区块链技术在物联网中的应用概述

郭才[1,2]，李续然[3]，陈炎华[2]，戴弘宁[1]
（1. 澳门科技大学，澳门 999078；2. 韩山师范学院，广东 潮州 521041；3. 山东师范大学，山东 济南 250014）

摘　要：物联网正在将传统工业重塑为以数据驱动决策为特征的智能工业。然而，物联网本身的特性带来了一系列挑战，如去中心化、互操作性差、存在隐私和安全漏洞等。区块链技术的出现为物联网应对挑战提供了新的解决途径。研究了区块链技术与物联网的融合，并把这种融合命名为物链网（BCoT, blockchain of things）。首先介绍物联网及区块链技术，然后着重介绍区块链和物联网的融合，提出了实现物链网体系结构的方案，并进一步讨论了物链网在工业中的应用问题，最后对该领域的开放性研究方向进行了概述。

关键词：区块链；物联网；智能合约；工业应用
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2021.00201

Blockchain technology for Internet of things: an overview

GUO Cai[1,2], LI Xuran[3], CHEN Yanhua[2], DAI Hongning[1]
1. Macau University of Science and Technology, Macau SAR 999078, China
2. Hanshan Normal University, Chaozhou 521041, China
3. Shandong Normal University, Jinan 250014, China

Abstract: Internet of things (IoT) is changing the data-driven smart industry due the massive availability of IoT data. Nevertheless, the IoT also poses some challenging issues like decentralization, poor interoperability, privacy and security vulnerabilities. The recent advent of blockchain can potentially tackle the above issues. The marriage of blockchain and IoT was investigated, and named this integration as blockchain of things (BCoT). In particular, the IoT and blockchain technology was introduced firstly. The convergence of blockchain and IoT was introduced, and the proposal of BCoT architecture was presented. The application of the Internet of things in the industry was further discussed. Finally, the open research directions in the field were outlined.

Key words: blockchain, Internet of things, smart contract, industrial application

1　引言

信息和通信技术的快速发展，促进了传统的计算机辅助工业向以数据驱动决策为特征的智能工业的发展[1]。在该过程中，物联网发挥了重要作用，物联网将物理工业环境与计算系统的网络空间连接起来，形成了一个信息物理系统。物联网旨在提高经营效率和生产能力，减少机器停工时间并且提高产品质量。它可以支持各种各样的工业应用，如制造业、物流业、食品工业和公共事业等。物联网具有以下特征：1) 物联网系统的去中心化；2) 物联网设备和系统的多样性；3) 物联网数据的异构性；4) 网络复杂性。这些特点也为物联网带来了挑战，如物联网系统的异构性、互操作性差、物联网设备的资源限制、存在隐私和安全漏洞等。

区块链技术的出现为解决上述问题提供了新

收稿日期：2020−06−30；**修回日期**：2020−09−10
基金项目：广东省科学技术厅科技计划项目（No.2017A040405063）
Foundation Item: The Science and Technology Program of Guangdong Province Science and Technology Department (No.2017A040405063)

的途径。区块链本质上是一个基于分布式系统的分布式记账平台，利用分散共识的方法，区块链可以在一个相互不信任的分布式系统中对交易进行验证，并且不需要可信第三方的干预。与现有的由中央机构对交易进行验证的交易管理系统不同，区块链可以实现交易的分散验证，节省了大量成本，避免了中央节点性能瓶颈。其次，保存在区块链中的每个交易本质上是不可变的，因为网络中的每个节点都保存了区块链中所有已提交的事务。同时，加密机制（如非对称加密算法、数字签名和哈希函数）保证了区块链中数据块的完整性，因此，区块链可以确保交易的不可否认性。另外，区块链中的每个交易都可以跟踪每个带有历史时间戳的用户。

从本质上来说，区块链是物联网的一个有力补充，具有更好的互操作性、保密性、安全性、可靠性和可扩展性。本文研究了一种将区块链与物联网结合的新模式，命名为物链网，物链网具备以下优点。

1) 互操作性：互操作性是指物理系统之间相互配合及信息交换的能力。它可以通过在不同物联网系统之间构建区块链复合层实现，该区块链复合层位于具有统一访问权限的对等（P2P, peer-to-peer）网络的顶部。

2) 可追溯性：物链网的可追溯性是指跟踪和验证区块链中保存的数据块的空间和时间信息的能力。当每个数据块保存在一个区块链上时会附加一个历史时间戳，以保证追溯数据的能力。

3) 可靠性：物链网的可靠性是指通过非对称加密算法、哈希函数和数字签名等密码学机制来保证数据的完整性，这些密码学机制是区块链本身具有的。

4) 自主交互作用：物链网系统的自主交互作用是指各个物链网系统在没有可信第三方干预的情况下互动的能力，这种自主性可以通过区块链启用的智能合约实现。

虽然物链网可以使物联网受益，但在物链网的潜力得到充分释放之前，还有许多问题需要解决。因此，本文旨在对物链网的最新进展、挑战和未解决的问题进行深入研究。

1.1　本文与现有研究的比较

目前，已有部分研究讨论了物联网与区块链的融合问题。文献[2]提出了一个使用区块链的物联网智能家居应用，根据文中的结果表明，其提出的基于区块链的智能家居框架可以满足安全要求，并且引入的开销（如流量、处理时间和能耗等方面）相对于其安全性和隐私增益是非常小的。文献[3]提出了一个基于智能合约和区块链的支持对等交易的商业模型，实现智能财产和物联网的付费数据交易。然而，上述研究仅局限于特定场景。关于区块链与物联网的融合，已有部分工作进行了讨论。文献[4]通过归纳一些实际案例，针对区块链与物联网的结合提出了系统性的文献综述。文献[5]提出了一个关于物联网安全的综述，并研究了区块链技术作为解决方案的可行性。Reyna 等[6]研究了区块链与物联网融合的可能性和可能存在的问题，如存储容量和可伸缩性、安全性、匿名性和数据隐私问题等。文献[7]对区块链和物联网在应用方面的融合进行了综述，对开发基于区块链的物联网应用这一过程进行了分析。文献[8]尝试对区块链技术在物联网中的应用做一个全面的总结，并研究基于区块链的物联网系统如何实现分散化以及如何保证安全性、可审计性的特点。文献[9]对区块链在物联网中的应用进行了分类，考虑了不同的应用领域、使用模式（包括设备操作和数据管理）以及解决方案的开发等。

现有的大多数研究存在以下局限性。

1) 没有为物链网提出总体架构。

2) 智能合约在物链网中扮演一个非常重要的角色，但大多数研究没有提及智能合约的生命周期。

1.2　本文贡献

本文的主要贡献如下。

1) 简要介绍了物联网及其面临的挑战，并分析了区块链的关键特征和现有区块链系统的分类。

2) 重点研究了区块链和物联网的融合。首先讨论了区块链与物联网融合的机会，然后提出了物链网的总体架构。

3) 总结了物链网的应用，并概述物链网中的开放问题及未来研究方向。

2　物联网与区块链技术

2.1　物联网概述

由于物联网和大数据分析技术的快速发展，传统工业正在经历从传统计算机辅助工业向智能工业的模式转变。在这个过程中，物联网起到了弥合物理工业环境和计算系统的网络空间之间的差异的关键作用，大数据分析可以帮助人们从大量的物联网数据中提取隐藏的价值，从而做出明智的决策。

物联网本质上是一个能提供各种工业服务的智能设备网络。典型的物联网系统由感知层、通信层和工业应用层组成，如图 1 所示。

1) 感知层：在感知层，物联网设备种类很多，包括传感器、条形码/二维码标签、无线射频识别标签、机械手、读卡器及其他无线/有线设备。这些设备可以从物理环境中感知和收集数据，同时，一些设备还可以在物理环境中主动工作。

2) 通信层：通信层包括各种无线/有线设备，如传感器、无线射频识别设备、其他标签连接物联网网关、无线接入点（AP, access point）、微型基站和宏基站，从而形成一个工业网络。这个网络连接是通过多种通信协议实现的，如蓝牙、近场通信（NFC, near field communication）、低功耗无线个人局域网（6LoWPAN）、可寻址远程传感器数据通路系统（WirelessHART）[10]、低功耗广域网（LPWAN, low-power wide-area network）技术等，其中低功耗广域网包括 Sigfox、LoRa、窄带物联网（NB-IoT, narrow band Internet of things）和工业以太网等。

3) 工业应用层：物联网可以广泛用于支持许多工业应用。典型的工业应用包括制造业、供应链、食品工业、智能交通、医疗健康和车联网等。

2.2 物联网面临的挑战

本文主要研究工业物联网，后文中提及的物联网一般是指工业物联网。物联网通过安装在工业设备上的各种电子或机械传感器、驱动器为软件系统收集相关物理环境数据，并做出响应。物联网的特点使其面临以下 6 个方面挑战。

1) 物联网系统的异构性。这个特性表现为物联网中设备异构性、通信原型异构性和数据类型（即结构化、半结构化和非结构化）异构性。异构性也是很多其他挑战的根源，如互操作性、隐私性和安全性等。

2) 网络的复杂性。物联网中存在多种通信/网络协议。典型的网络协议包括 NFC、蓝牙、6LoWPAN、WirelessHART、Sigfox、LoRa 和 NB-IoT，这些协议可以提供不同的网络服务。如 6LoWPAN 和 WirelessHART 的通信覆盖范围通常很小（小于 100 m），而 LPWAN 技术可以提供的覆盖范围为 1～10 km[11-12]。

3) 互操作性差。互操作性是指物联网系统（包括硬件和软件）交换、利用信息和相互协作的能力。由于物联网系统的去中心化和异构性，导致不同的工业部门与物联网系统进行交换数据成为一个挑战。因此，实现物联网的互操作性比较困难。

4) 物联网设备的资源限制。传感器、执行器、无线射频识别标签和智能仪表等物联网设备会受计算资源、存储资源和电池电量等有限资源的限制。如无线射频识别标签没有电池电量，只能从无线射频识别阅读器或周围环境中获取能量[13]。此外，资源限制也导致物联网设备容易受到恶意攻击。

