Journal of Computer Applications
计算机应用,2018,38(2):316-320,326
ISSN 1001-9081
CODEN JYIIDU
2018-02-10
http://www.joca.cn

文章编号:1001-9081(2018)02-0316-05
DOI:10.11772/j.issn.1001-9081.2017082170

# 基于区块链技术的高效跨域认证方案

周致成,李立新*,李作辉
(信息工程大学,郑州 450001)
(* 通信作者电子邮箱 alphalilixin@163.com)

**摘　要**:为解决现有公钥基础设施(PKI)跨域认证方案的效率问题,利用具有分布式多中心、集体维护和不易篡改优点的区块链技术,提出基于区块链技术的高效跨域认证方案,设计了区块链证书授权中心(BCCA)的信任模型和系统架构,给出了区块链证书格式,描述了用户跨域认证协议,并进行了安全性和效率分析。结果表明,在安全性方面,该方案具有双向实体认证等安全属性;在效率方面,与已有跨域认证方案相比,利用区块链不可篡改机制,使用哈希算法验证证书,能减少公钥算法签名与验证的次数、提升跨域认证效率。

**关键词**:跨域认证;区块链;授权中心;公钥基础设施;数字证书;数字签名
**中图分类号**:TP309;TP393.08　　**文献标志码**:A

## Efficient cross-domain authentication scheme based on blockchain technology

ZHOU Zhicheng, LI Lixin*, LI Zuohui
(*Information Engineering University*, *Zhengzhou Henan* 450001, *China*)

**Abstract:** To solve the efficiency problem of the existing Public Key Infrastructure (PKI) cross-domain authentication scheme, by using blockchain technology with the advantages of distributed multi-center, collective maintenance and not being easy to tamper, an effective cross-domain authentication scheme was proposed, including BlockChain Certificate Authority (BCCA) trust model and system architecture, blockchain certificate format and user cross-domain authentication protocol, as well as the security and efficiency. The results show that in terms of security, the scheme has security attributes such as mutual entity authentication; in terms of efficiency, compared with the existing cross-domain authentication scheme, by taking advantage of blockchain mechanism such as not being easy to tamper, and hash algorithm, the number of signature and verification of public key algorithm is reduced, which enhances the efficiency of cross-domain authentication.

**Key words:** cross-domain authentication; blockchain; Certificate Authority (CA); Public Key Infrastructure (PKI); digital certificate; digital signature

## 0　引言

信息安全已成为信息化发展中不可缺少的技术基础[1]。身份认证是保证信息安全的一种重要安全机制,而基于公钥基础设施(Public Key Infrastructure, PKI)的身份认证是目前较为成熟并取得普遍应用的认证技术[2]。在分布式环境中,各机构为了方便管理用户,设置认证服务器形成相对独立的信任域,然而单个独立的信任域不能提供多种服务,用户需要多域访问,因此出现跨域认证问题。

现有的以传统PKI为基础的认证框架,通常以安全套阶层身份认证协议(Secure sockets layer Authentication Protocol, SAP)实现双向身份认证。这种认证框架比基于对称密钥的认证框架如Kerberos等有了较大进步[3],但由于认证双方通过互发证书或证书链进行通信,证书维护过程如证书状态查询存在计算与通信开销较大的问题。因此,如何提高跨域认证的效率受到国内外学者的广泛关注。文献[5]直接根据各域已有的PKI结构及拓扑关系构建认证路径,但存在认证路径复杂、认证效率较低的问题。文献[6]采用桥证书授权中心(Certificate Authority, CA)的认证方案,建立一个所有域都信任的桥CA模型,该方案需要各域都信任这个可信第三方,实际应用困难,同时还存在如何跨域获取证书状态信息的问题。文献[7]借助虚拟桥CA模型,采用基于门限方案的椭圆曲线密码体制构建企业跨域认证体系,但由于门限方案通过拆分密钥因子造成交互代价比较大,使得成员加入、撤销的可扩展性不强。基于身份的密码体系(Identity-Based Cryptography, IBC)可以解决证书管理和传递开销的问题,但由于计算量与通信量过高,跨域认证效率不高。文献[8]提出一种基于身份的跨域认证方案,用户需要进行多次双线性对运算,计算开销较大,不适用于移动终端。文献[9]利用椭圆曲线加法群提出基于身份的签名算法实现跨域认证,避免了复杂的双线性对运算,计算开销明显减小;但方案只分析了实体与认证中心的认证过程,没有考虑认证中心与本地资源确认对方合法性带来的额外开销。文献[10]提出一种无线网格环境下的跨域认证密钥交换协议,但使用较多对称加密造成大量计算开销。综合以上研究成果,基于证书和基于身份的跨域认证仍存在诸多问题有待解决。

