物链网综述：区块链在物联网中的应用

史慧洋[1], 刘 玲[2,1], 张玉清[1,2]

[1]中国科学院大学 国家计算机网络入侵防范中心 北京 中国 101408
[2]西安电子科技大学 网络与信息安全学院 西安 中国 710071

摘要 物联网设备数量的激增和中心化的管理架构给物联网的发展带来了严峻的挑战, 区块链技术的去中心化和不可篡改等特点可以用来解决物联网的上述难题, 故此将区块链技术应用到物联网领域成为研究热点。随着区块链技术在物联网应用中的深入研究, 出现了一个新的概念: “物链网”。本文首先介绍了物联网的行业痛点和区块链相关技术, 然后分析了将区块链技术应用到物联网领域的论文和白皮书, 把融合文献分为平台架构和应用场景两类后, 进行归纳总结, 并调研了应用领域的典型公链和商业项目, 指出了将区块链技术应用于物联网领域所面临的挑战与机遇, 讨论了相应的解决方案, 最后展望了“物链网”未来的发展趋势, 提出未来研究方向应侧重于数据存储和数据管理方向。

关键词 物联网; 区块链; 物链网; 去中心化
中图法分类号 TP309.2 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2019.09.07

A review of BoT: Blockchain for the Internet of Things

SHI Huiyang[1], LIU Ling[2,1], ZHANG Yuqing[1,2]

[1] National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 101408, China
[2] School of Cyber Engineering, Xidian University, Xi’an 710071, China

Abstract The surge in the number of IoT devices and the centralized management structure have brought severe challenges to the in-depth development of the Internet of Things. The decentralization and non-tamperability of blockchain technology can be used to solve the above problems of the Internet of Things. Applying blockchain technology to the field of Internet of Things has become a research hotspot. With the deepening of the application research of blockchain technology in the Internet of Things, a new concept emerged: “BoT”. This paper first introduces the industry pain points and blockchain related technologies of the Internet of Things, then analyzes and summarizes the papers and white papers that apply blockchain technology to the Internet of Things field, classifies the fusion documents into two categories: platform architecture and application scenarios, summarizes them, and investigates typical projects and commercial projects in the application field, pointing out that the blockchain technology is applied to the challenges and opportunities faced by the Internet of Things field. The corresponding solutions are discussed. Finally,we look forward to the future development trend of the "BoT" and proposes that the future research direction should focus on data storage and data management.

Key words IoT; Blockchain; BoT; Decentration

1 引言

物联网是一个涵盖所有与互联网相连事物的总称。系统架构主要可分为三层: 感知层、网络层, 应用层。物联网在长期发展演进过程中, 让人们生活趋向智能化, NB-IoT 和 5G 等技术的发展让万物互联成为现实, 物联网应用正在向制造、政务、金融、交通、医疗等领域发展, 但同时也带来了数据存储、数据传输、设备安全、隐私泄露、通信兼容等问题[1], IoT 最大的问题是成本高, 其次是数据一致性和安全问题, 面临的挑战如下: 1)成本高: 中心化的平台需要维护, 升级, 成本压力较大, 传输海量数据也会产生较高的成本; 2)安全性差: 大多数物联网设备会接触更多隐私, 存在很多漏洞, 并且物联网以中心化的方式部署, 更容易受到恶意软件, 黑客的攻击; 3)隐私泄露: 物联网设备连接的传感器自动化搜集各种信息和数据, 这些数据可能会被恶意收集甚至泄露, 信息分散性造成了信息孤岛现象, 难以确保数据的

通讯作者: 史慧洋, 硕士研究生, 工程师, Email:shihuiyang@ucas.ac.cn。
本论文得到国家重点研发计划基金资助项目（No.2016YFB0800700）；国家自然科学基金资助项目（No.U1836210，No.61572460）资助。
收稿日期: 2019-05-31; 修改日期: 2019-08-17; 定稿日期: 2019-08-20

准确性、完整性; 4) 兼容性差: 目前物联网的发展还处于碎片化阶段, 底层智能硬件接口之间的传输协议不兼容[2]; 5)可靠性, 扩展性差: IoT 设备的分布式特点导致设备管理困难, 使系统的可靠性较差; 6)协作困难: 越来越多的应用场景需要跳出单个角色, 涉及多个对等实体间的协作, 因此建立信任机制的成本提高。

2008 年, 中本聪发表了一篇论文——比特币: 一种点对点式的电子现金系统[3], 区块链技术逐渐进入到公众的视野, 它本质上是一个去中心化的分布式数据库, 以块的形式存储数据。这些区块通过哈希的方式按时间顺序串在一起, 形成一条不可篡改的链, 并将该链共享且分发给所有参与实体。区块链最大的特点在于去中心化, 通过数据的存储方式、共识机制、加密算法等一些关键技术的配合, 在节点互不信任的系统中实现点对点的可信交易。共识机制主要包括: 工作量证明(PoW)、权益证明(PoS)、工作量证明与权益证明混合(PoS+PoW)、股份授权证明(DPoS)、实用拜占庭容错(PBFT)、改进的拜占庭容错(DBFT)、Tendermint 算法等。

区块链 1.0: 以比特币为代表的虚拟货币的时代, 特点为去中心化的数字货币交易, 结合了点对点共享和加密技术, 主要是数字货币支付、流通等职能应用, 具有分布式账本、链式数据、梅克尔树、工作量证明等特征。区块链 2.0: 其核心技术为智能合约, “以太坊”是区块链 2.0 的主要代表, 拥有自由的协议, 提供了让用户用以搭建应用的各种模块的平台, 可以极大增强数字经济中信息和价值共享的方式, 使区块链技术可应用于更多场景。区块链 3.0: 智能化社会时代, 超出金融领域, 为去中心化方案应用到各个行业当中, 同时保证高性能, 3.0 将更具实用性, 不再通过第三方获取信任与建立信用, 可以提高整体系统的工作效率。

由此看来, 区块链 1.0 是区块链技术的萌芽, 2.0 是区块链在金融、智能合约方向的技术落地, 3.0 则是解决各行业互信问题与数据传递安全性的技术实现[4]。区块链有着巨大的优势, 并开始在一些领域应用, 如金融行业, 支付行业, 物联网行业, 食品安全行业, 公共服务行业等, 但也面临着亟待解决的问题, 如: 不可篡改、无法撤销、无隐私、性能问题等, 优缺点见表 1。

随着区块链技术在各行业领域的不断应用, 共识机制、私钥管理和智能合约等面临的问题逐渐凸显, 安全事件层出不穷, 区块链架构分为: 存储层、协议层、扩展层和应用层[5]。各个层次面临的安全风险如下, 存储层安全风险包括: 数据泄漏、网络攻击和设备安全, 协议层包括来自协议漏洞、流量攻击、恶意节点的威胁, 区块链常见的攻击手段包括 eclipse 攻击、sybil 攻击、算力攻击和分叉攻击, 扩展层一般指来自代码的智能合约漏洞, 应用层涉及应用软件漏洞、DDoS 攻击、私钥管理等。

表 1 区块链优缺点

Table 1 Advantages and Disadvantages of Blockchain

优点	缺点
去中心化,分布式核算和存储 区块链的数据对所有人公开, 整个系统信息高度透明 采用基于协商一致的规范和协议 信息不可篡改,数据稳定可靠性 无须通过公开身份的方式让对方自己产生信任	能耗高, 消耗了大量能源 公链上交易数据公开透明, 不利于隐私保护 交易要被大多数节点认可, 下载、验证慢 操作不可逆转, 区块链数据无法变动 交易数据增大造成效率低下

此外, 我们列举了协议层上针对核心机制的下述几种典型攻击, 包括: 1. 以共识机制为目标的针对性攻击, 造成链上记录被篡改, 实现攻击者对区块链网络的高度控制权; 2. 分布式的存储机制增加了安全威胁, 攻击者获得数据的机会增加, 区块链系统内的攻击持续时间更长; 3. 密码学机制本身有一定的风险, 私钥丢失意味着资产的损失, 我们也无法找回, 量子计算技术的发展, 对于加密算法来说是个潜在的威胁。

我们通过调研 80 余篇区块链物联网应用方面的重要研究成果, 论文来源包括但不局限于 Web of Science、IEEE Xplore、Elsevier、Google Scholar、区块链项目白皮书和社区网站等在线资源, 文章调研范围从 2016 年开始, 2016 年是融合的开端, 2018 年出现爆发式增长, 其中 2019 年的文献只统计到 4 月份, 近 4 年的文章分布情况见图 1。

图 1 Blockchain-IoT 融合文献情况

Figure 1 The Situation of of Blockchain and IoT Integration Literature

物联网解决生产力问题, 区块链解决生产关系的问题, “物链网”是一个新概念, 代表物联网与区块链之间的融合, 2018 年, 微软、IBM 等公司在物联网行业会议(“物联网+区块链”应用峰会)上正式提出此概念, 被称为万物的区块链, 英文缩写为: Blockchain of Things, 定义为: 物链网 = 物联网 ×区块链, 物联网中的终端智能设备只进行数据传输和加密, 工作量计算由验证节点负责, 进行交易结算, 用户数据得到有效保障, 物联网也逐步向区块链网络转型。

区块链技术中的公开透明、共识机制、不可篡改解决物联网中的设备安全和设备激增问题, 区块链采用链式结构和智能合约技术, 哈希树结构可以用来进行数据处理, 解决了数据隐私问题, 因此, 区块链技术的引入解决了物联网中遇到的最大难题, 促进了物链网的应用实现。

