计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(3):178−187 [doi: 10.15888/j.cnki.csa.008407]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于教育区块链与无证书签名的身份认证方案①

王晓欣[1], 陈志德[2]

[1](福建师范大学 计算机与网络空间安全学院, 福州 350117)
[2](福建师范大学 福建省网络安全与密码技术重点实验室, 福州 350007)
通信作者: 王晓欣, E-mail: 2603956322@qq.com

摘　要: 针对当前教育资源共享安全性低和身份认证困难的问题, 提出了一种区块链技术与无证书签名相结合的可跨域身份认证方案, 将无证书签名技术的高安全性、无密钥托管问题等优点应用到区块链的分布式网络中, 实现了身份认证过程中用户安全、跨域认证、恶意用户可追溯、注册信息不可篡改. 首先, 基于教育区块链与无证书签名的身份认证方案是建立在区块链架构下的身份认证模型, 设计了域内区块链和跨域区块链, 建立了跨域认证的模型. 其次, 利用无证书签名以及陷门哈希函数, 确保认证过程用户安全以及恶意用户可追溯. 通过分析, 本方案满足相互认证、用户身份安全等安全属性. 与其他方案相比, 用户计算代价小, 安全性更高, 更能满足用户端算力有限的计算环境.

关键词: 区块链; 身份认证; 无证书签名; 可追踪恶意用户

引用格式: 王晓欣,陈志德.基于教育区块链与无证书签名的身份认证方案.计算机系统应用,2022,31(3):178–187. http://www.c-s-a.org.cn/1003-3254/8407.html

Identity Authentication Scheme Based on Educational Blockchain and Certificateless Signature

WANG Xiao-Xin[1], CHEN Zhi-De[2]

[1](College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China)
[2](Fujin Provincial Key Laboratory of Network Security and Cryptology, Fujian Norm University, Fuzhou 350007, China)

Abstract: To address the low security and identity authentication difficulties of education resource sharing, this study proposes a cross-domain identity authentication scheme based on Blockchain technology and certificateless signature. The user security, cross-domain authentication, traceability of malicious users, and non-tamperable registration information are realized during the identity authentication process by the sharing of high security and no need for key escrow in the certificateless signature technology with Blockchain distributed networks. First, intra-domain Blockchain and cross-domain Blockchain are designed to facilitate the cross-domain authentication by a Blockchain-based identity authentication model. Then, user safety and traceability of malicious users are guaranteed by certificateless signature and trapdoor hash functions in the authentication phase. Through the analysis, this scheme meets the security attributes such as mutual authentication and user identity security. Compared with other schemes, it has advantages in computing overhead and communication overhead. The scheme can better meet the computing environment with limited computing power on the user side.

Key words: Blockchain; identity authentication; certificateless signature; traceable malicious user

随着云计算技术和互联网技术的不断发展, 在教育领域, 教育云平台已经成为了实现教育信息化的重要方式, 而教育信息化的发展程度更是成为了衡量一个国家教育现代化程度的重要标志[1]. 教育云平台可以

① 基金项目: 广东省重点领域研发计划 (2019B010137002)
收稿时间: 2021-05-31; 修改时间: 2021-07-05; 采用时间: 2021-07-23; csa 在线出版时间: 2022-01-24

为用户提供方便快捷的教育资源和服务, 但是也带来了一些问题. 首先, 为了访问不同平台的资源, 用户需要注册多个平台, 这使得一旦一个平台泄露用户信息, 用户在其他平台的数据也可能会威胁; 另外大部分平台采用中心化的管理方式, 平台抵抗恶意攻击的能力差, 用户隐私数据也容易泄露; 最后, 对于用户来说, 管理多个账号信息也比较麻烦. 针对以上问题, 可以让同区域的教育云平台构建区域教育网络, 让用户注册一个账号就可以访问本域和权限范围内的异域教育平台的资源. 为了保证用户隐私安全, 因此需要在区域教育网络中建立一种安全、可跨域的身份认证方案.

目前, 在云环境中常用身份认证方案有以下几种: 1) 基于公钥基础设施 (public key infrastructure, PKI) 的身份认证方案[2]; 2) 基于无证书的公钥密码体制认证方案[3,4]; 3) 基于代理盲签名的认证方案[5]. 其中文献 [2] 改进了传统的 PKI, 设计了轻量型的 PKI 身份认证方案, 但是证书验证过程复杂.文献 [3] 和文献 [4] 则是引入无证书密码体制来解决了 PKI 体系中的证书问题, 其中文献 [3] 通过无对运算的聚合签名实现高效的批认证, 提高认证效率, 但未解决双向认证的问题; 文献 [4] 利用便携式 TPM (portable trusted platform module, PTPM) 实现任意终端与云端的双向认证, 但是未解决跨域认证问题. 在文献 [5] 提出了代理盲签名的异构身份认证方案, 解决了异构跨域身份问题, 但该方案中需要引入可信第三方, 一旦可信第三方遭受攻击便会对用户造成巨大损失.

区块链技术作为一种新兴的技术, 具有匿名性、去中心化、不可篡改、可追溯的特性, 因此在身份认证领域地吸引了大量学者进行研究. 文献 [6] 提出了一种基于区块链的分布式物联网设备认证框架, 解决了集中式认证兼容性低和单点故障的问题, 但未解决跨域认证的问题. 文献 [7] 提出了一种基于区块链的高效跨域认证方案, 解决了跨域认证问题, 并可以实现高效的身份认证, 但不能进行异构的身份认证; 文献 [8] 提出了一种基于区块链的跨异构的认证方案, 解决了异构的跨域认证, 但是该方案只能针对基于 PKI 的信任域和基于身份密码体制的信任域的异构跨域认证. 文献 [9] 设计了一种基于可编辑区块链的身份认证方案, 解决了跨域认证问题, 但是该方案需要网络供应商的参与, 方案实施比较困难.

