专题：网络空间安全

基于区块链的网络安全技术综述

陈烨，许冬瑾，肖亮
（厦门大学信息科学与技术学院，福建 厦门 361005）

摘　要：随着移动互联网与物联网技术的发展，网络空间承载了海量数据，必须保证其安全性和隐私性。基于区块链的网络安全机制具有去中心化、不可篡改、可追溯、高可信和高可用的特性，有利于提升网络安全性。探讨了区块链在网络安全方面的应用方案，分析了基于区块链的网络安全机制的主要技术特点和方法以及未来研究方向。首先探讨了数据管理体系应用区块链进行数据管理的方法，利用区块链不可篡改的特性提高数据的真实性和可靠性。其次分析了物联网应用区块链进行设备管理的方案，通过区块链记录和执行设备控制指令，强化物联网设备权限和通信管理。最后研究了域名系统应用区块链的部署方案，利用区块链的去中心化结构抵抗针对中心节点的分布式拒绝服务攻击。

关键词：网络安全；隐私；区块链
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2018135

Survey on network security based on blockchain

CHEN Ye, XU Dongjin, XIAO Liang
Department of Communication Engineering, Xiamen University, Xiamen 361005, China

Abstract: With the development of the mobile internet and IoT (internet of things), mass data are stored in the cyberspace. The network security and privacy are of great significance. The blockchain-based network security mechanism has the properties of decentralization, tamper-resistance, traceability, high availability and credibility, and can be applied to improve network security. The application of blockchain in the network security was explored. The main technologies and the future research direction of the blockchain-based network security mechanism were analyzed. Firstly, the blockchain-based data protection scheme was analyzed, which applied the tamper-resistance of the blockchain to improve the authenticity and reliability of data. Secondly, the blockchain-based IoT device management scheme was analyzed, which applied the blockchain to record and execute the device control instruction and improve the authority and communication of the IoT devices. Lastly, the blockchain-based domain name system was analyzed, which applied the decentralization of the blockchain to resist distributed denial of service effectively.

Key words: network security, privacy, blockchain

收稿日期：2017−12−01；**修回日期**：2018−03−01
基金项目：国家自然科学基金资助项目（No.61671396）；东南大学移动通信国家重点实验室开放基金资助项目（No.2018D08）；佛山市科技创新项目（No.2015IT100095）
Foundation Items: The National Natural Science Foundation of China (No.61671396), Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (No.2018D08), Science and Technology Innovation Project of Foshan City (No.2015IT100095)

1　引言

随着互联网与物联网技术的发展，部分应用程序为了向用户提供更精准的服务，需要采集各种用户数据[1]。海量数据呈碎片化，由不同服务提供商的数据中心进行管理。例如公民医疗信息和存储于电子设备的数据，隐私程度较高，总量庞大且碎片化。传统的数据存储和控制管理通常依赖于可信任的中央机构，中心节点的管理缺陷或遭到攻击可能导致隐私数据泄露甚至网络瘫痪[2-4]。因此去中心化的系统结构能够消除中心节点的安全风险。网络安全可以采用区块链（blockchain）技术，建立一个去中心化的、由各节点共同参与运行的分布式系统架构进行数据的管理，避免中心节点故障引起的网络安全事故[5]。

区块链是比特币（Bitcoin）的底层技术[6]。2013 年 12 月，以太坊的创始人 Vitalik Buterin 提出以太坊区块链平台，将智能合约（smart contract）应用到了区块链，使区块链在数字货币交易之外的领域发挥作用[7]。区块链不依赖可信任的中心节点进行信息的存储和更新，而是由系统中的所有用户各自保存一个“账本”，同时进行账本的记录和更新。因此区块链的结构和特点为其带来了不可篡改、可追溯、高可信和高可用的特性[8]，并开始应用于网络安全领域，见表 1。本文从数据管理和隐私保护、物联网设备的权限和通信管理、抵抗 DDoS（distributed denial of service，分布式拒绝服务）攻击的 3 个方面，介绍区块链技术在安全领域的应用。

传统的中心节点数据管理体系中，数据存储于中央机构，中央机构的管理缺失或设备故障可能造成数据的丢失或泄露[9]。基于区块链的数据管理体系采用去中心化的系统结构，并且将数据与数据存取权限分离。基于区块链的系统消除了中央机构存在的安全风险，同时应用程序对数据的一切操作过程均被记录，确保了数据的安全性[18]。

