文章编号:1671-4598(2021)08-0206-05 DOI:10.16526/j.cnki.11—4762/tp.2021.08.040 中图分类号:TP309;TP393 文献标识码:A

基于区块链和动态累加器的跨域认证方案

张 柯,黄晓芳
(西南科技大学 计算机科学与技术学院,四川 绵阳 621010)

摘要:基于区块链的跨域认证利用区块链代替传统的CA机构颁发区块链证书,借助区块链的去中心化和透明性,实现了信任的去中心化;针对现有基于区块链的跨域认证存在着跨域认证效率不高,没有完整的证书管理功能、区块链存储证书开销大的问题,提出了基于区块链和动态累加器的跨域认证方案,设计了区块链证书格式,描述了跨域认证协议,将区块链证书信息映射为累加值,提升了验证效率,通过在智能合约中构建动态累加器,实现证书的注册,撤销和查询功能;实验结果表明,该方案能够有效降低区块链证书存储成本,提升跨域认证效率。

关键词:区块链;跨域认证;动态累加器;智能合约

Cross—domain Authentication Scheme Based on Blockchain and Dynamic Accumulator

ZHANG Ke, HUANG Xiaofang
(College of Computer Science and Technology, Southwest University of Science and Technology, Mianyang 621010, China)

Abstract: Cross—domain authentication based on blockchain uses blockchain to replace traditional CA institutions to issue blockchain certificates, and with the help of the decentralization and transparency of blockchains, the decentralization of trust is realized. In view of the existing cross—domain authentication based on blockchain, the efficiency of cross—domain authentication is not high, there is no complete certificate management function, and the blockchain storage certificate is expensive. A cross—domain based on blockchain and dynamic accumulator is proposed. In the authentication scheme, the blockchain certificate format is designed, the cross—domain authentication protocol is described, the blockchain certificate information is mapped to the accumulated value, and the verification efficiency is improved. By constructing a dynamic accumulator in the smart contract, the registration and revocation of the certificate and query function are realized. Experimental results show that this scheme can effectively reduce the cost of blockchain certificate storage and improve the efficiency of cross—domain authentication.

Keywords: blockchain; cross—domain authentication; dynamic accumulators; smart contract

0 引言

随着互联网和数字经济的飞速发展,服务数字化的程度也在不断提高。例如,人们经常使用电子商务、在线支付、在线政务等,这些都需要可靠的安全机制进行保障,公钥基础设施(PKI, public key infrastructure)[1-2]利用公钥技术和数字证书提供服务,能够为用户在开放环境中进行安全的通讯提供保障。现有的证书颁发机构(CA, certificate authority)其公钥基础设施可能使用不同的密钥体系,不同的安全和认证策略,导致需要各自维护自己的信任域[3],当单个信任域提供的服务无法满足用户的需求,用户需要进行跨域访问,由此出现跨域认证问题。如何消除信任孤岛,打通信任体系,实现各CA之间证书的互认互通是亟需解决的问题。

国内外已经有大量的学者针对跨域认证进行了相关研究,并取得了一些成果,提出了一系列跨域认证模型。文献[4]提出了PKI域间认证模型,包括层次模型,网状模型和桥CA模型等,但建立桥CA存在实际困难。颜海龙等人[5]提出了CA互信互认标准体系框架,制定了多CA兼容的数字证书格式,将现有的数字证书格式规范化。彭博等人[6]利用桥CA实现不同CA的交叉认证,利用层次模型实现桥CA的互信,从理论上构建了跨域认证模型。以上研究成果表明,CA跨域认证仍然存在诸多问题有待解决。

