doi :10.3969/j.issn.1671-1122.2017.05.001

区块链技术驱动下的物联网安全研究综述

赵阔，邢永恒

（吉林大学计算机与科学技术学院，吉林长春 130012）

摘　要：物联网作为第三次产业革命和未来社会互联技术发展的新方向，继互联网之后，给人们的生产、生活带来了巨大变革。物联网技术的发展与应用在近几年取得了显著成果，大量传感器和机器设备相连接，并与互联网相结合，实现了智能化的管理与操作。与此同时，物联网的安全隐私问题是物联网技术所面临的威胁之一。由于物联网的拓扑结构以及资源的约束，传统的安全技术并不完全适用于物联网。区块链技术作为当今安全加密货币——比特币——的核心技术，具有去中心化、去信任化和数据加密等特点，尤其适合构建分布式系统。文章通过分析区块链技术特点来解决物联网应用中的安全问题，同时对区块链技术与物联网相结合后的安全性问题做出了探讨。

关键词：区块链；物联网；隐私保护

中图分类号：TP393　　**文献标识码：**A　　**文章编号：**1671-1122（2017）05-0001-06

中文引用格式：赵阔，邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息网络安全，2017（5）：1-6.

英文引用格式：ZHAO Kuo, XING Yongheng. Security Survey of Internet of Things Driven by Block Chain Technology[J]. Netinfo Security,2017(5):1-6.

Security Survey of Internet of Things Driven by Block Chain Technology

ZHAO Kuo, XING Yongheng

(*College of Computer Science and Technology*, *Jilin University*, *Changchun Jilin* 130012,*China*)

Abstract: Nowadays, after the Internet, Internet of Things brings great changes to people's production and life as a new direction of the third industrial revolution and the future internet technology. The development and application of Internet of Things has achieved remarkable results in recent years. A large number of sensors are connected to the machines and are combined with the Internet, which achieves intelligent management and operation. At the same time, the security and privacy problem in the Internet of Things environment is still the one of the threats to the Internet of Things technology. Because of the topology of the Internet of Things as well as the constraint of resources, the traditional security technologies are not entirely applicable to the Internet of Things. As the basic technology of bitcoin, block chain technology has the characteristics of decentralization, detrust, data encryption and so on. It is suitable for building a distributed system. This paper analyzes the characteristics of block chain technology to solve the security problems in the application of Internet of Things, and discusses the security problems of the combination of block chain and Internet of Things.

Key words: block chain; Internet of Things; privacy protection

收稿日期：2017-3-29

基金项目：国家科技支撑项目 [2014BAH02F00]；吉林省青年科学基金 [20160520011JH]；吉林省中青年科技创新领军人才及团队项目 [20170519017JH]

作者简介：赵阔（1977—），男，吉林，副教授，博士，主要研究方向为网络空间安全、大数据处理技术、云计算、物联网；邢永恒（1996—），男，吉林，硕士研究生，主要研究方向为物联网安全。

通信作者：赵阔 zhaokuo@jlu.edu.cn

0 引言

2005 年 11 月，在信息社会世界峰会（WSIS）上，国际电信联盟（ITU）发布了《ITU 互联网报告 2005：物联网》，引入了“物联网”概念。物联网相关应用的迅猛增长，使得对传统行业（如制造业）的需求减少。物联网通过各种有线或无线网络与互联网相融合，实现信息的实时传递。物体通过由 RFID 阅读器组成的接入网与应用服务器通信，为了保证交互是安全和可靠的，阅读器必须是可信节点，即管理员需对与物品标签交互的阅读器动态授权 [1]。随着 RFID 技术逐步发展成熟，以 RFID 设备和移动智能终端为支撑的物联网应用开始产生更具威胁的安全问题。物联网的安全威胁主要来自于应用层、网络层和感知层。图 1 所示为物联网主要层次架构中的应用，图 2 为物联网的主要安全威胁。

