Blockchain for Edge AI Computing: A Survey (□□□□□□□□□□□□□□□□□□□)

Article · January 2020

DOI: 10.3969/j.issn.0255-8297.2020.01.001

4 authors, including:

Kai Lei
Peking University
161 PUBLICATIONS **605** CITATIONS

SEE PROFILE

DOI: 10.3969/j.issn.0255-8297.2020.01.001

• 特邀论文 •

面向边缘人工智能计算的区块链技术综述

方俊杰[1, 2], 雷 凯[1, 2]
1. 北京大学 信息工程学院 深圳市内容中心网络与区块链重点实验室, 深圳 518055
2. 北京大学 互联网研究院 (深圳), 深圳 518055

摘 要: 区块链构建了一个分布式点对点的系统, 作为一种安全可验证的分散确认事务的机制, 广泛应用于金融经济、物联网、大数据、云计算和边缘计算领域. 边缘人工智能计算(edge AI computing) 即面向边缘网络应用场景的群智 AI 计算模式. 在无人驾驶等高动态、超低延时、资源受限、数据与计算解耦的边缘网络应用场景下, 跨域可信、隐私保护、入侵监测、细粒度激励等需求对区块链研究提出了进一步的挑战. 关注到人工智能向边缘网络下放的趋势, 该文讨论区块链在新兴的边缘人工智能计算领域的应用. 首先介绍了区块链技术的基础架构, 概述了相关研究和应用方向; 接着从边缘人工智能计算的概念与兴起出发, 详细分析并讨论了区块链技术在面向边缘人工智能计算领域的应用需求, 包括相关研究综述、应用趋势和未来研究方向. 此外, 还总结了区块链技术应用在边缘人工智能计算方面的优势和未来仍需关注的问题.

关键词: 区块链; 边缘人工智能计算; 泛中心; 群智计算
中图分类号: TP399 **文章编号:** 0255-8297(2020)01-0001-21

Blockchain for Edge AI Computing: A Survey

FANG Junjie[1,2], LEI Kai[1,2]
1. Shenzhen Key Lab for Information Centric Networking & Blockchain Technology, School of Electronics and Computer Engineering, Peking University, Shenzhen 518055, China
2. Internet Development Research Institution (Shenzhen), Peking University, Shenzhen 518055, China

Abstract: Blockchain builds a distributed point-to-point system, which is widely used in the fields of financial economy, Internet of Things (IoT), big data, cloud computing and edge computing. Meanwhile, edge artificial intelligence (AI) computing refers to the emergence of swarm intelligence AI computing model for edge network application scenarios. Although featuring in the characteristics of high dynamic, ultra-low delay, resource limitation, data calculation decoupling in application scenarios of edge networks such as intelligent car, blockchain faces further challenges including cross-domain trust, privacy protection, intrusion monitoring and fine-grained incentives. Focusing on the trend of transforming the algorithm and application of AI from cloud centers to the edges of networks, this paper

收稿日期: 2019-11-14
基金项目: 国家重大科技基础设施基金 (发改高技[2016] 2533号); 深圳市内容中心网络与区块链重点实验室基金 (No.ZDSYS201802051831427) 资助
通信作者: 雷凯, 副研究员. 研究方向为命名数据网络、区块链、联邦学习. E-mail: leik@pkusz.edu.cn.

discusses the application of blockchain in the emerging edge AI computing research. We first introduce the infrastructure of blockchain and summarize related researches and application directions. Then, beginning with the concept and rise of edge AI computing, the application requirements of blockchain in edge AI computing are analyzed and discussed in detail, including relevant research review, application trend and future research direction. Additionally, we summarize the advantages of applicating blockchain in edge AI computing and the deficiencies need to be addressed in the future.

Keywords: blockchain, edge artificial intelligence (AI) computing, ubiquitous centralization, crowd computing

区块链作为比特币的底层支撑技术，能在泛中心环境下以安全可验证的方式构建分类账，因而得到了广泛关注. 在区块链中，网络中的任何节点都可以进行事务的验证和转发. 所有节点共同维护包含事务的区块有序链接的分类账，从而构建了一个无法篡改的、全网一致的状态记录[1]. 因此，除了应用于数字货币领域外，区块链技术也正在改变着各种无信任环境下的交易模式[2]. 区块链可用于记录交易、消息传递、身份认证和访问控制管理等，在建立更安全的系统上具有相当大的潜力[2-3]. 虽然区块链技术呈现出极具潜力的应用需求，但考虑到区块链本身的特性和限制因素，针对其实际应用领域的探索工作也是学界的研究重点.

2017 年出现的云–边缘人工智能系统的概念[4]，催生出边缘人工智能计算的研究方向和发展. 随着物联网和移动计算的普及，分散的终端设备产生的海量数据存储在大量的边缘节点上，为人工智能应用提供数据来源. 然而，传统的以云计算为主的架构面临着数据收集的成本问题、终端敏感数据的隐私保护问题、终端数据与云计算交互的时延问题等，越来越无法满足当前人工智能的数据需求. 因此，将中心的计算和存储下放到边缘网络的新型人工智能范式逐渐成为一个具有重要意义的研究方向[5-7].

区块链天然的泛中心分布式可信特性为设计边缘人工智能计算的框架与范式提供了新的思路. 在边缘人工智能计算中，运行人工智能算法的多个设备分散在边缘网络中. 为了协作完成人工智能计算任务或联合进行智能群体决策，这些设备之间需要频繁通信. 然而，无论是设备本身还是设备间的通信都面临着多种网络安全攻击的威胁，如设备有可能发生故障或存有恶意，在这种情况下传输的信息可能泄露或被篡改. 区块链作为一种由密码学支撑的、可验证的、不可篡改的分类账，可以通过事务记录和对事务记录有效性的分布式共识来保障分散不可信环境中的安全交互，正好可以在边缘人工智能计算的场景下发挥作用. 同时，区块链的共识机制与激励机制配合智能合约天然适合构建一个经济市场，可以有效激励边缘人工智能计算中信息的共享与交互.

在现有的文献中，有研究人员对区块链、边缘计算与人工智能分别进行了综述，也有研究人员着眼于区块链与边缘计算[8]的结合或区块链与人工智能的结合[9]. 不过就区块链在边缘人工智能计算环境下的作用而言，到目前为止还缺乏探索性研究和综述工作. 为此，本文从区块链技术的架构出发，概述了区块链方向的相关研究成果；结合人工智能和边缘计算的发展，介绍了边缘人工智能计算的概念和发展需求；面向边缘人工智能计算的需求，详细分析并讨论了区块链技术与边缘人工智能计算相结合的需求及其发展方向；总结出区块链技术在边缘人工智能计算领域的应用优势和探索方向.

1 区块链及其研究概述

1.1 区块链技术背景

自 2008 年中本聪发表比特币白皮书[1]以来，区块链作为比特币的底层技术得到了广泛的

关注与讨论[10]. 简单来说，区块链是一个开放的、分布式的数字账本，以可验证且不可篡改的方式有效地记录各方之间的交易. 与传统的中心化账本系统相比，区块链系统中的所有参与节点通过共识算法共同维护分布式分类账. 区块链中的区块对其数据结构有严格的规范要求，其中所有的区块头都记录其先前区块的加密散列值，以确保历史事务记录的完整性与一致性.

从更广泛的意义上来说，区块链也可以作为一种底层框架. 区块链框架可以细分为网络层、数据层、应用层[2]，如图 1 所示. 数据层一般会给出区块链的数据记录类型和数据结构. 数据记录也被称作事务(transaction)，这些事务是特定时间发生的节点之间特定交互动作的证据，比如比特币中事务记录的是资金的转移. 从数据结构的角度来看，以比特币为代表的典型区块链是一系列不断增长的含有事务的区块的链表. 如图 2 中的(a)所示，一个区块通常由区块头和包含一系列事务的区块体组成. 每个区块包含一组新的事务，以及前一个块的散列值，以便将当前块链接到前一个块. 散列值和时间戳的设计使得修改记录变得困难，因为每一个区块都依赖于前一个区块和当前时间. 除了链式结构之外，近年来出现了基于有向无环图(directed acyclic graph, DAG)的新型数据结构[11]. 如图 2(b)所示，基于 DAG 结构的区块链消除了区块的概念，这样每个交易都是分布式账本中链接的单个节点. 这些节点不受单一主链的约束，它们之间的关系就像一张纠缠的网.