区块链作为驱动比特币的底层技术,其具有去中心化,防篡改,透明化的特性。其本质是一个分布式不可篡改的账本,底层依靠共识机制,点对点传输,加密算法等组合

收稿日期:2021-01-12; **修回日期**:2021-02-20。
基金项目:国家自然科学基金青年基金资助项目(61702429);四川省组织部基金资助项目(17sjjg02);四川省教育厅基金资助项目(17zd1119);四川省军民融合研究院基金资助项目(18sxb022);四川省科技厅重点研发项目(21ZDYF3119)。
作者简介:张 柯(1995-),男,四川德阳人,硕士,主要从事区块链、信息安全和数字签名方向的研究。
黄晓芳(1977-),女,四川广汉人,博士,教授,硕导,主要从事密码学、区块链和数字签名方向的研究。
引用格式:张 柯,黄晓芳.基于区块链和动态累加器的跨域认证方案[J].计算机测量与控制,2021,29(8):206-210.

而成。区块链是按照时间顺序将数据以一定的方式进行组合并形成的链式结构，将用户的身份信息存入区块链中，能够确保数据的安全和非法篡改。W. Wang 等人[7]首次提出了基于区块链的跨域认证模型，随着区块链的数据量不断增大，存在着用户跨域认证效率不高的问题，周致成等人[8]等针对传统 PKI 跨域认证方案的效率问题，通过与区块链技术相结合，提出了基于区块链的跨域认证方案，减少了签名与验证的次数，提升了跨域认证的效率，但用户仍然需要申请对应信任域证书，产生额外的证书开销，同时撤销需要多次操作区块链，效率不高。为了提升异构域的认证效率，马晓婷等人[9]提出了一种基于区块链技术的跨异构域认证方案，实现了 PKI 域和 IBC 域之间高效安全的通讯，简化了重认证过程，降低了用户端计算量。黄穗等人[10]针对区块链跨域认证效率低的问题，提出了利用布谷鸟过滤器提升证书的查询效率，但其存在着误删的情况，难以适应重要场合的跨域认证场景。

针对以上问题，本文提出了基于区块链和动态累加器的跨域认证方案，通过将不同的 CA 加入到区块链中作为分布式信任中心，消除了传统 CA 中心化信任的弊端。通过利用智能合约构造动态累加器，避免了传统区块链跨域认证中证书的操作难题，提升了跨域认证效率，减少证书存储开销，实现证书的高效查询、注册和撤销操作。

1　相关技术

1.1　区块链技术

区块链是一种去中心化的分布式不可篡改账本[11]，将数据按照时间先后顺序组合而成的块链式结构，依托密码学方式保证区块链的防篡改和不可伪造，通过共识机制将数据写入到区块链中，保证数据的一致性，利用智能合约进行数据的处理，能够在不安全的环境中进行可靠的信息交换，实现不同实体之间的信任传递[12]。

智能合约[13]是具有自动执行协议能力的计算机协议，合约包含可执行的代码和数据两部分，允许用户通过智能合约对区块链的数据进行相关的操作并对用户的输入和输出结果做出响应。比特币（BTC，Bitcoin）中的智能合约使用依靠的是 UTXO（unspent transaction outputs）模型，但合约功能有限，只能实现交易功能。以太坊依靠以太坊虚拟机（EVM，Ethereum virtual machine）运行智能合约，通过合约地址进行智能合约的调用与执行，消耗 GAS 作为智能合约执行成本。超级账本（Hyperledger）中链码（Chaincode）支持多种语言，其被编译成一个独立的应用程序，运行于隔离的 Docker 容器中。

通过将区块链跨域认证协议和密码累加器机制结合，利用智能合约构造出动态累加器，将区块链证书指纹存入动态累加器中，各节点通过共识机制将数据写入到区块链账本中，能够降低证书存储成本。

1.2　动态累加器

密码学累加器[14]最早是由 Josh Benaloh 和 Michael de Mare 提出的，它能够对一组元素进行绑定操作，并能够对集合中的任何元素提供简短的成员关系或者非成员关系证明。相较于其他累加器，动态累加器[15-16]能够实现添加或移除成员时间复杂度不会随着累加器中成员的数量增加而增加，其时间复杂度为 O（1）[16]，具有高效的成员添加和删除效率。Wang P 等人[17]给出了动态累加器的定义，下面给出动态累加器的形式化描述。

