基于区块链技术的车联网汽车身份认证可行性研究*

刘勇　李飞　高路路　徐翔

（成都信息工程大学，成都 610225）

【摘要】针对现有的假冒汽车身份攻击方法和多服务器身份认证问题，分析并总结了车联网安全和身份认证的相关研究和成果，基于区块链技术的特征和原理，将区块链技术与车联网相结合，应用在汽车身份认证中，提出适用于车联网身份认证的区块链系统框架，并基于该框架设计了汽车与多服务器、汽车及路边设施单元（RSU）之间的认证，分析了其可行性。

主题词：车联网　身份认证　区块链　V2X

中图分类号：U462.1　　**文献标识码：**A　　**DOI:** 10.19620/j.cnki.1000-3703.20180183

Feasibility Study of Automotive Identity Based on Blockchain Technology

Liu Yong, Li Fei, Gao Lulu, Xu Xiang

（Chengdu University of Information Technology, Chengdu 610225）

【Abstract】 In order to solve the problems associated with fake vehicle identity attack method and multi-server identity authentication, this paper analyzed and summarized the related research and achievement of the vehicle connectivity safety and identity authentication. It combined blockchain technology with vehicle connectivity and applied in the vehicle identity authentication based on the characteristic and principle of blockchain technology, and proposed a blockchain system framework suitable for vehicle connectivity identity authentication, and based on this framework, the authentication between vehicle and multi-server, vehicle and RSU was designed. Finally, its feasibility was analyzed.

Key words: Vehicle connectivity, Authentication, Blockchain, V2X

1　前言

智慧城市[1]是城市发展的高级产物，其核心理念是实现城市中各个物体的互联、动态感知、智慧管理，为未来城市提供了一种新的发展方向。智慧交通作为智慧城市的核心之一，涉及物联网、云计算、大数据等多项综合技术，使人、车、路协调运转[2]。而车联网作为智慧交通的核心领域，以车内网、车际网和车载移动互联网为基础[3]，实现车与车、车与建筑物、车与基础设施单元之间的信息交换，甚至可以帮助实现汽车与行人、汽车与非机动车之间的“对话”[4]。

在车联网中，由于车辆自身的移动特性，车载通信具有移动区域受限、网络拓扑变化快、网络频繁接入和中断、节点覆盖范围大、通信环境复杂等特点[5]。基于这些特点，目前车联网的发展面临几个主要问题：

a.　建设成本和能源消耗。在车载移动互联网中，路边设施单元（Road Side Unit，RSU）作为车辆自组织网（Vehicular Ad-hoc Network，VANET）无线接入点，将车辆和道路等信息上传至互联网并发布，这种车与基础设施（Vehicle to Infrastructure，V2I）的协作通信模型需要大量的RSU支撑，增加了建设的成本和能源消耗[6-7]。

b.　通信协议标准不统一。在车联网中存在着多种网络通信协议，不同网络数据传输需要进行协议转换，影响通信效率。此外，由于车辆高速行驶，需要快速可靠的网络连接和数据传输，这对网络通信时延有着极高的要求。

c.　安全问题：由于车联网采用无线通信，因此存在数据破坏、重放、假冒和监听等安全及个人隐私问题[8-9]，可能造成财产损失甚至危及驾乘人员的人身安全。

2　车联网身份认证研究现状

V2X（Vehicle to X）是自动驾驶的必要技术和智慧交通的重要一环，其中X可以表示基础设施、车辆、行人或道路等。目前V2X技术的两大阵营分别是由国内企

*基金项目：四川省科技项目（2016GZ0343；18PKX0699）。

业推动的车间通信长期演进（Long Term Evolution-Vehicle，LTE-V）技术和美国主导的专用短程通信（Dedicated Short Range Communications，DSRC）技术（基于IEEE 802.11p）。

现有的车联网通信中依旧存在很多安全性问题，例如，Sybil攻击[10-11]是一种基于假冒身份的车联网攻击方法，假冒节点通过伪造汽车身份标识控制车辆，发送虚假信息，伪造交通场景从而影响车辆的正常判断，导致交通网络运行瘫痪或引发交通事故等。

