息，这使区块链技术在安全隐私方面呈现劣势^[37-38]。

区块链技术诞生初期，保护用户隐私的方法是对称密钥、数字加密等。但这些传统方法无法真正保护企业和个人的隐私信息。目前区块链解决隐私问题的方案有很多，如零知识证明、环签名等。

零知识证明是指证明者在不向验证者提供任何有用信息的情况下，使验证者相信某种论断是正确

的^[39]。零知识证明技术能够隐藏交易的发送方、接收方以及交易的详细内容,保护双方隐私。2016年发表的Hawk方法正是基于这一原理开发的^[40]。使用Hawk方法的编程者无须在智能合约中实现加密,只需用直观的方式完成智能合约,Hawk方法的编译器就能自动生成有效的加密协议。通过Hawk方法加密过的智能合约不会在区块链上存储完整的金融交易,以保护交易者的隐私。2020年发表的ZEXE方案以分布式私有计算为基础^[41],其核心技术是一套去中心化加密计算方案。经过ZEXE加密后,无论何种线下计算,发生的交易都只有968 byte。这种方案既确保了数据的隐私性,又使交易能够快速进行。

Rivest R L、Shamir A 和 Adleman L^[42]在2001年首次正式提出环签名方法。环签名方法允许在一组用户中随机选择一个用户代表此组用户对交易进行签名,使攻击者无法确定交易者的身份^[43]。签名的用户匿名展示交易信息并完成交易,没有身份和隐私暴露的风险,且在环签名过程中,签名是不可伪造的,确保了系统的安全性。由于区块链的去中心化特性,依赖多个用户均权进行的环签名有了更契合的应用场景。

2 区块链技术在智能制造中的应用

广义的制造业不仅包含具体的工艺过程,还包括市场分析、产品设计、质量监控、生产过程、管理营销、售后服务直至产品报废处理在内的整个产品生命周期中一系列相互联系的生产活动^[44]。智能制造旨在通过工业互联网、工业大数据、工业机器人、人工智能、区块链等,将整条制造业链条连接起来共同发展。其中智能制造发展所需要的分布式制造、工业大数据共享及安全、透明物流、透明供应链等需求与区块链的优势不谋而合^[45]。

区块链的公开性能够使制造业上下游企业之间信息互通,交易更流畅,解决了信息不对等的问题。区块链技术的安全性和不可修改特性也能使产品溯源和审计更便利,更便于追踪、发现和解决问题。区块链中的智能合约能加速制造业业务运营,对生产过程全流程追踪,快速召回不合格产品。区块链也能融入产品营销,打通整条制造业产业链。下面介绍区块链在智能制造中的几个应用。

2.1 区块链实现供应链追踪

区块链技术本身具有不可修改的特性,在制造业产品流转过程中,能实现对源头及流转过程的追

溯,实现透明供应链。区块链与物联网结合、使用区块链间互操作技术等手段,能够在监测整个供应链上产品质量的同时,确保需求方的信息安全。

在此之后,Korpela K等人^[46]的研究给出了使用区块链技术完成供应链数字化转型的方案,这一研究通过云集成的方式管理供应链,实现供应链的数字化、网络化转型,满足了供应链对动态性能的需求。Saber S等人^[47]对供应链中的区块链应用进行了更深入的研究,着重研究了如何使用区块链技术解决供应链的可持续发展问题,并给出了未来可研究的命题和方向。Kouhizadeh M等人^[48]进一步研究了区块链在可持续性供应链管理(sustainable supply chain management, SSCM)中遇到的障碍,进一步指出了该研究的未来方向是打通面向应用的内部外部壁垒。

(1) 基于区块链的食品溯源系统

在具体的应用场景中,区块链支持的供应链技术已有成功案例,Tsang Y P等人^[49]提出了使用轻量级区块链实现食品追溯系统的方法。在引入区块链技术之前,食品追溯系统不能保证可靠性、可扩展性和信息准确性。现代溯源过程复杂又耗时,其中易腐食品供应链追踪在供应链管理中是一个有吸引力又颇具挑战的研究课题,且这一研究对解决目前国内存在的行政管理追踪等问题均有启示作用。基于区块链的食品溯源系统能够实现食物生产运输过程的全公开,消费者及下游生产厂商能够及时追踪并可靠地监控整条供应链。最终搭建的系统由3个模块组成:物联网监控模块、区块链数据管理模块及模糊食品质量评估模块。物联网与区块链结合的供应链管理系统框架如图3所示。

使用物联网技术收集食品识别信息、运输过程中的环境监测信息以及供应链可能发生的变动,然后将收集的数据用于评估食品保质期和质量衰减。区块链构造采用以DPoS为基础的网络架构,但并非原始DPoS使用的按照节点选举的方式分配增加区块的权益,而是按照供应链中各节点在物流中的作用分配权益。在整个食品追踪流程结束后,该食品对应的区块链会被销毁,以节约存储空间以及运算资源。最终通过模糊算法,对运输过程中记录的温度和湿度信息,结合特定食物对温度和湿度的敏感性进行模糊判断,对易腐食物在供应链末端的质量进行评估,确保食品质量。在这一应用案例中,为每一个产品建立独立区块链、销毁过期区块链的方式,避免了区块链延长时过度膨胀以及供应链缺