5) 隐私漏洞。隐私保护是指在未经用户同意时不泄露用户私人信息的前提下，保证物联网数据的合法使用。由于物联网系统等复杂性、去中心化以及物联网系统异构性等特点，使得在物联网中保护数据隐私成为一大挑战。此外，将物联网与可以提供物联网额外的计算和存储能力的云计算进行整

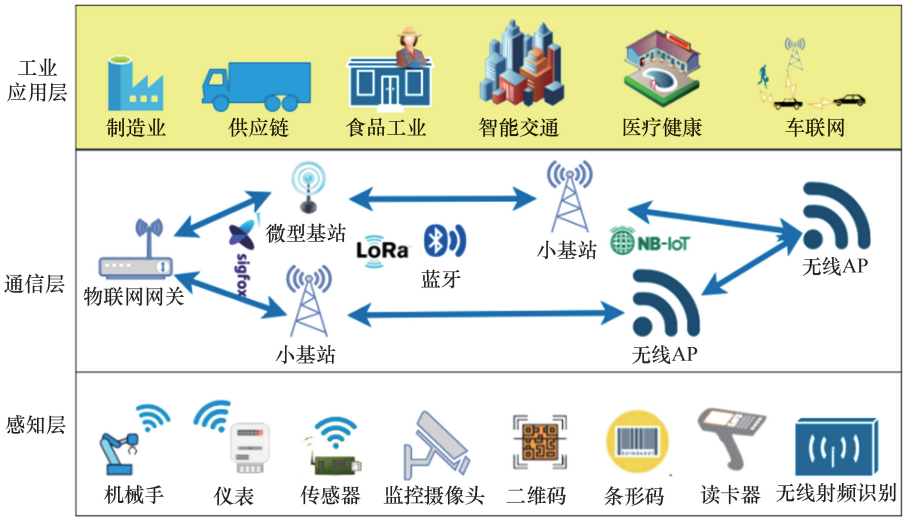

图 1 由感知层、通信层和工业应用层组成的物联网

合成为一种趋势。然而，将物联网数据上传到第三方云服务器也可能会出现隐私漏洞。

6) 安全漏洞。去中心化和物联网系统的异构性导致了物联网的安全难以得到保障，而安全对于企业来说至关重要。在资源受限的物联网系统中，由于应用安全问题的难度较大，一些典型的解决方案如认证、授权、通信加密等并不适合应用于物联网。此外，由于安全固件无法及时更新，物联网系统容易受到恶意攻击。

物联网的一些内在限制可以随着信息通信技术的进步得到解决。如环境反向通信可以帮助物联网节点从环境中获得额外的能量。同时，移动边缘计算可以通过将计算密集型任务分配到边缘服务器上来扩展物联网节点的能力[14]。更重要的是，区块链技术的不断发展为解决互操作性差、隐私和安全漏洞等问题提供了可行的解决方案。另外，区块链也有利于解决物联网系统的异构性。

2.3　区块链技术概述

2.3.1　区块链

区块链本质上是一个分布在整个区块链系统上的账本[15]。区块链的详细构成如图 2 所示，区块链中的每个块（除了第一个块）通过一个反向引用指向它的前一个块（称为父块），这个引用本质上是父块的哈希值。如块 i 包含如图 2 所示的块 i–1 的哈希值。区块链的第一个块叫做创世块，没有父块。具体来说，块结构由以下信息组成：1) 块版本（指示要遵循的验证规则）；2) 父块的哈希值；3) 时间戳记录当前时间（以秒为单位）；4) 随机哈希值；5) 交易数量；6) Merkle Root（即默克尔树根的哈希值，对应块中所有交易的哈希值）。

区块链的长度随着交易的增加不断增加。当生成一个新块时，网络中的所有节点都将参与块验证。一个经过验证的块将通过指向父块的反向引用自动附加到链的末尾。通过这种方式，可以很容易地检测到对以前生成的块进行的任何未经授权的更改。

由于篡改块的哈希值与未更改块的哈希值有显著差异，因此很容易检测到对以前生成的块进行的任何未经授权的更改。此外，由于区块链分布在整个网络中，篡改行为也可以很容易地被网络中的其他节点检测到。

区块链中的数据完整性保证。区块链利用密码技术保证数据完整性，具体来说，区块链通过以下两种机制来确保数据的完整性：1) 一个有序的链表结构，其中每个新增加的块必须包括前一个块的哈希值。通过这种方式，对前面的任何块进行伪造都将使后面的块无效。2) 默克尔树结构，其中每个块包含一个默克尔树的所有交易的哈希值。由于每个非叶节点本质上是其两个子节点的两个串联值的哈希值，因此，默克尔树通常是一棵二叉树。交易上的任何伪造都将导致在上一层产生新的哈希值，进而导致根节点哈希值出错，因此，任何伪造都很容易被发现。

2.3.2　共识算法

区块链技术的优势之一是在去中心化的不可信环境中验证区块的可信度，同时不需要可信的第三方授权。在分布式环境中，很难在新生成的块上达成共识，因为共识可能偏向于恶意节点。去中心化环境中的这种信任验证可以通过共识算法实现，典型的共识算法包括工作量证明（PoW, proof of work）、权益证明（PoS, proof of stake）和实用拜占庭容错算法（PBFT, practical Byzantine fault tolerance）[16]等。

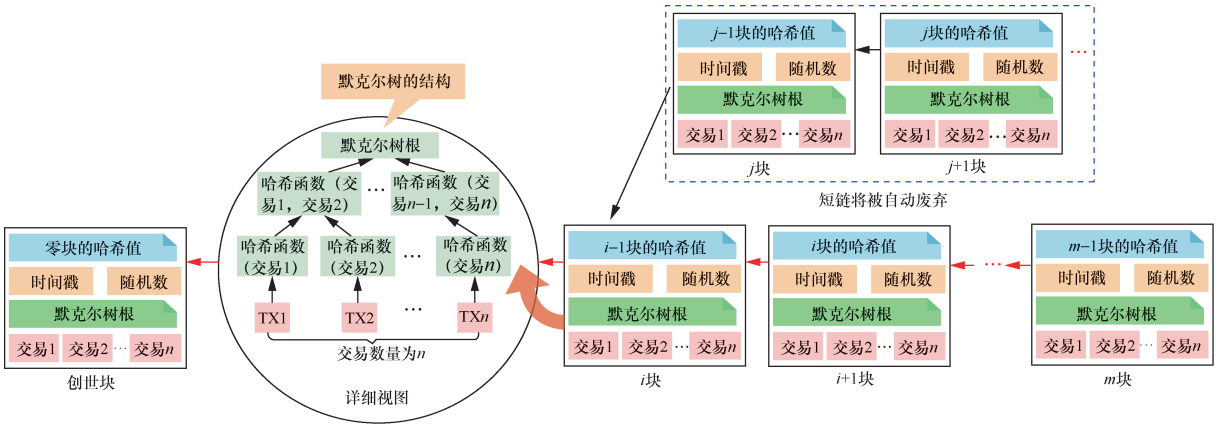

图 2　区块链的详细构成

以 PoW 为例。创建一个新生成的块相当于解决一个计算困难的问题，分布式 P2P 网络中的每个节点都可以参与验证过程[17]。第一个解决这个难题的节点可以将验证块附加到区块链上，这个节点也称为矿工。然后，将验证结果广播至整个区块链系统中，同时对其他节点进行验证，更新区块链中的新结果。最后，将发放一小部分奖金作为解决这个难题的补偿。

差异解。在分布式系统中，多个节点几乎可以同时验证块。同时，网络时延可能以某种方式同时生成分叉链。为了解决差异，大多数现有的区块链系统通常将维持最长的链作为有效链，较短的链将被自动废弃（如图 2 所示的蓝色虚线框），未来的验证工作将继续在最长的链上进行。

在 PoW 中，交易可信建立在大多数区块链节点可信任的基础上。一般来说，51%的算力是对恶意攻击容错的阈值。激励机制可以鼓励矿商诚实地反对妥协，同时，解决这个难题需要大量的计算能力。一个矿工解决难题的概率常常与这个矿工的计算能力和资源成正比[18]。

PoW 需要大量的计算，从而造成了大量的能量消耗。与 PoW 不同，PoS 需要所有权证明来验证块的可信度，因为拥有更多加密货币的用户比拥有更少加密货币的用户更可信。在 PBFT 中，每个具有平等投票权的节点将其投票状态发送至其他节点。经过多轮投票程序后，各方达成共识。共识算法的分类如表 1 所示。

表 1　　共识算法的分类

区别	概率共识算法	确定性共识算法
共识步骤	先保存再进行共识	先共识再保存
分叉	是	否
仲裁机制	当有多个分叉时，选择最长链	通过多轮通信投票解决争议
恶意攻击容错	<50% 算力	<1/3 投票节点
复杂性	计算难度大	网络需求大
举例	PoW、PoS、DPoS	PBFT、PBF 的变体

如表 1 所示，将典型的共识算法大概分为两类：1) 概率共识算法；2) 确定性共识算法。在概率共识算法（包括 PoW、PoS 和 PBFT）中，通常首先将验证块保存到链中，然后寻求所有节点的共识；而确定性共识算法首先同意该块，然后将验证块保存到链中。此外，概率共识算法一般会产生多个分叉链，并通过选择最长的分叉链来解决分叉问题。相比之下，确定性共识算法通过多轮通信来解决这一问题。

有许多研究尝试对现有的共识算法进行改进，如 Ripple[19]、Algorand[20]、Tendermint、权限证明（PoA，proof of authority）[21]、已用时间证明（PoET，proof of elapsed time）。为了满足不同应用的需求，目前的应用趋势是集成多种共识算法，而不是选择单一的共识算法。