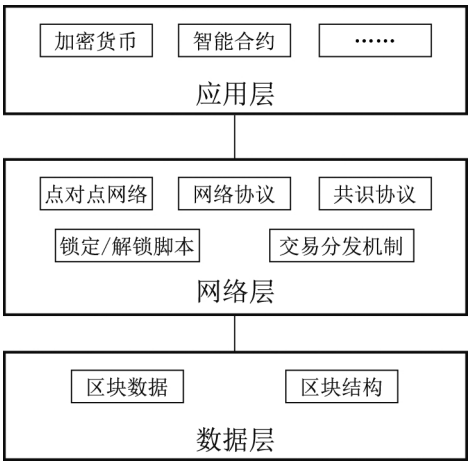
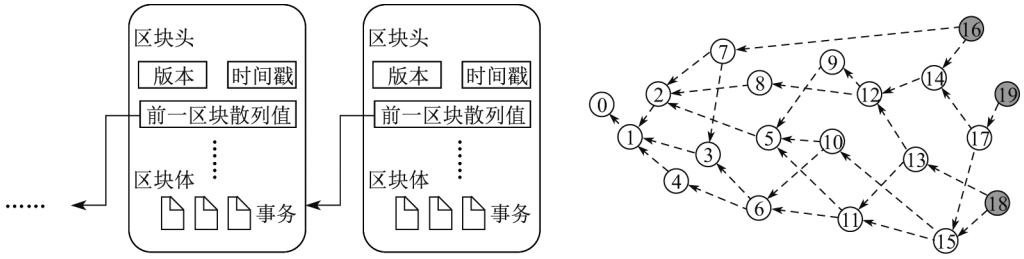


图 1　区块链框架

Figure 1　Blockchain framework



(a) 链式结构区块链
(a) Chain structure of blockchain

(b) 有向无环图结构区块链
(b) DAG structure of blockchain

图 2　区块链数据结构

Figure 2　Blockchain data structure

网络层则泛指整个应用区块链的交互环境，除了包括分布式点对点网络和在该网络运行的网络协议（如常见的 TCP/IP 协议）以及最重要的用于分布式网络生成新区块的共识机制外，还包括在用户之间更新和分发区块链的协议设计. 网络协议并不仅仅局限于当前的 TCP/IP 协议. 已有一些研究在未来新型网络架构的协议下部署区块链，比如命名数据网络(named data networking, NDN)[12]. 共识机制或共识算法是区块链系统的关键组成部分，由于没有中心节点来确保分布式节点上的账本都是相同的，区块链就需要一些协议来确保不同节点中的存储副本是一致的[3].

工作证明(proof of work, PoW)是在比特币网络[1]中使用的一种共识算法，该算法要求网络中的每个节点都计算一串特定的哈希散列值. 如果计算出的目标散列值的正确性得到了其他所有节点的验证，则该节点将会获得产生新区块的权利. 整个工作证明的过程被称为挖矿，计算散列值的节点被称为矿工. 矿工们不得不进行大量的计算，然而这些计算除了挑选出一个记录事务的节点外，并没有其他实际意义，因而这种共识因浪费太多的资源而被批判. 以太坊提出的股权证明(proof of stake, PoS)[13]是 PoW 的改进，此时矿工改为证明货币数量的所有权，而不是利用自己的算力计算没有特定含义的哈希散列值. 相比之下减少了资源浪费的现象，因此选出下一个生成区块节点的过程也更高效. 文献 [14] 使用的股权委托证明(delegated proof of stake, DPoS)是 PoS 的改进形式. DPoS 被认为是一种代议制民主，由节点投票选择出特定数目的代理节点来生成并验证区块. 因为验证块的节点数明显减少，所以加快了区块的确认速度，使事务得到了更快的确认. 实用拜占庭容错算法(practical Byzantine fault tolerance, PBFT)是可以容忍拜占庭故障的算法，整个共识过程分为预准备、准备和响应 3 个阶段. 在每个阶段，如果一个节点获得了所有节点中 2/3 以上的投票就可以进入下一个阶段. 因为要为节点投票，所以网络中的节点被要求掌握其他所有节点的信息并与之进行通信，可见该算法不太适用于网络规模较大的情况. PBFT 更多地用于节点数量较少的联盟链或者私有链，比如 Hyperledger Fabric[15]. 表 1 比较了这 4 种常见的共识算法，而最近又出现了许多改进的共识算法和全新的共识算法.

表 1 4 种典型共识算法比较

Table 1 Comparison of four typical consensus algorithms

常见共识算法	如何产生新区块	如何挑选节点	故障节点容忍率	缺陷	典型使用系统
PoW	挑选节点生成	算力	$< 51\%$	消耗算力资源	比特币
PoS	挑选节点生成	代币数量	$< 51\%$	拥有大量代币的节点可能主导区块链	点点币(Peercoin)
DPoS	挑选节点生成	节点投票数&代币数量	$< 51\%$	牺牲了一定的去中心化特性	比特股(Bitshares)
PBFT	主节点依据各节点发回的响应生成	/	$< 1/3$	适用于节点数量较少的联盟链或私有链	Hyperleder Fabric

应用层提供了各种应用程序. 区块链最常见的应用是以比特币为代表的数字加密货币，而另一个广泛的应用是智能合约. 智能合约的引入标志着区块链进入了 2.0 时代[16]. 智能合约依托区块链的分散共识机制，允许相互不信任的用户在不需要任何第 3 方可信的授权和监管

下完成数据交换或交易. 以太坊是目前使用最广泛的支持智能合约的区块链，多种多样的智能合约应用是基于以太坊进行开发的[13]. 当前，区块链作为一种可行解决方案可用于增强系统的可信性和安全性[17-22]，包括物联网(Internet of Things, IoT)、金融经济、云计算和边缘计算等.

自从区块链用于比特币等加密货币以来，随着工业界和学术界对其技术和应用的不断探索，人们对区块链的兴趣一直在增加[2-3]. 与此同时，学术界也在不断地改进区块链技术的数据层和网络层，以获得更好的性能为上层应用提供服务.

1.2　区块链技术研究简述

针对区块链的研究可以简单地分为两类：一类是对区块链自身加以改进，另一类则是将区块链作为一种解决方案应用于各种场景.

1.2.1　区块链自身改进

改进区块链自身的研究具体分为三部分：一是提出新的区块链共识算法以改进现有共识算法的不足，二是解决区块链的可拓展性问题，三是针对区块链系统的攻击问题给出解决方案.

在 PoW 算法中，各节点所计算出的都是一串具有特殊前缀的散列值，这样的计算不但没有附加价值，而且浪费了太多的资源. 因此，文献 [23] 提出将各节点计算无意义的哈希散列值改为计算额外的具有潜在科学价值的特殊素数，且使用这样的特殊素数可以保持 PoW 的一些重要特性，如被其他节点有效验证、不可重用、难度可调整. 在 PoW 算法中，每个区块的产生都要等待一个散列值的计算和验证，且一个区块因大小限制而导致包含的事务有限，因此系统吞吐量并不太高. 为了在保障区块链系统安全性不受影响的前提下提升系统吞吐量，文献 [24] 提出将共识过程解耦为两个操作：一是选举产生新区块的领导者，二是将事务序列化添加到区块链中. 这种算法不太频繁地随机选出领导者，并由领导者单方面主导将该时期内的事务添加到区块链中. 与此类似，文献 [25] 引入可验证随机函数(variable random function, VRF)来选举产生新区块的领导者. VRF 的特性保证了下一个领导者节点不可被预测，且随机产生的领导者可以被其余节点所验证.

区块链可拓展性问题可以分为 3 类：吞吐量问题、成本问题、容量问题[26]. 具体描述如下：1）比特币作为一种交易系统，目前每秒处理的事务大约是 7 笔，远落后于 Visa 系统每秒处理的上万笔[27]. 由于块大小的限制，区块链存在等待事务被包含到块中的问题. 如果为此缩短生成区块的间隔时间，就可能造成区块链分叉的问题. 2）根据比特币和以太坊的现有机制，用户创建一个事务需要向矿工付费，这是成本问题. 3）节点需要存储自创世区块以来全部的区块副本，如果所有的事务都存储在一个链中，那么这个链的账本容量就会变得太大而无法维护，这是容量问题. 目前以太坊的区块存储大小是 444.06 GB，已经是一个较大规模的体量[28].

第 1 种提高可拓展性方案的思路是更改比特币区块链的数据结构或交易确认方式. 文献 [11] 提出了基于有向无环图的结构，并将其称之为 Tangle. 链式结构的区块链要求将新事务附加到主链之前对其进行验证，以保证节点之间同步的一致性. 与之不同的是，Tangle 采用了异步一致的方式，在提交新事务之前节点必须验证两个以前的事务. 这两个被验证的事务已附加到有向无环图中但没有得到网络中其他节点规定次数的确认，之后节点运行 PoW 算法将这两个新的事务捆绑在一起广播到网络中. 每个新事务以后都将由其他更新的事务进行验证. 每个事务都有一个称为权值的度量，它与事务的验证次数成正比，权值越大，交易越难被篡

改. 理论上，这样的数据结构设计和交易确认机制可以提高网络吞吐量和系统响应时间. 权益证明协议(proof of property)[29]的提出可以在新事务中添加与当前系统状态有关的部分，这样其他节点无需存储完整的区块链也可以完成验证.

不改变区块链链式结构的性能提升方案进一步细分为链上解决方案、链下解决方案和跨链解决方案. 对于链上解决方案，最简单的方法是调整区块的大小和生成区块的间隔时间[30]，另外比较有代表性的是分片技术[31]. 分片技术可以类比于分布式数据库，其关键思路是将一个大型网络划分成一些小的委员会，每个委员会通过运行PBFT这样效率更高的共识算法来处理一组互不关联的事务. 分成多组委员会处理不同的事务不仅可以减少每个节点的负担，而且可以通过并行处理来提高整个系统吞吐量. 一个典型的链下解决方案是闪电网络[32]. 闪电网络主要用来提升比特币等电子支付系统的可拓展性，它的核心思想：不是每一笔交易事务都有必要放到区块中通过 PoW 共识得到全网确认，而是允许将一部分交易的记录和确认放到链下完成. 跨链解决方案提出可以通过多条相同类型或不同类型的区块链之间的相互合作来提供更丰富的功能和更强的性能，目标是将另一个区块链的功能引入当前的区块链，主要关注的是如何在多个区块链系统之间实现有效的通信和高效的数据传输[33-34].

