◆特邀专稿◆

工业区块链技术进展*

黄廷磊[1**],邓　松[2],张　姿[3],韩啸宇[1],蒋建辉[4],宗云兵[5]

(1.中国科学院软件研究所,北京　100080;2.南京邮电大学,江苏南京　210003;3.桂林电子科技大学,广西桂林　541004;4.广西科学院,广西南宁　530007;5.山东产业技术研究院,山东济南　250102)

摘要:工业互联网正在加速推进,其中数据隐私泄露、数据安全和数据追溯等问题严重制约了企业之间的信息流通和数据共享。区块链作为一种去中心化、无需中介、不可篡改、可追溯的技术,在金融、虚拟货币领域被广泛应用。应用区块链技术可以很好地解决工业互联网的应用难题。本文详细介绍工业区块链的内涵和应用现状,重点分析了工业区块链的核心技术和工业应用面临的难题,并对国内外在相关技术方面的研究进展进行了介绍。

关键词:工业互联网　工业区块链　交易性能　跨链交互　分布式账本

中图分类号:TP311.13　　**文献标识码**:A　　**文章编号**:1005-9164(2021)04-0331-10

DOI:10.13656/j.cnki.gxkx.20211119.001

0　引言

当前,国内外工业互联网产业体系已基本构建,全球工业互联网平台市场持续高速增长,行业应用水平持续提升,工业互联网取得重大发展成效。工业互联网的本质是设备、生产线、工厂、供应商、产品和客户紧密连接起来,共享各生产数据要素,通过自动化、智能化的高效生产方式降低经营和生产成本,推动工业转型发展[1]。工业互联网是全球工业系统与高级计算、分析、传感技术以及互联网的高度融合,它通过智能机器间的连接最终将人机连接,结合软件和大数据分析,重构全球工业、激发生产率,让世界更快速、更安全、更清洁且更经济[2]。

然而,随着工业互联网不断深入发展,数据隐私泄露、数据确权、数据安全、数据追溯等不少问题逐步凸显。在工业互联网中,数据作为一种新型生产资料要素,缺乏有效管理,直接制约不同参与方之间的可信协作。区块链采用一种分布式技术,其多方共治共管架构、密码学加密运算和共识合约机制,能够实现数据的多方维护、交叉验证、全网一致、防篡改、可追溯等,为工业互联网中数据要素的配置管理提供新的解决方案。作为七大新基建技术之一的区块链技术,必将成为数字时代和信息社会的信任基石,对各行各业影响深远[3]。区块链被称为第四次工业革命的支柱,将其与引发前几次工业革命的蒸汽机和互联网等

收稿日期:2021-07-10

*广西人才专项基金项目(AD18281059)和工信部大数据产业发展试点示范项目([2020]47号)资助。

【作者简介】

黄廷磊(1971-),男,教授,主要从事时空数据管理、区块链技术研究,E-mail:tinglei@iscas.ac.cn。

【**通信作者】

【引用本文】

黄廷磊,邓松,张姿,等.工业区块链技术进展[J].广西科学,2021,28(4):331-340.

HUANG T L,DENG S,ZHANG Z,et al.Progress of Industrial Blockchain Technology [J].Guangxi Sciences,2021,28(4):331-340.

技术进行比较,它有能力破坏现有的经济和商业模式,且已证明其在新兴市场经济体特别有价值。

1 工业区块链内涵

工业互联网作为工业全要素、全产业链、全价值链连接的枢纽,旨在实现设备、企业、人、机构之间的可信互联。而工业互联网中不同参与方之间的可信协作,需要对工业互联网数据要素进行有效管理。区块链作为数字加密技术、网络技术、计算技术、可信共享等多种信息技术交织融合的产物,能够利用密码学技术和分布式共识协议来保证网络传输与访问安全,实现数据多方维护、交叉验证、全网一致、不易篡改。区块链作为面向数据要素管理的新一代信息基础设施类技术[4],为工业互联网中数据要素的配置管理提供了新的解决方案。

工业区块链即是将区块链原理和技术运用于工业互联网领域,赋能工业互联网中的数据流通、数据安全和促进价值相关转换环节,为工业互联网上数据交换共享、确权、确责以及海量设备接入认证与安全管控等方面注入新的安全能力。区块链赋予数据难以篡改的特性,进而保障数据传输和信息交互的可信和透明,有效提升各制造环节生产要素的优化配置能力,加强不同制造主体之间的协作共享,以低成本建立互信的“机器共识”和“算法透明”,加速重构现有的业务和商业模式。

工业区块链的概念初见萌芽但尚未引起业内广泛研讨和充分重视。区块链作为信息技术时代新型基础设施建设的信任基石,无论从安全角度还是改善运营效率和降低成本的角度,其应用空间势必从虚拟货币、金融领域向工业互联网等影响人类生产生活更广泛的领域渗透。

2 工业区块链关键技术

目前,区块链技术已经发展到第四代,如图 1 所示[5]。前三代主要是做横向扩展,解决加密数字货币、超级账本和去中心化应用问题。随着工业 4.0 的推进,区块链将在性能和隐私方面深耕。与传统的区块链相比,工业区块链的四大核心技术依然是分布式账本、共识机制、密码学以及智能合约,它们分别起到数据存储、数据处理、数据安全以及数据应用的作用,但工业区块链对公用账本和分布式数据库的实时性能、大数据存储、隐私计算问题有更高要求。