传统的物联网设备管理系统采用中心化结构，设备的数据和控制信息都由中心节点控制和维护，增加了中心节点的计算负载和安全问题[14,15]。引入区块链，能够构建去中心化的物联网设备管理系统，进行设备的权限设置与通信控制。管理系统在区块链的记录之下，能够确保设备的权限与控制记录的完整和不可篡改[16,19]。

DDoS 攻击者通过一系列手段，向目标系统的中心节点发起大量请求，造成目标节点或网络的瘫痪[20,21]。基于区块链的系统能够将系统数据分布完整存储于多台设备。部分节点遭到攻击时，其余节点依然可以依靠完整的系统数据维持系统

表 1　基于区块链的安全领域相关工作概述

应用类型	相关工作	技术概述	性能优势
网络数据安全和隐私保护	移动平台上基于区块链的应用程序数据管理系统[9]	数据与权限分离，权限设置与数据访问情况记录于区块链	数据访问权限完全可控，数据操作过程对用户透明
	基于区块链与智能合约的医疗信息管理体系 MedRec[10,11]	数据权限与操作记录于区块链，由智能合约完成指令的执行	跨提供商整合完整的医疗信息，实现数据认证、保密、审计和共享
	基于区块链的无密钥签名架构[12,13]	每个时隙构造散列树，根散列值记录于区块链，进行多文件签名	对签名的文件进行篡改所需开销巨大，以保证文件的完整性
物联网设备的权限与通信管理	基于区块链的物联网设备管理和通信系统[14,15]	设备权限设置与设备控制指令记录于区块链，设备通过密钥进行	保障物联网设备的权限安全和数据隐私，提升系统的安全性
	基于云计算和区块链的制造产业管理体系[16]	物联网设备操作指令记录至区块链，生产和支付操作由智能合约执行	提供分布式资产清单和交易详情，保障记录的完整可靠和可追溯
抵抗 DDoS 攻击	基于区块链的分布式域名解析系统 Blockstack、Nebulis 等[17]	分布式存储，将域名解析逻辑与底层区块链共识机制进行分层	分布式存储域名与 IP 地址映射对，有效抵抗 DDoS 攻击

的运行。因此利用区块链的分布式特点，能够打造一个抵抗 DDoS 攻击的数据库系统[17,22]。

2 网络数据安全和隐私保护

传统的中心节点数据管理体系中，数据由中央机构进行存储和管理。中央机构的管理缺失或设备故障可能造成数据的丢失或泄露。基于区块链的数据管理体系采用去中心化的系统结构，能够消除中央机构的安全风险。区块链技术的不可篡改、可追溯的安全特性能够应用于大量隐私数据的管理，对数据真实性提供保证[23]。

将区块链技术和链外数据库结合，分离数据和数据权限，能够实现去中心化的个人数据管理系统[10,11]，进行数据和权限的管理。应用程序访问用户数据之前，需要得到用户的访问授权。区块链上记录用户和应用程序对数据的操作指令如图 1 所示，例如用户授权指令、信息存储和查询指令等。用户数据被加密后存放于区块链之外的分布式数据库。当用户希望改变某个应用程序对某项数据的授权时，进行权限设置，将所授予的权限和数据指针记录到区块链上。应用程序需要访问某项数据时，发出数据访问请求并记录至区块链。系统对签名以及区块链的记录进行检查，确认该应用程序是否拥有对应数据的访问权限。若检查通过，则将该操作记录在区块链，并由数据库将数据返回给应用程序。由于区块链对应用程序的行为进行了完整的记录，该系统中用户可以随时更改数据的访问权限。数据操作过程对用户是透明的、可审计的。用户能够追踪数据，得知何种数据在何时被何种应用通过何种方式获取，确保数据的安全性。

数字签名是一项用于证实某个文件或数据的完整性和来源的技术，确保文件或数据未被修改和不可抵赖。现阶段广泛使用的签名技术基于 PKI（public key infrastructure，公开密钥基础设施）。PKI 体系中，用户使用公钥—私钥对进行文件的签名和验证，同时需要一个可信的 CA（certificate authority，数字证书认证机构）进行密钥管理[12]。若 CA 密钥管理出现缺陷，失去可信度，将导致签名失效，文件完整性难以保证。因此能够利用区块链不可篡改的性质，构造基于区块链的文件签名体系。

