软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(6):1575−1576 [doi: 10.13328/j.cnki.jos.005747]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链与数字货币技术专题前言*

斯雪明[1], 陈文光[2]

[1](复旦大学 计算机科学技术学院,上海 201203)

[2](清华大学 计算机科学与技术系,北京 100084)

通讯作者: 斯雪明, E-mail: sxm@fudan.edu.cn

中文引用格式: 斯雪明,陈文光.区块链与数字货币技术专题前言.软件学报,2019,30(6):1575−1576. http://www.jos.org.cn/1000-9825/5747.htm

区块链是一种全局共享的分布式账本,具有去中心化、高公信力、数据不可篡改等特点.区块链技术被认为是数字经济的基石,广泛应用于金融、物联网、智能制造、供应链管理、数字资产交易等多个领域,在全球经济、产业、学术各个领域都获得了高度关注和认可.区块链技术被认为是最有可能引发颠覆式产业创新的新技术之一.为了更好地把握时机,迎接挑战,有必要对区块链技术的创新和区块链应用的拓展进行研究.

本专题聚焦区块链理论技术的创新以及区块链技术应用的拓展.采取公开征稿的方式,共有 28 篇稿件通过了形式审查.特约编辑先后邀请了各领域专家参与审稿,每篇稿件至少邀请 2 位专家进行评审,每篇稿件都经过两轮审稿,最终有 10 篇稿件通过评审,入选本专题.

《高性能联盟区块链技术研究》,研究高性能联盟区块链的优化算法,在联盟链关键技术研究的基础上,结合现有主板证券竞价交易系统的业务,提出了全新的系统架构以及关键技术的实现.对业务逻辑与共识分离、存储优化和数字签名验证优化(包括合并验签和 GPU 加速)等可提高联盟链性能的优化策略进行了详细的介绍和分析.

《基于许可链的 SWIFT 系统分布式架构》,基于许可链分布式共识机制提出了 BCSWIFT 系统.以优化 SWIFT 系统的报文传输业务为例,阐释了基于许可链的跨境金融通信的基本机理,为确保跨境支付、清算、结算的安全、高效、准确和低成本化运作提供了新的思路,也为区块链技术大规模商业应用提供了重要参照.

《基于联盟链的物联网动态数据溯源机制》,为解决大量物联网设备产生的动态数据安全存储与共享问题,建立了物联网动态数据存储安全问题的数学模型,提出了用于实现操作实体多维授权与动态数据存储的双联盟链结构,设计了基于验证结点列表的共识算法,给出了一种基于联盟链的动态数据溯源机制优化方案.能够有效杜绝攻击者对物联网动态数据的篡改、伪造等非授权访问操作,具有较好的应用价值.

《物联网下的区块链访问控制综述》,分析、总结了现有物联网中主流访问控制模型以及使用区块链后的访问控制模型,并对基于区块链的物联网访问控制在未来需要解决的问题进行了展望.

《区块链跨链技术进展研究》,对跨链技术领域的成果进行系统总结,介绍了 24 种主流跨链技术的原理与实现思路,综合分析跨链技术存在的安全性风险,并列举了 12 项主要问题.总结探讨跨链技术的未来发展趋势.

《应用区块链的数据访问控制与共享模型》,提出一种应用区块链的数据访问控制与共享模型,利用属性基加密对企业数据进行访问控制与共享,达到细粒度访问控制和安全共享的目的.在安全性和性能上能够较好地解决企业内部访问权限难控制、企业之间数据难共享的问题.

《响应式许可链基础组件——RepChain》,提出了一款目前国内唯一开源的响应式许可链基础组件,通过全新设计系统架构,突出了响应式、松耦合、轻量级、协同性共识、合约分级部署、运行状态可视化等特点;通过在身份准入的基础上建立安全信道,采用协同性共识代替公有链的竞争性共识,提高了交易的实时性和交易通量.响应式许可链在交易通量、实时性和韧性方面有较大提升.

收稿时间: 2019-02-18

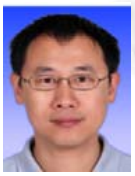
《拟态区块链——区块链安全解决方案》,针对区块链存在的潜在安全问题,借鉴动态异构冗余架构和密码抽签的思想,结合安全性定义和参数选择规则,从动态异构共识机制以及动态异构冗余签名算法两个角度提出了区块链的安全解决方案.

《基于 SM9 算法可证明安全的区块链隐私保护方案》,提出了一种基于身份认证的多 KGC 群签名方案,以联盟链为基础,设计了基于 SM9 算法可证明安全的区块链隐私保护方案,实现在节点间进行身份验证的同时,保护了节点的隐私.

《可监管匿名认证方案》,设计了一种可监管的匿名认证方案,采用安全的密码学算法构建,并通过了安全性的分析证明,能够高效实现可监管的匿名身份认证,适宜在区块链(联盟链)和其他具有匿名认证需求和可监管需求的系统中使用.

本专题面向区块链技术与应用的研究人员和工程人员,内容涵盖区块链性能、区块链体系结构、区块链应用、区块链安全与隐私保护等领域,反映了我国学者对于软件学科过去及未来的重要认识.感谢《软件学报》编委会、CCF 软件工程专委会、CCF 系统软件专委会对本专题工作的指导和帮助,感谢全体评审专家及时、耐心、细致的评审工作,感谢踊跃投稿的所有作者.希望本专题能够对软件学科的科研工作有所促进.

斯雪明(1966－),男,教授,中国计算机学会区块链专委会主任,主要研究领域为区块链,密码学,数据科学,计算机体系结构,网络与信息系统安全.



陈文光(1972－),男,博士,教授,主要研究领域为高性能计算,并行计算,分布式计算.

www.jos.org.cn