综述

面向物联网区块链的共识机制优化研究

宋琪杰[1]，陈铁明[1,2]，陈园[1]，马栋捷[1]，翁正秋[1,3]

（1. 浙江工业大学计算机科学与技术学院，浙江 杭州 310023;
2. 之江实验室工业互联网研究中心，浙江 杭州 310000;
3. 温州职业技术学院，浙江 温州 325035）

摘　要：区块链的本质是一个去中心化的分布式账本系统；物联网是由海量异构终端接入互联而成，具备天然的分布式特征，因此两者结合的物联网区块链被广泛看好。同时，由于物联网感知终端的异构性、计算存储及数据传输能力都受限等特性，使物联网区块链面临较大挑战，其中密码共识技术成为关键问题。在总结当前区块链共识算法的基础上，分析其对物联网区块链的适用性，介绍了几大物联网区块链平台及共识机制应用现状，并阐述了针对物联网区块链的共识机制优化研究进展。最后展望物联网区块链的优化技术，总结有潜力的研究方向。

关键词：区块链；物联网；共识机制；DAG；智能增强；轻量级密码

中图分类号：TP311

文献标识码：A

doi: 10.11959/j.issn.1000−0801.2020037

Research on consensus mechanism optimization for IoT blockchain

SONG Qijie[1], CHEN Tieming[1,2], CHEN Yuan[1], MA Dongjie[1], WENG Zhengqiu[1,3]

1. College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China
2. Industrial Network Research Center, Zhejiang Laboratory, Hangzhou 310000, China
3. Wenzhou Vocational & Technical College, Wenzhou 325035, China

Abstract: The essence of the blockchain is a decentralized distributed ledger system. The Internet of things is interconnected by massive heterogeneous terminals and has natural distributed characteristics. Therefore, the combinedIoT blockchain is widely optimistic. At the same time, due to the heterogeneity of the IoT-aware terminal, the limited computing capacity and the ability of data transmission, the IoT blockchain faces great challenges. The password consensus technology has become a key issue. On the basis of summarizing the current blockchain consensus algorithm, its applicability to the IoT blockchain was analyzed, the current application status of several IoT blockchain platforms and consensus mechanisms was introduced, and the optimization research progress of the consensus mechanismin IoT blockchain was described. Finally, the optimization technology of the IoT blockchain and the potential research directions were summarized.

Key words: blockchain, IoT, consensus mechanism, DAG, intelligent enhancement, lightweight password

---

收稿日期：2019−10−21；修回日期：2019−02−07

通信作者：陈铁明，tmchen@zjut.edu.cn

基金项目：国家自然科学基金资助项目（No.61202282，No.61772026）；国家自然科学基金与浙江省政府联合资助项目（No.U1509214）

Foundation Items: The National Natural Science Foundation of China (No.61202282, No.61772026), The Joint Project of National Natural Science Foundation and Zhejiang Provincial Government (No.U1509214)

1 引言

物联网[1]时代已经到来，信息传感设备被广泛应用于智慧社区、智慧农业、智慧交通、共享经济等领域，推动着人—机—物的全面互联与融合。物联网研究机构预测到 2020 年年底[2]，物联网终端设备数量将增加到 260 亿。与传统互联网相比，物联网架构将网络连接扩展到更丰富的物理空间。针对其海量异构且资源受限的物联网终端数据共享、隐私保护、入侵检测、访问控制和跨域认证等难题[3-4]，计算要求大、部署成本高昂的传统安全技术并不能直接适用于物联网平台，需要寻求新的安全解决方案。

从比特币底层架构抽离的区块链技术，可应用于任何无需相互信任的介质之间的价值传递，从而催生出以太坊、超级账本（hyperledger）等通用的区块链应用平台[5]。区块链具有去中心化、信息不可篡改、数据公开透明等基本特点以及共识机制、智能合约、非对称加密三大保障机制。如图 1 所示，区块链通常可分为数据层、网络层、共识层、激励层、合约层和应用层六大部分[6]。

区块链在本质上是通过节点对分布式账本的共同维护来达成共识的信任体系，而物联网通过海量感知终端汇聚数据，具备天然的分布式网络特征，因此区块链被认为是一种最有前景的物联网安全基础解决方案。目前已出现不少面向物联网行业的区块链平台[7]。由于一个完整的物联网平台通常覆盖海量的异构终端，其高交易吞吐量、低计算处理与存储能力、低带宽数据传输网络等矛盾，使传统的区块链方案无法直接适用，必须研究轻量优化的区块链系统。其中，影响区块链吞吐量最为直接的因素，是密码共识机制。实际上，共识机制通常包含两部分，一部分为达成共识所需的密码算法，即共识算法；另一部分为达成共识的规则，即共识规则。共识算法属于密码学基础应用研究，其创新突破面临极大挑战。因此，如何改进区块链数据层、网络层、应用层，对传统共识规则进行优化改进，使共识机制更适用于物联网应用环境，成为当下的研究发展重点。

2 区块链共识算法基础

作为区块链核心，共识算法主要具备两个特性：一是，一致性，去掉区块链的 k 个末端区块，使可信节点保存的区块前缀相同；二是，有效性，可信节点发布的交易信息会被其他可信节点记录在区块链中。表 1 将目前常用的传统区块链共识分别从分类、提出时间、计算消耗、容忍恶意节点数、去中心化程度、可监管性以及应用几个方面进行对比。例如在证明类共识中，比特币应用的 PoW 机制通过计算准确的 Nonce 值获取记账的权限，算力消耗极大，而 Permacoin 中使用 PoW 提供数据保存服务[8]；在拜占庭类共识中，PBFT[9-10]应用于超级账本，能容忍 $\frac{1}{3}$ 的错误节点，基于拜占庭的共识还有 Quorum/Update[11]、Hybrid Quorum[12]、FaB[13]、Spinning[13]、Robust BFT

