

区块链跨域身份管理系统的优化

陈立军

(广州软件学院 软件工程系, 广东 广州 510990)

摘要:身份认证是云计算的安全基础,当前云计算环境下不同信任域之间信息交互频繁,迫切需要研究安全且高效的不同信任域间的跨域身份认证。由于传统的中央式身份管理系统存在安全性和可扩展性问题,分散式身份管理受到了学术界和工业界的广泛关注,然而,随着各域之间共享交互的日益增多,分散身份的管理和认证对跨域信任提出了更高的要求,面临着巨大的实现挑战。该文提出了一种基于区块链的去中心化跨域身份管理系统(DCIMB),在此系统中设计了一个去中心化标识符,用于联盟区块链技术命名身份,同时,DCIMB系统中的每个节点都可以参与身份认证和信任建立,从而解决了中心化机制的单点故障问题。为了进一步提高认证效率,保护用户隐私,DCIMB引入了单向累加器作为身份数据结构,保证了实体身份的有效性,并从理论上分析了DCIMB的可行性和性能,并且与现有的身份管理系统相比,DCIMB在跨域身份验证方面实现了出色的优化。

关键词:身份管理;去中心化;区块链;单向累加器;跨域认证

中图分类号:TP311

文献标识码:A

文章编号:1673-629X(2023)02-0138-08

doi:10.3969/j.issn.1673-629X.2023.02.021

Optimization of Blockchain Cross-domain Identity Management System

CHEN Li-jun

(Department of Software Engineering, Software Engineering Institute of Guangzhou, Guangzhou 510990, China)

Abstract: Identity authentication is the security basis of cloud computing. In the current cloud computing environment, information interaction between different trust domains is frequent, so it is urgent to study the secure and efficient cross-domain identity authentication between different trust domains. Because of the security and scalability problems of traditional centralized identity management system, decentralized identity management has been widely concerned by academia and industry. However, with the increasing sharing and interaction between domains, decentralized identity management and authentication have put forward higher requirements for cross-domain trust, and are faced with great implementation challenges. We propose a decentralized cross-domain identity management system (DCIMB) based on blockchain. In this system, a decentralized identifier is designed to name identities for federated blockchain technology. Meanwhile, each node in the DCIMB system can participate in identity authentication and trust establishment, thus eliminating the single point of failure of the centralized mechanism. In order to further improve the certification efficiency and protect user privacy, DCIMB introduces one-way accumulator as identity data structure to ensure the effectiveness of the entity identity, and the feasibility and performance of DCIMB are analyzed theoretically. Compared with the existing identity management systems, DCIMB in cross-domain authentication excellent optimization is realized.

Key words: identity management; decentralization; blockchain; one-way accumulator; cross-domain authentication

0 引言

集中式身份管理系统的功能依赖于特定的身份服务器节点,导致单点故障问题,一旦这些身份服务器节点失效,网络中所有的身份注册、验证和更新操作都将中断,这一缺陷使得集中式身份系统容易受到分布式拒绝服务(DDoS)攻击^[1-2],给网络安全带来严重隐患。

集中式身份管理问题的另一个方面来自于互联网

上的孤立主义趋势,通过隔离,在集中式平台或机构中注册的用户身份和信息只能在特定的信任域^[3]中使用,不仅难以建立和维护不同信任域的身份提供者之间的关系,而且难以审计或跟踪数据滥用。为实现用户身份的交叉验证和相互信任,各平台和机构只能重复收集用户身份信息,造成存储和传输资源的浪费,给业务应用带来不便。因此,跨不同信任域进行实体身份验证和身份管理已经成为一个

收稿日期:2022-04-01

修回日期:2022-08-04

基金项目:2021年度广东省普通高校重点科研平台和科研项目(2021KTSCX160);广州软件学院科研项目(ky202116)

作者简介:陈立军(1974-),男,研究生,讲师,研究方向为区块链安全。

问题。

近年来,区块链逐渐发展成为一种分布式计算模式,具有去集中化、集体维护、可编程、可跟踪等特点,随着区块链技术研究的逐步深入,基于区块链的应用呈现出爆炸式的增长,并具有与其他领域交叉的广阔前景。

在区块链技术诱人特性的驱动下,该文提出了一种基于区块链的去中心化跨域身份管理系统(DCIMB),设计了一个基于联盟区块链技术的去中心化标识符(DID),可以使用一个身份证书(如公钥、密码或指纹)来颁发DID,以确保身份信息不会被篡改,同时,系统中的每个节点都可以参与认证和信任建立,解决了集中式机制的节点故障。

1 相关工作

1.1 国内现状

西安理工大学的左碧露^[4]针对传统物联网设备认证方案,提出了一个基于区块链和雾计算的去中心化物联网设备认证方案,利用区块链的不可篡改性来保证票证的真实性,但研究的不是跨域身份管理。

南京邮电大学的徐君泽^[5]针对基于区块链交易主体的可信性及多方交易的安全性,提出了新的跨域认证方法,他的方法提高了跨域认证效率,但研究范围局限于融资租赁系统。

同样的,也是南京邮电大学的江淳^[6]针对远程医疗系统,提出了一种基于区块链的远程医疗跨域认证模型,作者说他的模型有效提高了系统的通信效率,但作者在文中没有提及是否解决了传统中心服务器单点故障问题。

