DOI：10.19729/j.cnki.1009-6868.2018.06.010
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20181106.1020.002.html

区块链：描绘物联网安全新愿景

Blockchain: New Vision for Security of Internet of Things

中图分类号：TN929.5 文献标志码：A 文章编号：1009-6868 (2018) 06-0052-004

摘要： 认为物联网（IoT）安全防护技术是保障IoT快速、健康发展的重要基础。从IoT自身的特征及局限性入手，重点剖析了区块链与IoT两种技术结合的可能性、优势及发展趋势，提出了基于区块链的去中心化IoT安全防护新思路，对其中的基于区块链的IoT系统安全检测、分布式信任机制及隐私保护进行了相关分析与探讨，指出区块链在保证IoT系统安全方面的重要意义。

关键词： 区块链；IoT；安全防护；去中心化管控

Abstract: It is considered that the safety protection technology of Internet of things (IoT) is an important foundation to ensure the rapid and healthy development of IoT. Starting with the characteristics and limitations of IoT, the possibility, advantages and development trends of the combination of the blockchain and IoT are analyzed emphatically. In this paper, a new idea of decentralization of IoT security protection based on blockchain is proposed. The security detection, distributed trust mechanism and privacy protection of IoT system based on blockchain are then analyzed and discussed. The importance of blockchain in ensuring the security of IoT system is finally pointed out.

Key words: blockchain; IoT; security protection; decentralized management and control

徐恪/XU Ke[1]
吴波/WU Bo[1]
沈蒙/SHEN Meng[2]
（1. 清华大学，北京 100084；
2. 北京理工大学，北京 100081）
(1.Tsinghua University, Beijing 100084, China;
2 Beijing Institute of Technology, Beijing 100081, China)

1 物联网技术发展现状与挑战

近年来，以智能家居、智慧城市、车联网等应用场景为代表的物联网（IoT）技术已成为新型动态网络发展的核心技术之一。从美国政府的“智慧地球”，到中国倡导的“感知中国”；从智能设备的快速发展，到网络性能的日益提升，“万物互联”已成为当前不可阻挡的趋势，也展现了IoT在下一代互联网技术发展中举足轻重的地位。

IoT技术的愈发成熟带来用户资源与互联设备数量的爆炸式增长。2017年，IoT设备数量首次超越全球人口总数75亿，而到2020年，这个数量预计将会增长到300亿以上。届时，平均每人将具有4个左右的IoT设备，人们的生活也会朝着便利化、智能化的方向发展。

尽管市场不断扩大、业务不断增长，IoT仍处于技术发展的初期，依旧面临一系列的安全隐患，庞大的数量和自身的脆弱性使得IoT设备极易成为黑客的首选目标。电影《速度与激情8》中数以万计的智能车辆被“天眼”系统恶意操控，进而组成“僵尸车联网”围剿国防部长；再如，2016年下半年，Mirai病毒控制超过30多万台的IoT设备对Dyn公司、OVH公司发动大规模分布式拒绝服务（DDoS）攻击，致使164个国家或地区受到影响。因此，IoT产业化的日益加速与技术的安全可信之间的矛盾成为该领域急需解决的重要问题，也是推动新型IoT技术发展的重要因素之一。

为解系统面临的安全威胁，提升生态系统的安全可信，当前的IoT技术面临着诸多安全挑战，但归根结底是以下2方面的特性所致：

（1）设备数量庞大的分布式系统。IoT系统由多种感知设备（如传感器、射频识别（RFID）等）通过网络相互连接而成。不同于当前的互联网结构，IoT包含数以亿计的网络节点，庞大的设备数量增加了安全检测的难度；不同于软件定义网络（SDN）的架构，IoT实际上是一种大型的分布式系统，去中心化的网络特征增加了IoT集中式安全管控的难度。

（2）IoT设备自身的资源受限。IoT节点主要由一些嵌入式的传感设备组成，这类设备的计算能力、存储空间和通信效率极其有限。由于这

收稿日期：2018-10-16
网络出版日期：2018-11-06
基金项目：国家重点研发计划（2018YFB0803405）、国家杰出青年科学基金（61825204）、国家自然科学基金（61472212，61602039）、欧盟CROWN基金（FP7-PEOPLE-2013-IRSES-610524）