本文的主要贡献如下: 1. 分析物链网的研究现状, 把现有的融合技术研究成果分为平台应用和场景应用, 平台应用细分为: 数据管理、网络攻击、身份验证、隐私等七部分, 应用场景分为工业 4.0、车联网、智慧城市供应链和健康医疗等方面, 首次系统总结并阐述文献提出的解决方案; 2. 分析物链网的典型公链和其他商业应用, 指出公链的架构设计、机制、应用领域; 3. 指出物链网的挑战和机遇, 挑战包括延迟、高能耗、隐私安全, 数据存储等, 并指出未来的研究方向。

本文章节安排如下: 第二节是本文重点, 详细论述了区块链物联网的融合现状, 并做简要总结; 第三节介绍融合中的应用: 包括典型公链和商业项目; 第四节总结并指出未来的研究方向; 第五节为结束语。

2 区块链在物联网中的应用

物链网解决了物联网发展中遇到的痛点, 可以看作是物联网的进化形态, 区块链技术中的去中心化, 可溯源特性解决了传输数据的安全性和可信性。2017 年, 遨天摩公司开展的优物链计划是物链网的第一个生态, 代表了未来物联网的发展趋势。基于区块链的技术特点, 它会首先在以下四大领域应用: 物联网、医疗大数据、供应链数据管理、身份数据管理, 典型应用如: 车联网、智能家居、智慧医疗、工业物联网等, 本文讨论其在物联网中的应用[6]。

区块链的共识机制, 不可变更的特点保证了它可以在彼此没有信任的人或机构间建立合作关系, 随着区块链在物联网中的深入研究, 各国政府也开始重视区块链技术, 实现政务数字化, 图 2 是区块链技术和物联网融合进展图。

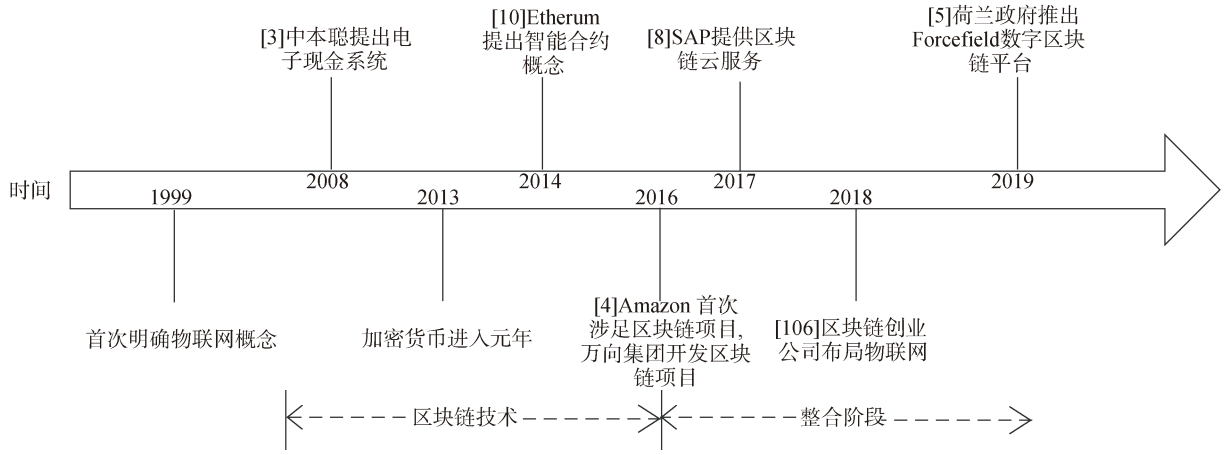

图 2 区块链技术和物联网融合的进展

Figure 2 Progress in the integration of blockchain and IoT

区块链物联网的基础架构分为四层: 感知层、公链层、合约层、应用层。公链层, 合约层统称区块链层, 感知层上搜集到的数据和信息在公链层传输, 一旦上链, 数据不可篡改, 通过 P2P 网络的形式实现信息传输, 在合约层上, 通过智能合约的运行实现系统的运行, 融合架构见图 3。

2.1 区块链与物联网融合的优点

随着 IoT 设备的数量激增, 智能设备快速发展, 造成隐私保护困难, 运维成本高等问题, 区块链技术可以解决物联网中遇到的上述挑战。

1) 数据存储

物联网的应用越来越广泛, 物联网设备收集的

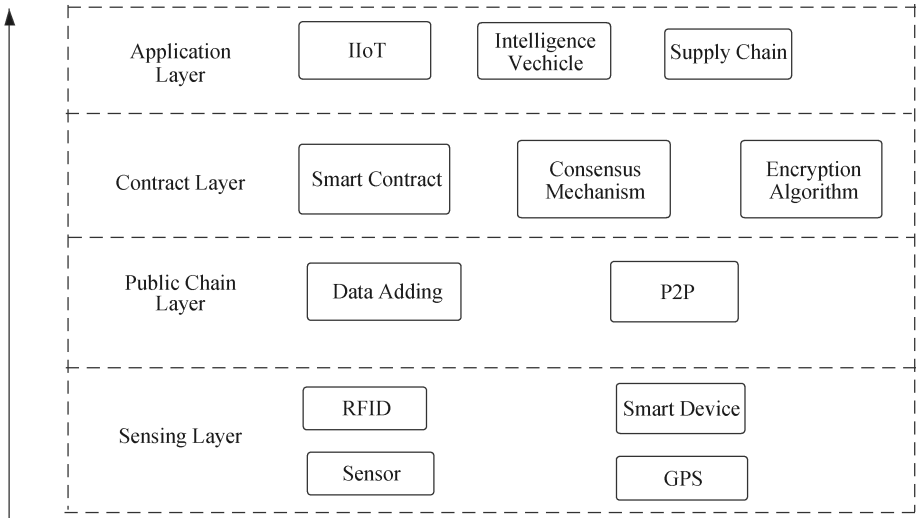

图 3　区块链物联网融合基础架构

Figure 3　Architecture for Blockchain-IoT

信息也越来越庞大，并且会持续增长。由于物联网是集中式部署，如何存储传感器收集的海量数据成为了一个挑战。区块链一个是去中心化、分布式连接的对等网络，节点之间完全平等，利用这个特性可解决物联网中海量数据需要汇聚到单一的控制中心集中存储的问题，从而在一定程度上缓解存储压力。

2) 数据传输，跨主体协作

区块链的互信机制可以使物联网收集到的数据和信息跨过第三方中介进行传播，提高了数据和信息在网络中的传输速率，减少传播时延。采用链下存储，只在需要的时候请求传输数据，可以减少网络的使用带宽，提高传输速率，同时公开透明的算法打破了信息孤岛的束缚，使信息充分地横向交流，多主体协作[7]。

3) 身份鉴权

区块链中的身份验证技术利用加密数字签名，散列技术来实现，去中心化的身份识别系统不受任何机构控制，这样能保证用户完全掌握自己的身份信息，区块链的验证和共识机制有助于避免非法或者恶意的节点接入物联网，提升系统安全性。

4) 隐私保护

物联网数据规模的增大、设备可能存在的漏洞、数据的集中存储和管理都给物联网的隐私保护增加了难度。物联网节点由各种传感器构成，主要负责收集数据，功能比较局限，对系统安全的检测能力较低甚至是没有[8]，区块链采用去中心化的分布式存储方式，使数据分布在各个网络节点，且运用非对称密码学技术对数据进行加密，为物联网的隐私保护提供了解决办法。

5) 降低成本

在物联网中应用区块链技术的去中心化结构，无需设立为全局服务的中心服务器，减去了中心服务器在能耗和企业成本支出方面存在巨大压力，节省了昂贵的运维费用[9]，应用智能合约的互信机制也可消除与第三方通信的成本。

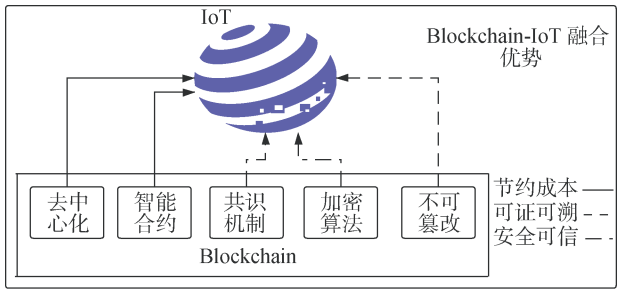

图 4　区块链物联网融合技术

Figure 4　The Technology of Blockchain-IoT integration

6) 可证可溯

在区块链中，修改区块计算力太大，因此链上的区块基本不可能被破坏，这意味着一定能达成共识[10]。同样，数据只要经过共识写入区块链，就难以篡改，并且在其链式结构中，除了第一个区块，其余的每一个区块都包含了上一区块的信息。在物联网中，可以依托此技术进行物联网应用的追本溯源。

区块链的信息不可篡改、去中心化特点减少了中心化运维带来的成本，加密技术和共识机制算法使身份认证安全可信，区块链的链式结构特点使数据可溯源，不仅促进了通信安全，解决数据库冗余问题，也使得系统更具灵活性，可自由添加新的设

备, 鉴于上述优势, IBM、微软已经开始在自己的平台上提供 BaaS (Blockchain as a Service)服务, 提前布局。

2.2 平台架构中的融合

根据全球移动和流量增长报告来看, 2022 年, 将会有 180 亿台 IoT 连接设备, 这些设备将会产生大量的数据, 而区块链物联网的融合可以解决传统架构中无法解决的问题[11], 因此我们需要提出新的解决方案或架构满足要求, 研究领域的架构分为: 理论研究、原型、产品三个阶段, 区块链物联网的应用分两类: 一类是基于区块链平台进行开发, 另一类是自己开发区块链物联网平台, 我们主要考虑前者, 论文整理了近四年关于平台应用中的 45 篇论文, 本小节对平台架构中的融合技术展开讨论, 包括: 数据管理、网络攻击、提供解决方案、身份验证、隐私、信任机制、访问控制。