Key Gen（k，M）：为了实例化参数而执行的概率算法，将安全参数 k 和上限 M 作为入参，将累加器参数 $P=(P_u, P_r)$ 作为返回结果，其中 P_u 表示累加器的公钥，P_r 表示累加器的私钥。

Acc Val（L，P）：用于计算累加值的概率算法，通过入参 P 和一组元素 $L=\{c_1, c_2, \ldots, c_m\}$（$1<m\leqslant M$）返回累加值 v 以及附加信息 a_c 和 A_l。

Wit Gen（a_c，A_l，P）：见证生成算法，为每一个元素创建成员见证的概率算法。输入 a_c、A_l 和参数 P，输出对于每一个 c_i（$i=1, 2, \ldots, m$）的见证值。

Verify（c，W，v，P_u）：验证算法，用来验证给定的值是否为成员身份的确定性算法。输入元素 c、证据 W、累加值 v 和公钥 P_u，通过证据 W 来验证 c 是否被累计入 v，返回 YES 或者 NO。

AddEle（L^+，a_c，v，P）：向累加器中添加新的成员值并生成新的累加值，将 $L^+=\{c_1^+, c_2^+, \ldots, c_i^+\}$（$L^+\subset C$，$1\leqslant i\leqslant M-m$），辅助信息 a_c 和累加值 v 作为入参和集合 $L^+\cup L$ 保持一致，将证据 $\{W_1^+, W_2^+, \ldots, W_i^+\}$ 返回，同时更新辅助信息 a_c 和 a_u。

Del Ele（L^+，a_c，v，P）：从累加值中删除某些元素的概率算法，将表示为待删除的元素 $L^-=\{c_1^-, c_2^-, \ldots, c_i^-\}$（$L^-\subset L$，$1\leqslant i\leqslant M-m$），辅助信息 a_c，累加值 v 和参数 P 作为入参，返回新的累加值 v' 保持和集合 $L\setminus L^-$ 一致，更新辅助信息 a_c 和 a_u。

UpdateWit（W_i，a_u，P_u）：用于对集合 L 进行添加或者删除操作后，更新累加在 v 和 v' 中的证据，将证据 W_i，辅助信息 a_u 和公钥 P_u 作为入参，返回更新后的见证 W'_i，用来证明元素 c_i 已经被累加在新的累加值 v' 中。

2　基于区块链和动态累加器跨域认证方案

本文采用区块链 3 种类型之一的联盟链，其具有拓展性强和共识速度快等特点，适合跨域认证场景下大规模认证操作，链上各 CA 节点需要经过授权才能够加入，CA 节点作为各个信任域的根信任节点，主要作用是负责验证用户身份的真实性和颁发区块链证书，同时接受跨域认证用户的请求，生成区块链跨域认证证书。区块链账本数据无需中心化的可信中心，通过多个 CA 节点共同维护，写入账本的数据需要大多数节点的同意，区块链上的数据是公开透明的，避免了传统基于 PKI 的数字证书存在的中心化信任和透明度缺失的问题。针对不同 CA 下用户跨域认

证问题，通过与区块链技术结合，形成统一的区块链证书，解决了传统跨域认证中存在的证书路径复杂，交叉互信难，单点故障问题。利用区块链将各 CA 形成统一的信任联盟，使得用户持有的区块链证书在不同信任域中得到认可，消除信任孤岛，提升跨域认证的效率，降低证书的管理成本。通过引入动态累加器提高身份认证的效率，降低节点的存储开销。本章主要设计了区块链证书模型和跨域认证协议。

2.1 区块链证书

区块链证书相较于传统的数字证书[2]，减少了签名模块部分，减轻了 CA 节点计算验证的压力。同时为了满足动态累加器的需求，在文献［7］提出的区块链证书基础上引入了当前累加值到区块链证书中。本文设计的区块链证书如图 1 所示。

