计算机科学
COMPUTER SCIENCE

一种基于区块链的身份鉴证与授权机制

林飞龙，岳跃栋，郑建辉，陈中育，李明禄

引用本文

林飞龙，岳跃栋，郑建辉，陈中育，李明禄.一种基于区块链的身份鉴证与授权机制[J]．计算机科学, 2023, 50(6A): 220700158-9.

LIN Feilong, YUE Yuedong, ZHENG Jianhui, CHEN Zhongyu, LI Minglu. Blockchain-based Identity Authentication and Authorization Mechanism [J]. Computer Science, 2023, 50(6A): 220700158-9.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220700158

一种基于区块链的身份鉴证与授权机制

林飞龙　岳跃栋　郑建辉　陈中育　李明禄
浙江师范大学数学与计算机科学学院　浙江 金华 321004

摘　要　身份信息滥用是社会顽疾问题。文中提出了一种基于区块链的身份鉴证与授权(Blockchain-based Identity Authentication and Authorization,BIAA)机制,该机制要求用户主体在对业务进行身份授权时提供有效身份证件和生物特征信息,确保业务为本人授权;同时将业务信息及身份授权写入区块链账本,进一步实现业务的安全存证与可追溯。为构建该机制,提出了"身份注册-身份授权"星形多区块链架构,身份注册链采用可控联盟链方式,由身份管理权威机构对身份信息注册实施管理,并提供身份鉴证服务;身份授权链可由各行业在获得权威机构许可后构建,其提供的相应业务在身份鉴证确认后,与身份授权信息写入身份授权链。在技术实现上,设计了一个身份注册-鉴证-授权(Identity Register-Authenticate-Authorize,IRAA)终端,将用户生物信息和身份证件信息读取后利用哈希运算转化为密文,确保用户明文信息不上线;设计了身份鉴证协议,实现身份鉴证链为各身份授权链提供身份鉴证服务,协议过程以密文形式进行;设计了身份授权通用智能合约,实现对应用业务的身份授权管理与存证。最后利用二代身份证和指静脉纹作为身份信息构建了原型系统,验证了 BIAA 机制的安全性、可行性与有效性,为解决身份信息滥用问题提供有价值的参考。

关键词:身份信息安全;身份鉴证;身份授权;区块链;智能合约
中图法分类号　TP309

Blockchain-based Identity Authentication and Authorization Mechanism

LIN Feilong,YUE Yuedong,ZHENG Jianhui,CHEN Zhongyu and LI Minglu
College of Mathematics and Computer Science,Zhejiang Normal University,Jinhua,Zhejiang 321004,China

Abstract　The abuse of people's identity information is a serious problem in nowadays society. In this paper,a blockchain-based identity authentication and authorization(BIAA) mechanism is proposed. BIAA requires users to provide the effective identity certificate and biological feature to authorize the business,to ensure that the business is authorized by the user. Then,the identity authorization together with the business contract will be written into the blockchain ledger with the secure and traceable manner. To fulfill BIAA,a stellate multi-blockchain structure is proposed for identity register and authorization. An identity register blockchain is built using consortium blockchain which is maintained by authorities to manage the identity registration. It also charges to identity authentication. Multiple identity authorization blockchains can be built with the permission from identity register blockchain. Each identity authorization blockchain can be maintained by a business sector and write the business contracts with identity authorizations into the blockchain ledger. For technical implementation,an identity register-authenticate-authorize (IRAA) terminal is designed. It transforms the identity and biological feature into ciphertext by hash function,thus to guarantee the identity information offline and secure. It is also embedded with the protocol to deal with the identity authentication in an encrypted way. IRAA terminal also charges to sign the business contract using digital signature and thus finish the identity authorization. Finally,a prototype system leveraging second-generation identity certificate and finger vein pattern as identity information is built,which verifies the security,feasibility,and effectiveness of BIAA mechanism and provides a valuable reference for solving the abuse of identity.

Keywords　Identity information security,Identity authentication,Identity Authorization,Blockchain,Smart contract

1　引言

身份信息是人的基本社会属性,大部分社会业务的办理都需要个人身份信息授权来确认业务的有效性和合法性,如银行业务、社保业务、城市服务业务等。许多社会业务在其提供服务时,需要客户提供身份信息复印件作为用户身份的

基金项目:国家自然科学基金(62273310);浙江省自然科学基金(LY22F030006)
This work was supported by the National Natural Science Foundation of China(62273310) and Natural Science Foundation of Zhejiang Province,China(LY22F030006).
通信作者:林飞龙(bruce_lin@zjnu.edu.cn)

凭证，并将复印件留存。身份信息的扫描件或复印件，可以再进行无限制复制，导致个人信息不安全；甚至为不法分子利用，在未经个人同意的情况下，利用其身份信息办理某些业务，损害身份信息所有者的利益，甚至造成更严重的问题[1-2]。另一方面，也有某些不法个人通过使用个人信息获得不法利益，却拒绝承认不法行为，为社会治理带来了障碍以及高额的成本。随着社会的发展，业务类型急剧增加，个人身份信息使用越来越频繁，其安全问题已经成为社会治理中一个刻不容缓的问题[3-4]。

本文认为，身份信息安全问题的根源在于缺乏安全可靠的身份信息授权管理机制。目前，身份信息授权记录由业务提供方保留，身份信息的安全也就依赖于业务提供方及其安全措施。大量的社会业务导致个人身份信息分散在大量的业务提供方中，且业务提供方对安全的认识以及安全措施的配备参差不齐，这很容易导致个人对身份信息失去控制。一旦身份信息被泄露，个人甚至无法确定是哪一个业务方泄露的。如若由于身份信息泄露导致个人损失，也无法拿出证据维护自己的合法权益。现在社会体系中，亟需有一种机制或技术手段，实现有公信力的、安全可靠的、可追溯验证的身份信息授权记录，一方面要求身份使用授权是有效的、保密的；另一方面要求身份使用授权记录是可靠的、可验证的。