本文针对多区域教育网络的身份认证问题, 提出了一种基于教育区块链和无证书签名的身份认证方案. 首先给出了身份认证模型, 通过建立本地链和跨域链, 来实现用户访问本地资源的本域身份认证和访问其他域的跨域身份认证. 利用无证书签名算法和用户身份证明来设计身份认证的具体过程, 保证了用户的安全也解决了密钥托管问题; 通过设置陷门哈希, 当有恶意节点出现时, 便可以追溯到真实的恶意用户. 本方案在安全性上实现了用户身份的匿名性, 以及用户和机构的双向认证, 可以抵挡多种安全攻击. 在性能上, 与其他方案相比, 用户的计算开销较少, 签名过程也比较简单.

1 相关知识

1.1 区块链技术

区块链最早是由中本聪在 2008 年的论文“Bitcoin: A peer-to-peer electronic cash system” [10] 中提出的. 在 2009 年, 中本聪建立了比特币网络, 并开发了其第一个区块, 名为创世区块. 区块链技术具备去中心化、可追溯、不可篡改等优势.根据准入机制的不同, 区块链可以分为 3 类: 公有链、联盟链和私有链. 其中公有链任何人都可以读取, 所有数据默认公开, 但交易速度慢; 私有链将区块链的写入权限仅仅在一个组织或者个人手里, 具备交易速度快、安全性更高但是中心化程度更高; 联盟链是介于公有链和私有链之间的区块链, 一般指若干机构或者组织共同参与管理的区块链, 其交易速度比公有链快, 去中心化程度比私有链好. 在本方案中, 我们域内区块链和跨域区块链都是联盟链.

1.2 无证书签名体制

在 2003 年, Al-Riyami 等人提出了无证书的密码体制 CL-PKC (certificateless public key cryptography, CL-PKC) [11]. 在该密码体制中其中用户的私钥是由密钥生成中心 KGC (key generation center) 生成的部分私钥和用户秘密值的组合. 因此, CL-PKC 解决了密钥托管问题. 对于无证书签名来说, 一般包含以下 6 个算法[12]: 系统初始化、部分私钥生成、秘密值的生成、用户公私钥生成、用户签名算法生成、签名验证.

在本方案中, 用户的部分密钥生成算法、秘密值的生成以及用户公私钥的生成均在用户注册过程中完成.

1.3 困难问题及假设

椭圆曲线离散对数问题 (elliptic curve discrete logarithm problem, ECDLP): 给定一个椭圆曲线群 G,

且$P,Q\in G$, 找到一个标量点$a\in Z_P$, 满足$Q=aP$, 其中, P 是群 G 的生成元, Q 是 G 中的一个元素.

2 基于教育区块链身份认证模型的设计

在本节介绍了基于教育区块链的身份认证模型的模型假设、身份认证模型以及设计目标.

2.1 模型假设

(1) 整个系统中的每一个节点都有唯一分配的地址, 对应其真实 ID;

(2) 假设方案初始化的阶段是安全的;

(3) 权威节点是教育局等权威机构, 具备完备的安全性;

(4) 权威节点和机构节点都具备一定的存储和计算能力;

(5) 用户可以下载机构节点和权威节点的公钥和身份.

2.2 教育区块链身份认证模型

基于教育区块链的身份认证方案, 设计了域内联盟链以及跨域联盟链两种类型的区块链. 域内区块链负责本域内用户对域内的机构进行访问时的身份认证; 跨域区块链在身份认证中负责用户对跨机构进行访问时的身份认证.

该模型有 3 种类型的参与者: 普通用户、机构、权威部门. 其中跨域区块链由教育局这样的权威部门构成权威节点来进行维护, 普通用户以及机构节点可以查看区块链中的信息; 域内区块链主要由本域的机构节点来维护账本信息, 本域内的普通用户节点只有查看的权限. 模型架构图如图 1 所示.

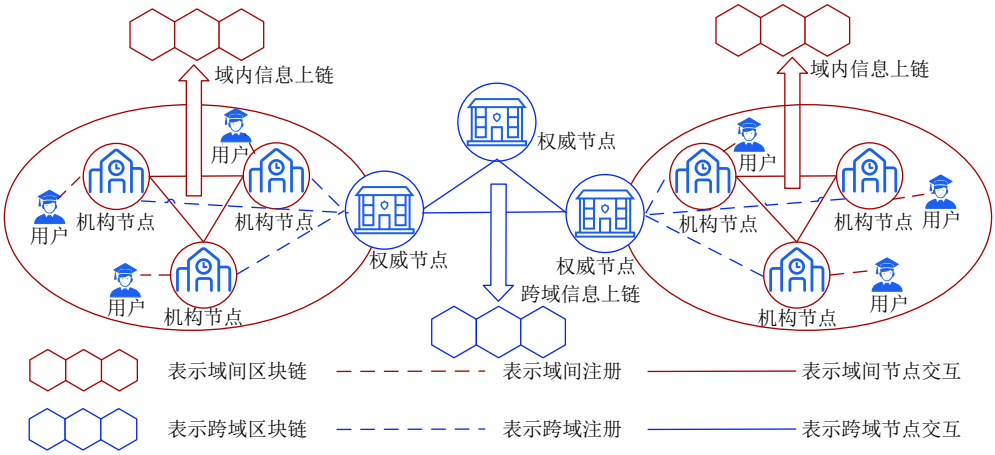

图 1 基于区块链的多域身份认证模型

权威节点: 主要负责机构节点的身份注册以及为合法的跨域用户颁发跨域身份证明, 并将跨域用户的信息进行上链处理.

机构节点: 主要包括学校、教育机构等, 他们负责帮助普通用户节点完成注册, 并将域内合法用户的注册信息写入到域内联盟链中.

普通节点: 主要由学生、教师等组成.他们是机构节点的用户, 教育资源的拥有者和使用者.

2.3 设计目标

在教育云场景中用户的身份隐私安全有比较高的需求, 设计了以下几个目标.

去中心化: 针对目前教育资源共享平台大多采用集中式的管理方式, 这使得用户的隐私数据很容易被第三方掌控, 一旦第三方被攻击, 很有可能会造成用户在各个平台数据的泄露.

用户身份安全: 教育资源共享平台往往掌握大量用户数据, 为了保证用户的隐私安全, 采用匿名的用户身份, 并且让用户私钥掌握在自己手中.