大多数区块链面临的特有安全攻击是针对比特币网络的[10]. 51% 攻击是指具有全网一半以上的算力就可以操纵新区块的生成. 自私攻击是指为了获得不适当的奖励而浪费诚实矿工的计算能力[35]. 攻击者不广播挖掘到的区块而是私下持有，之后自私的攻击者们会在这条私有链上继续进行挖矿，并试图保持一条比公共链更长的私有分支. 边界网关协议(border gateway protocol, BGP)劫持攻击[36]是一种劫持路由延迟网络消息的攻击，因为一些比特币矿池高度集中，所以 BGP 劫持攻击的攻击者可以使比特币网络分叉，或者延迟块传播的速度. 僵尸网络攻击[37]是由具有不同 IP 地址范围的机器人发起的，通过独占受害者的输入输出信道将受害者节点与网络其他节点隔离，从而使受害者节点接收不到区块链的最新信息. 活跃攻击[38]则是针对以太坊网络的，该攻击能够尽可能地延迟目标事务的确认时间. 针对安全攻击问题，现有的主要解决方案是提出新的矿池[39].

1.2.2 典型区块链应用

区块链的应用大致可以分为以下几类：金融和市场领域应用、声誉系统、安全和隐私增强[3]. 区块链在金融和市场领域最广泛而知名的应用就是以比特币[1]、以太坊[13]等为代表的电子加密货币，除此之外在构建点对点金融市场、跨域金融资产的清算结算、供应链流程追溯管理[40]方面也有大量的应用. 对于构建声誉系统[41]，区块链可以解决电子商务声誉方案中利用注册大量的虚假客户以获得高声誉的问题. 声誉信息因为存储在区块链上，所以无法篡改，且所有声誉变化都很容易检测. 针对安全增强问题，区块链可以解决重要的中心节点的单点故障问题. 由于可以减小公私钥分发设备受到攻击的影响，区块链甚至可以帮助构建更加可靠的公私钥基础设施[42]. 针对隐私保护，基于区块链构建的数据存储系统可以在确保用户拥有数据所有权的同时保障用户的匿名性[43].

将区块链应用到物联网、车联网、边缘计算等场景时，会面临一个常见的问题：网络中存在大量资源受限的设备. 这些受限设备的存储计算处理能力十分有限，很难存储完整的区块链账本或运行较耗费计算资源的 PoW 共识算法. 因此，当区块链应用在这些场景时，通常会考虑将路由器、边缘服务器等纳入考虑范围来设计系统框架. 以边缘计算为例，终端设备被认为是资源受限的设备，其存储计算处理能力十分有限，不适合部署区块链. 因此，只在边缘服务器层和云服务器层部署区块链，而终端设备通过与边缘服务器通信连接获取区块链上的信息[44-45]. 文献 [46-47] 则考虑让终端设备和边缘服务器都参与到区块链中. 文献 [48-49] 定义

了 3 种类型的节点：轻量级节点、标准节点和交换级节点. 其中：类似终端设备的轻量级节点保留一个带有区块链地址和余额的钱包，只执行提出交易等任务；标准节点保存部分区块链的副本信息，主要是收集轻量级节点的交易或相应轻量级节点的查询；交换级节点则保存了区块链的完整副本记录并可以提供区块链的分析服务. 文献 [46-47] 均考虑使用联盟链管理物联网虚拟资源，并将物联网虚拟资源(代码或数据) 存储在区块中. 与此同时，在联盟链中注册的多个用户可以定义和部署自己的虚拟系统，并对区块进行读写.

2　边缘人工智能计算

2.1　人工智能概要

根据《人工智能—一种现代方法》[50]一书的定义，人工智能是一种被人类设计出来的可以将感知信息映射到行动的智能体，它可以根据环境采取理性的行为并做出决策. 人工智能一词虽然在近些年来得到了社会各界的广泛关注，但不是一个新的术语，而是经过了数十年的起起落落发展的研究领域[51]. 人工智能之所以重新崛起，得益于硬件水平发展的支撑以及机器学习和深度学习方面取得的新突破[52].

机器学习是一门不需要明确编程就能让计算机运行的技术. 在过去的十几年里，机器学习使得物联网、智慧城市、智慧医疗、自动驾驶汽车、语音识别以及人类基因组等诸多方面得到了更深入的研究[53-58]. 许多研究人员认为，机器学习技术是向高水平的人工智能发展的最佳途径[51]. 然而，传统的机器学习技术处理原始数据的能力有限，构造一个机器学习系统通常需要拥有丰富专业知识的专家帮助设计一个特征提取器，以便将原始数据转换成机器学习系统内合适的表示方式或者特征向量[52]. 深度学习方法是一种具有多层表示的表示学习方法，允许向机器输入原始数据并自动学习出所需的表示. 它通过组合简单但非线性的模块来完成这一任务，其中每个模块将一个级别的表示转换为一个更高的、更抽象的表示[52]. 正因为这样的特性，深度学习在发现高维数据中的复杂结构方面表现得非常出色，在科学、商业和政府的许多应用领域均取得了重大进展.

卷积神经网络(convolutional neural network, CNN)、循环神经网络(recurrent neural network, RNN)、长短期记忆(long short-term memory, LSTM)网络和去噪自编码器(de-noising auto encoder, DAE)是目前广泛应用的深度学习方法. 其中，CNN 是最为常见的深度学习架构之一，常用于图像处理方面. 它 包含 3 种不同的模块（又可称为层），分别为卷积层、池化层和全连接层. 最常见的卷积神经网络架构有 GoogLeNet[59]、VGGNet[60]、AlexNet[61]、ResNet[62]等. RNN 主要用来识别序列输入，比如语音、文本等信息，它利用循环的连接结构并根据循环计算处理输入数据. 相较于 CNN，RNN 会区分不同时间的输入[63]. 随着时间的推移，它的输出会进入下一个时间段，而不是在同一时间段内进入下一层，这样之前的所有输入数据就可以和当前的输入数据一起共同计算最后的输出. LSTM 网络可以被看成一种拓展的循环神经网络，它通常包含输入门、输出门和遗忘门 3 个核心模块，可以控制何时让输入信息进入神经元并在多大程度上将前一个时间段中计算的内容纳入当前计算的考虑范畴. LSTM 可用于文字、语音序列识别和图像处理等[64]，其主要优点在于它的输出是根据当前时间的输入来决定的. DAE[65]是一种用于从噪声数据集中学习特征的非对称神经网络，主要由输入层、编码层和解码层组成.

2.2　边缘计算兴起

边缘计算是一个与云计算相对的概念. 随着用户对服务质量(quality of service, QoS)的要求不断提升，为了解决从云到用户中间长时间延迟的问题，文献 [66-67] 提出云服务应该被转

移到更靠近终端用户的地方，即移动网络的边缘节点，这就是所谓的边缘计算. 边缘计算的概念涵盖了多种不同领域的技术，包括软件定义网络(software-defined networking, SDN)、面向服务计算（service-oriented computing, SOC）、计算机体系结构等，其核心思想是将计算和通信资源从云转移到网络的边缘节点上，从而为边缘的用户提供更快的服务与计算响应，减少中间不必要的通信延迟和网络拥塞.

边缘计算一词常与移动边缘计算（mobile edge computing, MEC）、雾计算(fog computing, FC）等概念混淆. 移动边缘计算的概念由欧洲电信标准协会于 2014 年提出[66]，具体定义为“在无线接入网(radio access network, RAN)中向移动用户提供 IT 服务环境和云计算能力”的新平台. 雾计算则被认为是边缘计算更一般化的概念，由思科公司在 2012 年提出[67]，是一种使得位于网络边缘的数十亿连接设备运行应用程序成为可能的计算范式. 值得注意的是：边缘计算、雾计算和移动边缘计算的研究领域通常是重叠的，而且这几个术语经常可以互换使用. 为了避免混淆，本文将统一使用边缘计算这一术语.

边缘计算范式的建立基于网络功能虚拟化(network function virtualization, NFV)、信息中心网络(information-centric networking, ICN)和软件定义网络(software defined network, SDN)等方面研究的最新进展[68-70]. 具体来说，网络功能虚拟化使得单个边缘设备能够向多个移动终端设备提供计算服务，这样单个的边缘设备可以创建多个虚拟机来同时执行不同的任务或操作不同的网络功能. 信息中心网络则为边缘计算提供了一个端到端的服务识别范式，从以主机为中心转换为以信息为中心而实现可以感知内容的计算. 同时，软件定义网络允许网络管理员通过服务抽象来管理服务，以实现动态的可伸缩的计算.

边缘计算对于系统中的移动运营商、服务提供商和终端用户都是有利的[71]. 移动运营商能够以更加灵活便捷的方式部署它们的服务，比如提供存储资源、计算资源或者其他IT资源，同时根据所使用的服务进行收费而获利. 服务提供商们可以提供支持更高带宽和更低时延的服务并从这种更好的服务中获取利润. 对于终端用户来说，由于与服务者的物理距离更短以及无线接入网更加密集，用户体验可以得到有效提升，比如获得更高吞吐量的浏览、更快的视频缓存和更及时的域名系统相关服务等.

2.3 边缘人工智能计算(edge AI computing)

2.3.1 人工智能与边缘计算结合趋势

近年来，一种被称作边缘人工智能计算或边缘智能（edge AI/edge intelligence）的研究正获得越来越多的关注. 2017 年，美国加州大学伯克利分校发布的有关人工智能的白皮书中就提出云-边缘人工智能系统是一个重要研究方向[4]；2018 年，知名调研机构 Gartner 将边缘智能写入新一版的人工智能曲线[72]. 一个公认的事实是，人工智能与边缘计算的融合是自然而不可避免的. 边缘计算利用人工智能的技术和方法可以更大规模地释放其潜力，而人工智能借助边缘计算的场景和平台可以拓展更多的应用和技术[5-7].

