# 区块链在物联网系统中的应用探讨

高镇[1]，崔琪楣[2]，张雪菲[2]，王晓飞[1]
（1. 天津大学，天津 300072；2. 北京邮电大学，北京 100876）

**摘　要：**区块链技术近年来受到广泛关注，很多行业都在尝试基于区块链技术解决信息系统中传统中心化方案存在的可靠性与安全等难题。而将区块链网络与行业实体相关联必须依托物联网技术，因此，结合区块链和物联网技术解决不同领域中的多方协作问题是当前的研究热点。另一方面，物联网自身发展也受到中心化架构的限制，如何利用区块链技术解决现有物联网系统的不足也是一个重要问题。尽管当前区块链技术的相关应用非常多，但其中一些应用实际上并不适合采用区块链技术。首先介绍了区块链技术的应用逻辑，然后基于典型案例分析介绍区块链结合物联网的适用场景，最后讨论了 4 个区块链与物联网结合的共性问题。

**关键词：**区块链；物联网；应用分析
**中图分类号：**TP311
**文献标识码：**A
**doi:** 10.11959/j.issn.2096−3750.2020.00170

# Discussions about application of blockchain in IoT systems

GAO Zhen[1], CUI Qimei[2], ZHANG Xuefei[2], WANG Xiaofei[1]
1. Tianjin University, Tianjin 300072, China
2. Beijing University of Posts and Telecommunications, Beijng 100876, China

**Abstract:** Blockchain technology has attracted wide attention in recent years, and many industries are trying to solve the reliability and security problems of traditional centralized schemes in information systems based on blockchain technology. However, the connection between the blockchain network and industry entities must rely on the Internet of things (IoT) technology. Therefore, combining the blockchain and IoT technology to solve the pain points of vertical industries is the current research hotspot. On the other hand, the development of IoT itself is also limited by the centralized architecture, and how to use the blockchain technology to solve the predicament of IoT is also an important issue. Although there are many blockchain related applications, some of them are actually not suitable for blockchain technology. Firstly, the proper logic of blockchain applications was discussed. Then suitable application scenarios of blockchain technology were introduced by typical case analysis. Finally, four common problems when combining blockchain and IoT were discussed.

**Key words:** blockchain, Internet of things, application analysis

## 1　引言

区块链是比特币的底层技术，是一系列技术集成的代名词，包括区块链数据结构、非对称加密、点对点网络、共识算法、激励制度等[1]。由于比特币在完全没有人为管理的情况下一直能够正常运行，因此，产业界和学术界从 2015 年开始意识到区块链技术的巨大潜力，甚至将其看作是“继大型机、个人电脑、互联网、移动/社交网络后，计算机范式的第 5 次颠覆式创新”以及“人类信用进化史

**收稿日期：**2020−03−20；**修回日期：**2020−04−26
**通信作者：**崔琪楣，cuiqimei@bupt.edu.cn
**基金项目：**国家自然科学基金资助项目（No.61941114，No.61941105）；天津市自然科学基金资助项目（No.19JCYBJC15700）
**Foundation Items:** The National Natural Science Foundation of China (No.61941114, No.61941105), The Tianjin Natural Science Foundation (No.19JCYBJC15700)

上继血亲信用、贵金属信用、央行纸币信用之后的第 4 个里程碑”[2]。截至目前，区块链技术已经经历了以比特币为代表的可编程货币阶段（1.0 阶段）和以以太坊和超级账本为代表的可编程金融阶段（2.0 阶段），正在向可编程社会的 3.0 阶段发展。各个行业都在积极探讨如何利用区块链技术解决目前中心化系统无法解决的问题。

物联网（IoT, Internet of things）系统是联系人与社会、人与自然的媒介，是构建各类智能系统的基础设施，如智能家居、智慧城市等，已经逐步深入到人们生活的方方面面及各个垂直行业[3]。现有系统一般基于云计算系统来汇集IoT设备采集的数据，并基于数据分析结果对 IoT 设备发送控制指令[4]。对于时延敏感的 IoT 应用，可结合边缘计算来降低处理时延[5]，但总体来说还是中心化的数据收集和处理模式。随着各类 IoT 应用的大规模实践，这种中心化的处理方案逐渐显露出一些固有的问题，主要包括单点控制大规模 IoT 节点的巨大成本和容量限制、单个节点被攻击可导致整个系统受到威胁、云端数据可能被篡改或被滥用、用户隐私存在泄露风险等[6]。而区块链技术的兴起为解决上述问题提供了一个具有可行性的方案。