最近受到广泛关注的区块链[5]是一种新的分布式一致性技术协议。区块链综合了分布式网络技术和非对称密码学技术，实现了数据账本的分布式一致性存储，并且确保数据账本的不可篡改、不可销毁、不可抵赖等良好性质[6]。区块链技术将其所记录的信息按照发生时间顺序进行保存，数据账本由网络中各个节点用户进行冗余保存。使用数字签名等技术，确保账本中的信息仅信息相关方可解密，且其他用户可以通过区块链网络验证信息的有效性和正确性[7]。区块链的技术特点与优势，为身份信息授权管理提供了思路。利用区块链技术，可以设计公开的、安全可靠的、可验证的身份信息授权。使用区块链数据账本的优势在于：1）区块链分布式一致性技术易于实现社会业务中身份授权信息的收集与存储，且便于个人查询身份信息的使用状况；2）通过签名技术，可实现在未经个人许可的情况下，业务方不能使用个人身份信息，即或使用，也容易证明是非本人授权的，不被认可；3）在发生纠纷时，区块链所记录的授权信息可为公安、法院等社会治理机构提供有力证据，利于公正解决纠纷。

基于上述考虑，本文提出了一种基于区块链的身份鉴证与授权机制（Blockchain-based Identity Authentication and Authorization，BIAA），将身份信息授权行为转移到区块链上进行，使用区块链技术保证个人身份信息授权记录的一致性、安全性以及可验证性。本文工作具有如下创新和贡献点：

（1）提出了一种基于区块链的身份鉴证与授权机制。该机制采用“身份注册-身份授权”星形多区块链架构，身份注册链采用可控联盟链方式，由权威机构对身份信息注册和鉴证实施管理；身份授权链可由各行业在获得权威机构许可后构建，其提供的相应业务在身份鉴证确认后，与身份授权信息一起写入身份授权链进行存证。

（2）技术实现上，设计了一个身份注册-鉴证-授权（Identity Register-Authenticate-Authorize，IRAA）终端，读取用户生物信息和身份证件信息后利用哈希运算将其转化为密文，确保用户明文信息不上线；设计了身份鉴证协议，实现身份鉴证链为各身份授权链提供身份鉴证服务，协议过程以密文形式进行；设计了身份授权通用智能合约，实现对应用业务的身份授权管理与存证。

（3）利用二代身份证和指静脉纹作为身份信息构建了原型系统，验证了所提出的基于区块链的身份鉴证与授权机制的安全性、可行性与有效性，为解决身份信息滥用问题提供有价值的参考。

本文第2节对相关工作以及区块链技术进行了介绍；第3节介绍了基于区块链的身份鉴证与授权机制工作原理和系统构成；第4节详细给出了系统的设计；第5节通过构建原型系统对本文方案进行验证与分析；最后总结全文。

2 相关工作

2.1 身份信息安全

由于身份信息是人类基本社会属性，其安全性受到各行各业的共同关注[8-10]。诸多传统业务都是通过身份证件（如身份证、户口本、护照等）来确认用户身份，保存身份证件的纸质或者电子图像作为业务授权凭证。进入数字化时代，账号加口令、数字证书加私钥成为主流的两种数字身份安全管理技术。许多工作都致力于提供更高级别的个人身份信息安全保护。

在身份信息安全技术方面，文献[11]建议将生物特征作为身份信息的组成部分，因为来自人体本身的生物特征信息，比身份证件、数字证书等更可靠地关联到每个人。文献[12]利用心理测试方法，检测登陆社交网络的用户是否是身份冒充者，并利用机器学习手段，建立心理特征模型，实现对用户身份的智能识别。类似地，借助对用户的性别、教育背景、技术专长、社会声誉等信息的综合判断，可以实现社交网络中用户的真实性判断[10]。在数字化身份安全中，文献[13]提出一种两方共同生成签名的机制，将基于身份信息生成的私钥存储于两个设备中，由两个设备在不泄露私钥的前提下合作完成数字签名，该方法可以有效解决私钥泄露问题。数字证书机制在身份安全方面具有良好的安全性，但是在应用中需要建立和维护一个公钥基础设施（PKI），产生了额外的代价。因此在应用中，基于身份信息解决该问题的公钥技术和密钥协商机制也很受欢迎[14]。文献[15]提出一种基于身份信息的轻量级密钥协商机制和身份认证协议，采用椭圆曲线生成公私钥对，实现对数据的加密和签名。文献[16]对内积函数加密方案进行研究，提出了一种基于身份的可验证密钥的内积函数加密方案。针对多方交互，文献[17]和文献[18]分别研究了分簇网络环境下两层身份鉴证与数据安全机制和信息广播环境下的身份匿名与数据安全机制。

在身份信息安全防护应用方面，在当下的5G移动通信网络中，采用移动用户身份识别码和国际移动设备标识码对用户和设备进行识别，并利用内置在用户身份模块中的密钥算法进行接入安全管理，实现接入安全控制、数据加密及完整性、用户身份鉴证等管理[19]。面向物联网安全，文献[20]

提出了一种弱身份机制，使得物联网终端设备与用户的关联性减弱，例如尽量减少终端设备的命名、地址等涉及用户信息的属性，从而降低设备的可识别度，加强物联网的隐私保护。在云服务网络中，文献[21]通过基于身份的机制对云数据进行所有权的确权，并实现用户在数据共享时的匿名隐私安全。在移动边缘计算中，文献[22]提出了一种轻量级的匿名密钥协商协议，实现用户的匿名以及不可追踪，仅通过一轮信息交换即可完成一致密钥协商。在身份管理领域，文献[23]提出一种新的多目标身份管理算法，同时跟踪杂波中未知且时变的目标数目，并随着时间的推移高效地管理目标的身份。文献[24]针对现有身份管理安全隐患，提出一种使用智能合约的跨域自主权身份管理方案，有效地降低了传统身份管理方法的中心化服务器易泄露隐私的风险。基于身份的安全机制，还在车联网[25]、智能电网[26]、工业网络[27]等领域都有广泛的应用。