相互认证: 在用户注册以及认证过程, 不仅仅限于机构对用户进行认证, 用户同样也对机构进行认证. 双向认证可以提高用户的信任, 增加用户的使用率. 并且可以及时发现用户或者机构的恶意行为.

恶意用户追溯: 针对教育资源共享时, 用户量大. 确保当系统中出现恶意用户时, 可以及时将恶意用户记录在本域和跨域区块链上, 并且不再为该用户服务. 这样可以防止恶意用户在其他机构节点进行

再次注册, 同样也可以避免恶意节点占用通信资源. 因此本方案的设计目标可以实现恶意用户节点的可追溯, 从而追溯到真正的用户, 防止其恶意行为的再次发生.

3 跨域-追溯认证方案

本节介绍了基于教育区块链的身份认证方案的具体细节, 包含方案总述、具体方案两部分.

3.1 方案总述

在本方案中, 我们采用通过区块链技术来实现分布式的身份认证, 并根据文献 [3], 设计无双线性对的无证书认证方案, 来提高认证的效率.

该方案包含初始化阶段、注册阶段、认证阶段、恶意节点追溯阶段 4 个阶段.

(1) 初始化阶段. 初始化阶段主要生成全局参数以及权威节点的公私钥.

(2) 注册阶段. 包含机构注册和用户注册两部分. 用户通过域内联盟链的机构节点完成用户注册. 跨域区块链的权威阶段主要完成对机构节点的注册.

(3) 认证阶段. 包含域内认证和跨域认证. 对用户和机构进行双向身份认证, 从而保证双方访问的安全性.

(4) 恶意节点追溯阶段. 对于出现恶意节点, 通过查询区块链中的注册信息追溯恶意节点, 将恶意节点信息写入到联盟链中.

3.2 具体方案

(1) 初始化阶段

初始化阶段为系统生成全局参数进行广播, 每个权威节点也生成各自的公私钥对, 然后将他们各自公钥和权威节点身份上传到域间区块链.

KGC 作为全局的参数生成中心, 首先, 随机选择一个安全参数$k \in Z^+$作为输入; 然后 *KGC* 会选择一个椭圆曲线上的加法群 G, 素数 q, 并且 P 是 G 的生成元. 再选择 3 个抗碰撞的哈希函数$H_i : \{0,1\}^* \to Z_q^* \ \ (i = 1,2,3)$. 最后广播系统参数$params = \{G, q, P, H_1, H_2, H_3\}$.

对于每一个权威节点 AID_i, 随机选择数$y_i \in Z_q^*$, 并计算其公钥$PK_i = y_i P$, 私钥为$SK_i = y_i$, 并广播到跨域区块链上$\{AID_i, PK_{AID_i}\}$.

(2) 注册阶段

注册阶段包含机构的注册以及用户的注册. 当注册完成将会把它们的公钥以及身份信息分别上传到跨域区块链以及用户所在的域内区块链, 并且注册节点会为注册的机构和用户生成身份证明, 如表 1.

表 1 身份证明

名称	含义
ID	身份证明拥有者的ID
PK	身份证明拥有者的公钥
Reg-ID	身份证明颁发者的身份ID
T-begin	身份证明颁发时间
T-end	身份证明到期时间
Area	身份拥有者所属域
Sig	颁发者的签名信息

1) 机构节点的注册

机构节点注册需要经过权威节点对其进行身份验证, 验证通过便完成机构节点注册, 然后权威节点将注册信息上传到区块链中. 机构注册流程图如图 2 所示.

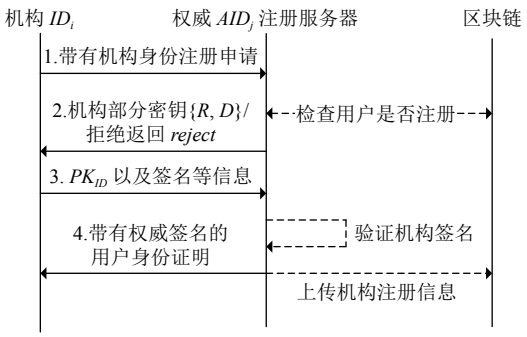

图 2 机构注册流程图

① ID_i向AID_j发送注册申请

机构ID_i先下载权威节点AID_j的公钥, 然后生成时间戳t_{reg}以及随机数N_1向本域的权威节点发送注册请求$reg_req_{ID_i}\left(En\left(ID_i, t_{reg}, N_1\right)_{PK_{AID_j}}, t_{reg}, AID_j\right)$.

② AID_j回复ID_i的注册请求

权威节点AID_j先检查t_{reg}是否合理. 解密消息之后, 检验t_{reg}是否一致, 然后查询域间的区块链上是否存在该机构. 如果存在则返回$reject$拒绝机构的注册申请; 如果ID_i不存在则允许机构用户进行注册, 并为ID_i生成部分私钥和部分公钥. 首先, 权威节点AID_j的 *KGC* 为其随机选择随机数$r_i \in Z_q^*$, 然后计算$h_{1,i} = H_1(AID_j, ID_i, R_i)$, 从而为机构$ID_i$生成部分公钥$R_i = r_i P$和部分私钥$d_i = (r_i + y_j h_{1,i}) \bmod q$. AID_j通过安全通道发送给ID_i带有其部分公私钥并允许机构注册的回复$rep_req_{AID_j}$ $(H_2(ID_i \| AID_j \| N_1), t_{req}, R_i, d_i)$.

③ ID_i生成公私钥并将公钥发送给AID_j

机构用户ID_i接收到消息先检查t_{req}是否合理, 然后

验证$H_2(ID_i\|AID_j\|N_1)$的正确性. 如果验证不通过则用户返回 *error*, 若想需要重新提交信息注册. 若验证通过, 机构节点ID_i随机选取一个随机数$x_i \in Z_q^*$, 计算$X_i = x_iP$和$h_{2,i} = H_2(AID_i, ID_i, X_i)$, 计算部分公钥$Q_i = R_i + X_ih_{2,i}$. 随后$ID_i$生成计算自己的公钥$PK_{ID_i} = (Q_i, X_i)$和私钥信息$SK_{ID_i} = (d_i, x_i)$. 然后$ID_i$生成自己的签名信息, 先随机选择一个$u_i \in Z_q^*$, 计算$U_i = u_iP$和$h_{3,i} = H_3(ID_i\|PK_i\|t)$, 生成签名 $\delta_{ID_i} = u_i + (d_i + x_ih_{2,i})h_{3,i} \bmod q$, 其中 t 是机构签名时间. 然后ID_i向AID_j发送带有签名和其公钥的回复消息$m = \{PK_{ID_i}, ID_i, En(t, \delta_{ID_i}, U_i)_{PK_{ID_i}}\}$.

