DOI:10.13878/j.cnki.jnuist.2019.05.010

桑安琪[1]　沈蒙[1,2]　祝烈煌[1]　刘胜[3]　殷舒[3]　肖尧[1]

基于区块链的多方协作安全身份认证机制研究

摘要

信息技术的快速发展使身份认证机制的安全性得到越来越广泛的关注.但现有的身份认证机制存在着隐私泄露等风险,这就要求设计出更加可靠的身份认证机制.本文利用区块链的去中心化、不可篡改等特性,设计出基于区块链的多方协作安全身份认证机制.在实现可靠身份认证的同时,保证信息的权威性,在一定程度上减少数据冗余,并提高身份认证效率,保证全面且准确的身份认证.最后实现支持多个数据服务商对身份信息进行加密签名,保护数据隐私,以及多方共享数据的身份认证系统.

关键词

区块链;身份认证;身份授权;多方协作

中图分类号 TP302.1

文献标志码 A

0　引言

互联网迅速演进到 web2.0 时代,网络应用和互联网服务涉及到人们网络生活的方方面面[1].互联网在带来便利的同时,也造成了日益严重的网络安全问题,使得个人信息、部门信息乃至国家机密等都面临着相应的威胁.身份认证便作为信息安全防护的第一个关卡,承担了重要的责任.身份认证机制在安全系统中是最基础的安全服务,只要身份认证系统受到攻击入侵,系统里的相应安全措施都将无法产生作用.并且黑客入侵的首要目标一般都是身份认证系统.所以,系统拥有一个安全可靠的身份认证机制是很有必要的.

当前的单一认证在攻击者的面前是很脆弱的,因为攻击者可以很轻易地通过伪造身份等方式来实施攻击[2-4].当只有密码认证时,账户等信息很容易便可被破解.例如,2015 年的网易邮箱过亿数据泄露导致 iPhone 手机用户被勒索等类似事件.因此,采取综合多因素的认证机制是很有必要的,这里的综合多因素包括综合账户口令、生物智能卡、指纹识别等多种类型的身份特征数据实现可靠认证[5-7].其次,单一机构很难提供全面的多因子认证所依赖的多种类型的身份特征数据.而且,当单一机构遭到攻击时,其本地的多因子的身份数据依然会泄露.因此,可以采用多机构、多数据源相结合的认证方式,实现更加安全且全面的身份认证机制.

然而,这种多机构、多数据源相结合的认证方式在实现中依然会遇到许多困难.首先,用户的身份特征数据关系到数据服务商的根本利益.若每个数据请求方都分别从数据服务商那里获得部分身份特征数据,然后私下交换,则存在数据所有权确定困难和隐私泄露等问题.其次,在多方协作的场景中,很难保证各个认证机构都可以提供高质量的身份特征信息.可能存在某些认证机构,为了谋取利益,提供大量低质量的身份特征数据,从而导致虚假、伪造身份特征数据等劣币驱逐良币现象.

区块链以其无中心化和无信任化的独特性质进入了广大研究者的视野中.区块链的分布式结构使得它可以在不需要中心化机构或可信第三方的前提下,实现多个弱信任实体间的交互,并保证这种交互数据不能被任意一方所篡改.因此,区块链的这种特点适用于多方认证场景.区块链作为一个底层的平台,多方协作的身份认证机制可以在它的基础上设计并实现.这种机制能够保证数据的可信性和可靠性,

收稿日期 2019-07-29

资助项目 国家重点研发计划(2018YFB0803405);国家自然科学基金(61602039,61872041);北京市自然科学基金(4192050);CCF-腾讯犀牛鸟基金微众银行专项基金项目

作者简介

桑安琪,女,硕士,研究方向为网络与信息安全.anqi_960123@163.com

祝烈煌(通信作者),男,博士,教授,博士生导师,研究方向为网络与信息安全.liehuangz@bit.edu.cn

1　北京理工大学 计算机学院,北京,100081

2　密码科学技术国家重点实验室,北京,100878

3　联动优势科技有限公司,北京,100082

并进一步通过加密处理增强对数据的隐私保护.

因为目前身份认证的痛点亟待解决,所以基于区块链设计一种多方身份认证的解决方案很有必要.因此,本文提出了一个基于区块链的多方协作安全身份认证机制,并构建了系统,可以满足多方身份认证的需求.同时,该系统提高了身份认证的可靠性、权威性和高效性,从而实现全面并且准确的身份认证,具有重要的现实意义.例如,当今中国互联网金融风险相关案件频频发生,Equifax 去年有 1.43 亿信用和信息服务客户的数据被泄露,规模庞大.类似案件影响了互金行业的健康发展,所以安全可靠的身份认证机制,正是解决问题的基础和关键.

1 相关工作

1.1 研究现状

区块链技术是近年来的热点,但将区块链技术与身份认证机制结合的探索目前还处于初期研究阶段[8-11].