所有的用户系统都有认证与授权功能[12]。在车辆身份认证领域，学者们提出了一些安全认证方案。王群[13]提出了基于射频识别（RFID）的车辆身份信息识别方法，车辆经过阅读器覆盖区域时，其电子标签被激活并被读写器识别，读写器将识别的车辆信息通过网络发送到中心数据库进行身份识别和验证。Z Gao等人提出了基于公钥基础设施（Public Key Infrastructure，PKI）的认证方法[14]，满足了不同用户甚至同一用户在不同场景下的安全需求。王文骏提出了基于证书的车辆身份认证方法[15]，车辆在区域服务器完成注册后获取证书，实现车辆身份匿名认证，并能够独立检测Sybil攻击，恶意车辆身份撤销由区域服务器完成，避免使用撤销列表，使车辆省去查找撤销列表的开销。Calandriello G等人提出了基于身份签名（Identity-Based Signature，IBS）的认证方法[16]，以确保合法节点可以匿名和更容易生成化名。此外还有基于群签名（Group Signature）的认证方法[17-21]等。但这些认证方法适用于简单通信环境，无法满足复杂环境中多信道的安全需求。文献[22]基于双线性映射理论设计出能实现复杂通信场景认证的会话密钥，通过优化通信负载、减少交互环节实现低时延的认证协议，使可信中心（Trusted Center，TC）能够验证车辆的合法性或对其授权。文献[23]提出了一个轻量级的自愈群密钥分配方案，该方案访问控制多项式和群密钥以指数的形式广播，并在广播消息中增加消息验证码，实现了群密钥的保密性和广播认证，利用滑动窗口机制恢复丢失的群会话密钥，缓解了通信开销，并针对车联网的子群和群间通信场景，提出子群自愈群密钥分配和安全群间通信方案，实现了子群之间的信息共享和信息保密。

随着云计算和大数据技术的快速发展，为车辆提供的各种云服务不断出现，但通常不同的云服务产品由不同的服务器维护，在传统的单一服务注册机制中，用户使用任一服务前必须在相应服务提供商注册，凭账号和密码登录。但这需要用户记住在每个服务商处的账号信息才能通过相应系统的身份认证，这给用户带来了极大的困扰。因此，一般用户为了避免记住大量的账号和密码，通常在众多服务器中使用相同的账号和密码。然而，这产生了另外2个问题：如果某一服务器出现账户信息泄露，很可能导致用户在其他服务器上的信息泄露[24]；随着用户数量的急剧增加，每个服务器需要维护海量的账户信息，造成众多服务器在用户管理方面出现资源叠加浪费，也可能因此导致服务器性能瓶颈[25]。区块链技术的去中心化、数据不可篡改等特点，可以使多个服务提供商共同维护一个账户信息账本，用户只需要记住该账本上的账户信息便可在多个服务器上完成身份认证，因此，汽车身份认证可以借鉴区块链技术。

3 区块链技术特点及应用场景

3.1 区块链技术特点

区块链作为比特币系统的底层技术，主要包括对等网络（Peer-to-Peer，P2P）技术、分布式账本技术、非对称加密技术、公式机制技术和智能合约技术[26-28]。区块链目前分为公有链、联盟链和私有链[29]，其共同特点是公开透明、不可篡改、可追溯、时间序列和加密等[30]，不同点在于去中心化的程度不同，共识机制和信任机制也不同。如图1所示，区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成[31-32]。