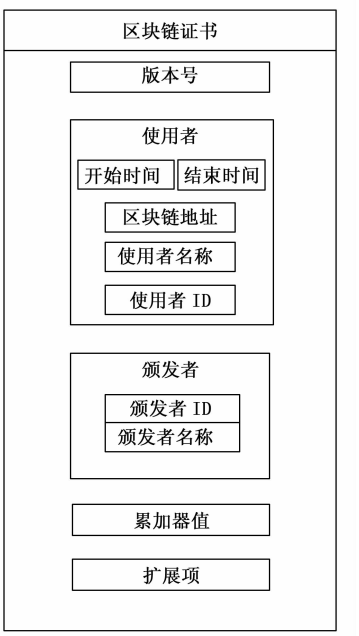

图 1 区块链证书

2.2 协议设计

传统的基于区块链的跨域认证模型[7]需要对区块链进行查询操作，随着区块链数据的增加，查询耗时会线性增长，针对跨域认证中高并发的场景下，现有的方案无法进行高效的查询和插入操作的问题，结合密码学累加器，设计基于区块链和累加器的跨域认证流程，认证流程如图 2 所示。

1）$U_A \rightarrow BCA_B$：用户 U_A 向 CA_B 发送区块链跨域认证请求。

2）$BCA_B \rightarrow U_A$：$\{R_1\}$：CA_B 节点收到请求响应后，将生成的随机数 R_1 发送给 U_A。

3）$U_A \rightarrow BCA_B$：$\{BCert_A, Sign_{priU_A}(R_1), R_1\}$：$U_A$ 将自己的区块链证书和 CA_B 传递过来的 R_1 进行签名值以及 R_1 返回给 CA_B。

4）$BCA_B \rightarrow BCA_A$：$\{GetCertCA_A, R_2\}$：CA_B 通过证书验证签名值是否有效，检查 $BCert_A$ 是否过期，根据证书中的颁发者向 CA_A 节点请求获得 CA_A 根节点区块链证书和随机数 R_2。

5）$BCA_A \rightarrow BCA_B$：$\{BCert_{CA_A}, R_2\}$：CA_A 节点收到来自 CA_B 节点的请求后，返回给 CA_B 自己的证书和随机数 R_2。

6）$BC \rightarrow BCA_B$：$\{Bcert_{A,CA_B}\}$：将生成的跨域证书 $BCert_{A,CA_B}$ 发送给 CA_B 并将生成的哈希值通过节点之间的共识算法写入到区块链中。

7）$BCA_B \rightarrow U_A$：$\{Bcert_{A,CA_B}\}$：CA_B 将跨域证书 $BCert_{A,CA_B}$ 发送 U_A，完成 U_A 和 CA_B 之间的跨域认证。

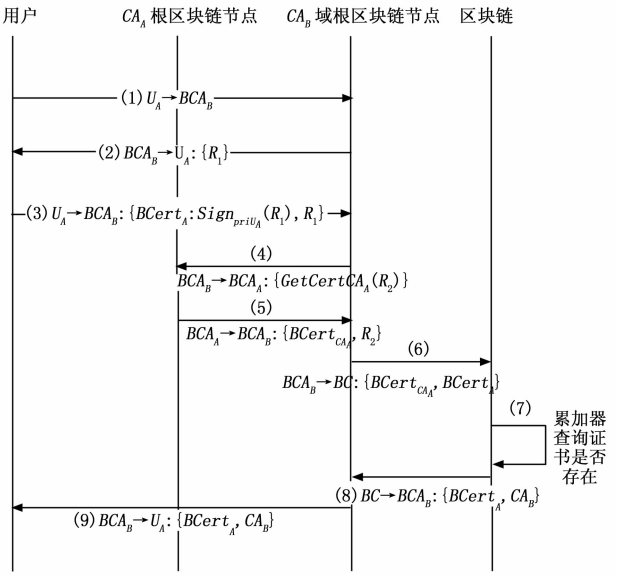

图 2 跨域认证流程

3 关键智能合约设计

传统区块链查询数据的方式需要遍历整个区块链，随着区块链的体积不断增大，查询效率会变得低下。本文通过利用智能合约构造动态累加器，将遍历区块链中数据的方式替换为证明成员在累加器中，使得查询的时间复杂度从 $O(n)$ 能够降低至 $O(1)$，降低了查询耗时，提升了跨域认证的效率。