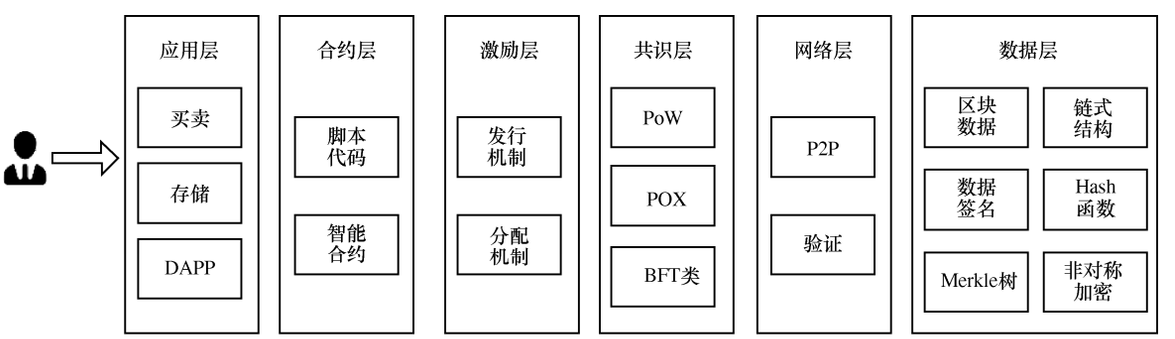

图 1 区块链典型分层结构

SMR[14]以及 Aliph[15]等，本文不做展开；其他还有区别于传统链式结构、以交易为粒度的无区块共识 DAG[16]（有向无环图），这种新型的区块链拓扑结构为共识研究提供新的思考。

目前应用于云区块链的共识机制在算力消耗、可监管性、去中心化以及安全性等方面仍然无法达到完美的平衡。而物联网领域中海量异构终端设备计算能力和存储能力受限，网络架构相对复杂，以及扩展需求强的特点，导致目前的共识并不完全适用于物联网。

3　物联网区块链的共识机制应用现状

区块链与物联网的深层结合实例仍处于不断创新与实践中。物联网通过传感器节点、协议等相关技术在一个对等开放的网络环境实现通信计算和数据传输交互。每个终端设备都可以作为区链的节点并参与共识维护区块链网络。下面将从物联网区块链共识机制的项目概况及共识优劣分析两个方面阐述基于物联网区块链的项目现状。

3.1　共识机制的项目概况

物联网区块链项目通过对现有共识算法优化改进，并运用主子链、算力芯片等技术助力强化共识规则，以弱化区块链应用物联网存在的矛盾。现有的物联网区块链系统主要有 IoTA、IoTEX、μNEST、EOSIoT 等。

3.1.1　IoTA

IoTA[16]是为物联网设计的新型交易结算区块链系统。区别于传统的链式区块链，IoTA 内部采用 Tangle（缠绕）——DAG 架构。转账不需要手续费，可扩性极强。随着节点的增加，系统的稳定性增强。在 DAG 系统中，新交易需要通过两笔历史交易指向进行验证。该机制中剔除矿工的设

表 1　区块链共识算法对比[17]

分类	共识算法	提出时间	计算消耗	容忍恶意节点数	去中心化程度	可监管性	应用
证明类共识	PoW[18] (Proof of Work)	1999 年	大	<1/2	完全	弱	比特币，Permacoin
	PoS[19](Proof of Stake)	2011 年	中等	<1/2	完全	弱	Peercoin
	DPoS[20](Delegated Proof of Stake)	2013 年	低	<1/2	完全	弱	EOS
	Ouroboros[21]	2017 年	低	<1/2	半中心化	强	Cardno
	PoA[22](Proof of Activity)	2014 年	大	<1/2	半中心化	强	以太坊私链，Oracles Network
	PoB[23](Proof of Burn)	2014 年	大	<1/2	半中心化	强	Slimcoin
	PoC[24](Proof of Capacity)	2016 年	大	—	完全	弱	文件共享
	PoD(Proof of Devotion)	—	中等	—	半中心化	强	星云链
	PoE[25](Proof of Existence)	2016 年	未知	—	完全	弱	HeroNode、DragonChain
	PoI[26](Proof of Importance)	2015 年	低	—	完全	弱	NEM
	PoR[27](Proof of Retrievability)	2014 年	低	<1/4	完全	弱	文件共享
	PoET[28](Proof of Elapsed Time)	2017 年	小	<1/2	半中心化	强	锯齿湖（sawtooth lake）
	PoP[29](Proof of Publication)	2012 年	大	<1/4	完全	弱	Bitcoin
拜占庭共识	PBFT[9,10]	1999 年	低	<1/3	半中心化	强	超级账本
	Raft	2013 年		—	半中心化	强	etcd
有向无环图	DAG[16](directed acyclic graph）	—	低	—	完全	弱	IoTA

置能够避免区块链遭受算力与双重攻击的威胁。同时，共识机制的改变有效提高交易的效率，提高吞吐量，大部分双花攻击将会被系统捕捉并立即制止。DAG 的网络拓扑也给用户一个更加清晰简明的模型架构。虽然 PoW 作为 DAG 的一部分仍需消耗算力，但基于 DAG 数据结构的全新区块链优势正在显现，IoTA 项目也得到了认可和快速的发展。

然而，高 TPS（transactions per second，每秒事务数）会带来以下问题：在 Tangle 中，一笔交易从提交到被确认的时间是未知的。此外，高性能会带来低安全性，攻击者通过较低的计算成本便能对网络进行攻击[30]。

3.1.2 IoTEX

IoTEX 项目具有很好的可扩性、隐秘性和隔离性。如图 2 所示，在架构上，项目采用包含根链和子链的链中链形式，内部仍然采用链式结构的账本存储。在作用方面，根链为公链，对子链起到管理作用；在扩展性方面，子链可根据需求设计出不同的扩展，以适应物联网功能的多样性；在安全方面，子链遭受攻击不影响根链的运行；在价值方面，子链之间的数据也可借由根链进行转移。

在 IoTEX 项目中，共识机制为基于随机功能可验证的随机共识机制（Roll-DPoS）[31]。IoTEX 以拜占庭容错算法（PBFT）作为基础，对节点进行投票，快速结算，构建高效、可扩展的区块链。