2.2 基于区块链的身份信息安全方案

区块链技术与密码学深度融合，在处理身份信息安全和存证方面有良好的技术优势。因此，区块链环境下的身份信息安全与应用也受到了广泛重视[28-29]。

联盟链代表性技术超级账本（Hyperledger）给出一种数字身份解决方案，即 Hyperledger Indy[30]。它提出了一种理念，将与个人身份相关的所有信息都汇聚成个人身份的属性（如出生信息、家庭住址、毕业证书、工作履历等），实现个人身份信息的数字化，并通过区块链技术确保身份信息的可信性并具有其他区块链技术的优点。文献[31]提出一种基于区块链的身份管理机制，在系统中用户自己生成身份信息及保护身份信息的公私钥对，然后将身份信息加密后存入区块链账本中，用于身份信息的鉴证。面向区块链账本信息透明存储带来的身份信息泄露问题，文献[32]利用零知识证明算法，设计了基于身份属性的数字身份安全机制，实现可控的身份信息安全。基于该机制，用户可以根据应用需求披露部分身份属性，但依然可以确保身份信息安全。在应用方面，面向物联网节点身份管理安全需求，文献[33]构建了混合区块链架构，实现多个物联网的安全身份管理，每个物联网维护一个本地区块链，负责网络内节点的身份认证与管理；各个物联网的基站或汇聚节点共同维护一个公共区块链，实现跨网络的身份鉴证与应用背书。文献[34]则基于区块链技术设计了轻量级的物联网用户身份认证与鉴证服务协议。在高速移动的车联网中，文献[35]给出了基于区块链的用户接入鉴证和用户撤销机制，利用区块链的快速共识和存证机制，实现高效实时的车联网用户身份动态管理。面向跨链身份认证，文献[36]提出了基于中继链的 IBE 的跨链身份认证方案，采用数字身份 ID 作为全局标识符，完成跨链交易的身份认定。文献[37]提出一种面向跨链系统的用户身份标识认证模型，引入椭圆曲线加密算法和零知识证明，实现跨链身份标识注册、更新以及认证，为用户的跨链访问、通信提供可信身份认证服务。

本文拟在已有研究工作的基础之上，结合区块链技术，确保身份信息授权为本人所为，以解决身份信息授权的安全和可信问题。Ren 等在文献[38]中初步提出了通过身份信息的注册和鉴证，加强身份授权的可信与安全。本文将进一步明确概念，采用新的技术路线，给出更通用的技术方案，设计并开发原型系统进行详细测试。

3 解决方案

3.1 系统架构

本系统构建了两种类型的数据账本，一种是身份注册链，提供身份鉴证服务，该链是权威且唯一的；另一种是身份授权链，该区块链由应用行业或联盟向权威机构申请后创建，记录应用行业发生的业务合约及相应的身份授权信息，身份授权过程需要向身份注册链申请身份鉴证服务。为了确保身份授权是身份信息持有者本人所为，本方案将身份信息与生物特征信息（如指纹、虹膜、指静脉等）进行绑定，只有身份信息与生物信息正确匹配时，才能对业务进行授权签名。

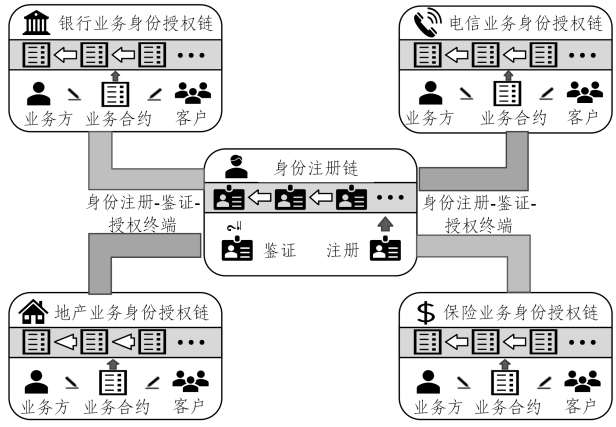

图 1 基于区块链的身份鉴证与授权机制示意图

Fig. 1 Schematic diagram of identity authentication and authorization mechanism based on blockchain

身份注册链和身份授权链构成了“身份注册-身份授权”星形多区块链架构，基于该架构的解决方案具备良好的可扩展性和安全性。身份注册链负责身份信息注册和鉴证服务及安全，不同行业维护独立的身份授权链，为应用带来灵活性的同时保证业务之间的安全隔离。以下对两类区块链，以及身份注册-鉴证-授权终端（本文系统方案中重要的一个组成）分别进行介绍。

3.1.1 身份注册链

身份注册链负责身份信息的注册服务和身份授权时的鉴证服务。该链采用联盟区块链方式，各地区管理身份信息的权威机构（如我国各地公安局）共同维护身份注册联盟链。考虑到身份信息隐私与安全，身份注册链的区块账本中存证的是身份信息和生物特征信息的哈希摘要。在注册和授权应用过程中，身份信息和生物特征信息均不暴露在线上，其技术实现将在后续章节中介绍。

身份注册链的安全性极为重要，因此，普通身份信息注册用户和各行业授权链请求身份鉴定的用户，其权限是严格限制的，只提供相关的请求和查询服务，不能作为身份注册/鉴证链账本冗余存储节点。

由于身份注册链采用联盟链形式，分布在各地区的节点均可提供身份注册和鉴证服务，如此可以有效提升服务的稳定性。

3.1.2 身份授权链

身份授权链由各应用行业或联盟创建，负责业务合约的存证。业务提供方和用户发起一项业务，在对业务条款达成一致后，需要双方或多方一起签署合约。各合约方均要进行身份鉴证与授权。在本方案中，各方只有提供正确的身份信息和生物特征信息才能通过身份鉴证。鉴证通过后，将业务合约信息和身份授权信息一起封装写入身份授权通用智能合约，并实现上链存证。身份信息授权以及通用智能合约的实现将在后续章节中介绍。

考虑到需要向身份注册链申请身份注册或鉴证服务，身份授权链需要向身份注册链进行备案或许可申请。

身份授权链于区块链的形式没有严格限定，可以是公有链、联盟链和私有链中的任意一种。考虑到业务信息的安全性和可信赖性，联盟链是更加合适的技术方案。

3.1.3 身份注册-鉴证-授权终端

身份注册-鉴证-授权（Identity Register-Authenticate-Authorize，IRAA）终端是 BIAA 系统的重要组成部分，实现身份和生物特征信息明文的离线保护，确保系统安全。其主要功能是：1）对身份信息和生物特征信息进行哈希变换，生成相关信息的哈希摘要；2）利用身份信息的哈希摘要作为种子随机数，生成用户公私钥对；3）完成信息加密和数字签名功能。该终端的提出，一方面可以保障用户身份和生物特征信息安全，另一方面可以免除用户因需要保护私钥而带来的各种困扰。终端的详细设计将在 4.1 节给出。