④ AID_j为ID_i生成身份证明并将其注册信息上链

AID_j解密消息, 提取出$\{t, \delta_{ID_i}, U_i\}$. 先计算$h_{3,i} = H_3(ID_i\|PK_i\|t)$. 验证机构$ID_i$的签名是否满足: $\delta_{ID_i}P \stackrel{?}{=} U_i + h_{3,i}(Q_i + PK_{AID_i}h_{1,i})$. 等式成立即代表对用户身份验证通过, 为其生成身份信息. 首先获取当前时间 t_{temp}, 并计算$T_1 = H_1(AID_i\|PK_{AID_i}\|t)$. 然后生成签名$\delta_{AID_j} = (r_{ID_i} + y_iH_1(ID_i\|AID_j))T_1$. 然后为机构注册节点$ID_i$颁发它的身份证明$\{En(cert_{ID_i})_{pk_{ID_i}}, t_{\text{temp}}\}$.

最后, ID_i解密消息先时间戳t_{temp}, 之后保存身份证明 $cert_{ID_i}$. 权威节点AID_j然后将机构ID_i注册信息$\{ID_i, PK_{ID_i}, H_1(ID_i\|AID_j)\}$上传到区块链中.

2) 普通用户的注册

普通用户的注册需要经过机构节点对其进行身份验证, 验证通过之后机构节点将注册信息上传到区块链. 普通用户的身份注册流程如图 3 所示. 为了保护用户的身份信息, 规定用户u_i的身份为 id_i=*hash*(u_i||ID_i). 注册具体过程如下.

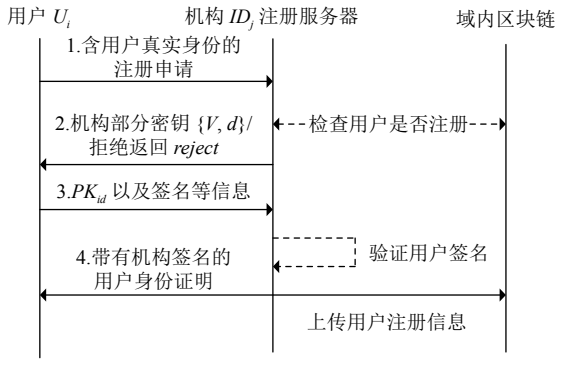

图 3　用户注册流程图

① id_i向ID_j发送注册申请

用户id_i先下载注册机构ID_j的公钥PK_{ID_j}, 然后生成时间戳t_{reg}以及随机数N_1. 然后向ID_j发送注册申请 $reg\_req_{id_i}\left(En(u_i, t_{reg}, N_1)_{PK_{ID_j}}, ID_j\right)$.

② ID_j回复id_i的注册请求

机构节点ID_j先解密消息之后, 检查t_{reg}是否合理, 再查询域间的区块链上是否存在该用户. 如果存在该用户则返回*reject*拒绝该用户的注册申请; 如果id_i不存在则允许用户u_i注册, 为它生成其部分私钥和部分公钥. 首先机构节点先生成随机数$v_i \in Z_q^*$, 计算出用户的部分公钥$V_i = v_iP$. 然后计算$h_{1,i} = H_1(ID_j, id_i, V_i)$再计算得到用户的部分私钥$b_i = (v_i + x_jh_{1,i}) \bmod q$. 通过安全信道发送回复 $rep\_req_{ID_j}(H_2(id_i\|ID_j\|N_1), t_1, V_i, b_i)$ 给用户.

③ id_i生成公私钥并将公钥发送给ID_j

机构用户id_i接收到消息先检查t_1是否合理, 然后验证$H_2(id_i\|ID_j\|N_1)$的正确性. 如果验证不通过则用户返回*error*, 若想继续注册则更换其他机构节点进行注册.验证通过后, 用户id_i提取出部分公钥V_{id_i}和部分私钥d_{id_i}. 然后id_i生成随机数$o_i \in Z_p^*$, 计算出用户u_i部分公钥$O_i = o_iP$, 随后计算$h_{2,i} = H_2(ID_j, id_i, O_i)$, 然后计算$C_i = V_i + O_ih_{2,i}$, 生成公钥$pk_{id_i} = (C_i, O_i)$和私钥$sk_{id_i} = (o_i, b_i)$. 然后用户$id_i$随机选择一个数$e_i \in Z_p^*$并计算$E_i = e_iP$和$h_{3,i} = H_3(id_i\|pk_i\|t_2)$, 生成签名信息$\sigma_{id_i} = n_i + h_{3,i}(b_i + o_ih_{2,i}) \bmod q$, 其中$t_2$是用户签名时间. 发送消息$m = \{pk_{id_i}, id_i, En(t_2, \sigma_{id_i}, E_i)_{PK_{ID_j}}\}$给$ID_j$.

④ ID_j为id_i生成身份证明并将其注册信息上链.

机构ID_j接收到消息m, 解密消息得到$\{t_2, \sigma_{id_i}, E_i\}$然后验证用户$id_i$签名的有效性. 首先, ID_j计算$h_{3,i} = H_3(id_i\|pk_{id_i}\|t_2)$, 然后用下面等式验证用户签名$\sigma_{id_i}P \stackrel{?}{=} E_i + (Q_i + X_jh_{1,i})h_{3,i} \bmod q$. 若等式不成立用户公钥有误, 要求用户重新发送带有公钥信息的签名消息.若等式成立, 则用户注册成功. 机构为用户id_i生成身份信息$m_{id_i} = \{id_i, pk_{id_i}, ID_j, T_{\text{begin}}, T_{\text{end}}, Area_{id_i}\}$, 其中$T_{\text{begin}}$是机构为用户生成身份信息的时间, T_{end}是失效时间.先生成随机数$s_i \in Z_p^*$, 计算$S = s_iP$, 再计算$T_2 = H_1(ID_j\|PK_{ID_j}\|m_{id_i})$, 为用户$id_i$计算出身份证明中的签名$\sigma_{ID_j} = s + (d_j + x_jH_2(AID_i, ID_i, X_i))T_2$. 然后, 为$id_i$生成它的身份证明$cert_{id_i} = \{m_{id_i}, \sigma_{ID_j}\}$.