2014 年,Fromknecht 等[12]提出利用加密货币(如比特币和 Namecoin)提供的一致性保证来构建可确保身份持有的公钥基础设施(PKI),并且构建了名为 Certcoin 的系统.该系统没有中央管理机构,需要使用安全的分布式字典数据结构来提供有效的支持.

2016 年,Isaakidis 等[13]提出了一个分散的、增强隐私的身份认证、授权和消息传递系统,它使用了基于代数 MAC 的盲签名来改进 OpenID,使用即时通讯程序以加密的形式传递信息,但不保护元数据且服务集中,该系统在区块链上以分散的方式搭建访问控制列表.

2017 年,Matsumoto 等[14]提出了 IKP 平台,它可以自动响应未经授权的证书,并为 CA(Certificate Authority,证书颁发机构)提供行为正确的激励,并为其他人报告潜在的未经授权的证书.通过利用智能合约和基于区块链的共识来使 IKP 去中心化,同时提供自动化激励.

现有的身份认证机制仍存在以下亟待解决的问题:

1)身份数据缺乏共享.当今各数据服务商都独自维护自己的身份信息数据库,缺乏有效的共享机制,很难实现多方协作的身份认证机制,使得认证结果不全面、不可靠.

2)身份数据面临泄露风险.现今多家企业在各自的数据库中冗余保存用户的身份数据,一旦被恶意者攻击,会大概率导致用户的身份信息很容易被泄露,引发一些不必要的损失.

3)身份认证过程不公开.目前各企业有各自的身份认证体系,采用集中式认证.同时可随时对本地的身份特征数据进行任意修改,容易引起不必要的损失,也很难溯源追责.

本文结合以上研究思想中的长处,针对目前需要解决的必要问题,在身份认证的场景下结合多方,充分利用区块链的特性,来保证身份数据的共享、身份数据的隐私保护、身份认证过程的透明.从而使得多方协作的身份认证机制是可信且可靠的.

1.2 国密算法

我国为了保障商用密码的安全性,自主研发了包括 SM2、SM3 等一系列密码算法,即国密算法.其中 SM2、SM3 等可以使用软件实现.

SM2 算法是一种基于椭圆曲线上点群离散对数难题的公钥密码算法,目前已在各大领域中得到了广泛的应用.该算法包括了主要用于实现数字签名密钥协商的数字签名算法和密钥交换协议,以及用于实现数据加密等功能的公钥加密算法[15].

SM3 算法是一种密码散列(哈希、杂凑)算法,其输出长度为 256 bit.因此 SM3 算法的安全性高于 MD5 和 SHA-1.此算法适用于商业密码的数字签名和验签、消息认证码的生成与验证,以及随机数生成,可满足多种密码应用的安全需求[16].

本文设计的基于区块链的多方协作安全身份认证机制使用 SM2 和 SM3 算法.其中 SM2 算法主要用于身份认证模块,如数据请求方请求认证时对认证请求内容使用 SM2 算法进行私钥签名,然后数据服务商使用 SM2 算法进行验签;SM3 算法主要用于身份授权模块,如数据服务商将授权用户的账户和该用户的多个身份特征信息使用 SM3 算法分别生成数字摘要等.

1.3 区块链相关技术

区块链是当前计算机应用技术领域最前沿的创新之一,也是未来数十年内最可能颠覆整个金融体系运行模式的重大技术.区块链因比特币的火爆而逐渐进入人们的视线.比特币的雏形是 2008 年中本聪在其发表的白皮书中提出的,由此比特币开始进入人们视野[17].随着比特币的发展,其底层的区块链技术因具有去中心化、不可篡改和去信任化等特点而得到产业界和学术界的重视.当前国内外研究机

构和金融机构都在抢占时机,努力抓住创新机遇,一场以区块链技术为基础的系统性创新正在拉开大幕.

区块链的本质是一种链式结构,它使用密码学的相关技术来保证区块数据的完整性和可验证性.同时区块链还使用共识算法,实现了分布式节点对区块数据的集体维护.在以太坊为首的区块链中,还可以利用智能合约对区块链中的数据进行操作.区块链每个数据块都详细标明了运用哈希算法构建的树状交易状态信息,这些信息确保了区块链里链接的区块和每个区块内的交易数据的确定性,均不可篡改.

区块链具备去中心化、不可篡改性、准匿名性和可编程性等特征.其系统自上而下依次由数据层、网络层、共识层、激励层、智能合约层组成[18].本多方协作安全身份认证机制的区块链系统模型架构如图1所示.