一方面，随着物联网和移动计算的普及，越来越多的数据并不像以往一样生成和存储在超大规模的数据中心中，而是分散地生成并存储在大量的边缘节点上. 鉴于当前人工智能技术还在极大程度上依赖大规模真实数据[73]，为了在边缘网络中有效使用人工智能技术进行数据的处理与分析，一种解决方案是将分散在网络各处的数据重新收集到传统的数据中心里，但是当关注到性能、成本以及隐私问题的时候，这种方案的缺陷比较明显[6]. 另外一种方案是在产生数据的本地运行人工智能程序，但是考虑到大量物联网设备和终端设备都是轻量级的，其运算和存储能力均十分有限，该方案目前的可行性较低. 综合来看，利用边缘计算在边缘服务器上运行人工智能应用是一种相比而言更为可行的解决方案. 举例来说，边缘计算有一个十

分具有代表性的人工智能应用是实时视频分析[74]. 该应用需要不断从监控摄像机中获取高清视频，且要求分析视频同时满足高计算量、高带宽、低延迟以及高隐私性保护的要求，而边缘计算正是能满足这些要求的最合适的技术.

另一方面，人工智能技术也能优化边缘计算的服务. 在边缘计算中，一直在讨论各种各样的资源分配问题. 如何优化资源分配以提高系统效率是边缘计算系统设计的目标之一，而人工智能技术，包括统计方法、深度学习方法和强化学习方法在这个问题上都可以提供一定的帮助[75-77].

2.3.2　边缘人工智能计算的概念与框架

许多研究者都给出了边缘人工智能计算的定义. 文献 [5] 认为边缘人工智能计算即是在边缘设备执行人工智能的算法；文献 [6] 则认为这样的定义缩小了边缘人工智能计算的范围，于是依据建模、模型训练、结果推导在云实现还是在边缘实现将边缘人工智能计算分为 6 个等级；文献 [7] 的划分则相对简单，将边缘人工智能计算划分为边缘服务的人工智能(AI for edge)和在边缘上的人工智能(AI on edge).

本文将边缘人工智能计算定义为在边缘网络上多个分布式设备协同共建的人工智能.

1）本文并不考虑在使用专有硬件的单个边缘设备上运行人工智能算法[78]的情况，因为这种情况与目前在大规模数据中心运行人工智能算法并没有本质上的区别. 本文同意文献 [6] 的观点：边缘人工智能计算中协同计算的多个设备绝不仅仅局限于边缘终端设备，相反地，边缘人工智能计算将充分利用终端设备、边缘服务器和云数据中心中的可用数据和资源. 2）本文认为的多个边缘设备协同计算共建人工智能，既可以是一个同样的人工智能算法通过多个设备协同完成计算以保护数据隐私或提升效率，也可以是一个单个设备或一个小型设备集群. 这样的一个单个设备或小型设备集群可以被抽象成一个自主化的智能体，它拥有可消耗的知识，由自身利益的目标驱动，为了实现群体目标与其他智能体交互，如共享知识数据或联合进行决策. 这样的相互连接和组织在网络中的松散耦合的多个智能体也被称为群体智能[79].

多个设备协同计算完成一个深度神经网络训练的的优势在于：使用可用的空闲设备使小型边缘设备集群，能够运行更大的模型或加速推理过程. 文献 [80] 将神经网络的每一层都并行化以加速整个模型的计算. 文献 [81] 提出的协同感知网络将一个深度神经网络模型整体进行划分，并将划分后的模型部分分配给多个边缘设备来完成计算. 目前，更多的框架设计会借用分布式深度神经网络的框架并对其进行修改以满足边缘网络的特殊需求. 常见的分布式深度神经网络框架有联邦学习(federated learning, FL)[82]，它要求随机客户端从服务器下载可训练的模型，用自己的数据更新模型并将更新后的模型上传到服务器，再由服务器聚合多个客户端更新，这样的过程将重复多次，直到服务器聚合后的人工智能模型收敛为止. 将分布式深度神经网络框架应用到边缘计算场景遇到的挑战是如何在资源受限的设备上提供足够的计算能力. 文献 [83] 提供了一个解决思路，就是在边缘设备中采用深度学习加速器(deep learning accelerator, DLA)，通过将关键计算操作实现为硬件连接逻辑来提升效率. 文献 [84] 提供的解决思路则是对参与本次训练的设备进行选择，尽可能选择更多的计算资源多且通信条件好的设备以满足本次训练的需要.

2.3.3　边缘人工智能计算的发展趋势

安全与隐私问题是任何应用和系统都会考虑的问题. 边缘人工智能计算的系统是在边缘网络上的一个分布式的系统，具有自主性、分散控制、成员数量多等复杂异构特征，面临着诸多潜在安全风险[85]. 首先，如果不能保证参与者之间的安全通信，协作的任务就无法完成. 其

次，系统内成员并不完全可信，它们可能怀有恶意或遭受到了攻击，因此判断其他成员传输的信息的可靠性也是必要的.

网络性能是边缘人工智能计算的影响因素之一. 文献 [86] 模拟移动设备和边缘服务器运行经典神经网络 AlexNet 的测试结果，如图 3 所示. 该结果表明：相比于移动设备，边缘服务器运行人工智能程序需要的时间更少，但是其运行时间对带宽高度敏感，显然受到了数据传输时间的影响. 因此，考虑到现实网络带宽资源的稀缺性，边缘人工智能计算的一个研究方向是优化模型和框架以降低网络对边缘智能系统性能的影响. 文献 [87] 融合早期的卷积层并在多个设备中并行化这些层，从而降低了通信成本. 文献 [78] 则提出一种自适应卷积网络，能将卷积层划分给相应的设备进行并行计算，这是根据计算资源的可用性和网络条件动态选择的.

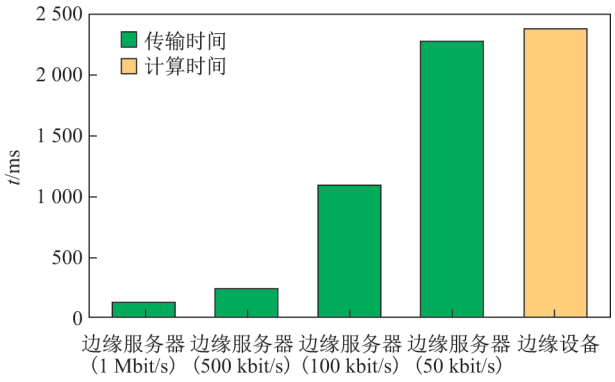


图 3 边缘移动设备和边缘服务器运行神经网络用时

Figure 3 Time of edge mobile devices and edge servers running deep neural networks

3 面向边缘人工智能计算的区块链研究

3.1 当前研究工作总结

表 2 简单总结了面向边缘人工智能计算的区块链研究工作，接下来将分类进行详细阐述.

3.1.1 基于区块链的边缘人工智能计算框架

在面向边缘人工智能计算区块链研究中，一个主要方向是引入区块链来构建边缘人工智能计算框架，原因如下：1）边缘人工智能计算中的节点本身及在相互通信的过程中都可能遭受网络攻击；2）参与边缘智能的节点可能存在恶意行为或者缺乏足够的激励而为系统积极贡献，引入区块链则可以成为有效的解决方案之一.

文献 [88] 讨论了联邦学习的安全问题，地理上分散的节点向集中的服务器发送更新参数时不仅容易受到网络攻击，而且存在着隐私泄露的问题. 区块链可以作为一种联邦学习中交换学习模型参数的安全方法，节点可以将自己的参数上传到区块链，同时也可以从区块链中获取他人更新的参数结果. 另外，区块链还可以支持对任意时期的子模型审计.

文献 [89] 指出：联邦学习中负责模型初始化和聚合参数的主服务器存在单点故障问题，如果主服务器受到攻击，那么其他参与节点将无法获知全局模型，为此该文献设计了一个基于区块链网络的联邦学习架构，提出了全局模型状态树的概念，以便将一个全局模型安全地存储为一个 Merkle-Patricia 树并放入区块链.

类似地，BlockFL[90]同样认为主服务器会受到单点故障的影响，因此他们关注的问题是如何在没有任何中心协调之下聚合全局模型. BlockFL 将全局模型更新后放入每个设备本地

并在区块链网络上传其最终的更新结果，同时 BlockFL 认为在缺乏有效激励措施的情况下有些设备可能有欺骗行为，即上传假的模型更新结果. 因此，它要求区块链网络在共识过程中验证节点上传的结果并给节点提供相应的奖励.

表 2　面向边缘人工智能计算的区块链研究工作

Table 2　Researches of blockchain in edge AI computing

文献	应用场景	关注问题	区块链作用
[88]	联邦学习	安全问题	安全可审计的交换模型参数
[89]	联邦学习	单点故障问题	安全存储全局模型
[90]	联邦学习	信任问题	共识验证模型结果+激励
[91]	联邦学习	信任问题	可信加密可审核存储参数+激励
[92-93]	联邦学习	安全问题	安全存储模型更新信息
[94]	联邦学习	安全问题	记录设备操作信息日志，共识识别拜占庭设备
[95]	联邦学习	信任问题	分布式信誉管理
[96]	医疗大数据	安全与隐私问题	安全私密的共享医疗记录数据集
[97]	多机器人系统	任务匹配	存储记录分配方案
[98]	多机器人系统	信任问题	智能合约进行信誉管理
[99]	无人机集群	分布式决策	以转账代表决策倾向
[100]	车联网	安全与隐私问题	安全隐私可追溯的存储车辆与设施交互数据
[101]	物联网	安全问题	安全存储决策结果
[102]	物联网	激励问题	激励知识管理与交易
[103]	金融	安全问题	防篡改存储历史金融信息
[104]	智能电网	安全问题	安全可审计的存储能源交易数据
[105]	智慧城市	激励问题	激励数据分析信息的共享

文献 [91] 同样认为联邦学习中节点可能是恶意的或者缺乏参与系统的动机，于是提出了 DeepChain 以便在数据保密性、计算可审核性、激励各方参与协同训练三方面提供支持. 具体来说，DeepChain 可以启动事务，从而将来自不可信节点的子模型参数安全地聚合在一起. 密码学技术保障了协同训练过程中的数据保密性和可审核性，并用一种被称作 DeepCoin 的资产奖励参与方对模型训练的贡献以达到激励效果.