由于 IoT 系统天然的分布式特性和应用场景中天然的多方参与特性，IoT 成为除金融以外区块链技术最热门的应用领域，近年来相关的应用研究和学术成果非常多。但是，由于区块链技术的综合性和复杂性，同时一些商业机构和研究机构从自身利益出发，很多应用示范案例并没有真正体现区块链的核心价值。虽然目前已经有很多综述性文章对区块链在 IoT 方面的应用进行了总结[7-11]，但其通常会汇总上百篇文章的结论，并没有对区块链技术在所述应用中的具体价值做详尽的分析。本文拟弥补这一缺失，通过列举一些典型的“区块链+IoT”应用案例，分析适合区块链应用的典型场景，从而为更好地挖掘区块链在 IoT 方面的创新应用提供思路。

## 2　区块链技术的适用场景和应用逻辑

### 2.1　区块链应用的典型特征

根据文献[12-14]的分析，一个典型的区块链应用应具备以下 5 个特征。

1) 需要不可篡改的数据库

狭义上来看，区块链系统本质上是一个分布式数据库，因此，区块链技术一定是被用来存储数据的。但区别于一般数据库，区块链维护的数据库只能增加条目，而不能删除或者修改已有条目，即这个数据库是不可篡改的，数据的不可篡改是应用区块链的最主要目的。由于所记录的数据都带有提交者的数字签名和时间标签，因此，具备了可追溯特性。

2) 需要多方共享与维护

区块链系统所针对的应用场景一定包含多方参与，共同维护数据库，不仅是多方可读，更重要的是多方可写。在区块链系统中，写区块链数据库的每一方都需要运行一个节点，并保存完整的区块链数据。写数据库的行为是由交易触发的，但产生交易的双方不一定都需要拥有过一个节点。

3) 多方之间缺乏信任

在区块链的应用场景中，区块链的多个维护方之间一定是缺乏信任的。具体包括两层含义：从写数据库的角度看，由于不信任，所以每一方都不愿意其他方修改自己维护的数据库；从读数据库的角度看，每一方都不相信其他方告知的查询结果。这种不信任主要来自于各方利益不同，这个利益可能是经济方面的或者是其他方面的。

4) 没有合适的第三方

对于一般的共享账本来说，解决多方不信任问题的一个方法就是寻找一个多方都信任的第三方，所有数据库的读写都交由这个可信的第三方进行。而区块链的应用场景一定是没有这样一个第三方的情况，通常是商业利益或者政策法规的限制不允许这样的第三方出现。此时，每个区块链参与方都独立地进行交易验证和账本读写。

5) 联系各方的交易

区块链最适用的应用场景一般存在一个特点，即交易产生于维护账本的各方之间，且交易之间存在关联。有了这个特性，一笔交易的验证就以之前相关交易的验证为前提，从而使参与交易的各方利益相互绑定。此时，各参与方才有意愿协作地共同维护这个关乎各方利益的账本。此外，为了使每个节点能够独立地进行交易验证，每个交易的合法性应该是可验证的。

总之，一个合适的区块链应用一定是建立在互不信任的多方之间，在没有可信第三方的情况下，基于相互关联的交易共同构建一个不可篡改的数据库，从而在公开、公平的情况下实现多方共赢，体现为提高效率或降低成本。

### 2.2　区块链技术适用场景的判断条件

迄今为止，区块链最活跃的应用领域仍然是金融，包括基于公有链的比特币、基于联盟链的跨境支付/清算等。在这些应用中，区块链记录的数据就是金融交易，即货币或数字资产的转移。在这种情况下，交易的合法性验证包括支付方的身份和支付方拥有的资产额，交易之间的联系也是天然的。而随着区块链技术在其他领域的广泛应用，链上存储的数据类型逐渐泛化，对数据可验证性的要求变弱。在这种情况下，对于是否使用区块链技术的判断主要基于 2.1 节所述的前 4 个特征，仍需结合具体应用场景设计交易的合法性验证方法，从而最大限度地体现区块链技术的价值。区块链技术适用场景的判断条件如图 1 所示，一个应用需求必须同时满足前 4 个特征才有必要使用区块链技术，否则就应该寻求传统解决方案[13-14]。