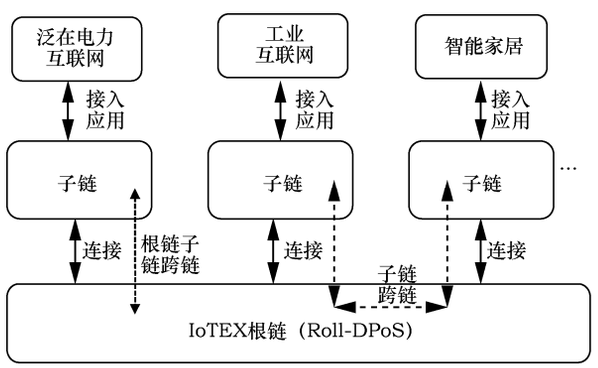

图 2 IoTEX 根链子链结构图

在节点的选择上，为提高效率，系统根据 RDPoS 算法，随机选择小组节点。相比于 DPOS，Roll-DPoS 借鉴 Algorand 算法[32]进行随机节点选择，使每个节点都有机会参与到共识建立中，避免节点的孤立。

将 IoTEX 应用于物联网，虽然通过架构的改变可以适应物联网的分布式环境，并增强共识的随机性，但是对于物联网设备功耗低、存储能力差、通信带宽小的弊端仍未做出应对。

3.1.3 μNEST

μNEST 项目与上述两者较为不同。该项目使用 DPoS 共识机制，DPoS 虽对 PoS 进行了改进并在验证效率以及出块速度上进行优化，但是针对物联网低能耗、高并发的现状仍然束手无策，而且内部的代币机制在物联网领域并不适用。μNEST 团队通过对密码学的研究以及高性能硬件的应用，降低共识机制中的算力消耗，提高物联网设备的计算能力，使得区块链程序可稳定运行于物联网设备之上。目前该项目仍在研发当中。

3.1.4 EOSIoT

EOSIoT 是 EOS 项目的物联网扩展，通过 RFID 系统，可将 RFID 电子标签发送到 EOS 链上，应用于新型供应链、制造、跟踪和访问控制等。该项目区别于上文中将物理设备作为节点，保留区块链和物联网的现有架构，通过智能合约为物联网系统提供基于 EOS 的区块链服务。EOS 采用 DPoS 共识机制。

3.2 共识机制的优劣分析

表 2 结合上述项目以及共识机制，针对现有物联网区块链技术的适用性进行总结比较，共识的应用主要取决于物联网设备的性能、可扩展性以及安全性。μNEST 和 EOSIoT 使用 DPoS 共识，存在的代币机制在物联网领域作用并不大，故可扩展性较差。其中，在 μNEST 项目中采用硬件方式增强设备性能，优化共识算法效率。IoTEX 项

表 2　项目及其共识优缺点

项目名称	共识算法	应用类型	缺点	优点	扩展性	安全性	性能
μNEST	DPoS	公链	去中心化程度低，内部共识依赖代币。节点少时代表性不强	效率上较 PoW 和 PoS 更好，出块速度更快	弱	强	较高
EOSIoT							
IoTEX	Roll-DPoS	公链	依赖代币，选取代表节点方式可能不适用于完全去中心化场景	通过随机选择节点，使每个节点都有机会参与到记账过程中	较强	强	较高
IoTA	DAG	公链	无全局排序，不支持强一性，高效实现较复杂	吞吐量高，异步通信无中央控制	强	弱	高

目采用主子链形式，可扩性强，适用于各种物联网领域，但是对于物联网设备固有弱势并未得到很大的改进，链式账本的存储方式，仍然限制低功耗、弱存储的物联网设备共识一致性的发挥。IoTA 项目采用新颖的 DAG 共识，虽然在性能上得到了提升，且易于扩展，但是在节点数量过少的情况下，去中心化程度远远低于链式结构区块链，引发安全性低、交易验证不及时等风险。对于其他未通过项目使用的共识，PoW 在开放网络中的安全性最高，但是庞大的计算资源需求在物联网设备中实施并不现实，所以项目中并未采用 PoW 共识。PoS 共识相较于 PoW 共识可以显著降低能耗，但仍需要消耗一定的算力资源进行挖矿，对于低功耗的物联网设备而言仍具有一定的运行压力。PBFT 在增加节点数量的同时，会降低全网的性能，且不能提高可靠性。因此，目前所用的大部分共识算法和规则在物联网领域仍然存在诸多可提升的空间。

4　物联网区块链共识机制的优化研究

通过上述分析比对，共识机制在物联网中的应用仍存在不足。结合物联网环境特点，学术界已提出不少优化方案，如表 3 所述，通过共识算法改进、数据层优化、架构服务优化 3 个方面，强化共识规则，助力物联网区块链。

4.1　共识算法改进

共识算法需要依靠节点的计算能力，同时生成的新区块通过共识规则同步至所有的节点进行备份。在物联网领域中存在的远远多于互联网环境的海量异构设备，计算能力和吞吐量都受到自身和运行环境的限制，并且设备存在易入侵、易模拟、易篡改等问题，增加了传统共识在物联网领域的安全隐患。μNEST 中使用硬件提高计算能力的方法并不适用于所有设备。因此如何优化共识机制，在节点选择、降低复杂度、提高安全性和吞吐量等方面至关重要。智能增强助力共识模型如图 3 所示，通过检测节点数据选择正常节点进行共识构建，提升安全性。

（1）恶意检测助力共识机制

Huang 等[33]提出的基于信任的 PoW 机制能有效增强区块链网络安全。在该种机制中，节点是否恶意通过积极部分和消极部分两部分进行衡量，这两部分可以分别通过配置权重进行调控。积极部分通过计算有效交易数量和交易验证数量获得；消极部分由节点进行恶意行为的时间与惩罚系数共同作用决定，其中惩罚系数分为两种，一种是认定节点为懒节点，即在共识过程中出力最少，另一种是认定节点为双花节点，即发送重复交易等恶意攻击。这两种惩罚系数会根据实际情况进行动态调整。通过树莓派进行机制的验证