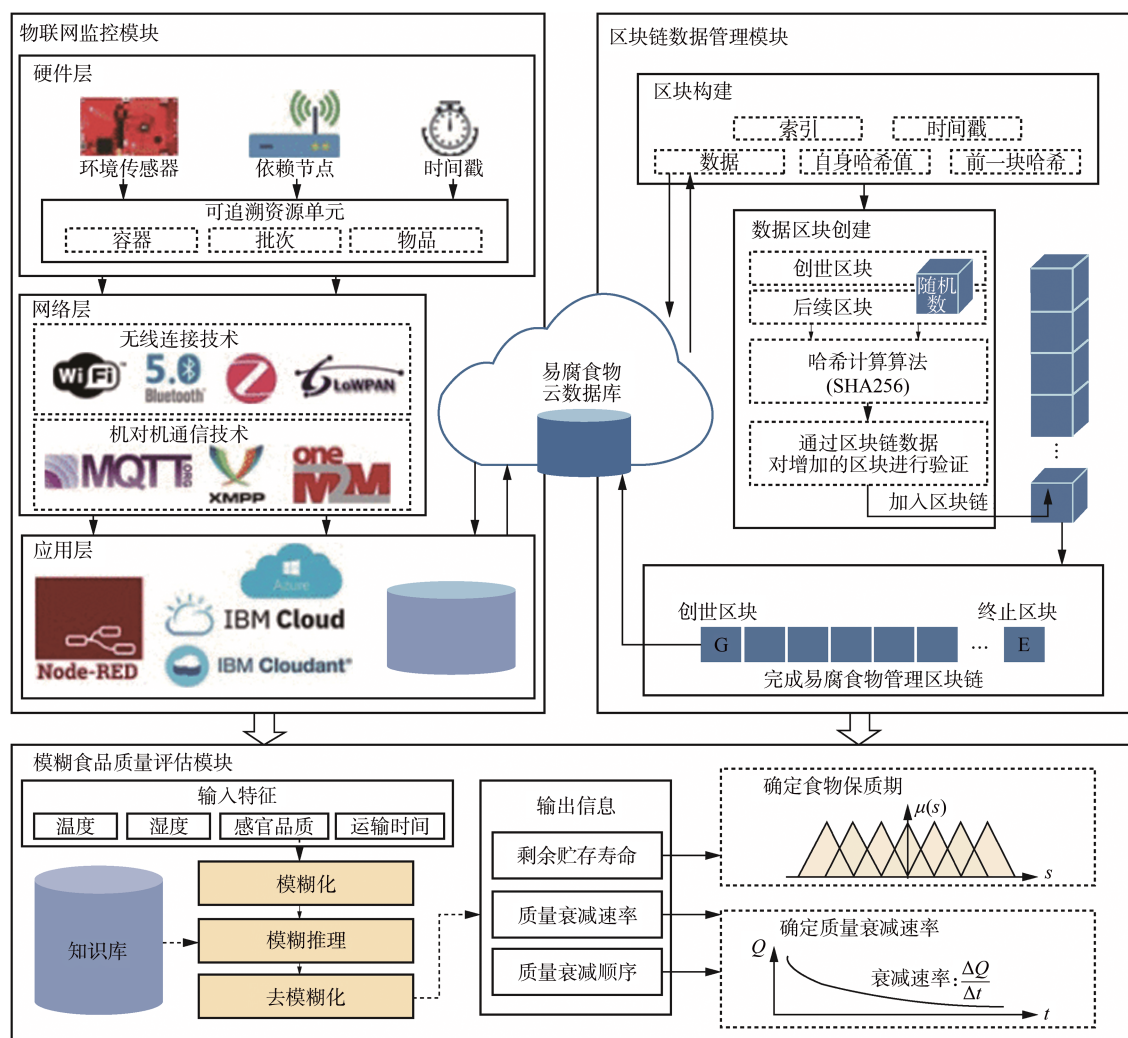


图3 物联网与区块链结合的供应链管理系统框架 [49]

乏可持续性的问题。

（2）基于区块链的军品级零件溯源

对于同样的供应链追踪需求，军品级零件的供应链对产品的质量有十分严格的要求，由于涉及国防工业的信息，对保密性的要求同样很高。且对于军品级零件，出厂并不意味着其生产的结束，在这之后仍存在一系列的运输、维护、维修等需要供应商提供的全生命周期的服务。鉴于此，用于军品级零件追溯的区块链设计十分困难。针对这一难题，美国海军航空系统司令部（NAVAIR）已通过SIMBA Chain平台的技术方案完成试点作业并取得了不错的成果^[50]。为了实现数据和访问权限的分离，技术提供方使用了两个单独的区块链：原始设备供应商的区块链网络使用Hyperledger Fabric搭建，用于美国海军航空系统司令部的区块链网络使用开源企业级以太坊平台Consensus Quorum搭建，

区块链互操作性架构如图4所示。通过实现两区块链之间单向通信的方式，确保美国海军航空系统司令部的信息不会泄露。基于两条链间的互操作性实现的供应链追踪系统更好地保证双方信息的安全性