3.2 工作流程

依据业务逻辑，将基于区块链的身份信息鉴证与授权工作流程分为 4 个步骤，如图 2 所示。

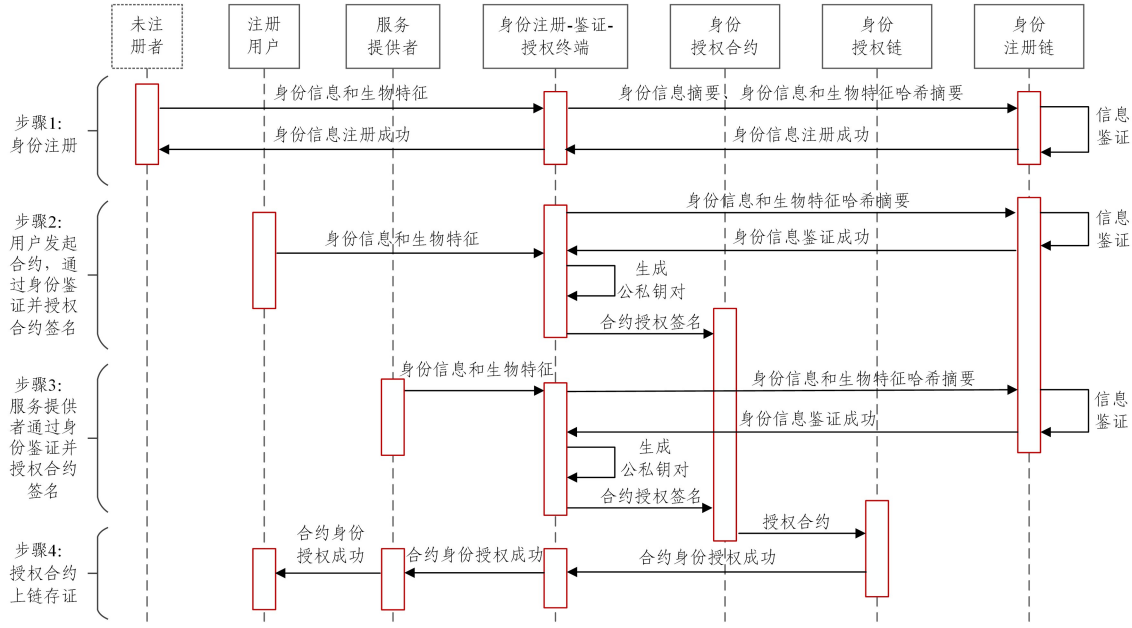

图 2 身份信息注册、鉴证、授权流程图

Fig. 2 Flow chart of identity information registration, authentication and authorization

步骤 1 身份注册：参与 BIAA 系统首先要进行用户注册。IRAA 终端读取待注册用户的身份信息和生物特征信息，将身份信息以及身份信息与生物特征的合并数据分别进行哈希运算；调用身份信息注册智能合约，将上述两项哈希摘要发送给身份注册链；身份注册链中的权威节点对身份信息进行验证，如果验证所提交身份信息是合法发放的身份信息，则将身份信息和生物特征合并数据的哈希摘要作为身份注册链中的有效注册身份，该注册合约写入区块链账本中。用户可以利用 IRAA 终端在身份注册链中查证是否成功注册。考虑到身份链的权威性和其安全的重要性，在应用实施时，可由权威机构提供身份注册服务，并保证身份信息的真实性。

步骤 2 用户对业务合约授权签名：注册用户要对合约进行授权签名，首先通过 IRAA 终端读取身份信息和生物特征信息，并计算其哈希摘要；IRAA 终端将摘要信息发送给身份注册链进行身份鉴证，如果该信息已在身份注册链账本中存证，则返回鉴证成功，否则鉴证失败并反馈身份信息无效或未注册；如果身份信息鉴证成功，则利用上述哈希摘要作为随机数，生成用户的公私钥对；将业务信息封装进身份授权合约，并对合约进行数字签名。

步骤 3 服务提供方对业务合约授权签名：在确认用户身份授权有效后，代表业务提供方的业务经理也要对业务进行身份授权和数字签名，以确保业务双方都进行了有效授权。服务提供方的身份授权和签名过程与步骤 2 类似，这里不再赘述。

步骤 4 身份授权合约写入身份授权链：业务双方身份授权完成后，将带授权信息的合约发送到身份授权链，经过身份授权链共识过程对相关信息进行验证并写入身份授权链账本。业务双方可以通过查看合约是否成功写入账本来确认业务存证与否。

4 系统设计

本节将给出 BIAA 系统各主要模块的详细设计。系统设计所涉及的主要符号及其释义如表 1 所列。

表1　主要符号及其释义

Table 1　Principal symbols and their definitions

符号	释义
ID	Identity，身份信息明文
BF	Biological feature，生物特征
u	ID 的哈希值
v	ID 和 BF 合并后的哈希值
w	ID 和 BF 合并后的二次哈希值
T	表示业务合约
PK	公钥，本文采用 RSA 算法生成，$PK=(n,e)$
SK	私钥，本文采用 RSA 算法生成，$SK=(n,d)$
T^{sign}	表示对 T 的数字签名
C	合约各方签名后封装成的智能合约
T'	根据数字签名验签算法得到的合约信息

4.1　IRAA 终端

IRAA 终端主要有 3 部分功能：读取用户身份信息和生物特征信息并通过哈希变换隐藏身份和生物特征明文信息，执行身份注册或者身份鉴证，基于哈希摘要生成用户公私钥对并对合约进行签名授权。该终端不输出用户身份信息和生物特征信息的明文，保障用户信息安全。