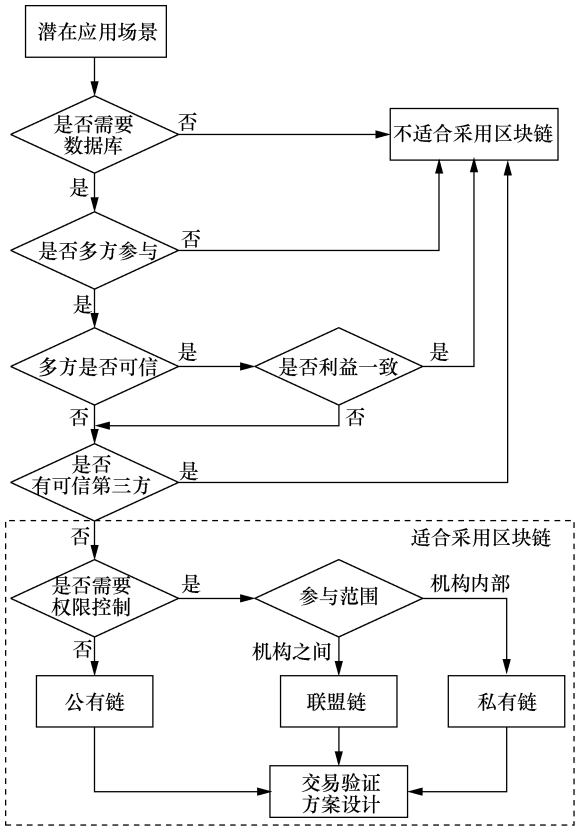



图 1　区块链技术适用场景的判断条件

进一步地，在确定使用区块链之后，还需要根据权限管理需求来决定区块链系统的类型。如果不限制参与节点的读写权限，则采用公有链；如果需要限制读写权限，则使用联盟链或者私有链，前者用于机构之间，后者用于机构内部。而对于后两种区块链系统而言，相关多方一般是有资质的团体，具备一定的可信性，但是由于利益不一致，仍然有破坏账本一致性的可能，因此，区块链才有应用的必要。

从 IoT 系统的角度来看，由于大多数应用在各个垂直行业之间或企业内部，参与各方大多是有资质的组织，且相关数据及交易都不希望对公众开放，因此，一般不采用公有链，而是以联盟链或私有链为主。

## 3　区块链在 IoT 领域的典型应用案例分析

区块链技术在 IoT 系统中的应用通常存在两种形式。一种是结合区块链和 IoT 技术解决某个应用场景中的问题，另一种是利用区块链技术解决 IoT 系统中的自身问题。本节列举 5 个例子（前 3 个例子属于第一种应用类型，后 2 个例子属于第二种应用类型），重点从区块链适用场景的判断条件出发，分析每个场景中区块链的价值。

### 3.1　基于区块链和 IoT 的供应链系统

供应链是指产品经过生产、质量检验、物流、经销商、零售商一直到用户手中的全过程。这个过程包含的环节很多，且各方独立保存各自的数据，信息缺乏透明度。在目前的供应链中，每个交接环节都需要交接双方进行基于文件的确认和审批。这种方式一方面会带来很大的时延，另一方面也面临文件的丢失和被篡改等安全问题。一旦产品在流转过程中出现问题，追责的成本大、时间久。可见，这是典型的多方参与、互不信任、利益不一致的场景，很适合结合区块链和 IoT 技术来解决。

文献[15]介绍了一个危险化学品供应链的案例，基于区块链和 IoT 的危险化学品供应链平台架构如图 2 所示。为了保证货品流转全程透明、可信，构建了一个包括工厂、鉴定部门、海关和物流在内的联盟，多方共建一个分布式数据库。产品在出厂时即绑定唯一数字 ID 和用户采集环境数据的 IoT 设备，同时将产品基本信息存在区块链上，鉴定部门和海关将各自的检验结果存在区块链上。在运输过程中，每个责任单位都将交接信息和货品状态上链，且 IoT 设备自动采集运输环境数据（包括温度、湿度、地理位置、时间等）并上链。最终，采购单位获得物品后可基于唯一数字 ID 查看货品的全流程、多维度数据。

在这个案例中，各方上传的数据合法性可从以下 3 个方面进行验证。1) 货品不可能同时处在多方

手中，具备类似于数字资产的唯一性；2) 每个数据上传都需要对应环节的数字签名，不能伪造；3) IoT 设备采集的数据没有人为参与，比较客观，因此，一些数据（如时间和地理位置信息）可用来参考判断各方上传数据的合法性。

最终，基于区块链和 IoT 技术的结合，这个平台实现了多方数据的透明共享和互信问题，简化了交接环节的程序，降低了相关单位的运营成本和遇到问题时的交涉成本。但需要明确的是，区块链保证上链数据的可靠性，不能解决恶意掉包的问题，这个问题只能通过合理的标签设计与绑定技术来解决。