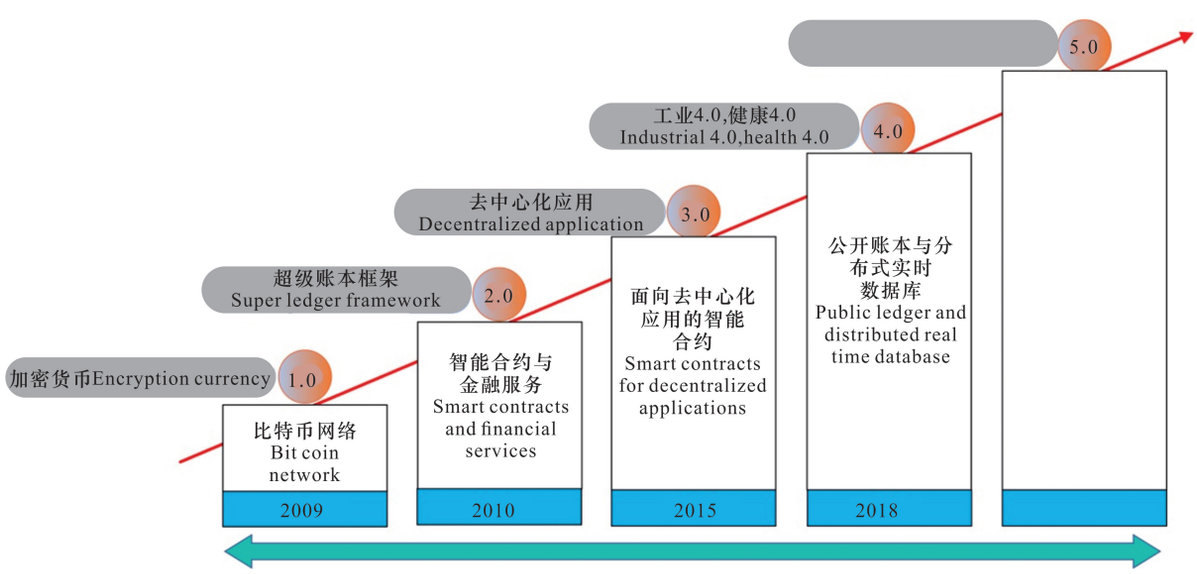

图 1 区块链发展路线示意

Fig.1 Diagram of blockchain development

2.1 分布式账本

分布式账本构建了区块链的框架,其本质是一个分布式数据库,在区块链中起数据储存的作用。跟传统分布式存储有所不同,区块链分布式存储的独特性主要体现在 2 个方面:一是区块链每个节点都按照块链式结构存储完整的数据,而传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的,依靠共识机制保证存储的一致性,而传统分布式存储一般是通过中心节点往其他备份节点同步数据。区块链作

为一种 IO 敏感的分布式数据库,底层存储通常首选效率较高的 NoSQL 数据库,例如 LevelDB、CouchDB、RocksDB 等。同时,鉴于应用层多使用关系型数据库的现实,链系统提供了灵活可插拔的多种数据库支持。

2.2 共识机制

共识机制在区块链中起统筹节点行为、明确数据处理的作用。因为分布式账本去中心化的特点,决定了区块链网络是一个分布式的结构,每个节点都可以自由地加入其中,共同参与数据的记录。但与此同时,衍生出令人头疼的"拜占庭将军问题",即网络中参与的节点数越多,全网就越难以达成统一,需要一套机制来协调全节点账目保持一致。区块链提出了4种不同的共识机制:工作量证明、权益证明、委托权益证明和重要性证明,适用于不同的应用场景,在效率和安全性之间取得平衡。目前主流的联盟链偏好高效、确定性的共识机制,多共识支持趋势凸显。相对于公链希望"全民公投"的共识,联盟链注重共识效率和共识确定性,例如类 BFT 共识、Raft 共识等。此外,为适应不同应用场景,联盟链产品已提供可插拔多种共识机制的支持,多共识支持逐渐成为主流。

2.3 非对称加密和授权技术

非对称加密和授权技术,保证了数据的安全,验证了数据的归属。存储在区块链上的交易信息是公开的,但是账户身份信息是高度加密的,只有在数据拥有者授权的情况下才能访问,从而保证数据的安全和个人的隐私。数据进入分布式数据库中,也不是单纯地打包,底层的数据构架则是由区块链密码学来决定的。打包好的数据块,会通过密码学中的哈希函数处理成一个链式的结构,后一个区块包含前一个区块的哈希值。因为哈希算法具备单向性、抗篡改等特点,所以在区块链网络中,数据一旦上链就不可篡改且可追溯。目前多数联盟链支持国密 SM2、SM3、SM4 配置,逐渐成为联盟链的标准配置。

2.4 智能合约

智能合约在区块链中起数据执行与应用的功能,可以自动化地执行一些预先定义好的规则和条款。在分布式账本的基础上,可以通过智能合约,将用户之间的约定由代码的形式把条件罗列清楚,并通过程序来执行,而区块链中的数据,则可以通过智能合约调用。依托 Hyperledger Fabric 和以太坊的强大生态,Chaincode 合约和 EVM 合约备受欢迎,成为多数联盟链都支持的合约类型。此外,WASM 合约凭借移植性好、加载快、效率高、社区生态好的特点,成为区块链合约体系的新宠。

总的来说,四大核心技术在区块链中各尽其职,它们共同构建了区块链的基础。

3 工业区块链研究现状

区块链价值的前景很吸引人,但区块链在工业应用中的适应和部署面临着许多挑战。一些关键挑战,既是技术性的,也是非技术性的。技术性的挑战与安全、性能和多链融合有关,而非技术性的挑战与隐私和政府法规有关。