种限制，当前互联网的诸多安全解决方案（例如：漏洞检测、流量审计、访问控制等）不能很好地迁移到IoT系统中，导致IoT设备在面对形如Mirai病毒时却无能为力，这种因设备资源受限而导致安全检测能力的降低（甚至丧失）给IoT系统的安全造成了严重的威胁。

2 基于区块链的安全防护新思路

2.1 区块链技术概述

近几年，以比特币为代表的数字货币成为众多投资者趋之若鹜的对象，它最早起源于中本聪2008年发表的一篇名为《比特币：一种点对点的电子现金系统》[1]的论文。比特币共有2 400万个，当前已经挖出超过1 700万，预计在2040年剩余的比特币将全部挖光。2017年12月，比特币价格接近20 000美元，足见其火爆程度。姑且不谈比特币是否真的具有价值，但其核心技术——区块链已经吸引了互联网、金融界足够多的眼球。简单来说，比特币是区块链的成功产物，区块链是比特币的底层技术，两者相辅相成。

从技术核心来看，区块链是一种基于密码学原理的分布式共识账本技术[2]。从组成结构来看，区块链是由一个个区块依次连接而成，而每个区块中包含多个以默克尔树的形式组织的交易记录。严格意义上讲，区块链并不是一项新的技术，而是现有多种技术的融合。就密码学而言，区块链使用了基于SHA-256和RIPEMD-160的哈希算法、基于椭圆曲线加密的密钥生成算法和非对称加密算法；就分布式结构而言，区块链使用了基于P2P网络的通信机制与验证方式；就共识账本而言，区块链使用了基于工作量证明（PoW）、权益证明（PoS）和股份授权证明（DPoS）等共识算法的分布式存储机制。从安全角度来讲，区块链利用去中心化的点对点（P2P）技术实现分布式共识机制，完全摆脱了传统的集中处理方式，在保证共识机制的同时，将系统的安全性提升到新的层次。

2.2 区块链与IoT结合的优势

区块链能够很好地弥补当前IoT技术在安全领域方面的缺陷，为IoT技术提供底层安全防护，推动其设备、系统和生态朝着更加安全可信的方向发展；而IoT同样能够为区块链技术的升级提供动力，使区块链能够为更多的应用场景提供安全验证与防护，如图1所示。

首先，区块链的去中心化特性与IoT的分布式结构能够较好地融合。区块链系统是一种完全的去中心化结构，不依赖于任何形式的集中式管控，这恰恰与当前IoT系统的分布式架构具有较高的契合度。基于区块链的IoT技术不仅能够依靠共识机制实现对IoT设备的分布式管控，同时还可以使用智能合约技术实现对相关感知信息的自动反馈。

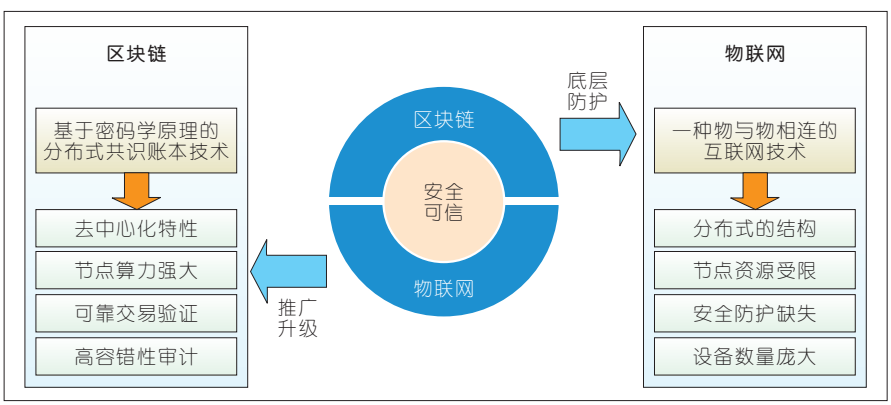
其次，区块链强大的节点算力能够较好地弥补IoT设备的资源受限。当前区块链矿工节点具有较强的算力，以比特币系统为例，目前的总算力已经超过5 500万TH/s。区块链技术能够为IoT提供较强的算力支持，设备的资源受限不再是制约IoT技术发展的关键因素，依托算力支持的安全验证等技术会进一步推动新型IoT技术朝着更加安全可信的方向发展。