表 3　物联网区块链共识机制优化研究现状与特点

应用方向	相关工作	概述	性能优势
共识算法改进	基于信任的 PoW 算法改进[33]	对节点的可信任性进行评估，通过系数调节每个节点的挖矿难度	增加恶意节点的算力消耗，使之得不到记账权，同时在选择时降低选中恶意节点的概率，增加容错性
	基于 PBFT 的容错优化[34]	使用离群检测算法，通过数据进行恶意节点划分	将共识算法分层，第一层使用恶意节点检测并分辨出恶意节点，第二层进行 PBFT 共识。增强容错性
	DRL 助力共识机制[35]	使用深度强化学习进行块生成等调整	将 DRL 技术运用于块的生成、调整，动态调节系统达到平衡、高效
	DAG 主链子链结合[36]	基于 DAG 的主链子链形式区分领域和区块	DAG 的主子链形式有效增加了区块链的吞吐量，同时减小了区块数据的存储
数据层优化	基于数据压缩的区块链系统[37]	将区块链中的数据区块进行压缩，降低存储空间，缓解设备存储压力	大大增强设备的存储能力，降低因设备存储空间过小造成的性能问题
	基于 FPGA 存储模块的高性能数据读写架构[38]	制作外部存储模块，通信过程中请求高性能存储模块而非服务器	高性能的存储模块有效提高了数据的读写，降低数据在传输过程中的性能消耗，提高共识效率
	通过边缘计算对数据进行整理优化[39]	通过边缘计算和分布式结合的方式验证数据质量	在区块链架构中提出边缘计算层，改善数据质量和错误数据检测，增强共识容错率
架构服务优化	物联网+区块链架构与服务[40-41]	将区块链中的不同层与物联网中不同层进行结合，构建新架构	架构的整合规避了物联网存在的缺点，将两者结合形成稳定的新结构，使区块链应用于物联网上

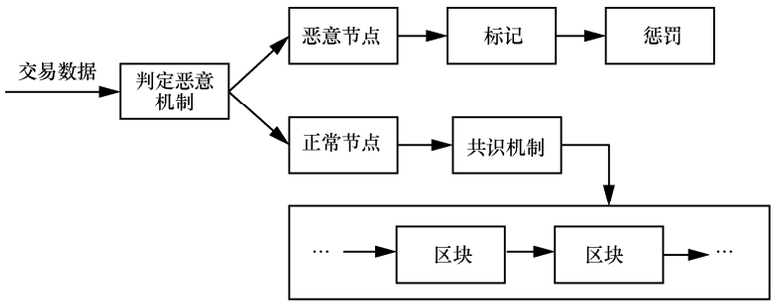

图 3　智能增强助力共识模型

证明，被判定为恶意的节点会设定较高的惩罚系数，产生较大的困难值，节点运行 PoW 共识算法的时间将远远大于正常节点。同时当对节点模拟恶意攻击行为时，消极响应部分的系数会马上呈现增长趋势，此种方式下，增强了传统 PoW 的 51% 容错率，恶意节点将永远得不到记账的权限[33]。通过这种方法进行节点的选择，有效降低非恶意节点的性能消耗，同时，增加恶意节点的 PoW 算法计算复杂性，有助于物联网区块链系统下共识算法的稳定性和健壮性。

Salimitari 等[34]基于 hyperledger fabric 与共识协议 PBFT，提出一种提升物联网区块链容错的恶意检测机制。通过对物联网设备的数据采集，形成数据矩阵 D，并通过离群点检测算法和低秩子空间回复模型训练数据矩阵 D 得到两种概率值：检测概率 P_{d} 和误报概率 P_{fa}，判断异常节点。在该共识机制中，异常节点检测算法作为第一层共识以脚本的形式运行于每个节点中，以验证新数据的兼容性并丢弃可疑数据。算法将不再选择存在恶意数据的节点作为记账节点进行区块链生成，

增强对第二层共识 PBFT 的容错性。在实验中，发现只有当离群检测设置非常不合理且存在误报概率和低检测概率时会出现小于33.3%的容错率。经过大量实验，证明在提升网络性能的同时，根据不同的模型参数，可以得到超过33.3%的容错率，甚至超过 50%。在实验环境下，检测概率 P_d=46%和误报概率 P_{fa}=5%，可得到容错率为 57.82%[34]。结果表明，异常点检测可以大大增强共识算法的容错率，增加物联网区块链网络的稳定及安全。

（2）深度强化学习动态调控共识建立

传统区块链存在一种三元悖论，只能满足三个属性中的两个：分散性、可扩展性、安全性。Liu 等[35]提出一种基于深度强化学习（DRL）技术的物联网区块链动态调整架构。使用 DRL 技术选择、调整块生成器、一致性算法、块大小和块生成间隔，内部结合 PBFT、Zyzzyva[42]和 Quorum[43]提出新的容错共识，以达到扩展性、分散性、安全性和吞吐量的动态平衡。方案分别用基尼系数、成块时延和容错率代表分散性、吞吐量和安全性，使用深度强化学习（主要为 Q-Network）进行训练获得合适的参数以选择合适的块生成节点、共识算法、区块大小以及区块生成间隔时间。经过大量实验，通过与现有未改动系统进行对比，提出的方案具备更高的性能和吞吐量[35]，有效证明该设计对物联网区块链性能的提升，以及对物联网分布式异构架构的动态适应。

（3）DAG 分片技术改进共识规则

作为一种新的区块链架构，基于 DAG 的改进优化也很多。不同于第 3.1.1 节中传统的 DAG 和 3.1.2 节中基于传统链式结构的主子链模式，Jiang 等[36]将 DAG 和主子链优势互补，提出一种基于 DAG 的交叉链解决方案。该方案基于有向无环图的主子链架构，一个领域内的节点共同维护一个账本，构成子链，同时以联盟链的形式将子链连接到主链上进行管理，维护一个主链账本。此种方案将不同节点进行分片共识后连接到主链，解决了因物联网环境中设备众多导致共识难以建立的情况，同时降低了大范围账本同步产生的网络消耗。经过大量实验，在不同内存和不同处理器服务器环境下运行，相比传统区块链，该架构的吞吐量得到明显提升，同时在区块信息的存储上，子链只存储特定领域的区块数据，存储量远远小于主链，降低主链节点和子链节点的存储压力。