区块链技术最早由化名为"中本聪"的学者在2008年的密码学邮件组发表的关于比特币的论文[11]中提出。作为分

**收稿日期**:2017-08-21;**修回日期**:2017-09-12。　**基金项目**:信息工程大学科研基金资助项目(2016609903)。
**作者简介**:周致成(1992—),男,河南郑州人,硕士研究生,主要研究方向:信息安全、区块链;　李立新(1967—),男,重庆人,研究员,博士,主要研究方向:网络与信息安全;　李作辉(1981—),男,湖南衡阳人,副研究员,博士,主要研究方向:公钥密码、网络安全。

布式存储、点对点传输、共识机制、加密算法等技术的集成应用,区块链技术的应用已延伸到物联网、人工智能、身份认证等多个领域。

区块链技术在身份认证领域的研究受到诸多研究机构的重视。文献[12]指出,区块链技术的发展对数字证书的发展和应用有极大的促进作用。文献[13]提出了以比特币区块链系统为框架的去中心化 PKI 认证体系,使用 Certcoin 代替 CA 提供高效密钥查询与身份保留功能,但存在因使用区块链公共总账直接记录用户身份和公钥的绑定造成用户隐私泄漏的问题; 文献[14]提出一种改进的 Certcoin 方案,提出了带隐私保护的 PKI 认证系统。文献[15]提出使用以太坊区块链平台的基于证书的 PKI 认证体系,解决了传统 PKI 证书管理与使用证书撤销列表( Certificate Reveocation List, CRL) 和在线证书状态协议( Online Certificate Status Protocol, OCSP) 通信量过大的问题。但是这些研究目前均未解决跨域认证问题。

针对以上问题,本文提出基于区块链技术的高效跨域认证方案。在不改变域内 PKI 认证体系的基础上,将各域的认证服务器和根 CA 证书服务器设置为区块链节点,域间跨域认证通过代理认证服务器查询验证对方域的根 CA 证书服务器发布于区块链的无签名证书的哈希值,代替传统 PKI 互发签名证书并验证签名的方式。本文方案能减少签名验证次数,提高认证效率,解决使用 CRL 和 OCSP 证书管理较复杂的问题; 而且系统基于联盟链的设计,可扩展性强。

## 1　区块链技术

### 1.1　区块链结构

区块链是一种按照时间顺序将数据区块以链条的方式组合而成的特定数据结构,并以密码学方式保证的不可篡改不可伪造的去中心化公共总账[16]。在区块链技术中,数据以区块的形式永久保存。每一个区块按照时间顺序先后生成并通过链式结构连接组成区块链。区块由区块头和区块体组成,如图 1 所示。

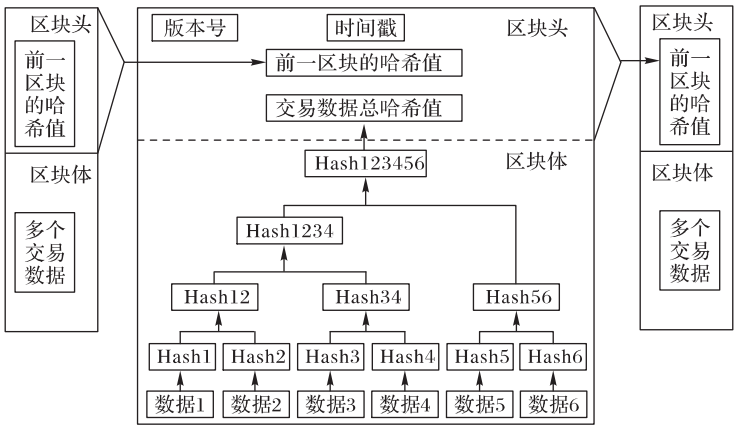



图 1　区块链结构

Fig. 1　Blockchain structure

如图 1 所示: 区块头内主要有版本号、时间戳,前一区块的哈希值、交易数据总哈希值,以及参与共识机制的有关数据( 随机数等,因为区块链平台共识机制的不同设计也有所不同,这里不再赘述) 。前一区块的哈希值是对前一区块头的各个模块数据进行哈希运算,区块之间通过这样的哈希值环环相扣依次连接。区块体中记录了自区块链创建以来到生成本区块期间所有的交易数据。以比特币区块链为例,数据通常以 Merkle tree 的方式,从叶子节点到父节点自下而上两两作哈希运算,最终形成这段时间内数据的总哈希值,存储在区块头内。

### 1.2　区块链特征

本文方案主要用到区块链技术分布式多中心、集体维护、不易篡改的特点。

1) 分布式多中心: 区块链系统节点基于分布式点对点结构,每个节点都存有系统内所有的交易数据,任意节点的损坏不影响整个系统的运作,系统冗余度高,具有极好的健壮性。

