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

successfully, which achieves the purpose of privacy preserving and access control in blockchain.

Key words: access control; privacy preserving; multi-authority; blockchain; attribute-based encryption

0 引言

区块链是比特币的底层技术[1]。基于去中心化、不可篡改性、可追溯性等优势，区块链能够使互不信任的节点在不依赖第三方可信机构的情况下建立起点对点的可信价值传递，能够显著降低信任成本，提高交互效率。因此，区块链近年来在金融、供应链、医疗、电子取证等领域得到了广泛应用。

一方面，区块链不存在中心节点，系统中所有节点都保存相同的数据副本，共同维护数据的完整性，因此区块链能够有效避免集中式服务器单点崩溃的风险。但是，区块链中所有数据都公开给所有节点，也显著增加了隐私泄露的风险。另一方面，与传统数据类似，区块链中的数据需要灵活的访问控制。例如，在基于区块链的医疗系统中，病人佩戴的可穿戴设备将病人身体状况信息实时发布到区块链上，以便对病人身体状况进行监控。但病人身体状况信息属于敏感信息，只有授权的医生或护士才可以查看，因此需要对此类信息进行必要的安全防护并实施灵活的访问控制。虽然可以采用加密技术保护信息的安全性，但是传统加密机制只能进行一对一加密，即用一个公钥加密的信息只能用对应的私钥才能解密。因此，传统加密机制仅能保证信息的机密性，而无法实现灵活、细粒度的访问控制。目前，区块链中的隐私保护与访问控制问题仍面临着极大的挑战。

属性基加密方案（Attribute-based Encryption，ABE）的提出为隐私保护与访问控制的融合提供支持[2]。在ABE中，用户私钥和密文都与一组属性相关联，只有用户私钥中的属性与密文中的属性相匹配，用户才可以成功解密获取明文。初期的ABE方案大都由单一授权中心负责属性和密钥的管理和分发，为了避免单一授权机构权限过大所导致的安全隐患，多授权中心的ABE方案（Multi-authority ABE，MA-ABE）得到了广泛研究[3]。MA-ABE将密钥的计算交由多个授权中心完成，每个授权中心只负责部分密钥的计算工作，而看不到完整的用户信息，既提高了用户信息的安全性，又降低了单个授权中心的计算负担。

为解决区块链中的隐私保护与访问控制问题，本文提出基于MA-ABE的隐私保护与访问控制方案，其中的多个授权中心由区块链中的节点轮值担任。由于区块链不适合保存体积较大的文件，本文引入IPFS（Interplanetary File System）进行数据存储，仅将IPFS路径加密后保存在区块链中，可有效减轻区块链节点的存储负担。

1 相关研究

针对区块链中的隐私保护与访问控制问题，学者们开展了广泛研究。为了保证数据所有者能够控制数据的访问权限，ZYSKIND[4]等人提出基于区块链的个人数据管理系统，但该系统要求数据所有者与数据访问者必须同时在线。ES-SAMAALI[5]等人提出基于区块链的访问控制模型，利用区块链的去中心化实现分布式环境中的访问控制。OUADDAH[6]等人提出的FairAccess系统实现了基于区块链的分布式访问控制模型。RAHULAMATHAVAN[7]等人将区块链与ABE相结合，解决了区块链中的数据保护问题，实现了IoT系统中端到端的隐私保护。

为解决单一授权中心在安全性上所带来的问题，CHASE[3]提出多授权中心的ABE方案，能有效降低用户私钥泄露风险。JUNG[8]等人提出一种基于多棵访问树的多授权属性基加密方案，魏江宏[9]等人提出一种前向安全的属性基加密方案，王光波[10]等人提出一种基于属性基加密的云存储方案。然而，以上方案仍然需要中央授权中心完成一定的工作。为完全去除中央授权机构，CHASE[11]等人在文献[3]的基础上进一步改进，通过阻止授权中心之间互相沟通用户的属性信息，提出无中央授权机构的ABE方案。随后，学者们相继提出了

类似方案[12-14]，主要解决访问控制粒度粗、计算效率低下等问题。

2 具体方案

2.1 主要思路

2.1.1 MA–ABE 方案

与单一授权中心ABE不同，MA-ABE包含多个属性权威（Attribute Authority，AA），每个AA负责一部分属性对应私钥构件的生成，用户申请私钥时需要同时向多个AA申请，组合成最终私钥进行解密。这样就实现了去中心化，AA无须完全可信，没有任何一个AA可以生成完整的用户私钥。MA-ABE的具体算法如下所示。

1）初始化（Setup）。该算法以安全参数为输入，每个AA根据自己负责的属性集合生成公共参数PK_k与主密钥MK_k。其中，MK_k由AA_k秘密保管，每个AA发布的PK_k组成系统公共参数PK。

