基于身份标识和区块链技术的粤港澳大湾区法人及其他组织跨境身份认证应用研究

黄润飞[1] 陈贤明[1] 黄燕玲[1] 陈树乐[2] 孙玉洁[2]

（1.广东省标准化研究院；2.广东省电子商务认证有限公司）

摘 要：针对目前粤港澳三地组织机构跨境身份认证机制不健全，传统身份认证体系认证过程复杂、证书维护管理困难等问题，本文提出了一种基于身份标识密码的联盟区块链跨境身份认证方案，通过利用组织机构编码这个身份标识信息代替数字证书进行身份认证和访问控制，在简化了认证过程、提高认证效率的同时，又避免了传统认证体系繁杂的证书管理。通过本文提出的认证方案，为推动粤港澳大湾区法人和其他组织实现身份互认、促进粤港澳大湾区法人和其他组织信息互联互通提供技术支撑，为国内经营主体进一步参与港澳的市场经济活动提供便利。

关键词：组织机构编码，跨境身份认证，身份标识，区块链

DOI编码：10.3969/j.issn.1674–5698.2023.08.008

Research on the Application of Cross Border Identity Authentication for Legal Persons and Other Organizations in the Guangdong-Hong Kong-Macao Greater Bay Area Based on Identity Identification and Blockchain Technology

HUANG Run-fei[1] CHEN Xian-ming[1] HUANG Yan-ling[1] CHEN Shu-le[2] SUN Yu-jie[2]

（1.Guangdong Institute of Standardization; 2.Guangdong Electronic Certification Authority Co., Ltd.）

Abstract: In response to the current issues such as inadequate cross-border identity authentication mechanisms for organizations in Guangdong, Hong Kong and Macao, as well as complex authentication processes and difficult certificate maintenance and management in traditional identity authentication systems, this paper proposes an alliance blockchain cross-border identity authentication scheme based on identity identification passwords. By using the identity identification information of organization codes to replace digital certificates for identity authentication and access control, the authentication process is simplified while improving authentication efficiency, it also avoids the complex certificate management of traditional authentication systems. The authentication scheme proposed in this article aims to provide technical support for promoting the mutual recognition of identities and the interconnection of information between legal persons and other organizations in the Guangdong-Hong Kong-Macao Greater Bay Area, and facilitate the further participation of mainland business entities in market economic activities in Hong Kong and Macao.

Keywords: organizational code, cross-border identity authentication, identity identification, blockchain

---

基金项目：本文受国家市场监督管理总局科技计划项目“粤港澳大湾区法人和其他组织跨境身份认证关键技术研究”（项目编号：S2022MK099）资助。

作者简介：黄润飞，硕士，信息标准化工程师，主要研究方向为统一社会信用代码信息应用。

0 引言

2019年2月份，中共中央、国务院印发了《粤港澳大湾区发展规划纲要》，提出要不断深化粤港澳互利合作，三地共同探索协同发展模式，实现粤港澳经营主体信息互通互认。2021年9月份，广东省人民政府发布《广东省深入推进资本要素市场化配置改革行动方案》，提到加速粤港澳大湾区金融市场互联互通，以区块链技术为基础，粤港澳共建“征信链”，促进粤港澳大湾区征信合作。粤港澳三地的融合发展都离不开经营主体的参与，由于港澳地区与内地制度不一致的原因，导致三地法人和其他组织登记管理模式、注册模式、数据采集定义等尚未达成统一标准，互认协商机制和数据共享机制尚未建立，阻碍了湾区三地经营主体身份的互通互认。

本文通过引入联盟区块链技术，以组织机构编码为基础，探索一种基于身份标识密码和联盟区块链技术的跨境身份认证机制，以推动粤港澳大湾区经营主体信息的互联互通，实现对三地经营主体身份信息的有效认证，为三地经营主体的互通合作提供支撑。