贵州大学的王琳杰^[7]就物联网数据安全及跨域认证提出一个模型,重点研究了物联网的数据安全,但与该文相比,该文的重点是解决传统中心服务器单点故障。

王晓欣、陈志德^[8]两作者针对教育资源共享安全性低以及身份认证困难的问题,提出基于区块链技术与无证书签名相结合的可跨域身份认证方案,但基于区块链系统的处理效率还有待提高。

桂林电子科技大学的徐娟娟^[9]基于云环境的异构跨域身份认证方案,但他们的重点是满足身份匿名性、抵抗替换性攻击、抵抗重放攻击和中间人攻击。

电子科技大学的王国安^[10]提出基于面向知识共享的跨域访问控制技术,提高了资源访问控制的安全性,与该文相比,侧重点还是不同的,该文的重点是研究跨域身份管理系统的优化。

1.2 国外现状

传统的身份管理系统,如OpenId^[11],主要是基于

PKI的集中式体系结构,为了防止公共文件被恶意篡改,每个数据都进行了数字签名,这样证书就可以在网络安全地分发^[12]。虽然PKI/CA系统可以实现双向认证,但在通信过程中需要从中心身份仓库获取第三方数字证书,这就要求中心节点具有高性能的响应处理能力,在基于PKI/CA的大规模系统中,随着系统规模的增加,中心节点将成为系统性能的瓶颈,并出现过载现象,除了可扩展性问题外,CA机制还存在单点信任的安全缺陷。

Nayak等人^[13]提出的D-FOAF模型通过社区驱动的接入授权机制将CA的权限分配给每个网络社区中的节点,以分散中心验证节点的压力;Pavithran等人^[14]考虑到只有基于公钥证书的身份管理机制需要CA等集中式节点来提供服务,提出了基于身份的密码学来替代基于公钥的密码学,然而,Lim的方案针对的是网格计算模型,是一种交互式认证机制,这给它的应用带来了许多限制。

随着比特币的出现,带有分布式账本技术的区块链也被用于实现身份管理系统,因为它去中心化,避免了身份信息被少数组织或个人掌握^[15];在文献[16]中,Mohanty等人开发了高效、轻量级、集成的区块链模型,以满足物联网的需求。然而,大多数基于区块链的身份管理系统并未考虑多个领域的身份识别和融合需求,而这正是该文的核心目标。

在传统的身份管理系统中,用户的身份被限制在信任域内,只有在同一信任域内的身份是可信的,因此,身份管理系统的热点问题主要集中在隐私保护和可扩展性两个方面。目前,无论是集中式云计算网络还是全分布式网络环境,都涉及到不同信任域的认证,跨域认证已成为身份管理系统中亟待解决的问题。

DCIMB在区块链技术的基础上设计了一个DID,解决了单点故障问题,提高了系统的可扩展性,与其他启用区块链的身份管理系统不同,DCIMB引入了单向累加器来验证身份的有效性,将身份验证的时间复杂度优化到恒定水平。此外,DCIMB还使用了联盟区块链系统,通过分布式共识保持了累加器状态的全局一致性和抗篡改性,提高了认证性能,保护了用户的隐私信息。

2 系统设计

2.1 概述

该文的核心工作是去中心化身份管理和跨域认证系统,设计目标是解决认证中心的单点故障问题,提高跨域认证场景下的认证性能。

单一信任问题使得它不适合跨信任域身份验证场景,DCIMB使用DID来识别身份实体,以消除单点依

赖。DID 由统一资源标识符 (URI) 和文档组成, URI 用作标识符, 文档存储用户的公钥、身份信息和其他数据, 当用户发送消息时, 接收方可以通过查找 DID 来验证用户的公钥信息, 以确定消息是否被篡改。

PKI 系统中的 CA 还负责确保用户的公钥信息的真实性, 在 DCIMB 中, 此功能由认证提供者 (IdP) 提供。IdP 是一个开放和可信的部门, 如政府、银行、个人或私人企业, 它只负责其领域内的身份发放, PKI/CA 系统采用集中式、分层或多组织结构, 因此, 当 CA 受到攻击时, 会影响整个系统, 导致单点故障问题。但是, DCIMB 通过区块链技术连接每个信任域中的 IdP, 当特定信任域中的 IdP 受到攻击时, 其影响范围仅局限于该信任域中的本地区域, 相比之下, 系统中的其他信任域仍然可以工作, 从而避免了全局 CA 中的单点故障问题。

身份实体通过创建 DID 来标识自己, DID 是一个通用的用户标识符, 它不包含任何用来证明身份的信息, 所有附加在 DID 上的身份信息都需要通过 IdP 颁发身份证书进行认证。因此, 在 DCIMB 中, DID (和 DID 文件) 被称为主身份, 而 IdP 颁发的身份证书被称为影子身份。DCIMB 不允许除身份所有者以外的其他各方通过身份证书来追踪身份的实际信息, 以保护用户隐私, 这种将用户标识符与特定用户标识属性分离的想法称为两级标识体系结构。

在 DCIMB 中, 身份识别和管理涉及两个方面:

(1) 准确识别和判断给定的标识符是否与公钥证书匹配;

(2) 判断标识符是否可以访问指定的资源, 在跨域认证中, 跨域认证还涉及到不同信任域之间的相互认证, 同时, 为了保护用户的隐私和匿名性, 有必要在认证过程中尽可能少地公开身份信息, 这是最小公开原则。