最后ID_j将$\{En(cert_{id_i})_{pk_{id_i}}, T\}$发送给注册用户$id_i$, 并将该用户注册信息$\{id_i, pk_{id_i}\}$上传到域间区块链上. 用户验证时间戳之后, 解密消息并保存身份证明 $cert_{id_i}$.

(3) 域内认证过程

用户注册成功, 就成为了本域的合法用户, 可以与其他节点进行通讯. 域内进行访问时, 只需要通过域内机构节点的参与下完成用户和机构的双向身份认证即可.

当用户 a 对域内的机构 B 进行访问时, 需要对完成 a 和 B 之间的双向认证. 首先, a 发送访问请求给机构 B $acc-connect_a(En(id_a,ID_B,cert_{id_a})_{PK_{ID_B}},id_a)$. 机构 B 收到请求之后, 用自己的私钥解密加密信息, 验证 id_a 的一致性, 然后域内区块链来验证身份证明. 在机构 B 发送回复 $acc-connect_B(En(ID_B,id_a,cert_{ID_B})_{PK_{id_a}},ID_B)$ 给用户 a, 用户用自己的私钥解密加密消息, 验证 id_a 的一致性, 然后将身份证明 $cert_{id_a}$ 交由域内区块链验证证明的有效性. 对以用户 id_a 证明验证的流程如下.

1) 首先查看证明里面的消息 m, 检查用户 a 信息;

2) 验证用户 a 注册的机构节点 A 签名的正确性;

3) 若全部验证成功, 则返回 *accept*, 否则返回 *reject*;

对机构 B 的身份证明验证同上, 当双方均收到 *accept* 则双方身份验证成功.

算法 1. 对用户 id_a 的身份证明进行验证过程如下:

其中在验证用户 a 的身份证明中的签名时, 首先计算 $T=H_1(ID_A\|PK_{ID_A}\|m_{id_a})$, 然后检查是否满足下式:

$$\sigma_{ID_A}P\stackrel{?}{=}S_a+(Q_A+PK_{AID_A}H_1(ID_A,R_{ID_A}))T$$

算法 1. 用户身份证明域内验证

输入: $cert_{id_a}$、ID_B

输出: *accept or reject*

Begin

// pb is an intra-blockchain

If ($Equal(Area_a,Area_B)$ = flase) **then**

  Return *reject*;

If ($UserExits(id_a,PB)$ = flase) **then**

  Return *reject*;

If ($NodeExits(ID_A)$ = flase) **then**

  Return *reject*;

If ($ValidTime(T_{\text{begin}},T_{\text{end}})$ = flase) **then**

  If ($Verify-sig(\xi_{AID_A})$=false)

    Return *reject*;

  Else return *accept*;

End

算法 2. 对机构 ID_B 的身份证明进行验证过程如下:

在验证机构 B 的身份证明中的签名时, 首先计算 $T=H(AID_B\|PK_{AID_B}\|m_{ID_B})$, 然后检查是否满足下式:

$$\delta_{AID_B}P\stackrel{?}{=}(R_{ID_B}+PK_{AID_B}H_1(ID_B\|AID_B))T$$

算法 2. 机构身份证明域内验证

输入: $cert_{ID_B}$、id_a

输出: *accept or reject*

Begin

// pb is an intra-blockchain

If ($Equal(Area_a,Area_B)$ = flase) **then**

  Return *reject*;

If ($NodeExits(ID_B,pb)$ = flase) **then**

  Return *reject*;

// PB is an intra-blockchain

If ($NodeExits(AID_A,PB)$ = flase) **then**

  Return *reject*;

If ($ValidTime(T_{\text{begin}},T_{\text{end}})$ = flase) **then**

  If ($Verify-sig(\xi_{AID_A})$=false)

    Return *reject*;

  Else return *accept*;

End

(4) 跨域认证过程

在跨域身份认证过程, 用户提出跨域申请, 然后权威节点为用户颁发跨域身份证明. 表 2 是用户跨域身份证明格式.

表 2 用户跨域身份证明

名称	含义
ID	用户的虚拟身份ID
PK	用户的公钥信息
f-Area	用户所属域的信息
State	用户身份证明颁发时间
T-begin	跨域身份证明颁发时间
T-end	跨域身份证明到期时间
Sig	本域的身份颁发者的签名信息

用户跨域的主要包含: 用户跨域身份证明的申请、用户申请跨域访问两部分, 其中前者主要为用户生成用户跨域证明, 而后者主要完成双方的身份认证.

1) 用户申请跨域身份证明

① id_a 发送跨域申请给 AID_A

用户 id_a 想要请求异域机构时的服务的时候, 先下载权威机构 AID_A 的公钥, 再发送给它注册请求.

$$reg\_carea(En(cert_{id_a},T,id_a)_{PK_{Auth\_A}},area_1).$$

② AID_A 为用户生成跨域身份

权威节点 AID_A 用私钥解密解密消息之后, 先检查时间戳 T 是否合理, 若合理将身份证明 $cert_{id_a}$ 发送给域 $area_1$ 进行验证, 否则则返回 *reject*.

若身份验证成功则为用户 id_a 生成跨域身份证明 $crocert_a=\{id_a,PK_{id_a},AID_A,T_{\text{begin}},T_{\text{end}},\xi_{AID_A}\}$ 其中, 令

$m=\{id_a, PK_{id_a}, T_{\text{begin}}, T_{\text{end}}, AID_A\}$, 然后随机生成随机数 $w_a \in Z_p^*$, 并计算$W_a = w_a P$, 随后计算用户跨域证明中的签名$\xi_{AID_A} = y_{AID_A} H_1(AID_A \| id_a \| T) + w_a$, 其中 T 是允许访问的时间. 然后将消息$\{En(crocert_a, W_a)_{pk_{id_a}}, T\}$给用户$id_a$.