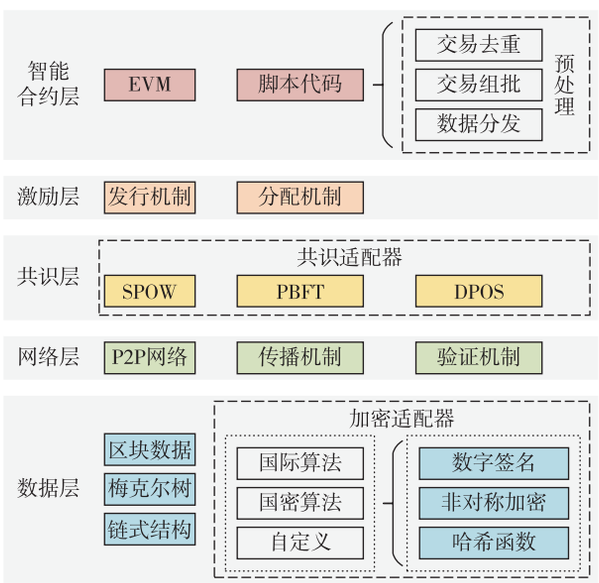


图1 区块链系统的模型架构

Fig. 1 Blockchain system model architecture

2 系统模型

基于区块链的多方协作安全身份认证系统(图2)主要包括3种角色:用户、数据服务商、数据请求方.

1)用户:指身份认证服务的使用者.用户能够在系统中自由创建任意个账户信息,并基于这些账户使用身份认证服务.

2)数据服务商:指拥有海量的、可信的用户身份信息的机构,如公安局、商业银行、电信运营商等.数据服务商负责对用户的账户进行身份认证,并将认证结果上链存储.

3)数据请求方:指为用户提供服务的机构,如商户、信贷机构等.数据请求方在收到用户的服务申请后,将利用认证系统对用户提供的账户进行身份认证,只有通过认证的用户才能使用服务.

日常生活中的很多行为都会涉及大量与身份相关的数据,比如电话号码、通讯地址、身份证照片等.这些身份数据不仅对于个人,对于提供服务的数据服务商和数据请求方也是至关重要的.首先数据服务商要保证身份数据的真实性,即用户的身份数据是真实可靠的.在此基础上,要保证身份数据的可追溯性,即一旦出现了虚假的或者不准确的身份数据,数据请求方或者数据服务商可以追溯到这些不可靠数据的来源.最后,身份数据应具备安全性和匿名性,避免因用户隐私泄露而导致的一系列问题.

本系统是基于区块链建立的开放式的多方协作安全身份认证系统,支持多个用户身份数据的加密共享,支持数据请求方按需索取身份特征信息,并能够在保护数据隐私的条件下结合多方数据完成身份认证服务.其利用支持隐私保护的多维身份认证数据共享机制,提交文字与图片类型的身份特征信息,执行双存储操作,将身份特征信息存储在已建立的授权业务数据库及授权信息区块链中;利用基于多方协作的身份认证机制,向多个数据服务商请求已有身份特征信息、验证身份特征信息的完整性和一致性.逐步形成统一、规范、标准的多方协作安全身份认证工作程序,力求实现各类身份信息的完整和可靠.同时利用密码学技术和区块链技术,做到身份特征信息的可信存储,提高身份认证的权威性和高效性,降低身份认证系统面临的单点崩溃和数据泄露风险.多方协作安全身份认证模型如图2所示.

3 关键技术

3.1 账户注册

用户在被数据服务商和数据请求方服务前,要先在自己的设备上注册账户.一个用户可拥有多个账户,每个账户信息都是在用户注册时随机生成的,这种随机性在一定程度上可以保护用户的隐私.每一个账户信息都包含随机生成的账号和随机生成的该账号对应的密钥对.账户生成的伪代码如图3所示.

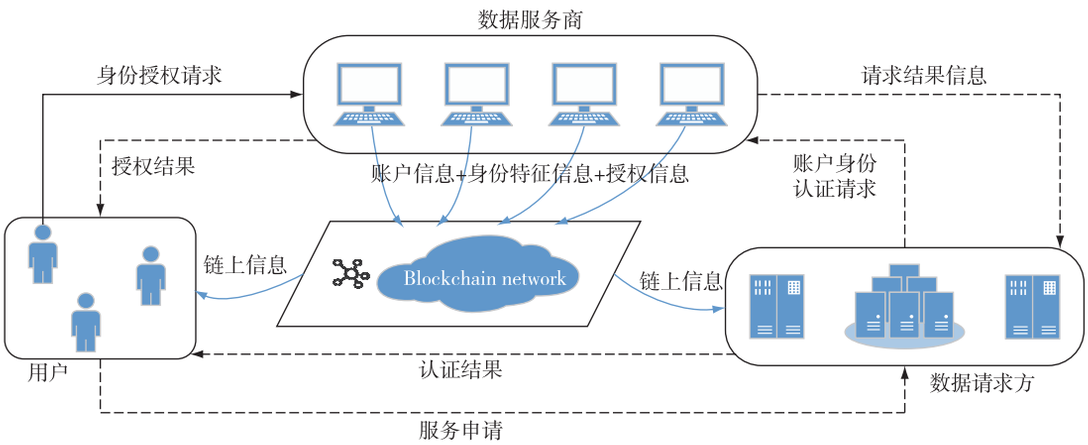


图 2　基于区块链的多方协作安全身份认证架构模型

Fig. 2　Architecture of blockchain-based multi-party collaboration security identity authentication model

```
1 func GenerateAccount(){
2     account,err :=rand.getRandomAccpunt(40) //随机生成账号
3     priv, err := sm2.GenerateKey()//生成密钥对
4     if err != nil {
5           t.Fatalf("Failed generating sm2 key [%s]", err)
6     }
7     sm2PrivateKey := &SM2PrivateKey{priv}//私钥
8     pk, err := sm2PrivateKey.PublicKey()//私钥生成公钥
9 }
```

