专题：区块链技术及其物联网应用

策划人简介

刘建伟

北京航空航天大学教授、博士生导师，网络空间安全学院院长、党委书记，中国密码学会理事，教育部高等学校信息安全专业教学指导委员会委员；长期从事网络安全、密码学的教学和科研工作；享受中华人民共和国国务院政府特殊津贴，科研成果分别获得国家技术发明一等奖、国防技术发明一等奖、山东省计算机应用新成果二等奖、山东省科技进步三等奖，2015年分别荣获北京教学名师奖、北航教学名师奖，2016年荣获中国互联网发展基金会网络安全优秀教师奖，2017年荣获北京市优秀教师奖、北京市教学成果二等奖等；发表SCI/EI收录论文200余篇，出版教材5部、译著1部，获授权发明专利46项，软件著作权登记3项。

内容导读

作为现代密码学、分布式计算、共识机制等技术的综合应用，区块链技术逐渐受到了社会各界的广泛关注。区块链技术具有去中心化、开放透明、信息不可篡改、隐私保护等特点，在数字经济、电子商务、身份认证、社交通信、物联网（IoT）、数据存证、食品安全等诸多领域有着良好的应用前景。区块链技术由此逐渐成为计算机科学领域的一项新兴热点技术。

快速发展的区块链技术也面临着巨大的挑战。首先，区块链作为分布式系统，需要花费一定的计算和通信资源来达成共识，严重制约了区块链的运行效率。虽然通过改进共识算法，区块链的处理能力从比特币每秒处理7次交易，提升到以太坊每秒处理20次交易，乃至到Omniledger每秒处理上千次交易；然而与当前主流支付系统如VISA、支付宝和银联等的交易吞吐率相比，现有的区块链方案还远远达不到日常的使用需求。其次，区块链在提供安全特性的同时，自身也存在着安全问题。据Carbon Black的调查数据，仅2018年上半年，有价值约11亿美元的数字加密货币被盗。如何更好地利用区块链技术服务实体经济，将区块链技术发展与国家信息科技发展结合起来依然是一个亟需解决的重要课题。

本期专题就区块链的技术原理、发展现状和趋势、关键技术和IoT应用展开讨论。在区块链的基础原理方面，《比特币生成原理及其特点》介绍了区块链最初的应用——比特币的生成原理和特色，简要讨论目前区块链技术存在的缺陷；《区块链共识机制研究：典型方案对比》主要介绍了区块链的核心共识算法的主要技术路线和当前的研究现状，分析了每一类共识机制的优缺点。在区块链中的安全风险方面，《区块链共识机制发展与安全性》着重对共识机制中存在的攻击威胁和防范策略进行解析；《区块链概念剖析及其在物联网中的部分应用》分析了IoT场景下几个典型的区块链项目，并对其中的主要问题和主要方法进行了分析，并指出IoT的数据体量和数据安全问题依旧需要重点考虑。在区块链的应用研究方面，《基于区块链的物联网密钥协商协议》提出使用基于身份的Schnorr签名替换原有的椭圆曲线数字签名算法（ECDSA）签名，实现IoT设备间轻量级的身份认证；《区块链技术在物联网中的身份认证研究》提出了应用于体域网身份认证的区块链系统框架，探讨了在IoT平台中区块链技术可能存在的问题和未来发展方向；《基于区块链的电子数据存证的设计与实现》介绍一种基于区块链的电子数据存证系统，致力于解决电子数据存证存在的安全问题；《一种基于区块链的身份识别技术》基于以太坊的智能合约技术提出一种新型身份识别系统，具有高拓展性、高可靠性、高安全性的特点，支持不同平台进行统一的身份认证。本期专题论文来自北京航空航天大学、人民大学、复旦大学、武汉大学、中山大学、南京信息工程大学、南京邮电大学、桂林电子科技大学等中国知名高校的区块链研究专家学者，凝聚了他们的研究成果和工作经验，希望能给读者提供有益的启示和参考。在此，对各位作者的大力支持表示衷心感谢。

刘建伟

2018年11月20日