用 ID 和 BF 分别表示用户的身份信息(Identity)和用户的生物特征(Biological Feature)，用 u,v,w 分别表示 ID 的哈希摘要、ID 与 BF 合并后的哈希摘要，以及 ID 与 BF 合并后的两次哈希摘要，即：

$$u=\text{hash}(ID) \tag{1}$$

$$v=\text{hash}(ID\cup BF) \tag{2}$$

$$w=\text{hash}(\text{hash}(ID\cup BF)) \tag{3}$$

其中，hash 表示哈希运算，$\cup$ 表示数据合并操作。

接下来，基于生成用户公私钥对，本文利用 RSA 算法生成用户公钥 PK 和私钥 SK：

(1)随机选择两个较大的质数 p 和 q，且 $p\neq q$。令 $n=p\times q$，计算 n 的欧拉函数：

$$\varphi(n)=(p-1)\times(q-1) \tag{4}$$

(2)将 v 通过 ASCII 码转换为二进制序列，即：

$$v^a=\text{ASCII}(v) \tag{5}$$

其中，ASCII(·)表示取 ASCII 码操作，并对 v^a 做如下处理：

$$v^b=\left\lceil\frac{v^a}{\varphi(n)}\right\rceil+\text{mod}(v^a,\varphi(n)) \tag{6}$$

其中，$\lceil\cdot\rceil$ 表示向上取整，mod 是求余函数。

(3)寻找质数 e，e 为大于等于 v^b 的第一个质数。

(4)计算 e 对 $\varphi(n)$ 的模反元素 d，即满足：

$$\text{mod}(e\times d,\varphi(n))=1 \tag{7}$$

式(5)可用扩展欧几里得算法求解。基于上述计算，所得公私钥分别为 $PK=(n,e)$，$SK=(n,d)$。

本文对 RSA 算法进行了适应性修改，将质数的获得通过第 2 和第 3 步与用户的身份信息和生物特征信息关联起来，即完成通过用户的身份信息和生物特征信息生成公私钥对。只要用户通过身份注册，鉴证终端就可以生成确定性的公私钥对，该方法既可以免除用户保存私钥的麻烦，也避免了私钥泄露导致的信息安全隐患。

RSA 公钥算法依赖于大数的质数分解，目前具有很高的安全性。在应用中，建议使用 1 024 比特位的密钥，可确保系统的高安全性。当然，本文方案中也可以使用椭圆曲线法等替换 RSA 来生成公私钥对，这里不再赘述。

4.1.1　身份注册

用户通过 IRAA 终端进行注册，终端调用身份注册合约将 u 和 w 送给身份注册/鉴证链，负责维护身份注册链的权威机构对用户身份信息进行审核。为了确保身份注册的真实性和安全性，权威机构需要对注册信息进行严格审核，如果审核通过，则将身份注册合约(包含 u 和 w)写入身份注册区块链账本中。一旦身份注册信息被写入账本，则表示身份注册成功。如果存在特殊情况导致原先的生物特征发生变化，可以申请重新注册。重新注册审核通过后，将在身份注册/鉴证链生成新的身份注册记录，并标注之前的注册记录无效。

4.1.2　身份鉴证

在进行身份授权之前，需要通过 IRAA 终端对身份进行鉴证。终端读取用户身份信息和生物特征信息，进一步得到哈希摘要 u 和 w。接着，调用身份鉴证合约，将 u 和 w 发送给身份注册链进行鉴证。如果在身份注册链中存在一致的注册记录 u 和 w，则表示该身份信息为有效注册信息，同时通过身份信息和生物特征的双重验证，确保是用户本人进行身份授权，允许进一步的授权操作。如果不存在 u 和 w，则提醒用户先进行身份注册；或存在 u 但不存在 w，则提示身份信息已注册，生物特征信息校验错误，拒绝进一步的授权操作。身份授权及数字签名相关操作将在下一节中介绍。

4.2　身份授权通用智能合约

将 3.2 节工作流程中的步骤 2－步骤 4 步均看作是身份授权合约的操作。进一步，i 表示业务用户，j 表示业务提供方，双方的公私钥 $\{PK_i,SK_i\}$ 和 $\{PK_j,SK_j\}$ 已通过 4.1 节提供的算法得到。用 T 表示双方制订的业务合约，考虑到合约信息安全需求，T 也可以是加密的合约信息或者合约的哈希摘要，本文统一用 T 表示。根据操作需求，合约及其身份授权相关算法如下。

(1)合约签名

合约双方利用各自的密钥进行数字签名.将合约信息 T 发送给 IRAA 终端，由 IRAA 终端对合约进行签名。$SK_i=(n,d_i)$ 和 $SK_j=(n,d_j)$ 分别是合约双方的私钥，由 IRAA 终端根据身份信息和生物特征信息生成。根据 RSA 数字签名算法，合约双方签名如下：

$$T_i^{\text{sign}}=\text{mod}(T^{d_i},n) \tag{8}$$

$$T_j^{\text{sign}}=\text{mod}(T^{d_j},n) \tag{9}$$

其中，T^{d_i} 表示 T 的 d_i 次幂，T^{d_j} 同理。

将合约双方身份和生物特征信息的哈希摘要 v_i 和 v_j、双方公钥 $PK_i=(n,e_i)$ 和 $PK_j=(n,e_j)$、双方签名封装进区块链智能合约，即：

$$C=T\cup v_i\cup v_j\cup PK_i\cup PK_j\cup T_i^{\text{sign}}\cup T_j^{\text{sign}} \tag{10}$$

所形成的智能合约 C，即可发送到用户所在联盟的身份授权链，进行合约验证与共识，以及上链存证。

上述签名方法还可以灵活推广到多重签名的智能合约中。当然，也可以采用更加复杂的安全多方签名等技术，来改进如签名文件大小、签名安全等性能。

(2)合约验证

经合约各方签名后封装的智能合约 C 将被发送至身份授权链进行验证和区块链共识。身份授权链上的节点均可以对提交到网络上的智能合约进行验证。合约验证分为用户

身份验证、公钥验证、签名验证 3 步。以下以验证用户 i 为例，用户 j 的验证同理可得。

第 1 步 从智能合约 C 中提取用户身份和生物特征信息的哈希摘要 v_i，经由身份注册链提供的查证服务，确认是否存在一个注册记录 w 与二次哈希值 hash(v_i) 一致。如果存在，表示该用户身份是注册有效的。

第 2 步 将 v_i 代入式(5)获得 v_i^a，进一步代入式(6)获得 v_i^b，接着验证用户公钥 PK_i 中的 e_i 是否是满足大于等于 v_i^b 的第一个质数。如果是，说明用户的公钥是由身份和生物特征的哈希摘要生成而来的，公钥验证通过。