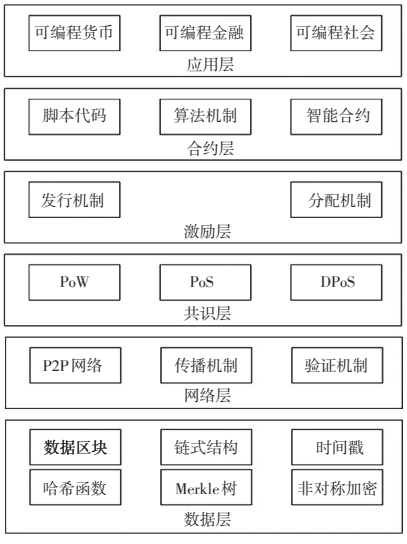

图1 区块链技术的基础架构模型

图1中，数据层包含数据的加密、封装及区块的打包；网络层包含数据的传播、验证机制，如比特币系统中采用拜占庭算法保证数据传播的一致性；共识层主要解决记账权问题，所有参与记账节点都通过共识机制选出一个记账节点，目前主要的共识机制有工作量证明（Proof-of-Work，PoW）、权益证明（Proof-of-Stake，PoS）、

（Delegated Proof-of-Stake，DPoS）、瑞波共识（Ripple Consensus）算法等[33]；激励层主要用于设计奖励机制，在比特币系统中，矿工记入一个有效区块时，系统会奖励一定的比特币作为奖励，此外还有该区块中所有的手续费作为奖励转给该矿工；合约层主要包含各类脚本、算法和智能合约，满足合约的触发条件时，系统会自动执行合约中的内容；应用层则封装了区块链的各种应用场景和案例。

3.2 区块链应用场景

区块链的特点使其可以应用到数字货币、数据存储、数据鉴证、金融交易、资产管理和选举投票等场景。目前，区块链技术主要应用在金融领域，如跨境支付、股权众筹等。近年，有学者提出区块链在物联网中的相关研究[34-38]，由于两者都具有去中心化、分布式的特点，基于这些特点，将区块链应用到物联网中可以解决传统中心化物联网管理方案的弊端，提高物联网的安全性。文献[39]将DistBlockNet模型与软件定义网络（Software Defined Network，SDN）和区块链相结合，提出了一种基于SDN架构的分布式区块链安全物联网网络，在该网络中，系统能够自动适应危险环境。文献[40]提出了一种基于区块链的固件更新方案，嵌入式设备要求在区块链网络节点得到固件是否最新的确定信息，它可以安全地检查固件版本，验证固件的正确性，并能够在物联网环境中下载最新的嵌入式设备固件。车联网作为物联网的一部分，国内外目前暂无车联网与区块链结合的相关研究，本文对区块链技术应用在车联网汽车身份认证方面进行研究和分析。

4 基于区块链的车联网汽车身份认证

4.1 车联网区块链系统架构设计

汽车正在向智能化、无人驾驶的方向发展，对车辆进行管理，实现汽车安全行驶是车联网的重要课题[41]。车联网属于物联网的一部分，同样具有分布式、去中心化等特点，因此，区块链技术可以解决车联网去中心化管理、隐私保护等问题。

本文设计的车联网区块链系统架构如图2所示，将车、RSU、可信中心（云服务提供商）三者构建成一个区块网络，在该网络中车辆节点不承担数据计算工作，不参与工作量机制证明，只进行数据的加密和传输，把数据作为区块链交易向RSU（或通信基站）进行传输，RSU（或通信基站）对接收到的数据进行验证，通过后将数据传送给可信中心，可信中心再根据共识机制选取其中一个中心进行记账，其余可信中心负责校验账本信息。

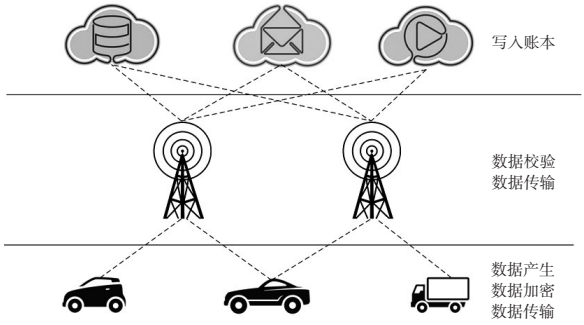

图2 车联网区块链系统架构

设现有的主要汽车生产商、政府管理机构为创世节点。为了保证新加入节点（如新加入的汽车生产商、云服务提供商等）身份的真实性、可靠性，共识机制采用瑞波共识算法。记账节点对发起申请的节点身份资料进行审核，审核通过则进行签名，当签名数大于等于本系统中节点个数的51%时，系统自动认为该申请节点通过审核，将该节点加入记账节点，并记录到区块链中，否则此次申请请求无效，可有效防止恶意节点随意加入。新节点加入的智能合约设计如图3所示。