2.2.1 数据管理

随着时间的推移, 智能设备会产生大量有用的数据, 但是仍然缺乏可以有效传输和利用物联网数据的平台。

Yu 等[12]引入区块链的分布式网络架构, 智能设备节点映射等技术, 以及 PBFT-DPOC 一致性算法(委托贡献证明), 通过共识算法实现账户的共享, 这种算法需要候选人提供硬件设施(包括计算能力, 带宽和存储), 并参与节点投票, 最终实现智能设备的分散自治。Kumar 等[13]提出了基于三种新兴技术: 雾计算、SDN(软件定义网络)和区块链的分布式云架构, 架构层包括设备层、雾层、云层。云层采用基于区块链的云, 这种架构可以实现实时数据交付, 安全性, 低延迟, 满足以较小的成本管理大型生成的数据流。

区块链的共识机制消耗了大量的计算资源, 分类账的存储也消耗了大量的存储资源, 因此有限的物联网设备不能承受计算资源, 缓存资源, 文献[14]把边缘计算和区块链结合起来, 利用边缘服务器的计算和缓存能力, 帮助物联网设备达成共识, 存储数据。文献[15]提出了一种基于区块链名为 Sapphire 的存储系统, 基于 OSD 的智能合约(OSC)方法, 该方法在 Sapphire 中用作交易协议, 大规模存储系统的并用性可以减少数据分析的时间, 结果表明, Sapphire 大大降低了物联网中数据分析的开销。文献[16]提出管理物联网设备, 构建密钥管理系统的方法: 通过配置区块链保护传感器中的数据采集配置物联网设备, 使用 RSA 公钥密码系统管理密钥, 同时选择以太坊作为区块链平台, 编写图灵完整代码。

以上文献表明, 区块链技术的引入解决了物联网的数据管理问题, 传统物联网架构僵化, 加上物联网数据的持续增长, 导致所有数据流都汇总在中心控制系统内, 而区块链技术的存储系统大大降低了开销, 最终实现设备的分散自治, 在数据管理系统中, 共享数据也是要解决的问题, 数据共享平台应满足三个条件: 平台数据跟平台无关, 安全可靠, 数据共享内容的控制方法灵活可靠, 未来需要进一步的研究来提出解决方案。

2.2.2 系统安全

随着区块链技术的迅速发展, 许多基于区块链的应用迅速出现, 其中区块链, 物联网的结合是最有价值的研究方向之一, 这种结合带来非常多的好处, 但也更容易受到外部攻击, 比如一些恶意节点影响时间同步, 使物联网系统出现严重攻击事故[17]。

文献[18]基于 SDN 和区块链技术提出了一种新的模型: DistBlockNet, 这种架构利用区块链技术更新、下载并验证物联网设备得最新流规则表, 使得网络架构主动适应环境, 并能以低性能开销检测到网络中的攻击, 灵活有效可扩展。文献[19]采用改进的实际拜占庭容错(PBFT)共识机制实现物联网设备的时间同步, 从而减少来自外部的攻击, 使系统高效安全。文献[20-21]指出 IoT 设备的部署导致攻击增加, 采用区块链技术中的智能合约提高了系统的安全性, 区块链机制(BCM)成为物联网防御得一种手段。文献[22]分析了区块链技术中属于新型池挖掘攻击中的硬币跳跃攻击, 深入分析了其实施条件, 提出防御策略: 核查矿工工作检测池管理者的异常行为; 改进公示协议, 跟踪恶意池管理器。文献[23]提出的 Fastpay 技术可以有效解决该问题, Fastpay 协议原理是建立名为 Broker 的用户充当中间人, 实现安全支付。Polkadot, Cosmos 是跨链中项目, 实现万链互联, 文献[24] 设计出一种 Hybrid-IoT(物联网的混合区块链架构), 把 IoT 设备转化为 PoW 子链上的对等体, PoW 子块链之间的连接采用 BFT 互连器, 此架构通过了性能和安全性评估, 文献[25]在系统模型和性能分析的基础上设计了一种算法, 在最大化事务吞吐量的标准下, 确定区块链系统的最优全功能节点部署。最后分析了三种典型攻击的安全性能, 实验结果验证了文中所提的最优节点部署算法的准确性。

物联网设备安全问题包括平台架构安全、通信安全、设备安全, 本小节研究了平台架构安全中存在的安全问题, 区块链技术可以解决以上安全问题, 如区块链的共识机制可用于交易验证并防范恶意攻

击, 篡改, 减少网络攻击, 恶意节点的欺骗, 如在分布式网络中利用封闭的区块链记录和广播时间, 减少了来自外部环境的攻击, 通过对存储开销, 收敛时间等实验数据显示, 基于区块链技术下的IoT数据更加可靠。

2.2.3 计算、存储和网络资源解决方案

在实现区块链技术落地的过程中, 包含了计算、存储、网络的基础设施, 因此这三种资源是物联网急速发展时期需解决的问题。

文献[26]为了解决物联网中计算资源, 存储资源稀缺的问题, 提出了一种基于语义区块链的新型面向服务的体系结构(SOA), 该架构通过智能合约用于注册, 发现, 选择和支付, 实验评估了该提案的可持续性。文献[27-28]为物联网中广域网络的解决方案提出新架构, 该架构通过在各网络层部署区块链技术, 提供了较高的安全性和可信度保证, 还在此基础上提出了优化机制, 通过监控计算负载来分配工作负载, 从而优化计算负荷。文献[29]指出区块链的每个方面都可以根据所需应用的要求进行定制, 文中提供了将区块链与物联网耦合的设计, 确保传感器中采集的数据安全可靠, 为数据存储提供与有效的解决方案。文献[30]从协议出发, 针对轻量级物联网客户端设计了一种区块链系统方案, 仅在更新时下载有用的数据, 该设计降低物联网设备的通信成本。文献[31]指出区块链物联网融合的最大挑战是: 区块链技术中的可扩展性和交易速度, 提出通过使用本地对等网络弥补差距, 实施方法是通过可扩展的分类账限制进入全局区块链的交易数量, 从而提高交易处理的速度。

存储资源指物联网数据保存在哪里, IPFS 这个项目的设计初衷是把闲置的存储空间利用起来, Storj 利用文件分片打散存储数据, 并通过端到端保护数据隐私, 计算能力是数据的处理快慢, DxChain 项目参考了Hadoop架构, 希望同时解决存储和计算问题, 而通信能力是数据、价值状态的连接网络, 通过上述文章分析, 通过智能合约的运用, 基于语义区块链的新型面向服务的体系结构可解决存储和计算资源短缺, 在各网络层部署区块链可以解决网络资源问题, 提升网络性能, 未来的目标是提出新的架构同时解决 IoT 数据的计算、存储、网络资源问题。

2.2.4 身份验证

身份验证管理系统大多出自学术研究, 只有少数初创公司在做身份验证系统的研发, 一般而言, 解决方案分为两类: 依赖于公共区块链平台的身份解决方案, 具有许可身份的块生成器的身份解决方案, 前者主要使用以太坊智能合约来设计数字身份模型, 并确保通过一组操作(即密钥撤销)确保身份的可靠性和可用性, 后者在对等网络中建立了一个公共许可的区块链, 其中节点被划分为经过验证的验证器节点和观察者节点, 以确保高性能和可扩展性。

Bassam[32]引入了基于区块链的 PKI, 提供了基于以太坊智能合约的解决方案。在他的工作中, 定义了几个与身份相关的操作, 例如添加属性、签署属性、撤销签名, 还计算了以太坊平台不同运营的成本。文献[33]提出了带外双因素认证方案, 设备关系存储在区块链上, 即使访问令牌被窃取, 认证方案也可以组织外部恶意设备的访问, 仿真实验表明设备的内存和 CPU 开销在可以接受的前提下, 解决了大规模物联网设备的验证难题。文献[34]提出了物联网系统中身份管理系统的要求: 可扩展性, 互操作性, 移动性, 安全性, 隐私性, 并研究了区块链主权身份解决方案, 最后阐述了物联网构建完整身份管理系统的挑战。文献[35-36]通过约束公众, 开发了基于以太坊智能合约的身份管理系统密钥, 用户的实体信息。除身份管理部分外, 他们还重新定义了令牌, 以符合他们提出的声誉模型, 反映用户的声誉。奥古特等人[37]修改了比特币堆栈以构建身份管理解决方案, 并把零知识证明称为品牌选择性披露方案, 以确保匿名身份。文献[38]设计了 NEXTLEAP, 这是一个非中心化的身份框架, 具有使用盲签名的隐私保护功能, 此外, 他们使用身份解决方案提供的身份验证服务构建更安全的消息传递应用程序 Azouvi 等。

物联网具有可扩展性, 移动性强, 互联网领域中的身份管理系统无法直接应用在物联网环境中, 区块链技术的去中心化做到不依赖第三方的情况下, 允许用户设备管理自己的身份, 通过对学术研究中的身份管理系统充分调研, 区块链技术的引入为身份管理提供了可行的解决方案。

2.2.5 隐私保护

隐私保护是指用户的敏感信息, 包括身份信息, 来自服务商提供的敏感数据, 我们可以通过更改权限保护自己的隐私数据, 然而由于第三方的存在, 不可避免的泄露自己的身份信息, Blockchain 是比特币加密货币系统背后的技术, 因此被用于确保物联网(IoT)生态系统中增强安全性和隐私性。