图 3　账户注册伪代码

Fig. 3　Account registration pseudo code

伪代码第 2 行可获得账号,此随机账号生成功能是利用 rand 里的 getRandomAccpunt( ) 函数实现的.第 3 行是通过 sm2 里的 GenerateKey( ) 函数来先获取到使用 SM2 签名算法随机生成的密钥对.第 7 行是从新生成的密钥对中得到 SM2 签名算法生成的用户私钥;第八行是利用用户私钥推出的用户公钥.

最后,再将生成的账号和该账号对应的密钥对显示给注册用户即可.但此账号信息的显示是一次性的,即只出现一次,需要用户自己妥善保存.这样就可以保证用户账号信息泄露风险的概率会大大降低,使用户隐私尽可能的得到保护.

3.2　基于区块链的数据存储

由于区块链中可存储内容长度有限,所以将授权内容存储在数据服务商本地数据库,区块链中只存储数据服务商标识、用户账户散列值和授权内容散列值等相关参数.在用户查询链上数据时,数据访问程序会根据经过该用户公钥加密后的数据服务商标识和账户散列值找到区块链上对应的字段进行查询.

用户身份特征信息授权算法流程如图 4 所示,将用户的账户和多个身份特征信息使用 SM3 算法分别生成数字摘要,并用井号将他们组合,连接为字符串,形成数据服务商数字摘要组合.然后再次使用 SM3 算法将用户账户哈希,生成用户数字摘要.之后用户数字摘要和数据服务商数字摘要组合,分别与数据服务商标识用井号进行连接,对应生成用户字符串组合和数据服务商字符串组合.再使用该被授权用户的公钥,运用 RSA 算法,对用户字符串组合进行非对称加密,形成用户公钥加密密文.同理,使用数据服务商的公钥,运用 RSA 算法,对数据服务商字符串组合进行非对称加密,形成数据服务商公钥加密密文.然后将两份密文使用井号组合,并将组

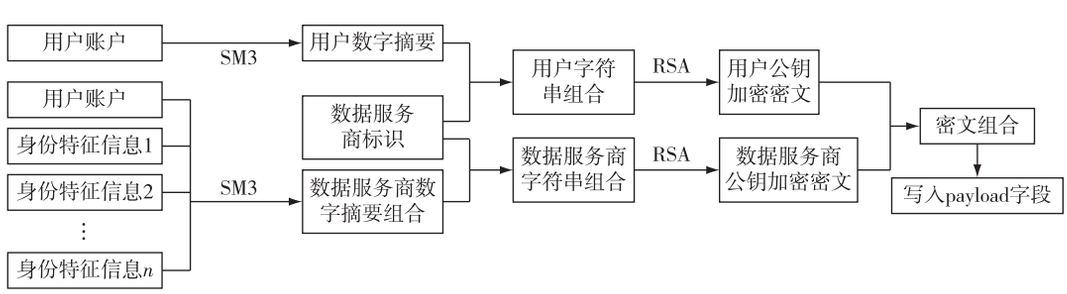


图 4　身份特征信息授权算法流程图

Fig. 4　Flow chart of identity feature information authorization algorithm

合后的密文写入 payload 字段(指记载着上链的信息的那部分字段).这样就可以保证授权内容可以写入区块链且不会被篡改.

3.3 区块链核心功能

区块链核心功能主要包含身份特征信息上链和身份特征信息查询两个核心功能.区块链核心功能时序如图 5 所示.

1) 身份特征信息上链

数据服务商对用户线下提交的身份信息和用户账户信息进行整理后,提取出必要的身份特征信息,并按一定的格式存入本地数据库.当数据服务商管理员确认用户身份信息无误时,数据服务商管理员就可以对该用户进行准备上链操作.前端代码在获取前端的 post 请求后,上链之前,调用 datahandle( ) 函数,利用 3.2 节所述的数据存储方法,将用户账户和对应的多个身份特征信息使用 SM3 算法生成数字摘要,并与数据服务商标识连接.然后分别使用用户公钥和数据服务商公钥,运用 RSA 算法,对字符串组合进行非对称加密.

之后将最终密文写入交易的 PoeData 字段中,再调用区块链底层接口函数 PoeSet( ).该函数中利用 Http 协议的 Post 接口方法,根据配置文件 interfaceConfig.yaml 中设置的 poe_post URL 接口(用于向链上发送数据),向指定的资源提交要被处理的数据结构.最后,区块链底层平台调用 AppImpl 接口中的 AppProcess( ) 函数将数据结构上链存储.存储结果被全网确认后,返回区块链交易码,数据上链成功,如图 5a 所示.