第 3 步 利用公钥 PK_i 验证数字签名，即：

$$T_i' = \mathrm{mod}((T_i^{\mathrm{sign}})^{e_i}, n) \tag{11}$$

如果验签得到的 T_i' 与 C 中封装的原合约 T 完全一致，则数字签名验证通过。

当合约签名各方都通过上述 3 步验证，则认为合约签名有效。区块链网络节点会按照共识机制将该合约写入区块链账本中。

4.3 安全分析

本文所提出的身份鉴证与授权机制建立在区块链技术基础之上，并利用哈希变换、数字签名等密码学技术对身份鉴证和授权进行安全强化。以下就系统安全和算法安全进行简要分析。

(1)系统安全

首先，本文设计了 IRAA 终端，通过该终端，身份和生物特征信息转换成哈希摘要，系统中的通信和算法处理的都是密文信息，可以有效保护用户明文信息。第二，系统构建了区块链底层，所处理身份注册或授权业务，都写入区块链账本，由区块链技术支持所存证的信息具有不可删除、不可篡改、不可否认以及可以公开验证等特点。第三，用户身份注册过程由权威部门参与(如身份信息发放管理部门)，保障系统各组件采集信息的安全有效，确保身份注册信息的真实可信。第四，本文构建了“身份注册-身份授权”星形多区块链架构，身份注册链由各权威部门维护，提供去中心化的服务，保障注册身份信息安全；业务信息根据不同行业应用，构成不同的身份授权链，对业务的身份授权进行存证，本系统构成具有良好的安全性和可靠性。

(2)算法安全

在身份注册过程中，使用哈希散列算法将身份和生物特征信息进行明文隐藏。通信和存储在身份注册链中的身份信息都是哈希摘要，哈希摘要的单向运算特点确保明文信息不可逆推出来。在身份鉴证过程中，对身份信息的哈希摘要进行对比，但不会泄露明文信息，确保用户隐私更安全。

本文采用了基于 RSA 算法的密钥生成和数字签名算法，保障身份授权的安全。尽管在身份注册信息和合约授权过程中，可以得到 u，v，w 这些身份信息的哈希摘要，但由表 2 中的数据可知，攻击者很难对大整数 n 进行质因数分解得到 p，q(p，q 是不公开的)，也就无法得到欧拉函数 $\varphi(n)$，而 $\varphi(n)$ 是计算私钥 $SK=(n,d)$ 中 d 的必要条件。因此，尽管在存证合约 C 中包含公钥等信息(见式(10))，RSA 算法仍然可以保障授权签名的安全。

表 2 整数因子分解研究进展

Table 2 Advances in integer factorization

二进制位数	十进制位数	时间	二进制位数	十进制位数	时间
332	100	1991-04	576	174	2003-12
365	110	1992-04	663	200	2005-05
398	120	1993-04	768	232	2009-12
431	130	1996-04	795	240	2019-12
530	160	1999-08	829	250	2020-02

另外，本文对 RSA 算法做了部分修改，将身份与生物特征信息的哈希摘要 v 与 RSA 生成密钥对关联起来(见式(5)和式(6))，避免用户私钥泄露导致的安全隐患。本节分别对传统 RSA 算法和本文修改后的算法采用暴力攻击(Brute-force)进行破解，攻击耗时如表 3 所列，随着素数 n 比特位的提高，破解传统算法与改进算法的耗时会逐渐增加。由此可见，改进算法不仅免除了用户保存私钥的麻烦，在安全性上同样有较好的保障，进一步强化系统的安全性与可靠性。

表 3 攻击耗时

Table 3 Attack time

(单位：ms)

n 位长/bit	传统 RSA	改进算法
64	26.8	30.2
128	342.2	449.1
192	2763.0	2962.0
256	102619.0	110360.0

5 验证与评估

本文实现了 BIAA 原型系统，如图 3 所示，用于测评所提方案的可行性与性能指标。系统由嵌入式计算机承载 IRAA 终端功能，其配置为：Ubuntu 18.04.2 LTS 操作系统，Intel i5 四核处理器，主频 1.6GHz，8GHz 内存，新中新身份信息读取终端，圣点指静脉采集终端。

图 3 BIAA 原型系统

Fig. 3 BIAA prototype system

5.1 基于指静脉和二代身份证的身份鉴证模块

(1)IRAA 响应时间

本节测试了在不同参数下 IRAA 终端读取身份信息所需的时间、生成公私钥耗时与签名耗时，实验重复 50 次。用 $T1$ 表示身份信息读取耗时，$T2$ 表示指静脉读取耗时，$T3$ 表示生成公私钥耗时，$T4$ 表示数字签名耗时。实验统计结果如表 4 所列。

表 4 v^b 对 IRAA 响应时间的影响

Table 4 Effect of v^b on IRAA response time

(单位：ms)

v^b 位长	$T1$	$T2$	$T3$	$T4$
8	4003	2510	33.4	0.55
16	4003	2510	35.2	0.78
32	4003	2510	58245.0	0.38

表 4 测试了在 v 为 256 比特位、n 为 1024 比特位的情况下，v^b 的长度对 IRAA 终端操作响应时间的影响。考虑到寻找质数 e 是一个耗时的计算过程，我们对 v^b 做了如下处理：$v^b \leftarrow \mathrm{mod}(v^b, 2^\theta)$，可将 v^b 的比特位位数缩小至 θ。如表 4 所列，v^b 的长度越长，生成公私钥的时间就越久，安全性就越高，但高安全性往往意味着对设备、算力、耗时的高要求，因此在实际应用场景中，使用者可以根据性能与安全性的具体需求来权衡 v^b 的大小。

表 5 测试了在 v^b 为 16 比特位、n 为 1024 比特位的情况下，v 的长度对 IRAA 终端操作响应时间的影响。可以看出 v 的比特位数对公私钥的生成时间也有一定影响，v 越长，生成公私钥的耗时也会增加，但增加幅度较小。

表 5 v 对 IRAA 响应时间的影响

Table 5 Effect of v on IRAA response time

（单位：ms）

v 位长	$T1$	$T2$	$T3$	$T4$
256	4003	2510	35.2	0.78
384	4003	2510	38.1	0.64
512	4003	2510	48.6	0.89