4.2　数据层优化

物联网从各种类型终端设备中收集、存储数据并提供中心化服务。如果服务器被攻击，则存在数据泄露的风险。为解决数据集中化存储问题，引入区块链技术，但是轻量级设备的存储能力低下导致区块链共识机制无法长期运行。同时，物联网感知层各种传感器产生实大量实时数据，如果全交由区块链进行存储，会对节点和网络产生巨大的压力。

（1）区块压缩机制节省存储空间

结合共识规则，将早期数据进行压缩处理，保证区块链一致性的同时降低区块数据的存储，是解决物联网设备存储限制的一种方式。Kim 等[37]提出一种区块压缩存储的方式，提高设备存储空间。物联网设备的不间断运行将产生海量的实时数据，此类数据具有数据量大、有效期短等特性，在保证区块链共识建立前提下进行前置区块的有效压缩，可以保证区块链网络中轻量级物联网设备中的存储容量。当物联网设备节点加入网络后，要求向全网同步节点的存储能力。改进 PBFT 共识，如图 4 所示，在选择 Leader 节点进行交易成块的过程中，通过对自身设备存储能力的评估；若小于设置的阈值，则正常进行共识机制的建立：若大于设置的阈值，则启动数据压缩程序，将原有区块进行压缩，即通过 Hash 运算生成新区块，新区块的父区块 Hash 值即为压缩后区块 Hash 值，并对压缩后的区块以及新生成区块进行全网节点同步操作，全网节点更新成最新的区块链。基于区块压缩的区块链模型和传统区块链模型进行对

比，随着节点数量的增加，成块时延增加幅度小于 1 s，区块链每个数据块平均存储空间减少近63%，运行一段时间后，压缩模型在总存储上减少约 63%的空间，并趋于稳定[37]。虽然压缩算法消耗一定的成块时间，但是结合共识进行数据压缩，有效解决在物联网设备中数据存储空间不足的问题。

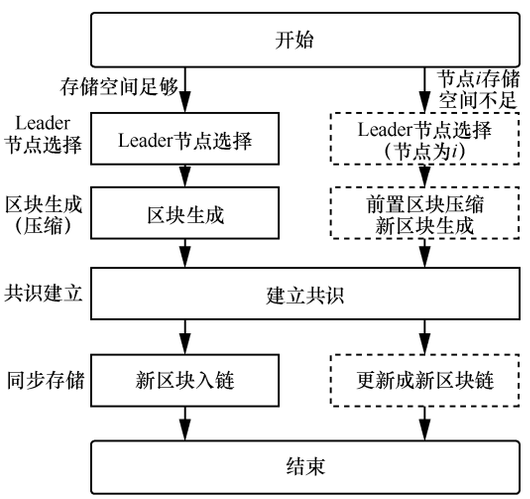

图 4　区块压缩模型[31]

（2）高性能缓存与边缘计算提升吞吐量

物联网设备的异构数据与低通信带宽之间仍存在矛盾，大量异构数据在低带宽的信道中传输时延必然会大大影响区块链一致性算法的运行，影响共识的建立。Sakakibara 等[38]提出一种高性能缓存设备以提升读写性能。将外置高效读写设备制作成的硬件缓存模块加入物联网，将交易信息存储在缓存模块中，减少服务器的工作量，并提高物联网区块链中物理设备的存储能力。在网络中，若缓存中存在目标数据，则直接在缓存模块中读取，反之，则向节点获取。使用缓存技术，减轻数据在网络中的资源消耗，提高吞吐量。经过大量实验，使用缓存模块的物联网区块链比不使用吞吐量小了好几倍。随着交易量的增加，吞吐量呈现反比曲线，并逐渐收敛趋于稳定，而缓存中数据的命中率则随着交易数量的不断增加呈现正比趋势，不断提高[38]。这说明缓存模块的应用有效降低物联网区块链中因异构数据传输导致的吞吐量的提高，降低低带宽通信给设备造成的负荷。同时，也可采用基于博弈论的分布式合作算法[33]，通过在网络边缘设备中改善数据质量、进行错误数据检测，增强入链数据的安全性，提高网络吞吐量。

4.3　架构服务优化

区别于第3.1.4节中通过智能合约将区块链作为云端服务对边缘设备提供服务的方式，将区块链和物联网的不同层结合形成新的架构[40-41]。如图 5 所示，通过网关、路由等网络设备对网络中的物联网设备节点进行互联，同时在本地和云端构建数据存储仓库，以保证物联网设备的数据存储问题。在节点网络中，将具备高性能运算能力及高可用存储能力的节点设置为全节点，将功耗低且存储能力较弱的节点设置为轻节点。全节点具备参与维护账本的能力，与其他全节点共同建立共识，同步账本；轻节点不参与账本的维护，只进行区块头信息的同步（例如当区块链网络中出现新区块时，轻节点仅下载区块头，并发送特定状态的默克尔证明请求）。在此类架构下，区块链和物联网有机结合，设备作为区块链的轻节点存在，共同维护一个网络。经过模拟，该架构能有效解决物联网设备无法满足区块链算力需求和账本存储的问题，为区块链和物联网的结合提供新思路。

区块链也可以通过智能合约对物联网提供数据防篡改、数据溯源、信任凭证等业务，此类应用中，物联网不参与对区块链的维护。

5　物联网区块链共识机制优化的研究展望

通过以上阐述可知，物联网和区块链的结合主要受限于设备计算能力、存储能力和吞吐量。针对目前区块链共识可扩展性差、算力消耗巨大、交易确认效率低下、节点容错性与性能难以平衡等问题，在物联网与区块链结合时，如何选择符合物联网场景的共识算法，如何指定符合物联网