文献[39-40]采用 PoW 共识机制, PK(公钥)来记录用户身份, 私钥用来加密, 提供了一个使用区块链来保护物联网安全的模型。Axon[41]分析了隐私设计分散式 PKI 系统时提出的要求, 提出了一种具有

隐私意识的基于区块链的 PKI, 除了注册, 撤销和恢复等一系列操作外, 他们还引入了邻居组的概念, 以提高隐私保护的性能。Hardjono [42]在许可的区块链环境中使用零知识证明引入了一种基于区块链的隐私保护身份解决方案, 称为 ChainAnchor。在本方案中, 经过验证的节点具有编写或处理事务的权限, 且都建立在防篡改硬件上, 为用户提供隐私保护服务。文献[43-44] 引入区块链技术中的智能合约, 能够将复杂的多步骤流程自动化, 实现加密可验证性。文献[45-50]将其与监管框架规定联系起来, 提供了区块链的隐私和数据保护方面的解决方案, 随着区块链产品的开发, 还需要考虑遵守数据隐私监管框架。

区块链技术使身份控制权从第三方提供商返给用户, 零知识证明的加密方案可以在不泄露隐私的情况下确认身份, 通过链下存储构建平台可以保护个人数据的隐私, 智能合约的执行可实现加密壳验证性, 合同违约时, 被欺骗的当事人可获得相应的赔偿, 需要指出的是, 智能合约应用在物联网中仍需学术界的进一步研究和工业界的实践验证。

2.2.6 信任机制

信任机制非常重要, 与隐私和身份验证紧密相关。区块链是一种新兴的范例, 提供以无信任, 可审计的方式与其他网络设备交互, 解决物联网(IoT)平台的信任问题。

现有的信任机制研究大部分脱离物联网环境, 文献[51]提出一种适用于分布式物联网的信任管理方法, 借助区块链实现信任数据的共享, 该方案经实验表明, 能够有效量化信任, 保护数据不被篡改。文献[52]在 IETF 草案(“约束节点的区块链事务协议”)中引入了 BIoT 范例, 主要思想是在区块链事务中插入传感器数据, 由于对象没有逻辑连接到区块链平台, 因此控制器实体会转发事务伪造所需的所有信息。为了生成加密签名, 对象需要一些可信的计算资源, Liu 等人在文献[53]提出了一种通过量身定制的以太坊令牌建立信任声誉的方法。Zhu 在文献[54]将所有物联网实体之间的区块链和社交网络结合起来, 为物联网构建了一个安全架构, 也为信任管理奠定了坚实的基础。文献[55] 提出了一个信任列表, 信任列表的原则是自动化怀疑, 验证和信任物联网服务和设备的过程, 以有效地防止攻击和滥用, 并通过集成区块链和软件定义网络(SDN)在边缘网络上提供物联网交通管理的自动执行。文献[56]提出了一种基于区块链的社会物联网可信服务管理框架。该框架通过区块链的去中心化特性在服务请求者和服务提供者之间直接建立信任关系, 利用智能合约产生并管理新的交易, 实现交易过程透明化并减少管理维护成本。

对信任机制研究有以下两种: 基于策略制定的机制和基于信誉的机制, 上述文献在两种机制的研究基础上引入区块链技术, 使研究成果应用到分布式物联网中, 随着 IoT 设备的智能化程度提高, 引入风险概念后的信任机制需要进一步的研究。

2.2.7 访问控制

访问控制作为一种安全机制, 规定了是否可以访问计算机系统中的哪种资源和服务, 传统的访问控制包括访问控制列表、给予角色的访问控制、给予属性的访问控制、给予能力的访问控制, 传统的机制很难满足物联网现在的发展, 区块链技术的引入使得访问控制策略变得透明[57]。

文献[58]提出了 FOCUS 架构, 他们利用三维社交网络构建以用户为中心的访问控制机制, 可以管理所有类型的访问控制, 整个访问控制机制建立在无信任物联网环境中基于区块链的身份管理系统上, 保证了用户的安全性和隐私性。文献[59]提出了 IoTChain 架构, 它是 OSCAR 架构和 ACE 授权框架的组合, 为安全授权访问物联网资源提供端到端解决方案, OSCAR 使用公共分类帐为授权客户端设置多播组。文献[58]提出了一种动态访问控制方案, 以解决现有的设备间直接数据通信访问控制方法的问题, 并应对物联网的动态环境。文献[61-63]提出了 FairAccess 框架, 这个框架的优势是使用智能合约创建去中心化的假名和隐私保护授权管理框架, 其中智能合约用来表示访问控制策略, 既保留了区块链带来的优势, 同时克服了区块链在访问控制策略上的挑战。文献[64]为 IoT 设备描述了一种新颖的防伪方法, 利用存储芯片的独特特性来获取加密, 结合区块链进行可靠和可靠的设备身份验证。

上述文献均提出了一种新的体系结构, 架构是基于区块链技术的物联网全分布式访问控制系统, 包括: 1)无线传感器网络; 2)管理节点; 3)代理节点; 4)智能合约; 5)区块链网络; 6)管理中心。该体系结构由概念验证实现支持, 并在实际的物联网场景中进行评估, 结果表明区块链技术可以用作特定可扩展物联网场景中的访问管理技术。

2.3 应用场景中的融合

本小节对 35 篇各领域的融合文章进行分析, 融合分类见表 2, 我们选择了应用广泛的三个应用领域: 工业物联网, 车联网, 智慧城市进行了详细论述, 并对应用领域中出现的亮点进行归纳总结。

表 2 区块链物联网应用领域的研究亮点

Table 2 Research Highlights in the Applications Domains

Application Scenarios	Highlights
工业界: Industrial Sector (14 papers)	1. Energy blockchain; 2. Software-defined industrial IoT; 3. Proposed a consensus mechanism called Synergistic Multiple Proof and a lightweight data structure called LightBlock;
智慧交通: Intelligent Vehicles (6 papers)	1. Security and Privacy issues in the vehicle IoT environment; 2. Bayesian inference model to verify received messages from neighboring vehicles; 3. Blockchain technology used in car clouds
智慧城市: Intelligent Cities (5 papers)	1. Providing a secure communication platform for smart cities; 2. Sharing economy
智能家居: Smart Home (4 papers)	1. Optimize the smart home environment; 2. Every smart home is equipped with miners
供应链: Supply Chain (3 papers)	1. Create a transparent food supply chain; 2. Use an object-based attestation authentication protocol
医疗健康: Medical Health (3 papers)	1. Provide and store reliable health records; 2. Use the Inter Planet file system to store records of discharged patients

2.3.1 工业 4.0

随着通信技术和智能制造的发展, 工业物联网应运而生, 如制造自动化, 远程机器诊断, 工业机器的预测健康管理, 区块链和工业物联网(IIoT)的交叉点最近引起了相当大的研究兴趣[65-66]。

文献[67]采用的方法是基于区块链技术以防篡改的方式存储从物联网智能计量设备收集的能量消耗信息, 同时自动执行智能合约以编程方式定义每个消费者级别的预期能量灵活性, 相关奖励或罚款, 以及平衡能源需求与电网能源生产的规则。文献[68]首先提出了软件定义的工业物联网和基于区块链的共识协议和详细的共识步骤, 区块链作为可信第三方收集和同步不同 SDN 控制器之间的网络范围视图。文献[69] 提出了一个名为 Synergistic Multiple Proof(SMP)的绿色共识机制(用于激发 IIoT 设备的协作)和一个称为 LightBlock(LB)的轻量级数据结构, 以简化广播内容。此外, 还设计了一种无关块过滤器(UBOF), 以避免分类账的无限增长而不影响区块链的可追溯性。文献[70]为了协助工业物联网(IIoT)网络计算任务, 将云计算服务引入区块链平台, 此外还研究了云提供商和矿工之间的资源管理和定价问题。

文献[71]首先引入提出能源链的概念, 提出的方法使节点能够通过本地存储的能量满足其电力负荷, 如果有相当多的剩余电力, 可作为卖方参与, 若无则可以在更安全的环境中减轻操作开销, 这种方法可以在信贷效用和运营开销之间实现良好的权衡。文献[72]利用联盟区块链技术提出了一种名为能源区块链的安全能源交易系统, 同时提出了使用 Stackelberg 博弈进行信贷贷款的最优定价策略, 基于真实数据集的结果表明, 所提出的能源区块链和基于信用的支付方案在 IIoT 中是安全有效。

文献[73]为智能电网网络提出了一个模型: Permissioned Blockchain Edge Model(PBEM-SGN), 该模型通过组合区块链和边缘计算技术来解决智能电网中隐私保护和能源安全中的两个重大问题。文献[74]解决了在不依赖可信第三方的情况下为分散式智能电网能源提供交易安全性的问题, 通过采用区块链技术, 多重签名和匿名加密消息流实现分散式能源交易系统的概念验证, 使同行能够匿名协商能源价格并安全地执行交易。

文献[75]提出了一种隐私保护和高效的数据聚合方案。该方案将用户划分为不同的组, 每个组都有一个私有区块链来记录其成员数据。为了保护组内的内部隐私, 使用假名来隐藏用户的身份, 同时采用 bloom 过滤器进行快速认证。

区块链技术在工业物联网中的应用主要体现在能源交易中, 例如: 微电网(带太阳能电池板的发电机); 能量收集网(移动充电桩); 车辆到电网网络, 通过使用区块链技术, IIoT 平台中的网络对等体无需可信中介能够彼此交互, 实现 P2P 能量交易。