再次，区块链可保证智能IoT交易的安全可信。随着人工智能领域的异军突起，IoT技术也朝着智能化的方向发展，智能化设备将满足更加人性化的需求，而价值互连与智能传输将会成为新型IoT技术的一大特色。基于区块链的去中心IoT安全增强技术将极大程度地保障智能设备间交易的安全性，防范双花攻击与恶意欺诈，推动IoT智能经济的健康稳定发展。

最后，基于区块链的去中心化安全基础设施能够对庞大数量的IoT设备进行安全审计与验证。区块链可以作为去中心化的安全基础设施为新型IoT技术的发展提供真实可信的安全保障，基于区块链的IoT技术具有较强的容错性，保证只有少数设备发生故障或被恶意控制时依然保持健壮性。去中心化的安全基础设施能够对数以亿计的IoT设备进行安全验证与审计，有利于增强IoT系统抵御攻击的能力，提升生态安全性。

在未来几年，IoT的规模将变得更加庞大，设备也会变得更加智能化、人性化和多元化；同时，安全性与隐私性也会逐渐成为IoT用户的迫切需求。如何提升IoT设备抵御恶意攻击的能力，如何保证IoT用户的隐私不受侵害，如何增强IoT生态中智能化交易的安全性等都成为新型IoT技术需要解决的难题。

区块链的去中心化特征与内生的安全防护属性能够很好地弥补当



▲图1 区块链与物联网技术

前IoT技术的缺陷，有助于推动新型IoT安全增强技术的发展。一方面，基于区块链的去中心化安全基础设施可以增强对IoT系统的安全监测控制能力，提升系统的对恶意行为的抵抗力，保障系统的安全可信；另一方面，基于共识机制的分布式管控可以保证IoT策略与行为验证的一致性，提升系统的容错力，保障系统的健壮性。由此可见：IoT与区块链技术的融合将会是未来发展的一种趋势。

3 基于区块链的去中心化IoT安全防护系统

区块链技术可以为IoT提供较强的安全防护。首先，区块链内生的激励机制可以吸引更多的安全服务商加入到IoT系统的检测中来，有利于形成更加系统权威的检测报告；其次，区块链衍生的大规模去中心化系统可以为IoT提供分布式信任机制，保障IoT跨域互联互通的安全性；最后，区块链自身的隐私防护特性可使得IoT智能交易更具匿名性，有效地保护用户的隐私信息不受侵害。

3.1 基于区块链的IoT系统安全检测

当前IoT系统面临较大的安全威胁，其主要原因在于IoT设备中的高危漏洞。而设备旧化、系统防护较弱、安全设计缺失等问题都是众多安全漏洞频现的原因，这导致IoT系统在面对网络攻击时表现得不堪一击。针对上述问题，多数IoT厂商通过修复漏洞、更新版本的方式来提升系统的安全可信，但这也引入了2个问题：系统版本的更新可能引入新的未知漏洞；集中式的安全厂商由于检测能力的差异并不一定能发现所有的漏洞[3]。

如图2所示，基于区块链的IoT系统安全检测技术可实现以下几方面的优势：(1)通过创建激励机制可吸引众多检测者参与到IoT系统的检测中来，基于多方协同检测的安全增强技术可以较为容易地获得完整、全面的检测结果；(2)通过创建惩罚机制可进一步约束IoT厂商的行为，恶意系统的发布会致使相关厂商受到相应的制裁；(3)通过创建公开透明的检测结果账本可较好地指引IoT设备对系统安装的选择，安全级别更高的系统更容易得到普及。这样，IoT系统中出现漏洞的概率大大减小，也有利于创建更加安全可信的IoT生态系统。