2.3.3　区块链的工作流程

通过一个例子说明区块链的工作流程。区块链的工作流如图 3 所示。假设 Alice 想把一笔钱转给

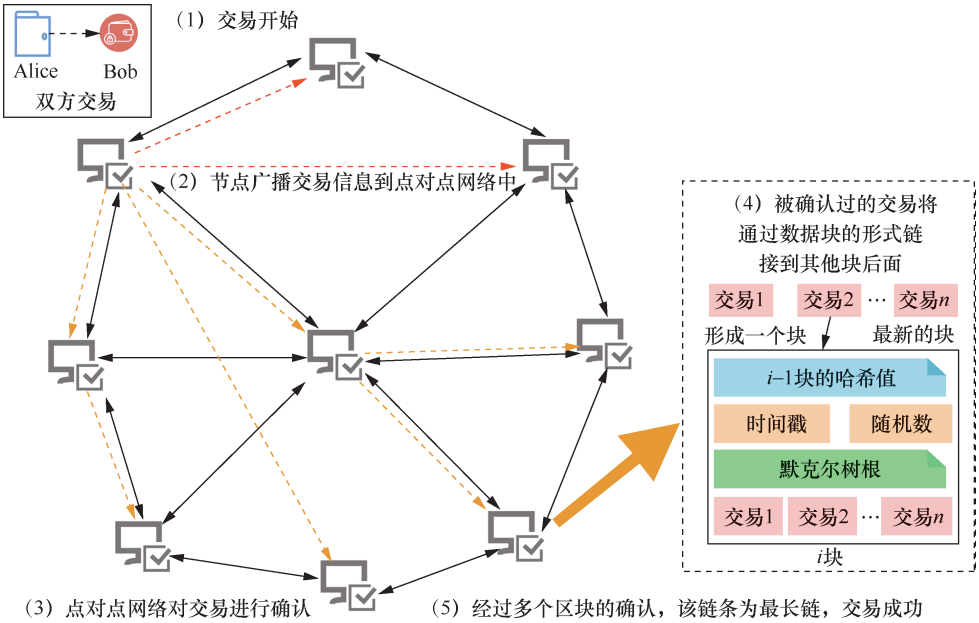

图 3　区块链的工作流

Bob。首先，Alice 通过其比特币钱包在计算机上开始交易（即步骤 1），交易包括信息如发件人的钱包、收件人的地址和金额。该交易由 Alice 的私钥签名，其他用户通过 Alice 的公钥进行访问和验证。然后，计算机将发起的事务广播到 P2P 网络中的其他计算机或节点（即步骤 2）。接下来，一旦矿工成功地解决区块难题，一个经过验证的交易将被追加到交易链的末端，在区块链中形成一个新的块（即步骤 3）。当验证的交易被附加到区块链上时，每个节点保存一个更新的区块链的副本（即步骤 4）。最后，经过多个区块确认该链条为最长链，交易成功（即步骤 5）。

2.4　区块链的特点

2.4.1　区块链技术的关键特征

1) 去中心化。在传统的交易管理系统中，通过受信任的机构（如银行、政府）进行交易验证。这种集中化的方式必然会导致交易系统额外成本、性能瓶颈和单点故障。相比之下，区块链允许交易在两个节点之间进行验证，不需要中央机构的认证、管辖权或干预，从而降低了服务成本，减少了性能瓶颈，降低了单点故障风险。

2) 不可篡改性。区块链由连续链接的区块组成，其中每个链接本质上是前一个块的逆哈希点。对前一个块的任何修改都会使所有因此生成的块失效。同时，默克尔树的根哈希值包含所有已提交交易的哈希值。任何交易上的更改都会生成一个新的默克尔树根，因此，任何伪造很容易被发现。逆哈希点与默克尔树的结合可以保证数据的完整性。

3) 不可否认性。在区块链中，私钥用于将签名放到交易中，然后其他人可以通过对应的公钥访问和验证该交易。因此，交易发起方不能拒绝用密码签名的交易。

4) 透明度。对于大多数公共区块链系统（如比特币、以太坊）而言，每个用户都有平等访问以及与区块链网络通信的权利。此外，每个新的交易都被验证和保存在区块链中，因此区块链系统对每个用户来说都是可用的。因此，区块链数据本质上是透明的，每一个区块链用户都能访问和验证其中的交易。

5) 匿名。尽管区块链数据具有高透明度，区块链系统可以通过使区块链地址匿名来保留一定程度的隐私。如文献[22]中提出了一种区块链的应用，可以保护个人数据的隐私。然而，区块链只能在一定程度上保护隐私，因为区块链地址本质上是可以被推算出来的[8]。如文献[23]中显示，区块链数据的分析可以帮助检测欺诈和非法交易。因此，区块链只能保留假名而不是完全隐私。

6) 可追溯性。在区块链中保存的每个交易都附有一个时间戳（交易发生时记录）。因此，用户可以通过分析带有相应时间戳的区块链数据，方便地验证和跟踪历史数据项的来源。

2.4.2　智能合约

智能合约是区块链技术的一个巨大进步[24]。在 20 世纪 90 年代，Nick Szabo 把智能合约被定义为执行协议合约条款的计算机化交易协议，智能合约中嵌入的合约条款在满足某些条件时将自动生效（如违反合约的一方将自动受到惩罚）。

区块链使得智能合约成为可能。本质上，智能合约是在区块链的顶部实现的。经过验证的合约条款会被转换成可执行的计算机程序，而合约条款之间的逻辑联系也以程序中逻辑流的形式保留下来（如 if-else-if 语句），每个合同语句的执行都被记录为一项不可变的事务存储在区块链中。智能合约保证合适的访问控制和合约执行，具体来说，开发人员可以为合约中的每个函数分配访问权限。一旦智能通道中的任何条件得到满足，被触发的语句将以可预测的方式自动执行相应的函数。如 Alice 和 Bob 就违反合约的惩罚达成了一致，如果 Bob 违反合约，那么相应的罚款（合约中规定的）将自动从 Bob 的押金中支付。

智能合约的整个生命周期包括 4 个连续的阶段，智能合约的生命周期如图 4 所示。

1) 创建智能合约。参与方首先就合约的义务、权利和禁止条件进行谈判。经过多轮讨论和谈判，双方达成协议。律师或顾问将帮助当事人起草一份初始合约协议。然后，软件工程师将用自然语言编写的协议转换成用计算机语言编写的智能合约，包括声明式语言和基于逻辑的规则语言[25]。与计算机软件的开发类似，智能合约转换的过程包括设计、实现和验证。需要说明的是，智能合约的创建是一个涉及多轮协商和迭代的过程。同时，它还涉及与多方合作，如利益相关者、律师和软件工程师。

2) 部署智能合约。经验证的智能合约可以部署到区块链顶端的平台上。由于区块链的不可篡改性，存储在区块链上的合约不能被修改，任何修改都需要制定新的合约。一旦在区块链上部署了智能

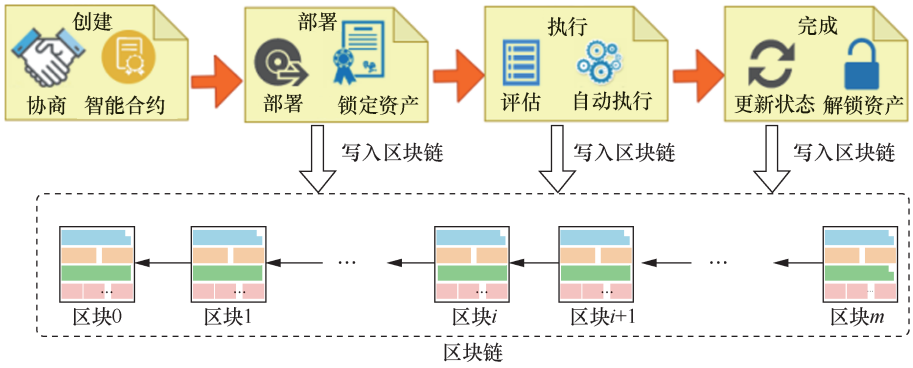

图 4　智能合约的生命周期

合约，各方都可以通过区块链访问合约。此外，通过冻结相应的数字钱包可以锁定智能合约双方的数字资产。

3) 智能合约的执行。在部署智能合约后，对合约条款进行监督和评估。一旦合约条款达成（如产品接收），合约条款（或功能）将自动执行。需要注意的是，一个智能合约包括一些声明性陈述与逻辑联系。当一个条件被触发时，相应的语句将被自动执行，然后区块链中的矿工将执行并验证交易。已提交的交易和更新状态随后被存储到区块链上。

4) 完成智能合约。在智能合约执行之后，所有相关方的新状态将被更新。因此，在执行智能合约期间的交易以及更新状态都存储在区块链中。同时，数字资产已经从一方转移到另一方（如从买方到供应商的资金转移），相关各方的数字资产被解锁。至此，智能合约完成了整个生命周期。

需要指出的是，在智能合约的部署、执行和完成过程中，执行了一系列交易（每个交易对应智能合约中的一个语句），并将其存储在区块链中。因此，智能合约的部署、执行和完成阶段都需要写数据到区块链中，如图 4 所示。

2.5　区块链类别

将区块链系统分为 3 种类型：公共区块链、私有区块链、联盟（或社区）区块链[26]。大多数数字货币（如比特币、以太坊）是在公共区块链上实现的，因此 P2P 网络中的任何人都可以访问。私有区块链与之不同，可以由单一组织管理或控制，而联盟区块链则介于两者之间。3 种区块链系统的比较如表 2 所示。

接下来，对公共区块链、私有区块链和联盟区块链在以下 5 个方面的异同进行对比。

1) 去中心化。公共区块链是完全去中心化的，而私有区块链和联盟区块链被一个或多个组部分或完全控制。此外，在公共区块链中篡改交易几乎是不可能的，因为每个节点都有一个区块链的复制品（包含所有交易），而占主导地位的组织或多方联合体和私有区块链可以修改区块链。同样，公共区块链可以充分确保交易的不可否认性、透明度和

表 2　3 种区块链系统的比较

区别	公共区块链	私有区块链	联盟区块链
去中心化	是	否	部分
不可篡改性	是	否	部分
不可否认性	是	否	部分
透明度	是	否	部分
可追溯性	是	是	部分
可扩展能力	弱	强	中等
灵活性	弱	强	中等
访问是否需要许可	否	是	是
共识算法	PoW、PoS	Ripple	PBFT、PoA、PoET
举例	比特币、以太坊	GEMOS、多链	超级账本、以太坊

可追溯性，而私有区块链和联盟区块链不能或只能部分确保这些属性。

2) 可扩展能力。虽然公共区块链可以保证去中心化、不可篡改性、透明度、不可否认性和可追溯性，但其特点在于低交易验证率、高时延和额外的存储空间消耗，限制了公共区块链的可扩展性。与公共区块链相比，私有区块链和联盟区块链具有更好的可扩展性，因为区块链完全由单个组织或多个组织控制，很容易达成共识。