2) 集体维护: 区块链构建了一套完整的协议机制,系统中的节点不仅参与记录数据,而且参与验证其他节点记录数据的正确性。只有当大部分节点或者多个关键节点认可数据的正确性时,数据才能被记入到区块当中。现行 IBM 的超级账本 Fabric 平台采用两种类型节点:

a) 验证节点( Validating Peer, VP) 。VP 执行数据的读写、查询操作,借助区块链共识算法、一致性协议,维护区块链账本数据库。

b) 非验证节点( Nonvalidating Peer, NVP) 。NVP 用来连接用户和邻近的 VP,执行查询验证操作,不执行记入交易数据操作。

3) 不易篡改: 区块链技术采用哈希算法对记入区块的数据进行完整性保护,以链式结构连接数据区块并存储于系统中的所有节点。如果一个区块被改变,那么之后的每一个区块都将被改变。区块链上数据区块越多,数据越难篡改,因此改变某一区块及区块内的数据几乎是不可能的。以比特币区块链为例,只有对 51% 的节点攻击才能篡改数据。正是由于区块链技术具有不易篡改的特性,为记录可信凭证提供了可能。

### 1.3　区块链类型及性能特点

根据区块链的中心化程度的差异,可以将区块链分为公有链、联盟链和私有链,这三种类型区块链的性能特点如表 1 所述。综合各类型区块链特点,本文方案采用联盟链为原型。采用联盟链为方案原型,一方面符合政府、企业等多域间跨域认证需要,另一方面由于区块链共识算法的不同,联盟链效率较高,系统可扩展性强。

## 2　基于区块链的跨域认证方案

基于证书的传统 PKI 跨域认证模型普遍存在认证路径复杂、签名验证次数较多、证书管理困难等问题; 而基于身份的密码体系的计算量与通信量较高,跨域认证效率不高,实际应用困难。本章主要设计了区块链 CA( Blockchain Certificate Authority, BCCA) 信任模型和系统架构,给出了区块链证书格式,并在此基础上完成跨域认证协议。

### 2.1　BCCA 信任模型

信任模型用于描述和分析同一 CA 管理域内部或不同 CA 管理域之间的信任关系的建立和传递过程。为解决多个域的跨域认证问题,本文提出了 BCCA 信任模型。

BCCA 信任模型如图 2 所示,其中: 矩形框表示 VP,即根 CA; 空心圆表示域内用户。为实现跨域认证,多个域的信任

锚根 CA 经过许可后，加入联盟链，构成联盟链的 VP。在本文方案中，加入联盟链的根 CA 是可信的，作为 VP 自生成根 CA 区块链证书，并将证书的哈希值记入不易篡改的区块链内，作为各域的信任凭证。如果一个域不再有跨域需要，或者该域不再可信，对加入联盟链的许可进行撤销，实现盟员的退出。

**表 1 区块链类型及性能特点**

Tab. 1 Type and performance characteristics of different blockchains

| 区块链 | 参与模式 | 节点身份 | 应用平台 | 共识算法 | 共识算法的特点 | 交易时间 | 容错能力 |
|---|---|---|---|---|---|---|---|
| 公有链 | 人或机构 | 无许可(任何用户，可能包含恶意成员) | 比特币 | POW | 多块确认，耗电量大 | 耗时长(单位: min) | 49% 故障 |
| | | | 以太坊 | POS | | | |
| 联盟链 | 多个机构 | 许可(经过指定，可信的成员) | 超级账本 | PBFT | 立即确认，耗电量小 | 耗时短(单位: s) | 33% 故障 |
| 私有链 | 单机构内 | | 瑞波币 | RPCA | | | 20% 故障 |

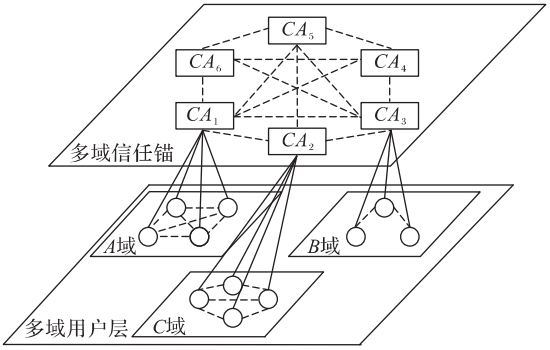



图 2 BCCA 信任模型

Fig. 2 Trust model of BCCA

## 2.2 系统架构

如图 3 所示，多个域的根 CA 作为联盟链 VP，通过自生成区块链证书，并把证书的哈希值记入区块链作为各域的信任凭证。为了实现多域信任凭证的传递与确认，本文方案添加代理认证服务器作为区块链系统的 NVP，通过 NVP 查询验证存储在区块链上的信任凭证，实现跨域认证。加入 NVP，一方面可发挥代理认证服务的功能，另一方面也解决了在仅有 VP 的联盟链框架下用户与 VP 交互时因通信量过大造成的阻塞。