除此之外，还有一些工作只是针对具体的应用场景而不是提出一个通用的框架. 文献 [96] 给出了针对医疗大数据的体系结构，其核心在于分布式数据管理、分布式数据共享和分布式计算分析. 对于分布式数据管理和数据共享，该框架提出将区块链智能合约技术和监控节点用于建立安全私密的共享医疗记录数据集. 区块链技术将有助于建立这样一个大型核心初始数据集，并保障所有数据的透明度和完整性. 监控节点则用于监视希望访问数据集的所有相关智能合约事件以提供及时的响应. 对于分布式计算分析，该框架则借鉴了联邦学习和转移学习的核心思想.

值得一提的是，基于区块链的联邦学习的性能与独立的联邦学习的性能几乎相当[106]，并没有因为引入区块链而对整体系统的性能造成显著的影响.

3.1.2 基于区块链的多智能体协作与决策增强

在边缘人工智能计算中，多智能体达到有效协作的挑战之一是设计恰当的任务分配机制[107]，这需要考虑不同类型任务的定义和分配、智能体的异构性等. 鉴于中心式的任务分配机制会受单点故障的影响，文献 [97] 提出了一种动态的基于市场的任务分配方法，由任务发布者向智能体提供任务，且发布者与智能体在整个任务分配与完成的动态过程中彼此共享信息. 其中，发布者与智能体的通信、协调以及信息共享是基于联盟链完成的. 简单地说，智能体可以通过区块链控制器获取执行任务，并计算这些任务的报价. 如果它决定执行该任务便可以通过区块链投标并广播给所有其他智能体，而其他投标的智能体会检查是否放弃并竞标下一个任务直至所有智能体都同意当前分配方案.

在一个典型的边缘人工智能计算场景中，多智能体协作决策的应用案例是无人机自主集群. 多架无人机分别从多个视点感知信息，同时需要就群体的目标达成一致的决策，比如前方要走的路如何避开障碍，收集到的信息究竟是什么等等. 当前，如何在大量智能体之间进行分布式决策仍然是一个开放的问题，存在一些诸如决策速度与决策准确性之间的两难权衡问题[99, 108]. 文献 [99] 给出了一个简单的如何使用区块链技术辅助智能无人机集群的决策过程的例子. 当无人机集群需要商议一致的时候，一架无人机可以通过区块链创建出一个特殊的事务. 这个事务包含了决策的不同选项所对应的数字地址，当该事务得到全网的节点确认之后，其他集群成员可以对自己支持的选项进行投票，方式是向该选项对应的数字地址转账代币. 举例说明，一架无人机观察到了一幅图片，需要判断图片内容是杯子还是亲吻的人脸，于是创建一笔特殊事务. 事务中指明杯子对应 SK343 开头的地址，亲吻的人脸对应 S0631 开头的地址，之后其他无人机做出判断并向这两个地址开头的账户转入代币，经过一段时间后无人机比较两个账户的代币数，发现 SK343 开头的地址收到的代币较多，则做出图片是无人机的决策. 由于所有参与者都可以监控整个投票过程，该群体决策是安全且可审核的.

3.1.3 基于区块链的边缘人工智能计算可信增强

在边缘人工智能计算系统框架中，安全攻击与安全威胁是该系统实际部署过程中必须考虑的问题. 文献 [92] 指出，在协作进行模型更新的过程中，移动设备可能面临中毒攻击(poisoning attack)或者信息泄漏攻击(information leakage attack)，于是提出将模型更新信息存储在区块链中并在区块链平台进行聚合，同时利用拒绝负面影响(reject on negative impact, RONI)这一防御机制来删除中毒的更新参数. 类似地，文献 [93] 也使用区块链存储和验证设备的本地子模型，进一步通过调整区块生成速率来优化端到端学习完成的延时. 文献 [94] 则指出了另外一个安全威胁，一个或多个拜占庭故障的设备足以让当前的联邦学习机制面临不可预测或灾难性的结果，因此采用区块链技术建立安全的协同训练机制并识别和排除拜占庭成员.

边缘人工智能计算面对的是多个异构设备节点之间的相互协作，网络中的单个节点很难决策如何选择来自不同信息源的意见，因此设计一种衡量“可靠性”的机制是必要的. 一种常见的衡量节点可靠性的机制是构建信誉系统，即基于之前的行为构建对未来行为的感知和期望. 文献 [95] 关注的是在联邦学习框架中如何挑选可靠训练节点和激励的问题，参与的节点有可能因为缺乏激励而懈怠工作或者上传伪造的模型更新参数，因此引入区块链实现分布式的不可篡改的信誉管理，并依据信誉衡量设备可靠性和可信度以选择可靠的高质量的联邦学习参与节点. 边缘服务器将成为主要的区块链存储节点和矿工，对于特定的移动设备，任务发布者将其直接信誉意见与来自其他任务发布者的声誉意见整合在一起，为设备产生综合信誉价值，并将信誉值作为之后挑选可靠的参与节点的重要指标. 文献 [98] 基于 Hyperledger

Fabric 设计了一种多个智能体的任务协作系统，智能体在区块链发布自己可以提供的服务和选择自己请求的服务. 由于受到不同利益的驱动，智能体可能会表现出恶意行为，可见对智能体进行信誉管理是必要的，因此该文献提出使用另外一个并行的区块链账本来存储与服务提供者和请求服务的智能体之间相关评估的信息，并使用智能合约进行信誉管理.

另外一些工作关注的是：在特定应用场景部署边缘人工智能计算时如何增强整个系统的安全性与可信性.

文献 [100] 关注的是电动汽车边缘计算网络，该网络中的电动汽车配备着多种智能应用，同时电动汽车之间、电动汽车和基础设施之间存在着大量信息和能源的交互. 引入区块链可以增强安全性和隐私性，一是因为区块链可以追溯交互数据以避免交互数据可能被恶意利用或篡改，二是因为区块链可以在保护隐私的前提下实现匿名数据传输和批量认证.

文献 [101] 关注的是物联网中的智能物体(smart things). 智能物体即物联网中借助人工智能技术实时进行自我推断和自我监控的设备，这些设备需要协同工作以进行复杂的决策. 为了确保智能物体之间的通信与决策的安全可靠，使通信避免网络攻击的影响，使决策不受恶意节点的影响，该文献基于联盟链的多链机制在多链上接收数据和存储数据，并将数据分发给集群中的所有节点，使节点能够实时且安全地传达决策的结果.

文献 [103] 关注的则是金融数据. 边缘智能在该网络中的功能是进行实时数据监测和动态数据分析，而区块链的引入有两个作用：一是区块链能支持加密密钥分发和网络权限管理，二是区块链存储的借款等历史信息有助于信用评估，提高了应用的安全性.

文献 [104] 则将目光聚焦于能源基础设施建设. 人工智能使得在电网边缘的自动化监控和审计成为可能，而区块链可以提供一种无密钥签名的基础设施，有助于保护这些关键的能源数据. 分布式数字账本和对交易数据进行密码学签名可以保障能源交易数据的完整性，另外采用智能合约的数据交换平台也可以在电力生产价值链中实现合约的自动交易和结算.

针对提升系统中各种实体之间的信任水平，文献 [109] 提出了一个基于区块链的智能契约和专门设计的智能预言机（smart oracles）的信任管理架构. 该架构在以太坊上实现，并基于摄像机信任管理、可信数据流和基于 QoS 的计算节点选择这3个场景，展示了在实体、服务之间建立信任关系的优势. 从本质上来说，区块链消除了信任第 3 方的必要性，为交互提供了透明度和可跟踪性，而智能预言器的使用减少了在区块链上进行代价高昂的交易的必要性.

3.1.4　基于区块链的边缘人工智能信息共享

关于在边缘计算场景中多个节点协同训练人工智能模型，现有的工作通常只专注于如何依据大量的数据信息更好地训练模型，而没有将数据信息的产生、汇集与之后的交换纳入考虑的范围[102,105].

文献 [102] 提出：物联网中自私的异构的边缘智能设备会产生孤立的、分布式的知识片，而物联网智能应用完成复杂的任务却需要知识的协作与交换. 一个有效激励边缘智能设备共享知识信息的办法是实现知识的付费共享，因此该文提出了一个基于联盟链构建的市场，可以提供安全而有效的知识管理和交易. 该联盟链的设计包括一个加密货币、智能合约和一个新的共识机制交易证明（proof of transaction, PoT）. 文献 [105] 关注的则是在智慧城市中实现基于物联网的可持续共享经济. 大量的物联网数据在边缘节点被生成和处理，人工智能会处理并提取其中重要的事件信息，生成语义数字分析后将结果保存在区块链中. 区块链则提供一系列共享经济服务，包括将哪些数据交给人工智能分析及其分析得出的重要信息的交易，从而使得有价值的互联网信息得到充分的利用.