随着互联网技术的发展,企业原来的层级式组织、集中管控模式朝着自组织、生态组织发展演化。市场竞争格局以组建生态联盟为主,联盟内企业越来越多地依赖与外界进行交互和协同。企业在系统内部容易建立信任,但系统之间的信任却难以实现。以区块链为代表的新一代信息技术,基于密码学原理而无需第三方信任中介参与,实现互联网上的企业可信价值传递。由多个区块链系统信任链接形成多方协作的平台,这就是联盟链的基础。

面对工业互联网的发展问题,区块链应用面临着交易性能不足、跨链交互难以实现及隐私保护薄弱等多个主要问题。在交易性能方面,目前研究热点主要是采用分片、链下存储和链下支付网络等技术;在跨链交互方面,主要研究热点是公证人机制、侧链、哈希锁定和分布式密钥控制技术;在隐私保护方面,主要研究热点是支持最新国密算法、二级证书、访问控制等技术。

3.1 交易性能

交易性能通常用每秒交易数量来表征。传统比特币项目中,比特币的交易性能为7,以太坊为15,远低于中心化交易系统 Visa 的 1 700,不能和天猫 50 多万的交易吞吐能力相比。分片是为了解决交易性能的不足,许多研究者提出了分片、链下存储、链下支付网络等技术。

3.1.1 分片

分片技术的思想源自传统中心化系统的分布式架构,例如谷歌 BigTable 和 MapReduce,Apache 基金会的 Hadoop 和 Cassandra 等系统。分布式架构通过增加节点数量实现系统性能的线性增加,该过程的核心技术之一就是分片。分片是先将整个系统的状态划分为多个独立的子状态,之后构建节点集群并行处理各子状态。因此,分片实现了由单路串行到多

路并行的跨越,从而实现交易吞吐量的提升。可以这样理解分片:分片涉及将一个数据表拆分为可以用作新表的行,这些行称为分区,并且包含不依赖于其他表中存储的数据。这些分区有助于降低每个节点上数据库的大小,从而改进数据库的性能。

2016年,Elastico协议被提出,被认为是对区块链分片的早期探索。作为第一代分片扩容方案,Elastico采用PoW进行节点身份建立,并采用BFT达成共识,对后续多个项目起到了很好的指导作用。值得一提的是,分片在一定程度上降低了区块链系统的安全性,为此需要对所有分片进行拜占庭校验,以限制恶意节点的最大数量。杨耀东等[6]在区块链性能提升技术研究中提到,在设计分片时要考虑分区状态的选择、确保操作语义完整性、负载均衡和重新分片等问题;并以QuarkChain为例,介绍了分片方案的总体设计、系统状态的分割、QuarkChain转账和再分片等内容。潘晨等[7]介绍了区块链可扩展性的研究。

上海交大、国防科大等团队在区块链扩容相关研究中,详细介绍了典型区块链项目Elastico和Zilliqa[7,8]。Elastico和Zilliqa都采用PoW作为分片算法,片内的共识过程则采用PBFT算法。为了抵御女巫攻击[9],在共识之初,进行简单的工作量证明以建立参与PBFT共识的身份。将全网节点划分为不同子集的判据主要基于PoW的结果。通过建立一个随机模型可以获得这样的结论:当分片大小超过600时,即使攻击者掌握1/3以上的算力,其控制一个分片的概率可以忽略不计。Elastico方案主要基于UTXO模型[10],用户在链上进行交易时需要创建一个收据,这样就可以允许用户将数据存储到一个特定的分片中,并且分片上的用户可以创建一个消费收据的交易。因此,在交易过程中Elastico能够有效抵御双花攻击[11]。Zilliqa主要基于账户模型,交易进行时,通过发送者的身份作为基准来映射到不同的分片。在共识过程中,不同发送者的交易可能会映射到不同的分片中,但同一发送者的交易会映射到同一分片,因此也能够抵御双花攻击。Hafid等[12]就区块链的扩容性进行了全面研究,并按照共识算法的不同将主要的分片方案进行综述,分为(1)基于PoW和PFT的分片方案,(2)基于PoS和PFT的分片方案,(3)基于其他共识算法的分片方案。

3.1.2 链下存储

在实际商务和工业互联网环境中,多种设备和系统会产生大量数据。由于区块链特性,每一个节点必须保存和处理上链的完整交易数据,以实现去中心化要求。在这种情况下,工业区块链几乎无法满足正常的存储和计算要求,因此必须研究链下存储方案,释放链上存储和计算压力。

Zyskind等[13]采用分布式哈希表设计了链下存储方案。原始全量数据存储在链下的哈希表里,链上只存储原始数据的引用。数据引用一般通过SHA-256哈希处理获得。分布式哈希表(Distributed Hash Table,DHT)是一种分布式存储技术,无需中心服务器,每个区块链节点负责局部路由并存储小部分数据,从而实现网络寻址和存储[14]。星际文件系统(Inter Planetary File System,IFPS)是一种分布式文件系统[15,16],具有内容寻址特性,即内容本身决定了内容位置。文件存储后,经过哈希处理会得到一个文件引用。文件引用可以作为文件索引,也可以检验文件内容是否被篡改。Xie等[17]还提及,IPFS内置了激励层Filecion和新的共识协议存储证明(Proof of Storage,PoS)。

此外,基于美国SLAC国家加速器实验室,研究者还搭建了联合DHT和IPFS的融合链下存储框架[18,19]。Ali[20]和He等[21]团队提出了基于云模式的链下存储方案。