3) 灵活性。相比于私有区块链和联盟区块链，公共区块链具备更多配置选项，但其灵活性较差。

4) 许可。许可指同意或授权访问区块链。公共区块链允许公众参与，因此不需要许可。而在私有区块链和联盟区块链中，一个或多个用户按照不同的权限访问和交互是被允许的。如一些用户只能读取区块链数据，而其他用户可以读取或启动交易。

5) 共识算法。公共区块链通常使用 PoW 和 PoS 作为共识算法，这些算法具有拜占庭容错能力，同时导致了大量的资源消耗。私有区块链可以很容易地实现认证用户之间的共识。用于私有区块链的典型共识算法包括 PBFT、PoA 和 PoET。此外，联盟区块链是公共区块链和私有区块链的混合类型。其中，Ripple[19]是 PBFT 的一个变体，通常用于联盟区块链。

比特币[27]和以太坊是两个典型的公共区块链平台。GEMOS 是一个私人的医疗和供应链区块链平台。另外，MultiChain 是一个允许实现私有区块链的开源平台。至于联盟区块链，Hyperledger 正在开发商业联合区块链框架。此外，以太坊还提供了构建联盟区块链的工具。

3　区块链与物联网的结合

在本节中，首先讨论将区块链与物联网进行融合。然后，提出区块链和物联网融合的体系结构，这种融合结构称为物链网。最后，讨论物链网的部署问题。

3.1　区块链与物联网融合概述

正如前文所概括的，物联网系统正面临着许多挑战，如物联网系统的异构性、互操作性差、物联网设备的资源限制、存在隐私和安全漏洞等。区块链技术可以使物联网系统具有更高的互操作性和更高的隐私性和安全性。此外，区块链还可以提高物联网系统的可靠性和可扩展性[6]。把这种区块链与物联网的整合称为物链网，与现有的物联网系统相比，物链网具有以下优点。

1) 增强物联网系统的互操作性。区块链可以通过将物联网数据转换和存储为区块链数据，从根本上提高物联网系统的互操作性。在此过程中，异构类型的物联网数据被转换、处理、提取、压缩，最终存储在区块链中。此外，由于区块链建立在接入互联网的 P2P 网络之上，互操作性还表现在可以轻松地通过不同类型的分散网络并进行连接。

2) 改善物联网系统的安全性。一方面，物联网可以通过区块链来保护数据，因为数据是以区块链交易的形式存储的，而区块链交易是通过加密密钥进行加密和数字签名的。此外，物联网系统与区块链技术（如智能合约）的集成可以帮助提高物联网系统的安全性，通过自动更新物联网设备硬件对易受攻击的漏洞进行补救，从而提高系统的安全性[28]。

3) 物联网数据的可追溯性与可靠性。区块链数据可以随时随地进行识别和验证。同时，所有存储在区块链中的历史交易都是可追踪的。如文献[29]中开发了一个基于区块链的可追溯系统产品，为供应商和零售商提供可追踪的服务，通过这种方式，产品的质量和原创性可以得到检验和验证。此外，区块链的不可篡改性确保了物联网数据的可靠性，因为它几乎不可能改变或伪造任何存储在区块链中的交易。

4) 物联网系统的自主交互。区块链技术理论可以赋予物联网设备或子系统自动相互交互的能力。如文献[30]中建议建设分布式自治公司实现交易自动化，在这种交易中，没有政府或公司等传统角色参与支付。通过智能协议实现，可以在无人干预的情况下自动工作，节省了交易成本。

3.2　物链网的体系结构

物链网的体系结构如图 5 所示。该体系结构主要由感知层、通信层、区块链复合层及工业应用层构成。

在该体系结构中，区块链复合层起到了物联网和工业应用之间的中间件作用。这种设计有两个优点：一方面，从物联网的底层抽象出来；另一方面，为用户提供基于区块链的服务。特别是区块链复合层隐藏了下层的异构性（如物联网中的感知层和通信层）。区块链复合层提供了许多基于区块链的服务，这些服务本质上是支持各种工

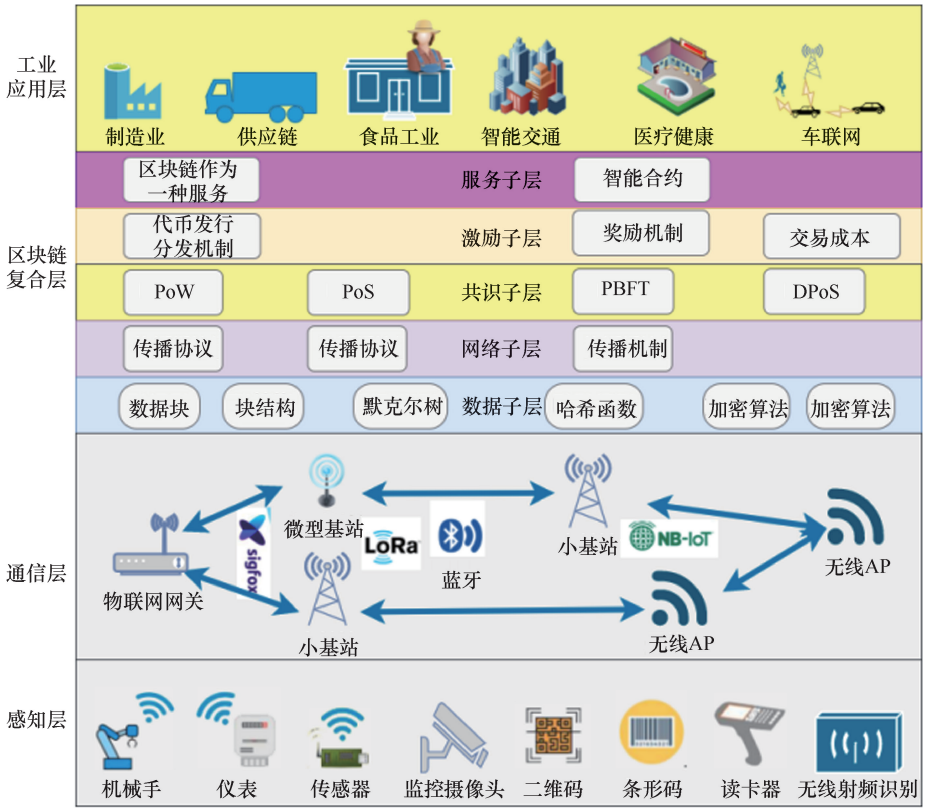

图 5　物链网的体系结构

业应用的应用程序编程接口。因此，由于区块链复合层提供的服务，使得开发工业应用程序的难度降低了。

具体来说，区块链复合层由 5 个子层组成，如图 5 所示（自下而上）。

1) 数据子层从较低层（如感知层）收集物联网数据，并通过哈希函数和非对称加密算法完成数据加密及加密后的数字签名，这些数据块经过分布式验证后形成区块链。不同的区块链平台可以选择不同的加密算法和哈希函数，如比特币区块链选择 SHA-256 作为哈希函数，将椭圆曲线数字签名算法作为签名算法。在这一层面上，物联网数据的隐私性通过区块链的数据加密得到了保证。

2) 网络子层实质上是在通信层顶部运行的 P2P 网络，由底层通信网络（有线/无线）中连接节点的虚拟或物理链路组成。一个节点仅向其连接的节点广播交易块，其他对等点一旦接收了交易块，将在本地进行验证，如果有效，则进一步通过网络传播到其他节点。利用物链网上区块链提供的接入接口，物联网设备通过对应接口进行互联，有效解决了异构性问题，物联网由于异构性差导致的操作性差也能迎刃而解；同时，物链网基于 P2P 网络的网络子层能够兼容多种通信/网络协议，从而解决了物联网网络复杂性问题。

3) 共识子层主要涉及对区块信任的分布式共识。共识机制可以通过各种共识算法来实现，如 PoW、PoS、PBFT 和 DPoS。值得一提的是，块传播机制（如中继网络程序和基于广播的传播[17]）是分布式共识协议的前提。

4) 激励子层负责以下任务：① 数字货币发行；② 数字货币分配；③ 设计奖励机制（特别是对矿工）；④ 处理交易成本等。其中，重点在于设计恰当的数字货币政策（即货币的创造和分配），奖励促成分配共识的参与者。

5) 服务子层为用户提供以区块链为基础的服务，包括制造业、物流、供应链、食品工业和公共事业等。区块链作为一种服务可以通过智能合约实现，当特殊事件发生时，可以自动触发。

区块链节点结构与 P2P 网络层如图 6 所示，建立在通信层顶部的网络子层是对底层通信网络的抽象，从而提供了跨不同网络的通用网络接入。图 6 也显示了区块链节点的结构，该结构包括区块链数据子层中的其他要素。

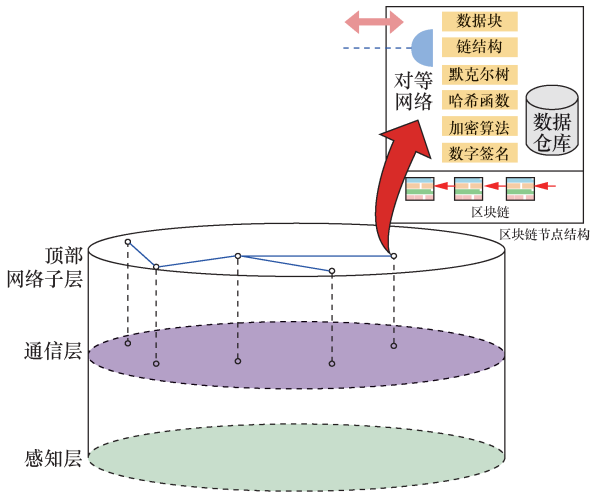

图 6　区块链节点结构与 P2P 网络层

与物联网运行过程相关的设备资源局限可以通过物链网实际部署过程采用的云服务器（全存储）或边缘服务器（部分存储）进行解决，具体将在第 3.3 节进行详述。

3.3　物链网的部署

物链网的实际部署是非常重要的一步。由于物联网设备的资源限制，在物联网设备上存储整个区块链将是一个挑战。具体来说，目前有两种模式来存储区块链数据[6]：1) 全存储，整个区块链存储在本地；2) 部分存储，只有一个子集的数据块存储在本地。因此，将完全存储区块链数据的节点命名为完全节点，将部分存储区块链数据的节点命名为轻量级节点。实际上，一个完整的节点可以是拥有足够的计算资源的云服务器或边缘服务器，因为需要一个大的存储空间来保存整个区块链（根据统计报告，截至 2020 年 12 月底，整个比特币区块链占用了近 300 GB），并且具有解决共识难题（即挖掘）的强大计算能力。而资源受限的物联网设备是轻量级节点，具有验证交易可信度的能力，不需要下载或保存整个区块链（即只保存部分区块链数据，如哈希值）。需要指出的是，轻量级节点高度依赖于完整的节点。