1 组织机构身份识别应用情况

统一社会信用代码是我国内陆地区法人和其他组织的“数字身份证”，具有唯一性，是经营主体身份信息的唯一识别码。自2015年国务院关于统一社会信用代码制度改革以来，我国建设完成了全国统一社会信用代码数据库，归集来自市场监督管理局、民政、编办、司法、总工会、民宗委等18个登记管理部门48个机构类型的经营主体数据，形成了完整、准确、权威、覆盖全面的组织机构数据服务中心。近年来，广东省以统一社会信用代码数据为基础，在多个应用领域持续开展了多项研究并取得了很好的成果[1]，港澳地区在金融、海关、电商等领域持续开展组织机构身份认证应用，不断推进可信数字身份的创新应用。

1.1 统一社会信用代码应用成果

（1）有效识别法人和其他组织机构身份信息

基于统一社会信用代码唯一标识的特性，对法人和其他组织机构信息进行核查校验，最终实现身份识别。目前，广东省在出入境备案审查、团员组织关系转接、虚假注册地址识别等应用中，充分发挥了统一社会信用代码对法人和其他组织机构身份进行有效识别的作用，根据法人和其他组织统一社会信用代码判断信息的真实性和有效性，准确识别身份信息，提升对法人和其他组织机构的管理效率。

（2）法人和其他组织机构信息关联比对分析

通过统一社会信用代码查询法人和其他组织机构的相关信息，核查比对数据的准确性，根据数据比对结果，对存在差异数据的法人和其他组织机构进行核实确认，甄别异常机构。基于统一社会信用代码数据的特性，广东省在金融领域已经有深入的探索应用，为银行等机构提供了稳定可靠的数据比对分析服务，提升了银行对公账户的管理效率，加强了金融机构防范风险的能力。

1.2 组织机构身份识别应用优势

（1）身份识别唯一标识

统一社会信用代码作为法人和其他组织机构的“数字身份证”，能够唯一且准确地标识身份信息。不同于数据的其他属性项信息内容，统一社会信用代码在数据库中是作为主键配置的，属性的配置决定了数据项的唯一性，不会出现字段数据重复的情况。一旦机构提交注册信息，登记管理部门配发统一社会信用代码后，这条数据就会及时生效，只要机构处于存续状态且未发生变更，该统一社会信用代码就会与机构进行绑定，通过代码就能准确识别到该机构。

（2）实现跨境信息连通

虽然港澳地区和内地的制度不一致，但对从事市场活动的法人和其他组织机构的管理手段都是通过组织机构编码进行识别和管理。我国内地的机构标识码是用18位阿拉伯数字或大写英文字母组成的统一社会信用代码表示，香港地区是16位的商业登记证编码，澳门地区则是7位的商业登记号[2]。数据结构的不一致会导致数据表示、标识规则、语义表达上出现差异，但是，通过对三地数据项进行合理地处理，比如：采用交集或并集，再根据语义分析对数据项进行转换，就可以构建粤港澳

三地都能识别的数据项，为湾区三地经营主体信息互通共享奠定基础，也可以作为打通港澳地区与内地经营主体之间活动的桥梁。

（3）便于跨境身份核验

在粤港澳大湾区三地法人和其他组织机构信息互通共享的基础上，通过建立大湾区经营主体身份信息互认机制，为三地经营主体进行商贸、文化等经济活动和社会活动提供便利。标识码是连接港澳地区和内地经营主体信息的纽带。通过对标识码的识别和验证，可以有效核验跨境经营主体的身份信息，即可以确保身份识别的准确性，又可以提高信息数据的安全性，为进一步促进跨境经贸活动，实现三地融合发展提供支撑。

2 身份认证技术

2.1 PKI认证

公开密钥基础设施（Public Key Infrastructure，PKI）是一套通过公钥密码算法提供安全服务的基础设施。PKI采用数字证书对公钥进行管理，通过第三方的可信任机构（CA），把用户的公钥和其他标识信息捆绑在一起，实现对用户身份信息的实效认证[3]。

在PKI身份认证体系中，为保证信息发送方能够正确获取接收方的公钥，需要一个可信的第三方机构（CA）来绑定实体与其拥有的密码对，CA只有在确认实体知道其公钥所对应的私钥后，才会为主体颁发证书，证书中包含了实体的标识信息、公钥以及CA的电子签名。信息发送方首先需要获得接收方的证书，在验证证书的合法性之后，信息发送方会通过证书中的公钥对信息进行加密并发送。发送方与接收方的交互过程如下。