3.1.3 链下支付网络

网络是影响区块链交易性能的又一重要因素。传统区块链网络是一种广播机制,要求每一个节点对所有交易进行中继转播。当面临大量、频繁交易时,传统区块链网络往往由于带宽不足而导致严重拥堵,最终导致交易性能下降。采用链下支付网络,可以将大量频繁的交易迁移到链下进行,即采用链下支付网络的方式降低链上数据存储、传输、计算的压力,从而提升交易性能。需要注意的是,链下支付网络降低了区块链系统的去中心化程度,这在公链(非许可链)中有一定的安全隐患,但在工业区块链(许可链)的场景下,特别是对节点用户有一定准入门槛要求的情况下,影响较小。链下支付网络比较经典的有比特币的闪电网络[22]和以太坊的雷电网络[23]。这2种网络在保证区块链底层协议不变的同时,将交易搬运至链下进行。可以理解为,交易过程中,只有粗粒度的交易目录记录在链上,交易详情则记录在链下。

闪电网络是最早通过链下支付通道形成支付网

络,实现交易吞吐量提升的方案。闪电网络本质上是一种状态通道,它使用智能合约技术来实现链下安全交易,包括可撤销顺序完备合约(Recoverable Sequence Maturity Contract,RSMC)和哈希时间锁合约(Hashed Time-Lock Contract,HTLC)[24]。RSMC实现了双人双向交易通道。它通过押金机制建立资金池,每次交易涉及对资金池分配方案的调整和签名验证。交易结束时,智能合约按照最新资金分配方案在链上广播,并由节点确认。HTLC通过资金冻结、哈希运算、哈希验证等实现交易。基于哈希时间锁合约,可以将RSMC中的资金池连成网络,进而可以为网络中的任意2个节点间搭建交易通道。

雷电网络的提出,主要是为了解决闪电网络方案中效率、可用性不足的问题。雷电网络承接了闪电网络的基本架构[25],但在脚本系统方面完全突破了比特币网络的限制,可以实现灵活的智能合约,完善了支付通道惩罚交易的存储策略。雷电网络中,惩罚交易基于交易双方的交易轮数的签名,只要一方出示更高交易轮数的签名,即可判定另一方存在作恶[26]。

其他常见链下支付网络技术还有Sprites[27]、微雷电网络、Trinity[28]等。

3.2 跨链交互

区块链在设计之初并未考虑不同链之间的信息交互需求,导致在不同企业或企业不同部门分别部署区块链后,无法进行链间数据资产交换,从而无法实现价值传输。跨链主要分为2个阶段:资产在A链上的锁定和相应资产在B链上的解锁。如何确保锁定与解锁以及确保锁定与解锁成功或失败的原子性,是跨链技术的主要问题。为解决这些问题,目前研究的主流技术包括公证人机制、侧链/中继、哈希锁定和分布式密钥控制技术等。

3.2.1 公证人机制

在工业区块链中,如果需要交易的2条区块链没有形成非常信任的关系,则需要找第三方中介作为公证人,由这个公证人作为中介进行跨链消息的验证和转发。公证人机制主要包括3种类型:单签名公证人、多签名公证人和分布式签名公证人。单签名公证人通常由单一指定的独立节点或者机构充当,同时承担数据收集、交易确认和验证等任务。多签名公证人通常由多节点或机构充当。他们在各自账本上共同签名达成共识后才能完成交易。分布式签名公证人类似多签名公证人机制,但不同的是它采用了多方计算技术,安全性更高。

3.2.2 侧链/中继

与公证人机制不同,侧链更加强调通过去中心化的方式实现跨链沟通。侧链的实现基于某种通用证书在主链上的锚定。侧链通过简易支付验证(Simplified Payment Verification,SPV)楔入技术实现主链资产向侧链转移,侧链上的功能操作仅对被转移资产有效,而不会对主链造成影响。

BTC-Relay是一种代表性侧链技术。作为最早的侧链技术,通过使用以太坊的智能合约,BTC-Relay连接了以太坊和比特币的网络,并最终实现了用户在以太坊网络上验证比特币上的交易。一定程度上,可以说BTC-Relay创造了另一个比特币子网络。

Cosmos是另一种侧链技术。该技术是Tendermint团队研发的一种异质跨链网络[29]。Cosmos采用了Tendermint共识协议[30],它具有类似拜占庭容错共识引擎的高性能、一致性特点,同时严格限制了分叉。Cosmos使用中继技术实现不同区块链之间的通信。在Cosmos中,通过Hub连接所有区块链并实现中继功能。任何连接的区块链需实时将更新状态告知Hub。

3.2.3 哈希锁定

哈希锁定的主要特点是用户双方共用一个密钥完成资产交换,并采用时间锁和智能合约来保证交易的原子性[31]。哈希锁定的主要原理如下:在不同链之间设定相互操作的触发器,该触发器通常为某个待披露明文随机数的哈希值。该哈希值作为一个通信密钥,只有获得密钥的用户,才能获得资产。同时,哈希锁定中还构造了2个赎回合约,需要在有限时间内完成双重签名。

3.2.4 分布式密钥控制技术

分布式密钥控制技术由Fusion提出,通过分布式密钥生成算法和门限签名技术保证了跨链资产的锁定和解锁[32]。该技术的核心在于分布式控制权的管理,即将资产的所有权和使用权分离,将原链上数字资产的控制权安全地转移至非中心化系统中,规定参与共识的所有节点通过分布式密钥控制技术才可完成锁定和解锁,从而避免了少数节点作恶的发生。

3.3 隐私保护

每种类型的区块链都有不同的隐私问题。全部参与者的公共区块链都可以查看,因此很难维护任何参与的行业实体的隐私,以及在此类区块链中进行一些交易。对于财团区块链,隐私不能完全维护,因为有一些被选择的参与者可以查看所有事务。私有区