物链网的未来应用场景如图 7 所示，其中云服务器和边缘服务器可能存储整个区块链或部分区块链数据，而物联网设备可能只保存部分区块链数据。除了部署物链网之外，物联网和区块链之间还有 3 种可能的交互方式[8]：1) 物联网和区块链之间的直接交互，物联网设备可以直接访问与物联网网关、宏基站或小型物联网网关共处的边缘服务器上保存的区块链数据；2) 物联网节点之间的直接交互，物联网节点可以通过 D2D（device-to-device）链路直接交换或访问部分区块链数据；3) 云和边缘服务器与物联网设备的混合交互，物联网设备可以通过边缘/云服务器与区块链数据交互。

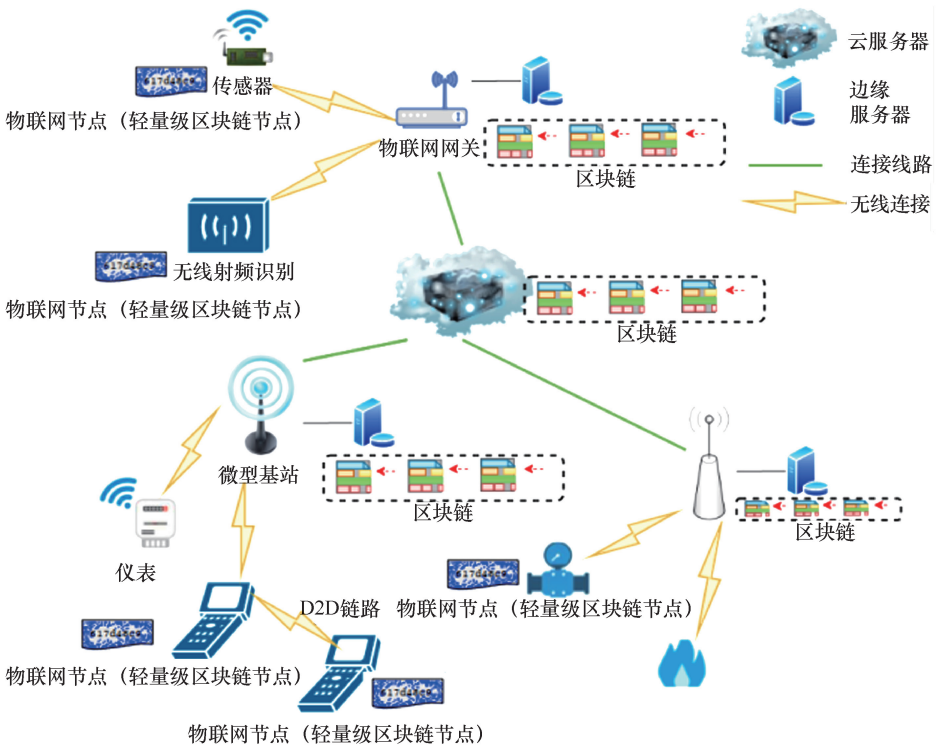

图 7　物链网的未来应用场景

4　物链网的应用

将区块链技术应用于物联网正在逐渐成为趋势，因为区块链技术可以帮助解决物联网面临的挑战。本节将对物链网的应用进行概述，区块链的应用范围非常广泛，从智能制造到车联网及无人机网络。本文主要关注物链网的工业应用，将物链网的应用分为 6 种类型，物链网的应用如图 8 所示。

4.1　智能制造

目前，制造业正在经历从自动化制造升级到智能制造[31]，制造业数据的大数据分析在升级过程中发挥了重要作用。在产品生命周期的各个阶段（包括产品设计、原材料供应、制造、配送、零售和售后服务）都会产生大量的数据。然而，制造数据这个过程是高度分散的，因此导致数据聚合和数据分析的难度加大。物链网可以通过 P2P 网络将物联网系统相互连接，并允许跨行业部门的数据共享来解决互操作性问题。如几个分布式区块链可以被构造为不同的部门服务，每个区块链服务于一个或一个以上部门。

物链网还可以提高智能制造的安全性。限制工厂升级的主要瓶颈之一是物联网系统的集中维护方式，如物联网设备需要通过定期升级固件对漏洞进行修复。然而，由于大多数物联网设备的固件需要从中央服务器下载到本地再手动安装，造成在分布式物联网中固件的安装和升级既昂贵又低效。文献[28]提出了一种基于智能合约和区块链的自动固件升级解决方案，描述了将固件升级方式的智能合约（如在何时何地升级固件）部署在整个工业网络中。然后，设备可以通过自动执行的智能合约下载并安装固件，这样可以大大节省安全维护成本。此外，文献[32]提出了一个基于分布式区块链的自动化生产平台，提供比传统的集中式架构更好的安全性和隐私保护。

在智能制造方面，区块链提供了弹性的、分布式的对等系统，以及以一种不需要信任的、可审计的方式与同行交互的能力，可以提高智能制造的互操作性。智能合约允许自动化复杂的多步骤过程，提高了智能制造的效率并降低了维护成本，但该应用对区块链的数据处理能力要求较高。

4.2　供应链

一种产品通常由多个国家不同的制造商提供的多个部件组成，在该过程中，一些伪造（或低质量）零件可能混入供应链。在产品的每个部分应用

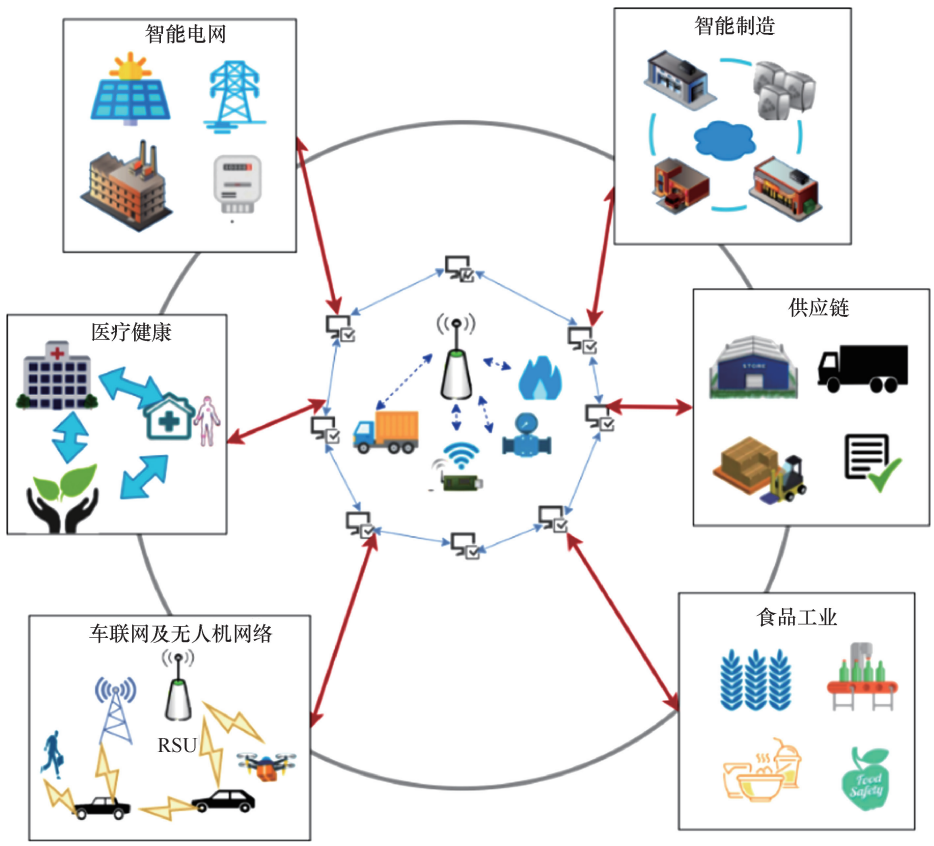

图 8　物链网的应用

反欺诈技术的成本很高，区块链和物联网的融合可以解决这个问题。特别是每个部分都将与创建的唯一身份标识（ID，identity document）相关联，同时，这个 ID 还附加了一个不可变的时间戳。另外，每个部分的识别可以被保存到一个区块链中，这是防篡改和可追踪的。文献[33]的工作表明，产品的部分所有权可以通过基于区块链的系统进行验证。此外，文献[34]提出了一种基于以太坊区块链平台的物联网和区块链技术融合的可追溯技术理论，该文提出的框架用于保证供应链数据来源。

物链网也可以用来降低供应链管理中售后服务的成本。文献[35]的工作展示了一个汽车保险的用户案例，其中理赔可以通过基于区块链的智能合约实现自动化，提高了效率，缩短了理赔处理时间。文献[36]表明，在供应链管理中，将区块链与物联网相结合可以降低成本，加快速度，降低风险。文献[37]提出了一个基于区块链的机器学习平台，确保不同企业之间的数据共享，提高客户服务质量。

在供应链管理方面使用区块链，可以使用二维码、无线射频识别等电子标签方法来识别产品，然后使用区块链对相关产品信息进行处理。区块链的开放性和分布式优势，有助于整合不同国家、不同制造商提供的产品信息。

4.3　食品工业

物链网可以提高产品（特别是食品行业）的生命周期的透明度。具体来看，食品的可溯源性是保证食品安全的必要条件。然而，对现有物联网来说，保证整个食品供应链的食品可溯源性是一个挑战[38]。如一个食品公司可能有许多供应商，可溯源性要求将从原材料到食品生产的各个部门各个环节的原始数据进行数字化。在这个过程中，区块链技术可以确保食品行业数据是可溯源的。