2.3.2 车联网

智能汽车正在经历工业的革命性增长, 但它仍然存在许多安全漏洞, 随着汽车工业和物联网(IoT)的快速发展, 车载网络的安全性日益受到重视。

文献[76]研究了支持 SDN 的 5G-VANET 中的交通系统和车载物联网环境中的安全和隐私问题。文献[77]提出了一种用于分布式 VFS 的区块链辅助轻量级匿名认证(BLA)机制, BLA 通过有效地结合现代密码技术和区块链技术实现了这些优势。文献[78]提出了一种基于区块链技术的车载网络中的分散式信任管理系统。在该系统中, 车辆可以使用贝叶斯推

理模型验证来自相邻车辆的接收消息。文献[79]首先研究了区块链技术如何扩展到车辆网络的应用, 提出了车辆中的数据向外传输的模型, 然后给出了详细的理论分析和数值结果, 为区块链在车辆网络中的应用提供指导。文献[80]提出使用区块链技术在智能交通之间进行通信的 Trust Bit(TB), 在车载云中使用了区块链技术可以存储所有 Trust 位详细信息, 并且可以随时随地通过智能交通访问。针对车载网络的数据认证和完整性, 文献[81]提出了一种基于区块链技术的数据可信度评估信誉系统。在该系统中, 车辆基于对交通环境的观察对接收的消息进行评级, 并将这些评级打包成“块”。

上述文献中的仿真结果表明, 区块链技术在车载网络中收集, 验证和存储车载信息是可靠的, 因此, 车载网络中存在的安全问题可以使用区块链技术得到解决。

2.3.3 智慧城市

人口激增, 气候变化和资源稀缺给城市带来了危机, 基于区块链技术的物联网安全框架应运而生, 区块链技术的引入给共享经济带来好处, 为市民带来更好的生活, 万物互联是智慧城市的重要组成部分。

文献[82]提出了一种安全框架, 将区块链技术与智能设备集成在一起, 为智能城市提供安全的通信平台, 并指出未来方向是创建一个通用平台或设计一个系统级别模型, 以研究智能城市中使用不同平台的互操作性和可扩展性。拼车使乘客能够共享车辆, 以减少行驶时间, 车辆碳排放和交通拥堵。文章[83]提出了一种有效且隐私保护的拼车方案, 该方案使用区块链辅助车辆雾计算来支持条件隐私, 一对多匹配, 目的地匹配和数据可审计性, 此外, 采用私密接近测试来实现一对多的邻近匹配并将其扩展为在乘客和驾驶员之间有效地建立秘密通信密钥。

2.3.4 其他

除了上述三种场景应用外, 物链网也可以应用到智能家居、供应链、健康医疗等场景中。

文献[84]概述了各种核心组件智能家居层, 提出了一个关于其安全性和隐私的全面分析, 仿真结果表明, 采用的方法开销低, 可以管理低资源 IoT 设备。

Mondal [85-87]提出了用于创建透明的食品供应链的物链网架构, 架构使用基于对象的证明身份验证协议, RFID 提供产品和传感器数据的独特标识, 有助于实时质量监控, 通过在物理层集成基于 RFID 的传感器和在网络层集成区块链来实现完整的架构, 有助于在每个实例中创建用于食品包装的防篡改数据库。

研究表明, 提供医疗保健的延迟与患者信心和康复机会直接相关, 不可靠的健康记录存储只会加剧这个问题, 文献[88-90]将生物传感器测量并收集关于患者医疗状态的实时数据并存储在区块链中, 产生数据的快速报告和防篡改存储。通过部署智能合约, 计算最终的医院账单以及保险范围, 同时还提出使用 Inter 行星文件系统来存储出院病人的记录, 减少实际区块链的负担。总体而言, 通过创建安全透明的环境以及快速响应患者的需求, 使患者和医生均受益。

通过对区块链物联网的以上应用场景分析, 无论是在工业物联网, 还是车载网和智慧城市领域, 我们看到垂直行业的生态格局已初步具有雏形, 行业应用也处于爆发阶段, 但大多数应用案例都处于概念验证阶段, 区块链技术中的处理能力, 扩展性差, 能耗高, 网络割裂等问题尚需要解决, 物链网作为一种新兴技术, 无论是初创公司, 还是物联网行业巨头公司都需要时间解决上述瓶颈问题。

3 物链网应用: 典型公链, 商业项目

互联网改变了人与人的关系, 使信息交流更为通畅, 物联网改变了物与物的交互, 新兴的区块链技术给物联网带来革命性的影响, 两者融合后, 社会加速迈进智能化的步伐, 智能化赋予每个物体一个 IP, 每个设备像有了新的生命, 能够实现自我管理和自我修复的功能。

全球区块链创业公司, 物联网巨头公司纷纷在“区块链+物联网”领域布局, 截至目前为止, 全球有 66 个公链项目, 而亚马逊、Microsoft、PREDIX、SAP、阿里巴巴等巨头公司也开始进军该领域, 为未来物联网设备的大量接入提供资源池做超前布局。

区块链分为三类: 公链、私链、联盟链, 公有链是指全世界任何人都可以随时进入到系统中读取数据、发送可确认交易、竞争记账的区块链。私链非公开, 需要授权才能加入节点, 联盟链是由若干机构或组织共同发起并参与维护的链, 应用代表: 超级账本(Hyperledger), 本节我们重点介绍公链。

3.1 典型公链

3.1.1 艾欧塔—IOTA

本项目在 2014 年发起, 为物联网应用场景打造分布式账本, 专注于物联网的支付和通信, 设计目标是轻量化, 解决了物联网的扩展性问题, 提出了 DAG(有向无环图)即 Tangle 方案的数据结构, 使机

器能够安全地交换数据和通证, 解决了小额, 高频次, 低延时的交易, 为物联设备赋予价值, 开创了全新的价值网络, 推进物了联网生态系统共享数据经济, 为移动、能源、工业 4.0 等新应用和商业模式开创了新的道路, IOTA 有几个优点: 一是零交易费用, 二是确认速度快, 三是网络越大越安全, 因此网络越大, 确认速度越快, 网络越安全。因此, IOTA 项目切中了现在的两大热门技术(物联网技术与区块链技术), 合理的利用去中心化的方式解决物联网实际需求。

Tangle 技术是指验证新的交易时, 只需验证此前的两个交易即可, 在这两个交易前被验证过的交易也得到间接验证。并在 2018 年 6 月上线 Qubic, Qubic 引入了预言机(Oracles)、智能合约(Smart Contracts)和外包计算(outsourced computations)三大功能, 预言机将链外数据引入到链内, 打通区块链世界与物联网世界的桥梁, 智能合约实现设备之间的自动化和智能化, 带来更多的应用场景, 外包计算将密集计算外包给算力强大的第三方, 使一般设备也能通过 IOTA 与其他设备交互, IOTA 致力于成为物联网领域的基础设施, Qubic 将成为 IOTA 物联网基石[91]。

但是 DAG 也存在一些问题: WOT 的签名方案会暴露用户的私钥, 降低安全性; IOTA 协调员(Coordinator)是中心化的, 团队并未给出今后的发展路线; 无交易费用会带来拒绝服务攻击, 网络多次受到攻击导致无法使用; IOTA 技术中的散列算法存在漏洞, 开发团队违背加密技术法则, 自己构建算法; 允许开源软件存在漏洞违背了开源软件精神, IOTA 仍处在初级阶段, 离一个成熟的生态系统还有一定的距离, 我们期待这一领域的进一步研究。

3.1.2 沃尔顿链—WTC

项目起始于 2017 年, 沃尔顿链将区块链技术引入物联网, 利用区块链去中心化、不可篡改等特点, 结合 RFID 系统, 采用双链架构设计, 提出了最新的跨链连接和确认机制, 有效解决子链与母链之间的数据交换和价值交换的问题, 共识机制主要由 PoW、PoS 及 PoL(Proof of Labor)三个部分组成。其中前两者主要针对母链, 解决数据验证、数据存储等问题, PoL 主要用于母链与子链以及各子链之间的数据传输等证明, 从而实现物联网数据和服务的共识、共享、共治、共联。

其架构分为六层: 设备层、基础层、核心层、扩展层、服务层和应用层, 设备层通过研发基于哈希签名的数据自验证 RFID 芯片设计方法, 实现了区块链硬件系统, 保证源头可靠; 核心层和扩展层被称为沃尔顿母链, 采用软硬融合, 数据定制合约模式和跨链技术实现数据的融合流通, 验证和存储, 应用广泛, 其生态系统框架已经使用于多个商业场景中, 如食品溯源、服装溯源、物流追踪和食品药品溯源[92]。

此外, 第一个支持物联网全栈开发端到端分布式应用的链 Ruff 项目采用 DPoS 算法, 让现实世界的智能合约成为可能, 如产权转让和租赁, 资产管理和证券化, 供应链融资等, Exergy 利用区块链技术中的智能合约构建能源服务令牌系统, 实现更具参与性的能源范例。IoTeX 是物联网(IoT)的自动可扩展和以隐私为中心的区块链基础设施, 致力于以经济高效的方式最大限度地提高可扩展性, 安全性和隐私性, 构建支持物联网应用的下一代区块链平台[93-94]。

3.2 商业项目

科学界和工业领域都投入了研究, 国家能源 2015 年成立区块链能源实验室, 阿里巴巴与普华永道开展战略合作, 共同打造透明可追溯的跨境食品供应链, IBM、华为、亚马逊和 SAP 都在各自的物联网云平台上提供区块链技术的相关服务。例如, IBM 正在推进近 500 个区块链商业化项目, 其中 30 多个商用区块链已经运行[95]。