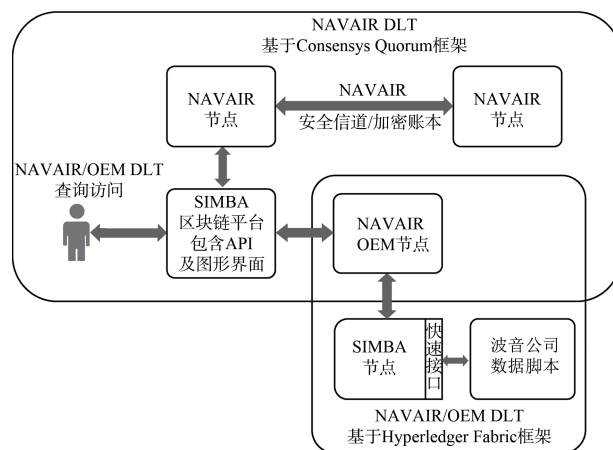


图4 区块链互操作性架构

和保密性,但链间验证和通信会带来较高的时间成本和计算成本。

区块链能够很好地解决智能制造中的供应链追踪问题,但其实现追踪时面临的挑战也不可忽视。在易腐食物供应链追踪过程中,食品的各项物流信息应只对消费者和供应链中的企业公开;在军品级零件供应链追踪的应用中,信息的隐私性和安全性更是重中之重。然而将区块链中公开数据和隐私数据分隔开的技术仍处于探索阶段,这将是使用区块链技术实现供应链追踪的未来研究热点。

2.2 区块链实现工业大数据流转

智能制造的根基之一就是智能化生产过程中

产生的大量可用数据。在制造业的发展过程中,物联网技术可以将传统制造系统转变为现代数字化系统,进而通过行业重塑产生新的可发展方向。工业物联网使现代化企业能够采用新的数据驱动战略,从而更轻松地应对全球竞争压力^[51]。在这一过程中产生的大量可用数据称为工业大数据。尽管大数据应用有许多优势,但大数据分析、大数据管理以及大数据隐私和安全仍然存在有待探索的问题。在这一过程中,区块链因其良好的安全性和去中心化特性,成为解决大数据流转的最佳方案,区块链技术在大数据管理中的应用如图5所示。

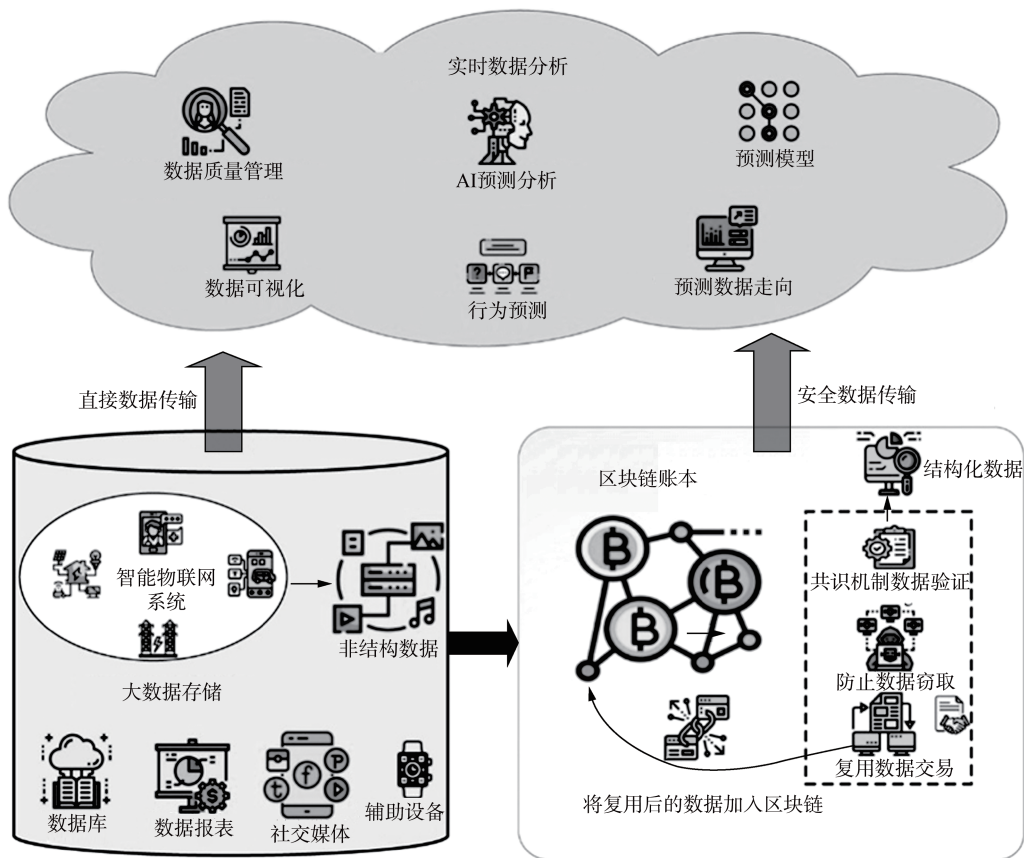


图5 区块链技术在大数据管理中的应用^[51]

区块链技术用于大数据管理仍处于发展阶段,Karafiloski E 等人^[52]对这方面的应用进行了分析。区块链技术可以在用户身份验证、设置访问权限、记录数据访问历史和数据加密等方面发挥关键作用。这在一些需要高度保密性和安全性的系统中起到关键作用。