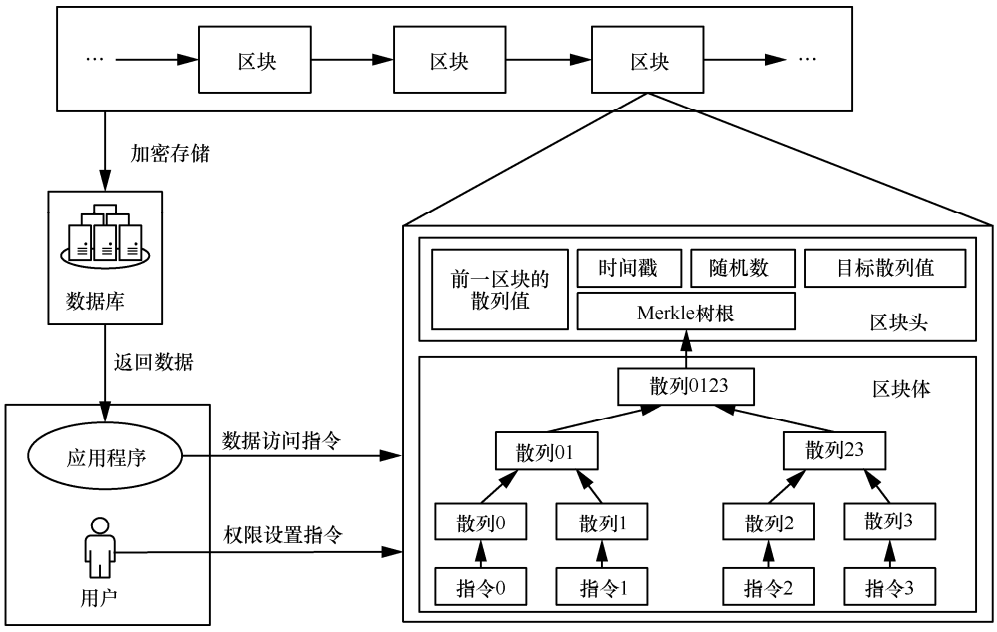


图 1 基于区块链的用户数据管理系统[9]

基于 KSI（keyless signatures' infrastructure，无密钥签名架构）的签名体系是一种基于区块链技术的无密钥签名认证体系[13]。KSI 是一种多签名的体系，即每个时隙能够一次性签名多个文件。每个时隙内，系统收集当前需要签名的所有文件各自的散列值。系统将散列值作为叶节点，构建 Merkle 树并计算获得根节点值。系统将每个时隙计算得到的根节点值进行公开，记录于区块链，分布式存储在每个节点上。区块链确保所记录的根节点值的不可篡改性。系统发布了记录着根节点值的区块之后，文件发送者将对应的根节点值和时间戳等信息构造成对应文件的签名。发送文件时，文件发送者需要将文件与对应的签名同时发送给文件接收者。接收者收到文件和对应的签名后，需要对文件签名进行验证。接收者提取出签名中的节点信息，运行散列算法，构建 Merkle 树并计算根节点值。接收者计算出根节点值之后，将其与区块链上存储的数据进行对比，若二者相等则可验证文件的完整性。KSI 体系中，散列函数的单向性以及区块链的不可篡改性确保了签名的可靠性。通过 KSI 进行签名的文件难以被黑客篡改，以此保证文件的完整性。

3　物联网设备的权限与通信管理

传统的物联网设备管理系统采用中心化结构，设备的数据和控制信息都由中心节点控制和维护，增加了中心节点的计算负载和安全问题[24,25]。区块链技术能够应用于物联网，构建去中心化的物联网设备管理系统，消除中心节点的安全风险，对物联网设备的权限和设备间通信进行有效管理[14,15]。

图 2 是基于区块链技术的物联网设备管理体系。设备之间能够进行相互通信或相互控制，例如存取数据等。指令只有在设备拥有权限的情况下才能被执行。区块链上记录设备间的通信或控制指令以及权限情况。系统运行的初始阶段，系统生成所需要的密钥以及初始区块。由用户定义系统所需的策略后，将其记录至初始区块。系统运行期间，设备之间需要进行相互通信或控制。设备需要先得到用户授权，才能得到系统分发的密钥进行通信或控制，确保权限安全和通信隐私。设备间的通信以及控制指令依照时间顺序，记录至区块链。区块链系统发布了记录着指令的区块后，设备身份和权限得到确认，指令才能执行。因此设备的安全性和数据的机密性、完整性、可用性能够得到保障。该系统不需要中心节点进行设备的统一管理，消除了中心节点的安全风险，能够有效抵抗 DDoS 攻击和链接攻击[26]。设备运行记录真实有效，完整可靠，可追溯。