块链可以提供相对更好的隐私程度,但只由单个实体控制[33],通常被认为是一个不安全的环境。

区块链针对网络层和数据层分别有不同的隐私保护策略。网络层防御机制的重点是增加攻击者搜索网络层数据的难度,主要包括限制接入、恶意节点检测、数据混淆等具体技术;数据层保护机制的侧重点是在满足区块链正常运行的技术上,防止恶意节点获得准确的交易数据,主要包括数据失真、数据加密、限制发布等具体技术。

3.3.1 国密算法

作为一种颠覆性的革命技术,区块链的发展尤为迅速,我国对于区块链的研究更是处于世界前列。但是,也如我国在某些科研领域存在"卡脖子"问题一样,在区块链技术中也因为其采用国际通用密码算法作为安全模块,使得当前的区块链架构缺乏自主可控性,制约了区块链技术在我国的发展。国产密码算法的安全性、稳定性、自主可控性可弥补区块链在密码算法方面的缺陷。因此,Frage-lamas等[34]提出基于国密算法的区块链架构——"国密链",以国密算法SM2、SM3替换国际通用密码算法的ECC、SHA-256。同时,针对当前区块链架构面临的共识算法妥协的现状,设计"可插拔共识"协议,解决当前区块链架构面临的共识算法不可更改的问题。实验结果表明,"国密链"与普通区块链架构在一致性、有效性相近的情况下,拥有更高的共识效率、更低的资源开销。"基于国密算法的区块链架构研究"是一套以区块链作为存储媒介及基础网络架构,并将区块链核心密码算法替换为国产商密算法的新型通用区块链架构模型,其主要目的为通过以国密算法替换比特币中通用密码算法的方式,在保证区块链功能简洁高效的同时,实现区块链的安全并自主可控,是一次将区块链技术与国产密码技术相结合的科技创新。

3.3.2 二级证书

二级证书机制由开源联盟链Hyperledger Fabric设计并提出。二级证书指的是注册证书(Ecert)和交易证书(Tcert)。Fabric中的成员管理服务为区块链网络提供了基于PKI的身份管理机制,实施交易的权限管制。成员管理服务利用注册-交易两级安全证书体系实现前台匿名、后台可监管的需求。

Jovic´等[35]提出了一种改进方案,针对证书公钥生成过程中复杂的密钥派生算法进行了优化,不仅提高了密钥派生算法的效率,而且减少了Tcert证书的存储空间,降低了数据库密钥存储的压力。同时,改进后的方案同样满足交易的匿名性、无关联性和可监管性。

3.3.3 访问控制

访问控制是改善工业物联网系统隐私和安全性的一个关键方面。联盟是一个由2个或2个以上的机构、企业和公司组成的团体,它们合作实现共同目标或形成资源库,以实现共享经济。然而,大多数访问控制方法都基于集中式解决方案,这可能导致数据泄漏和单点故障等问题。区块链技术具有其固有的分布式特征,可以解决传统访问控制方案的集中式问题。然而,区块链本身也有一些局限性,比如缺乏可扩展性和性能差。为了弥补这些局限,Fortuna等[36]提出一种基于分散能力的访问控制体系结构,该体系结构设计用于工业物联网联盟网络。该解决方案使用基于区块链的数据库,以获得更好的性能,显示了区块链和传统数据库的良好特性,可满足企业和业务的需求,并适用于不同的工业物联网互操作性场景。

4 工业区块链应用现状

在工业区块链应用方面,已有国内外许多学者和研究团队针对工业区块链的应用现状作了综述性观察分析和研究,应用领域包括智能制造、物联网、能源、教育、供应链、电子商务、知识产权确权、医疗等[5,37-45]。在细分领域方面,已有不同团队针对汽车、水运、食品等领域就如何结合工业区块链开展场景应用作了研究[46]。

工业互联网产业联盟等发布的《工业区块链应用白皮书》(以下简称《白皮书》)也着重探讨了工业区块链的应用原理、应用架构、应用场景、应用价值、应用案例等[47]。基于区块链的高安全可信、多方验证、无需第三方中介等优势,工业区块链的应用主要分为两方面:一是企业层区块链应用,包括企业内数据安全共享和企业内设备安全管理;二是产业层区块链应用,包括产业链协同和产融协同。企业层应用方面,主要解决设备身份管理、设备访问控制和设备生产流程管理。产业链协同应用方面,《白皮书》指出,产业链协同网络由多方构成,从产品生产端到消费端。产业链主体地理位置分散、难以交互,提高了多方协同的门槛和复杂度。通过工业区块链技术,可以实现信息资源共享,从而提升透明度和协同性。例如,通过工业区块链实现供应链可视化、工业物流管理、分布式生产和工业品回收利用等。产融协同应用方面,基于产业体系内部可信业务信息,金融业务可以嵌入开

展,形成产融协同新模式。通过工业区块链平台的共享账本,可以实现产业运作真实过程数据的共享,实现对目标客户提供多样化、定制化金融服务的目的。例如开展工业企业供应链金融、工业设备融资租赁、工业设备二手交易、新能源消纳等场景应用。

5 展望

区块链在许多领域仍处于起步阶段,需要进一步研究和开发。区块链收益的前景是强大的,但目前仍难以充分挖掘这些收益的潜力,其中很多问题是由前面讨论的要求决定的。任何工业应用的主要问题是安全和隐私引入使可能的解决方案进一步复杂化。尽管已做出了相当大的努力,但仍然难以在所有类型的区块链工业应用程序的可接受水平上实现安全性,必须解决各种限制条件和问题,例如资源的可用性、性能和所需的保护水平。