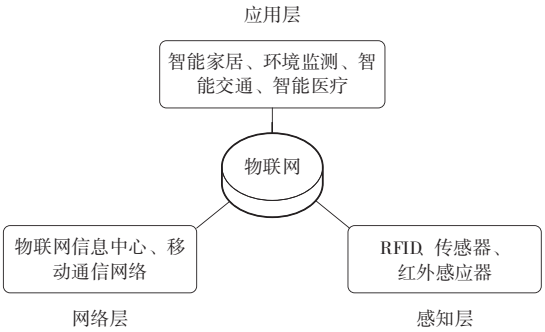

图 1 物联网主要层次架构中的应用

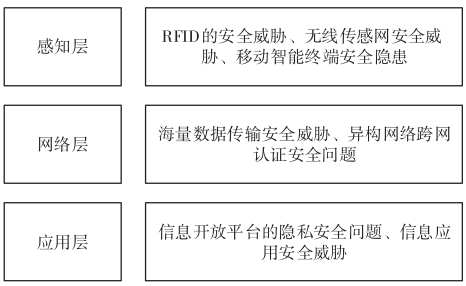

图 2 物联网的主要安全威胁

“区块链”概念是在《2014—2016 全球比特币发展研究报告》中提出的，其本质是一个去中心化的数据库。区块链技术是比特币的底层技术，它将数据信息分布式记录，由所有参与者共同记录。这些数据信息存储在所有节点中，而不是存储在唯一的中心化机构。区块链技术保障了系统对价值转移的活动进行记录、传输和存储，其最后的结果一定是可信的 [2]。区块链的优势是对外公开，每位用户都能看到区块链中的数据记录。

1 物联网发展中存在的主要安全问题

1.1 隐私保护

传统物联网在用户隐私和信息安全传输方面有许多不足 [3,4]：1）标签被嵌入任何物品，用户在没有察觉的情况下个人隐私被暴露；2）射频识别系统对物品进行跟踪，使隐私受到破坏；3）物品的详细信息在本地物品信息服务器（Local Information Server of Things, L-TIS）与远程物品信息服务器（Remote Information Server of Things, R-TIS）间传输，易受流量分析。

传统的信道安全不能满足“一对多”、“多对多”环境下抵抗密钥共享攻击等基于应用的隐私保护的需求 [5]。嵌入 GPS、WiFi 等定位装置的移动智能手机使用户的位置隐私暴露在公共场合中。美国 Sense Network 公司每天处理超过 40 亿条的位置数据，从而提取用户的爱好、习惯等隐私信息 [6]。RFID 装置、红外感应器、移动互联设备、GPS 定位系统能否对用户的隐私数据做到完全保密，这些信息是否被生产厂商所监控，都是物联网安全需要面对的重要问题。

1.2 认证与访问控制

网络中的认证主要有两种，即身份认证和消息认证。身份认证是通过密钥来保证的，如果通信双方中有一方的密钥被盗取，通信双方的会话数据就会被攻击者窃取，造成通信双方的损失。消息认证是发送方和接收方在通信时用来保证信息安全和完整的一种认证方法。物联网中的认证是指发送方和接收方确定通信时的一个消息认证码，发送方根据返回信息的消息认证码确认接收方已接收它发送的消息。但在通信过程中，消息认证码一般是静态数据，攻击者可以通过穷举、数据流监听等方法伪装成接收方来获取发送方所发送的信息，发送方接收到的返回信息的消息认证码也是正确的，这样就会导致物联网中如信息泄露等安全问题。

访问控制是指根据授权策略，控制对一定资源所进行的访问，从而减少非法用户的入侵，保证对资源的合法访问。目前信息系统的访问控制机制主要是基于角色的访问控制机制 (Role-based Access Control，RBAC) 及其扩展模型 [7]。保证访问控制过程中的信息安全是物联网发展中的主要安全问题。

1.3 数据安全

传统的数据库系统处理的是离散数据，物联网中处理的是流式数据。流式数据是实时的、连续的，一旦被攻击，所有流式数据信息都会被窃取。随着大数据和物联网的结合，物联网中海量数据的存储和处理面临巨大的安全挑战[8]。如图 3 所示，物联网是通过传感器来获取数据，通过 MYSQL、ORACLE 等数据库进行存储，其他非结构化数据的存储则通过 HDFS、GFS 云存储等来实现[9]。云存储是目前常用的存储方法，但数据在使用时需要反复传输，导致中央云服务器的负荷极大，且数据的安全性没有得到保证。物联网应用需要考虑数据的安全性和私密性，尤其在物联网的无线传输过程中，要防止数据被非授权用户所使用。