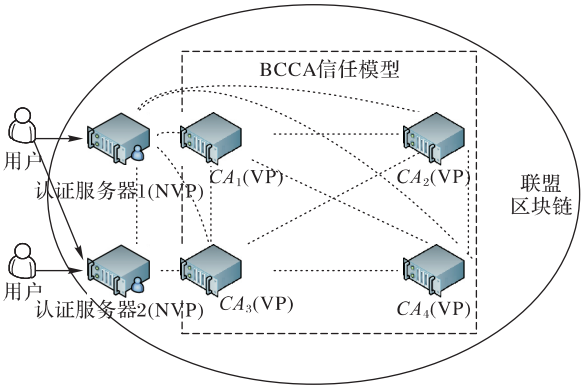



图 3 系统架构

Fig. 3 System structure

## 2.3 区块链证书

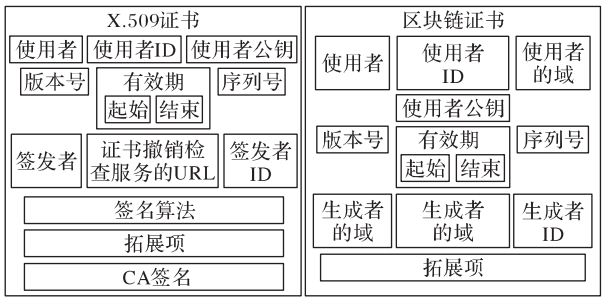
本文设计一种区块链证书，由许可加入联盟链的多个域的根 CA 自生成，并记入区块链，作为不可篡改的信任凭证。X.509 证书与本文设计的区块链证书如图 4 所示。

与传统 X.509 数字证书比较，主要有以下改进：

1) 本文方案在数字证书中添加了使用者域与生成者域的名称。该证书不仅作为域间跨域认证的信任凭证，在用户实现跨域认证之后，认证域的根 CA 对请求认证的用户生成跨域证书，传给用户，并以哈希值的形式记入区块链，方便用户再次访问时提供快速认证。

2) 本文方案在数字证书中省去了签名与签名算法模块。传统 PKI 通过使用数字签名判断证书是否被篡改，使数字证书具有防伪性，保证数字证书中身份和公钥的绑定值得可信。由于区块链天然的具有不易篡改的特性，可信域的根 CA(VP) 生成区块链证书并将证书的哈希值记入区块链作为多域信任凭证，代替 CA 对证书的签名过程；认证服务器(NVP)通过在区块链内查验多个域的可信凭证，代替对证书的签名验证的过程。

3) 本文方案设计的数字证书没有证书撤销检查服务的 URL 模块。即在区块链上发布的证书没有 CRL 与 OCSP 管理服务。区块链不能更改已经写入的数据，只能在写入时附加数据的状态。文献[17]定义写入区块链的接口为 put(action,data)，action 表明用户对数据的处理意图，可以是 create、insert、update 或 delete。本文方案把证书写入区块链的接口定义为 put(action,Hash(Cert))，参数 action 定义为本证书当前状态，分为 issue 或 revoke 两种状态。区块链查询接口定义为 query(condition)，参数 condition 表示用户查询的条件，可以是交易的哈希值或块的哈希值[17]，也可以是待查询有关数据的主键。




(a) X.509数字证书 (b) 本文设计的区块链证书

图 4 X.509 数字证书与区块链证书

Fig. 4 X.509 digital certificate and blockchain certificate

## 2.4 基于区块链的跨域认证协议

根据上述信任模型、系统架构和区块链证书，本文提出基于区块链的跨域认证协议。假定经许可加入联盟链的域是可信的，跨域认证协议开始之前，各个域的根 CA 区块链证书的哈希值和写入状态已经保存在区块链的区块中。

以 *A* 域和 *B* 域作跨域认证为例，基于区块链的跨域认证方案由用户、信任锚根 CA 证书服务器、代理认证服务器组成。信任锚根 CA 证书服务器、代理认证服务器作为区块链节点，分别执行生成证书并记入区块链和查询区块链验证证

书的任务。表 2 为协议中用到的符号说明,协议流程如图 5 所示。

**表 2　协议符号说明**

Tab. 2　Description of the protocol symbol

| 符号 | 含义 |
|---|---|
| $A \rightarrow B: m$ | 表示实体 $A$ 向实体 $B$ 发送消息 $m$ |
| $U_X$ | $X$ 域用户 |
| $AS_X$ | $X$ 域证书验证服务器 |
| $Cert_{U_X}$ | $X$ 域用户 $U_X$ 的证书 |
| $BCert_{CA_X}$ | $X$ 域信任锚根 $CA_X$ 自生成的区块链证书 |
| $BCert_{U_X,CA_Y}$ | $Y$ 域信任锚 $CA_Y$ 生成的 $X$ 域用户 $U_X$ 的跨域区块链证书 |
| $Sign_{sk_X}(\ )$ | 签名算法 |
| $N_x$ | 随机数 |