2) 身份特征信息查询

用户在区块链客户端中选择查看自己的身份特征信息授权结果.前端代码获取前端 get 请求,调用 datahandle( ) 函数.然后通过区块链底层接口函数 PoeGet( ) 调用 Http 协议的 Get 接口方法,根据配置文件 interfaceConfig.yaml 中设置的 poe_get URL 接口(用于从链上查询数据),从指定的资源请求数据.之后区块链底层平台调用 AppImpl 接口中的 Query( ) 函数查询相应数据,并返回最终查询结果,如图 5b 所示.

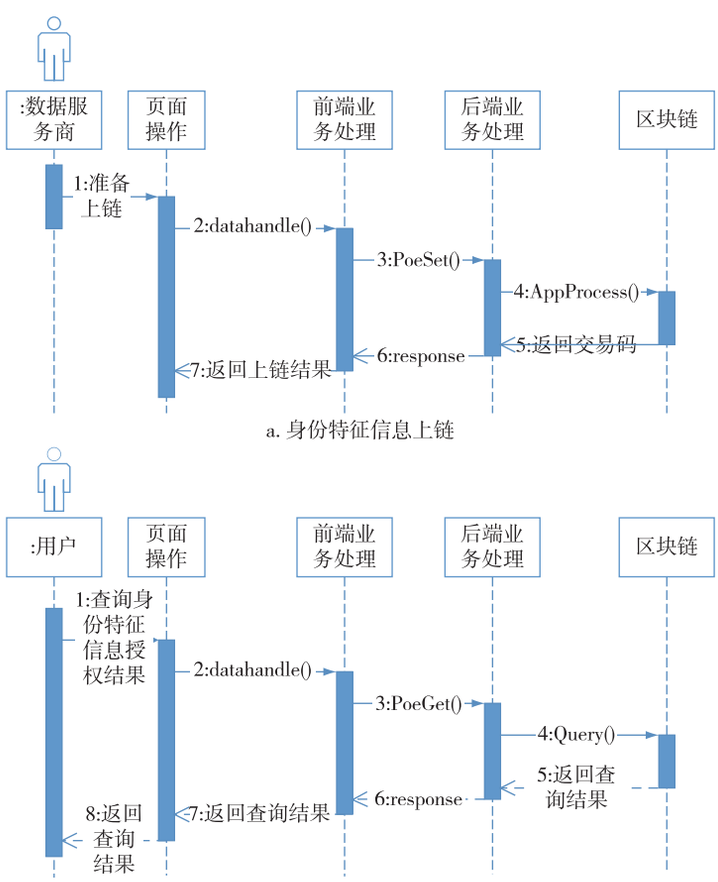


图 5 区块链核心功能时序图

Fig. 5 Sequence diagram of blockchain core functions

3.4 安全身份认证

用户的账户信息、身份特征信息和授权信息上链后,用户即可开始申请使用数据请求方所提供的相关服务.届时数据请求方根据用户服务申请,与一个或多个数据服务商分别协商会话密钥,然后数据请求方将使用协商的会话密钥加密认证请求,并分别发送给对应的数据服务商,从而完成对用户的安全身份认证.多方协作安全身份认证流程如图 6 所示.

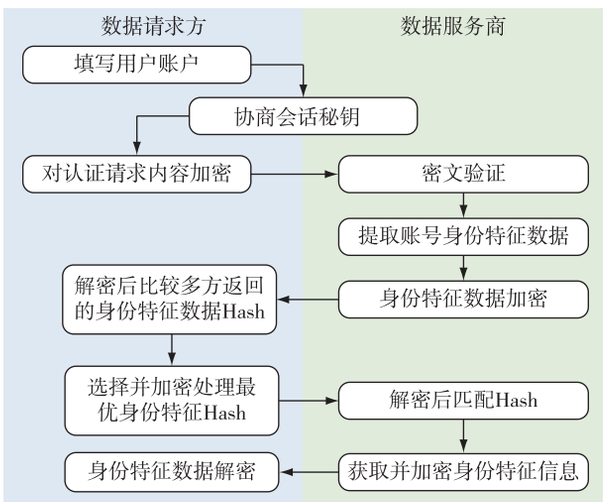


图 6 多方协作安全身份认证流程

Fig. 6 Flow chart of multi-party collaboration security identity authentication

数据服务商根据数据请求方请求认证的账号查询数据库,将查询结果使用会话密钥加密处理后发送给数据请求方.数据请求方用会话密钥解密,然后对比提取最优身份特征信息散列值.之后将该散列值用会话密钥加密后,分别发送给数据服务商,向其请求此散列值对应的明文.数据服务商解密后,结合账户信息,根据此散列值查询数据库,找到相应的最优身份特征信息明文,然后将此明文用会话密钥加密,再传输给数据请求方.数据请求方将接收到的密文解密,并存储进本地数据库.