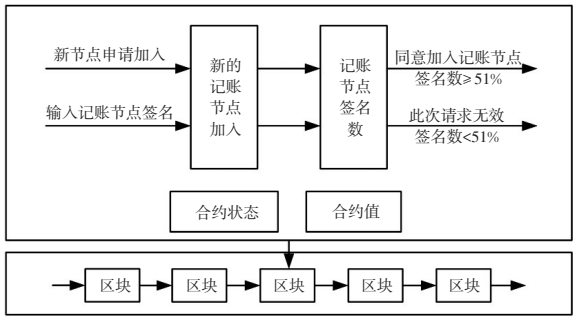

图3 新节点加入的智能合约

本文区块链结构设计如图4所示，包括区块头和区块体两部分内容。

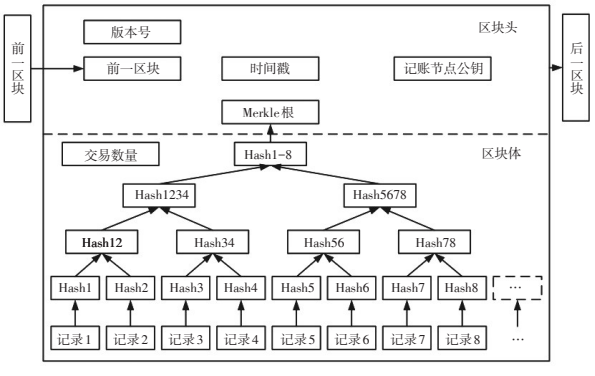

图4 区块链结构

4.2 基于区块链技术的汽车身份认证

传统的PKI认证技术的密钥分配方案分为集中式和分散式两种，其中集中式密钥分配方案如图5所示，由一个可信的中心节点负责密钥的产生并分配给各通

信方，其主要任务是数字证书的颁发和管理。

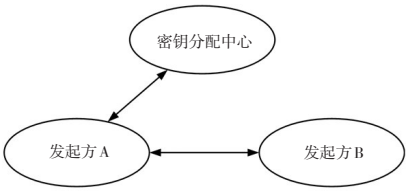

图5　集中式密钥分配方案

基于区块链的车联网汽车身份认证可在上述集中式密钥分配方案基础上进行改进。在图2所示的框架中，上层各云服务提供商通过共识机制，代替传统PKI中的密钥分配中心（Key Distribution Center，KDC）进行数字证书的发放和管理，改进后的分配方案如图6所示，其中发起方A为RSU，发起方B为汽车，创世节点和各服务商作为记账节点，各节点之间通过共识机制构成“1个密钥分配中心”。例如，汽车首先向具有记账权的云服务商提交注册申请，该服务商通过共识机制核实汽车身份后，自动产生包含汽车公钥的数字证书并记入自己的账本中，它包含汽车的真实身份，并证明汽车公钥的有效期和作用范围（交换密钥或数字签名），再将该信息通过P2P网络发送给其他服务商节点，其他服务商节点只要能验证证书的真实性，并信任所颁发证书的记账者身份，就将该条信息记录到自己的账本。这种方案可以避免用户多次在各服务器注册身份信息，同时也避免了集中式密钥分配带来的效率低、管理难等问题。