为了高效判断集合成员, 有现成的方案, 如环签名和群签名, 但是, 由于这些方案需要可信的设置阶段, 因此不适合部署分布式环境。为了加速认证和公共集合成员的判断, DCIMB 引入了单向累加器作为密码原语来构建认证机制, 对于大型集合成员的判断问题, 单向累加器可以显著降低存储和通信成本, 具体来说, 对于每个域有 m 个域和 n 个账户的系统, 集合成员身份识别签名从 $O(mn)$ 减少到 $O(m)$, 这意味着每个域的空间复杂度可以达到一个恒定的水平。

对于大量的主身份账户, 必然有大量的累加器状态, 如果这些状态需要通过全局数据库或目录 (按照 PKI 的设计) 进行保存, 则不可避免地会出现单点故障和信任。类似地, 跨多个域的累加器状态的同步和认证将难以实现, 所以 DCIMB 选择了区块链技术来维

护全局状态并存储和寻址 DID 文档, DCIMB 在联盟区块链系统中维护累加器状态, 而用户的影子身份数据 (如指纹、公钥等) 则存储在链下。

如图 1 所示, 不同信任域中的已识别实体通过单向累加器证明其身份有效性, 每个域中的 IdP 证明了有关其身份的附加信息, 不同信任域的 IdP 基于联盟区块链系统和共识协议对身份有效性、IdP 权限和跨域认证达成一致, 对于跨域认证, 身份依赖方读取被认证方的 DID 文档, DID URI 寻址该文档, 它通过被认证方提供的累加器凭证来确认身份的真实性, 身份附加属性的真实性可以通过与被认证方域中的 IdP 通信来确认。

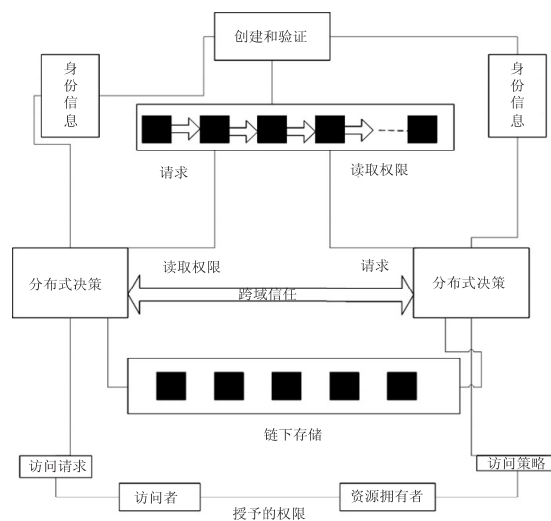


图 1 DCIMB 系统架构

2.2 单向累加器的设计

DCIMB 的核心数据结构是单向累加器, 像 Merkle 树一样, 单向累加器提供了集合成员的有效包含证明, 大大节省了识别的存储成本。在单向累加器的基础上, DCIMB 构造了一系列用于用户身份管理和身份验证的基本组件。

DCIMB 中的单向累加器借鉴了参考文献 [17] 中提出的无碰撞累加器, 特别地, 下列 5 种多项式时间算法用于单向累加器。

(1) $\text{AccGen}(1^k) \rightarrow a_0$: 概率生成算法接受秘密参数 k , 并为空累加器生成初始累加值 a_0 ;

(2) $\text{AccAdd}(a, y) \rightarrow (a', w)$: 接受当前累加值 a 和要累加的数据 y , 累加后输出值 a' 和要见证的元素 w ;

(3) $\text{AccWitAdd}(w, y) \rightarrow w'$: 输入要累加的数据 y 和当前见证 w , 输出新的见证 w' ;

(4) $\text{AccVer}(a, y, w) \rightarrow b \in \{0, 1\}$: 输入当前累加器的累计值 a 、要验证的数据 y 、要见证的 w , 如果 y 属于累加器, 则返回 1, 否则, 返回 0;

(5) $\text{AccDel}(\text{aux}, a, y) \rightarrow a'$: 输入 trapdoor 函数

aux, 累加值 a 和要删除的数据 y , 删除 y 后输出新的累加值 a' 。

密码学中的累加器可以快速确定元素是否属于特定集合的一种方式, 在 DCIMB 中, 累加器的内容是键值对 (did, pk) , 其中 did 是给定的身份标识符, pk 是对应的公钥, 对于任何有效的识别密钥对 (did, pk) , 有:

$$AccVer(a, (did, pk)) = 1 \quad (1)$$

式 1 称为单向累加器的包含证明, a 为累加器 Acc 的累加值。

由于身份必须是可公开验证的, 整个区块链网络需要维护一个通用的全局累加器状态来支持所有节点的身份验证, 每次创建、更新或撤销公钥时, 处理交易的矿工都需要更新累加器并将更新后的累加器值 a' 添加到累加器的信息中, 由于累加器的共同可检查性属性, 网络中的任何节点都可以检查更新的累加器 a' 是否正确包含新值并验证计算的正确性。此外, 由于累加器公开存储在区块链中, 因此累加器难以破解, 避免了对累加器初始化的欺骗。