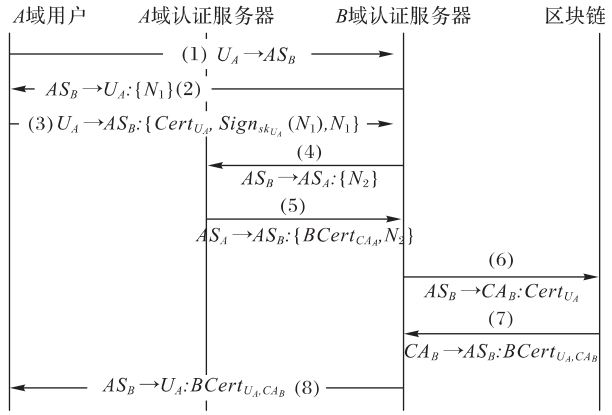



图 5　本文协议流程

Fig. 5　Flow chart of the proposed protocol

具体协议如下:

1) $U_A \rightarrow AS_B$

$A$ 域用户 $U_A$ 请求访问 $B$ 域认证服务器 $AS_B$。

2) $AS_B \rightarrow U_A$:{$N_1$}

$B$ 域认证服务器 $AS_B$ 收到用户 $U_A$ 的请求后,响应请求并向 $A$ 域用户 $U_A$ 发送随机数 $N_1$。

3) $U_A \rightarrow AS_B$:{$Cert_{U_A}$,$Sign_{sk_{U_A}}(N_1)$,$N_1$}

(i) $A$ 域用户 $U_A$ 收到 $B$ 域认证服务器 $AS_B$ 的响应,使用用户 $U_A$ 的私钥 $sk_{U_A}$ 对随机数 $N_1$ 签名生成 $Sign_{sk_{U_A}}(N_1)$;

(ii) $A$ 域用户 $U_A$ 响应 $B$ 域认证服务器 $AS_B$ 的请求,把用户证书 $Cert_{U_A}$、签名 $Sign_{sk_{U_A}}(N_1)$、随机数 $N_1$ 作为消息发送给 $B$ 域认证服务器 $AS_B$。

4) $AS_B \rightarrow AS_A$:{$N_2$}

(i) $B$ 域认证服务器 $AS_B$ 收到消息,检查随机数 $N_1$ 是否有效;

(ii) 使用 $Cert_{U_A}$、$N_1$ 验证 $Sign_{sk_{U_A}}(N_1)$ 是否正确,解析证书,查看证书有效期,通过证书或证书链确定 $A$ 域信任锚 $CA_A$;

(iii) $B$ 域认证服务器 $AS_B$ 向 $A$ 域认证服务器 $AS_A$ 发送请求申请得到 $A$ 域信任锚 $CA_A$ 的区块链证书 $BCert_{CA_A}$,并发送随机数 $N_2$。

5) $AS_A \rightarrow AS_B$:{$BCert_{CA_A}$,$N_2$}

$A$ 域证书认证服务器 $AS_A$ 收到请求及随机数 $N_2$,将 $A$ 域信任锚 $CA_A$ 的区块链证书 $BCert_{CA_A}$、随机数 $N_2$ 作为消息发给 $B$ 域认证服务器 $AS_B$。

6) $AS_B \rightarrow CA_B$: $Cert_{U_A}$

(i) $B$ 域认证服务器 $AS_B$ 收到消息后,检查随机数 $N_2$ 是否有效;

(ii) 解析 $BCert_{CA_A}$ 查看有效期,根据区块链使用的哈希算法把 $BCert_{CA_A}$ 作哈希运算得到 Hash($BCert_{CA_A}$);

(iii) $B$ 域认证服务器 $AS_B$ 使用 Hash($BCert_{CA_A}$) 查询区块链,得到在区块链上查询的结果:

(a) 若无查询结果,则由于 $A$ 域认证服务器提供了不正确的信任锚 $CA_A$ 区块链证书,认证失败;

(b) 若查询结果为 issue 和 revoke,则由于 $A$ 域信任锚 $CA_A$ 的区块链证书已为撤销状态,认证失败;

(c) 若查询结果仅有 issue,则 $A$ 域信任锚 $CA_A$ 的区块链证书为已发布状态,认证成功。

(iv) 认证成功后,$B$ 域认证服务器 $AS_B$ 向 $B$ 域信任锚 $CA_B$ 发送用户 $U_A$ 证书 $Cert_{U_A}$。

7) $CA_B \rightarrow AS_B$: $BCert_{U_A,CA_B}$

$B$ 域信任锚 $CA_B$ 收到用户 $U_A$ 证书 $Cert_{U_A}$ 后,解析用户 $U_A$ 证书,生成跨域区块链证书 $BCert_{U_A,CA_B}$,并记入区块链,同时反馈给 $AS_B$。