2）私钥生成（KeyGen）。该算法以PK、MK_k、用户属性策略T为输入，每个AA根据T为用户生成私钥构件，用户拿到所有AA生成的私钥构件后，计算出解密私钥SK_T。

3）加密（Encrypt）。该算法以PK、访问控制策略w、消息m为输入，输出密文C_w。

4）解密（Decrypt）。该算法以PK、SK_T以及C_w为输入，当且仅当w与T相匹配时，算法输出明文m。

初始化时，每个AA需要通过安全通道与其他AA协商两个AA之间的秘密参数。例如，AA_k与AA_j协商的秘密参数为$s_{kj}=s_{jk}$，作为主密钥的一部分由AA秘密保存。在私钥生成过程中，用户拿到所有AA生成的私钥构件后计算得出解密私钥，在该计算过程中，所有AA之间的秘密参数，即s_{kj}/s_{jk}等，将抵消掉。因此，用户解密私钥与AA之间的秘密参数没有关系，该特点将有助于区块链中灵活的AA选择。

为防止所有AA串谋生成解密密钥而解密密文，加密密钥由K_1和K_2两部分组成，K_1由数据所有者秘密分发给数据访问者，K_2用ABE加密，计算$K=K_1\otimes K_2$，利用K对数据进行加密。数据访问者访问数据时，首先从数据所有者那里获取K_1，如果其属性满足访问控制策略，则可以通过MA-ABE解密获得K_2，从而计算获得K实现数据解密。这样做的优势是：如果数据访问者不满足访问控制策略，则仅能获得K_1而不能获得K_2；即使全部AA串谋，也仅能获取K_2，而无法获得K_1。从而更大程度保护数据的安全性。

2.1.2 AA 的选择

基于股份授权证明（Delegated Proof of Stake，DPoS）共识机制，从区块链节点中选择一定数量的节点作为AA，具体选择方法如下：

1）根据业务需要，从所有节点中投票选出$2n$或$3n$（或者更多）个节点，其中n为需要的AA数量。本文假设选出$3n$个节点。

2）将$3n$个节点分成3组，分别为Nodes1、Nodes2、Nodes3，每组n个节点，分别承担n个AA的工作。例如，Nodes1中包含$\{Nodes1_1, Nodes1_2,\cdots, Nodes1_n\}$，$Nodes1_1$负责$AA_1$的工作，$Nodes1_2$负责$AA_2$的工作，以此类推。由此看来，每个AA的工作由3个节点负责，而这3个节点位于不同的组中。例如，AA_1的工作分别由$Nodes1_1$、$Nodes2_1$、$Nodes3_1$负责。

3）3组节点轮值为用户生成私钥，并设置有效期。首先，由Nodes1履行AA的职责，到达有效期后，Nodes2成为当值组。负责同一个AA工作的3个节点需要使用相同的公共参数和主密钥，除两个AA之间的秘密参数s_{kj}/s_{jk}外，其他公共参数与主密钥都由Nodes1生成，并通过安全通道分享给下一组负责同一个AA工作的节点。由于两个AA之间的秘密参数s_{kj}/s_{jk}不会对最终的用户私钥产生影响，这些参数由当值组的节点自行协商。

4）如果某个节点由于信誉等原因无法再承担AA的工作，则再次投票选举候补节点接替该节点的工作。候补节点当值时，从上一组承担相同AA工作的节点获取公共参数及主密钥，并与当值组中的其他节点协商秘密参数。

上述过程如图1所示。

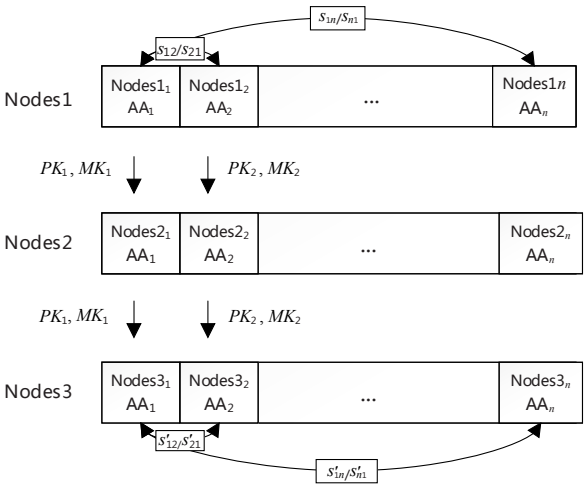

图 1 AA 选择示意图

数据访问者从所有 AA 获取私钥构件后，计算得到最终的解密私钥。只有使用从同一组当值节点获取的私钥构件才能够计算得出最终解密私钥，从不同组节点获取的私钥构件中的s_{kj}无法互相抵消，也就无法计算出最终解密私钥，这从一定程度上可以抵抗节点之间的串谋。