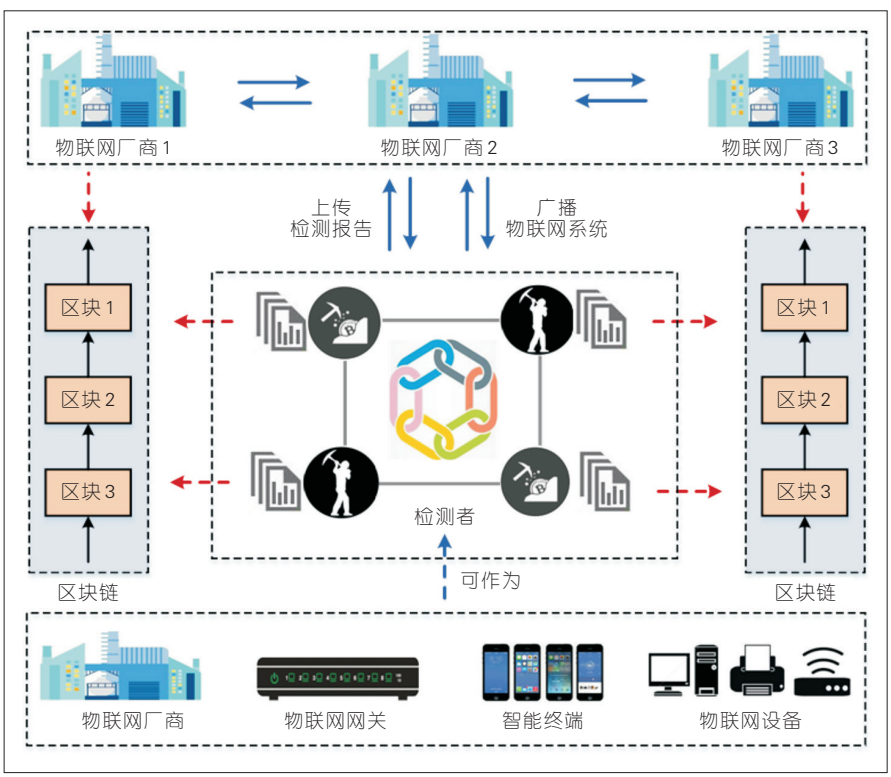
3.2 基于区块链的IoT分布式信任机制

当前IoT系统普遍存在多个管理域，如智慧小区、智慧学校、智慧医院等，出于安全考虑，不同管理域之间是彼此“绝缘”的，如何实现IoT跨域的互联互通及相关安全协议的研究成为新型IoT安全增强技术的重要目标之一。

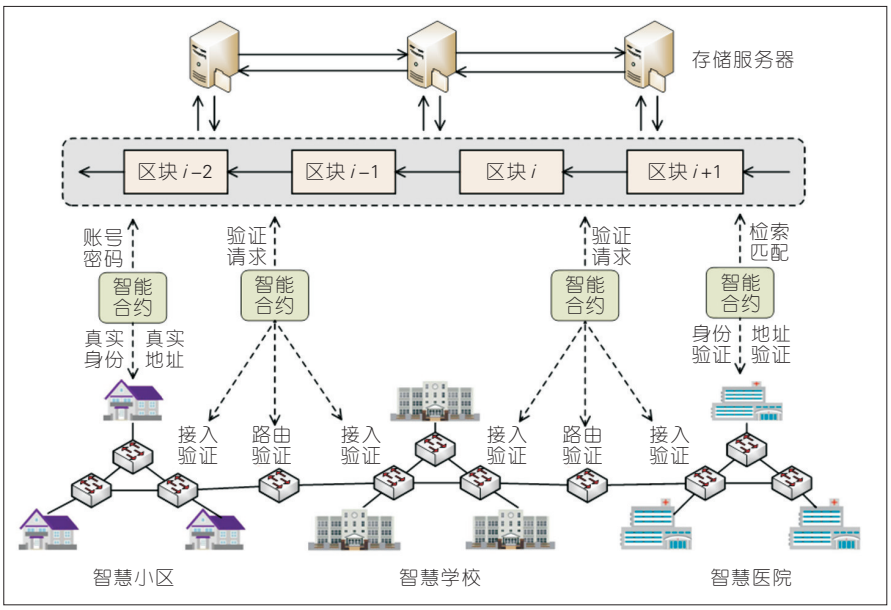
IoT更高级别的安全防护都是以密码学为基础的，而当前安全密钥的创建与分发都是过度依赖集中式的基础设施，而这类设施极易成为黑客攻击的首选目标，成为威胁IoT系统安全的重要因素。基于区块链的去中心化密钥基础设施可以更好地保障系统密钥的安全，为IoT密钥的创建、管理和分发提供鲁棒性更强、容错率更高的安全保障。