另一个需要考虑的领域是使用区块链来启用以前不可能实现的新业务模型。在这种情况下,考虑如何开发、部署和测量这些新模型很重要,必须考虑各种不确定性。由于目前没有模型来衡量,许多行业不愿进入新的商业模式。而研究人员和工业社区需要在管理、控制、测量和质量等方面仔细分析,以获得区块链支持的新的商业模型。

此外,部署区块链工业应用程序必将涉及到与当前操作系统的集成。其中一些系统是现代的,很容易与新的应用程序集成,然而在许多组织和行业中仍有诸多遗留应用程序在使用。当新应用程序需要使用或与这些遗留系统交互时,将产生另一个问题。在很大程度上,不同类型的应用程序和系统之间的有效集成是有问题的,需要仔细地分析并使用有效的方法促进集成,同时保留遗留系统的原始操作标准。

当前,工业区块链尚未实现大规模应用,甚至小规模应用也无从谈起。抛开政策、法规和行业标准等因素,其主要原因仍在于工业区块链自身技术并不成熟,不能够有力支撑工业互联网的全面应用,导致业界对工业区块链的认知度和重视度不高。因此,未来工业区块链发展的主要突破口在于相关技术的发展,尤其要在贴近工业互联网应用场景,在交易性能效率、跨链数据通信等方面着重发力。

在区块链"不可能三角"的约束下,要结合工业互联网的场景特点。例如上链用户一般是工商登记后可信的用户,那么在安全性方面可以稍作放松,从而把重点放在性能改进上。又如,根据企业业务特点,在利用区块链时,可能仅有 2 个节点或少数节点上链,此时可以考虑区块容量的扩大或缩小区块的生成间隔。总之,要结合工业区块链的具体应用场景进行技术选型的优化。可以从链上和链下两方面出发开展多目标优化研究,搭建性能优化模型。总体来看,可以从以下几个方面开展技术研究和技术方案优化:(1)开展区块参数、数据隔离见证、DAG 数据存储等研究,实现区块链基础链上性能优化;(2)开展分布式并行计算分片、多共识机制融合研究,在分片中引入激励机制,在共识中引入随机算法,在提高性能和安全性的同时为链下扩容打好可行性、安全性基础;(3)融合状态通道、侧链等链下方案技术优势,研究适配的智能合约、网络通信技术,完成链下性能优化。综合 TPS 交易性能和去中心化安全要求等,搭建高效可用的区块链模型,支撑区块链开展广泛的行业应用。另外,云服务模式下的区块链服务,把区块链作为基础设施来满足不同用户的需求,即区块链即服务的模式(Blockchain as a Service,BaaS)将会是一个重要发展方向。

当前,仍有许多有待解决的问题需进一步研究和分析,以创建更可行和有效的工业应用程序,以充分受益于区块链,并实现预期的目标。这些开放问题的例子包括安全性、隐私、可伸缩性、与其他系统的集成(更具体地说是与遗留系统的集成),以及法规和接受问题。该领域未来的工作需要解决这些问题,并缩小更高效、可扩展和安全的区块链工业应用程序的差距。

参考文献

[1] 杨帅.工业 4.0 与工业互联网:比较,启示与应对策略[J].当代财经,2015(8):99-107.

[2] 谢文.工业互联网是对传统产业的重定义[EB/OL].[2021-08-05].https://www.tmtpost.com/44668.html.

[3] NOFER M,GOMBER P,HINZ O,et al. Blockchain [J]. Business & Information Systems Engineering,2017,59(3):183-187.

[4] 谢家贵,李海花.区块链与工业互联网协同发展构建新基建的思考[J].信息通信技术与政策,2020(12):38-45.

[5] BODKHE U,TANWAR S,PAREKH K,et al. Blockchain for industry 4.0:A comprehensive review [J]. IEEE Access,2020,8:79764-79800.

[6] 杨耀东,周期,杜挺.区块链性能提升技术[M].北京:北京邮电大学出版社,2020.

[7] 潘晨,刘志强,刘振,等.区块链可扩展性研究:问题与方法[J].计算机研究与发展,2018,55(10):2099-2110.

[8] 上海万向区块链股份公司.基于区块链的虚拟机内存自动扩容系统和方法:CN202011505434.9[P].2021-03-19.

[9] DOUCEUR J R. The sybil attack [C]//International Workshop on Peer-to-peer Systems. Berlin, Heidelberg:Springer,2002:251-260.

[10] ÖZYILMAZ K R,PATEL H,MALIK A. Split-scale: Scaling bitcoin by partitioning the UTXO space [C]//2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS). Beijing, China:IEEE,2018:41-45.

[11] PINZÓN C,ROCHA C. Double-spend attack models with time advantange for bitcoin [J]. Electronic Notes in Theoretical Computer Science,2016,329:79-103.

[12] HAFID A,HAFID A S,SAMIH M. Scaling blockchains: A comprehensive survey [J]. IEEE Access, 2020,8:125244-125262.

[13] ZYSKIND G,NATHAN O,PENTLAND A S. Decentralizing privacy:Using blockchain to protect personal data [C]//2015 IEEE Security and Privacy Workshops. San Jose,CA,USA:IEEE,2015:180-184.

[14] 孙知信,张鑫,相峰,等.区块链存储可扩展性研究进展[J].软件学报,2021,32(1):1-20.

[15] BENET J. IPFS-content addressed,versioned,p2p file system[Z]. [2021-09-03]. https://ui. adsabs. harvard. edu/abs/2014arXiv1407. 3561B/abstract.