IBM 最早宣布对区块链的开发计划公司之一, 已在多个不同层面与很多公司建立了合作关系, 计划组建区块链与物联网研究团队, 2016 年 10 月推出 Bluemix 云平台上的区块链服务(BaaS)。IBM 曾在一篇研究报告中指出, 在物联网中, 最大的挑战不是去中心化, 而是建立一个能保证隐私安全和无信任的、可以不断扩展的通用物联网, 而区块链技术可以提供优秀的解决方案。IBM 还与三星专为下一代的物联网系统建立了一个概念证明型系统, 该系统基于 IBM 的 ADEPT(自治分散对等网络遥测), ADEPT 平台由三个要素组成: 以太坊、Telehash 和 BitTorrent。IBM 希望使用该平台, 带来一个能自动检测问题, 自动更新, 不需要任何人为操作设备, 这些设备也将能够与其他附近的设备通信, 以便于为电池供电和节约能量。

4 挑战和展望

目前, 区块链技术处于待成熟, 未定型阶段, 跨链整合、分区、共识机制等技术需要增强, 行业标准需要建立, 因此将区块链技术应用到物联网领域存在以下挑战。

1) 数据存储

SPV 是“Simplified Payment Verification”(简单支

付验证)的缩写。中本聪曾在论文中简要地提及了这一概念: 不运行完全节点也可验证支付, 用户只需要保存所有的区块的头部信息即可, SPV 极大地节省存储空间, 减轻了终端用户的负担, 即使用户使用的是最低端的设备, 正常情况下也完全能够负载, 因此 SPV 技术仅需少量资源, 可以部署在物联网设备上[96-97]。

区块头中有三个关键字段, 一是 prev block hash (前一区块的 hash 值, 确保了区块链所记录的交易次序); 二是 bits(当前区块的计算难度), 三是 merkle root hash(借助 merkle tree 算法, 确保收录与区块中所有交易的真实性), 为了简化模型, 我们假设用 tx_hash 来定位区块。SPV 尚存的问题是如何才能通过 tx_hash 定位到该交易所在的区块, 以往的比特币协议中缺少对此相应的支持。Bloom 过滤器解决了客户端检索的问题, 方法是: 它可以快速判断出某检索值一定不存在于某个指定的集合, 从而过滤掉大量的无关数据, 减少客户端不必要的下载量。这样的节点可以为去中心化方式 SPV 查询提供必要的支持, 从而从安全性上得到一定的保证, 同时由于数据的不可篡改, 可编辑的区块链需要保证编辑过程的安全条件和记录, 在满足条件时删除或修改某些区块链, 目前, 可编辑的区块链已经被设计成密码算法, 如哈希函数的变体[98-99]。

2) IoT 的移动性和分区容忍

区块链作为一个记账或者账本系统, 这其中存在一个很大的问题, 即关于吞吐量的问题, 比特币的底层设计仅支持每秒 7 笔交易, 还不及传统支付工具 Visa 每秒 8000 笔交易的一个零头, 严重制约了去中心化应用的发展, 如果用户想进行一笔简单的转帐, 必须支付更高的手续费才能完成这笔交易。因此, 低吞吐量导致了目前还没有相关领域的杀手级应用, 链下存储技术可以解决这个问题, 即对应比特币的闪电网络(Lightning Network)和以太坊的 Raiden Network, 用户提前支付一些以太坊或比特币作为押金, 之后便可以在链下通过一些手段, 来跟其他人进行交易。交易结束后, 用户要把这个结算放在区块链上面。因为在链下处理交易时, 可以使用性能极为强大的服务器, 大幅度提升系统的吞吐量, 达到每秒上万, 甚至是几十万的交易量。

物联网中, 移动设备产生的数据需要迁移, 借助侧链技术和令牌可以以分散的方式在不同的区块链之间转移。资产转移过程与货币类似交换[100], 链下存储虽然能够达到高的吞吐量, 交易却失去了开放性、透明性的优势, 使用链下交易, 没有那么多节点去进行行为监督, 也就少了去中心化的优势, 同时, 普通的物联网节点失效, 退网是常见现象, 针对可能存在的网络割裂, 可以选择支持链上链下交易, 并在系统设计时支持多个集群。

3) 高延迟

针对如何增大区块链的吞吐量这一问题, 业界也一直在不断努力尝试。有两个测量指标与区块链扩展性直接相关: 交易吞吐量(区块链可以处理交易的最大速率), 延迟(确认交易已包含在区块链中的时间)。吞吐量和延迟是提升区块链性能的瓶颈, 区块链技术中最大的挑战是: 交易速度慢, 主要原因是每个节点(又叫矿工)处理网络上的每笔交易, 下载慢, 验证慢, 随着节点越来越多的加入, 交易量越来越大, 以太坊的网络速度会越来越慢。“分片”来源于传统的数据库概念, 将完整的数据库进行分片管理, 每个分片保留相同的数据库结构。在以太坊中, 借用数据库中分片的思想, 现将网络中的每个区块拆分成一个个子区块, 每个子区块可以容纳若干个(目前是 100 个)存有交易数据的校验块(Collation), 这些校验块最终组成一个在主链上的区块, 由于分片中的节点只需要负责所在片区 处理, 不需要广播到整个网络, 因此提升了处理交易。

表 3 物链网研究面临的挑战与机遇

Table 3 Chanllenges and Opportunites of BoT Research

挑战	机遇
区块链的高延迟	Sharding, GHOST 协议, 链式结构改变
IoT 的移动性和分区容忍	侧链
数据存储	SPV, 可编程区块链
数据传输能力	5G 移动通信技术
高能耗	共识算法改进
隐私安全	硬件和协议加密
数据可靠性缺乏监管	立法
安全标准缺失	编程接口和跨链协议需要统一

在物联网环境下我们可开发出分片区块链的机会[101-103], 管理操作都在不同的分片上并存储在不同的服务器中完成, 从而将大问题拆分成小问题解决, 不同的链按重要程度记录数据, 保证全局和本地所有记录的完整性, 我们还可以使用 GHOST(Greedy Heaviest-Observed Sub-Tree)协议。GHOST 可以加快生成块的速度, 从比特币中的每块 10 分钟到以太坊中的每块 12 秒, 也可以基于软件区块链平台做改进, 例如, IOTA 提出不使用链式结构, 采用 DAG 的数据结构, 再加上随着封装工艺等新架构的不断成熟, 小体积低功率的传感器节点越来越受欢迎, 从而提升了交易性能。

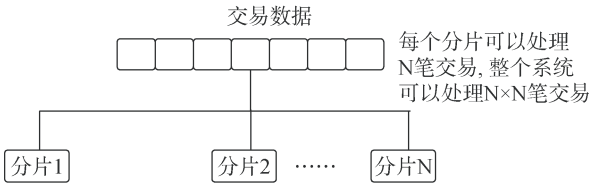

图 5　分片技术

Figure 5　The Technology of Sharding

4) 高能耗

区块链中数据全网广播、全网存储和全网校验需要消耗很大的网络带宽资源, 存储资源和算力资源, 对于资源消耗大的共识机制, 我们可以改变共识算法, 使用资源消耗低的算法[104-105], 如 PBFT 和 Tendermint 算法等, 在物联网领域, 随着低功耗广域网(LPWAN)技术的发展, 传输质量、传输距离、功耗、蓄电量的问题有望逐步得以解决。

此外, 数据传输能力差, 延迟性高依赖 5G 技术的崛起, 2019 年 6 月份, 工信部发布了 4 张 5G 商用牌照: 中国电信、中国移动、中国联通、中国广电, 5G 网络加速推进了物联网的发展; 隐私安全也需要进一步加强, 我们可以通过硬件或协议加密的方式解决[107-108]; 物联网厂商构建自己的信息平台造成信息不兼容以及数据可靠性缺乏监管都是需要面临的挑战。本文研究区块链与物联网融合的技术, 区块链的技术特点决定了这项技术会在产生大量数据和共享数据的领域使用, 因此未来研究应侧重于数据存储, 数据管理方向[109], 怎么灵活控制使用和共享他人数据, 怎么快速处理数据, 怎么利用缓存或优化减少延迟等, 怎么使用 SPV 技术、可编程区块链存储数据, 以上研究成果会对物联网发展产生很大的影响。

5　结束语

区块链技术的发展使物联网领域产生了重大的改变, 二者的融合带来了新的机遇, 同时也带来了很多挑战。本文首先介绍了物联网的当前发展现状和存在的问题, 然后介绍了区块链技术的发展历程并分析其优缺点和面临的重要挑战, 通过对区块链与物联网融合的论文和白皮书进行广泛调研, 我们认为物链网应用有很大的发展前景, 但目前还处于探索阶段, 高延迟、高能耗、分区容忍和隐私[110]等问题需要通过进一步研究来解决。值得注意的是, 5G 技术的崛起将会改进区块链网络的性能, 增加网络带宽, 降低延迟性, 对物联网和区块链提供更好的支持, 这对未来物联网生态体系的构建至关重要。

参考文献

[1] “IoT Security WhitePaper,” IoT, http://www.cbdio.com/BigData/2018-09/25/content_5847152.htm, Sept. 2018.

[2] F. Al-Doghman, Z. Chaczko, and J. Jiang, “A Review of Aggregation Algorithms for the Internet of Things,” in 2017 25th International Conference on Systems Engineering (ICSEng), Las Vegas, NV, pp. 480–487, 2017.

[3] Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System.”, https://nakamotoinstitute.org/, 2008.

[4] S. Manglekar and H. A. Dinesha, “Block Chain: An Innovative Research Area,” in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, pp. 1–4, 2018.

[5] “Blockchain Security WhitePaper,” Blockchain, http://www.sohu.com/a/314558225_405262 ,Sept.2018.