Step1：接收方向CA请求证书；

Step2：CA接受请求并为接收方颁发证书；

Step3：接收方将证书中的公钥向发送方公开；

Step4：发送方获得接收方公钥后请求CA验证该公钥的合法性；

Step5：CA验证接收方证书并向发送方确认；

Step6：发送方用接收方的公钥加密信息并发送给接收方；

Step7：接收方用自己的私钥解密信息。

在PKI认证体系中，每一个主体都需要一个证书，当用户数量迅速增加时，证书的管理和维护将非常困难，同时，发送方在发送信息时首先需要获得接收方的证书，并请认证中心CA对证书的合法性进行验证，只有验证通过之后才会继续发送信息，导致了认证过程非常复杂。

2.2 基于联盟链的跨域身份认证

在基于联盟链的跨域认证模型中，不同区域的CA将各自信任域内的证书状态变更信息同步到联盟链上，不同域的实体通过联盟链进行身份验证[4]，基于联盟链的跨区域身份认证模型如图1所示。

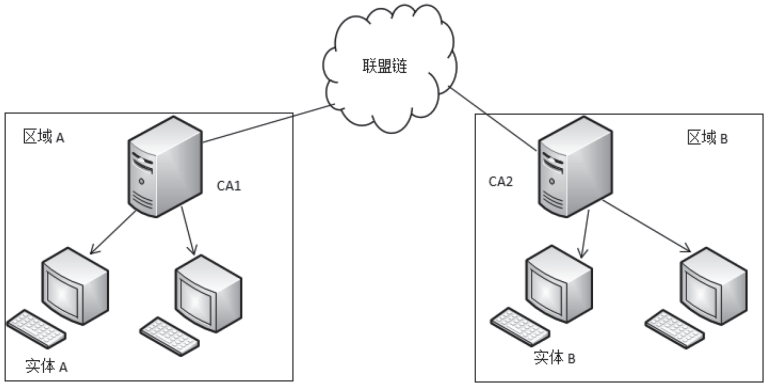

图1 基于联盟链的跨域身份认证模型

通过联盟区块链的方式，区域A中的实体要实现与区域B中实体的身份互认，只需要在联盟链上查找对方的当前CA证书状态信息，减少了CA证书的认证次数以及认证链路的复杂度，提升了跨域身份认证效率。

传统联盟区块链仍然是通过PKI实现各实体之间的访问控制。PKI通过认证机构CA提供安全服务，从而保障实体身份信息的可信任。由于存在CA单点故障问题，认证链路的稳定性得不到保障，同时，CA证书维护管理难的问题依旧存在。对于不同区域之间的实体，要实现跨域身份认证，就需要对不同的实体颁发不同的CA证书，也加大了跨域认证互联的难度。

2.3 基于标识密码的身份认证

基于标识密码（Identity Based Cryptography，IBC）的身份认证，通过将实体的身份标识信息与公钥进行绑定，每个主体的身份标识就是公钥[5]。2016年3月，国家密码管理局正式发布GM/T 0044–2016《SM9 标识密码算法》，SM9算法是一种基于标识的公钥密码算法，其中公钥数据就是可以唯一标识主体身份的信息，比如：电子邮件、电话号码等唯一属性都可以作为主体的公钥。

IBC通过将主体唯一标识属性作为公钥并公开发布，不需要额外生产和存储，可以不用依赖证书和证书管理系统，简化了认证过程和密码管理的复杂度，也有效解决了PKI身份认证需要大量交换数字证书的问题，提高了身份认证效率[6]。

主体根据IBC体系中公钥的唯一性，可以对数据进行签名，即“数字签名”，通过“数字签名”可以对主体的身份信息进行验证。比如：主体A将加密的身份信息发送主体B，主体B就可以根据该主体A的公钥对其身份进行验证（因为公钥是公开且唯一的，只有用公钥对应的私钥加密的信息才能用公钥解密）。IBC数字签名过程如下。