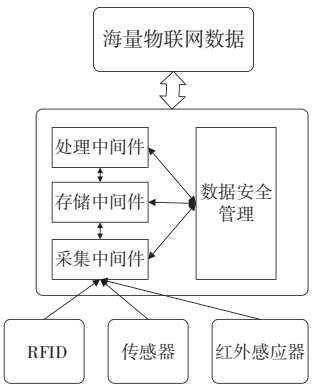

图 3 物联网数据存储和处理结构

2 区块链技术在物联网中应用的特点

当前，物联网需要连接数以亿计的设备，很难保证其设备数据的隐私安全。由于点对点网络下存在较高的网络延迟，当节点数过多时，各个节点在一段时间内所观察到的事务发生先后顺序不可能完全一致，因此需要设计一种机制，对在差不多时间段内发生的事务的先后顺序进行共识。这种用于对一段时间内事务发生的先后顺序达成共识的机制称为共识机制，这种机制使物联网设备之间传递的数据的隐私安全得到保证。区块链的特点能够给物联网安全提供共识机制，使物联网设备之间传递的数据的隐私安全得到保证。区块链共识机制的实现需要以下 5 个特点。

2.1 去中心化

区块链技术的最典型特点是去中心化，也是用在物联网安全中最广泛的特点。在区块链网络中，没有中心化的节点或管理结构，大量节点构成了一个去中心化的网络，如图 4 所示。网络中各项功能的安全维护取决于网络中所有具有安全维护能力的节点。各个节点之间没有管理机制，每个节点之间都是平等的。每个节点都有对完整数据库信息的记录。当一个节点收到另一个节点传来的数据时，该节点会验证另一个节点的身份信息。如果验证成功，就将它所接收到的信息广播到整个网络。

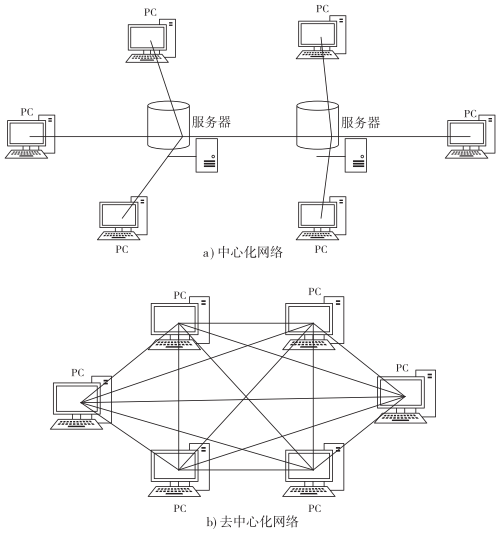

图 4 中心化网络与去中心化网络

区块链网络中数据的验证、存储、维护和传输等过程都是基于分布式系统结构实现的，采用数学方法而不是中心机构建立节点之间的信任[10]，因此区块链技术对于物联网的中心化结构有较好的优化作用。利用区块链去中心化的特点可以改善数据存储中心化、物联网结构中心化的现有状态，减少物联网对中心结构的依赖，防止由于中心结构的损坏导致的整个系统的瘫痪。

2.2 去信任化

由于区块链技术具有去中心化的特点，因此网络中节点之间的数据传输是去信任和开放的。区块链中区块的组成结构如表 1 所示。其中，默克尔（Merkle）树根用来存放区块中所有交易数据的一个统一哈希值；时间戳用来标记区块产生的时间；随机数用来记录解密该区块相关数学题的答案。区块链将所有交易数据存储在它的各个区块中，区块链使用者能够实时获得区块链中的全部数据，使得交易去信任化。区块链去信任化的特点能够用在物联网的互信机制中，使用户之间的交易更加透明化。

表 1 区块的组成结构

区块头	版本号
	父区块哈希值
	默克尔树根
	时间戳
	随机数
	目标阈值
区块内容	交易数量
	交易集合

2.3 时序数据

区块链用时间戳来确认和记录每笔交易，从而给数据增加了时间维度，这样也就可以记录交易的先后顺序，使得数据具有可追溯性。当创世区块建立后，将新生成的交易数据记录到当前区块中，在当前区块中生成此区块所有交易数据的默克尔树。默克尔树根的值被保存到当前区块的区块头中，默克尔树被存储到当前区块的区块内容中。将当前区块的区块头数据通过一定的算法生成一个哈希值，并被加入到当前区块的父区块哈希值属性中，由此类推形成区块链，这个过程是不可逆的。区块链结构如图 5 所示。