针对上述问题提出如下建议。首先，文献[39]建议使用无线射频识别和区块链技术，在中国建立一个从农业种植到食品生产的供应链平台，该系统已成功应用于保障食品供应链数据溯源。同时，文献[40]的工作表明，区块链技术可以通过提供溯源技术来改善食品安全。此外，文献[41]表明，食品供应链中区块链技术的应用可以让消费者跟踪食品生产的整个过程，还给出了一个使用区块链技术在哥伦比亚有机咖啡产业应用的用户案例。另外，文献[42]提出了一个基于区块链和产品电子码（EPC, electronic product code）物联网标签的可溯源食品安全系统，该系统可以通过智能合约防止数据篡改和隐私泄露，通过实现该系统的原型来验证其所提出方案的有效性。

与供应链管理方面的应用类似，借助区块链的开放性和分布式优势，可以更好地处理食品原料及产品的时间、质量等信息。有了食品原料及产品的信息，食品安全在很大程度上可以得到保证。

4.4　智能电网

分布式可再生能源的出现正在重塑能源消费者的角色，将其从纯粹的消费者变成可以利用可再生能源生产能源的生产者，拥有额外产能的消费者可以把能源卖给其他消费者，把这种能源交易称为对等能源交易。然而，在分布式环境中，如何确保两个交易方之间的能源交易安全和可信是一个挑战。

区块链技术的出现为这种能源交易的安全性提供了保障。近期一些研究建议使用区块链技术来应对这些挑战，如文献[43]开发了一个基于联盟区块链的安全能源交易系统，这个系统通过分布式共识的区块链大大节省了交易成本。此外，Aitzhan 和 Svetinovic 开发了一个基于区块链技术的去中心化能源交易系统。该系统验证了在去中心化智能电网系统中对能量交易进行保护的效果。此外，文献[44]的工作提出了一个基于区块链的机制，为智能电网提供了一个安全、透明的能源需求侧管理。

区块链可以对智能电网中的能源使用及交易等进行分布式管理、控制和验证。在该过程中，能源交易的安全性也可以由区块链来保证。

4.5　医疗健康

人口老龄化使得医疗卫生成为社会经济的重大问题之一，医院资源有限给传统医疗卫生服务带来了新的挑战。可穿戴设备的最新进展以及健康数据方面的大数据分析，为推广家庭或诊所的远程健康服务带来了机遇，医院资源的负担可能被减轻[45]。如居住在家中的老年人可以穿戴这种健康护理设备，这些可穿戴设备不断地测量和收集健康数据，包括心率、血糖和血压读数等。医生和健康护理团队可以随时随地通过健康护理网络获取健康数据。此外，物联网应用于医疗领域对大规模传染性疾病（如新型冠状病毒肺炎）的防控具有良好的辅助作用。如基于智慧医疗的远程监护是实现对患者生命体征实时、连续和长时间监测，将获取的生命体征数据和危急报警信息通过网络传送给医护人员的

一种远程监护；在公共交通、人群密集区域，采用热成像技术，可以快速完成大量人员的测温及体温监控，识别出体温异常的个体，并发出异常预警。智慧医疗可以在很大程度上减少医护人员与患者之间的直接接触，降低医护人员进行重复劳动的工作量，有助于疫情防控。然而，使用医疗数据及医疗监控也会带来隐私和安全问题。健康护理设备的脆弱性和健康护理网络的多样性，对保护隐私和保障健康数据的安全形成了挑战[46]。

将区块链融入医疗物联网可能会面临保护隐私和保障健康数据安全方面的挑战。如文献[47]提出了一个基于区块链的智慧医疗网络架构，以解决智慧医疗系统的安全和隐私问题，并且从多个角度讨论了使用该网络架构应对新型冠状病毒肺炎的解决方案。文献[48]的工作表明，使用区块链技术可以保护存储在云服务器中的卫生健康数据。Griggs 等[49]开发了一个基于区块链的系统，确保私人医疗健康数据管理，医疗传感器产生的健康数据可以通过智能合约自动收集并传输到系统，从而支持对病人的实时监测。在整个过程中，可以通过区块链技术提供对隐私的保护。文献[50]的工作提出了一个基于区块链的解决方案来管理个人医疗健康数据，并支持不同医院、医疗中心、保险公司和患者之间进行数据共享。在整个过程中，医疗数据的隐私性和安全性可以得到保障。Sun 等[51]提出了一个基于属性的签名方案的医疗健康区块链系统。一方面，该方案可以验证医疗数据的真实性，并可以识别医疗数据所有者；另一方面，该方案可以保护医疗数据所有者的隐私。文献[52]提出了一个融合物联网和基于移动边缘计算方案区块链的家庭治疗管理框架，提供保密和匿名保证，并在原型系统上验证了该系统的有效性。

综上所述，区块链在医疗健康方面的应用主要集中在患者的医疗数据安全领域。区块链可以为来自健康护理设备的患者医疗数据提供匿名处理、身份识别及使用记录等。实现该应用的关键在于区块链系统针对患者的不同类型电子医疗数据的处理机制。

4.6 车联网及无人机网络

车联网基本上集成了车辆对车辆网络、车辆对路边网络、车辆对基础设施网络和车辆对行人网络。车联网的去中心化、异构性和不可信性对确保消息传输和事务执行方面构成了挑战，通过整合区块链和车联网可以应对上述挑战。举例来说，文献[53]开发了一个基于区块链的车联网信任管理平台，其中车联网信息的真实性可以由路边单位执行 PoW 共识机制或 PoS 共识机制进行验证。此外，区块链技术可以用来保护电动汽车[54]和混合动力电动汽车在智能电网中的能源和信息交互。在未来，结合人工智能、移动边缘计算和区块链可以进一步优化车联网的资源分配[55]。

近年来，无人机通信网络可以作为无线通信网络充分覆盖的补充[56]，受到更多人的关注。同时，无人机也可以用于交付产品项目[57]及取得实时交通流量数据[58]。此外，文献[59]的研究表明，无人机可用于支持以内容为中心的网络和移动边缘计算。然而，在分散的非可信无人机网络中，如何保证网络的可信性和限制无人机的不正常行为是一个挑战。区块链技术与无人机网络的融合可以保证无人机之间的互信。文献[60]开发了一个基于以太坊区块链的自治平台来提供无人机的信任管理。另外，国际商业机器公司（IBM, International Business Machines Corporation）[61]申请了一项基于区块链的保障无人机数据隐私和安全性的系统。在区块链中的数据块将存储与无人机相关的信息，包括型号类型、制造商、限制区域。因此，无人机的不良行为可以得到及时监测和识别。

区块链有助于解决车联网的去中心化、异构性和不可信性在确保信息传输和事务执行方面的问题。区块链在车联网和无人机通信方面的应用需要满足较高的数据处理速度要求。

物链网应用场景对比如表 3 所示，总结了主要的物链网应用程序。具体来说，表 3 中结合区块链和物联网说明了物链网应用的优势。概括来说，物链网具有降低可信第三方成本、保证安全、提高数据溯源、验证数据真实性和保护隐私等优点。

表 3 物链网应用场景对比

应用	优势
智能制造[28,31-32]	提高互操作性，自动化 P2P 商业交易，降低可靠第三方的成本
供应链[33-37]	保证数据来源，降低售后服务的成本，减小供应链风险
食品工业[38-42]	提高数据可溯性，增强食品安全性
智能电网[43-44]	保护能量交易安全，提高透明度，保护隐私
医疗健康[45-52]	保证安全性，保护隐私，验证真实性
车联网及无人机网络[53-61]	保证消息的可信度，在电动车中保护能量交易的安全，保证无人机之间的相互信任

5　存在的问题及建议

尽管区块链和物联网的融合为产业升级带来了许多机遇，但在充分发挥物链网的潜力之前，还有许多挑战需要解决。本节明确了将区块链融入物联网面临的主要挑战，并讨论了潜在的解决方案。物链网待解决的研究问题如图 9 所示，图 9 总结了区块链待解决的研究问题。

5.1　资源限制

大多数物联网设备是资源受限的，如传感器、无线射频识别标签和智能仪表的计算能力较差，存储空间有限，电池电量低，网络连接能力差等。然而，去中心化共识算法的区块链往往需要强大的计算能力和能源消耗。如比特币的 PoW 算法会消耗高能量[6]。因此，对于低功耗物联网设备来说，具有巨大能耗的共识机制可能不可行。

大量的区块链数据也导致在物联网上完全部署区块链的不可行性。同时，以近乎实时的方式生成的大量物联网数据使这种现状更糟糕。此外，区块链主要是为了稳定的网络连接设计的，这对于物联网来说可能不可行，因为物联网设备的网络连接很差，并且由于节点的故障（如电池耗尽）会导致网络不稳定。

在这个问题上，将移动边缘计算和云计算技术整合到物链网中可能会克服物联网设备的资源限制。如云服务器或一些移动边缘计算服务器可以充当完整的节点，存储整个区块链数据，并参与大多数区块链操作，如启动交易、验证传输（即挖掘），而物联网设备可以充当轻量级节点，只存储部分区块链数据甚至区块链数据的哈希值，并承担一些计算量较小的任务（如启动交易）[62]。在物链网中，移动边缘计算和云计算的编排成为分配资源的一个重点[63]。

5.2　安全漏洞

尽管将区块链技术引入物联网可以通过区块链的加密和数字签名提高物联网的安全性，但由于物联网系统和区块链系统的脆弱性，安全性仍然是物链网的重点。

将无线网络应用于工业环境正在逐渐成为趋势，但是开放的无线媒介也使物联网遭受如被动窃听、干扰、重放等安全攻击。由于物联网设备的资源限制，传统的重加权加密算法可能不适用于物联网。此外，在分布式环境中管理密钥（对于加密算法来说至关重要）也是一个挑战。

区块链系统自身也存在安全漏洞，如智能合约的程序缺陷[17]。特别是，文献[64]中表明，恶意用户可以利用边界网关协议（BGP, border gateway protocol）路由方案劫持区块链消息，导致块广播时延更高。