### 3.2　基于区块链和 IoT 的智能汽车生态系统

近年来，自动驾驶汽车领域发展十分迅速，随着车载智能化的逐步增强和各类传感器装备的不断丰富，在可预期的未来，自动驾驶汽车将具备很强的智能和自维护功能。例如，每辆智能自动驾驶汽车可以根据电量（或汽油）存量自主前往充电桩（或加油站）进行补充；智能自动驾驶汽车可以根据自检系统判断各个部件的健康状况，自动与 4S 店或维修厂预约维修时间，并在指定时间自动前往维修厂。另外，汽车生产商需要时刻监控每台智能自动驾驶汽车的状态，并基于这些信息预测某些部件的故障可能性和运行寿命，从而及时采取应对措施。进一步地，智能自动驾驶汽车可以在车主的授权下自主完成加油、充电和维修的账单支付。可见，围绕智能自动驾驶汽车形成了一个生态链，是一个典型的多方参与场景。由于利益不一致，在智能自动驾驶汽车出现事故的情况下，汽车生产商、车主和维修厂各方可能由于掌握数据不一致而各执一词，没有可信的第三方进行公正的裁决，因此，是一个很好的区块链应用场景。

文献[16]提出了一个基于区块链的未来智能汽车生态系统，基于区块链和 IoT 的智能汽车生态系统架构如图 3 所示。为了能够根据智能汽车自身传感器采集的客观数据自动进行可靠的交互，构建了一个包括智能汽车生产商、经销商、4S 店/维修厂、充电桩/加油站、智能汽车本身、车主以及保险公司等多方在内的联盟链。智能汽车生产商在智能汽车出厂时为智能汽车绑定唯一的数字 ID，并将相关信息上链；智能汽车通过经销商或 4S 店转给车主的同时，转交智能汽车控制权和链上数据读写权；智能汽车自身的传感数据和维修预约交易直接上链；4S 店或维修厂根据链上数据规划维修方案，并将维修过程和结果数据上链；智能汽车自主充电/加油之后，智能汽车和加油站/充电桩各自上传服务过程数据；智能汽车生产商和保险公司通过读取链上数据监控智能车的状态；智能汽车所有自动进行的交互和支付操作都在车主的授权下进行。

在这个案例中，链上存储的交易包括传感数据、服务信息和支付信息，其合法性验证包括：传感数据基于数字签名保证客观性；服务信息基于双方数字签名保证不可伪造，并与传感数据相互印证；支付信息基于账户余额和数字签名保证合法性。

### 3.3　基于区块链和 IoT 的共享经济模式

共享经济主要是在物品的拥有者和使用者之间进行物品使用权的临时转移，是典型的多方参与、点对点应用场景。但是由于物品拥有者和使用者之间通常互不信任，因此，目前主要依托第三方平台完成双方的对接并达成交易。这种方式主要存在两个问题：1) 第三方平台会收取一定费用，增加了租用者的成本；2) 由于第三方平台控制所有数据，可能为了自身利益而篡改物品的相关数据，不

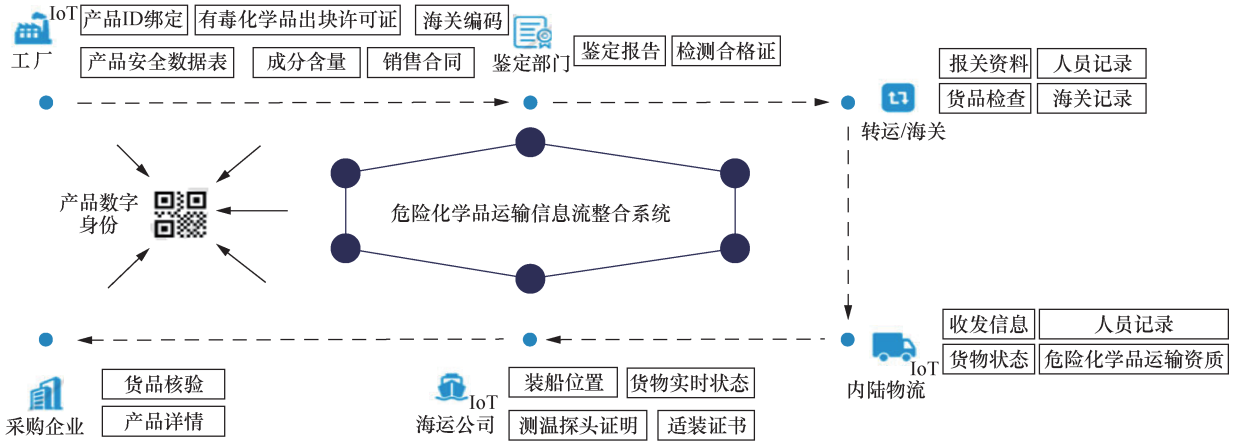



图 2　基于区块链和 IoT 的危险化学品供应链平台架构[15]