除了标记和验证主身份的有效性外, 单向累加器还用于快速验证影子身份是否属于主要身份, 即验证影子身份的合法性。图 2 显示了 DCIMB 中的影子身份验证, 其中 m 和 n 分别是信任域的数量和每个域中的账户数量, $sid_{i,j}$ 表示第 i 个信任域中的第 j 个影子身份。如图 2 所示, 除了全局累加器状态外, 每个主身份都需要一个单向累加器来累加其他身份证书, 例如指纹和密码。主身份 did 拥有的累加器记录为 $Accs(did)$, 这个累加器不需要全局可见, 由于单个身份的累积数据有限, 因此 $Accs(did)$ 使用 Merkle 哈希树构建, 第 i 个影子身份累加器的中间状态表示为 mid_i , 在全局累加器 Acc_g 中维护。

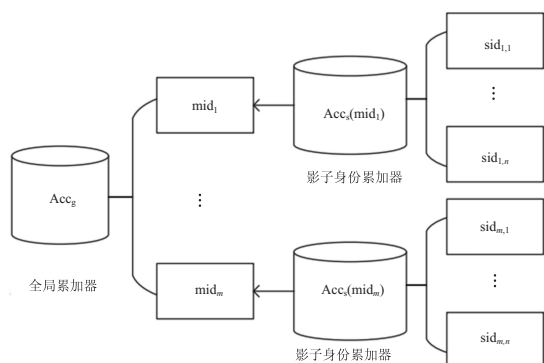


图 2 DCIMB 中的影子身份验证

2.3 去中心化标识符

为了更好地表示用户的身份和属性, DCIMB 中将用户身份分为主身份 id_m 和影子身份 id , 分别表示用户的唯一身份和属性身份, 主标识用于唯一标识区块链网络中的用户, DID 通常与存储与身份信息和认证相

关的其他元数据的 DID 文档相关联。如图 3 所示, 主标识由一个 DID (例如, DID: exmp:1234567890abcde) 或一个有意义的层次命名标识符 (例如, DID: exmp:/cn/guangzhou/pku/2021/chenlijun) 唯一确定, 在主标识的 DID 文档中, 存储一个主公钥 pk_m , 主公钥密钥用于发布其他身份类型, 而与 pk_m 对应的私钥 sk_m 用于撤销已发布的身份信息。

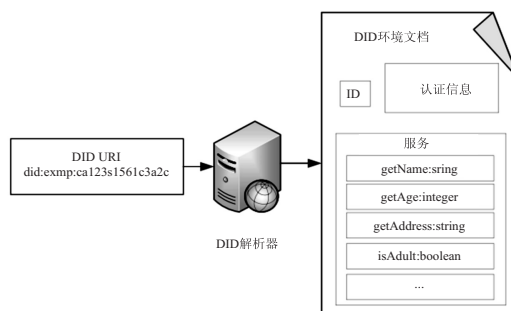


图 3 DID 映射到文档的示意图

DID 的机制可以看作是一个分散的键值数据库, 通过用户身份提供对 DID URIs 和 DID 文档的访问, DID 文档的目的是描述公共密钥、身份验证协议和服务端点, 以指导与已识别实体的加密和可验证交互, DID 文档格式中 id 字段是与该文档相对应的 DID URI, 认证字段提供了一组在线主公钥, 公钥用于加密和其他加密操作, 这些操作是身份验证或服务端点建立自治愈合通信的基础。此外, 公钥可能在 DID CRUD 操作的授权机制中发挥作用, 如果在 DID 文档中不存在公钥, 则必须假定该密钥已被撤销或未被验证, 包含被撤销密钥的 DID 文档还必须包含或引用被撤销密钥的信息。

DID 文档还提供了一组服务端点, 即文档的服务字段, 服务端点可以代表身份主体提供的任何服务, 包括用于进一步发现、身份验证、授权或交互的分散身份管理服务。

主标识是用户的唯一标识, 然而, 在许多身份验证场景中, 不需要显示真实的身份, 此外, 由于特定类型的身份凭证 (如指纹) 的特征, 主身份有时不能直接关联, 因此, 在某些特定的场景下, 需要使用影子身份进行身份验证和识别。

影子身份标识可以是钥匙、密码或其他生物特征信息, 主标识可以与多个影子标识相关联, 这些影子标识可以证明特定的用户属性, 如年龄和性别或主标识授予的权限, 给定一个影子标识 id , 它可以确定这些 id 是否属于一个特定的主标识 id_m , 除了 id_m 所有者之外, 其他用户无法根据 id_m 找到相应的 id 集合 (无论是 id_m 还是 pk_m), 有效保护用户隐私和身份安全。

2.4 身份操作

在 DCIMB 中, 每个物理用户或设备由 DID 唯一

标识, DID 可能有多个密钥对, 用于发出不同的标识属性, DID 标识所有者可以从链外私有存储的文档中读取与该标识关联的所有公钥和文档, 但是, 不能直接从公钥获取用户的 DID 身份, 身份操作包括系统中的身份注册、身份更新、身份撤销和身份验证, 该文档将 DID 的公钥集标记为 G_{did} , 用户为 G_{did} 生成的累加器记录为 ACC_{did} 。