8) $AS_B \rightarrow U_A$: $BCert_{U_A,CA_B}$

$B$ 域证书认证服务器 $AS_B$ 发给用户 $U_A$ 跨域区块链证书 $BCert_{U_A,CA_B}$。

9) 同理使用 1) ~8) 实现 $A$ 域对 $B$ 域的反向认证。

10) 由 1) ~9) 实现 $A$、$B$ 两域的双向认证。

重认证:

再次认证时,$A$ 域用户 $U_A$ 直接把跨域区块链证书 $BCert_{U_A,CA_B}$ 发给 $B$ 域认证服务器 $AS_B$,由 $AS_B$ 作哈希运算,并查询区块链,验证证书有效性即可。

## 3　方案分析

### 3.1　安全性分析

#### 3.1.1　证书存在性与所有权

本文方案将各个域与用户的证书文件进行哈希运算,再将证书的哈希值存入在区块链中。哈希函数具有以下特性:

性质 1　单向性: 给定 $h$,根据 hash($m$) = $h$,计算 $m$ 是不可行的;

性质 2　抗碰撞性: 给定算法 hash(),要找到两个不同的消息 $x_1 \neq x_2$,使其哈希值 hash($x_1$) = hash($x_2$) 是计算不可行的。

哈希函数的单向性与抗碰撞性能够使任何区块链节点匿名和安全地存储信任凭证。通过在区块链上存放文件的密码学哈希值,以及提交该文件哈希值至区块链中的时间信息,来证明证书文件的存在性与所有权。

#### 3.1.2　双向实体认证

在每个信任域内,通过域内原有的认证方式实现用户和认证服务器的认证。在多域间联盟链的框架下,认证服务器通过请求获得待认证域的根 CA 区块链证书,作哈希运算后查询区块链内已保存的信任凭证,确认信任关系,实现用户与对方域的服务器的认证。凭借本域用户与对方域服务器的认

证,对方域服务器与对方域用户的认证,实现两个域间用户的双向实体的认证。

3.1.3 防止重放攻击

本协议使用了询问-应答的握手方式,在传递消息的同时添加随机数。这个随机数保存在询问服务器内,验证反馈信息之前,首先验证随机数,通过验证随机数和原服务器保存的一样,起到防止重放攻击的效果。

3.1.4 抵抗分布式拒绝服务(DDoS)攻击

区块链的分布式架构天然地拥有点对点、多冗余特性,即使一个节点失效,其他节点也不受影响,因此不存在单点失效问题。它对拒绝服务攻击的方式比中心化系统灵活很多,一旦节点失效,与失效节点连接的用户即无法进入系统。

### 3.2 效率分析

如图 3 所示,本节对协议的计算开销进行分析,并与文献[7]方案和文献[9]方案作比较。特别说明的是,为保证方案顺利实现,又与其他文献方案处于平等复杂程度,不失一般性,设置本文方案与文献[7]方案盟员数均为 2。表 3 为三个方案的效率比较,单位为运算次数,其中公钥加密与解密、数字签名与验证两栏计算的是分步次数的总和。

**表 3 计算开销对比**

Tab. 3 Comparison of computation overhead

| 方案 | 公钥加密与解密次数 | 数字签名与验证次数 | 哈希运算次数 |
|---|---|---|---|
| 文献[7]方案 | 0 | 12 | 4 |
| 文献[9]方案 | 2 | 4 | 10 |
| 本文方案 | 0 | 4 | 2 |

与文献[9]方案相比,本文方案减少了 8 次数字签名与验证次数。文献[9]基于门限方案,数字签名与验证的次数会随着盟员数量的增加呈倍数增长;而本文方案基于分布式联盟链,不受盟员的增加而导致两方跨域认证时使用公钥算法次数的增加,但客观上会出现由于区块链集体维护账本导致的哈希运算次数的增加。因此本文方案使用的公钥算法的次数远小于文献[9]方案。由于哈希算法的效率远高于公钥算法,因此本文方案在多域联盟下的跨域认证具有明显优势。

与文献[7]方案相比,本文方案减少了 2 次公钥加密与解密,数字签名与验证次数相同,因此本文方案使用公钥算法的次数少于文献[7]方案。在盟员数为 2 的情况下,本文方案使用哈希算法次数也少于文献[7]方案;但随着盟员数的增长,本文方案使用哈希运算次数随之增加。在同等配置的机器上测试,RSA-1 024 的耗时约为 ECDSA-192 的 1/2,SHA-256 的计算耗时约为 RSA-1 024 的 1/10,所以哈希算法的计算速度远高于公钥算法,速度甚至超过几十倍。所以即使在多域联盟环境下,与仅有两域相比,本文方案实现跨域认证的效率与承载力还是可观的。