在区块链大数据管理的实现方面,Li Y 等人^[53]的研究给出了具体的框架。在该框架中,系统被分

为3个部分,即数据生产者、区块链网络和数据用户。数据生产者将数据写入区块链,然后利用智能合约管理数据用户的访问权限,达到数据安全共享的目的。Li Y 等人给出的框架是一种泛化的方法,并非针对制造业的特定环境。该区块链系统在设计时注重去中心化属性,需要进行专有化适配才能在生产制造领域应用。

此后,Chen H F 等人^[54]针对工业大数据的区

区块链管理做了具体研究,提出的方案解决了区块链在大数据流转时面临的存储爆炸问题。通过Shamir密钥分享算法,在不增加总体通信成本的同时,实现存储轻量化。

与之相比,Xu C H等人^[55]的研究更注重解决共享问题。这项研究涉及与大数据相关的另一个重要领域:边缘计算。边缘计算能够将网络、存储、计算、应用合成一体化平台,从而提供更高效的服务。边缘计算见证了属于不同利益相关者的边缘设备数据量的快速增长,但是由于缺乏信任,这些数据无法在它们之间共享,这也是工业大数据面临的问题。将区块链技术与边缘计算融合所形成的大数据安全共享框架可以解决这一问题,该框架包含降低存储资源、算力资源和通信资源的3种创新性技术。

(1) 提出基于PoC (proof-of-collaboration) 的共识机制。PoC机制计算复杂度低,有利于节约增加区块时的算力资源,且其规定了一种根据成员对大数据贡献计算奖励的算法,而不是单纯基于无意义的计算。

(2) 提出可以显著降低存储开销的区块链交易过滤和卸载方案,提出新的防止二次交易和违规增加区块的方法,避免下载整个区块链占用用户的存储空间。

(3) 提出新型区块链交易 (express transaction) 和区块 (hollow block), 提升沟通效率。

目前区块链支持大数据安全共享仍处于研究和实验阶段,如何将其部署到实际应用中是相关研究的热点。Xu C H等人^[55]在研究的验证阶段分别从计算、网络和存储方面对实验结果进行了分析,且在实验中取得了较好的成果。

大数据处理本身就是需要消耗大量算力的任务,与基于工作量的区块链结合会进一步增加算力的消耗。过量的算力消耗会导致智能制造产业链的创收能力受限,甚至无法达到加入区块链前的水平。如何解决这一问题将在后续内容中讨论。

2.3 区块链实现云制造

云制造是随着云计算的发展而诞生的概念。云制造技术通过将分布式资源封装到云服务中,实现对产品全生命周期的管理。在此过程中,客户可以依据个性化需求获取产品设计、制造、测试、管理等产品生命周期中所有阶段的服务^[56]。云制造给客户带来便利的同时也存在一些问题。

云制造需要将所有资源整合,作为云端的资源

供需求者选择,而这些资源显然不是单一供应商能提供的。依赖第三方管控的中心化管理虽然能够完成这一任务,但其在灵活性、效率、可用性和安全性等方面存在问题,不适合作为云制造的核心。因此,需要引入基于区块链技术的云制造去中心化网络架构来解决这个问题。

为了实现云制造系统的去中心化,Li Z等人^[57]提出了一种完整的、基于区块链技术的分布式制造网络平台。为了实现云制造从中心化到去中心化的转变,该团队建立了一种新型的区块链云制造可信平台。为了确保云制造平台的效果,该团队对5个制造服务提供商和15个用户进行了调研,基本证实了平台的可行性。但是在实际应用中的效果还需要进一步测试来验证。

此后,Aghamohammadzadeh E等人^[58]也对区块链在云制造中的应用进行了研究。该团队提出了一种以区块链技术为基础的服务组合模型Block-SC。Block-SC模型定义了一个能够创建和提交合适服务包的分布式云平台,用户可以根据需求获取服务并将其组合,获取所需服务包。Block-SC模型应用了DPoS共识机制,减少了不必要的资源消耗,在实际测试中,服务组合问题的最优化性能得到改善,云制造平台的响应时间也有所缩短。

Wang B N等人^[59]以上述研究为基础提出的服务平台模型有其独特优势。这种基于区块链的架构提出了投票机制,可以通过剥夺服务提供商或参与者使用资格的方式,消除云制造提供商和服务相关参与者之间的第三方信任问题。在研究中提出的Logit-SVM算法能够容忍恶意数据的存在,相较以往的平台模型更具安全性。

由于具有云计算的基础,区块链在云制造中的应用要比在大数据中的应用更加完善,研究人员已经提出了较多的服务平台方案。但目前仍存在以下3个问题。

(1) 目前的研究中很少有在实际应用场景中验证过的方案,实际应用中产生的效果未知,在证明其有效性之前难以投入实际应用。

(2) 云制造难以事先确定参与者身份和数量,导致无法使用对算力浪费最少的PBFT算法,这也就意味着维护区块链本身会消耗较大的能源成本和存储空间。

(3) 服务提供方与参与者之间的信任仍难以保障,云制造服务双方没有传统制造业中的沟通环节,没有信任基础。

为了解决这些问题,需要进行进一步的实测研究,以增强服务提供方和用户对上述平台模型的信任。

2.4 区块链实现ICT制造

信息与通信技术(information and communication technology, ICT)是智能制造的核心,在具体的生产流程和制造资源共享中均有建树。由于区块链本身属于ICT,因此ICT制造与前文介绍的内容多有交叉,是互联网+、云技术、区块链技术等综合应用。