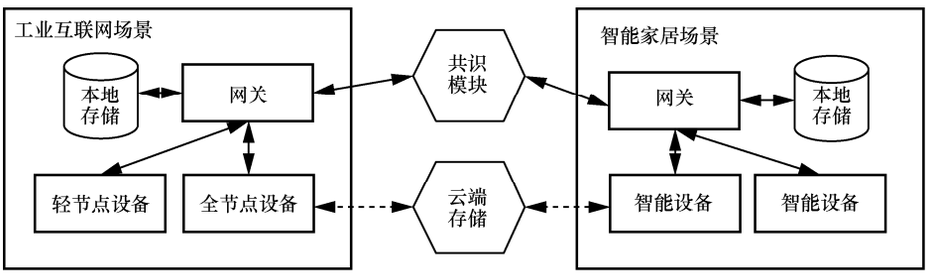

图 5　区块链+物联网新架构

业务场景的共识规则，如何确保网络的安全性、稳定性、扩展性还有许多工作需要开展和完善。结合目前的研究，表 4 从共识机制的智能增强、数据的合理优化、物联网区块链新架构和交易性能提升 4 个方面进行展望。

表 4　物联网区块链共识机制优化研究方向展望

研究方向	简要概述
共识机制的智能增强	（1）结合人工智能创新共识机制
	（2）传统共识智能优化
	（3）智能主力 DAG
	（4）大规模分布式共识机制研究
数据的合理优化	（1）区块数据存储优化
	（2）存储模式性能优化
物联网区块链新架构	（1）轻节点应用研究
	（2）侧链和扩展性研究
交易性能提升	（1）雾节点计算的应用
	（2）面向区块链的计算芯片研制
	（3）轻量级密码的研究应用
	（4）面向物联网区块链的分片技术

5.1　共识机制的智能增强

人工智能是一门用人工方法，模拟、延伸和扩展人的智能，通过对数据的挖掘、分析、训练，实现机器智能化的科学技术。区块链与人工智能结合，为区块链内部增强、外部治理智能化提供方向。人工智能与物联网区块链共识机制的结合，主要在以下几个方面进行深入扩展。

（1）结合人工智能创新共识机制[44]。目前的共识主要从证明类共识和拜占庭类共识中进行选择，并无法完全适用于物联网的特殊环境，结合物联网数据实时要求高、数据量大的特点，并根据学习模型的质量，搜索策略的有效优化以及数据质量等开创基于 AI 的共识新机制。

（2）传统共识智能优化。利用深度强化学习的感知和决策能力，对传统共识的算力消耗、Leader 节点选择等进行智能化改进，以达到合理分布物联网区块链算力、增强网络容错性以及强化去中心化特性的目的。

（3）智能助力 DAG[45]。有向无环图的新型共识机制模式目前仍然处于发展阶段，使用 AI 技术强化 DAG 在交易确认和安全性方面的缺点，也是需要进行深入研究的方向。

（4）大规模分布式共识机制研究。物联网实质上是一个大型分布式系统，海量节点导致的网络拓扑错综复杂，可通过对分布式共识机制的研究，建立多层共识机制，使不同区域建立共识后再向上进行共识，直至全网达成共识，达到降低吞吐量和缓解算力消耗限制的目的。

5.2　数据的合理优化

区块链由于吞吐量的限制无法适应物联网实时大数据的环境，因此，对于数据而言可以进行以下研究。

（1）区块数据存储优化[46]。物联网设备数据具备实时性特点，一些早期入链的数据除了进行共识机制的建立外已经没有用处。因此，如何在不影响共识机制建立的前提下，合理地删减区块

链存储的账本数据，使区块账本数据可持续存储可深入研究的数据。

（2）存储模式性能优化。由于物联网设备存储能力低下，可深入研究如何改进现有的存储模式，运用缓存机制或改进区块存储中间件，增强区块数据的读写能力，适应物联网的低带宽数据传输网络。

5.3 物联网区块链新架构

物联网算力低、存储空间小的弊端限制了区块链技术完全应用于物联网环境，但是两者的分层结合仍然可以为物联网提供强有力的辅助。主要可以从以下几个方面展开。

（1）轻节点的应用研究[47]。轻节点的特点是只对区块头进行数据同步，可以在存储性能不同的物联网设备上构建基于轻节点和全节点的区块链架构，合理进行共识机制的建立以及区块的同步存储。

（2）侧链和扩展性研究[48]。通过侧链技术对物联网区块链应用的领域进行有效扩展，实现更加灵活的用户自定义。如何设计侧链、如何强化扩展属性以及如何在侧链之间实现数据的交互是未来的研究方向。

5.4 交易性能的提升

交易性能是区块链在物联网领域无法得到有效利用的限制条件之一，面对物联网的海量数据环境，区块链的吞吐量无法得到彻底满足。因此，对于改善区块链的吞吐性能，以下方向可进行研究。

（1）雾节点计算的应用[49]。雾计算作为一种新的计算范例，将存储和计算下沉到靠近数据生成的位置，在物联网末梢端建立本地小型云，实现本地化计算或存储，降低消息的带宽占用，减少中心节点的计算压力，加快共识机制的建立。

（2）面向区块链的计算芯片研制。设备计算性能低下主要受限于处理器性能，可研制面向区块链的计算芯片，增加物联网和区块链的兼容性。

（3）轻量级密码的研究应用[50]。区块链是密码学的应用体现，使用安全的轻量级密码代替原有的高消耗密码，提高运算效率，是研究的重点之一。

（4）面向物联网区块链的分片技术[51]。分片的原理是将一个大型数据库分割成小的数据碎片，并将碎片存储于不同的服务器上。将共识机制与分片技术结合，能有效改善区块链的一致性共识建立速度。

6 结束语

物联网作为未来发展的关键领域之一，与具备去中心化、数据不可篡改、集体维护等特性的区块链结合，或将在海量异构终端设备的可信安全接入以及数据安全管理方面产生颠覆性的影响，成为改变未来不可或缺的技术之一。从最新的研究中可以看出，在共识机制的增强、数据的合理优化、物联网区块链新架构以及交易性能提升等方向，物联网和区块链的结合还存在亟待解决的问题，值得进一步深入研究。

参考文献：

[1] KHODADAD F, DASTJERDI A V, BUYYA R. Internet of things: an overview[M]. San Francisco: Margan Kaufmann, 2016.

