doi :10.3969/j.issn.1671-1122.2020.09.010

基于属性基加密的区块链隐私保护与访问控制方法

汪金苗[1,2]，谢永恒[1]，王国威[3]，李易庭[3]

（1. 北京锐安科技有限公司，北京 100192；2. 北京市网络空间数据分析与应用工程技术中心，北京 100192；
3. 北京市公安局，北京 100055）

摘　要：区块链中所有节点都保存相同样本，随着区块链技术的广泛应用，区块链隐私保护与访问控制问题日益突出。文章基于多授权中心的属性基加密算法提出了面向区块链的隐私保护与访问控制方案。多授权中心可以由区块链中的权威节点轮值担任，有效解决了单一授权中心权限过大的问题。采用该方案后，所有数据采用属性基加密算法加密后保存在区块链中，只有属性满足访问控制策略的用户才能成功解密数据，从而实现区块链中的隐私保护与访问控制。

关键词：访问控制；隐私保护；多授权中心；区块链；属性基加密

中图分类号：TP309　文献标志码：A　文章编号：1671-1122（2020）09-0047-05

中文引用格式：汪金苗，谢永恒，王国威，等 . 基于属性基加密的区块链隐私保护与访问控制方法 [J]. 信息网络安全，2020，20（9）：47-51.

英文引用格式：WANG Jinmiao, XIE Yongheng, WANG Guowei, et al. A Method of Privacy Preserving and Access Control in Blockchain Based on Attribute-based Encryption[J]. Netinfo Security, 2020, 20(9): 47–51.

A Method of Privacy Preserving and Access Control in Blockchain Based on Attribute-based Encryption

WANG Jinmiao[1,2], XIE Yongheng[1], WANG Guowei[3], LI Yiting[3]

(1. *Run Technologies Co., Ltd. Beijing, Beijing* 100192, *China*; 2. *Beijing Cyberspace Data Analysis and Applied Engineering Technology Research Center, Beijing* 100192, *China*; 3. *Beijing Municipal Bureau of Public Security, Beijing* 100055, *China*)

Abstract: All nodes in the blockchain keep the same information. With the wide application of blockchain technology, the problem of blockchain privacy protection and access control is becoming increasingly prominent. Based on multi-authority attribute-based encryption (MA-ABE), this paper proposes a privacy preserving and access control scheme for blockchain. The authorities are acted by the nodes in blockchain, which effectively solves the problem that the centralized authority is too large. By deploying the proposed scheme, data are encrypted by using MA-ABE and stored in the blockchain. Only users whose attributes meet the access control policy can decrypt the data

收稿日期：2020-7-16

基金项目：北京市青年骨干个人项目 [201800002685XG357]

作者简介：汪金苗（1987—），女，山东，博士，主要研究方向为数据安全与访问控制；谢永恒（1972—），男，湖北，高级工程师，硕士，主要研究方向为大数据分析与挖掘；王国威（1977—），女，北京，高级工程师，硕士，主要研究方向为信息安全；李易庭（1988—），男，山西，工程师，本科，主要研究方向为侦查学。

通信作者：汪金苗 jinmiao_wang@163.com