3.2 区块链为边缘人工智能计算带来的好处

就现有的研究成果而言，本文认为区块链可以有效加速边缘人工智能计算的落地. 1）以区块链作为底层支撑的边缘人工智能计算架构更适合于边缘计算情况下的人工智能场景；2）区块链可以有效提升边缘人工智能计算系统中数据管理、存储和传输的安全性；3）为了促进边缘人工智能计算的发展，人工智能的核心——信息与数据是不可或缺的，而区块链可以有效激励边缘智能场景中信息与数据的共享与交换. 另外，也有研究指出区块链可以提升对人工智能模型的信任并有利于优化人工智能的模型.

3.2.1 区块链可增强边缘人工智能计算框架的健壮性

边缘人工智能计算不再是基于云上的数据中心进行人工智能应用的处理，而是保持数据在设备本地，同时将人工智能的部分工作转移到设备上，此时边缘人工智能计算所面对的是大量异构的计算资源和大量存在着掉线或被劫持的可能性的节点[110]. 因此，传统的适用于云的中心化人工智能的框架并不适合直接套用，而以区块链作为支撑的新型架构开始得到探讨，比如一种基于区块链的联邦学习结构. 在该结构中，各节点利用本地数据分散训练，依照区块链的共识机制分散地进行数据交换和子模型更新的验证，而无需任何集中的数据训练或协调[90,111].

3.2.2 区块链可增强边缘人工智能计算数据管理、存储和传输的可靠性

首先，边缘人工智能计算场景的网络是典型的点对点网络，诸如多跳连接、缺少中心、缺乏明确防御机制等问题都使这个网络不够稳定. 许多常见网络攻击，包括重放攻击、拒绝服务攻击（denial of service, DoS）、窃听、虫洞攻击、伪装攻击等都可能对这个网络造成灾难性的后果[112-113]. 其次，对于边缘人工智能计算场景来说，信息是非常重要的[114]. 由于大量由边缘设备产生的信息可能是带有隐私的敏感信息，防止用户的隐私在边缘人工智能计算的操作中泄露是必须考虑的设计目标，同时一些伪装或劫持攻击会导致虚假信息的传播，影响边缘人工智能计算应用的效果[111]. 为了增强边缘人工智能计算场景中数据存储、传输和管理的安全性，区块链可以被当成一种潜在的解决方案[115-116]，能够利用多种加密算法在保障隐私的情况下建立多方之间的协作关系. 在区块链中添加新块需要经过共识机制确认，任何块都记录并存储一个与前一个块相连接的数据，并且只有当相应的消息通过大多数参与者的验证时，才会将一个新块附加到分类账上. 这样特殊的机制设计保障了在单点故障下很好的健壮性，并避免了数据的恶意篡改.

3.2.3 区块链可激励边缘人工智能计算中信息共享与交易

在典型的边缘计算场景（如物联网场景）中，大量异构的设备分散地产生孤立的信息，而复杂人工智能应用任务的完成需要信息的交换与协作，因而如何促进网络中众多“自私”的节点分享、交换与协作是要考虑的问题[102,105]. 区块链可以成为促进边缘人工智能计算场景信息共享与交换的一种有效解决方案. 首先，区块链天然的点对点的网络架构符合边缘智能场景下大量分散孤立节点的要求；其次，区块链的加密货币可以成为一种促进各节点信息共享的有效激励手段[111]，区块链的智能合约有助于构建信息相互分享交易的市场. 更重要的是，依托区块链技术建立起的信息共享交换市场是安全可靠的，每一笔交易都可以经过共识机制的验证，也可以有效防止篡改和双重支付问题.

3.2.4　区块链可以提升人工智能决策的可信任性

人工智能受到大众质疑的一点是它就像一个黑匣子[117]，其结果难以从理论上解释，而区块链正是以点对点分散场景中安全准确无篡改的记录交易而闻名. 以区块链记录人工智能的中间结果和决策过程能够增加其透明度，有利于公众接受和信任决策，也便于相关人员的审计[9, 99]. 同时，在边缘人工智能计算这种可能涉及多方智能共同决策的场景中，区块链也可以帮助它们在不需要第 3 方审核的情况下以分布式的方法实现统一的意见[118].

另外，虽然还没有成为学界广泛的共识，但已有研究着眼于利用区块链改进并提出更好的人工智能模型. 文献 [119] 提出了一种基于区块链思想的边缘智能算法，试图利用区块链和交易的思想在神经网络中更快速且更智能地寻找合适的模型权重. 在他们的构想中，一个交易是一个特定的需求，之后全网的“矿工”们都会训练出合适的模型并提交申请，同时执行此任务的“矿工”们会比较结果并将最好的结果写入块，使该交易成为一个完成的任务.

4　未来研究方向

之前的章节已经综述了目前面向边缘人工智能计算的区块链研究方向. 经相关论文总结，本文认为未来将有以下 4 个研究方向.

4.1　区块链性能改进：提升面向资源受限计算环境的扩展性

尽管本文已经探讨了将区块链技术引入边缘人工智能计算的诸多优势，但是与区块链本身相关的许多技术挑战还需要进一步研究. 这些问题本身可能不会对基于区块链技术的边缘人工智能计算的解决方案的发展产生直接影响，但是会在一定程度上限制这些解决方案的实际应用. 与区块链本身相关的技术挑战大多聚焦于区块链的性能问题，尤其是事务吞吐量、交易确认时延、区块容量等问题. 比特币区块链目前每秒处理的事务大约是 7 笔，一笔事务的确认大约需要 10 min[27]，这样的性能无法满足边缘人工智能计算中很多协调和共同决策场景的需求. 以无人机集群为例，无人机之间应快速地提供可靠信息并达成共识以协调整个群体的运动，10 min 的时间足以使无人机撞上障碍，因此未来区块链应该探索针对边缘人工智能计算的性能改进. 目前，以太坊的区块大小是 444.06 GB[28]，且随着事务数量的增长该账本大小也会随之增长. 然而，对于硬件能力十分有限的边缘设备来说，它们很难在本地保存完整的区块链账本，因此未来应该探索对资源有限设备更加友好的区块链.

4.2　区块链应用：构建跨域/泛中心网络中的分布式信任

在边缘智能计算的场景中，存在着更多设备与设备之间的合作. 比如：多个拥有本地数据的设备共同收敛全局人工智能模型；在智慧交通中，多个车辆共同协助反馈交通信息；多智能体之间联合进行决策等. 合作的基础是合作方之间存在信任，即对方提供的信息、做出的决策是真实可靠的. 现有的信任构建方式主要包括两种：一种是基于身份管理和访问控制的方式，一般是在一个域内设立一个中心管理机构来管理身份或以分布式的形式验证身份，如果身份被验证为可靠，则其受允许的行为便值得信任，但是如何进行身份的相互验证是一个难点. 另一种是基于信誉反馈的方式，即相关方给出有关信任的评价，综合得出关于某节点值得信任的程度，但是相关评价是否可靠又成为了一个问题. 区块链以其不可篡改性保证记录数据的真实性，以其可追溯性和共识机制有助于确认记录数据的可靠性，因而可以在跨域/开放网络中更好地构建信任，但这一方面研究的难点在于：如何通过模拟实验来验证所提方案的有效性，如何设定信任的衡量方式，以及如何模拟部分节点不同程度的“不可信”情况.

4.3 区块链应用：群智计算与数据隐私的权衡

在系统设计中，保护安全与隐私的目标并不是一个新话题，而区块链具有匿名性、分散性、安全性等关键特性，因而被认为能够方便、高效、可靠、安全地应对系统中的安全和隐私问题. 使用区块链提升系统的隐私和安全性往往伴随着相关的密码学算法的使用与设计，比如一种常见的用于保护隐私的密码学手段是零知识证明. 但是，这些密码学中的算法还需要进一步设计与研究，比如交互式的零知识通信协议过于复杂，以致容易受到恶意软件的攻击；若采用非交互式简洁零知识证明技术(zero knowledge succinct non-interactive argument of knowledge, zk-SNARK)，如 Zcash[120]，其证明过程需要大量的内存，这意味着在受限设备上很难使用.

5 结 语

本文调研并回顾了目前较新的有关边缘人工智能计算的区块链研究. 首先概述了区块链的概念和区块链的研究方向，同时介绍了边缘人工智能计算的发展趋势，总结了边缘人工智能计算的概念、框架与发展需求；然后从基于区块链的边缘人工智能计算框架、基于区块链的多智能体协作与决策增强、基于区块链的边缘人工智能计算安全性和可信性增强，以及基于区块链的边缘人工智能计算信息共享等方面对面向边缘人工智能计算的区块链研究进行了详细的介绍，总结并讨论了为边缘人工智能计算引入区块链的各种优势. 文献综述表明：在边缘人工智能计算中引入区块链的研究还处于起步阶段，未来仍需针对边缘人工智能计算场景的需求和目标对区块链自身加以改进，还应更多地探索结合边缘人工智能计算与区块链的优势.

参考文献:

[1] Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2019-11-16]. https://bitcoin.org/en/bitcoin-paper.

[2] Gao W, Hatcher W G, Yu W. A survey of blockchain: techniques, applications, and challenges [C]// 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018: 1-11.

[3] Zheng Z, Xie S, Dai HN, et al. Blockchain challenges and opportunities: a survey [J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.

[4] A berkeley view of systems challenges for AI [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1712.05855.

[5] OpenEI: an open framework for edge intelligence [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1906.01864v1.

[6] Edge intelligence: paving the last mile of artificial intelligence with edge computing [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1905.10083v1.