Step1：主体A用个人信息向密钥生产中心申请密钥对；

Step2：密钥生成中心为主体A分发密钥对；

Step3：主体A用私钥签名信息并发送给主体B；

Step4：主体B用主体A的公钥验证签名信息。

签名验证如图2所示。

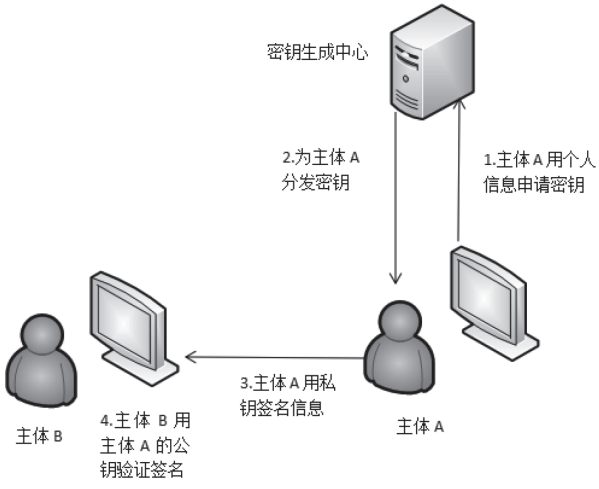

图2 基于标识密码的签名验证

3 法人和其他组织跨境身份认证

3.1 现状及问题

（1）组织机构数据异构

由于粤港澳三地法律制度差异性等原因，内地和港澳地区关于法人和其他组织机构的登记注册管理模式还没有统一，数据的采集定义也没有达成统一的标准，在推动实现大湾区互联互通、融合发展方面的探索，目前也只是处于初期阶段，还未形成统一协调发展的有效模式和典型经验。因此，要实现粤港澳大湾区法人和其他组织机构信息的互联互通，首先需要统一湾区三地组织机构身份标识的数据基础项，解决湾区三地组织机构标识长度不一致、信息语义表达存在二义性、数据差异性等问题。

（2）身份互认机制未建立

目前，关于粤港澳大湾区法人和其他组织的跨境身份认证机制一直处于待研究阶段，还未形成成熟、稳定的认证体系，这也就导致了湾区三地组织机构在跨境贸易活动中，会出现身份信息认证渠道不流畅、认证过程复杂困难、认证结果准确性得不到保证甚至认证失败等问题。因此，湾区三地法人和其他组织机构在开展跨境业务时，如何正确识别主体身份信息，有效构建身份认证体系，实现互通有无，就成为了一个关键问题。

3.2 基于身份标识和区块链的跨境身份认证

内地的组织机构统一社会信用代码和港澳地区的组织机构编码都具有唯一性，都能够唯一标识组织机构的身份信息。根据基于标识密码（IBC）的身份认证，可以将组织机构编码作为主体身份信息的唯一标识码，构建一种基于身份标识密码和联盟区块链的跨境身份认证体系[7]。在该体系中，密钥生成中心可以是联盟区块链中的任一节点，主体A向联盟链节点发出请求后，节点会确认信息并发放密钥对给主体A，其中公钥是主体A的身份信息和该节点的唯一标识信息（即机构编码）的拼接信息，私钥则是根据SM9标识密码算法计算生成，当主体A向节点发送交互请求时，只需用私钥签名并附上公钥、交互信息，节点就会对签名的合法性进行验证。主

体和联盟区块链节点的交互过程如下。

Step1：申请主体通过发送身份标识信息（机构编码）向联盟区块链节点请求密钥；

Step2：区块链节点审核主体身份信息后，将主体身份标识信息和本节点的自身标识信息（机构编码）拼接后形成公钥，同时根据SM9标识密码算法计算得到私钥，公钥私钥一同发送给申请主体；