### 3.3 可行性分析

在计算方面,方案基于联盟区块链架构进行设计。目前已知联盟链平台每秒可并行处理几千到几万笔交易,满足跨域认证的功能需要。

在存储方面,因为区块链存储数据是永久性的,把大量原数据直接存储在区块链上是不妥的。所以区块链通常采用 SHA256 哈希函数,将任意长度的交易数据经过哈希运算后转换为长度为 32 字节的二进制数,然后通过 Merkle 树的记录方法,计算出一个 Merkle 根哈希值,作为交易数据的总哈希值存储在区块头内。采用 Merkle 树的好处是,如果一个交易数据没有后续交易产生,可以删除这个交易数据,只保留 Merkle 树中这个交易数据的 Hash 值即可。这样,对整个区块来说,不仅没有改变它的密码学安全性和完整性,数据量也可以大大减小。

在部署成本方面,方案不改变原有各域信任体系的认证方式,将各域的信任锚加入区块链社区,即联盟链的环境中,以实现多域间的跨域认证,因此,系统的可扩展性强。

## 4 结语

本文提出了基于区块链的跨域认证方案。该方案在不改变域内 PKI 认证模型的前提下,将经过许可的域加入联盟链,实现双向实体跨域认证,并提供快速重认证。与已有跨域认证方案相比,本文方案在保证安全的基础上,通过减少签名与验证签名的次数,能有效提升跨域认证的效率;而且系统基于联盟链的设计,可扩展性强。

**参考文献:**


[1] 荆继武,林璟锵,冯登国. PKI技术[M]. 北京:科学出版社,2008:6. (JING J W, LIN J Q, FENG D G. PKI Technology [M]. Beijing: Science Press, 2008: 6.)

[2] 关振胜. 公钥基础设施 PKI 及其应用[M]. 北京:电子工业出版社,2008:14-16. (GUAN Z S. Public Key Infrastructure PKI and Its Application [J]. Beijing: Publishing House of Electronics Industry, 2008: 14-16.)

[3] 路晓明,冯登国. 一种基于身份的多信任域网格认证模型[J]. 电子学报,2006,34(4):577-582. (LU X M, FENG D G. An identity-based authentication model for multi-domain grids [J]. Acta Electronica Sinica, 2006, 34(4): 577-582.)

[4] BUTLER R, WELCH V, ENGERT D, et al. A national-scale authentication infrastructure [J]. IEEE Computer, 2000, 33(12): 60-66.

[5] ROUIBAH K, OULD-ALI S. Dynamic data sharing and security in a collaborative product definition management system [J]. Robotics and Computer-Integrated Manufacturing, 2007, 23(2): 217-233.

[6] MILLÁN G L, PÉREZ M G, PÉREZ G M, et al. PKI-based trust management in inter-domain scenarios [J]. Computers & Security, 2010, 29(2): 278-290.

[7] 张文芳,王小敏,郭伟,等. 基于椭圆曲线密码体制的高效虚拟企业跨域认证方案[J]. 电子学报,2014,42(6):1095-1102. (ZHANG W F, WANG X M, GUO W, et al. An efficient inter-enterprise authentication scheme for VE based on the elliptic curve cryptosystem [J]. Acta Electronica Sinica, 2014, 42(6): 1095-1102.)

[8] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报,2006,29(8):1271-1281. (PENG H X. An identity-based authentication model for multi-domain [J]. Chinese Journal of Computers, 2006, 29(8): 1271-1281.)

[9] 罗长远,霍士伟,邢洪智. 普适环境中基于身份的跨域认证方案[J]. 通信学报,2011,32(9):111-115. (LUO C Y, HUO S W, XING H Z. Identity-based cross-domain authentication scheme in pervasive computing environments [J]. Journal on Communications, 2011, 32(9): 111-115.)


(下转第 326 页)

ZENG Z Y, ZHANG X F. Outsourced decryption scheme supporting attribute revocation [J]. Journal of Tsinghua University (Science and Technology), 2013, 53(12): 1664 - 1669.)

[5] BENABBAS S, GENNARO R, VAHLIS Y. Verifiable delegation of computation over large datasets [C]// CRYPTO 2011: Proceedings of the 2011 Annual Cryptology Conference, LNCS 6841. Berlin: Springer, 2011: 111 - 131.

[6] BARBOSA M, FARSHIM P. Delegatable homomorphic encryption with applications to secure outsourcing of computation [C]// CT-RSA 2012: Proceedings of the Cryptographers' Track at the RSA Conference, LNCS 7178. Berlin: Springer, 2011: 296 - 312.

[7] FIORE D, GENNARO R. Publicly verifiable delegation of large polynomials and matrix computations, with applications [C]// CCS '12: Proceedings of the 2012 ACM Conference on Computer and Communications Security. New York: ACM, 2012: 501 - 512.