2016年中国信息通信研究院发布的《ICT制造业发展报告》(以下简称《报告》)对国内ICT制造的发展现状及未来趋势进行了介绍。《报告》对ICT制造的介绍十分完善,但受当时科技发展水平的影响,其中尚未体现共享的概念。《报告》中的ICT制造由上游的软件、IT服务,中游的端设备、管理设备、云设备和下游的电子元器件、控制设备和仪表构成,并非本文介绍的广义制造业。

5G技术和区块链技术的发展为ICT制造注入了新的活力。5G虽然出现在区块链之后,但在工业中的应用比区块链技术更加成熟。相较于4G及之前的网络技术,5G具有更强的移动带宽、更大规模可支持通信、更高可靠性和更低的延迟^[60]。但在支持5G的工业环境中,基于集中式架构的设备在处理数据、控制访问权限等方面难以适应未来应用。区块链的去中心化特性可以解决这一问题。

Mistry I等人^[61]对区块链解决5G物联网关键问题展开了研究。在5G网络构建的物联网中,各种不同的电子或电气设备能够使用任何开放渠道(如物联网)实现交互。但是这种交互是有缺陷的:随着网络连接设备的增加,受到外部攻击的风险也在增加;在物联网和云上流转的数据隐私会受到威胁;设备交互缺乏统一标准;多个设备在有中心的网络中交互存在延迟。这些缺陷都可以通过区块链技术弥补。在此基础上Yu C Y等人^[62]对ICT制造展开了进一步研究,其研究重点在于共享制造,以使更多人参与生产过程。共享制造是一种基于点对点的资源共享模式,这与区块链的根本特点相吻合。研究将制造业的参与者从企业变成个人,将只在行业中共享的数据共享给整个社会,让所有有资格参与生产过程的人都参与到生产制造中。研究人员还提出了一种新的共识机制:参与证明(proof-of-participation, PoP),其倾向于让更多参与制造的成员拥有更大的增加区块的权限,确保了共享的公平性。

目前的ICT制造企业主要采用5G物联网技术,结合区块链技术的ICT制造只发展到具有成熟框架但较少投入实际应用的阶段。文献调研表明,区块链技术目前在军用领域有小规模应用,在其他领域也开始逐步落地。

3 挑战与展望

区块链技术与人工智能、物联网等技术相比,属于新兴领域,仍处于探索发展阶段。区块链技术本身还存在一定的问题,如存储空间爆炸问题、可扩展性和连接性问题、算力浪费问题及安全性匿名性问题等。在与智能制造技术交叉融合的过程中,又出现一些新的问题,如通信速度和实时性问题、额外的安全保障问题及用户对区块链技术的信任问题等。

3.1 区块链存储空间爆炸问题

区块链的存储空间爆炸问题是制约区块链可扩展性的主要原因。如前文提到的,区块链的延长会占用大量存储空间,每个参与到区块链中的用户都需要下载整个区块链来验证收到的信息是否正确及获得在区块链中增加区块的权限。

而存储设备的投入是非常巨大的,这给中小型企业带来了负担。在智能制造的预想中,大、中、小型企业都应做到信息公开、合作共赢,并按照最终实际贡献的多少分配利益。如果不能解决区块链的存储问题,会导致区块链仅存储在大型制造业企业的服务器中,这样增加区块及区块链验证的权力仍然会被大型企业把持,失去了引入区块链的意义。这一问题可以通过云存储技术解决。以新型大数据架构IoTA(internet of things application)方案为例,其设定标准数据模型,通过边缘计算将所有的计算过程分散在数据产生、计算和查询的过程中。在这些过程中,统一的数据模型始终没有发生改变,提高了整体的运算效率。将IoTA方案加入区块链能够使区块链成员分担存储和计算负担,避免产生存储爆炸的问题。

3.2 区块链可扩展性和连接性问题

前文介绍了区块链跨链技术和互操作性实现供应链追踪的方法。随着去中心化应用的增多,区块链的个数和种类会越来越多,而不仅拘泥于以太坊等主流区块链体系,这就要求存在一种区块链之间进行通信的技术。区块链互操作性是指将多个区块链网络连接在一起的能力,它能够解决区块链平台

的可扩展性问题和连接性问题^[63]。

不仅如此,链间的互操作性可以解决联盟链的一些固有问题,如前文中提到的使用PBFT算法面临的重大问题便是当成员增加时,通信成本会大幅度上升。该算法的最大成员个数是100,即使是改进后的SBFT算法也只能容纳200个左右的成员。这对于一条产业链显然是不够的,如果将企业内部的物联网并入区块链,其容量更加有限。跨链技术使产业链中每组相近的企业在同一条区块链上,所有的区块链并入一条主链进行管理。通过这种方式,在降低通信成本的同时,还能减轻每个成员的存储负担,有利于共享制造技术的推广。因此,如何安全快速地实现跨链是区块链的未来研究方向之一。

3.3 区块链算力浪费问题

前文介绍了区块链算力消耗主要取决于所采用的共识机制。区块链的算力消耗直接决定了投入实际应用的价值。而这些共识机制中,对算力浪费最少的是基于信任的共识机制。但这种共识机制也有去中心化程度低、需要建立区块链前就确定成员身份这些缺陷,不能适用于所有的应用场景。