最后并将用户的跨域信息上传到区块链上$\{id_a, pk_{id_a}, AID_A\}$. 而用户$id_a$接收到消息之后, 用自己的私钥解密消息之后, 保存$\{crocert_a, W_a\}$.

2) 用户跨域访问

① 当用户id_a要访问异域的机构ID_{1_B}时, 先在跨域区块链中下载它的公钥$PK_{ID_{1_B}}$, 再给异域机构发送访问请求$acc_req(En(crocert_a, W_a, id_a, t)_{PK_{ID_{1_B}}})$.

② 机构ID_{1_B}收到访问请求后, 先用私钥$SK_{ID_{1_B}}$解密消息, 检查时间 t 和id_a是否合理. 若一致发送$acc-rep(En(ID_{1_B}, id_a, cert_{ID_{1_B}}, T)_{PK_{id_a}})$给$id_a$, 同时将$\{crocert_a, W_a, id_a\}$发送给跨域区块链, 让跨域区块链验证$id_a$的身份. 身份验证成功, 跨域区块链会生成 *accpet*; 否则返回 *false*.

③ 用户id_a收到ID_{1_B}的消息后, 用自己的私钥解密, 验证时间戳 T 是否合理, ID_{1_B}是否正确. 若均通过验证, 用户便将$\{ID_{1_B}, cert_{ID_{1_B}}\}$交由跨域区块链对$ID_{1_B}$进行身份认证.

④ 若跨域区块链对id_a的跨域身份证明和ID_{1_B}的身份均验证成功, 则分别向双方返回 *accept*; 若一方身份验证未成功, 则分别对应返回 *reject*.

算法 3. 跨域身份认证

输入: $crocert_a$、ID_{1_B}、W_a
输出: *accept or reject*

```
Begin
// PB is an cross-blockchain
If (UserExits(id_a,PB) = flase) then
   Return reject;
If (NodeExits(AID_A) = flase) then
  Return reject;
If (ValidTime(T_begin,T_end) = flase) then
  If (Verify-sig(ξ_AID_A)=false)
     Return reject;
   Else return accept;
End
```

其中验证的AID_A签名ξ_{AID_A}, 先计算$H_1(AID_A \| id_a \| T)$, 验证下列等式是否成立:

$$\xi_{AID_A} P \stackrel{?}{=} PK_{AID_A} H_1(AID_A \| id_a \| T) + W_a$$

若上述认证算法执行完毕, 输出 *accept*, 则对跨域用户id_a完成了身份认证; 否则输出 *reject*, 则对td_a身份认证失败.

在跨域认证中, 除了验证节点变成了权威节点, 对于机构ID_{1_B}的身份认证算法基本与域内算法一致, 这里就不再陈述.

(5) 恶意用户追溯

当出现恶意用户的时候, 恶意用户可能会将自己的私钥泄露给别人, 和其他恶意用户发动共谋攻击; 或者进行重放攻击占用通信资源. 机构节点监测到用户出现上述恶意行为时, 将会通过共识机制和各个机构节点达成共识, 然后通过查询区块链中的注册信息, 让该用户的注册节点追溯用户真实身份, 然后触发智能合约将用户真实身份写入区块链中. 恶意用户真实身份信息记录在区块链上, 可以避免恶意用户更换注册节点, 进行身份再注册.

对于恶意用户, 机构节点无法知道用户的真实身份信息, 仅仅知道其"假身份"id_a是恶意的, 被访问的机构节点通过查询区块链上的信息$\{id_a, pk_{id_a}, ID_B\}$, 然后各个节点通过达成对$id_a$真实身份的追溯的共识, 然后$id_a$的注册节点$ID_B$将在本机构注册的全部用户的$u_i$带入到式子$id_a \stackrel{?}{=} H(u_i \| ID_B) \quad (i = 1, \cdots, N)$, 其中 N 为在该机构进行注册的用户数量.直到找到u_s满足上述等式, 便找到了恶意用户u_s, 各个节点对于结果达成一致共识之后, 便可以将恶意用户真实信息上传到区块链中, 实现恶意用户的记录. 当然对于可能误判的或者可能被窃取的恶意用户, 用户可以向权威部门进行申请, 然后权威部门将恶意记录进行消除. 将恶意节点记录在区块链中一方面可以约束用户的行为, 另一方面可以防止恶意用户的再注册, 避免浪费计算资源和通信资源.

4 方案分析

本节主要对本方案与文献 [4,13,14] 在安全性、计算开销和通信开销等方面进行分析和比较.

4.1 安全分析

在本节对方案进行了安全性的分析, 并与其他方案进行比较, 比较结果见表 3.

1) 身份安全

在本方案中, 用户进行访问时, 采用的身份是 $hash(u_i \| ID_j)$ 的虚拟身份, 用户的公钥 PK、私钥 SK 都是由用户自己生成的. 权威节点对机构进行身份认证,

用户由机构节点进行认证, 并分别为他们的身份证明进行签名, 确保身份的有效性. 权威节点对注册机构、机构节点对注册用户将他们的注册信息分别上传到域间区块链、跨域区块链上, 因此任何敌手都不能篡改. 每一个合法的机构和用户的 (*PK*, *SK*) 都是基于离散对数困难问题生成的, 对于任何一个概率多项式时间的敌手都不能根据公钥或者加密消息计算出私钥. 在本方案中用户和机构的私钥由用户自己生成, 用户只使用私钥解密消息和签名, 用户私钥只掌握在自己手里.

表 3 安全性属性比较

方案	文献[4]	文献[13]	文献[14]	本文方案
单点故障	×	√	√	√
重放攻击	√	×	×	√
内外部攻击	×	√	√	√
相互认证	√	√	√	√
去中心化	×	√	√	√

2) 双向认证

在用注册过程, 无论是用户注册还是机构的注册都实现了用户与机构的双向身份认证、机构与权威节点的双向的身份认证. 在域内和跨域过程中通过区块链验证用户和机构的身份证书, 实现了用户对访问机构的身份认证, 以及被访问机构对用户的身份认证.