真实身份与真实地址是实现IoT互联互通的关键因素，而当前身份伪造、地址哄骗等都是造成信息泄露、隐私窃取的重要原因。如图3所示，针对IoT的大规模分布式异构问题，基于区块链的去中心化真实身份与真实地址生成与验证技术可以有效地保证IoT设备的真实性，有利于防止跨域用户的越权访问，降低数据隐私泄露的风险，也为IoT互联互通提供重要的安全保障。

IoT系统策略的安全性是保障其正确运行的重要基础，也是各类IoT设备行为一致性验证的重要前提，而基于SDN架构的安全策略分发已不再适应日益扩大的IoT规模。相比较而言，基于区块链的IoT去中心化安全管控不仅能够实现庞大IoT设备数量下安全策略的分发，更能为异构



▲图2 基于区块链的物联网系统安全验证技术



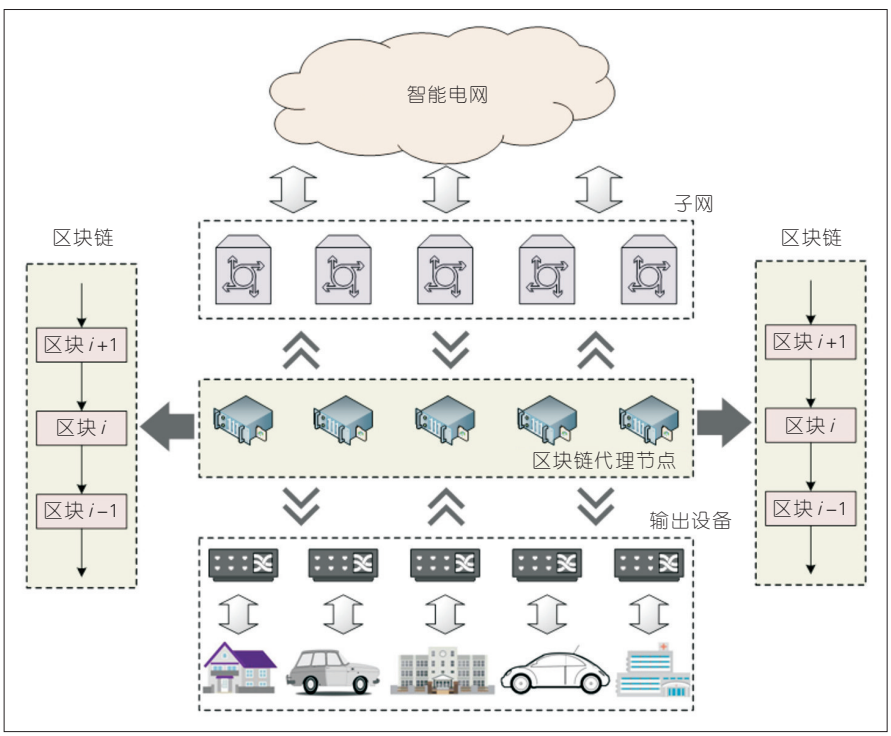
▲图3 基于区块链的去中心化信任机制

IoT系统提供较高的容错性，是新型IoT技术发展的一个很好趋势。

3.3 基于区块链的IoT匿名支付隐私保护方案

IoT的智能化趋势势必会带来频繁的交易行为，而基于这类交易的隐私泄露也给IoT用户带来一定的安全隐患[3]。以智慧小区为例，供电公司可以轻易地获取每个家庭的用电记录，进而推测出业主的用电规律、用电行为等隐私信息；再如，车联网中电动汽车的充电记录也会暴露车主的驾车习惯、行车轨迹等私密信息。仔细分析不难发现，隐藏交易记录是不现实的，因为供电机构无法确认应该给哪个家庭或电车供电；所以，最有效的方式应该是隐藏用户的身份标识信息。借助区块链技术的节点标识策略，基于区块链的IoT匿名支付方案将有利于防止各类交易信息中用户隐私的泄露，将IoT的安全防护提升至一个新的台阶。

为了实现上述的IoT匿名支付方案，可在IoT支付双方（即供给方与需求方）之间引入区块链代理节点。以智能电网供需电为例，如图4所示，无论是家庭业主还是电动车车主，都具备独一无二的加密身份标识，而该标识不能反映其他信息。当业主或车主向智能电网购买电力资源时，双方的交易信息通过区块链代理节点进行确认。在此期间，智能电网无法识别业主或车主的身份，因为它只需向对应的电力输出设备供电即可。



▲图4 基于区块链的物联网匿名支付方案

在这种情况下，IoT用户的身份信息、用电规律、驾车习惯等隐私在没有暴露给智能电网的同时，仍然有效地获取了电力资源。

4 区块链与IoT技术融合的挑战与趋势

虽然IoT与区块链技术在各自的领域已经得到快速发展，但2种技术的融合仍然面临很多的挑战，总结起来主要有以下几个方面：

（1）效率问题。基于区块链的新型IoT安全增强技术主要依赖区块链作为分布式账本来存储各类IoT信息，而区块时间和共识效率将会是制约数据存储、安全验证、信息获取等的效率的关键因素。

（2）存储问题。以比特币为例，当前矿工针对交易记录的存储已经达到100 G以上，而拥有大量设备的IoT势必需要更多的存储空间才能容纳各类交易记录、验证结果等信息。

（3）资源浪费问题。仅就比特币、以太坊而言，每年挖矿所消耗的

➡下转第64页