[7] Edge intelligence: the confluence of edge computing and artificial intelligence [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1909.00560.

[8] Yang R, Yu F R, Si P, et al. Integrated blockchain and edge computing systems: a survey, some research issues and challenges [J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1508-1532.

[9] Salah K, Rehman M H U, Nizamuddin N, et al. Blockchain for AI: review and open research challenges [J]. IEEE Access, 2019, 7: 10127-10149.

[10] Li X, Jiang P, Chen T, et al. A survey on the security of blockchain systems [J]. Future Generation Computer Systems, 2017.

[11] The Tangle: an illustrated introduction [EB/OL]. [2019-11-16]. https://iota.org/IOTA_Whitepaper.pdf.

[12] Jin T, Zhang X, Liu Y, et al. BlockNDN: a bitcoin blockchain decentralized system over named data networking [C]//2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), 2017: 75-80.

[13] Wood G. Ethereum: a secure decentralised generalised transaction ledger [J]. Ethereum Project Yellow Paper, 2014, 151(2014): 1-32.

[14] Bitshares 2.0: general overview [EB/OL]. [2019-11-16]. https://cryptorating.eu/whitepapers/BitShares/bitshares-general.pdf.

[15] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains [C]//Proceedings of the Thirteenth EuroSys Conference, 2018: 30.

[16] Turk Ž, Klinc R. Potentials of blockchain technology for construction management [J]. Procedia Engineering, 2017, 196: 638-645.

[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.

[18] Hurich P. The virtual is real: an argument for characterizing bitcoins as private property [J]. Banking & Finance Law Review, 2016, 31(3): 573.

[19] Dorri A, Kanhere S S, Jurdak R, et al. Blockchain for IoT security and privacy: the case study of a smart home [C]//2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom workshops), 2017: 618-623.

[20] Zhang Y, Wen J. The IoT electric business model: using blockchain technology for the internet of things [J]. Peer-to-Peer Networking and Applications, 2017, 10(4): 983-994.

[21] Stanciu A. Blockchain based distributed control system for edge computing [C]//2017 21st International Conference on Control Systems and Computer Science (CSCS), 2017: 667-671.

[22] Ouaddah A, Abou E A, Ait O A. FairAccess: a new blockchain-based access control framework for the Internet of Things [J]. Security and Communication Networks, 2016, 9(18): 5943-5964.

[23] Primecoin: cryptocurrency with prime number proof-of-work [EB/OL]. [2019-11-16]. https://www.techylib.com/en/view/tangibleassistant/primecoin_cryptocurrency_with_prime_number_proof-of-work.

[24] Eyal I, Gencer A E, Sirer E G, et al. Bitcoin-ng: a scalable blockchain protocol [C]//13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), 2016: 45-59.

[25] Dfinity technology overview series, consensus system [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1805.04548.

[26] Kim S, Kwon Y, Cho S. A survey of scalability solutions on blockchain [C]//2018 International Conference on Information and Communication Technology Convergence (ICTC), 2018: 1204-1207.

[27] Luu L, Narayanan V, Zheng C, et al. A secure sharding protocol for open blockchains [C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016: 17-30.

[28] Bit Info Charts [EB/OL]. [2019-11-16]. https://bitinfocharts.com/ethereum/.

[29] Ehmke C, Wessling F, Friedrich C M. Proof-of-property: a lightweight and scalable blockchain protocol [C]//Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, 2018: 48-51.

[30] Garzik J. Block size increase to 2MB [J]. Bitcoin Improvement Proposal, 2015, 102.

[31] Backman J, Yrjölä S, Valtanen K, et al. Blockchain network slice broker in 5G: slice leasing in factory of the future use case [C]//2017 Internet of Things Business Models, Users, and Networks, 2017: 1-8.

[32] The bitcoin lightning network: Scalable off-chain instant payments [EB/OL]. [2019-11-16]. https://lightning.network/lightning-network-paper.pdf.

[33] Enabling blockchain innovations with pegged sidechains [EB/OL]. [2019-11-16]. URL: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains.

[34] Poon J, Buterin V. Plasma: scalable autonomous smart contracts [J]. White Paper, 2017: 1-47.

[35] Eyal I, Sirer E G. Majority is not enough: bitcoin mining is vulnerable [J]. Communications of the ACM, 2018, 61(7): 95-102.

[36] Apostolaki M, Zohar A, Vanbever L. Hijacking bitcoin: routing attacks on cryptocurrencies [C]//2017 IEEE Symposium on Security and Privacy (SP), 2017: 375-392.

[37] Heilman E, Kendler A, Zohar A, et al. Eclipse attacks on bitcoin′s peer-to-peer network [C]//24th USENIX Security Symposium (USENIX Security 15), 2015: 129-144.

[38] Kiayias A, Panagiotakos G. On trees, chains and fast transactions in the blockchain [C]//International Conference on Cryptology and Information Security in Latin America, 2017: 327-351.

[39] Luu L, Velner Y, Teutsch J, et al. Smartpool: practical decentralized pooled mining [C]//26th USENIX Security Symposium (USENIX Security 17), 2017: 1409-1426.

[40] Tian F. An agri-food supply chain traceability system for China based on RFID & blockchain technology [C]//2016 13th International Conference on Service Systems and Service Management (ICSSSM), 2016: 1-6.

[41] Dennis R, Owen G. Rep on the block: a next generation reputation system based on the blockchain [C]//2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015: 131-138.

[42] Axon L. Privacy-awareness in blockchain-based PKI [J]. Cdt Technical Paper Series, 2015.

[43] Zyskind G, Nathan O. Decentralizing privacy: using blockchain to protect personal data [C]//2015 IEEE Security and Privacy Workshops, 2015: 180-184.

[44] Sharma P K, Chen M Y, Park J H. A software defined fog node based distributed blockchain cloud architecture for IoT [J]. IEEE Access, 2017, 6: 115-124.

[45] Li C, Zhang L J. A blockchain based new secure multi-layer network model for Internet of Things [C]//2017 IEEE International Congress on Internet of Things (ICIOT), 2017: 33-41.

[46] Samaniego M, Deters R. Hosting virtual iot resources on edge-hosts with blockchain [C]//2016 IEEE International Conference on Computer and Information Technology (CIT), 2016: 116-119.

[47] Samaniego M, Deters R. Virtual resources & blockchain for configuration management in IoT [J]. Journal of Ubiquitous Systems and Pervasive Networks, 2017, 9(2): 01-13.

[48] Veena P, Panikkar S, Nair S, et al. Empowering the edge-practical insights on a decentralized Internet of Things [J]. Empowering the Edge-Practical Insights on a Decentralized Internet of Things. IBM Institute for Business Value, 2015: 17.

[49] Adept: an iot practitioner perspective [EB/OL]. [2019-11-16].

[50] Russell S J, Norvig P. Artificial intelligence: a modern approach [M]. Malaysia: Pearson Education Limited, 2016.

[51] Goodfellow I, Bengio Y, Courville A. Deep learning [M]. Cambridge, Massachusetts: MIT Press, 2016.

[52] Lecun Y, Bengio Y, Hinton G. Deep learning [J]. Nature, 2015, 521(7553): 436-444.

[53] Diamant A, Chatterjee A, Vallières M, et al. Deep learning in head & neck cancer outcome prediction [J]. Scientific Reports, 2019, 9(1): 2764.

[54] Liu Y. Novel volatility forecasting using deep learning-long short term memory recurrent neural networks [J]. Expert Systems with Applications, 2019, 132: 99-109.

[55] Whatmough P N, Lee S K, Brooks D, et al. DNN engine: a 28 nm timing-error tolerant sparse deep neural network processor for IoT applications [J]. IEEE Journal of Solid-State Circuits, 2018, 53(9): 2722-2731.

[56] Liu Y, Wang Y, Yang X, et al. Short-term travel time prediction by deep learning: a comparison of different LSTM-DNN models [C]//2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), 2017: 1-8.

[57] Uddin M Z, Kim M R. A deep learning-based gait posture recognition from depth information for smart home applications [M]. [S.l.]: Springer, 2016: 407-413.

[58] Taya A, Nishio T, Morikura M, et al. Deep-reinforcement-learning-based distributed vehicle position controls for coverage expansion in mmwave V2X [J]. IEICE Transactions on Communications, 2019: 2018EBP3299.

[59] Szegedy C, Liu W, Jia Y, et al. Going deeper with convolutions [C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2015: 1-9.

[60] Very deep convolutional networks for large-scale image recognition [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1409.1556.

[61] Krizhevsky A, Sutskever I, Hinton G E. Imagenet classification with deep convolutional neural networks [C]//Advances in Neural Information Processing Systems, 2012: 1097-1105.

[62] He K, Zhang X, Ren S, et al. Deep residual learning for image recognition [C]//Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, 2016: 770-778.

[63] Min S, Lee B, Yoon S. Deep learning in bioinformatics [J]. Briefings in Bioinformatics, 2017, 18(5): 851-869.

[64] Al Rahhal M M, Bazi Y, Alhichri H, et al. Deep learning approach for active classification of electrocardiogram signals [J]. Information Sciences, 2016, 345: 340-354.

[65] Vincent P, Larochelle H, Lajoie I, et al. Stacked denoising autoencoders: learning useful representations in a deep network with a local denoising criterion [J]. Journal of Machine Learning Research, 2010, 11(Dec): 3371-3408.

[66] Hu Y C, Patel M, Sabella D, et al. Mobile edge computing-a key technology towards 5G [J]. ETSI White Paper, 2015, 11(11): 1-16.