3) 数据完整性

区块链作为一种分布式账本技术, 其中每一个区块链节点都会保存完整的区块链信息, 一旦某个节点出现的区块信息出现缺失, 可以通过更新区块信息, 保证本地的账本信息与其他节点一致. 从而保证节点中的区块信息的完整性, 也避免了恶意攻击篡改部分节点中的信息, 实现了区块链系统中的数据完整性.

4) 分布式拒绝服务攻击

区块链的去中心化以及点对点的交互, 即使有一个或者少部分节点失效, 其余节点也不会受其影响, 并且如果需要的话在多个节点中会有一个合法节点取代失效节点工作; 恶意节点的操作也不会在共识阶段通过.因此本方案可以抵抗分布式拒绝服务攻击.

5) 重放攻击

在本方案中, 对消息添加时间戳以及采用提问、应答方式. 即使敌手截获了之前的消息, 目标服务器通过检查消息的新鲜性也会拒绝为敌手提供服务.

6) 内部攻击和外部攻击

外部攻击者即使获取了权威机构的公钥或者机构的公钥, 但是也无法计算出来用户的私钥. 对于内部攻击者来说, 仅仅根据用户的公钥也无法计算出其私钥. 因此本文提出的方案能够有效地抵抗外部攻击和内部攻击.

7) 女巫攻击

在本文的涉及方案中, 每一个用户在网络中都有一个唯一标识 *ID*, 通过使用机构注册节点的信息生成唯一的标识, 并且在每次通信之前都会对用户信息进行身份认证, 认证在域内联盟链或者域间联盟链中进行, 因此攻击者无法伪装网络中的合法节点与其他节点进行通信.

以上是对本方案的安全性分析, 与近几年的跨域方案相比较, 从表 3 可以看出, 本方案在安全性上的优越. 在安全性上, 本方案通过区块链技术解决了认证过程中中心化可能带来的单点故障等问题; 引入无证书签名解决了密钥托管的问题; 设计时间戳机制, 解决了重放攻击; 在方案的各个阶段也都进行了通信双方的身份认证, 实现了双向的相互认证; 通过无证书机制, 让用户自己掌握自己的私钥, 也解决了内外攻击的问题. 本方案与其他认证方案在安全属性的比较如表 3.

在安全属性的比较上, 与其他方案相比安全属性更好. 其中文献 [4] 必须集中式的认证方案, 因此不满足去中心化, 另外不能抵抗重放攻击; 文献 [13] 中未加入时间戳机制因此无法抵御重放攻击, 用户私钥也被存放在密钥生成中心, 容因此不满足内外部攻击; 文献 [14] 不能抵抗重放攻击. 本方案对于解决上安全问题上具备一定优势.

4.2 方案性能分析

对本方案的性能分析, 主要从计算开销和通信开销来与其他方案进行比较.

4.2.1 计算开销

文献 [4,13,14] 是基于离散对数数学困难问题来进行双线性对计算和指数计算设计认证方案, 计算开销大; 而本文采用的是基于椭圆曲线上的离散对数困难问题, 通过椭圆曲线上的加法运算和倍点运算来实现认证方案的设计, 计算开销小. 通过 Thumbur 等人 [15] 的仿真实验可知, 椭圆曲线上的加法运算大约是倍点运算的 200 多倍, 在各个方案的计算开销比较上作用也微乎其微. 因此在计算开销的比较上, 不考虑椭圆去线上的加法运算. 为了对方案进行比较, 定义以下符号: T_B 表示一次双线性对运算开销; T_E 表示一次指数运算开销; T_{GM} 表示运行椭圆曲线上群 G 上一次点乘运算

的开销, “—”表示不具备此功能.

根据文献 [3] 在 i5-4460s 2.90 GHz CPU 的计算机上部署大数运算函数库 (MIRACL), 对双线性对运算、指数运算以及椭圆曲线上的倍点运算的仿真实验结果如表 4.

表 4 运算操作的运行时间 (ms)

运算操作	运行时间
T_B	5.427
T_E	0.339
T_{GM}	0.538

在我们的方案中, 为了实现机构和用户的双向认证, 与其他方案不同的是, 本方案也为机构也颁发了身份证明, 而且机构的数量相比较普通用户而言少很多, 因此在总体计算开销的用户注册阶段, 仅仅考虑普通用户注册时的计算开销.

本方案与文献 [4,13,14] 所提出的方案在用户计算开销对比如表 5. 通过表格可以明显地看出来与其他认证方案相比较本方案在计算开销上有明显优势, 并且文献 [4] 和文献 [14] 不支持跨域认证, 文献 [13] 未对域内认证进行分析, 而本方案对域内和域外身份认证均进行了设计.因此本方案更加全面, 计算开销也更低.

表 5 计算开销比较

方案	用户注册阶段	域内认证	跨域认证
文献[4]	$5T_B$+$4T_E$	$3T_B$	—
文献[13]	$2T_B$+$2T_E$	—	$3T_B$+$4T_E$
文献[14]	$3T_E$	$4T_B$	—
本文方案	$6T_{GM}$	$6T_{GM}$	$4T_{GM}$

4.2.2 通信开销

在通信开销的比较上, 由于文献 [14] 未设计详细的交互过程, 因此不参与比较, 并且为了更为直观的进行比较, 仅对用户的通信开销进行比较.假设所有的方案的身份 ID 长度都一致, 群上的消息长度也一致, 加密消息的长度与消息本身长度一致, 群变量信息长度是时间戳的 10 倍, 随机数不计入长度, 身份证明的长度与群变量一致. 现定义$|p|$代表群变量的信息长度, $|G|$代表椭圆曲线上的信息长度, $|t|$代表时间戳的信息长度, $|id|$代表用户和匿名身份的长度, $|hmac|$代表 HMAC 的信息长度. 并假设$|id|$的长度为 80 bit; 时间戳 16 bit; 群变量 160 bit; 证书密文 160 bit; 身份的 80 bit, $|hmac|$是 160 bit.

对于文献 [4] 所述方案, 在用户注册阶段用户发送的注册信息长度为 $3|p|+|id|$在认证阶段, 用户通信开销为 $2|p|+|id|+|hmac|$.