2.1.3 分布式文件存储

IPFS 是点对点的分布式文件系统，IPFS 不存在单点故障，各节点之间无须互相信任。从某种意义上说，对 IPFS 的使用类似于互联网的使用：当上传文件到 IPFS 系统后，将得到唯一的哈希字符串，利用该字符串可对文件进行检索。该哈希字符串可被认为互联网中的 URL，即文件的存储地址，也被称为“路径”。

在实际应用中，需要保护的文件通常体积较大。例如，病人的病历及检查结果通常包含图像文件。区块链要求所有节点都保存相同的副本，导致节点间的传输量以及节点的存储量较大，因此区块链不适合存储较大的文件。针对该问题，本文方案利用 IPFS 存储加密后的文件，仅在区块链中存储 IPFS 路径。IPFS 路径同样采用 ABE 加密，只有当数据访问者的属性满足数据所有者设置的访问控制策略时，数据访问者才可以解密存储在区块链中的 IPFS 路径，从而获得文件的存储地址，根据存储地址从 IPFS 中下载文件并解密。

2.2 具体设计

本文方案中，数据所有者发布数据、AA 向数据访问者发送私钥构件以及数据访问者访问数据均作为一条记录保存在区块链中。因此，区块链中的记录分为 3 种，即数据发布记录、私钥生成记录以及数据访问记录：

1）数据发布记录主要保存数据所有者发布的数据信息，包括数据 ID、数据发布者 ID、访问控制策略、发布时间、密文等。

2）私钥生成记录由每个当值 AA 分别发布，包括私钥构件 ID、AA 的 ID、数据访问者 ID 以及生成时间。为保护用户隐私，用户属性不保存在区块链中。

3）数据访问记录主要保存数据访问者对数据的访问信息，包括数据访问者 ID、数据 ID 以及访问时间。

本文方案的数据发布与访问流程如图 2 所示，具体分析如下：

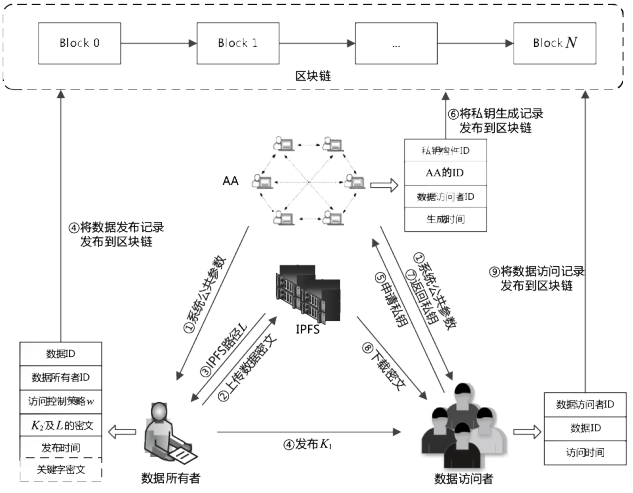

图 2 数据发布及访问流程

1）区块链节点投票选出至少一组轮值节点，由首批当值节点生成系统公共参数及主密钥。

2）数据所有者随机选择K_1和K_2，生成K，利用K对数据加密，将密文上传至 IPFS 系统，获得该密文的访问路径L；数据所有者制定访问控制策略w，利用w将K_2及L加密；数据所有者为该数据选择唯一 ID，并将数据 ID、数据所有者 ID、w、K_2和L的密文以及发布时间通过区块链中的“钱包”（Wallet）发送到区块链中。

在该步骤中，K_1由数据所有者通过安全通道分发给可能的数据访问者。此外，为便于数据访问者检索，可结合可搜索加密算法以及区块链检索技术，为密文

设置搜索关键字并加密，将关键字密文与其他内容一同发布到区块链中。

3）数据访问者向当值AA发起私钥生成请求。数据访问者利用自己的私钥将ID进行签名，并将签名发送给当值AA。当值AA收到私钥生成请求后，根据数据访问者ID查询其所具有的属性，根据其属性为数据访问者生成私钥构件，通过安全通道发送给数据访问者；同时将本次私钥生成信息，包括私钥构件ID、AA的ID、数据访问者ID以及私钥生成时间，通过“钱包”发布到区块链中。

4）数据访问者利用可搜索加密算法以及区块链检索技术检索需要访问的密文，利用私钥解密该密文。如果数据访问者的属性策略T与密文的访问控制策略w相匹配，则可解密获得K_2和L。数据访问者根据L从IPFS下载对应密文，利用从数据所有者那里获取的K_1，将K_1与K_2进行计算得到K，从而解密获得明文。一旦数据访问者成功解密ABE密文，数据访问者的“钱包”就将本次访问信息，包括数据访问者ID、数据ID以及访问时间发布到区块链中。