本章主要描述了基于 Hyperledger Fabric 进行基于智能合约实现动态累加器的区块链证书成员添加，区块链证书成员证明，区块链证书成员删除的链码实现。

3.1 区块链跨域证书添加

当节点成功验证用户身份后，从区块链账本中读取当前累加器对象，通过用户提交的证书信息生成区块链证书，并通过 $sha256(cert)$ 生成证书的指纹和随机数 n，使得 $mem=H(sha256(cert), n)$ 满足裴蜀定理，动态累加器首先通过成员搜索函数 verifyMembership 验证当前待添加的证书是否已经存在，若未存在则动态累加器 acc 通过

proveMembership 计算并生成新的累加值 *accValue* 和用户身份信息对应见证 *witness*。算法描述如算法 1 所示：

算法 1：区块链跨域证书添加

1)Input：ctx,certValue

2)Output：accVaule,witness

3)ChaincodeStub stub = ctx.getStub();

4) byte[] ojectBytes = stub.getState(Accumulator.class.getSimpleName());

5)Accumulator acc = deserialize(ojectBytes);

6)Integer mem = H(sha256(cert),n)

7)witness1=acc.proveMembership(sha256(cert,n));

8)return accVaule,witness;

3.2 区块链跨域证书验证

用户将区块链证书 *cert*、见证值 *witness*、当前证书累加值 *value* 传递给节点，节点读取账本的数据，反序列化动态累加器对象，通过传入的 *cert*，*n*，生成区块链成员对象 *mem* 用来验证区块链证书是否在累加器中，若验证通过返回 true，验证不通过返回 false。其中 *value* 表示当前累加器值，*mem* 表示证书成员指纹，*n* 表示随机数由区块链证书添加时生成，*witness* 表示通过累加器生成的见证值。算法描述如算法 2 所示：

算法 2：区块链跨域证书成员验证

1)Input：ctx,value,mem,witness

2)Output：验证响应 success/false

3)ChaincodeStub stub = ctx.getStub();

4) byte[] ojectBytes = stub.getState(Accumulator.class.getSimpleName());

5)Accumulator acc = deserialize(ojectBytes);

6)boolean verifyPass = acc.verifyMembership(value, mem,n, witness, acc.getN());

7)if(witness.modPow(mem,acc.getN()).comparteTo(A)==0){

8)return true;

9)}

10)return false;

3.3 区块链证书删除

首先从区块链账本中获取当前动态累加器对象，通过算法 2 验证区块链证书是否在累加器中，若验证通过，从累加器中去掉该成员后重新计算累加器的值，返回删除区块链证书成员操成功响应当前并通过区块链节点共识将累加器写入到账本中，若验证失败则返回删除成员失败，终止操作。

算法 3：区块链证书删除

1)Input:ctx,mem

2)Output：删除响应 success/false

3)ChaincodeStub stub = ctx.getStub();

4) byte[] ojectBytes = stub.getState(Accumulator.class.getSimpleName())

5)Accumuldator acc = deserialize(ojectBytes);

6)BigInteger product = BigInteger.ONE;

7)for(BigInteger cert:certs){

8)product =product.multiply(H(sha256(cert),cert.getNonce())

9)}

10)acc.value = acc.value.modPow(product,acc.getN())

11)return acc.value;