为将区块链投入智能制造领域应用,不能完全按照主流的共识机制进行构建。如以DPoS为基础的食品供应链参与机制和PoP共识机制,增加了应用背景所需的评价指标。这些共识机制虽然仍属于基于工作量的共识机制,但却有和DPoS类似的低算力消耗且符合实际的管理员选取标准。但是这种方式仍存在的问题,如低利润率企业可能由于算力不足拖慢整个交易进行的速度。

对于智能制造应用而言,最好的方案是找出一种几乎不消耗算力的方案。基于信任的区块链能够满足这一需求,但也存在前文所述的缺陷。区块链在智能制造中如果想要更进一步,在节约算力上有两个可行方案,具体如下。

(1) 根据每个实际应用场景,设计出合适的DPoS改进算法,避免增加区块的权力被垄断。

(2) 进一步改进PBFT算法,使其参与成员及权限能够在确保安全可信的前提下进行微调,解决灵活度较低的问题。

3.4 区块链安全性和匿名性问题

区块链的安全性和匿名性包含多个方面,如确保区块链中的数据不被篡改、窃取,防止恶意信息的录入,在对有权限人群公开的同时确保数据隐私等,这些是区块链在智能制造中得以广泛应用的

前提。

通过区块链搭建可信的制造资源共享平台可以打通产业链上下游、同种类公司之间的数据壁垒。由于同类公司之间的竞争关系,在区块链加入前,资源共享显然是不可能的。区块链的共识机制能够在没有公证第三方的前提下达成一致,完成交易。通过这样的交易平台,将制造能力细分,使用者能够根据自己的需求获取制造服务。通过这种方式,能够避免制造企业频繁更换生产线造成的生产力浪费,使用者也能在具有不同特色和专长的企业中获取所需服务,从而实现智能制造服务提供商之间、服务提供商与用户之间的互联。搭建这一平台的前提是确保区块链的安全性和匿名性。

区块链的匿名性也对国家信息安全造成威胁。为了降低完全匿名交易带来的犯罪风险,针对区块链上“交易匿名性”的破解工作也在稳步进行,这与区块链安全性和匿名性的发展形成了对抗关系。而作为同样需要区块链技术的智能制造当然也会受到波及,因此,如何进一步确保区块链安全性和匿名性将成为区块链在智能制造中应用的未来研究热点。

4 结束语

本文介绍了区块链技术的基本原理和发展,概括说明了共识机制、智能合约、区块链安全以及权限划分,由此引发了对区块链与智能制造融合领域的思考。区块链与以往的网络框架不同,是一种具有去中心化、公开性、安全性、匿名性、不可修改等特性的网络架构。目前的区块链仍存在存储空间爆炸,可扩展性和连接性、算力利用率和安全性、匿名性难以保证等问题。与智能制造结合后这些问题就体现在难以处理工业大数据、较难确保企业信息安全等方面。在对区块链与智能制造融合的讨论中,指出了区块链在供应链、大数据流转、云制造以及ICT制造中的应用前景,分析了已有的研究成果在解决二者融合领域重点问题的优势。最后探讨了区块链与智能制造融合的未来发展方向,为后来研究者提供参考。

参考文献:

- [1] 曹俊,林亮,李云,等. 区块链研究综述[J]. 重庆邮电大学学报(自然科学版), 2020, 32(1): 1-14.
CAO B, LIN L, LI Y, et al. Review of blockchain research[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2020, 32(1): 1-14.