[16] 孙恩昌,姚勇锋,王勇,等.一种基于区块链和星际文件系统的企业间标准共识方法:CN201911090615.7[P].2020-03-06.

[17] XIE J F,YU F R,HUANG T,et al. A survey on the scalability of blockchain systems [J]. IEEE Network, 2019,33(5):166-173.

[18] MATTHEWS W,COTTRELL L. The PingER project: Active Internet performance monitoring for the HENP community [J]. IEEE Communications Magazine,2000,38(5):130-136.

[19] ALI S,WANG G J,WHITE B,et al. A blockchain-based decentralized data storage and access framework for PingER [C]//2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). New York,NY,USA:IEEE,2018:1303-1308.

[20] ALI M. Trust-to-trust design of a new Internet [D]. Princeton:Princeton University,2017.

[21] HE G B,SU W,GAO S. Chameleon:A scalable and adaptive permissioned blockchain architecture [C]//2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). Shenzhen,China:IEEE,2018:87-93.

[22] POON J,DRYJA T. The bitcoin lightning network: Scalable off-chain instant payments (2016) [EB/OL]. (2016-04-19)[2021-09-23]. https://lightning. network/lightning-network-paper. pdf.

[23] 邵奇峰,金澈清,张召,等.区块链技术:架构及进展[J].计算机学报,2018,41(5):969-988.

[24] FRANKENFIELD J. Hashed timelock contracts (HTLC)[Z/OL]. Cryptocurrency: Cryptocurrency Strategy & Education. (2021-02-11)[2021-09-03]. https://www. investopedia. com/terms/h/hashed-timelock-contract. asp.

[25] 王驰宇.区块链闪电网络的研究与实现[D].成都:电子科技大学,2018.

[26] PETERSON D. Sparky: A lightning network in two pages of solidity [EB/OL]. (2016-07-19)[2021-09-02]. https://www. blunderingcode. com/a-lightning-network-in-two-pages-of-solidity/.

[27] MILLER A K,BENTOV I,KUMARESAN R,et al. Sprites:Payment channels that go faster than lightning [J/OL]. Computer Science, 2017, Corpus ID: 14781824(aRXiv). [2021-09-03]. https://arxiv. org/pdf/1702. 05812. pdf.

[28] TRINITY. Universal off-chain scaling solution. [P/OL]. [2020-01-28]. https://trinity. tech/#/writepaper.

[29] KWON J,BUCHMAN E. Cosmos whitepaper:A network of distributed ledgers [EB/OL]. [2020-10-08]. https://v1. cosmos. network/resources/whitepaper.

[30] KWON J. Tendermint:Consensus without mining [Z/OL]. [2021-09-03]. http://diyhpl. us/~bryan/papers2/bitcoin/tendermint_v03. pdf.

[31] DENG L P,CHEN H,ZENG J,et al. Research on cross-chain technology based on sidechain and hash-locking [C]//International Conference on Edge Computing. Cham:Springer,2018:144-151. DOI:10. 1007/978-3-319-94340-4_12.

[32] FUSION. An interoperable ecosystem for financial innovations [EB/OL]. [2021-08-08]. https://www. fusion. org/en.

[33] ZHENG Z B,XIE S A,DAI H N,et al. Blockchain challenges and opportunities:A survey [J]. Internation-

al Journal of Web and Grid Services,2018,14(4):352-375. DOI:10.1504/IJWGS.2018.095647.

[34] FRAGA-LAMAS P,FERNÁNDEZ-CARAMÉS T M. A review on blockchain technologies for an advanced and cyber-resilient automotive industry [J]. IEEE Access,2019,7:17578-17598.

[35] JOVIĆ M,FILIPOVIĆ M,TIJAN E,et al. A review of blockchain technology implementation in shipping industry [J]. Pomorstvo,2019,33(2):140-148. DOI:10.31217/p.33.2.3.

[36] FORTUNA F,RISSO M. Blockchain technology in the food industry [J]. Symphonya. Emerging Issues in Management,2019(2):151-158. DOI:http://dx.doi.org/10.4468/2019.2.13fortuna.risso.

[37] FERNANDEZ-CARAMES T M,FRAGA-LAMAS P. A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories [J]. IEEE Access, 2019, 7: 45201 - 45218. DOI: 10.1109/ACCESS.2019.2908780.

[38] ASANTE M,EPIPHANIOU G,MAPLE C,et al. Distributed ledger technologies in supply chain security management: A comprehensive survey [Z]. IEEE Transactions on Engineering Management,2021:1-28. DOI:10.1109/TEM.2021.3053655.

[39] 蔡晓晴,邓尧,张亮,等.区块链原理及其核心技术[J].计算机学报,2019,44(1):84-131.

[40] LONE A H,NAAZ R. Applicability of blockchain smart contracts in securing internet and IoT:A systematic literature review [J]. Computer Science Review, 2021, 39: 100360. DOI: 10.1016/j.cosrev.2020.100360.

[41] ISMAIL L,MATERWALA H. A review of blockchain architecture and consensus protocols:Use cases,challenges,and solutions [J]. Symmetry, 2019, 11(10): 1198. DOI:10.3390/sym11101198.

[42] ALLADI T,CHAMOLA V,PARIZI R M,et al. Blockchain applications for industry 4.0 and industrial IoT: A review [J]. IEEE Access, 2019, 7: 176935 - 176951. DOI:10.1109/ACCESS.2019.2956748.

[43] MUSHTAQ A,HAQ I U. Implications of blockchain in industry 4. O [C]//International Conference on Engineering and Emerging Technologies (ICEET). Lahore, Pakistan: IEEE, 2019: 1 - 5. DOI: 10.1109/CEET1.2019.8711819.