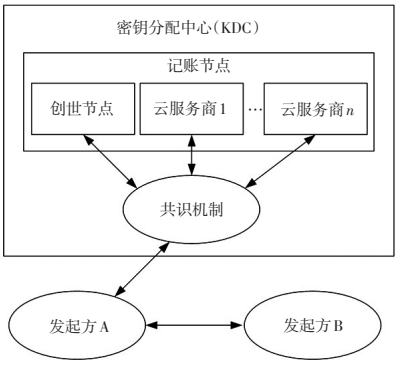

图6　改进的密钥分配方案

车辆B向该系统注册的具体流程为：

a.　B→KDC：$E_{PKDC}(R_1||M_1)$，车辆B利用KDC的公钥P_{KDC}加密其注册时提交的信息M_1（包括唯一识别码ID）和随机数R_1，并将加密结果发送给KDC；

b.　KDC→B：$E_{R1}(K_B||P_B)$，KDC得到信息后，利用自己的私钥K_{KDC}进行解密，得到R_1和M_1，并对内容进行审核，若内容为真，则生成对应的公钥P_B和私钥K_B，并用随机数R_1加密后发送给车辆B。

其中，E为加密函数。此时，车辆B的注册尚未完成，还需要同步至其他云服务提供商。

KDC将信息发送给车辆B后，会将该注册信息写入记录，并广播给其他记账节点。区块链认证记录信息数据格式设置如表1所示。

表1　记录信息的区块数据格式

数据项	描述
版本号	表示当前区块链版本信息
认证请求	发起需要身份认证的车辆公钥
认证者列表	认证该车辆的认证者签名列表
认证时间	认证时的时间
有效期	为空表示该记录为认证记录，非空表示注册记录
内容	描述该记录

其他记账节点收到该条记录时，会对其中的内容进行检查，核实版本信息、认证者列表信息的真实性等，若信息正确，将该条信息发送给其他节点，同时放入记录队列等待打包计入账本区块中，否则丢弃该记录。

汽车身份认证分为汽车与云服务器之间的认证、汽车与RSU之间的认证和汽车与汽车之间的认证。

汽车与云服务提供商（亦密钥分配中心）之间的认证流程为：

a.　B→KDC：$E_{PKDC}(P_B||M_1||R||time)$，车辆B向云服务提供商发送自己的公钥$P_B$和请求的服务内容$M_1$，并加随机数$R$和时间戳$time$，利用对应服务商的公钥$P_{KDC}$加密这些内容，并发送出去；

b.　KDC→B：$E_{PB}(M_2||R)$，云服务提供商用私钥K_{KDC}进行解密，判断时间戳$time$是否正确，并利用P_B在区块链上查找该汽车的身份信息，若信息核实为真，则利用P_B加密返回服务内容M_2和随机数R，否则丢弃。

汽车与RSU之间的初始化认证流程为：

a.　A→KDC：$P_A||P_B||R_1$，RSU发送自己和车辆B的公钥P_A、P_B以及随机数R_1给KDC；

b.　KDC→A：$E_{PA}[K_s||P_A||P_B||R_1||E_{PB}[K_s||P_A]]$，KDC收到2个公钥，并在区块链上查找对应信息，若核实为真，则产生会话密钥K_s，并将该次认证记录内容添加到区块中，发送给RSU；

c.　A→B：$E_{PB}[K_s||P_A]||E_{Ks}[R_2]$，RSU用私钥解密后得到会话密钥$K_s$、$P_B$和$E_{PB}[K_s||P_A]$，此时完成了对车辆B的认证，用$K_s$加密随机数$R_2$，一起发送给车辆B；

d.　B→A：$E_{Ks}[f(R_2)]$，车辆B用自己的私钥解密得到K_s和P_A，即完成了对RSU的认证。

汽车和RSU初始化认证后，得到两者之间的会话密钥K_s，可设置K_s的有效时长，即每隔一定时间汽车和RSU更新一次K_s。

汽车与汽车之间的认证流程为：

a. B→C：$P_B||E_{KB}(M_1||R||time)$，汽车B向汽车C发送自己的公钥$P_B$和用自己的私钥$K_B$加密的请求服务内容$M_1$、随机数$R$和当前时间戳$time$；

b. C→B：$P_C||E_{KC}(M_2||R)$，汽车C用汽车B的公钥P_B进行解密，得到P_B、M_1、随机数R和当前时间戳$time$，并判断P_B和$time$是否正确，若正确，则利用自己的私钥K_C加密返回服务内容M_2和随机数R，将公钥P_C一起发送给汽车B，并将该次记录发送到区块链网络中，等待记账节点写入区块中，否则丢弃。