2.4.1 身份登记

在身份注册操作中, 身份所有人首先将交易发布到链上, 其中 did 为要发布的身份标识符, pk_{on} 和 pk_{off} 分别为身份所有人的在线和离线公钥, σ_{on} 和 σ_{off} 分别是身份所有人的在线私钥 pk_{on} 和离线私钥 pk_{off} 的签名, 即:

$$T_{reg} = ((did, register, online, values) = (pk_{on}, \sigma_{on}), (did, register, offline, values) = (pk_{off}, \sigma_{off})) \quad (2)$$

$$\sigma_{on} = \text{sig}(sk_{on}, did) \quad (3)$$

$$\sigma_{off} = \text{sig}(sk_{off}, did) \quad (4)$$

挖掘节点验证接收到的交易, 如果下列条件没有被占用, 均满足, 则身份登记视为有效, 交易确认, 否则, 交易操作将被忽略, 对于条件(5), 可以通过全局维护的累加器来判断是否有一对 (did, pk') 满足 $pk' \neq pk$ 。

$$\begin{cases} \text{AccVer}(pk_{on}, \sigma_{on}, did) = 1 \\ \text{AccVer}(pk_{off}, \sigma_{off}, did) = 1 \end{cases} \quad (5)$$

身份登记流程如图4所示。当注册一个标识时, DCIMB 首先检查用户的累加器是否存在, 如果不存在, 将创建一个新的累加器, 块矿机执行概率生成算法:

$$\text{AccGen}(1^k) \rightarrow a_0 \quad (6)$$

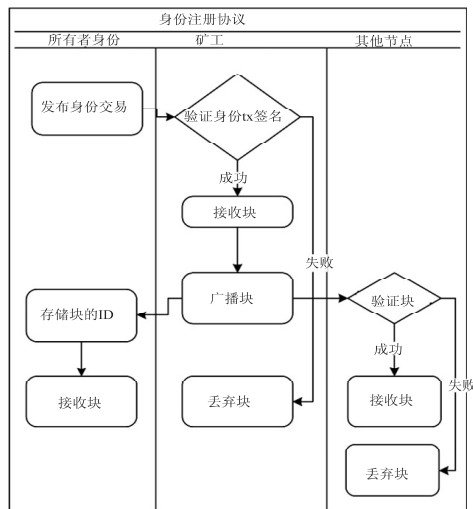


图4 DCIMB 中的身份注册过程

初始值 a_0 被写入创建的块 B_k , 同时, 累加器的秘密参数(如 trapdoor 函数)被离线密钥安全地存储在链

下存储系统中, 所有接收到块 B_k 的节点都将验证创建累加器的正确性, 如果验证失败, 则直接丢弃该块, 否则, 累加器 a_0 将被确认保存。

身份注册成功后, 用户需要主动更新全局单向累加器值 a_g , 以确认用户身份的合法性:

$$\text{AccAdd}(a_g, did) \rightarrow (a'_g, w) \quad (7)$$

此外, 用户需要更新链上的身份累加器, 并为已注册的用户生成单向累加器:

$$\text{AccGen}(did, 1^k) \rightarrow a_0 \quad (8)$$

此步骤用于初始化用户账户状态。

2.4.2 身份更新

随着授权身份的增加, 需要不断地向 G_{did} 添加一个键, 相应地, 累加器的值也需要更新, 在用户主动授权 pk_i 之后, 操作将被执行, 其中 a' 是 did 的累加器更新后的累加值, pk_i 身份所有者持有 w 以证明该身份已被 did 授权。

$$\text{AccAdd}(did, pk_i) \rightarrow (a', w) \quad (9)$$

当身份所有者希望使用新的公钥 pk_{new} 而不是旧的公钥 pk_{old} 时, 事务将被发布在如下的表达式中, 为使用旧私钥 sk_{old} 的 did 和 pk_{new} 的签名, 它确保标识所有者不能篡改更新与 did 相对应的公钥信息。

$$T_{upd} = (did, update, values = (pk_{old}, pk_{new}, \sigma_1, \sigma_2, aux)) \quad (10)$$

$$\sigma_1 = \text{sign}(sk_{old}, (did, pk_{new})) \quad (11)$$

$$\sigma_2 = \text{sign}(sk_{new}, did) \quad (12)$$

为使用新的私钥 sk_{new} 的 did 签名, 证明身份所有者对 pk_{new} 的所有权, aux 字段包含当 pk 或 sk 泄漏时撤销密钥对的辅助信息。

当区块链网络中的矿机接收到 T_{upd} 时, 检查式(13)的条件, 如果不满足式(13)的任何条件, 事务将被忽略, 其他接收到该块的节点也会验证 T_{upd} 的有效性, 如果检测失败, 则丢弃该块。

$$\begin{cases} \text{是否} \text{与} \text{交易中的} pk_{old} \text{ 相对应?} \\ \text{AccVer}(pk_{old}, \sigma_1, (did, pk_{new})) = 1 \\ \text{AccVer}(pk_{new}, \sigma_2, did) = 1 \end{cases} \quad (13)$$

2.4.3 身份认证

在传统的基于区块链的身份管理系统中, 由于区块的仅追加特性, 需要遍历整个链中的所有区块来确定身份的有效性, 身份验证的时间复杂度为 $O(n)$, 其中 n 为网络的身份号。为了降低时间复杂度, 该文提出了一种基于单向密码累加器的身份验证方案, 身份认证函数接受用户提交的参数 did, pk_m 和将要见证的 w , 判断式(14)条件是否合适, 该操作的时间复杂度为 $O(1)$, 因为全局累加器的值 a_g 对区块链网络中的所有节点都是可见的, 所以任何节点都可以作为身份

