

中国科学引文数据库核心期刊 (CSCD)

中国科技核心期刊 (CSTPCD)

ISSN 2095-7025

CN 10-1195/TN



密码学报

JOURNAL OF CRYPTOLOGIC RESEARCH

第5卷 第5期 Vol.5 No.5

2018年10月

区块链技术专刊



主办



中国密码学会

北京信息科学技术研究院



中国科学技术出版社

中国科学引文数据库核心期刊(CSCD)

中国科技核心期刊(CSTPCD)

密码学报
(Mima Xuebao)

第5卷第5期
2018年10月

目次

区块链技术专刊

专刊责任编辑：冯登国, 欧阳永贵

区块链技术专刊序言 (中英文).....	冯登国, 欧阳永贵 (455)
区块链安全研究综述.....	斯雪明, 徐蜜雪, 苑超 (458)
比特币挖矿攻击研究.....	韩健, 邹静, 蒋瀚, 徐秋亮 (470)
区块链理论研究进展.....	单进勇, 高胜 (484)
可更改区块链技术研究.....	李佩丽, 徐海霞, 马添军, 穆永恒 (501)
基于超奇异同源的鉴别方案.....	林齐平, 高胜 (510)
一个高传输效率的多值拜占庭共识方案.....	郭兵勇, 李新宇 (516)
基于 Borromean 环签名的隐私数据认证方案.....	张凡, 黄念念, 高胜 (529)
一种清算结算区块链设计.....	王志鹏, 伍前红 (538)
基于区块链的公平多方不可否认协议.....	苑博奥, 刘军, 李戈 (546)
基于区块链的高效公平多方合同签署协议.....	高莹, 吴进喜 (556)
基于区块链技术的高校成绩管理系统.....	孙韵秋, 王启春 (568)
《密码学报》投稿指南.....	(封三)

CONTENTS

Special Issue: Blockchain Technology FENG Deng-Guo, OUYANG Yong-Gui

Preface of Special Issue on Blockchain Technology
..... FENG Deng-Guo, OUYANG Yong-Gui (455)

Survey on Security of BlockchainSI Xue-Ming, XU Mi-Xue, YUAN Chao (458)

Research on Mining Attacks in Bitcoin
..... HAN Jian, ZOU Jing, JIANG Han, XU Qiu-Liang (470)

Research Progress on Theory of Blockchains SHAN Jin-Yong, GAO Sheng (484)

Research on Fault-correcting Blockchain Technology
..... LI Pei-Li, XU Hai-Xia, MA Tian-Jun, MU Yong-Heng (501)

Identification Scheme Based on Supersingular Isogenies
..... LIN Qi-Ping, GAO Sheng (510)

Multi-valued Byzantine Consensus Scheme with High Transmission Efficiency
..... GUO Bing-Yong, LI Xin-Yu (516)

Privacy Data Authentication Schemes Based on Borromean Ring Signature
..... ZHANG Fan, HUANG Nian-Nian, GAO Sheng (529)

Design of Blockchain for Clearing and Settlement
..... WANG Zhi-Peng, WU Qian-Hong (538)

Fair Multi-party Non-repudiation Protocol Based on Block Chain
..... YUAN Bo-Ao, Liu Jun, Li Ge (546)

Efficient Multi-party Fair Contract Signing Protocol Based on Blockchains
..... GAO Ying, WU Jin-Xi (556)

University Score Management System Based on Blockchain Technology
..... SUN Yun-Qiu, WANG Qi-Chun (568)

密码学报
Mima Xuebao
(双月刊, 2014年创刊)
第5卷 第5期 2018年10月

Journal of Cryptologic Research
(Bimonthly)
(Started in 2014)
Vol.5 No.5 Oct. 2018

编辑 《密码学报》编辑部
(北京市海淀区永翔北路9号 邮编100878)
电话: 86-10-82789618
传真: 86-10-82789618
E-mail: jcr@cacrnet.org.cn
<http://www.jcr.cacrnet.org.cn>

Edited by Editorial Board of Journal of Cryptologic Research
(No. 9, North Yongxiang Road, Haidian District,
Beijing 100878, P. R. China)
Tel: 86-10-82789618
Fax: 86-10-82789618
E-mail: jcr@cacrnet.org.cn
<http://www.jcr.cacrnet.org.cn>

主编 裴定一
主办单位 中国密码学会
北京信息科学技术研究院
中国科学技术出版社

Editor-in-Chief PEI Ding-Yi
Sponsored by Chinese Association for Cryptologic
Research (CACR) and Beijing Academy of Information
Science & Technology (BAIST) and China Science and
Technology Press

主管单位 中国科学技术协会
出版 中国科学技术出版社
印刷 北京科信印刷有限公司
发行 《密码学报》编辑部

Supervised by China Association for Science and
Technology (CAST)
Published by China Science and Technology Press
Printed by Beijing Kexin Printing Co., Ltd.

ISSN 2095-7025
CN 10-1195/TN

邮发代号: 80-918
公开发行业

定价:60.00元