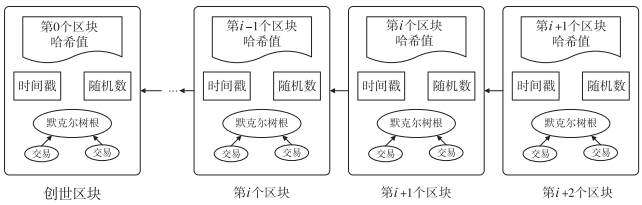

图 5 区块链结构示意图

时间戳方法不仅能保证数据的原始性，也降低了交易追溯的成本。时序数据强化了信息的不可篡改性，对保障物联网中的物品流通安全起到很大的作用。

2.4 数据加密

区块链利用非对称密码学原理对数据加密。非对称密码学在区块链中有两个用途：1）数据加密；2）数字签名[11]。区块链中的数据加密能够保证物联网中交易数据的安全，降低交易数据丢失的风险。在交易过程中，区块链技术采用时间戳机制为每笔交易生成一个 ID，用户可以根据 ID 查询到相应的交易数据。系统将不断生成的交易加入到所有区块中，当新区块生成条件得到所有用户的认证之后，当前区块就被加入到主区块链中，每个区块采用通过一定算法生成的哈希值来标识自身的唯一性。如果攻击者想篡改数据，就必须修改所有区块中的数据，对于一个成熟的区块链来说，这是不可能实现的，由此实现了对交易数据的加密。

交易数据要在网络中传播，还要经过数字签名，以表明签名人的身份以及对这项交易数据内容的认可。在区块链技术中常用的数字签名的典型算法是椭圆曲线数字签名算法（ECDSA）[12]。

2.5 智能合约

“智能合约”这个概念是 Nick Szabo 提出的，他认为智能合约是一套以数字形式定义的承诺[10]。从用户的角度来说，智能合约通常被认为是一个自动担保程序。例如，当特定的条件满足时，智能合约就会自动释放和转移相应的信息。从技术的角度来讲，智能合约被认为是网络服务器，但这些服务器不是架设在互联网上，而是架设在区块链上，从而可以在这些服务器上运行特定的合约程序。CHRISTIDIS 和 DEVETSIKIOTIS 认为通过智能合约能够预测每一个合约的结果[13]。智能合约是一种可编程的合约，能够将人与人之间的合约转化为代码的形式存放在区块链中，并用一个唯一的区块链地址来标记。当合约成立的条件达到时，代码合约就会自动执行。区块链技术给智能合约注入了活力，使智能合约实现了自我管理，甚至可能具有法律效能。智能合约强化了物联网中用户之间的互信机制，能够实现物联网中的去信任化。智能合约实现了最小化信任，已经成为区块链 2.0 的核心技术。

3 区块链技术下的物联网安全

物联网安全面临的最大挑战是当前物联网服务器/客户端模式的生态架构。设备通过中心服务器进行连接识别，显然这种架构模式无法适应当今日益强大的物联网生态系统。区块链技术能够改善物联网安全当前的境况。将区块链技术的特点应用在物联网安全中，能够推动物联网的发展，降低物联网应用的成本。表 2 为采用区块链技术改善物联网相关领域安全的实例，后面分节做了具体分析。

表 2 采用区块链技术改善物联网相关领域安全的实例

物联网相关领域	面临的安全问题	区块链技术对其作用
金融经济	信息伪造、银行信用、骗货挪用、异地监管等	区块链去信任化以及数据加密的特点能够用来改善金融领域的安全问题，实现货运金融一体化等
中介机构	虚假信息、用户隐私安全等	利用区块链中的智能合约实现双方互信，保证用户信息的安全，削弱中介机构的控制
数据存储	存储中心化、数据安全等	利用区块链的去中心化改善大数据存储的中心化现状，利用区块链数据加密技术保证文件安全
公共服务	食品安全、医疗安全、交通拥堵等	利用区块链时序数据标记食品的产地、日期且不可更改；对医疗数据加密，保护用户隐私；利用区块链技术实现交通信息实时共享

3.1 物联网经济的安全保障

区块链技术带动了金融领域的改革，许多金融行业开始研发区块链技术。在 R3CEV 的发起下，目前已有 40 多家跨国银行集团组成区块链联盟，致力于金融领域的区块链技术的应用、开发。货运物联网金融是在货运车联网技术的基础上创新的金融服务 [14]，通过金融卡集成货运车辆运营中的一切商业活动，如加油服务、保险服务等。区块链技术能够提高货运物联网金融的效率，避免冗余的中心化处理过程，实现货运金融快捷安全的交易。