[2] ASHTON K. That ‘internet of things’ thing[J]. RFID journal, 2009, 22(7): 97-114.

[3] WANG X, ZHA X, NI W, et al. Survey on blockchain for internet of things[J]. Computer Communications, 2019(107): 10-29.

[4] 张玉清, 周威, 彭安妮. 物联网安全综述[J]. 计算机研究与发展, 2017, 54(10): 2130-2143.
ZHANG Y Q, ZHOU W, PENG A N. Survey of internet of things security[J]. Journal of Computer Research and Develpoment, 2017, 54(10): 2130-2143.

[5] 邵奇峰, 金澈清. 区块链技术:架构及进展[J]. 计算机学报, 2018, 41(5): 3-22.
SHAO Q F, JIN C Q. Blockchain: architecture and research progress[J]. Chinese Journal of Computer, 2018, 41(5): 3-22.

[6] 李董, 魏进武. 区块链技术原理、应用领域及挑战[J]. 电信科学, 2016, 32(12): 20-26.
LI D, WEI J W. Theory, application fields and challenge of the blockchain technology[J]. Telecommunications Science, 2016,

32(12): 20-26.

[7] PAN J, YANG Z. Cybersecurity challenges and opportunities in the new edge computing+ IoT world[C]// The 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, Mar 19-21, 2018, Tempe, AZ, USA. NewYork: ACM Press, 2018: 29-32.

[8] MILLER A, JUELS A, SHI E, et al. Permacoin: repurposing bitcoin work for data preservation[C]// 2014 IEEE Symposium on Security and Privacy, May 18-21, 2014, Berkeley, CA, USA. Piscataway: IEEE Press, 2014: 475-490.

[9] CASTRO M, LISKOY B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

[10] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//The Thirteenth EuroSys Conference, April 23-26, 2018, Porto, Portugal. New York: ACM Press, 2018: 30.

[11] ABDBD-EL-MALEK M, GANGER G R, GOODSON G R, et al. Fault-scalable byzantine fault-tolerant services[J]. ACM SIGOPS Operating Systems Review, 2005, 39(5): 59-74.

[12] COWLING J, MYERS D, LISKOY B, et al. HQ replication: A hybrid quorum protocol for Byzantine fault tolerance[C]// The 7th symposium on Operating systems design and implementation, November 6-8, 2006, Seattle, WA, USA. Berkeley: USENIX, 2006: 177-190.

[13] MARTIN J P, ALVISI, L. Fast byzantine consensus[J]. IEEE Transactions on Dependable & Secure Computing, 2006, 3(3): 202-215.

[14] VERONESE G S, CORREIA M, BESSANI A N, et al. Spin one's wheels? byzantine fault tolerance with a spinning primary[C]//28th IEEE Symposium on Reliable Distributed Systems (SRDS 2009), September 27-30, 2009, Niagara Falls, New York, USA. Piscataway: IEEE Press, 2009: 135-144.

[15] CLEMENT A, WONG E L, ALYISI L, et al. Making byzantine fault tolerant systems tolerate byzantine faults[C]// NSDI, Apr 22-24, 2009, Boston, MA, USA. Berkeley: USENIX, 2009: 153-168.

[16] POPOV S. The tangle[EB]. 2019.

[17] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11):93-104.
YONG Y, NI X C, ZENG S, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 93-104.

[18] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB]. 2008.

[19] COURTOIS N T. On the longest chain rule and programmed self-destruction of crypto currencies[J]. arXiv:1405.0534, 2014:1-89.

[20] LARIMER D. Delegated proof-of-stake[EB]. 2014.

[21] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol[C]//Annual International Cryptology Conference, August 20-24, 2017, Santa Barbara, CA, USA. Piscataway: IEEE Press, 2017: 357-388.

[22] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity: extending bitcoin's proof of work via proof of stake[J]. IACR Cryptology ePrint Archive, 2014: 452.

[23] BACK A, CORALLO M, DASHJR L, et al. Enabling blockchain innovations with pegged sidechains[EB]. 2014.

[24] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-ng: a scalable blockchain protocol[C]//13th Symposium on Networked Systems Design and Implementation, March 16-18, 2016, Santa Clara, CA, USA. Berkeley: USENIX Association, 2016: 45-59.

[25] UNDERWOOD S. Blockchain beyond bitcoin[J]. Communications of the ACM, 2016, 59(11), 15-17.

[26] NOMURA Research Institute. Survey on blockchain technologies and related services FY2015 Report[EB]. 2015.

[27] MILLER A, JUELS A, SHI E, et al. Permacoin: repurposing bitcoin work for data preservation[C]//2014 IEEE Symposium on Security and Privacy, May 18-21, 2014, Berkeley, CA, USA. Piscataway: IEEE Press, 2014: 475-490.

[28] CHEN L, XU L, SHAH N, et al. On security analysis of proof-of-elapsed-time (poet)[C]// International Symposium on Stabilization, Safety, and Security of Distributed Systems, November 5-8, 2017, Boston, MA, USA. New York: ACM Press, Cham, 2017: 282-297.

[29] CLARK J, ESSEX A. Commitcoin: carbon dating commitments with bitcoin[C]//International Conference on Financial Cryptography and Data Security, Februray 27-March 2, Kralendijk, Bonaire. Berlin: Springer, 2012: 390-398.

[30] LATHIF, MOHAMED R A, PEZHMAN N. CIDDS: aconfigurable and distributed DAG-based distributed ledger simulation framework[C]// The 19th International Middleware Conference (Posters), December 10-14, 2018, Rennes, France. New Yew: ACM Press, 2018:7-8.