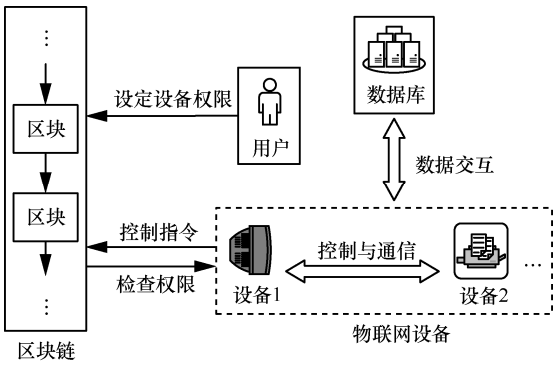


图 2　基于区块链的物联网设备管理系统[15]

基于区块链的模型对比基于中心的模型，访问指令的执行时间比增加约 50.0%，能量损耗增加约 20.6%。存储—查询指令的执行时间增加约 46.8%，能量损耗增加约 19.2%。存储周期增加约 43.5%，能量损耗增加约 14.7%[15]。引入区块链会带来额外的信息加密和散列计算的开销，因此系统开销增大，但是区块链的引入消除了中心节点的安全风险，保障了设备权限和通信的安全性[15]。

4　抵抗 DDoS 攻击

DDoS 攻击者通过一系列手段，向目标系统的中心节点发出大量的请求，占用中心节点的计算资源或网络资源，引起目标系统或网络的瘫痪[20]。

传统的中心化系统依靠中心节点提供服务，难以抵挡 DDoS 攻击。基于区块链的去中心化系统结构能够将系统数据分布存储于多台设备，不存在可攻击的系统中心节点。因此，基于区块链的去中心化系统能够有效抵抗 DDoS 攻击[27]。

基于区块链的系统能够提供分布式、无中心节点的系统结构，系统所需的数据完整存储于多台设备。区块链的每个节点都具备完整的数据，并且能够对其他节点的数据有效性进行验证。即使某个节点被攻破，整个系统也不会完全瘫痪。依靠剩余的节点依然可以维持整个区块链系统的正常运转，并能够恢复被破坏的节点的数据和功能。因此区块链技术能够用于打造一个抵抗 DDoS 攻击的数据库系统[27]。

将区块链应用于 DNS（domain name system，域名系统），能够消除单点失败，有效抵抗 DDoS 攻击，保障系统的整体安全[28]。目前已经提出的基于区块链的 DNS 有 Namecoin、Blockstack 和 Nebulis 等。以 Blockstack 为例。图 3 为 Blockstack 系统的结构，其主要组成部分是区块链、本地数据库和云存储。系统由多个逻辑层构成。底层为区块链，记录用户对系统的操作，例如注册和更新域名等，并记录着区域文件的散列值。系统的安全性和可靠性依赖于底层区块链。路由层的功能是提供区域文件散列值到区域文件路径的映射。用户得到底层返回的区域文件散列值后，路由层根据散列值在数据库中查找对应的区域文件。存储层存放着加密的用户数据。用户得到区域文件后，提取出其中的目标数据存储路径，存储层根据路径将目标数据返回给用户。

5 结束语

本文讨论了区块链在保护网络数据安全与隐私，物联网设备管理和 DDoS 防御等网络安全技术的应用。基于区块链的数据管理系统消除了传统中央机构易遭受攻击而导致数据泄露甚至网络瘫痪的安全风险，防止攻击者对中心节点的入侵，用户能够完全控制网络数据的权限与使用情况。基于区块链的 KSI 体系用于文件签名，不依赖可信的 CA 进行密钥管理，使攻击者难以篡改文件与签名。基于区块链的物联网设备管理系统将区块链用于物联网设备的权限和通信管理，防止攻击者对物联网的中央控制节点进行入侵和破坏，保证设备的权限设置、通信与控制记录的完整和