- [2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[Z]. 2008.
- [3] VITALIK B. Ethereum: a next-generation smart contract and decentralized application platform[Z]. 2014.
- [4] LINNHOFF-POPIEN C, SCHNEIDER R, ZADDACH M. Digital marketplaces unleashed[M]. Heidelberg: Springer, 2018.
- [5] MAESA DD F, MORI P. Blockchain 3.0 applications survey[J]. Journal of Parallel and Distributed Computing, 2020, 138: 99-114.
- [6] LINUX FOUNDATION X. Blockchain for business: an introduction to Hyperledger technologies[Z]. 2019.
- [7] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger Fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the 13th EuroSys Conference. [S.l.:s.n.], 2018: 1-15.
- [8] 周珍妮, 陈碧荣. Web3.0——全新的互联网时代[J]. 科技广场, 2008(7): 235-237.
ZHOU Z N, CHEN B R. Web3.0—a new age of Internet[J]. Science Mosaic, 2008(7): 235-237.
- [9] LI R N, SONG T Y, MEI B, et al. Blockchain for large-scale internet of things data storage and protection[J]. IEEE Transactions on Services Computing, 2019, 12(5): 762-771.
- [10] GUÉGAN D. Blockchain versus private blockchain[J]. Université Paris1 Panthéon-Sorbonne (Post-Print and Working Papers), 2017.
- [11] FERDOUS M S. A survey of consensus algorithms in public blockchain systems for crypto-currencies[J]. Journal of Network and Computer Applications, 2021, 182.
- [12] LAI R, LEE KUO CHUEN D. Blockchain—from public to private[M]//Handbook of block chain, digital finance, and inclusion. Amsterdam: Elsevier, 2018: 145-177.
- [13] PAHLAJANI S, KSHIRSAGAR A, PACHGHARE V. Survey on private blockchain consensus algorithms[C]//Proceedings of 2019 1st International Conference on Innovations in Information and Communication Technology. Piscataway: IEEE Press, 2019: 1-6.
- [14] DIB O, BROUSMICHE K L, DURAND A, et al. Consortium blockchains: overview, applications and challenges[J]. International Journal on Advances in Telecommunications, 2018, 11(1&2): 51-64.
- [15] WANG Y H, CAI S B, LIN C L, et al. Study of blockchains's consensus mechanism based on credit[J]. IEEE Access, 7: 10224-10231.
- [16] ZHANG C Q, WU C S, WANG X Y. Overview of blockchain consensus mechanism[C]//Proceedings of the 2020 2nd International Conference on Big Data Engineering. New York: Association for Computing Machinery, 2020: 7-12.
- [17] SCHMIDT D. Delegated proof of stake[Z]. 2020.
- [18] 顾顾菲. 基于EOS平台和面向服务架构的OA系统的构建[D]. 上海: 复旦大学, 2010.
GU Y F. Construction of OA system based on EOS platform and service-oriented architecture[D]. Shanghai: Fudan University, 2010.
- [19] LI C, PALANISAMY B. Comparison of decentralization in DPoS and PoW blockchains[C]//Proceedings of International Conference on Blockchain. Cham: Springer, 2020: 18-32.
- [20] KIM M, KIM Y. Development of IoT device management system using blockchain DPoS consensus algorithm[J]. Journal of IKEEE, 2019, 23(2): 508-516.
- [21] SUKHWANI H, MARTINEZ J M, CHANG X, et al. Performance modeling of PBFT consensus process for permissioned blockchain network (Hyperledger Fabric)[C]//Proceedings of 2017 IEEE 36th Symposium on Reliable Distributed Systems. Piscataway: IEEE Press, 2017: 253-255.
- [22] CRAIN T, GRAMOLI V, LARREA M, et al. DBFT: efficient leaderless Byzantine consensus and its application to blockchains[C]//Proceedings of 2018 IEEE 17th International Symposium on Network Computing and Applications. Piscataway: IEEE Press, 2018: 1-8.
- [23] 方维维, 王子岳, 宋慧丽, 等. 一种面向区块链的优化PBFT共识算法[J]. 北京交通大学学报, 2019, 43(5): 58-64.
FANG W W, WANG Z Y, SONG H L, et al. An optimized PBFT consensus algorithm for blockchain[J]. Journal of Beijing JiaoTong University, 2019, 43(5): 58-64.
- [24] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]//Proceedings of 2014 USENIX Annual Technical Conference. [S.l.:s.n.], 2014: 305-319.
- [25] GOLAN GUETA G, ABRAHAM I, GROSSMAN S, et al. SBFT: a scalable and decentralized trust infrastructure[C]//Proceedings of 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Piscataway: IEEE Press, 2019: 568-580.
- [26] WANG S, YUAN Y, WANG X, et al. An overview of smart contract: architecture, applications, and future trends[C]//Proceedings of 2018 IEEE Intelligent Vehicles Symposium. Piscataway: IEEE Press, 2018: 108-113.
- [27] NASIR Q, QASSE I A, ABU TALIB M, et al. Performance analysis of Hyperledger Fabric platforms[J]. Security and Communication Networks, 2018.
- [28] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.
- [29] MOHANTA B K, PANDA S S, JENA D. An overview of smart contract and use cases in blockchain technology[C]//Proceedings of 2018 9th International Conference on Computing, Communication and Networking Technologies. Piscataway: IEEE Press, 2018:1-4.
- [30] ZHANG R, XUE R, LIU L. Security and privacy on blockchain[J]. ACM Computing Surveys, 2020, 52(3): 1-34.
- [31] SAAD M, SPAULDING J, NJILLA L, et al. Exploring the attack surface of blockchain: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1977-2008.
- [32] GUO H Q, YU X J. A survey on blockchain technology and its security[J]. BlockChain: Research and Applications, 2022, 3(2): 102-116.
- [33] LI X Q, JIANG P, CHEN T, et al. A survey on the security of blockchain systems[J]. Future Generation Computer Systems, 2020, 107: 841-853.
- [34] TSANKOV P, DAN A, DRACHSLER-COHEN D, et al. Securify: practical security analysis of smart contracts[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 67-82.
- [35] SIDDIQUI S T, AHMAD R, SHUAIB M, et al. Blockchain security threats, attacks and countermeasures[C]//Proceedings of Ambient Communications and Computer Systems. [S.l.:s.n.], 2020: 51-62.
- [36] ZHANG R, XUE R, LIU L. Security and privacy on blockchain[J]. ACM Computing Surveys, 2020, 52(3): 1-34.
- [37] HENRY R, HERZBERG A, KATE A. Blockchain access privacy: challenges and directions[J]. IEEE Security & Privacy, 2018, 16(4): 38-45.
- [38] MOHANTA B K. Blockchain technology: a survey on applications and security privacy Challenges[J]. Internet of Things, 2019, 8.
- [39] GOLDREICH O, OREN Y. Definitions and properties of zero-knowledge proof systems[J]. Journal of Cryptology, 1994, 7(1): 1-32.
- [40] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]//Proceedings of 2016 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2016: 839-858.
- [41] BOWE S, CHIESA A, GREEN M, et al. ZEXE: enabling decentralized