[31] FAN X, CHAI Q, Roll-DPoS: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems[C]//Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, November 5-7, 2018, New York, USA. New Yew: ACM Press,2018:482-484.

[32] GILAD Y, HEMO R, MICALI S, et al. Algorand: Scaling byzantine agreements for crypto currencies[C]// The 26th Symposium on Operating Systems Principles, October 28-28, 2017, Shanghai, China. New York: ACM Press. 2017: 51-68.

[33] HUANG J, KONG L, CHEN G, et al. Towards secure industrial IoT: blockchain system with credit-based consensus mechanism[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 1-1.

[34] SALIMITARI M, MOHSEN J, MAINAK C. An outlier-aware consensus protocol for blockchain-based IoT networks using hyperledger fabric[J]. 2019. arXiv:1906.08177.

[35] LIU M, YU R, TENG Y, et al. Performance optimization for blockchain-enabled industrial internet of things (iiot) systems: A deep reinforcement learning approach[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3559-3570.

[36] JIANG Y M, CHEN X W, HUANG Y, et al. A cross-chain solution to integration of IoT tangle for data access manage-

ment[C]// 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Dec 20-22, 2018, Hammamet, Tunisia. Piscataway: IEEE Press, 2018:1035-1041.

[37] KIM T, JAEWON N, SUNGH Y C. SCC: storage compression consensus for blockchain in lightweight IoT network[C]// 2019 IEEE International Conference on Consumer Electronics (ICCE), Jan 11-13, 2019, Las Vegas, NV, USA. Piscataway: IEEE Press, 2019: 1-4.

[38] SAKAKIBARA Y, NAKAMURA K, MATSUTANI H. An FPGA NIC based hardware caching for blockchain[C]// The 8th International Symposium on Highly Efficient Accelerators and Reconfigurable Technologies, June 7-9, 2017, Bochum, Germany. New York: ACM Pres, 2017: 1.

[39] CASADO V R, DELA P F, PRIETO J, et al. Blockchain framework for IoT data quality via edge computing[C]// The 1st Workshop on Blockchain-enabled Networked Sensor Systems, November 4, 2018, Shenzhen, China. New York: ACM Press, 2018: 19-24.

[40] SAGIRLAR G, CARMINATI B, FERRARI E, et al. Hybrid-iot: hybrid blockchain architecture for internet of things-pow sub-blockchains[C]// 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), July 30-Aug 3, 2018, Halifax, NS, Canada. Piscataway: IEEE Press, 2018: 1007-1016.

[41] DORRI A, KANHEREE S S, JURDAK R, et al. LSB: A lightweight scalable blockchain for IoT security and privacy[J]. Journal of Parallel and Distributed Computing, 2019, 134: 180-197.

[42] KOTLA R, ALVISI L, DAHLIN M, et al. Zyzzyva: speculative byzantine fault tolerance[J]. ACM Transactions on Computer Systems (TOCS), 2009, 27(4): 7.

[43] AUBLIN P L, GUERRAOUI R, KNEZEVIC N, et al. The next 700 BFT protocols[J]. ACM Transactions on Computer Systems (TOCS), 2015, 32(4): 12.

[44] SALAH K, RHMANE M H, NIZAMUDDIN N, et al. Blockchain for AI: review and open research challenges[J]. IEEE Access, 2019(7): 10127-10149.

[45] PERVEZ H. A comparative analysis of DAG-Based blockchain architectures[C]//2018 12th International Conference on Open Source Systems and Technologies (ICOSST), Dec 19-21, 2018, Lahore, Pakistan Piscataway: IEEE Press, 2018.

[46] 陈烨, 许冬瑾, 肖亮. 基于区块链的网络安全技术综述[J]. 电信科学, 2018, 34(3): 10-16.
CHEN Y, XU D J, XIAO L. Survey on network security based on blockchain[J]. Telecommunications Science, 2018, 34(3): 10-16.

[47] REILLY E. An IoT integrity-first communication protocol via an ethereum blockchain light client[C]// 2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT), May 27, 2019, Montreal, QC, Canada. Piscataway: IEEE Press, 2019: 53-56.

[48] 闵新平, 李庆忠, 孔兰菊, 等. 许可链多中心动态共识机制[J]. 计算机学报, 2018, 41(5): 39-54.
MIN X P, LI Q Z, KONG L J, et al. Permissioned blockchain dynamic consensus mechanism based multi-centers[J]. Chinese Journal of Computers, 2018, 41(5): 39-54.

[49] XIONG Z, FENG S , WANG W, et al. Cloud/fog computing resource management and pricing for blockchain networks[J]. IEEE Internet of Things Journal, 2017, 6(3): 4585-4600.

[50] 武传坤.物联网安全关键技术与挑战[J]. 密码学报, 2015, 2(1):40-53.
WU C K. An overview on the security techniques and challenges of the internet of things[J]. Journal of Cryptologic Research, 2015, 2(1): 40-53

[51] WEI T, DONGX W, SHEN Y L, et al. A hierarchical sharding protocol for multi-domain IoT blockchains[C]// ICC 2019 - 2019 IEEE International Conference on Communications (ICC), May 20-24, 2019, Shanghai, China. Piscataway: IEEE Press, 2019: 1-6

[作者简介]

宋琪杰（1994− ），男，浙江工业大学计算机科学与技术学院硕士生，主要研究方向为区块链和物联网安全。

陈铁明（1978− ），男，博士，浙江工业大学计算机科学与技术学院教授，主要研究方向为网络空间安全与大数据智能分析。

陈园（1994− ），女，浙江工业大学计算机科学与技术学院硕士生，主要研究方向为物联网安全。

马栋捷（1994− ），男，浙江工业大学计算机科学与技术学院硕士生，主要研究方向为信息安全。

翁正秋（1981− ），女，浙江工业大学计算机科学与技术学院博士生，温州职业技术学院大数据技术与应用专业负责人、副教授，主要研究方向为数据安全与大数据技术。