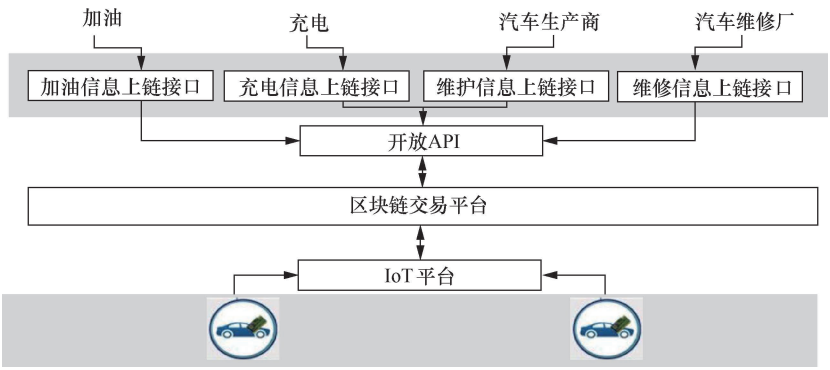



图 3　基于区块链和 IoT 的智能汽车生态系统架构

利于租用者事先掌握物品的真实信息。

为了解决以上问题，可基于区块链技术搭建一个由物品拥有方、平台维护方、政府监管方和保险公司组成的联盟链，并基于 IoT 技术将共享物品与区块链平台连接起来。例如，Slock 公司的 Share & Charge 项目实现了在没有第三方参与的情况下完成充电桩共享[17]。在这个项目中，充电桩将配备 IoT 智能设备，可以与用户手机上的 Share & Charge App 进行交互。在智能合约的控制下，充电桩可以给合法用户充电，并在完成充电后自动完成转账。类似地，该公司开发了房屋共享业务。房间智能锁能够与区块链交互，当用户基于 App 进行房间预约之后，合法用户可通过与智能锁的交互获得解锁密码，与此同时，在链上智能合约账户中锁定一部分代币。当用户完成房屋使用后，智能合约自动将合约账户中的代币转给房主，并将剩余部分返还给租户。

这个案例中的区块链主要保存以下 4 类信息：1) 物品拥有者上传的物品状态数据，通过数字签名验证提交者的合法性；2) 租用者提交的共享申请，通过数字签名验证提交者的合法性；3) IoT 设备上传的物品状态信息和共享双方提供的服务及交易数据，前者可辅助验证后者的合法性；4) 租用者对共享服务的评价数据可与物品拥有者提交的物品状态数据相互印证，有利于租用者掌握真实的物品状态。

### 3.4　基于区块链的健康监护生态系统

随着人们健康意识的不断提升，基于可穿戴设备的健康监护应用得到快速发展。典型的应用场景包括两个步骤：1) 用户佩戴的可穿戴设备实时采集用户的健康数据，并通过 App 将数据提交到云端；2) 应用服务提供方读取云端数据并进行分析，将结果返回给用户，并提出合理建议。这个过程涉及多个利益不一致的相关方，包括云服务方、应用软件开发方、传感器设备提供方和使用者。一旦由于某个环节出现问题导致用户发生意外，则很难进行追责。例如，可能是云服务的时延或者不稳定性导致没有及时预警，可能是云端应用程序出现 bug 导致数据分析错误，或者是使用者没有佩戴好设备导致数据读取错误，也可能是设备本身故障导致数据没有上传。这其中任何一方都不掌握系统的整体情况，因此，很难找到问题的根源。此时只能依托某个第三方进行故障追踪和裁决，但又面临过程不透明、权力滥用以及追责行动不易执行等问题。

为了解决以上问题，文献[18]提出了一个基于区块链的健康监护的生态系统联盟链，维护记账的相关参与方包括云服务方、应用软件开发方、传感器设备提供方和保险公司。各方按照事先协商好的规定上传各自负责部分的状态数据，并将异常事件处理规则和问责流程写入智能合约。该系统利用了区块链的以下特性：1) 各方基于数字签名提交数据，对各方透明，不可抵赖；2) 各方利益不一致，形成互相监督机制，保证数据不可篡改；3) 基于智能合约自动完成异常处理，解决追责不易执行的问题。

这个案例本质上类似于供应链，不同点在于多方共同完成的是健康数据的传递和使用，每一个环节都要交接双方进行确认，形成对数据有效性的验证。

### 3.5　基于区块链的可穿戴设备二手市场

随着可穿戴设备的功能升级和新型设备的更新换代，如何处理原有可穿戴设备成了用户需要考虑的一个重要问题。很多用户的原有设备功能正常，完全可以继续使用，因此，大部分用户希望能够将其转让给其他人，这就形成了一个巨大的二手可穿戴设备交易市场。但这个市场涉及多方的不同利益：首先，用户出售可穿戴设备后担心与该设备