[67] Bonomi F, Milito R, Zhu J, et al. Fog computing and its role in the Internet of Things [C]//Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, 2012: 13-16.

[68] Mach P, Becvar Z. Mobile edge computing: a survey on architecture and computation offloading [J]. IEEE Communications Surveys & Tutorials, 2017, 19(3): 1628-1656.

[69] Mao Y, You C, Zhang J, et al. A survey on mobile edge computing: the communication perspective [J]. IEEE Communications Surveys & Tutorials, 2017, 19(4): 2322-2358.

[70] Roman R, Lopez J, Mambo M. Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges [J]. Future Generation Computer Systems, 2018, 78: 680-698.

[71] Abbas N, Zhang Y, Taherkordi A, et al. Mobile edge computing: a survey [J]. IEEE Internet of Things Journal, 2017, 5(1): 450-465.

[72] Panetta K. trends emerge in the Gartner hype cycle for emerging technologies [J]. Retrieved November, 4: 2018.

[73] Lee G, Jayasinghe U. AI and blockchain enabled edge of things with privacy preserving computation [C]//Conference Proceedings of XIII International Scientific Conference Perspective Technologies in the Information Transfer Means, 2019: 39-43.

[74] Ananthanarayanan G, Bahl P, Bodík P, et al. Real-time video analytics: the killer App for edge computing [J]. Computer, 2017, 50(10): 58-67.

[75] He X, Wang K, Huang H, et al. Green resource allocation based on deep reinforcement learning in content-centric IoT [J]. IEEE Transactions on Emerging Topics in Computing, 2018.

[76] Qiu X, Liu L, Chen W, et al. Online deep reinforcement learning for computation offloading in blockchain-empowered mobile edge computing [J]. IEEE Transactions on Vehicular Technology, 2019, 68(8): 8050-8062.

[77] Huang L, Bi S, Zhang Y J. Deep reinforcement learning for online computation offloading in wireless powered mobile-edge computing networks [J]. IEEE Transactions on Mobile Computing, 2019.

[78] Zhou L, Wen H, Teodorescu R, et al. Distributing deep neural networks with containerized partitions at the edge [C]//2nd USENIX Workshop on Hot Topics in Edge Computing (HotEdge 19), 2019.

[79] Calvaresi D, Dubovitskaya A, Calbimonte J P, et al. Multi-agent systems and blockchain: results from a systematic literature review [C]//International Conference on Practical Applications of Agents and Multi-agent Systems, 2018: 110-126.

[80] Mao J, Chen X, Nixon K W, et al. Modnn: local distributed mobile computing system for deep neural network [C]//Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017, 2017: 1396-1401.

[81] Hadidi R, Cao J, Woodward M, et al. Distributed perception by collaborative robots [J]. IEEE Robotics and Automation Letters, 2018, 3(4): 3709-3716.

[82] Federated learning of deep networks using model averaging [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1602.05629v1.

[83] Chen Y H, Krishna T, Emer J S, et al. Eyeriss: an energy-efficient reconfigurable accelerator for deep convolutional neural networks [J]. IEEE Journal of Solid-State Circuits, 2016, 52(1): 127-138.

[84] Nishio T, Yonetani R. Client selection for federated learning with heterogeneous resources in mobile edge [C]//ICC 2019-2019 IEEE International Conference on Communications (ICC), 2019: 1-7.

[85] Roscia M, Longo M, Lazaroiu G C. Smart city by multi-agent systems [C]//2013 International Conference on Renewable Energy Research and Applications (ICRERA), 2013: 371-376.

[86] Li E, Zhou Z, Chen X. Edge intelligence: on-demand deep learning model co-inference with device-edge synergy [C]//Proceedings of the 2018 Workshop on Mobile Edge Communications, 2018: 31-36.

[87] Zhao Z, Barijough K M, Gerstlauer A. Deepthings: distributed adaptive deep learning inference on resource-constrained iot edge clusters [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37(11): 2348-2359.

[88] Dillenberger D, Novotny P, Zhang Q, et al. Blockchain analytics and artificial intelligence [J]. IBM Journal of Research and Development, 2019, 63(2/3): 5:1-5:14.

[89] Majeed U, Hong C S. FLchain: federated learning via MEC-enabled blockchain network [C]// 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2019: 1-4.

[90] On-device federated learning via blockchain and its latency analysis [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1808.03949v1.

[91] Towards fair and decentralized privacy-preserving deep learning with blockchain [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1906.01167.

[92] Biscotti: a ledger for private and secure peer-to-peer machine learning [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1811.09904.

[93] On-device federated learning via blockchain and its latency analysis [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1808.03949v1.

[94] Zhu X, Li H, Yu Y. Blockchain-based privacy preserving deep learning [C]//International Conference on Information Security and Cryptology, 2018: 370-383.

[95] Kang J, Xiong Z, Niyato D, et al. Incentive mechanism for reliable federated learning: a joint optimization approach to combining reputation and contract theory [J]. IEEE Internet of Things Journal, 2019, 6(6): 10700-10714.

[96] Shae Z, Tsai J. Transform blockchain into distributed parallel computing architecture for precision medicine [C]//2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018: 1290-1299.

[97] Basegio T L, Michelin R A, Zorzo A F, et al. A decentralised approach to task allocation using blockchain [C]//International Workshop on Engineering Multi-Agent Systems, 2017: 75-91.

[98] Calvaresi D, Dubovitskaya A, Retaggi D, et al. Trusted registration, negotiation, and service evaluation in multi-agent systems throughout the blockchain technology [C]//2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), 2018: 56-63.

[99] Ferrer E C. The blockchain: a new framework for robotic swarm systems [C]//Proceedings of the Future Technologies Conference, 2018: 1037-1058.

[100] Liu H, Zhang Y, Yang T. Blockchain-enabled security in electric vehicles cloud and edge computing [J]. IEEE Network, 2018, 32(3): 78-83.

[101] Samaniego M, Deters R. Internet of smart things-IOST: using blockchain and clips to make things autonomous [C]//2017 IEEE International Conference on Cognitive Computing (ICCC), 2017: 9-16.

[102] Lin X, Li J, Wu J, et al. Making knowledge tradable in edge-AI enabled IoT: a consortium blockchain-based efficient and incentive approach [J]. IEEE Transactions on Industrial Informatics, 2019, 15(12): 6367-6378.

[103] Li Y, Shi W, Kumar M, et al. DyCREM: dynamic credit risk management using edge-based blockchain [C]//2018 IEEE/ACM Symposium on Edge Computing (SEC), 2018: 344-346.

[104] Mylrea M. AI enabled blockchain smart contracts: cyber resilient energy infrastructure and IoT [C]//2018 AAAI Spring Symposium Series, 2018: 2.

[105] Rahman M A, Rashid M M, Hossain M S, et al. Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city [J]. IEEE Access, 2019, 7: 18611-18621.

[106] Preuveneers D, Rimmer V, Tsingenopoulos I, et al. Chained anomaly detection models for federated learning: an intrusion detection case study [J]. Applied Sciences, 2018, 8(12): 26-63.

[107] Yan Z, Jouandeau N, Cherif A A. A survey and analysis of multi-robot coordination [J]. International Journal of Advanced Robotic Systems, 2013, 10(12): 399.

[108] Pourmehr S, Monajjemi V M, Vaughan R, et al. "You two! Take off!": Creating, modifying and commanding groups of robots using face engagement and indirect speech in voice commands [C]//2013 IEEE/RSJ International Conference on Intelligent Robots and Systems, 2013: 137-142.

[109] Kochovski P, Gec S, Stankovski V, et al. Trust management in a blockchain based fog computing platform with trustless smart oracles [J]. Future Generation Computer Systems, 2019, 101: 747-759.

[110] Park J, Samarakoon S, Bennis M, et al. Wireless network intelligence at the edge [J]. Proceedings of the IEEE, 2019, 107(11): 2204-2239.

[111] Mobile edge computing, blockchain and reputation-based crowdsourcing IoT federated learning: a secure, decentralized and privacy-preserving system [EB/OL]. [2019-11-16]. https://arxiv.org/abs/1906.10893?context=cs.CR.

[112] Mukherjee M, Matam R, Shu L, et al. Security and privacy in fog computing: challenges [J]. IEEE Access, 2017, 5: 19293-19304.

[113] Ferrag M A, Derdour M, Mukherjee M, et al. Blockchain technologies for the Internet of Things: research issues and challenges [J]. IEEE Internet of Things Journal, 2018, 6(2): 2188-2204.

[114] Boonstra A, Broekhuis M. Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions [J]. BMC Health Services Research, 2010, 10(1): 231.

[115] Porambage P, Kumar T, Liyanage M, et al. Sec-edgeAI: a vision for using artificial intelligence for securing the edge [C]//10th Nordic Workshop on System and Network Optimization for Wireless (SNOW).

[116] Kumar T, Porambage P, Ahmad I, et al. Securing gadget-free digital services [J]. Computer, 2018, 51(11): 66-77.

[117] Olah C, Satyanarayan A, Johnson I, et al. The building blocks of interpretability [J]. Distill, 2018, 3(3): e10.

[118] Brambilla M, Ferrante E, Birattari M, et al. Swarm robotics: a review from the swarm engineering perspective [J]. Swarm Intelligence, 2013, 7(1): 1-41.

[119] Winnicka A, Kęsik K. Idea of using blockchain technique for choosing the best configuration of weights in neural networks [J]. Algorithms, 2019, 12(8): 163.

[120] Zcash protocol specification [EB/OL]. [2019-11-16]. raw.githubusercontent.com.

(编辑：秦　巍)