3 结束语

本文基于MA-ABE算法，提出区块链中的隐私保护与访问控制方案。由区块链中的节点轮值担任授权中心，更好地体现了区块链去中心化的特点，可有效解决单一授权中心权限过大所导致的安全隐患。通过将加密密钥拆分为两部分，可防止轮值授权中心串谋获取解密密钥，从而更大程度地保护数据的安全性。为减轻区块链节点的存储负担，采用IPFS保存数据本身，而将IPFS路径加密后保存在区块链中。本文方案中，只有属性满足访问策略的用户才能成功解密，其他用户均无法获得数据，从而实现了区块链中的隐私保护与访问控制。（责编 马珂）

参考文献：

[1] NAKAMOTO S. Bitcoin: A Peer-to-peer Electronic Cash System[EB/OL]. https://bitco.in/pdf/bitcoin.pdf, 2020-1-3.

[2] SAHAI A, WATERS B. Fuzzy Identity-based Encryption[M]// Springer. Advances in Cryptology – EUROCRYPT. Heidelberg: Springer Berlin Heidelberg, 2005: 457-473.

[3] CHASE M. Multi-authority Attribute-based Encryption[C]// Springer. The 4th Conference on Theory of Cryptography, February 21-24, 2007, Amsterdam, The Netherlands. Berlin: Springer-Verlag, 2007: 515-534.

[4] ZYSKIND G, NATHAN O, PENTLAND A S. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C]//IEEE. 2015 IEEE Security and Privacy Workshops, May 21-22, 2015, San Jose, CA, USA. NJ: IEEE, 2015: 180-184.

[5] ES-SAMAALI H, OUTCHAKOUCHT A, LEROY J P. A Blockchain-based Access Control for Big Data[J]. Journal of Computer Networks and Communications, 2017, 17(5): 137-147.

[6] OUADDAH A, ELKALAM A A, OUAHMAN A A. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT[M]//Springer. Europe and MENA Cooperation Advances in Information and Communication Technologies. Cham: Springer, Cham ,2017:523-533.

[7] RAHULAMATHAVAN Y, PHAN R C W, MISRA S, et al. Privacy-preserving Blockchain-based IoT Ecosystem Using Attribute-based Encryption[C]//IEEE. IEEE International Conference on Advanced Networks and Telecommunications Systems(ANTS), December 17-20, 2017, Bhubaneswar, India. NJ: IEEE, 2017: 1-6.

[8] JUNG T, LI Xiangyang, WAN Zhiguo, et al. Privacy Preserving Cloud Data Access with Multi-authorities[C]//IEEE. IEEE INFOCOM, April 14-19, 2013, Turin, Italy. NJ: IEEE, 2013: 2625-2633.

[9] WEI Jianghong, LIU Wenfen, HU Xuexian. Forward-secure Ciphertext-policy Attribute-based Encryption Scheme[J]. Journal on Communications, 2014, 35(7): 38-45.
魏江宏，刘文芬，胡学先 . 前向安全的密文策略基于属性加密方案 [J]. 通信学报，2014，35（7）：38-45.

[10] WANG Guangbo, WANG Jianhua. Research on Cloud Storage Scheme with Attribute-based Encryption[J]. Journal of Electronics & Information Technology, 2016, 38(11): 2931-2939.
王光波，王建华 . 基于属性加密的云存储方案研究 [J]. 电子与信息学报，2016，38（11）：2931-2939.

[11] CHASE M, CHOW S S M. Improving Privacy and Security in Multi-authority Attribute-based Encryption[C]//ACM. The 16th ACM Conference on Computer and Communications Security, November 9-13, 2009, Chicago, Illinois, USA. New York: ACM, 2009: 121-130.

[12] LIN Huang, CAO Zhenfu, LIANG Xiaohui, et al. Secure Threshold Multi Authority Attribute- based Encryption without a Central Authority[J]. Information Sciences, 2010, 180(13): 2618-2632.

[13] LI Xiehua, ZHANG Mengmeng, LIU Hong, et al. Multi-authority ABE for Access Control in Cloud Storage[J]. Journal of Hunan University(Natural Sciences), 2015, 42(10): 133-140.
李谢华，张蒙蒙，刘鸿，等 . 基于 MA-ABE 的云存储访问控制方法 [J]. 湖南大学学报（自然科学版），2015，42（10）：133-140.

[14] GUAN Zhitao, YANG Tingting, XU Ruzhi, et al. Multi-authority Attribute-based Encryption Access Control Model for Cloud Storage[J]. Journal on Communications, 2015, 36(6): 120-130.
关志涛，杨亭亭，徐茹枝，等 . 面向云存储的基于属性加密的多授权中心访问控制方案 [J]. 通信学报，2015，36（6）：120-130.