对于用户个人，在物联网环境下，用户可以把物品货币化，分享闲置资源、创造价值。利用区块链技术，用户可以通过一个不可更改的账本来记录共享经济环境下的数据信息，并通过区块链数据加密来保证数据的安全性，从而保护用户隐私。

3.2 物联网环境的弱中介化

随着第四代移动通信技术的普及，用户能够在高速率、高效率的环境下传输大量信息。随着第五代通信技术的应用，越来越多的物联网应用得以实现。目前，如何削弱第三方控制是物联网安全中的一个问题。现在许多交易平台发布虚假信息来诱导用户通过其平台购买商品，在此过程中，第三方的参与不仅增加了用户的成本，还降低了效率。用户之间交流的信息可能被中间机构所监听 [15]。近期，维基解密称，美国能够通过手机和智能电视监控全球，把电子设备及操作系统产品变成麦克风进行窃听。区块链技术能够实现真正的去中介化。区块链技术能够在没有第三方的干预下实现 P2P 的支付，通过其去信任化以及智能合约的特点来保证用户双方的相互信任 [16]。Slock.it[17] 就是一家致力于通过区块链技术实现无中间商交易的公司，让用户之间实现真正的共享经济。

3.3 保证数据存储的隐私安全

当今通过 NFC、RFID、二维码能够获取物品所包含的信息，甚至可以通过智能标签进行交易。区块链的去中心化、数据加密以及每个节点都存储数据的特点使其适用于存储和处理这些隐私数据，并有效防止因中心机构被攻击而导致的数据丢失损坏。例如，政府部门掌握着大量高精度的核心数据，如医疗数据、指纹记录、土地产权、房屋所有权等，区块链通过数据加密技术进行安全保护。此外，数据存储在区块链上，用户能够在不访问原始数据的情况下对数据进行访问，自己管理自己的隐私信息，不再需要担心将信息传递到云服务器中的安全性。因为即使有黑客入侵了服务器，也不会得到用户的信息。用户还可以用区块链指定自己发送到互联网上的文章、视频、音乐等的所有权，从而起到一个版权保护的作用 [18]。

3.4 公共服务安全保障

当前，物联网服务渗透到人们生活的方方面面，物联网服务所产生的数据的安全问题需要一种可靠的机制来保障。目前，区块链对公共服务数据的安全保障可以体现在以下 3 个方面：

1）区块链 + 智能医疗。智能穿戴设备走进了人们的生活。例如，智能手环可以检测用户个人心率、对用户运动计步、监测用户睡眠状况等，这些用户每天的身体状况信息被存储到智能手机中。智能手机等智能设备通过网络把所得到的个人身体状况信息发送到社交圈。在区块链技术下，用户不需担心个人身体状况信息被篡改，用户个人身体状况信息被加密，且能保证信息的正确性。当用户的身体状况信息有了较大波动时，区块链能够保证信息的安全且能分享给医生，医生可以通过这些辅助信息对用户的身体状况做出准确的诊断，提高医治效果。如果用户的个人身体状况信息等能够用于全球科研机构的共同研究，将会给人类带来很大的便利。

2）区块链 + 物联网交通。尽管物联网改善了交通运输领域，但物联网交通仍存在许多问题。例如，通过电子传感技术获得的信息需要通过交通指挥中心共享给用户，从而在信息的传递上产生了延迟，用户无法实时得到数据信息，如果交通指挥中心的数据库被攻击，整个交通系统都会陷入瘫痪。利用区块链的去中心化特点能够实现去中心化的交通网络，且能保障交通网络的安全。物联网交通 [19] 将传感器技术、数据通信技术、人工智能等有效地应用在交通运输方面，再与区块链相结合，形成区块链开放式的分布网络。该网络无需交通中心的指挥调度，每辆车都能够直接接收交通信息、共享交通路况，甚至在自动定位和导航系统的帮助下实现自动驾驶。采用区块链技术也能利用网络追踪智能设备，实现车辆之间的通信。

3）区块链 + 物联网环境下的食品安全。食品安全是人

们越来越关注的话题，将食品安全与物联网相结合能够实现食品的生产过程、运输过程的全程监控。采用区块链技术能保证食品的生产日期等数据的真实性，从而确保食品安全。如果将区块链技术应用到食品的供应过程中，还可以减少食品的浪费。Provenance 是一家英国软件公司，致力于用“区块链 + 物联网”的方式运输农产品食材，采用由传感器或 RFID 生成的标签将食材记录在区块链上，从而保证食材的新鲜性。Filament 是一家无线电感应器生产商，利用感应器检测农作物的健康指数，并把相应的信息记录在区块链上，通过物联网将这些信息传递到物联网中的其他设备上 [20]。