表 6 测试了在 v 为 256 比特位、v^b 为 16 比特位的情况下，n 的长度对 IRAA 终端操作响应时间的影响，n 的长度直接决定所生成公私钥的长度，n 越长，公私钥长度越长，安全性越高。可以看出，n 的长度对生成公私钥时间也有一定影响，n 为 512 比特位时，耗时最少，1024 比特位次之，2048 比特位耗时最多，耗时变化幅度较小。

表 6 n 对 IRAA 响应时间的影响

Table 6 Effect of n on IRAA response time

（单位：ms）

n 位长	$T1$	$T2$	$T3$	$T4$
512	4003	2510	11.4	0.35
1024	4003	2510	35.2	0.78
2048	4003	2510	24.8	0.56

（2）IRAA 计算消耗

本小节测试了从获取用户身份信息与指静脉信息到签名成功整个算法执行期间的 CPU 与内存占用率，如图 4 所示，本算法的 CPU 占用率保持在 1.5%～2.5%之间，内存占用率稳定在 0.1%，可见本算法所占用的计算资源极小，低配置设备也可以支持 IRAA 终端的功能。

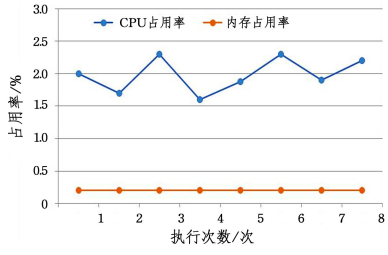

图 4 IRAA 执行操作期间的 CPU 与内存占用率

Fig. 4 CPU and memory usage during IRAA operation

5.2 基于区块链的身份鉴证与授权系统原型

本文采用联盟链 Hyperledger Fabric 作为区块链底层平台，使用 2 台云服务器搭建了基于 Fabric 的身份注册链与身份授权链，并编写了相应的智能合约以实现身份注册、鉴证与授权功能，服务器配置与 Fabric 网络配置如表 7 所列。

表 7 区块链网络配置

Table 7 Blockchain network configuration

操作系统	Ubuntu 18.04.2LTS
处理器	Intel 2.10GHz× 32
内存/GHz	32
网络带宽/(Mb/s)	10000
Fabric 版本	V2.2.0
共识算法	Raft
操作系统	Ubuntu 18.04.2 LTS

图 5－图 7 测试了身份注册、鉴证、授权相关智能合约的性能指标，实验设定为：每组测试都以特定的交易发送速率向身份注册链发送持续一分钟的交易，客户端数量设为 10，即 10 个客户端同时发送交易。图 5 给出了 4.1.1 节身份注册功能的吞吐量与平均延迟时间，吞吐量最初随着交易发送率的提高而增加，在发送率为 1000 时达到最高，为 960 TPS，随后便略微下降。平均延迟时间最初随着发送率的提高而略微降低，在发送率超过达到 800 之后，延时迅速增加，因为交易发送率达到一定程度后，会积压未完成交易，发送率越高，积压的交易就越多，导致交易处理的延时增加。图 6 测试了 4.1.2 节中身份鉴证功能的吞吐量与平均延时时间，身份鉴证只需要将身份注册链账本中已存在的信息取出，然后与终端发送过来的信息进行比对，无须向账本写入数据，故吞吐量要比注册功能高得多，吞吐量基本与发送率持平，最高保持在3000 TPS 左右，延时也远远低于身份注册功能，始终保持在0.1 s。图 7 给出了 4.2 节中合约验证功能的性能指标，合约验证包括用户身份验证、公钥验证、签名验证和将合约信息写入账本 4 个步骤，总体性能略低于身份注册功能。

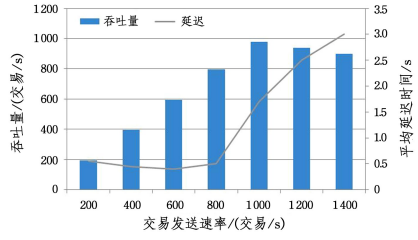

图 5 身份注册性能分析

Fig. 5 Identity registration performance analysis

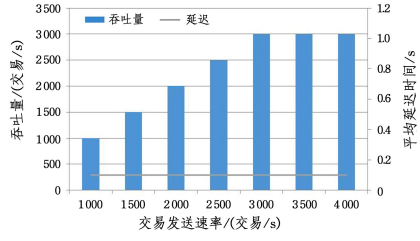

图 6 身份鉴证性能分析

Fig. 6 Identity identification performance analysis

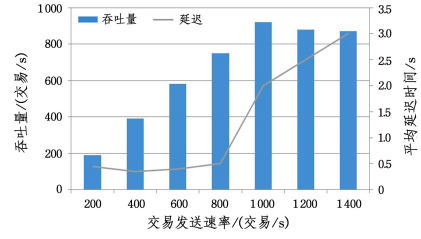

图 7 合约验证性能分析

Fig. 7 Contract validation performance analysis

实验证明，身份注册链对处理身份注册、鉴证与授权功能具有良好的性能，可以适用于较大规模的应用场景。

结束语 针对身份信息安全问题，本文提出了一种基于区块链的身份鉴证与授权机制(BIAA)。该机制要求用户主体在对业务进行身份授权时提供有效身份证件和生物特征信息，确保业务为本人授权；设计了完善的安全机制与算法实现，开发了身份信息授权终端软硬件原型，确保用户身份信息及其授权使用的安全；构建了基于区块链的身份鉴证与授权原型系统，充分验证了所提机制的有效性和可用性。未来，我们将继续优化 BIAA 的效率与安全设计，以及推广在具体场景中的应用。

参 考 文 献

[1] SMITH R G, National identity security strategy estimating the cost to Australian businesses of identity crime and misuse[OL]. https://www.aic.gov.au.

[2] Personal information security and privacy protection in China [R]. CYU Internet Law Research Center, 2016.

[3] KHODAEI M, JIN H, PAPADIMITRATOS P. SECMACE: Scalable and robust identity and credential management infrastructure in vehicular communication systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19(5): 1430-1444.

[4] CHENG X, ZHANG Z, CHEN F, et al. Secure identity authentication of community medical Internet of things[J]. IEEE Access, 2019, 2019(7): 115966-115977.

[5] NAKAMOTO S, Bitcoin: A peer-to-peer electronic cash system, White Paper, 2008[OL]. https://bitcoin.org/bitcoin.pdf.