验证节点。

$$\text{AccVer}(a_g, (\text{did}, \text{pk}_m), w) = 1 \quad (14)$$

2.4.4 身份撤销

传统的PKI系统使用证书撤销列表或在线证书状态协议发布身份撤销信息,在DCIMB中,标识符和公钥之间的绑定关系通过发送区块链交易来释放,具体来说,IdP或身份所有者将向区块链发送撤销交易,矿工节点收到撤销交易后,将检查以下条件是否满足,如果不满足这些条件中的任何一个,撤销交易将被忽略,否则,交易是符合的,矿工将删除公钥并更新全局累加器值。

$$\begin{aligned} \text{Trevo} = & ((\text{did}, \text{revocation}, \text{online}, \text{values}) = \\ & (\text{pk}_{\text{on}}, \sigma_{\text{on}}), \text{did}, \text{revocation}, \text{offline}, \text{values} = \\ & (\text{pk}_{\text{off}}, \sigma_{\text{off}})) \end{aligned} \quad (15)$$

$$\begin{cases} \text{did 是无效时:} \\ \text{AccVer}(\text{pk}_{\text{on}}, \sigma_{\text{on}}, \text{did}) = 1 \\ \text{AccVer}(\text{pk}_{\text{off}}, \sigma_{\text{off}}, \text{did}) = 1 \end{cases} \quad (16)$$

$$\text{AccDel}(\text{aux}, a_g, (\text{did}, \text{pk}_{\text{on}})) \rightarrow a_g \quad (17)$$

2.4.5 跨域身份验证

跨域认证的前提是建立不同域之间的信任关系,不同信任域签发的身份证书具有不同的证明效果,为了鼓励区块链网络中的节点执行诚实认证并惩罚虚假身份证书,这些必须包括控制和管理连接节点的机制,因此,DCIMB采用联合体区块链,财团区块链是一个被许可的区块链,只允许一组预先选定的节点进行计费,而其他节点只能参与交易。

图5给出了跨域认证的总体流程。对于跨域认证,域B的身份依赖方(通常也是认证方)RP_B首先将交易 $T_{\text{ver}}(\text{id}_i, w_i)$ 发布到链上,其中 id_i 是请求认证的参与方, w_i 是验证其身份组的参与方,在域A中的任何可用IdP(记录为IdP_A)接收到 T_{ver} 后,它根据 w_i 验证该交易属于在域A中注册的身份,如果RP_B不需要进一步验证 id_i 的公钥,IdP_A可以直接向RP_B确认身份,否则,IdP_A搜索与 id_i 对应的 pk_i 并返回公钥信息。

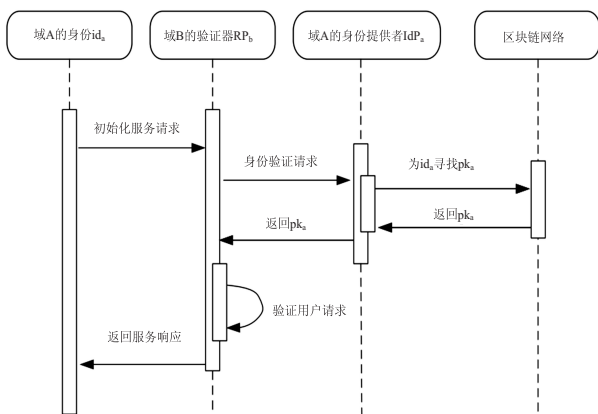


图5 DCIMB中的跨域认证过程

3 实验和评估

在本部分中,从安全、可扩展性和跨域认证三个方面对DCIMB的性能进行了评估,构建了一个基于以太坊的财团区块链,并实现了一个DCIMB原型系统,系统部署在四台高性能服务器上,硬件参数如表1所示。在该文的原型系统中,Docker用于发布以太坊节点的多个应用图像,由此建立了一个简单的20个节点的区块链网络。

表1 原型系统硬件配置

硬件	型号
CPU	Intel (R) Xeon (R) CPU E5-2630 v3 @ 2.40 GHz
内存	32 GiB DDR3 1 600 MHz ECC
硬盘	1 TiB SAS RAID5
网卡	Intel I350 Gigabit Ethernet

3.1 安全

由于在DCIMB中,一个实体的标识信息的有效性由单向累加器保存,单向累加器的安全性直接决定了标识的安全性,Camenisch J和Lysyanskaya A在参考文献[17]中提供了单向累加器安全性的证明,由于篇幅的限制,这里就不作进一步的分析了。另一方面,身份实体使用基于非对称加密的会话密钥协商机制与IdP和认证方进行通信,位于认证过程中的公钥是唯一的、防篡改的,可以由双方独立确认,另外,即使在认证会话中协商的密钥被泄露,攻击者也无法获得用户的私钥和累加器凭证,因此,他们不能在保证签名完整性的同时篡改通信数据,该特性使DCIMB能够有效地防止中间人攻击。