Step3：申请主体获得密钥后，用私钥进行签名，随后将交互信息、公钥、签名信息一并发送给区块链节点；

Step4：区块链节点收到信息后对签名和身份标识进行验证，身份验证通过后接受申请主体的本次交互，完成对申请主体的身份认证。

在该认证过程中，区块链节点对每一次交互的密钥进行管理和配发，由于标识信息的唯一性，决定了每一次交互的对象都是特定的，区块链节点配发的密钥只能对本节点进行访问，节点对认证的申请主体身份有效性负责。

基于身份标识和联盟区块链的粤港澳大湾区跨境身份认证模型如图3所示。

其中，域代理服务器用于维护管理本地主体身份标识信息（机构编码）并同步到联盟链，在该模型中，广东的主体请求香港主体进行认证，香港主体通过联盟链获得广东主体的标识信息后形成密钥发送给广东主体，并根据上述主体和联盟区块链节点的交互过程完成身份认证。

该模型在不需要任何数字证书的情况下就能对发起方的身份进行认证，即完成了对发起方的访问控制，又解决了PKI体系证书管理难的问题。

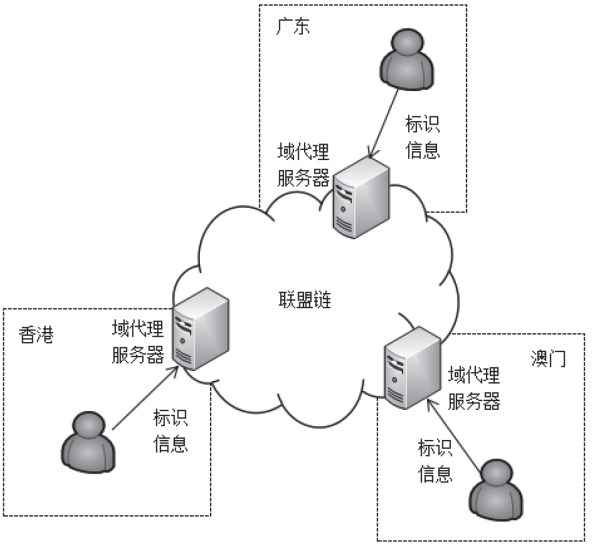

图3 基于身份标识和区块链的跨境身份认证

4 结 语

本文从技术应用层面提出了一种基于身份标识和区块链的粤港澳大湾区法人和其他组织跨境身份认证方案，通过组织机构编码唯一性的这个属性特点，结合区块链去中心化、可追溯、不可篡改等技术特点，以解决湾区三地主体跨境身份认证难等问题。通过本文提出的跨境身份认证方案，可以优化解决传统认证体系证书维护管理成本高、认证效率低等缺点，为实现湾区三地经营主体自由便利往来提供技术支持。本文的认证方案是基于现有技术的基础上提出来的，仍然需要进一步的深化研究，特别是对加密算法的优化。同时，随着相关技术的不断迭代更新和新技术的不断涌现，跨境身份认证的应用研究将会更加成熟、全面和高效。

参考文献

[1] 陈贤明,高丽涛,覃震宇,等. 基于广东组织机构数字证书的网上办事大厅身份识别技术研究[J]. 标准科学, 2015(2):94–96.

[2] 陈贤明,黄润飞,黄燕玲. 粤港澳大湾区市场主体身份信息共享机制研究[J]. 中国标准化, 2021(18):25–29.

[3] 陈立全,李潇,杨哲懿,等. 基于区块链的高透明度PKI认证协议[J]. 网络与信息安全学报, 2022(4):1–11.

[4] 黄逸翔,王亚威,陈文轩,等. 基于联盟链的PKI跨域认证模型[J]. 计算机工程与设计, 2021(11):3043–3051.

[5] 姚英英,常晓林,甄平. 基于区块链的去中心化身份认证及密钥管理方案[J]. 网络空间安全, 2019,10(6):33–39.

[6] 黄仁季,吴晓平,李洪成. 基于身份标识加密的身份认证方案[J]. 网络与信息安全学报, 2016,2(6):00047–1–00047–6.

[7] 邱炜伟,李伟,梁秀波,等. 一种基于身份标识密码的联盟区块链访问控制方法[P]. CN201811636140.2,2019,5.