4 安全性分析及实验

4.1 安全性分析

4.1.1 证书存储安全性

将区块链证书经过 $Hash\ (bcer) = m$ 后存储在区块链上，*Hash* 函数的单向性保证了攻击者无法通过 m 反推 *cert*，通过 *Hash* 的抗碰撞性能够保证选择任意的区块链证书 $bcert_1$ 和 $bert_2$，使得 $Hash\ (bcert_1) = bcert_2$ 是计算上不可行的。

4.1.2 累加器安全性

本文的动态累加器基于强 RSA 假设，在该假设下寻找满足条件的 $f\ (w,\ m) = w^m\ mod\ n$ 的问题是多项式时间内难解的。如果存在攻击者 C 能够找到一组 $v = f\ (x,\ y)$，使得 $v = f\ (x,\ y) = w^m\ mod n$，其中 n 是由两个大素数产生，那么强 RSA 假设不成立。因此在强 RSA 假设下，给定 v，m，找到一个 w 使得 $v = f\ (x,\ y)$ 是困难的，所以动态累加器 $f\ (w,\ m) = w^m\ mod\ n$ 是一个安全的累加器。

4.1.3 非法跨域认证安全性分析

跨域认证中存在着非授权的跨域认证等安全性问题。因此，为了防止非授权用户进行跨域认证，在跨域认证中，用户与目标节点会通过挑战－应答方式验证用户身份的合法性，目标节点会校验用户提供的证书和源跨域 CA 节点进行比对，确保需要验证的随机数和目标节点保存的随机数一致，确保用户的证书由源节点签发的同时起到了防止重放攻击的效果，同时在区块链证书的拓展项中加入节点白名单，只有当跨域认证用户的区块链证书里包含了目标节点的唯一 ID，用户才能够与目标节点进行跨域认证操作，从而杜绝了用户非法进行跨域认证操作的可能。

4.2 实验

4.2.1 实验环境

实验开发环境为 AMD Ryzen 5 2600X 3.60 GHz CPU 和 24 GB 内存的 PC 机。利用 VMware Workstation Pro 10.0.177 63 创建虚拟机，并在虚拟机中通过 Docker 创建节点，为每个 peer 节点分配 1 G 内存和 10 G 存储空间。Hyperledger Fabric 版本为 2.2.0，链码使用 Java 1.8 开发，Docker 版本为 19.03.13。

4.2.2 实验比较

实验开始前，先批量创建区块链跨域证书 3000 条作为测试数据集，其中 RSA 动态累加器模数是一个长度为1 024 的正整数，是由两个通过 Miller－Rabin 素性检测算法生成和的乘积。为了避免偶发性误差，将实验重复进行 5 次计

算平均值。图 3 表示查询 50，100，150，200 张证书的平均耗时。表 1 表示不同文献中的优缺点比较。图 4 表示不同方法在区块链上的存储成本比较。

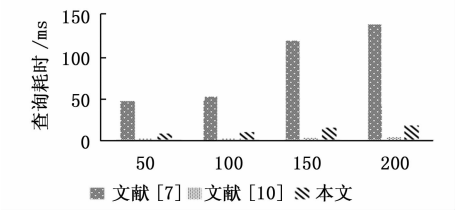

图 3 证书查询平均耗时

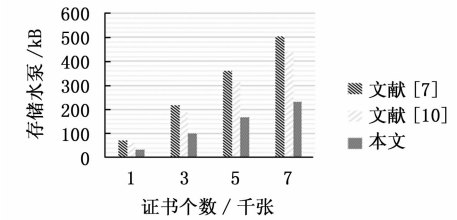

图 4 证书存储成本对比

通过证书查询平均耗时看出，文献 [7] 的查询耗时随着证书的个数增长而线性增长，本文的耗时随着证书数量的增加波动不大，并且查询 10 000 张证书耗时仍然为 1 秒左右，能够满足批量跨域认证应用场景，虽然查询速度落后于文献 [10]，但文献 [10] 存在着 3%的误判概率，这在一些重要的身份认证场景是难以忽略的。同时，本文的证书存储相较于其他方法，存储的消耗约为其他方法的一半，随着区块链数据的增加，能够进一步降低区块链证书数据存储的成本。综上所述，本文将区块链和动态累加器相结合，在避免误判的前提下，提升了跨域认证的效率，降低了证书的存储成本。实现结果表明，该方法具备一定的有效性和可行性。