4 安全性分析

身份特征数据既涉及到用户的个人隐私,也涉及到各个数据服务商的根本利益,因此,一旦这些数据泄露或被攻击者所篡改,对用户和服务商都会产生很大的损失.因此,多方协作安全身份认证机制在安全性方面满足以下要求:

1)数据访问控制

实时监测用户状态,对用户的登录状态和所有与身份信息相关的操作进行严格的控制.如用户在登录后 30 min 内未在界面中进行任何操作就自动退出登录,重新进行登录操作;登录检测通过,则用户可以进入区块链客户端,查看相关信息.如果用户要进行申请授权的操作,则使用持有注册账户成功时返回的私钥,对操作进行数字签名,最大限度的保护身份数据的安全.

2)数据隐私保护

为了防止攻击者查看、篡改或伪造身份数据、账户数据或者授权信息,对数据和信息进行加密操作,将身份特征数据的明文,利用确定的密码学加密算法进行处理,使其变为密文.使用非对称密码算法(RSA、ECDSA)、单向散列算法(SHA256)和国密算法(SM2、SM3).三者的结合为多维身份认证数据的共享和多方协作的安全身份认证提供了支持,同时在密码学层面上保证了区块链的高度隐私.

3)匿名化

为了避免攻击者通过统计分析等方式将身份信息和账户一一对应,对身份特征数据进行匿名化处理.利用加密算法(RSA)和哈希算法(SM3)对账户加密,使攻击者在无用户私钥时不可查.从而达到消除或混淆账户与用户真实身份、授权信息和认证信息之间的实际联系的目的.

4)日志管理

为了严密监控,且减少多方协作安全身份认证机制出现巨大损害的可能性,利用日志管理将系统上的所有访问和操作都记录下来,并且在后台记录操作的摘要,从而提高系统运行的安全性.因为系统存储的身份信息可能随时会发生改变,所以详细地记录每一次改变,有助于根据日志索引进行定位,在必要时也可完成追责功能.

5 实验

5.1 实验部署

基于区块链的多方协作安全身份认证系统使用的底层平台搭建在 Linux 操作系统环境之上,平台的核心功能使用 Go 语言进行实现,可以进行跨平台的开发和布置.在部署新链之前,配置 Go 语言环境.本系统使用的是 go 1.9.1 版本环境.

链的部署主要分为 peer.yaml 配置文件修改、添加 URL 接口、区块链底层编译、区块链应用编译、应用注册、启动节点、网页访问,共 7 个步骤.

系统部署后的物理结构如图 7 所示.1)客户端:系统功能是以网页的形式呈现,因此计算机中可运行的浏览器都属于系统的客户端.2)系统服务器:系统使用 Tomcat 服务器,支持全部 JSP(Java Server Pages,java 服务器页面)以及 Servlet 规范,用于存放静态页面,实现业务逻辑处理等功能.3)区块链分布式网络:专指底层区块链网络,各节点之间网络互通,以便多个节点之间进行共识交互,以及区块同步等操作.

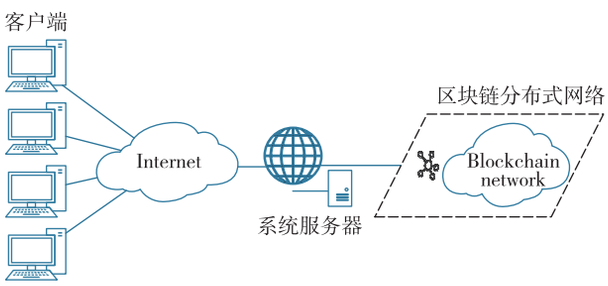


图 7 基于区块链的多方协作安全身份认证机制物理结构

Fig. 7 Physical structure of blockchain-based multi-party collaborative security identity authentication mechanism

5.2 性能评估

为了检验基于区块链的多方协作安全身份认证机制的效率,选取了吞吐量、出块时间和存储空间这 3 个方面来进行评估.

1)吞吐量

吞吐量是指单位时间内成功地传送数据的数量.对于区块链来说,吞吐量就是每秒进行的交易数量(笔/s).本身份认证机制的底层区块链平台是以 Fabric 为基础进行开发的,但在存储性能上相比于 Fabric 有大幅度的提升.表 1 针对凭证存储业务,罗列了目前主流的三种开源区块链框架的吞吐量.

表 1 用于存证的主流区块链平台的吞吐量差异

Table 1 Throughput comparison of mainstream blockchain platforms for deposit verification

区块链平台	链类型	吞吐量(笔/s)
超级账本(Fabric)	联盟链	300
以太坊(Ethereum)	公有链	25
公证通(Factom)	公有链	27

由表 1 可知,基于 Fabric 的身份认证机制的底层区块链平台以 25 000 TPS(Transaction Per Second,每秒事务处理量)的吞吐量对身份信息进行存储处理,可以满足实验环境下的需求,且吞吐量远高于以太坊等区块链平台.