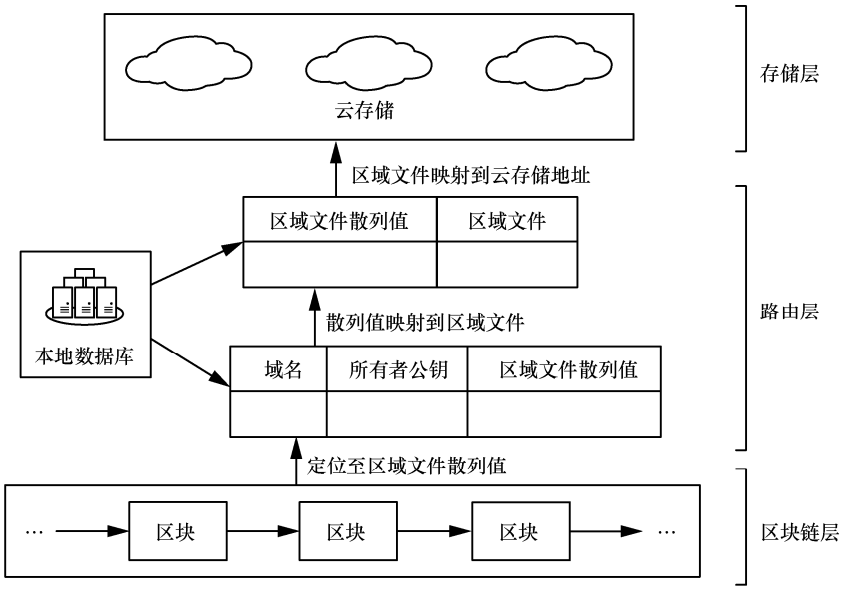


图 3 基于区块链的域名系统结构[17]

不可篡改。基于区块链的 DNS 包括 Blockstack 和 Nebulis 等系统，利用区块链的分布式结构特点抵抗 DDoS 攻击，并提高系统的吞吐量。基于区块链的网络安全技术尚处于发育初期，存在挑战急需解决：网络安全系统中引入区块链引发加解密计算和散列计算等计算开销，降低了系统的吞吐量，增加系统的能耗。因此必须研究如何降低区块链系统计算开销。其次，区块链系统一旦在所有节点成功运行，系统协议的更新例如加密算法替换将难以进行。因此系统运行之后，如何快速进行系统更新是未来的一个研究方向。最后，区块链记录着系统启动之后所有的记录信息，存储成本将随着时间增长急剧上升，因此未来需要对降低区块链系统存储成本的问题进行研究。

参考文献：

[1] XIAO L, LI Y, HAN G, et al. A secure mobile crowdsensing game with deep reinforcement learning[J]. IEEE Transactions on Information Forensics & Security, 2017, 136(1): 35-47.

[2] 肖亮, 李强达, 刘金亮. 云存储安全技术研究进展综述[J]. 数据采集与处理, 2016, 31(3): 464-472.
XIAO L, LI Q D, LIU J L. Survey on secure cloud storage[J]. Journal of Data Acquisition & Processing, 2016, 31(3): 464-472.

[3] XIAO L, XU D, XIE C, et al. Cloud storage defense against advanced persistent threats: a prospect theoretic study[J]. IEEE Journal on Selected Areas in Communications, 2011, 35(3): 534-544.

[4] 刘明辉, 张尼, 张云勇, 等. 云环境下的敏感数据保护技术研究[J]. 电信科学, 2014, 30(11): 2-8.
LIU M H, ZHANG N, ZHANG Y Y, et al. Research on sensitive data protection technology on cloud computing [J]. Telecommunications Science, 2014, 30(11): 2-8.

[5] 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.

[6] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted, 2008.

[7] BUTERIN V A. Next-generation smart contract and decentralized application platform[R]. 2014.

[8] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2017: 1-20.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain technology: architecture and progress[J]. Chinese Journal of Computers, 2017: 1-20.

[9] ZYSKIND G, NATHAN O. Decentralizing privacy: Using blockchain to protect personal data[C]//IEEE Security and Privacy Workshops, May 21-22, 2015, San Jose, CA, USA. Piscataway: IEEE Press, 2015: 180-184.

[10] WOOD G. Ethereum: a secure decentralised generalized transaction ledger[EB]. 2014.

[11] AZARIA A, EKBLAW A, VIEIRA T, et al. MedRec: using blockchain for medical data access and permission management[C]//IEEE International Conference on Open and Big Data, Dec 5-8, 2016, Washington, DC, USA. Piscataway: IEEE Press, 2016: 25-30.

[12] BULDAS A, LAANOJA R, TRUU A. Keyless signature infrastructure and PKI: hash-tree signatures in pre- and post-quantum world[J]. International Journal of Services Technology & Management, 2017, 23(1/2): 117.

[13] BULDAS A, LAANOJA R, TRUU A. Efficient quantum-immune keyless signatures with identity[J]. IACR Cryptology ePrint Archive, 2014: 321.