BGP的域间二维路由的设计方案，域间二维路由在进行路由决策的时候同时考虑目的地址和源地址，实现了灵活的流量控制，能够满足用户的多样化需求。本文中我们设计了域间二维路由协议的控制层，使用MP-BGP的可选属性携带二维路由的配置信息，同时兼容传统路由协议，方便ISP进行增量部署。我们还给出了适用于域间二维路由的数据层设计，使用前人提出的FISE转发表结构，可以解决二维转发表造成的TCAM空间爆炸的问题。整体而言，域间二维路由是一种新型路由方式，灵活和细粒度的流量控制使得其具有很好的应用前景。

参考文献
[1] Framework for Multi-Protocol Label Switching (MPLS)- Based Recovery: RFC 3469[S]. IETF, 2003
[2] McKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow [J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74. DOI:10.1145/1355734.1355746
[3] RUCHANSKY N, PRPSERPIO D. A (not) NICE Way to Verify the Openflow Switch Specification [C]// ACM SIGCOMM 2013, ACM Special Interest Group on Data Communication 2013. China: ACM, 2013. DOI:10.1145/2486001.249171
[4] VISSICCHIO S, TILMANS O, VANBEVER L, et al. Central Control over Distributed Routing [J]. ACM SIGCOMM CCR, 2015, 45 (4): 43-56
[5] A Border Gateway Protocol 4 (BGP-4): RFC1771[S]. IETF, 2005
[6] Multiprotocol Extensions for BGP-4: RFC4760[S]. IETF, 2007
[7] XIAO L, WANG J, NAHRSTEDT K. Optimizing IBGP route reflection network [C]// IEEE ICC 2003, IEEE International Conference on Communications 2003. USA: IEEE, 2003: 1765-1769. DOI: 10.1109/ICC.2003.1203903
[8] SMIRNOV A. Draft-Ietf-Rtgwg-Dst-Src-Routing-06[R].Internet Draft, 2017
[9] YANG S, XU M W, WANG D, et al. Scalable forwarding Tables for Supporting Flexible Policies in Enterprise Networks[C]//IEEE INFOCOM 2014, IEEE Conference on Computer Communications, 2014. USA: IEEE, 2014: 208-216. DOI:10.1109/INFOCOM.2014.6847941