物链网的安全漏洞可以通过增强物联网系统的安全或区块链的漏洞修复来补救。如文献[65]利用基于密钥生成方法研究了协同干扰方案，提高了物联网系统的安全性，同时对现有物联网节点不需要提供额外的硬件设备。

5.3　隐私泄露

区块链技术具有的特殊机制在一定程度上保证了区块链中交易记录的数据隐私。如比特币的交易是通过互联网协议（IP, Internet protocol）地址而不是用户的真实身份进行的，从而确保了一定的匿名性。此外，在比特币中生成一次性账户，实现用户匿名。

然而，这些保护计划还不够健全。文献[18]通过学习和推断与一个共同用户相关的多个交易，可以破解用户的假名。此外，区块链上交易数据的完整存储也可能导致潜在的隐私泄露[66]。一种潜在的解决方案是通过混合币来对付攻击者，使攻击者无法推断出一笔交易所花费的真实虚拟币的确切数量。文献[66]提出了一种内存优化和灵活的区块链数据存储方案，也在一定程度上降低了隐私泄露的风险。

5.4　物链网中的激励机制

一个适当的激励机制是对区块链系统的良性刺激。如首先解决计算任务的矿工将获得一定数量的比特币奖励。为物链网设计一个合适的激励机制来满足不同应用的需求是一个挑战。如每增加 210 000 个区块，比特币奖励将减半[67]。奖励减

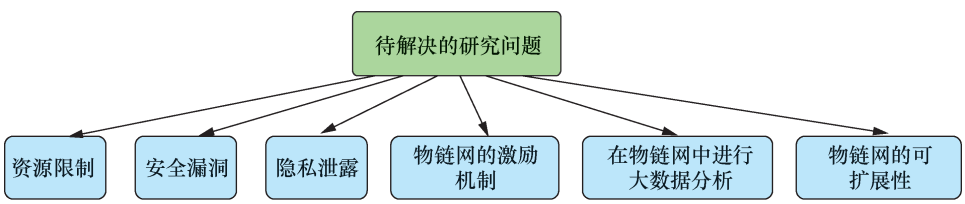

图 9　物链网待解决的研究问题

少将阻碍矿工为解决难题做出贡献，从而使矿工迁移到其他区块链平台。设计一个合适的数字货币奖励和发布机制是保证区块链系统稳定性的必要条件。

声誉和诚实是私有区块链或联盟区块链系统的用户影响因素。因此，除了数字货币以外，声誉信用还可以在个人声誉系统[68]、共享经济[69]、数据来源[70]和药品供应链[71]等情况下用作激励手段。

5.5 物链网大数据分析的困难性

大量的物链网数据以近乎实时的方式产生。物链网数据具有海量性、异构性和巨大的商业价值。对物链网数据的大数据分析可以提取隐藏的价值并帮助做出明智的决策。目前，在物链网中应用传统的大数据分析方案面临如下挑战。

由于资源的限制，传统的大数据分析方案不能应用于物联网设备。由于物联网设备的计算能力较差，复杂的大数据分析方案不能直接应用于物联网设备。此外，区块链数据的庞大体积也导致在物联网设备上存储区块链数据的不可行性。虽然云计算可以解决这些问题，但是将数据上传到远程云服务器可能导致隐私泄露和增大时延等问题[72]。

区块链技术可以通过数据加密和数字签名来保护数据隐私记录。然而，在进行数据分析之前，往往需要对数据进行解密。解密过程通常很耗时，导致数据分析效率低下[73]。设计不需要解密的区块链数据的数据分析方案具有挑战性。

移动边缘计算是云计算的一个重要补充，它将计算任务从远程云服务器转移到移动边缘计算，与用户接近。与云计算相比，移动边缘计算可以改进响应、保护隐私和上下文感知。因此，将大数据计算任务下载到移动边缘计算服务器，可以潜在地解决使用区块链的云计算的隐私泄露和长时延问题[74]。

5.6 物链网的可扩展性

现有区块链的可扩展性限制了区块链在大规模物联网中的广泛应用。区块链的可伸缩性可以通过每秒传输操作的吞吐量、物联网节点的数量和并发工作负载的数量对比来衡量。许多区块链系统的吞吐量很低，如文献[75]中比特币每秒只能处理 7 次交易。相比之下，VISA 信用卡平台每秒可以处理约 2 000 笔交易，PayPal 支付平台每秒可以处理 170 笔交易[76]。总之，现有的区块链系统可能不适合交易量大的应用，尤其是物联网。

提高物联网区块链可伸缩性有两个可能的方向：1) 设计更具可伸缩性的共识算法；2) 为物联网构建私有区块链或联盟区块链。对于设计更具可伸缩性的共识算法来说，可以选择协商一致的本地化策略来提高交易的吞吐量。同时，可以实现一些新的区块链结构。如有向无环图（DAG, directed acyclic graph）[77]允许来自侧链的非冲突块与主链组装，降低了解决分歧的成本。此外，可以考虑将 PoW 和 PBFT 集成起来，提高 PoW 的吞吐量，这与文献[78]提出的 Sharding 协议类似，在 PoW 中首先解决计算量较小的难题，然后在多个小组中达成共识。针对为物联网构建私有区块链或联盟区块链问题，由于系统是完全受控的和用户数量是有限的，私有区块链和联盟区块链的交易可以比公共区块链处理得快得多。同时，在私有区块链和联盟区块链中也很容易达成共识。

6 结束语

现有的物联网系统面临着异构性、互联能力差、资源约束、隐私和安全漏洞等挑战。区块链技术的出现为增强互操作性、隐私性、安全性、可追溯性和可靠性等提供了解决方案。

本文对区块链与物联网的融合进行了全面研究。首先简要介绍物联网和区块链技术，然后讨论了物联网和区块链结合可以带来的机遇，进一步提出了物联网和区块链结合的架构—物链网。此外，还讨论了物链网的应用，最后概述了物链网的开放性问题并展望了未来的研究方向。

参考文献：

[1] LADE P, GHOSH R, SRINIVASAN S. Manufacturing analytics and industrial Internet of things[J]. IEEE Intelligent Systems, 2017, 32(3): 74-79.

[2] DORRI A, KANHERE S S, JURDAK R, et al. Blockchain for IoT security and privacy: the case study of a smart home[C]//Proceedings of 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). Piscataway: IEEE Press, 2017: 618-623.

[3] ZHANG Y, WEN J T. 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.

[4] CONOSCENTI M, VETRÒ A, DE MARTIN J C. Blockchain for the Internet of things: a systematic literature review[C]//Proceedings of 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). Piscataway: IEEE Press, 2016: 1-6.

[5] BANERJEE M, LEE J, CHOO K K R. A blockchain future for Internet of things security: a position paper[J]. Digital Communications and

Networks, 2018, 4(3): 149-160.

[6] REYNA A, MARTN C, CHEN J, et al. On blockchain and its integration with IoT. Challenges and opportunities[J]. Future Generation Computer Systems, 2018, 88: 173-190.

[7] FERNˆ T M, ANDEZ C, FRAGA-LAMAS P. A review on the use of blockchain for the Internet of things[J]. IEEE Access, 2018, 6: 32979-33001.

[8] ALI M S, VECCHIO M, PINCHEIRA M, et al. Applications of blockchains in the Internet of things: a comprehensive survey[J]. IEEE Communications Surveys Tutorials, 2019, 21(2): 1676-1717.

[9] PANARELLO A, TAPAS N, MERLINO G, et al. Blockchain and IoT integration: a systematic survey[J]. Sensors, 2018, 18(8): 2575.

[10] PETERSEN S, CARLSEN S. WirelessHART versus ISA100.11a: the format war hits the factory floor[J]. IEEE Industrial Electronics Magazine, 2011, 5(4): 23-34.

[11] CHEN M, MIAO Y M, HAO Y X, et al. Narrow band Internet of things[J]. IEEE Access, 2017, 5: 20557-20577.

[12] KHUTSOANE O, ISONG B, ABU-MAHFOUZ A M. IoT devices and applications based on LoRa/LoRaWAN[C]//Proceedings of IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society. Piscataway: IEEE Press, 2017: 6107-6112.

[13] LU X, NIYATO D, JIANG H, et al. Ambient backscatter assisted wireless powered communications[J]. IEEE Wireless Communications, 2018, 25(2): 170-177.

[14] HE J H, WEI J, CHEN K, et al. Multitier fog computing with large-scale IoT data analytics for smart cities[J]. IEEE Internet of Things Journal, 2018, 5(2): 677-686.

[15] WANG H M, ZHENG Z B, XIE S A, et al. Blockchain challenges and opportunities: a survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.

[16] MIGUEL C, BARBARA L. Practical Byzantine fault tolerance[C]//Proceedings of the third Symposium on Operating Systems Design and Implementation. [S.l.:s.n.], 1999: 173-186.

[17] LI X Q, JIANG P, CHEN T, et al. A survey on the security of blockchain systems[J]. Future Generation Computer Systems, 2020, 107: 841-853.

[18] CONTI M, SANDEEP K E, LAL C, et al. A survey on security and privacy issues of bitcoin[J]. IEEE Communications Surveys & Tutorials, 2018, 20(4): 3416-3452.

[19] CHASE B, MACBROUGH E. Analysis of the XRP ledger consensus protocol[J]. arXiv preprint arXiv: 1802.07242, 2018.

[20] GILAD Y, HEMO R, MICALI S, et al. Algorand: scaling Byzantine agreements for cryptocurrencies[C]//Proceedings of the 26th Symposium on Operating Systems Principles. New York: ACM Press, 2017: 51-68.

[21] YU F R, LIU J M, HE Y, et al. Virtualization for distributed ledger technology (vDLT)[J]. IEEE Access, 2018, 6: 25019-25028.

[22] ZYSKIND G, NATHAN O, PENTLAND A. Decentralizing privacy: using blockchain to protect personal data[C]//Proceedings of 2015 IEEE Security and Privacy Workshops. Piscataway: IEEE Press, 2015: 180-184.

[23] CHAWATHE S S. Clustering blockchain data[M]. Berlin: Springer, 2018.

[24] REAM J, CHU Y, SCHATSKY D. Upgrading blockchains: smart contract use cases in industry[M]. Australia: Deloitte Press, 2016.