为了进一步测试系统的安全性,该文生成了三组身份公钥对,每组10万对,这三个数据组分别对应有有效的标识、被篡改的标识和不存在的标识,该文的原型系统对这些公钥对的认证结果如表2所示。所有有效身份的公钥对都能成功通过认证,但是,对于被篡改的身份或不存在的身份,所有身份验证都失败,虽然这个实验不能完全模拟所有的恶意攻击,但足以证明系统的安全性。

表2 不同身份公钥对的认证结果

组	通过	失败	精度/%
有效身份	100	0	100
干扰身份	0	100	100
不存在的身份	0	100	100

3.2 可扩展性

对于以比特币为代表的区块链系统来说,可扩展性的主要限制是共识算法效率低,比特币系统需要所有节点对每一笔交易达成一致,以确保网络中的数据一致性,因此,如果采用类似于比特币的公共区块链系

统,大量用户身份信息的实时更新将给整个链带来巨大的性能压力;另一方面,如果采用像 Certcoin 这样的方案,将用户的身份信息保存在链上,整个区块链网络的账簿规模将是巨大的,此外,为特定用户检索和更新身份数据的时间复杂性也很高。

DCIMB 在两个方面优化了可扩展性。首先,基于联盟区块链机制,采用随机算法选择共识节点,降低共识形成成本;其次,与现有的 Certcoin 系统不同,DCIMB 中采用了累加器,取代了存储证书、指纹等用户身份数据的顺序块结构,添加新用户标识只需要对单向累加器的内部状态进行访问和简单的模求幂,而且,对于频繁的用户身份验证操作,它更加简单,它只需要两个大整数的模幂,这取决于累加器的比特数,从而大大降低了查找图书数据的时间成本,提高了系统的性能和吞吐量。

为了测试 DCIMB 的可扩展性,通过 GnuPG 加密套件生成了大量的密钥对,并随机分配它们来识别系统中的实体,该文以传统的基于 UTXO 的区块链身份管理系统 Certcoin 作为评估基准,值得肯定的是, Certcoin 是最具代表性的基于区块链的身份管理系统,它不仅具有对认证机构的开放性和适用性,而且具有分散的信任网络和无单点故障的优点。首先,测量了单域认证中认证延迟与身份数量之间的关系,图 6 为域中节点数为 5 的实验结果。从图 6 可以看出, Certcoin 的认证延迟是线性增加的,这是因为 Certcoin 需要遍历所有块来验证用户的公钥的有效性,相比之下,对于 DCIMB,身份验证时间不受累积身份数量的影响。

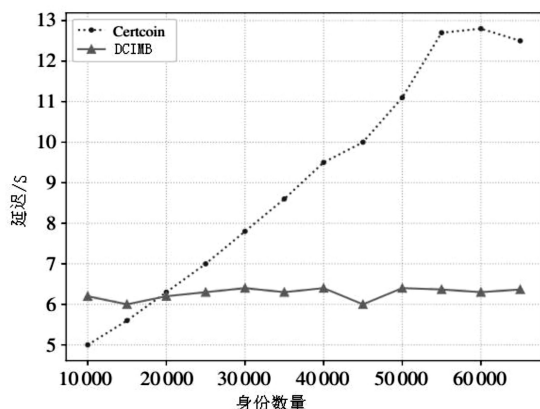


图6 单域场景下不同身份数的认证延迟

3.3 跨域身份验证

在本节中,首先测量随着域数量的增加而跨域身份验证的延迟,逐渐增加域的数量,并在每个域固定 1 000 (id, pk, w) 的条件下测量身份验证所需的延迟,实验结果如图 7 所示。随着域数量的增加,传统的认证方法需要在不同的域之间达成一致,这导致认证时

间呈线性增长,然而,DCIMB 将跨域身份验证委托给域中的任何节点 (IdP),确保了大约恒定的时间复杂度。

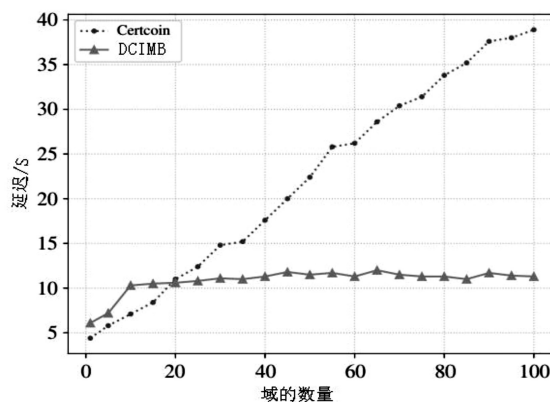


图7 不同域数量下的认证延迟

对于跨域认证的性能,还有两个重要的指标:

- (1) 重复跨域认证的延迟,随着身份数量的增加而增加;
- (2) 重复跨域认证的延迟。

该文使用 Docker 生成 15、20、25、30 个不同的信任域,测试每个域中不同证书标识号下的认证延迟变化趋势,实验结果如图 8 所示。从图 8 可以看出,无论信任域数量是多少,随着身份号的增加,DCIMB 的延迟总是增长非常缓慢。这是因为该文引入了单向累加器作为身份验证的数据结构,DCIMB 可以通过单向累加器判断身份数据是否存在于有效集合中,且时间复杂度接近常量,随着信任域的增加,DCIMB 的认证延迟总是保持在 10 秒之内,然而, Certcoin 最坏情况下的延迟超过 1 分钟,这在实时性要求较高的情况下是不可接受的。