相关的个人数据被滥用；第二，设备生产商需要跟踪设备拥有者的变更情况，从而能够继续在保质期内为用户提供保修服务，并在发现质量问题时及时召回；第三，健康监护应用提供方（通常也是设备销售方）需要跟踪设备拥有者的变更情况，从而能够针对新用户的身体特征提供定制化服务。由于这个过程中涉及用户隐私数据的保护，且需要多个利益方协作完成，并不适用于中心化的处理方式。

为了解决上述问题，文献[19]提出了一个基于超级账本的区块链解决方案，用于 IoT 设备的注册、拥有权的转移及数据使用权的控制。区块链系统的账本存储节点由三方构成，包括 IoT 设备生产商、IoT 设备销售商和政府监管方。首先，设备生产商将所有 IoT 设备的 ID 信息注册在链上，备注设备的状态（合格、有问题等），并出售合格产品。第二，设备销售商可验证链上设备来自可信生产商，并购买状态为合格的设备，此时生产商将设备的拥有者信息更新在链上。在出售商品时，销售商将设备拥有权转移信息上链，并附加价格。第三，用户可以在链上验证设备是否来自可信生产商，并在购买设备后有两个权限：1) 当转售设备时在链上提交拥有权转移信息及价格；2) 允许他人使用数据时，在链上提交授权许可和使用价格。此外，当设备生产商发现设备有潜在问题时，将链上设备状态标记为不可再用，则用户不能再出售设备。最后，政府监管机构有权读取链上的所有数据，从而对设备的流转途径、数据使用情况和销售价格进行全面监管。基于区块链智能合约的可穿戴设备转卖平台如图 4 所示[19]，以上操作流程都被固化在智能合约中，每个交易行为所触发的后续流程将自动在链上完成。

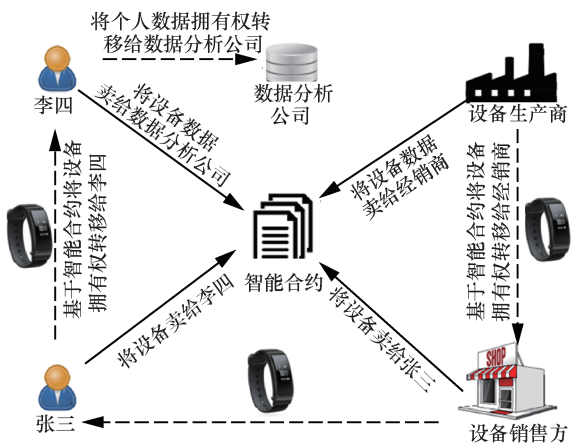



图 4　基于区块链智能合约的可穿戴设备转卖平台

以上方案适用于其他具备用户数据存储功能的设备交易场景，本质上与共享经济案例类似，不同点在于共享的是 IoT 设备本身，而且涉及用户数据的隐私保护。数据的有效性验证依托于设备控制权的唯一性、控制权交出者的数字签名和控制权接收者的公钥地址。

## 4　区块链与 IoT 结合的共性问题

### 4.1　IoT 系统中的信任问题

信任问题是结合区块链与 IoT 技术经常提及的一个方面，当前多数研究通常从两个角度描述该问题：1）IoT 设备可能来自不同厂商，这些设备之间的交互存在不信任问题；2）IoT 设备通常通过中心化的云服务器进行交互，这个云端可能是不可信的，存储于云上的数据有可能被篡改。与所有应用场景一样，区块链在 IoT 系统中的核心价值是保证数据上链之后不被篡改，但是如果原本交互双方不信任对方发送的数据，那么该数据上链之后仍然是不被信任的[20]。因此，区块链技术不能解决 IoT 设备之间的不信任问题。此外，使用区块链系统代替中心化云服务有可能解决 IoT 设备对数据的不信任问题，但前提是系统中的多个参与方选择合理，即没有相同的利益背景，从而能够在维护各自利益的动机下保持数据不被篡改。