[44] KHAN M A,SALAH K. IoT security:Review,blockchain solutions,and open challenges [J]. Future Generation Computer Systems,2018,82:395-411.

[45] ZHANG Y Y,KASAHARA S,SHEN Y L,et al. Smart contract-based access control for the internet of things [J]. IEEE Internet of Things Journal, 2018, 6(2):1594-1605. DOI:10.1109/JIOT.2018.2847705.

[46] REJEB A,KEOGH J G,ZAILANI S,et al. Blockchain technology in the food industry:A review of potentials, challenges and future research directions [J]. Logistics,2020,4(4):27. DOI:10.3390/logistics4040027.

[47] 工业互联网产业联盟.工业区块链应用白皮书[EB/OL].[2021-08-05]. https://www.aii-alliance.org/upload/202009/0907_221833_524.pdf.

Progress of Industrial Blockchain Technology

HUANG Tinglei[1],DENG Song[2],ZHANG Zi[3],HAN Xiaoyu[1],JIANG Jianhui[4],ZONG Yunbing[5]

(1. Institute of Software Chinese Academy of Sciences,Beijing,100080,China; 2. Nanjing University of Posts and Telecommunications,Nanjing,Jiangsu,210003,China; 3. Guilin University of Electronic Technology,Guilin,Guangxi,541004,China; 4. Guangxi Academy of Sciences, Nanning, Guangxi, 530007, China; 5. Shandong Institutes of Industrial Technology, Ji′nan, Shandong, 250102,China)

Abstract:Industrial Internet is accelerating,among which the problem of data privacy disclosure,data security and data tracing have seriously restricted the information flow and data sharing among enterprises. As a decentralized,intermediary-free,non-tampering and traceable technology,blockchain is widely used in the fields of finance and virtual currency. The application of blockchain technology can effectively solve the application

problems of industrial Internet. The connotation and application status of industrial blockchain are introduced in detail, the key technology of industrial blockchain and the problems faced by industrial application are analyzed emphatically, and the research progress of related technologies at home and abroad are introduced in this paper.

Key words: industrial Internet, industrial blockchain, transaction performance, cross chain interaction, distributed ledger

责任编辑:陆　雁

投稿指南

1　来稿要求

1.1　稿件要素

稿件内容必须包括题目、作者姓名、作者所在单位、作者所在省份和城市、邮政编码、中文摘要、关键词、英文题目、作者英文姓名、作者英文单位、英文摘要、英文关键词、正文、致谢(非必选)、参考文献等内容。

1.2　题目

应以简明、确切的语言反映稿件的重要思想和内容,一般不超过20字。

1.3　作者与单位

多位作者姓名用逗号隔开。所有作者均须注明所在单位全称、省份城市及邮编。

1.4　汉语姓名译法

姓在前名在后,姓用大写字母,名首字母大写(如:欧阳奋发,OUYANG Fenfa)。

1.5　中、英文摘要

用第三人称撰写,应完整准确概括论文的实质性内容,试验研究论文摘要须包含目的、方法、结果、结论4个要素。英文摘要与中文摘要内容相对应。

1.6　首页脚注标识要素

资助项目:项目名称(项目编号)。作者简介包括姓名(出生年—),性别,职称或职务,主要研究方向。如有通信作者,请注明×××为通信作者,包括姓名(出生年—),性别,职称或职务,主要研究方向,E-mail。

1.7　稿件正文

试验研究论文应包括引言、材料与方法、结果与分析、讨论、结论等要素。引言须包含研究意义、前人研究进展、本研究切入点、拟解决的关键问题等基本内容,“讨论”与“结论”部分须分开阐述。各层次标题用阿拉伯数字连续编号,如0;1,1.1,1.1.1……;2,2.1,2.1.1……层次划分一般不超过3级。

1.8　参考文献

参考文献表采用顺序编码制组织,其编排格式示例如下:

[1]　陈宝玲,宋希强,余文刚,等.濒危兰科植物再引入技术及其应用[J].生态学报,2010,30(24):7055-7063.

[2]　CHEN B L,SONG X Q,YU W G,et al. Re-introduction technology and its annlication in the connervation of endangered orchid [J]. Acta Ecologica Sinica,2010,30(24):7055-7063.

1.9　图和表

稿件可附必要的图和表,表用三线表表示,忌与文字表述重复,表的主题标目要明确。图表名、图表注及图表中所有的中文须有英文对照。图要大小适中,清晰,标注完整;照片尽量选用黑白照片。

1.10　量和单位

量名称及其符号须符合国家标准,采用法定计量单位(用国际通用符号,如面积单位“亩”换算成“公顷 hm^2”)。书写要规范化,并注明外文字母的大小写、正斜体及上下角标。容易混淆的字母、符号,请特别注明。

2　注意事项

2.1　本刊已开通网络投稿系统,投稿请登录 http://gxkx.ijournal.cn/gxkx/ch/index.aspx,使用网上投稿和查稿系统。我刊审稿周期为1个月,1个月后未收到审稿结果可另投他刊。

2.2　稿件一经采用,酌收版面费;刊登后,付稿酬含网络发行(《中国学术期刊(光盘版)》、中国期刊网、万方数据网及台湾华艺CEPS中文电子期刊服务网等)的稿酬,同时赠送样刊2本。

2.3　本刊入编《中国学术期刊(光盘版)》、中国期刊网、万方数据网及台湾华艺CEPS中文电子期刊数据库并已签订CNKI优先数字出版合作协议。

2.4　囿于人力、物力有限,我刊只通过期刊采编系统发送“稿件处理意见”,如需纸质意见,请向编辑部索取。