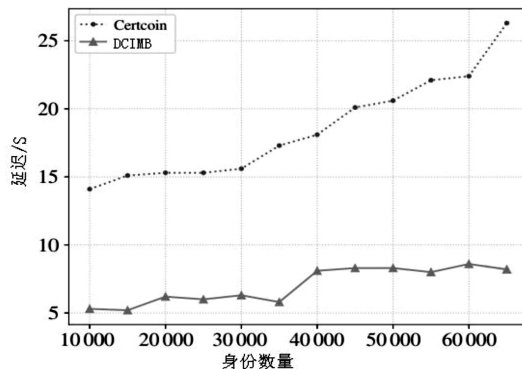


图8 对于15个域,不同数量的身份验证延迟

为了测试重复跨域认证的延迟,该文在系统中生成了 4 万个身份公钥对,并将它们均匀地分布在不同的信任域中,在不同的信任域之间重复执行 30 次认证操作,对应的延迟如图 9 所示。对于传统的基于区块链的认证系统,重复跨域认证所需的时间比 DCIMB 更差,第一次认证后,DCIMB 获得了身份证书,其他域

的 IdP 会缓存该证书的有效性,因此,DCIMB 支持快速身份验证,而不必每次都检索存储节点。

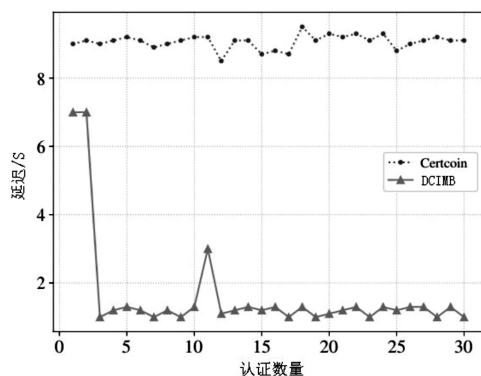


图9 30次重复认证操作后的认证延迟

4 结束语

传统的集中式认证系统由于过度依赖中心,容易出现单点故障风险和隐私保护问题,为了解决这些问题,设计了一种基于区块链的去中心化跨域身份管理系统(DCIMB),并对系统性能进行了评估,证明了该系统的可扩展性和跨域认证效率得到了有效提高。

参考文献:

- [1] LOHACHAB A, KARAMBIR B. Critical analysis of DDoS—an emerging security threat over IoT networks[J]. Journal of Communications and Information Networks, 2018, 3(3): 57–78.
- [2] KARAARSLAN E, ADIGUZEL E. Blockchain based DNS and PKI solutions[J]. IEEE Communications Standards Magazine, 2018, 2(3): 52–57.
- [3] HAKAK S, KHAN W Z, GILKAR G A, et al. Securing smart cities through blockchain technology: architecture, requirements, and challenges[J]. IEEE Network, 2020, 34(1): 8–14.
- [4] 左碧露. 基于区块链和雾计算的物联网设备认证方案研究[D]. 西安: 西安理工大学, 2021.
- [5] 徐君泽. 基于智能合约的融资租赁系统关键性技术研究[D]. 南京: 南京邮电大学, 2021.
- [6] 江 淳. 基于区块链的远程医疗跨域认证系统[D]. 南京: 南京邮电大学, 2021.
- [7] 王琳杰. 物联网数据安全及跨域认证模型研究[D]. 贵州: 贵州大学, 2021.
- [8] 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[J]. 计算机系统应用, 2022, 31(3): 178–187.
- [9] 徐娟娟. 云环境下基于密算的异构跨域身份认证方案[D]. 桂林: 桂林电子科技大学, 2021.
- [10] 王国安. 面向知识共享的跨域访问控制技术研究[与实现[D]. 成都: 电子科技大学, 2021.
- [11] WILSON Y, HINGNIKAR A. Solving identity management in modern applications: demystifying OAuth 2.0, OpenID Connect, and SAML 2.0[M]. New York: Apress, 2019.
- [12] XU L, LI J, CHEN X, et al. Tc-PEDCKS: towards time controlled public key encryption with delegatable conjunctive keyword search for Internet of Things[J]. Journal of Network and Computer Applications, 2019, 128: 11–20.
- [13] NAYAK S, NARENDRA N C, SHUKLA A, et al. Saranyu: using smart contracts and blockchain for cloud tenant management[C]//2018 IEEE 11th international conference on cloud computing (CLOUD). Yokohama: IEEE, 2018: 857–861.
- [14] PAVITHRAN D, AL-KARAKI J N, SHAALAN K. Edge-based blockchain architecture for event-driven iot using hierarchical identity based encryption[J]. Information Processing & Management, 2021, 58(3): 102528.
- [15] BODKHE U, BHATTACHARYA P, TANWAR S, et al. Blo-HoST: blockchain enabled smart tourism and hospitality management[C]//2019 international conference on computer, information and telecommunication systems (CITS). Piscataway: IEEE, 2019: 1–5.
- [16] MOHANTY S N, RAMYA K C, RANI S S, et al. An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy[J]. Future Generation Computer Systems, 2020, 102: 1027–1037.
- [17] HÖLZL M, ROLAND M, MIR O, et al. Disposable dynamic accumulators: toward practical privacy-preserving mobile eIDs with scalable revocation[J]. International Journal of Information Security, 2020, 19(4): 401–417.