2)出块时间

不同于公有链比特币每隔 10 min(600 s)产生一个区块、以太坊每 15 s 产生一个区块的固定出块策略,Fabric 出块可配置时间、大小,甚至交易的上限大小,非常灵活.本身份认证机制的底层区块链平台最终确认一个区块的时间只需 2 s.图 8 是身份信息密文上链时间图.由图可知密文上链 1 000~10 000 笔交易(块),上链时间在 16~156 s 之间,且上链时间随交易数量的增多而增加.本身份认证机制的底层区块链平台的出块时间等于上链时间加上区块最终确认时间,此结果的数值远小于比特币、以太坊等区块链平台.所以本身份认证机制的出块时间短,上链时间快且稳定.



图 8 身份信息密文上链时间

Fig. 8 Time spent for identity information ciphertext uploaded to blockchain

本方案还做了一组对比实验,测试分析了身份信息明文上链的时间情况,如图 9 所示.由图可知明文上链 1 000~10 000 笔交易,上链时间在 16~166 s 之间,且上链时间随交易数量的增多而增加.对比身份信息明文上链时间与身份信息密文上链时间,后者的时间开销在不同交易数量的情况下,与前者均相差不超过 10 s,且后者的时间开销小于前者的时间开销.所以相比于明文上链,采用密文上链的方式,在时间开销基本持平的情况下,更能保护身份特征数据的隐私安全.

3)存储空间

表 2 列出了身份特征数据上链后明文和密文的存储空间大小对比,交易数量从 2 000~10 000 笔.由表 2 可知,当交易数量增多时,明文和密文所需的存储空间也相应的增加.并且加密操作会使链上占用的存储空间增大.表 2 显示存储 10 000 笔身份信息密文交易大约需要 221 184 KB 的空间,存储10 000

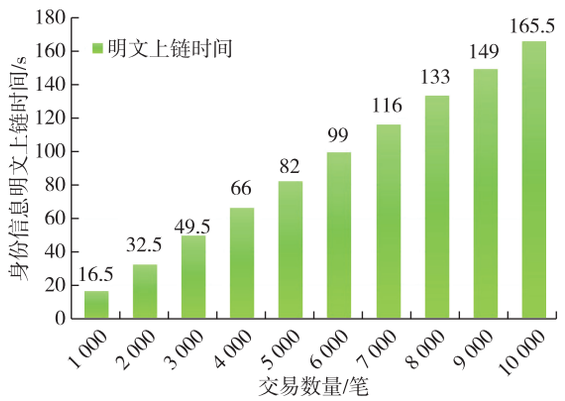


图 9　身份信息明文上链时间

Fig. 9　Time spent for identity information plaintext uploaded to blockchain

笔身份信息明文交易大约需要 219 136 KB 的空间.可以看出,在同样的交易数量下,身份信息密文占用的存储空间比身份信息明文占用的存储空间大,但是基本在一个数量级上,且存储空间增加量不超过百分之五,属于可接受范围.

表 2　链上身份信息存储空间差异表

Table 2　Storage space comparison of identity information on blockchain

交易数量/笔	身份信息密文/KB	身份信息明文/KB
2 000	45 056	43 008
4 000	86 016	86 016
6 000	135 168	133 120
8 000	180 224	176 128
10 000	221 184	219 136

通过对吞吐量、出块时间和存储空间这 3 个性能指标进行评估,可以得出基于区块链的多方协作安全身份认证机制的效率较高,其吞吐量优于其他主流存证区块链平台,出块时间也比比特币、以太坊等主流区块链平台快,存储复杂度可接受.所以,基于区块链的多方协作安全身份认证机制在实现支持隐私保护的可靠且准确的身份认证的同时,又保证了身份认证的效率.

6　结束语

针对当前身份认证机制存在的诸如数据泄露等问题,为了解决现有身份认证痛点,结合区块链技术,利用区块链的去中心化和不可篡改等特性,提出了保障身份数据完整性、可靠性和可信性的基于区块链的多方协作安全身份认证机制.进而实现了基于区块链的多方协作安全身份认证系统,在区块链上完成了身份授权、身份认证和数据共享等功能,且在实现可靠身份认证的同时,还保证了信息的权威性,并在一定程度上减少了数据冗余,提高了身份认证效率,保证了全面且准确的身份认证.从而为将来研究支持多种类身份特征信息认证机制等相关技术提供了基础研究.