作者简介

耿男，清华大学计算机系在读博士生；主要研究方向为流量工程、二维路由、路由协议等。

金飞蔡，电子科技大学计算机学院在读硕士生；现任中兴通讯股份有限公司承载网产品线平台系统部项目经理；主持研究了“863”计划项目，国家重点研发计划和省重点研究项目4项；发表专利10余篇。

徐明伟，清华大学教授、博士生导师；主要研究方向为互联网体系结构、互联网路由、高性能路由器、网络安全等。

上接第55页

电力远远超过全球一些小国家（如约旦等）一年的用电量，相比于IoT设备的低耗能，区块链技术带来的安全防护可能远远小于它的资源浪费。

（4）跨链访问问题。可以预见，未来将会有更多的基于区块链的IoT平台出现，如基于区块链的车联网平台和基于区块链的智慧小区，而如何保证不同区块链平台的互通/互操作将会是促进区块链快速部署的重要条件。

（5）区块链自身的安全问题。区块链在为IoT提供安全防护的同时，自身也面临着一些安全威胁，如eclipse攻击、路由劫持攻击、51%攻击、智能合约漏洞等，这同样为2种技术的融合带来一定的安全隐患。

未来，区块链与IoT这2种技术将进一步融合，面向IoT安全的区块链技术也将逐渐兴起。共识效率更高、存储空间更小、绿色环保的安全区块链技术更能适应新型IoT技术的需求；而容错率高、鲁棒性强、去中心化的IoT安全管控势必会推进区块链应用技术的发展。

5 结束语

基于区块链的新型IoT技术还处在“萌芽”阶段，对学术界与工业界来说既是机遇又是挑战。区块链与IoT两种技术的融合势必会推动IoT安全的迅猛发展，并由此带来技术的巨大升级。研究适合IoT特征的区块链安全防护技术是未来的一种趋势，但也存在各种挑战而任重道远。

参考文献
[1] NAKAMOTO S. A Peer-to-Peer Electronic Cash System[EB/OL].(2008-10-31)[2018-10-16].https://nakamotoinstitute.org/bitcoin/
[2] 徐恪,李沁.算法统治世界[M]. 北京:清华大学出版社, 2017
[3] WU B, LI Q, XU K, et al. SmartRetro: Blockchain-Based Incentives for Distributed IoT Retrospective Detection[C]//IEEE MASS 2018. USA:IEEE, 2018
[4] GAO F, ZHU L, SHEN M, et al. A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks [EB/OL].(2018-07-04)[2018-10-16]. http://www.x-mol.com/paper/635775

作者简介

徐恪，清华大学教授、博士生导师、计算机系副主任，国家杰出青年科学基金获得者，中国计算机学会理事；主要从事计算机体系结构、网络空间安全和网络经济学等方面的研究；获国家技术发明二等奖1次、国家科技进步二等奖1次、中国电子学会电子信息科学技术奖一等奖1次，其他省部级一等奖3次等；发表论文20余篇，完成著作6本，获得中国发明专利20余项，美国发明专利授权8项。

吴波，清华大学在读博士研究生；主要研究方向为网络体系结构、网络安全和区块链等；发表论文6篇，获中国发明专利5项，参与制定中国通信行业标准3项。

沈蒙，北京理工大学副教授、硕士生导师，并担任多本国际期刊的审稿人，以及IEEE ICC、IEEE Globecom等国际会议的程序委员会委员；主要研究领域为区块链与数据隐私保护；已发表论文30余篇，获得中国发明专利授权12项，美国发明专利授权2项。