### 4.2　身份管理与接入控制

在区块链与 IoT 相结合的文献中，经常提到 IoT 设备的身份管理以及与之相关的接入控制问题。这个问题本质上是对 IoT 设备控制者的信任问题，一般认为只要是可信的拥有者在链上注册了设备 ID 并进行了数字签名，则该设备就是可信的，相应的链上数据读写权限就可以被认定。但是从第 2 节的区块链应用判断条件可知，尽管这个过程中涉及多个 IoT 设备拥有者，但是每一个链上注册的设备 ID 信息与其他设备注册信息之间没有联系。在这种情况下，各方对上链数据只能进行上传者数字签名验证，没有其他合法性验证手段，因此，基于多节点共同维护一个不可篡改的共享数据库的逻辑不够清晰。文献[21]专门讨论了基于区块链的身份管理问题，基本结论是如果只是单方将一个 ID 信息写在链上，那么区块链的意义就不大。但如果多方共同对同一个 ID 的状态进行跟踪，如某个难民的迁移路径，则区块链的溯源作用是有意义的。

### 4.3 IoT 数据的隐私和使用权管理问题

在很多场景中，IoT 系统收集的数据会保护用户的许多隐私信息，如支付细节、个人活动安排、个人生活习惯、个人健康状况等。以往基于中心化云存储的方案存在隐私泄露风险，因此，一些文献提出了基于区块链技术解决这个问题的方案[22-24]，其思路是由用户控制数据的读取权限，任何数据的读取请求都需要在用户允许之后才能进行。基于这种方案，用户可以选择性地将不包含隐私信息的数据暴露给被认证的请求者。但是随着数据挖掘技术的不断进步，数据获得方仍然有可能从中挖掘出用户的隐私信息，且用户无法对数据的后续流转进行控制。因此，最理想的方式是用户在不暴露原始数据的情况下，返回申请者需要的数据处理结果。很多与区块链有关的技术可以实现这个目标，如盲签名、群/环签名、零知识证明、同态加密、安全多方计算等[25-26]，但其中一些技术离大规模应用还有一段距离。

### 4.4 IoT 的数据存储问题

一般基于区块链的 IoT 系统都希望基于区块链技术解决数据可信的问题，但是由于 IoT 系统一般包括大量 IoT 设备，且这些设备可能频繁提交数据，其中一些数据的体量可能很大。在这种情况下，将所有数据都存储在区块链上是不现实的。实际系统中通常会采取折中的办法，即将数据指纹（哈希值）存储在链上，而将数据本身存储在链下。如文献[19, 22]都是将数据存在云端，但这种方案不能保证云端数据不被篡改，只能通过对比原始数据哈希值与链上哈希值来确认数据是否被篡改。为了解决这个问题，文献[27]及区块链数据方案提供商 Datum 提出将原始数据存储在星际文件系统（IPFS, inter-planetary file system）[28]上。IPFS 本身也是一个基于区块链的分布式数据存储系统[29]，可以更好地维护数据的完整性。

## 5 结束语

IoT 是区块链技术应用的一个重要领域，既可以将两个技术结合起来解决其他行业面临的困难，也可以利用区块链技术解决 IoT 系统自身的问题。但一个应用是否真的需要区块链技术，应结合区块链的本质特征和目标应用的核心痛点进行具体分析。本文结合 5 个典型的应用案例深入剖析了区块链能解决哪些问题，以及如何真正地在具体应用中发挥区块链的价值。尽管区块链技术在实际场景中的应用形式可以是多种多样的，现在也没有相关法规和标准来说明怎样的应用可以被称作是基于区块链的，但是只有找到真正适合区块链核心特征的应用才有助于区块链技术的发展，人们所憧憬的可编程社会才有可能真正到来。

## 参考文献：


[1] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[2] 梅兰妮·斯万. 区块链: 新经济蓝图及导读[M]. 北京: 新星出版社, 2016.
MELANIE S. Blockchain: blueprint for a new economy[J]. Beijing: New Star Press, 2016.

[3] 邬贺铨. 物联网技术与应用的新进展[J]. 物联网学报, 2017, 1(1): 1-6.
WU H Q. Technology and application progress on Internet of things[J]. Chinese Journal on Internet of Things, 2017, 1(1): 1-6.

[4] 张琦, 杨浩, Tony Q. S. Quek, 等. 物联网的核心本质——数据联网[J]. 物联网学报, 2018, 1(3): 10-16.
ZHANG Q, YANG H, QUEK TONY Q S, et al. Kernel of Internet of things: Internet of data[J]. Chinese Journal on Internet of Things, 2017, 1(3): 10-16.

[5] 吴大鹏, 张普宁, 王汝言. “端—边—云”协同的智慧物联网[J]. 物联网学报, 2018, 2(3): 21-28.
WU D P, ZHANG P N, WANG R Y. Smart Internet of things aided by “terminal-edge-cloud” cooperation[J]. Chinese Journal on Internet of Things, 2018, 2(3): 21-28.