[6] CAI X, DENG Y, ZHANG L, et al. The principle and core technology of blockchain[J]. Chinese Journal of Computers, 2021, 44(5): 84-131.

[7] ANTONOPOULOS A M. Mastering Bitcoin: Unlocking digital cryptocurrencies[M]. O'Reilly Media, Inc., Sebastopol, USA, 2014.

[8] SLOMOVIC A. Privacy issues in identity verification[J]. IEEE Security & Privacy, 2014, 12(3): 71-73.

[9] WALT E, ELOFF J. A Big Data Science Experiment-Identity Deception Detection[C]// International Conference on Computational Science & Computational Intelligence. IEEE, 2015: 416-419.

[10] ZOU Y, ROUNDY K, TAMERSOY A, et al. Examining the adoption and abandonment of security, privacy, and identity theft protection practices[C]// Proceedings of the CHI Conference on Human Factors in Computing Systems. Honolulu USA, 2020: 1-15.

[11] AKHTAR Z, HADID A, NIXON M S, et al. Biometrics: In search of identity and security (Q&A)[J]. IEEE Multimedia, 2018, 25(3): 22-35.

[12] ESTEE V D W, ELOFF J H P, GROBLER J. Cyber-security: Identity deception detection on social media platforms[J]. Computers & Security, 2018, 78(sep.): 76-89.

[13] HE D, ZHANG Y, DING W, et al. Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 17(5): 1124-1132.

[14] CHEN J, HAO G, LIANG Y. Strongly secure identity-based authenticated key agreement protocols without bilinear pairings [J]. Information Sciences, 2016, 367(Nov.): 176-193.

[15] DANIEL R M, RAJSINGH E B, SILAS S. An efficient eCK secure identity based two party authenticated key agreement scheme with security against active adversaries[J]. Information and Computation, 2020, 275(Dec.): 1-20.

[16] DENG Y, SONG G, YANG B, et al. Identity-based inner product functional encryption with verified secret key[J]. Chinese Journal of Computers, 2021, 44(5): 908-920.

[17] MEZRAG F, BITAM S, MELLOUK A. IDSP: A new identity-based security protocol for cluster-based wireless sensor networks[C]// Proceedings of the IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications. Istanbul, Turkey, 2019: 1-6.

[18] KAI H, JIAN W, LIU J N, et al. Anonymous identity-based broadcast encryption with chosen-ciphertext security[C]// Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. Xi'an China, 2016: 207-222.

[19] KHAN R, KUMAR P, JAYAKODY D, et al., A survey on security and privacy of 5G technologies: potential solutions, recent advancements and future directions[J]. IEEE Communications Surveys & Tutorials, 2019, 22(1): 196-248.

[20] WANG Z. A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity[J]. Future Generations Computer Systems, 2018, 82: 342-348.

[21] WANG H, HE D, YU J, et al. Incentive and unconditionally anonymous identity-based public provable data possession[J]. IEEE Transactions on Services Computing, 2019, 12(5): 824-835.

[22] JIA X, HE D, KUMAR N, et al. A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing[J]. IEEE Systems Journal, 2019, 14(1): 1560-571.

[23] ZHANG C Y, KIM D, HWANG I. Multi-target Identity Management for Unknown and Time-Varying Number of Targets in Clutter[J]. European Journal of Control, 2021, 60: 20-35.

[24] NIU J L, REN Z Y. A self-sovereign identity management scheme using smart contracts [J]. MATEC Web of Conferences, 2021, 336: 08005.

[25] SONG L, SUN G, YU H, et al. FBIA: A fog-based identity authentication scheme for privacy preservation in Internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2020, 69(5): 5403-5415.

[26] WANG Z. An identity-based data aggregation protocol for the smart grid[J]. IEEE Transactions on Industrial Informatics, 2017, 13(5): 2428-2435.

[27] KARATI A, ISLAM S H, BISWAS G P, et al., Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of things environments[J]. IEEE Internet of Things Journal, 2018, 5(4): 2904-2914.

[28] DUNPHY P, PETITCOLAS F. A first look at identity management schemes on the Blockchain[J]. IEEE Security and Privacy Magazine, 2018, 16(4): 20-29.

[29] XU K,LING S,LI Q,et al. Research progress of network security architecture and key technologies based on blockchain[J]. Chinese Journal of Computers,2021,44(5):55-83.

[30] Hyperledger Indy:Hyperledger-Powered Digital Identity Solutions[OL]. https://www.hyperledger.org/use/hyperledger-indy.

[31] XU J,XUE K,TIAN H,et al. An identity management and authentication scheme based on redactable blockchain for mobile networks[J]. IEEE Transactions on Vehicular Technology,2020,69(6):6688-6698.

[32] YANG X,LI W. A zero-knowledge-proof-based digital identity management scheme in blockchain[J]. Computers & Security,2020,99(Dec.):1-17.

[33] CUI Z,XUE F,ZHANG S,et al. A hybrid blockchain-based identity authentication scheme for multi-WSN[J]. IEEE Transactions on Services Computing,2020,13(2):241-251.

[34] YANG X,YANG X,YI X,et al. Blockchain-based secure and lightweight authentication for Internet of things[J]. IEEE Internet of things Journal,2022,9(5):3321-3332.

[35] MALIK N,NANDA P,ARORA A,et al. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks[C]// Proceedings of the 17th IEEE International Confe- rence on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering. New York,NY,USA,2018:674-679.

[36] WANG S S,MA Z F,LIU J W,et al. Research and Implementation of Cross Chain Security Access and Identity Authentication Scheme of Blockchain[J]. Netinfo Security,2022,22(6):61-72.

[37] WANG S S,DAI B R,ZHU M L,et al. User Identity Authentication Model for Cross-Chain System[J]. Computer Engineering and Applications,2022,58(19):135-141.

[38] REN X,LIN F,CHEN Z,et al. BIA:A blockchain-based identity authorization mechanism[C]// Proceedings of the IEEE 16th International Conference on Mobility, Sensing and Networking. Tokyo,Japan,2020:98-105.

LIN Feilong, born in 1982, Ph.D, associate professor. His main research interests include blockchain technology, edge computing, and industrial Internet of Things.