[6] “2018 Internet of Things and Blockchain Application Summit,” http://www.whatsmeeting.com/news/view7465.html, 2018.

[7] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, “Security Services Using Blockchains: A State of the Art Survey”, *IEEE Communications Surveys & Tutorials*, vol.21, no.1, pp.858-880, 2019.

[8] K. Xu, B. Wu, and M. Shen, “Blockchain: A New Vision for IoT Security,” *ZTE Corporation*, vol.24, no.6, pp.52-55, 2018.
(徐恪, 吴波, 沈蒙, “区块链: 描绘物联网安全新愿景,” *中兴通讯技术*, 24(6):52-55, 2018。)

[9] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, “Algorand: Scaling Byzantine Agreements for Cryptocurrencies,” in Proceedings of the 26th Symposium on Operating Systems Principles - SOSP ’17, Shanghai, China, pp. 51–68, 2017.

[10] Beck, “Into the Ether with Ethereum Classic”, https://www.ethereum.org/, 2017

[11] 吴迪, 崔翔, 刘奇旭, 张方娇. 泛在僵尸网络发展研究[J]. *信息网络安全*, 2018(07):16-28.

[12] S. Yu, L. Kun, S. Zhou, Y. Guo, J. Zhou and B. Zhang, “A High Performance Blockchain Platform for Intelligent Devices,” In Proc. *IEEE International Conference on Hot Information-Centric Networking* (HotICN’18), pp.260-261, 2018.

[13] P. Kumar, M. Chen and J. Park, “A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT,” *IEEE Access*, vol.6, pp.115-124, 2018.

[14] F. Xu, F. Yang, C. Zhao and C. Fang. “Edge Computing and Caching Based Blockchain IoT Network,” In Proc. *IEEE International Conference on Hot Information-Centric Networking* (HotICN’18), pp.238-239, 2018.

[15] Q. Xu, K. Aung, Y. Zhu and K. Yong, “A Blockchain-Based Storage System for Data Analytics in the Internet of Things,” *New Ad-*

vances in the Internet of Things, vol.715, pp.119-138, 2018.

[16] S. Huh, S. Cho and S. Kim, "Managing IoT Devices Using Blockchain Platform," In Proc. *International Conference on Advanced Communication Technology* (ICACT'17), pp.464–67, 2017.

[17] 周振飞, 方滨兴, 崔翔, 刘奇旭. 基于相似性分析的 WordPress 主题恶意代码检测[J]. 信息网络安全, 2017(12): 47-53.

[18] P. K. Sharma, S. Singh, Y. Jeong and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," *IEEE Communications Magazine*, vol.55, no.9, pp.78-85, 2017.

[19] F. Kai, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li and Y. Yang, "Blockchain-Based Secure Time Protection Scheme in IoT," *IEEE Internet of Things Journal*, pp.1-1, 2018.

[20] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," Internet of Things, vol. 1–2, pp. 1–13, Sep. 2018.

[21] F. Dinan, K. Mutijarsa, "Secure IoT Communication Using Blockchain Technology," In Proc. *International Symposium on Electronics and Smart Devices* (ISESD'18), pp.1-6, 2018.

[22] S. Zhu, W. Li, H. Li, L. Tian, G. Luo and Z. Cai, "Coin Hopping Attack in Blockchain-Based IoT," *IEEE Internet of Things Journal*, pp.1–1, 2018.

[23] Z. Hao, R. Ji and Q Li, "FastPay: A Secure Fast Payment Method for Edge-IoT Platforms Using Blockchain," In Proc. *IEEE/ACM Symposium on Edge Computing* (SEC'18), pp.410–415, 2018.

[24] G. Sagirlar, B. Carminati, E. Ferrari, J. Sheehan and E. Ragnoli, "Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-Blockchains," ArXiv:1804.03903 [Cs], 2018.

[25] S. Yao, L. Zhang, G. Feng, B. Yang, B. Cao and M. Ali Imran, "Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment," *IEEE Internet of Things Journal*, pp.1-1, 2019.

[26] M. Ruta, F. Scioscia, S. Ieva, G. Capurso and E. Sciascio. "Semantic Blockchain to Improve Scalability in the Internet of Things," *Open Journal of Internet of Things*, vol.3, no.1, pp.46-61, 2017.

[27] L. Cheng, L. Zhang, "A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things," In Proc. IEEE International Congress on Internet of Things (ICIOT'17), pp.33–41, 2017.

[28] R. Chakraborty, M. Pandey and S. Rautaray, "Managing Computation Load on a Blockchain – Based Multi – Layered Internet – of – Things Network," *Procedia Computer Science*, vol.132, pp.469–476, 2018.

[29] J. Song, M. Demir, J. Prevost and P. Rad, "Blockchain Design for Trusted Decentralized IoT Networks," In Proc. *Annual Conference on System of Systems Engineering* (SoSE'18), pp.169–174, 2018.

[30] D. Pietro, A. Kalor, C. Stefanovic and P. Popovski, "Delay and Communication Tradeoffs for Blockchain Systems With Light-weight IoT Clients," *IEEE Internet of Things Journal*, vol.6, no.9, pp.2354-2365, 2019.

[31] S. Biswas, K. Sharif, F. Li, B. Nour and Y. Wang, "A Scalable Blockchain Framework for Secure Transactions in IoT," *IEEE Internet of Things Journal*, pp.1-1, 2018.

[32] A. Mustafa, "SCPKI: A Smart Contract-based PKI and Identity System," In Proc. *ACM Workshop on Blockchain, Cryptocurrencies and Contracts* (BCC'17), pp.35-40, 2017.

[33] L. Wu, X. Du, W. Wang and B. Lin, "An Out-of-Band Authentication Scheme for Internet of Things Using Blockchain Technology," In Proc. *International Conference on Computing, Networking and Communications* (ICNC' 18), pp.769–773, 2018.

[34] X. Zhu and Y. Badr, "Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions," Sensors, vol.18, no.12, pp.4215-4215, 2018.

[35] K. Prabhu, and K. Prabhu, "CONVERGING BLOCKCHAIN TECHNOLOGY WITH THE INTERNET OF THINGS," *Information Technology*, vol.3, no.2, 2017.

[36] M. Miraz and A. Maaruf, "Blockchain Enabled Enhanced IoT Ecosystem Security," In Proc. *International Conference on International Conference on Emerging Technologies in Computing* (ICETIC'18), 2018.

[37] D. Augot, H. Chabanne, O. Clémot, and W. George, "Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain," arXiv:1710.02951 [cs, math], Oct. 2017.

[38] H. Halpin, "NEXTLEAP: Decentralizing Identity with Privacy for Secure Messaging," In Proc. *International Conference on Availability, Reliability and Security* (ARES'17), 2017.

[39] M. Miraz and A. Maaruf, "Blockchain Enabled Enhanced IoT Ecosystem Security," In Proc. *International Conference for Emerging Technologies in Computing* (ICETIC'18), pp.38-46, 2018.

[40] M. Singh, A. Singh and S. Kim, "Blockchain: A Game Changer for Securing IoT Data," In Proc. *IEEE 4th World Forum on Internet of Things* (WF-IoT'18), pp.51–55, 2018.

[41] Axon, L, "Privacy-Awareness in Blockchain-Based PKI," Oxford University Research Archive: Oxford, UK, 2015.

[42] T. Hardjono, A. Pentland, "Verifiable Anonymous Identities and Access Control in Permissioned Blockchains," pp. 9, 2016.

[43] K. Christidis and M Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol.4, pp.2292–2303, 2016.

[44] N. Kshetr, "Can Blockchain Strengthen the Internet of Things," *IT Professional*, vol.19, no.4, pp.68-72, 2017.

[45] L. Zhou, L. Wang, Y. Sun and P. Lv, "BeeKeeper: A Blockchain-Based IoT System With Secure Storage and Homomorphic Computation," *IEEE Access*, vol.6, pp.43472-43488, 2018.

[46] N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, “Secured by Blockchain: Safeguarding Internet of Things Devices,” *IEEE Consumer Electronics Magazine*, vol.8, no.3, pp.28-34, 2019.

[47] M. Conoscenti, A. Vetro and J. Martin, “Peer to Peer for Privacy and Decentralization in the Internet of Things,” In Proc. *IEEE/ACM 39th International Conference on Software Engineering Companion* (ICSE-C’17), pp.288-290, 2017.

[48] N. Fabiano, “The Internet of Things Ecosystem: The Blockchain and Privacy Issues. The Challenge for a Global Privacy Standard,” In Proc. *International Conference on Internet of Things for the Global Community* (IoTGC’17), pp.1–7, 2017.

[49] H. Shafagh, A. Hithnawi, L. Burkhalter, P. Fischli, and S. Duqennoy, “Secure Sharing of Partially Homomorphic Encrypted IoT Data,” In Proc. *ACM Conference on Embedded Networked Sensor Systems* (SenSys’17), 2017.

[50] H. Shafagh, L. Burkhalter, A. Hithnawi and S. Duquennoy, “Towards Blockchain-Based Auditable Storage and Sharing of IoT Data,” 2017.

[51] Y B. Ren, X H. Li, H. Liu, Q F. Cheng, J F. Ma, “Blockchain-Based Trust Management Framework for Distributed Internet of Things,” *Journal of Computer Research and Development*, vol.55, no.7, pp.108-124, 2018.
(任彦冰, 李兴华, 刘海, 程庆丰, 马建锋, “基于区块链的分布式物联网信任管理方法研究，” *计算机研究与发展*, 2018, 55(07):108-124.)