[8] ZHANG L F, SAFAVI-NAINI R. Private outsourcing of polynomial evaluation and matrix multiplication using multilinear maps [C]// Proceedings of the 12th International Conference on Cryptology and Network Security, LNCS 8257. Cham: Springer, 2013: 329 - 348.

[9] 任艳丽,谷大武,蔡建兴,等. 隐私保护的可验证多元多项式外包计算方案[J]. 通信学报,2015,36(8):23 - 30. (REN Y L, GU D W, CAN J X, et al. Verifiably private outsourcing scheme for multivariate polynomial evaluation [J]. Journal on Communications, 2015, 36(8): 23 - 30.)

[10] PAPAMANTHOU C, SHI E, TAMASSIA R. Signatures of correct computation [C]// Proceedings of the 10th Theory of Cryptography Conference on Theory of Cryptography, LNCS 7785. Berlin: Springer, 2013: 222 - 242.

[11] FIORE D, GENNARO R, PASTRO V. Efficiently verifiable computation on encrypted data [C]// CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2014: 844 - 855.

[12] ZHANG L F, SAFAVI-NAINI R. Batch verifiable computation of polynomials on outsourced data [C]// ESORICS 2015: Proceedings of the 2015 European Symposium on Research in Computer Security, LNCS 9327. Cham: Springer, 2015: 167 - 185.

[13] SUN Y, YU Y, LI X, et al. Batch verifiable computation with public verifiability for outsourcing polynomials and matrix computations [C]// Proceedings of the 21st Australasian Conference on Information Security and Privacy: Part I, LNCS 9722. Cham: Springer, 2016: 293 - 309.

[14] GARG S, GENTRY C, HALEVI S. Candidate multilinear maps from ideal lattices [C]// EUROCRYPT 2013: Proceedings of the 2013 Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 7881. Berlin: Springer, 2012: 1 - 17.

[15] BONEH D, GOH E-J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts [C]// TCC 2005: Proceedings of the 2005 Theory of Cryptography Conference, LNCS 3378. Berlin: Springer, 2005: 325 - 341.

This work is partially supported by the National Natural Science Foundation of China (U1636114, 61572521), the National Code Development Program of China (MMJJ20170112), the National Key Research and Development Program of China (2017YFB0802002), the Natural Science Foundation of Shaanxi Province (2016JQ6037).

**LUO Xiaoshuang**, born in 1992, M. S. His research interests include information security, cryptology.

**YANG Xiaoyuan**, born in 1959, M. S., professor. His main research interests include information security, cryptology.

**LI Cong**, born in 1990, M. S. candidate. His research interests include public cryptography.

**WANG Xu'an**, born in 1981, Ph. D., assistant professor. His research interests include information security, cryptology.

(上接第 320 页)

[10] LI Y, CHEN W, CAI Z, et al. CAKA: a novel certificateless-based cross-domain authenticated key agreement protocol for wireless mesh networks [J]. Wireless Networks, 2016, 22(8): 2523 - 2535.

[11] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2017-03-22]. http://tmtfree.hd.free.fr/albums/files/TMTisFree/Documents/Economy/Bitcoin.%20A%20Peer-to-Peer%20Electronic%20Cash%20System.pdf.

[12] 工信部. 中国区块链技术和应用发展白皮书[R]. 北京: 工信部,2016: 23. (Ministry of Industry and Information Technology. White paper for Chinese blockchain technology and application development [R]. Beijing: Ministry of Industry and Information Technology. White paper, 2016: 23.)

[13] FROMKNECHT C, VELICANU D, YAKOUBOV S. CertCoin: a namecoin based decentralized authentication system [R/OL]. (2014-05-14) [2017-05-08]. http://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf

[14] AXON L. Privacy-awareness in blockchain-based PKI, CDT technical paper series 21/15 [R/OL]. [2017-05-08]. https://ora.ox.ac.uk/objects/uuid:f8377b69-599b-4cae-8df0-f0cded53e63b.

[15] LEWISON K, CORELLA F. Backing rich credentials with a blockchain PKI [EB/OL]. [2017-04-12]. https://pomcor.com/techreports/BlockchainPKI.pdf.

[16] 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 Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481 - 494.)

[17] 蔡维德,郁莲,王荣,等. 基于区块链的应用系统开发方法研究[J]. 软件学报,2017,28(6):1474 - 1487. (CAI W D, YU L, WANG R, et al. Blockchain application development techniques [J]. Journal of Software, 2017, 28(6): 1474 - 1487.)

This work is partially supported by the Information Engineering University Research Fund (2016609903).

**ZHOU Zhicheng**, born in 1992, M. S. candidate. His research interests include information security, blockchain.

**LI Lixin**, born in 1967, Ph. D., research fellow. His research interests include network and information security.

**LI Zuohui**, born in 1981, Ph. D., associate research fellow. His research interests include public key cryptography, network security.