4 结束语

随着物联网和区块链技术的发展以及各行业对物联网的依赖，区块链技术将得到更广泛的应用 [21]。从本文可以看出，区块链对物联网安全的改善十分明显。区块链的去中心化能提供安全的环境，实现真正意义上的分布式系统；去信任化以及智能合约增强了物联网中的互信机制，降低成本；时序数据和数据加密保障了物联网中的数据安全。总之，区块链能够加强物联网应用层、网络层、感知层的安全性。物联网增强了物和物之间的联系，区块链给这种联系提供了安全保障。对于区块链对物联网安全的更多作用，需要未来更深层次的研究与探索。（责编 马珂）

参考文献：

[1] 刘文懋，殷丽华，方滨兴，等 . 物联网环境下的信任机制研究 [J]. 计算机学报 , 2012, 35(5): 846−855.
[2] 林小驰，胡叶倩雯 . 关于区块链技术的研究综述 [J]. 金融市场研究 , 2016 (2): 97−109.
[3] 吴振强，周彦伟，马建峰 . 物联网安全传输模型 [J]. 计算机学报 , 2011, 34(8): 1351−1364.
[4]LUIGI A，ANTONIO I，GIACOMO M. The Internet of Things: A Survey[J]. Computer Networks, 2010, 54(15): 2787−2805.
[5] 董晓蕾 . 物联网隐私保护研究进展 [J]. 计算机研究与发展 , 2015, 52(10): 2341−2352.
[6] 聂金慧，苏红旗 . 物联网位置数据安全策略研究 [J]. 信息网络安全 , 2014(6): 6−10.
[7] 杨庚，许建，陈伟，等 . 物联网安全特征与关键技术 [J]. 南京邮电大学学报（自然科学版）, 2010, 30(4): 20−29.
[8] 张玉婷，严承华，魏玉人 . 基于节点认证的物联网感知层安全性问题研究 [J]. 信息网络安全，2015（11）: 27−32.
[9] 张桂刚，毕娅，李超，等 . 海量物联网数据安全处理模型研究 [J]. 小型微型计算机系统 , 2013, 34(9): 2090−2094.
[10] 袁勇，王飞跃 . 区块链技术发展现状与展望 [J]. 自动化学报 , 2016 (4): 481−494.
[11] 朱岩，甘国华，邓迪，等 . 区块链关键技术中的安全性研究 [J]. 信息安全研究 , 2016 (12): 1090−1097.
[12] ZHENG Zibin，XIE Shaoan，DAI Hongning，et al. Blockchain Challenges and Opportunities: A Survey[EB/OL]. https://www.researchgate.net/publication/310328910_Blockchain_Challenges_and_Opportunities_A_Survey,2017−3−15.
[13]CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access, 2016(4): 2292−2303.
[14] 武晓钊 . 物联网时代的金融服务与创新 [J]. 中国流通经济 , 2013, 27(7): 21−24.
[15] 凤凰资讯 . 维基解密：全球手机成 CIA 窃听器 关机也能录音 [EB/OL]. http: // news. ifeng. com/a/ 20170308 / 50761051_0. shtml, 2017−3−8.
[16]ZHANG Yu, WEN Jiangtao. The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things[J]. Peer−to−Peer Networking and Applications, 2016, 10(4):983−994.
[17] HUCKLE S, BHATTACHARYA R, WHITE M, et al. Internet of Things, Blockchain and Shared Economy Applications [J]. Procedia Computer Science, 2016(98):461−466.
[18] 江瀚 . 区块链，打开物联网的风口 [J]. 金融博览 , 2016(22): 45−47.
[19] 李野，王晶波，董利波，等 . 物联网在智能交通中的应用研究 [J]. 移动通信 , 2010, 34(15): 30−34.
[20] 金评媒 . 区块链将被应用于食材跟踪 保证食材品质 [EB/OL]. http: // www. jpm.cn/article−13731−1. html，2016−8−7 .
[21] 谢辉，王健 . 区块链技术及其应用研究 [J]. 信息网络安全，2016（9）: 192−195.