综上所述，区块链技术结合PKI认证机制可以解决车联网中汽车与服务器和RSU的身份认证问题，同时也解决了用户账号管理问题，可以实现同一账号多处登录。此外，区块链自带的加密技术可用于对汽车身份信息的加密，防止用户信息泄露。总的来说，应用区块链技术可以解决车联网中多服务系统的身份认证问题和身份假冒问题。

5 结束语

目前，区块链技术多应用于金融领域，现有的区块链数据结构不能直接应用在车联网中，本文研究了基于区块链技术的车联网汽车身份认证的可行性，总结了现有的车联网认证方案，分析其各自的特点和不足，结合区块链技术特点设计出车联网区块链系统架构和相关区块链结构、完成节点加入的相关智能合约，在该框架上结合现有的PKI认证机制提出了新的修改思路，完成车辆的注册、汽车与汽车、服务器和RSU相关认证功能，为车联网区块链技术的后续研究提供参考。

将区块链技术应用于车联网汽车身份认证，还需要解决汽车认证中的隐私保护问题。每辆汽车在区块链网络中只拥有唯一的公钥P和对应的私钥K，虽然本文采用联盟链，对加入的记账节点进行严格审查，以确保账本的机密性，但汽车在认证或提供服务时，需要暴露自己的公钥P，存在位置跟踪的危险，如何保护汽车公钥P，是解决隐私保护问题的首要任务。

此外，由于汽车数量多，通信频繁，因此对身份认证的请求次数较多，建立高效、快速的共识机制是必然选择，不过随着区块链技术的快速发展，交易处理速度不断加快，目前可达到每秒处理百万笔交易，未来，更多针对车联网的研究将满足更多场景的需求。

参 考 文 献

[1] Neirotti P, Marco A D, Cagliano A C, et al. Current Trends in Smart City Initiatives: Some Stylised Facts[J]. Cities, 2014, 38(5):25-36.

[2] 苑宇坤, 张宇, 魏坦勇,等. 智慧交通关键技术及应用综述[J]. 电子技术应用, 2015, 41(8):9-12.

[3] 王良民, 刘晓龙, 李春晓,等. 5G车联网展望[J]. 网络与信息安全学报, 2016, 2(6):1-12.

[4] 惠伟, 孙伟华, 何蔚. 车联网发展中的机遇与挑战[J]. 信息安全与技术, 2015, 6(12):5-7.

[5] Mershad K, Artail H. A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks[J]. IEEE Transactions on Vehicular Technology, 2013, 62(2): 536-551.

[6] Sharef B T, Alsaqour R A, Ismail M. Vehicular Communication Ad Hoc Routing Protocols: A Survey[J]. Journal of Network & Computer Applications, 2014, 40(1): 363-396.

[7] Mumtaz S, Huq K M S, Ashraf M I, et al. Cognitive Vehicular Communication for 5G[J]. IEEE Communications Magazine, 2015, 53(7):109-117.

[8] Vinel A, Ma X, Huang D. Guest Editors' Introduction: Special Issue on Reliable and Secure VANETs[J]. Dependable & Secure Computing IEEE Transactions on, 2016, 13(1):2-4.

[9] 李馥娟, 王群, 钱焕延. 车联网安全威胁综述[J]. 电子技术应用, 2017, 43(5):29-33.

[10] Druschel P, Kaashoek M F, Rowstron A I T. Revised Papers from the First International Workshop on Peer-to-Peer Systems[C]// Revised Papers from the First International Workshop on Peer-to-Peer Systems. Springer-Verlag, 2002:1571-1572.

[11] 鲍美英, 马礼, 高玉斌. 网格环境下授权策略的研究[J]. 微电子学与计算机, 2010, 27(3):43-46.

[12] 李馥娟. 基于OAuth的开放授权技术及在云计算中的应用[J]. 计算机系统应用, 2015, 24(4):228-232.

[13] 王群, 钱焕延, 赵钢. 一种面向车联网的身份识别与定位方法[J]. 计算机科学, 2012, 39(s3):131-134.