表 1 文献优缺点比较

文献	证书管理	无误判
文献[7]	否	是
文献[10]	是	否
本文	是	是

5 结束语

本文首先阐述了区块链技术、动态累加器的相关知识。针对传统的区块链跨域身份认证存在的证书查询效率低下，重认证耗时长的问题。提出了基于区块链和动态累加器的跨域认证方案，通过在智能合约中生成动态累加器，利用动态累加器的高效可验证特性和成员元素支持动态添加和删除的特点，构造包含累加值的区块链跨域证书，将证书的指纹作为成员值写入到累加器中，通过区块链共识机制共同维护累加器状态，提升了链上数据庞大时的查询效率，降低了证书存储开销。通过实验数据进行分析比较，结果表明，该方法能够有效提升跨域认证效率，降低证书链上存储成本。

参考文献：

[1] 盛伟瑜. 基于 PKI 的统一信任管理平台设计与实现 [J]. 信息系统工程，2018 (4)：75－76.

[2] 肖 凌，李之棠. 公开密钥基础设施 (PKI) 结构 [J]. 计算机工程与应用，2002，38 (10)：137－139.

[3] 董贵山，陈宇翔，李洪伟，等. 异构环境中基于区块链的跨域认证可信度研究 [J]. 通信技术，2019 (6)：1450－1460.

[4] LINN J. Trust models and management in public－key infrastructures [J]. RSA Laboratories，2000，12.

[5] 颜海龙，闫 巧，冯纪强，等. 基于 PKI/cA 互信互认体系的电子政务 [J]. 深圳大学学报：理工版，2012，29 (2)：113－117.

[6] 彭 博，刘 进，龚 智，等. 一种树型桥 CA 跨域信任传递模型研究 [J]. 舰船电子工程，2017，37 (3)：66－69.

[7] WANG W，HU N，LIU X. BlockCAM：A blockchain－based cross－domain authentication model [C] //2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)，2018：896－901.

[8] 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 [J]. 计算机应用，2018，38 (2)：316－320.

[9] 马晓婷，马文平，刘小雪. 基于区块链技术的跨域认证方案 [J]. 电子学报，2018，46 (11)：2571－2579.

[10] 黄 穗，李 健，范冰冰. IABC：一种基于区块链和布谷鸟过滤器的跨域认证方法 [J]. 小型微型计算机系统，2020，41 (12)：2620－2625.

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

[12] 唐晓华，余益民，陈韬伟，等. 浅析基于区块链技术的跨域认证方案 [J]. 网络安全技术与应用，2019 (9)：22－25.

[13] ZHANG Y，KASAHARA S，SHEN Y，et al. Smart contract－based access control for the internet of things [J]. IEEE Internet of Things Journal，2018，6 (2)：1594－1605.

[14] BENALOH J，DE Mare M. One－way accumulators：A decentralized alternative to digital signatures [C] //Workshop on the Theory and Application of of Cryptographic Techniques，1993：274－285.

[15] 汤凌韬，许 敏，金玉荣. 基于区块链的身份认证机制的效率优化方法研究 [J]. 计算机应用研究，2019 (10)：2783－2787.

[16] 张 琰，王瑾璠，齐竹云，等. 基于动态累加器的去中心化加密搜索方案 [J]. 网络与信息安全学报，2019，5 (2)：23－29.

[17] WANG P，WANG H，PIEPRZYK J. A new dynamic accumulator for batch updates [C] //International Conference on Information and Communications Security，2007：98－112.