对于文献 [14], 用户在注册阶段的计算开销为 $|t|+3|q|$, 在认证阶段用户的通信开销为 $5|p|+|t|+|id|$.

对于本文方案, 在用户注册阶段, 用户发送给机构的注册信息$\left\{En\left(u_i,t_{reg},N_1\right)_{PK_{ID_j}},ID_j\right\}$的通信长度为 $2|id|+|t|$, 用户给机构发送的消息$\left\{pk_{id_i},id_i,En(t_2,\sigma_{id_i},E_i)_{PK_{ID_j}}\right\}$的信息长度为 $3|G|+|t|+|id|+|p|$; 在认证阶段, 仅对用户域内认证进行分析, 用户提交的$En(crocert_a,W_a,id_a,t)_{PK_{ID_{1_B}}}$的通信长度为 $2|t|+|G|+4|p|+|id|$.

从表 6 可以看出, 总体来看文献 [4] 的通信开销最小, 但是认证阶段本方案最优, 而且在这 3 个方案中, 用户只需要注册一次, 之后再进行访问只需要对其进行认证即可, 在认证阶段, 本方案的通信开销最小.总之, 对于用户来说本方案的通信开销可行.

表 6 用户通信开销比较

方案	注册阶段	认证阶段	总开销 (bit)
文献[4]	$3\|p\|+\|id\|$	$2\|p\|+\|id\|+\|hmac\|$	1 120
文献[13]	$\|t\|+3\|q\|$	$5\|p\|+\|t\|+\|id\|$	1 392
本文方案	$2\|t\|+2\|id\|+4\|p\|$	$\|t\|+2\|p\|+\|id\|$	1 168

另外, 本方案采用基于联盟链的基础架构, 由机构节点和权威节点具备交易权限, 并且节点数目远小于公有链. 并且本文采用本地链和跨域链两种区块链. 因此机构节点和权威节点的计算开销和通信开销与单链架构情况下相比要小得多.

对于方案的存储需求, 区块链上的数据都是经过哈希处理的, 最终转化为固定字节的二进制数, 然后通过默克尔树来进行记录, 区块头仅存放默克尔根的哈希值. 而且区块链上存储的也仅是用户的注册信息以及恶意用户记录因此不会占据大量内存, 因此满足存储需求.

5 总结与展望

针对目前在教育场景下集中式的身份认证的弊端, 本文提出了基于无证书签名与区块链的身份认证方案. 利用区块链的分布式架构解决了集中式的单点故障问题; 利用无证书签名让用户生成自己的公私钥, 避免了密钥托管的问题; 通过颁发身份证明实现域内、跨域认证; 通过区块链技术来辅助用户来进行身份认证, 降

低了用户的计算开销; 另外通过哈希函数实现用户的真实身份可追溯. 最后, 将本文所提出的身份认证方案与其他方案进行性能比较分析. 结果表明该方案具备去中心化、可跨域、隐私保护、用户可追溯的特性, 并且在安全属性和用户开销上有一定的优势. 本文虽然在教育场景下的身份认证的安全性上提供了有效的解决办法, 但仍存在较大的提升空间, 下一步利用分片技术、多通道等技术区块链系统的处理效率以及提高区块链系统的可扩展性, 并进一步研究基于教育区块链的身份认证领域.

参考文献

1 章泽昂, 邬家炜. 基于云计算的教育信息化平台的研究. 中国远程教育, 2010(06): 66–69, 80. [doi: 10.13541/j.cnki.chinade.2010.06.015]

2 Park S, Kim H, Ryou J. Utilizing a lightweight PKI mechanism to guarantee a secure service in a cloud environment. The Journal of Supercomputing, 2018, 74(12): 6988–7002.

3 张文芳, 雷丽婷, 王小敏, 等. 面向云服务的安全高效无证书聚合签名车联网认证密钥协商协议. 电子学报, 2020, 48(9):1814-1823.[doi:10.3969/j.issn.0372-2112.2020.09.020]

4 王中华, 韩臻, 刘吉强, 等. 云环境下基于 PTPM 和无证书公钥的身份认证方案. 软件学报, 2016, 27(6): 1523–1537. [doi: 10.13328/j.cnki.jos.004992]

5 江泽涛, 徐娟娟. 云环境下基于代理盲签名的高效异构跨域认证方案. 计算机科学, 2020, 47(11): 60–67. [doi: 10.11896/jsjkx.191100068]

6 谭琛, 陈美娟, Ackah AE. 基于区块链的分布式物联网设备身份认证机制研究. 物联网学报, 2020, 4(2): 70–77.

7 周致成, 李立新, 李作辉. 基于区块链技术的高效跨域认证方案. 计算机应用, 2018, 38(2): 316–320, 326.

8 马晓婷, 马文平, 刘小雪. 基于区块链技术的跨域认证方案. 电子学报, 2018, 46(11): 2571–2579. [doi: 10.3969/j.issn.0372-2112.2018.11.002]

9 Xu J, Xue KP, Tian HY, *et al*. An identity management and authentication scheme based on redactable blockchain for mobile networks. IEEE Transactions on Vehicular Technology, 2020, 69(6): 6688–6698. [doi: 10.1109/TVT.2020.2986041]

10 张福泰, 孙银霞, 张磊, 等. 无证书公钥密码体制研究. 软件学报, 2011, 22(6): 1316–1332.

11 Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

12 Al-Riyami SS, Paterson KG. Certificateless public key cryptography. Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security. Taipei: Springer, 2003. 452−473.

13 杨小东, 安发英, 杨平, 等. 基于无证书签名的云端跨域身份认证方案. 计算机工程, 2017, 43(11): 128–133, 145. [doi: 10.3969/j.issn.1000-3428.2017.11.021]

14 Hung YH, Tseng YM, Huang SS. A revocable certificateless short signature scheme and its authentication application. Informatica, 2016, 27(3): 549–572. [doi: 10.15388/Informatica.2016.99]

15 Thumbur G, Rao GS, Reddy PV, *et al*. Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices. IEEE Communications Letters, 2020, 24(8): 1641–1645.