- private computation[C]//Proceedings of 2020 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2020: 947-964.
- [42] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.
- [43] FUJISAKI E, SUZUKI K. Traceable ring signature[C]//Proceedings of International Workshop on Public Key Cryptography. Heidelberg: Springer, 2007: 181-200.
- [44] 王飞跃, 高彦臣, 商秀芹, 等. 平行制造与工业5.0: 从虚拟制造到智能制造[J]. 科技导报, 2018, 36(21): 10-22.
WANG F Y, GAO Y C, SHANG X Q, et al. Parallel manufacturing and industries 5.0: from virtual manufacturing to intelligent manufacturing[J]. Science & Technology Review, 2018, 36(21): 10-22.
- [45] ZHANG Q, LIAO B Y, YANG S L. Application of blockchain in the field of intelligent manufacturing: theoretical basis, realistic plights, and development suggestions[J]. Frontiers of Engineering Management, 2020, 7(4): 578-591.
- [46] KORPELA K, HALLIKAS J, DAHLBERG T. Digital supply chain transformation toward blockchain integration[C]//Proceedings of the 50th Hawaii International Conference on System Sciences. [S.l.:s.n.], 2017.
- [47] SABERI S, KOUHIZADEH M, SARKIS J, et al. Blockchain technology and its relationships to sustainable supply chain management[J]. International Journal of Production Research, 2019, 57(7): 2117-2135.
- [48] KOUHIZADEH M, SABERI S, SARKIS J. Blockchain technology and the sustainable supply chain: theoretically exploring adoption barriers[J]. International Journal of Production Economics, 2021, 231.
- [49] TSANG Y P, CHOY K L, WU C H, et al. Blockchain-driven IoT for food traceability with an integrated consensus mechanism[J]. IEEE Access, 2019, 7(1): 129000-129017.
- [50] ASUNCION F, BRINCKMAN A, COLE D, et al. Connecting supplier and DoD blockchains for transparent part tracking[J]. BlockChain: Research and Applications, 2021, 2(3): 17-30.
- [51] DEEPA N, PHAM Q V, NGUYEN D C, et al. A survey on blockchain for big data: approaches, opportunities, and future directions[J]. Future Generation Computer Systems, 2022, 131: 209-226.
- [52] KARAFILOSKEI E, MISHEV A. Blockchain solutions for big data challenges: a literature review[C]//Proceedings of IEEE EUROCON 2017 17th International Conference on Smart Technologies. Piscataway: IEEE Press, 2017: 763-768.
- [53] LI Y, HUANG J Q, QIN S Z, et al. Big data model of security sharing based on blockchain[C]//Proceedings of 2017 3rd International Conference on Big Data Computing and Communications. Piscataway: IEEE Press, 2017: 117-121.
- [54] CHEN H F, WU H L, CHANG C C, et al. Light repository blockchain system with multisecret sharing for industrial big data[J]. Security and Communication Networks, 2019.
- [55] XU C H, WANG K, LI P, et al. Making big data open in edges: a resource-efficient blockchain-based approach[J]. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(4): 870-882.
- [56] XU X. From cloud computing to cloud manufacturing[J]. Robotics and Computer-Integrated Manufacturing, 2012, 28(1): 75-86.
- [57] LI Z, BARENJI A V, 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.
- [58] AGHAMOHAMMADZADEH E, FATAHI VALILAI O. A novel cloud manufacturing service composition platform enabled by blockchain technology[J]. International Journal of Production Research, 2020, 58(17): 5280-5298.
- [59] WANG B N, WANG P, TU Y L. Customer satisfaction service match and service quality-based blockchain cloud manufacturing[J]. International Journal of Production Economics, 2021, 240: 1-13.
- [60] CHENG J F, CHEN W H, TAO F, et al. Industrial IoT in 5G environment towards smart manufacturing[J]. Journal of Industrial Information Integration, 2018, 10: 10-19.
- [61] MISTRY I, TANWAR S, TYAGI S, et al. Blockchain for 5G-enabled IoT for industrial automation: a systematic review, solutions, and challenges[J]. Mechanical Systems and Signal Processing, 2020, 135: 106382.
- [62] YU C Y, JIANG X L, YU S Q, et al. Blockchain-based shared manufacturing in support of cyber physical systems: concept, framework, and operation[J]. Robotics and Computer-Integrated Manufacturing, 2020, 64: 101931.
- [63] QASSE I A, TALIB M A, NASIR Q. Inter blockchain communication: a survey[C]//Proceedings of the ArabWIC 6th Annual International Conference Research Track. [S.l.:s.n.], 2019: 1-6.

[作者简介]



林知微 (1969-), 女, 北京理工大学自动化学院、复杂系统智能控制与决策国家重点实验室副教授, 中国人工智能学会机器博弈专业委员会副秘书长, 主要研究方向为目标检测、传感器网络以及区块链技术。



张嵩川 (1999-), 男, 北京理工大学自动化学院硕士生, 主要研究方向为目标检测、区块链技术。



王成吉 (1997-), 北京理工大学自动化学院硕士生, 主要研究方向为目标检测、无监督学习。



周亦炜 (1999-), 北京理工大学自动化学院硕士生, 主要研究方向为目标检测、数据库技术。