[14] Gao Z, Hu Y, Kai L. CPTIAS: A New Fast PKI Authentication Scheme Based on Certificate Path Trust Index[J]. Journal of Ambient Intelligence & Humanized Computing, 2015, 6(6):721-731.

[15] 王文骏, 刘亚伟. 车联网中基于证书的车辆身份认证方案[J]. 无线通信技术, 2015, 24(2).

[16] Calandriello G, Papadimitratos P, Hubaux J P, et al. Efficient and Robust Pseudonymous Authentication in VANET[C]// International Workshop on Vehicular Ad Hoc Networks, Vanet 2007, Montréal, Québec, Canada, September. OAI, 2007:19-28.

[17] Zhu X L, Yang L U, Hou Z F, et al. Strong Privacy Protection Scheme Based on Oblivious Transfer and Group Signature in VANET[J]. Application Research of

Computers, 2014.
[18] 朱昶胜, 刘鹏辉, 王庆荣,等. 适合移动 Ad hoc 网络基于群签名认证的弹性组密钥管理方案[J]. 计算机应用研究, 2011, 28(10):3811-3816.
[19] 李海峰, 刘云芳. 移动 Ad Hoc 网络中应用自认证的(t,n)门限群签名方案[J]. 北京联合大学学报, 2006, 20(3):19-22.
[20] 肖平安. 基于群签名的身份认证方案研究[D]. 兰州大学, 2013.
[21] 刘辉, 李晖. 采用群组密钥管理的分布式车联网信息认证方案[J]. 西安交通大学学报, 2013, 47(2):58-62.
[22] 刘宴兵, 宋秀丽, 肖永刚. 车联网认证机制和信任模型[J]. 北京邮电大学学报, 2017, 40(3):1-18.
[23] 吴海云. 面向车联网的群密钥管理方案的研究[D]. 安徽大学, 2017.
[24] Wang D, Wang N, Wang P, et al. Preserving Privacy for Free: Efficient and Provably Secure Two-Factor Authentication Scheme with User Anonymity[J]. Information Sciences, 2015, 321:162-178.
[25] Wang D, Wang N, Wang P, et al. Preserving Privacy for Free: Efficient and Provably Secure Two-Factor Authentication Scheme with User Anonymity[J]. Information Sciences, 2015, 321:162-178.
[26] 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.
[27] 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, 2(12):1090-1097.
[28] Pilkington M. Blockchain Technology: Principles and Applications[J]. Social Science Electronic Publishing, 2016.
[29] Underwood S. Blockchain Beyond Bitcoin[J]. Communications of the Acm, 2016, 59(11):15-17.
[30] 张苑. 区块链技术对我国金融业发展的影响研究[J]. 国际金融, 2016(5):41-45.
[31] Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia[J]. Social Science Electronic Publishing, 2015.
[32] Pierro M D. What Is the Blockchain?[J]. Computing in Science & Engineering, 2017, 19(5):92-95.
[33] 王晓光. 区块链技术共识算法综述[J]. 信息与电脑, 2017(9):72-74.
[34] Christidis K, Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access, 2016, 4:2292-2303.
[35] Kshetri N. Can Blockchain Strengthen the Internet of Things?[J]. It Professional, 2017, 19(4):68-72.
[36] 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.
[37] 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.
[38] 何渝君, 龚国成. 区块链技术在物联网安全相关领域的研究[J]. 电信工程技术与标准化, 2017, 30(5):12-16.
[39] Sharma P K, Singh S, Jeong Y S, et al. DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks[J]. IEEE Communications Magazine, 2017, 55(9):78-85.
[40] Lee B, Lee J H. Blockchain-Based Secure Firmware Update for Embedded Devices in an Internet of Things Environment[J]. Journal of Supercomputing, 2016, 73(3):1-16.
[41] 杜玲利, 程明敏, 董伟. 浅谈车联网[J]. 汽车实用技术, 2017(1):58-60.

（责任编辑　斛　畔）

修改稿收到日期为2018年3月28日。