[14] DORRI A, STEGER M, KANHERE S, et al. Blockchain: a distributed solution to automotive security and privacy[J]. IEEE Communications Magazine, 2017, 55(12):119-125.

[15] DORRI A, KANHERE S, JURDAK R, et al. Blockchain for IoT security and privacy: the case study of a smart home[C]// IEEE International Conference on Pervasive Computing and Communications, March 13-17, 2017, Kona, HI, USA. Piscataway: IEEE Press, 2017: 618-623.

[16] BAHGA A, MADISETTI V K. Blockchain platform for industrial Internet of things[J]. Journal of Software Engineering and Applications, 2016, 9(10): 533.

[17] ALI M, NELSON J, SHEA R, et al. Blockstack: a global naming and storage system secured by blockchains[C]//USENIX Annual Technical Conference, July 12-14, 2016, Santa Clara, CA, USA. Piscataway: IEEE Press, 2016: 181-194.

[18] AITZHAN N, SVETINOVIC D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams[J]. IEEE Transactions on Dependable & Secure Computing, 2016(99): 1.

[19] 赵明慧, 张琭, 亓晋. 基于区块链的社会物联网可信服务管理框架[J].电信科学, 2017, 33(10): 19-25.
ZHAO M H, ZHANG L, QI J. A framework of trusted services management based on block chain in social internet of things [J]. Telecommunications Science, 2017, 33(10): 19-25.

[20] WANG B, ZHENG Y, LOU W, et al. DDoS attack protection in the era of cloud computing and software-defined networking[J]. Computer Networks, 2015(81): 308-319.

[21] 李传煌, 孙正君, 袁小雍, 等. 基于深度学习的实时 DDoS 攻击检测[J]. 电信科学, 2017, 33(7): 53-65.
LI C H, SUN Z J, YUAN X Y, et al. Real-time DDoS attack detection based on deep learning [J]. Telecommunications Science, 2017, 33(7): 53-65.

[22] 王帅, 汪来富, 金华敏, 等. 网络安全分析中的大数据技术应用[J]. 电信科学, 2015, 31(7): 145-150.
WANG S, WANG L F, JIN H M, et al. Big data application in network security analysis[J]. Telecommunications Science, 2015, 31(7): 145-150.

[23] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]//IEEE Symposium on Security and Privacy (SP), May 23-25, 2016, San Jose, CA, USA. Piscataway: IEEE Press, 2016: 839-858.

[24] SIVARAMAN V, CHAN D, EARL D, et al. Smart-phones attacking smart-homes[C]//ACM Conference on Security & Privacy in Wireless and Mobile Networks, July 18-20, 2016, Darmstadt, Germany. New York: ACM Press, 2016: 195-200.

[25] HU Q, LV S, SHI Z, et al. Defense Against advanced persistent threats with expert system for internet of things//IEEE/IFIP International Conference on Wireless Algorithms Systems and Application, June 19-21, 2017, Guilin, China. Piscataway: IEEE Press, 2017.

[26] NARAYANAN A, BONNEAU J, FELTEN E, et al. Bitcoin and cryptocurrency technologies: a comprehensive introduction[M]. Princeton: Princeton University Press, 2016.

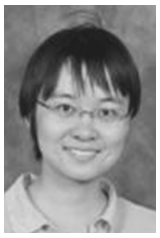
[27] RODRIGUES B, BOCEK T, LAREIDA A, et al. A blockchain-based architecture for collaborative DDoS mitigation with smart contracts[C]//IFIP International Conference on Autonomous Infrastructure, Management and Security, July 10-13, 2017, University of Zurich, Zurich, Switzerland. Berlin: Springer-Verlag, 2017: 16-29.

[28] HU W, AO M, SHI L, et al. Review of blockchain-based DNS alternatives[J]. 网络与信息安全学报, 2017, 3(3): 71-77.
HU W, AO M, SHI L, et al. Review of blockchain-based DNS alternatives[J]. Chinese Journal of Network and Information Security, 2017, 3(3): 71-77.

[作者简介]

陈烨（1995−），男，厦门大学信息科学与技术学院硕士生，主要研究方向为网络安全、无线通信。

许冬瑾（1994−），女，厦门大学信息科学与技术学院硕士生，主要研究方向为网络安全、无线通信。



肖亮（1980−），女，厦门大学信息科学与技术学院教授、博士生导师，主要研究方向为网络安全、无线通信。