[52] P. Urien. “Blockchain IoT (BIoT): A New Direction for Solving Internet of Things Security and Trust Issues,” In Proc. *3rd Cloudification of the Internet of Things* (CIoT’18), pp.1–4, 2018.

[53] Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan and S. Wang, “An Identity Management System Based on Blockchain,” *Annual Conference on Privacy, Security and Trust* (PST’17), pp.44-4409, 2017.

[54] X. Zhu, and Y. Badr, “A Survey on Blockchain-based Identity Management Systems for the Internet of Things,” In Proc. *IEEE International Conference on Internet of Things* (iThings’18), pp.1568-1573, 2018.

[55] K. Kataoka, S. Gangwar and P. Podili, “Trust List: Internet-Wide and Distributed IoT Traffic Management Using Blockchain and SDN,” In Proc. *World Forum on Internet of Things* (WF-IoT’18), pp.296–301, 2018.

[56] M.H.Zhao,L.Zhang and J.Yuan, “Blockchain-based social Internet of things trusted service management framework, ” topic: Internet of Things technology and applications, 2017.
(赵明慧, 张碌, 亓晋, 基于区块链的社会物联网可信服务管理框架, *专题: 物联网技术与应用,* 2017)

[57] O. Novo, “Scalable Access Management in IoT using Blockchain: a Performance Evaluation,” *IEEE Internet Things J.*, pp. 1–1, 2018.

[58] X. Zhu and Y. Badr, Fog Computing Security Architecture for the Internet of Things using Blockchain-based Social Networks. In Proceedings of the 2018 IEEE Symposium on Blockchain,pp. 1361-1366, 2018.

[59] O. Alphand *et al.*, “IoTChain: A blockchain security architecture for the Internet of Things,” in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, Barcelona, pp. 1–6, 2018.

[60] Reyna, Ana, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz. “On Blockchain and Its Integration with IoT. Challenges and Opportunities.” Future Generation Computer Systems, 2018.

[61] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “Harnessing the power of blockchain technology to solve IoT security & privacy issues,” in *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing - ICC ’17*, Cambridge, United Kingdom, pp. 1–10, 2017.

[62] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, “FairAccess: a new Blockchain-based access control framework for the Internet of Things: FairAccess: a new access control framework for IoT,” *Security Comm. Networks*, vol. 9, no. 18, pp. 5943–5964, Dec. 2016.

[63] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT,” in *Europe and MENA Cooperation Advances in Information and Communication Technologies*, vol. 520, Á. Rocha, M. Serrhini, and C. Felgueiras, Eds. Cham: Springer International Publishing, pp. 523–533, 2017.

[64] M. Á. Prada-Delgado, I. Baturone, G. Dittmann, J. Jelitto, and A. Kind, “PUF-derived IoT identities in a zero-knowledge protocol for blockchain,” *Internet of Things*, p. 100057, May 2019.

[65] D. Miller, “Blockchain and the Internet of Things in the Industrial Sector,” *IT Prof.*, vol. 20, no. 3, pp. 15–18, May 2018.

[66] A. Bahga and V. K. Madisetti, “Blockchain Platform for Industrial Internet of Things,” *JSEA*, vol. 09, no. 10, pp. 533–546, 2016.

[67] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, “Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids,” *Sensors*, vol. 18, no. 2, p. 162, Jan. 2018.

[68] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, “Blockchain-Based Software-Defined Industrial Internet of Things: A Dueling Deep Q-Learning Approach,” *IEEE Internet Things J.*, pp. 1–1, 2018.

[69] Y. Liu, K. Wang, Y. Lin, and W. Xu, “LightChain: A Lightweight Blockchain System for Industrial Internet of Things,” *IEEE Trans. Ind. Inf.*, pp. 1–1, 2019.

[70] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, “Resource

Trading in Blockchain-based Industrial Internet of Things," *IEEE Trans. Ind. Inf*, pp. 1–1, 2019.

[71] W. Hou, L. Guo, and Z. Ning, "Local Electricity Storage for Blockchain-based Energy Trading in Industrial Internet of Things," *IEEE Trans. Ind. Inf.*, pp. 1–1, 2019.

[72] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Trans. Ind. Inf.*, pp. 1–1, 2017.

[73] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned Blockchain and Edge Computing Empowered Privacy-preserving Smart Grid Networks," *IEEE Internet Things J.*, pp. 1–1, 2019.

[74] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," *IEEE Trans. Dependable and Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2018.

[75] Z. Guan *et al.*, "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[76] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.

[77] Y. Yao, X. Chang, J. Misic, V. B. Misic, and L. Li, "BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3775–3784, Apr. 2019.

[78] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[79] T. Jiang, H. Fang, and H. Wang, "Blockchain-based Internet of Vehicles: Distributed Network Architecture and Performance Analysis," *IEEE Internet Things J.*, pp. 1–1, 2018.

[80] M. Singh and S. Kim, "Trust Bit: Reward-based intelligent vehicle commination using blockchain paper," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, pp. 62–67, 2018.

[81] Jianjun Sun1, Jiaqi Yan1* and Kem Z. K. Zhang , "Blockchain-based sharing services:What blockchain technology can contribute to smart cities, "Financial Innovation,2016.

[82] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," in *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Sydney, Australia, pp. 1392–1393, 2016.

[83] M. Li, L. Zhu, and X. Lin, "Efficient and Privacy-preserving Carpooling using Blockchain-assisted Vehicular Fog Computing," *IEEE Internet Things J.*, pp. 1–1, 2018.

[84] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Perva*sive Computing and Communications Workshops (PerCom Workshops), Kona, HI, pp. 618–623, 2017.

[85] S. Mondal, K. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain Inspired RFID based Information Architecture for Food Supply Chain," IEEE Internet Things J., pp. 1–1, 2019.

[86] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital Supply Chain Transformation toward Blockchain Integration," presented at the Hawaii International Conference on System Sciences, 2017.

[87] N. Dilawar, M. Rizwan, F. Ahmad, and S. Akram, "Blockchain: Securing Internet of Medical Things (IoMT)," *ijacsa*, vol. 10, no. 1, 2019.

[88] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, "HealthSense: A medical use case of Internet of Things and blockchain," in *2017 International Conference on Intelligent Sustainable Systems (ICISS)*, Palladam, pp. 486–491, 2017.

[89] R. Jayaraman, K. Saleh, and N. King, "Improving Opportunities in Healthcare Supply Chain Processes via the Internet of Things and Blockchain Technology:," *International Journal of Healthcare Information Systems and Informatics*, vol. 14, no. 2, pp. 49–65, Apr. 2019.

[90] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[91] "The Tangle | IOTA Documentation,"IOTA, https://www.iota.org, Apri.2018.

[92] "Waltonchain White paper." Waltonchain, https://www. waltonchain.org, 2017.

[93] "Introduction to Exergy."I Exergy, https://exergy.energy/,Dec.2017.

[94] "A Decentralized Network for Internet of Things Powered by a Privacy-Centric Blockchain,"IOTEX, https://iotex.io/white-paper, May. 2018.

[95] "ADEPT: An IoT Practitioner Perspective," ADEPT, https://www.ibm.com/blockchain,2018.

[96] X. Wang *et al.*, "Survey on blockchain for Internet of Things," *Computer Communications*, vol. 136, pp. 10–29, Feb. 2019.

[97] Vbuterin, "On sharding blockchains," https://github.com/ethereum/wiki/wiki/Sharding-FAQ?from=groupmessagef, 2017.

[98] A. Back *et al.*, "Enabling Blockchain Innovations with Pegged Sidechains," p. 25,2014.

[99] B. C. Florea, "Blockchain and Internet of Things data provider for

smart applications," in 2018 7th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2018, pp. 1–4.

[100] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Montreal, QC, 2017, pp. 1–5.

[101] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *IJWGS*, vol. 14, no. 4, p. 352, 2018.

[102] T. M. Fernandez-Carames and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[103] E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. de A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," *Security and Communication Networks*, vol. 2018, pp. 1–27, Apr. 2018.

[104] V. Rakovic, J. Karamachoski, V. Atanasovski, and L. Gavrilovska, "Blockchain Paradigm and Internet of Things," *Wireless Pers Commun*, vol. 106, no. 1, pp. 219–235, May 2019.

[105] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[106] "Blockchain IoT Industry Report," Blockchain , https://wxappres.feeyan.com/block/2018/11/op3RH9ZOUabCPuSQW7w0r4fkY65dFsIB.pdf,2018.

[107] M. Samaniego and R. Deters, "Blockchain as a Service for IoT," in *2016 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)*, Chengdu, China, pp. 433–436, 2016.

[108] S. Roy, Md. Ashaduzzaman, M. Hassan, and A. R. Chowdhury, "BlockChain for IoT Security and Management: Current Prospects, Challenges and Future Directions," in *2018 5th International Conference on Networking, Systems and Security (NSysS)*, Dhaka, Bangladesh, pp. 1–9, 2018.

[109] G. Zyskind, O. Nathan, and A. "Sandy" Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in 2015 IEEE Security and Privacy Workshops, San Jose, CA, 2015, pp. 180–184.

[110] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 839–858.

史慧洋 2013 年在北京邮电大学获得信号与信息处理硕士学位，现在中国科学院大学攻读博士学位，研究方向为网络与信息安全。Email: shihuiyang@ucas.ac.cn

刘 玲 2013 年在西安电子科技大学获得信息安全学士学位，现在西安电子科技大学攻读博士学位，研究方向为网络与信息安全。Email: liul@nipc.org.cn

张玉清 于 2000 年在西安电子科技大学获得博士学位。现任中国科学院大学教授，博士生导师。主要研究方向为网路与信息系统安全。Email: zhangyq@nipc.org.cn