参考文献

References

[1] 荆继武.网络可信身份管理的现状与趋势[J].信息安全研究,2016,2(7):666-668
JING Jiwu. The development status and tendency of Internet trusted identity management[J].Journal of Information Security Research,2016,2(7):666-668

[2] 夏振杰.基于人脸识别技术的身份认证系统实现简介[J].科技信息,2010(5):44,23
XIA Zhenjie. Introduction to identity authentication system based on face recognition technology[J].Science & Technology Information,2010(5):44,23

[3] 王帅,常朝稳,魏彦芬.基于云计算的 USB Key 身份认证方案[J].计算机应用研究,2014,31(7):2130-2134
WANG Shuai,CHANG Chaowen,WEI Yanfen.USB Key authentication scheme based on cloud computing[J].Application Research of Computers, 2014, 31(7):2130-2134

[4] 余幸杰,高能,江伟玉.云计算中的身份认证技术研究[J].信息网络安全,2012(8):71-74
YU Xingjie,GAO Neng,JIANG Weiyu.Research on the authentication in cloud computing[J].Netinfo Security,2012(8):71-74

[5] 杨勇,许杰.个人身份认证技术及其研究进展[J].通信技术,2017,50(1):124-128
YANG Yong,XU Jie.Personal identity verification technology and research progress[J].Communications Technology,2017,50(1):124-128

[6] 张利华,沈友进.基于 ECC 和指纹 USBKey 的身份认证协议[J].华东交通大学学报,2014,31(2):95-98
ZHANG Lihua,SHEN Youjin.A novel user authentication scheme based on ECC and fingerprint USBKey[J].Journal of East China Jiaotong University,2014,31(2):95-98

[7] 徐钦桂,黄培灿,杨桃栏.增强的基于生物密钥智能卡远程身份认证方案[J].计算机研究与发展,2015,52(11):2645-2655
XU Qingui,HUANG Peican,YANG Taolan.An enhanced biometrics-key-based remote user authentication scheme with smart card[J].Journal of Computer Research and Development,2015,52(11):2645-2655

[8] Hammudoglu J S, Sparreboom J, Rauhamaa J I, et al. Portable trust:biometric-based authentication and blockchain storage for self-sovereign identity systems[J].arXiv e-print,arXiv:1706.03744

[9] Moinet A,Darties B,Baril J-L.Blockchain based trust &

authentication for decentralized sensor networks[J]. arXiv e-print,arXiv:1810.01291
[10] Alexopoulos N, Daubert J, Muhlhauser M, et al. Beyond the hype: on using blockchains in trust management for authentication[C]//IEEE Trustcom/BigDataSE/ICESS, 2017, DOI:10.1109/Trustcom/BigDataSE/ICESS.2017.283
[11] Lundbaek L N, D'Iddio A C, Huth M. Optimizing governed blockchains for financial process authentications[J]. arXiv e-print, arXiv:1612.00407
[12] Fromknecht C, Velicanu D, Yakoubov S. A decentralized public key infrastructure with identity retention[J]. IACR Cryptology ePrint Archive, 2014, 2014:803
[13] Isaakidis M, Halpin H, Danezis G. UnlimitID: privacy-preserving federated identity management using algebraic MACs[C]//ACM on Workshop on Privacy in the Electronic Society, 2016, DOI:10.1145/2994620.2994637
[14] Matsumoto S, Reischuk R M. IKP: turning a PKI around with decentralized automated incentives[C]//IEEE Symposium on Security and Privacy, 2017, DOI:10.1109/SP.2017.57
[15] 李珊,余少标,王功文,等.基于NFC和商用密码技术的防伪溯源系统研究[J].数码世界,2017(5):58-60
LI Shan, YU Shaobiao, WANG Gongwen, et al. Research on anti-forgery traceability system based on NFC and commercial cryptography[J]. Digital Space, 2017(5): 58-60
[16] 丁冬平,高献伟.SM3算法的FPGA设计与实现[J].微型机与应用,2012,31(5):26-28
DING Dongping, GAO Xianwei. Design and implementation of SM3 algorithm on FPGA[J]. Microcomputer & Its Applications, 2012, 31(5):26-28
[17] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].[2019-07-01].https://bitcoin.org/bitcoin.pdf
[18] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,42(4):481-494
YUAN Yong, WANG Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4):481-49

Research on blockchain-based multi-party collaborative security authentication mechanism

SANG Anqi[1] SHEN Meng[1,2] ZHU Liehuang[1] LIU Sheng[3] YIN Shu[3] XIAO Yao[1]
1 School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081
2 State Key Laboratory of Cryptology, Beijing 100878
3 Union Mobile Financial Technology, Beijing 100082

Abstract With the rapid development of information technology, the security of authentication mechanism has received more and more extensive attention. However, the existing identity authentication mechanism has the risk of privacy threat. Thus, designing a more reliable authentication mechanism is in urgent need. This paper designed a multi-party collaborative security authentication mechanism based on the blockchain for its decentralized and tamper-proof features. While achieving reliable identity authentication, it ensures the authority of information, reduces data redundancy, improves the authentication efficiency, and realizes comprehensive and accurate authentication. Finally, the authentication system is implemented, which enables multiple data service providers to encrypt and sign identity information, protect data privacy, and share data with multiple parties.

Key words blockchain; authentication; authorization; multi-party collaboration