[6] KSHETRI N. Can blockchain strengthen the Internet of things?[J]. IT Professional, 2017, 19(4): 68-72.

[7] WU M, WANG K, CAI X, et al. A comprehensive survey of blockchain: from theory to IoT applications and beyond[J]. IEEE Internet of Things Journal, 2019, 6(5): 8114-8154.

[8] TIAGO M, FERNÁNDEZ-CARAMÉS, FRAGA-LAMAS P. A review on the use of blockchain for the Internet of things[J]. IEEE Access, 2018, 6: 32979-33001.

[9] DAI H N, ZHENG Z, ZHANG Y. Blockchain for Internet of things: a survey[J]. IEEE Internet of Things Journal, 2019, 6(5): 8076-8094.

[10] FERRAG M A, DERDOUR M, MUKHERJEE M, et al. Blockchain technologies for the Internet of things: research issues and challenges[J]. IEEE Internet of Things Journal, 2019, 6(2): 2188-2204.

[11] 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.

[12] DRESCHER D. Blockchain basics: a non-technical introduction in 25 steps[M]. New York: Springer, 2017.

[13] 中国信息通信研究院. 区块链白皮书(2018)[R]. 2018.
CAICT. Blockchain white paper(2018)[R]. 2018.

[14] CHOWDHURY M J M, COLMAN A, KABIR M A, et al. Blockchain versus database: a critical analysis[C]//2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). IEEE, 2018: 1348-1353.

[15] 可信区块链推进计划项目组. 区块链溯源应用白皮书(1.0 版)[R]. 2018.
Trusted Blockchain Initiatives. Blockchain trace application white paper (V1.0)[R]. 2018.

[16] MILLET D. Blockchain and the Internet of things in the industrial sector[J]. IT Professional, 2018, 20(3): 15-18.

[17] Slock.it Team. Use cases[EB/OL]. 2020.

[18] ALZUBAIDI A, SOLAIMAN E, PATEL P, et al. Blockchain-based SLA management in the context of IoT[J]. IT Professional, 2019, 21(4): 33-40.

[19] YU B, WRIGHT J, NEPAL S, et al. Trust chain: establishing trust in the IoT-based applications ecosystem using blockchain[J]. IEEE Cloud Computing, 2018, 5(4): 12-23.

[20] CAO B, LI Y, ZHANG L, et al. When Internet of things meets blockchain: challenges in distributed consensus[J]. IEEE Network, 2019, 33(6): 133-139.

[21] COOPER A. Does digital identity need blockchain technology?[S]. 2016.

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

[23] OUADDAH A, ABOU ELKALAM A, AIT OUAHMAN A. FairAccess: a new blockchain-based access control framework for the Internet of things[J]. Security and Communication Networks, 2016, 9(18): 5943-5964.

[24] LIANG X, ZHAO J, SHETTY S, et al. Towards data assurance and resilience in IoT using blockchain[C]//MILCOM 2017 IEEE Military Communications Conference (MILCOM). IEEE, 2017: 261-266.

[25] 袁勇, 王飞跃. 区块链理论与方法[M]. 北京: 清华大学出版社, 2019.
YUAN Y, WANG F Y. Blockchain theory and method[M]. Beijing: Tsinghua University Press, 2019.

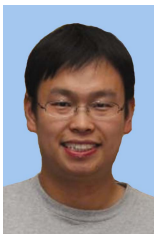
[26] EVANS D, KOLESNIKOV V, ROSULEK M. A pragmatic introduction to secure multi-party computation[M]. Boston: NOW Publisher, 2018.

[27] ALI M S, DOLUI K, ANTONELLI F. IoT data privacy via blockchains and IPFS[C]//Proceedings of the 7th International Conference on the Internet of Things. 2017: 1-7.

[28] HAENNI R. The decentralized data marketplace: datum network white paper[R]. 2017.

[29] BENET J. IPFS-content addressed, versioned, P2P file system (draft 3)[J]. arXiv: 1407.3561, 2014.

[作者简介]



**高镇**（1982– ），男，河北张家口人，博士，天津大学副教授，主要研究方向为容错信号处理与区块链技术优化与应用。

**崔琪楣**（1979– ），女，河南驻马店人，博士，北京邮电大学教授，主要研究方向为移动网络与智能计算、车联网和无线接入安全。

**张雪菲**（1988– ），女，北京人，博士，北京邮电大学讲师，主要研究方向为区块链、移动边缘计算和车联网。

**王晓飞**（1982– ），男，河北保定人，博士，天津大学教授，主要研究方向为移动边缘计算、边缘智能、物联网与智慧城市。