[25] IDELBERGER F, GOVERNATORI G, RIVERET R, et al. Evaluation of logic-based smart contracts for blockchain systems[M]. Berlin: Springer, 2016.

[26] XU X W, WEBER I, STAPLES M, et al. A taxonomy of blockchain-based systems for architecture design[C]//Proceedings of 2017 IEEE International Conference on Software Architecture (ICSA). Piscataway: IEEE Press, 2017: 243-252.

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

[28] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the Internet of things[J]. IEEE Access, 2016, 4: 2292-2303.

[29] LU Q H, XU X W. Adaptable blockchain-based systems: a case study for product traceability[J]. IEEE Software, 2017, 34(6): 21-27.

[30] ZHANG Y, WEN J T. An IoT electric business model based on the protocol of bitcoin[C]//Proceedings of 2015 18th International Conference on Intelligence in Next Generation Networks. Piscataway: IEEE Press, 2015: 184-191.

[31] KUSIAK A. Smart manufacturing[J]. International Journal of Production Research, 2018, 56(1/2): 508-517.

[32] WAN J F, LI J P, IMRAN M, et al. A blockchain-based solution for enhancing security and privacy in smart factory[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3652-3660.

[33] KONSTANTINIDIS I, SIAMINOS G, TIMPLALEXIS C, et al. Blockchain for business applications: a systematic literature review[M]. Berlin: Springer, 2018.

[34] KIM H M, LASKOWSKI M. Toward an ontology-driven blockchain design for supply-chain provenance[J]. Intelligent Systems in Accounting, Finance and Management. 2018, 25(1): 18-27.

[35] TAPSCOTT A, TAPSCOTT D. How blockchain is changing finance[J]. Harvard Business Review, 2017(1): 2-5.

[36] KSHETRI N. 1 Blockchain's roles in meeting key supply chain management objectives[J]. International Journal of Information Management, 2018, 39: 80-89.

[37] LI Z, GUO H Y, WANG W M, et al. A blockchain and AutoML approach for open and automated customer service[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3642-3651.

[38] TSE D, ZHANG B W, YANG Y C, et al. Blockchain application in food supply information security[C]//Proceedings of 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). Piscataway: IEEE Press, 2017: 1357-1361.

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

[40] SANDER F, SEMEIJN J, MAHR D. The acceptance of blockchain technology in meat traceability and transparency[J]. British Food Journal, 2018, 120(9): 2066-2079.

[41] BETTÍN-DÍAZ R, ROJAS A E, MEJÍA-MONCAYO C. Methodolog-

ical approach to the definition of a blockchain system for the food industry supply chain traceability[C]//Proceedings of Computational Science and its Applications-ICCSA 2018. Berlin: Springer Press, 2018: 19-33.

[42] LIN Q J, WANG H Z, PEI X F, et al. Food safety traceability system based on blockchain and EPCIS[J]. IEEE Access, 2019, 7: 20698-20707.

[43] LI Z T, KANG J W, YU R, et al. Consortium blockchain for secure energy trading in industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3690-3700.

[44] POP C, CIOARA T, ANTAL M, et al. Blockchain based decentralized management of demand response programs in smart energy grids[J]. Sensors, 2018, 18(2): 162.

[45] WANG K, SHAO Y, SHU L, et al. Mobile big data fault-tolerant processing for ehealth networks[J]. IEEE Network, 2016, 30(1): 36-42.

[46] LI X R, DAI H N, WANG Q, et al. Securing Internet of medical things with friendly-jamming schemes[J]. Computer Communications, 2020, 160: 431-442.

[47] DAI H N, IMRAN M, HAIDER N. Blockchain-enabled Internet of medical things to combat COVID-19[J]. IEEE Internet of Things Magazine, 2020, 3(3): 52-57.

[48] ESPOSITO C, DE SANTIS A, TORTORA G, et al. Blockchain: a panacea for healthcare cloud-based data security and privacy?[J]. IEEE Cloud Computing, 2018, 5(1): 31-37.

[49] GRIGGS K N, OSSIPOVA O, KOHLIOS C P, et al. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring[J]. Journal of Medical Systems, 2018, 42(7): 1-7.

[50] BHUIYAN M Z A, ZAMAN A, WANG T, et al. Blockchain and big data to transform the healthcare[C]//Proceedings of the International Conference on Data Processing and Applications-ICDPA 2018. New York: ACM Press, 2018.

[51] SUN Y, ZHANG R, WANG X, et al. A decentralizing attribute-based signature for healthcare blockchain[C]//Proceedings of 2018 27th International Conference on Computer Communication and Networks (ICCCN). Piscataway: IEEE Press, 2018: 1-9.

[52] RAHMAN M A, HOSSAIN M S, LOUKAS G, et al. Blockchain-based mobile edge computing framework for secure therapy applications[J]. IEEE Access, 2018, 6: 72469-72478.

[53] YANG Z, YANG K, LEI L, et al. Blockchain-based decentralized trust management in vehicular networks[J]. IEEE Internet of Things Journal, 2019, 6(2): 1495-1505.

[54] LIU H, ZHANG Y, YANG T. Blockchain-enabled security in electric vehicles cloud and edge computing[J]. IEEE Network, 2018, 32(3): 78-83.

[55] DAI Y Y, XU D, MAHARJAN S, et al. Artificial intelligence empowered edge computing and caching for Internet of vehicles[J]. IEEE Wireless Communications, 2019, 26(3): 12-18.

[56] ZENG Y, ZHANG R, LIM T J. Wireless communications with unmanned aerial vehicles: opportunities and challenges[J]. IEEE Communications Magazine, 2016, 54(5): 36-42.

[57] KIMCHI G, BUCHMUELLER D, GREEN S A, et al. Unmanned aerial vehicle delivery system[P]. United States: 9,573,684. 2017.

[58] WANG L, CHEN F L, YIN H M. Detecting and tracking vehicles in traffic by unmanned aerial vehicles[J]. Automation in Construction, 2016, 72: 294-308.

[59] CHENG N, XU W C, SHI W S, et al. Air-ground integrated mobile edge networks: architecture, challenges, and opportunities[J]. IEEE Communications Magazine, 2018, 56(8): 26-32.

[60] KAPITONOV A, LONSHAKOV S, KRUPENKIN A, et al. Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs[C]//Proceedings of 2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS). Piscataway: IEEE Press, 2017: 84-89.

[61] KUMAR A, KUNDU A, PICKOVER C A, et al. Un-manned aerial vehicle data management[J]. US Patent, 2018.

[62] DAI Y Y, XU D, MAHARJAN S, et al. Joint computation offloading and user association in multi-task mobile edge computing[J]. IEEE Transactions on Vehicular Technology, 2018, 67(12): 12313-12325.

[63] TRAN T X, HAJISAMI A, PANDEY P, et al. Collaborative mobile edge computing in 5G networks: new paradigms, scenarios, and challenges[J]. IEEE Communications Magazine, 2017, 55(4): 54-61.

[64] APOSTOLAKI M, ZOHAR A, VANBEVER L. Hijacking bitcoin: routing attacks on cryptocurrencies[C]//Proceedings of 2017 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2017: 375-392.

[65] DORRI A, KANHERE S S, JURDAK R. Lora-key: secure key generation system for loRa-based network[J]. IEEE Internet of Things Journal, 2019, 6(4): 6404-6416.

[66] DORRI A, KANHERE S S, JURDAK R. MOF-BC: a memory optimized and flexible blockchain for large scale networks[J]. Future Generation Computer Systems, 2019, 92: 357-373.

[67] SAITO K, IWAMURA M. How to make a digital currency on a blockchain stable[J]. arXiv preprint arXiv: 1801.06771, 2018.

[68] YASIN A, LIU L. An online identity and smart contract management system[C]//Proceedings of 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). Piscataway: IEEE Press, 2016: 192-198.

[69] BOGNER A, CHANSON M, MEEUW A. A decentralised sharing app running a smart contract on the ethereum blockchain[C]//Proceedings of IoT'16: the 6th International Conference on the Internet of Things. [S.l.:s.n.], 2016: 177-178.

[70] LIANG X P, SHETTY S, TOSH D, et al. ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability[C]//Proceedings of 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). Piscataway: IEEE Press, 2017: 468-477.

[71] GLOVER D G, HERMANS J. Improving the traceability of the clinical trial supply chain[J]. Applied Clinical Trials, 2017, 26(11): 36-38.

[72] WANG P, GAO R X, FAN Z Y. Cloud computing for cloud manufacturing: benefits and limitations[J]. Journal of Manufacturing Science and Engineering, 2015, 137(4): 040901.

[73] WANG N, XIAO X K, YANG Y, et al. PrivTrie: effective frequent term discovery under local differential privacy[C]//Proceedings of 2018 IEEE 34th International Conference on Data Engineering (ICDE). Piscataway: IEEE Press, 2018: 821-832.

[74] DAI Y Y, XU D, MAHARJAN S, et al. Blockchain and deep reinforcement learning empowered intelligent 5G beyond[J]. IEEE Network, 2019, 33(3): 10-17.

[75] CROMAN K, DECKER C, EYAL I, et al. On scaling de-centralized blockchains[C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin: Springer Press, 2016: 106-125.

[76] ALBRECHT S, REICHERT S, SCHMID J, et al. Dynamics of blockchain implementation-a case study from the energy sector[C]//Proceedings of the 51st Hawaii International Conference on System Sciences. [S.l.:s.n.], 2018.

[77] LEWENBERG Y, SOMPOLINSKY Y, ZOHAR A. Inclusive block chain protocols[M]. Berlin: Springer, 2015.

[78] LUU L, NARAYANAN V, ZHENG C D, et al. A secure sharding protocol for open blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016.

[作者简介]

郭才（1984− ），男，澳门科技大学博士生，韩山师范学院实验师，主要研究方向为深度学习、区块链。

李续然（1991− ），男，山东师范大学讲师，主要研究方向为无线网络安全、医疗物联网、区块链。

陈炎华（1985− ），男，韩山师范学院实验师，主要研究方向为软件开发、区块链。

戴弘宁（1977− ），男，澳门科技大学副教授、博士生导师，主要研究方向为工业物联网、大数据分析、区块链、移动智能和大规模无线网络。