(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118381663 A
(43)申请公布日 2024.07.23

(21)申请号 202410806278.1

(22)申请日 2024.06.21

(71)申请人 中国科学技术大学
地址 230026 安徽省合肥市包河区金寨路96号

(72)发明人 王峰 张烨 艾明瑞 罗昕怡 薛开平

(74)专利代理机构 北京科迪生专利代理有限责任公司 11251
专利代理师 江亚平

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)
H04L 9/00(2022.01)
G06Q 50/20(2012.01)

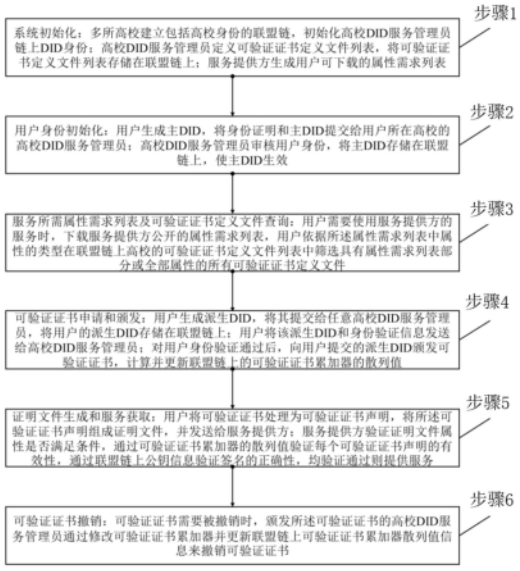
权利要求书5页 说明书8页 附图1页

(54)发明名称

一种基于区块链和DID的高校联盟用户身份管理方法

(57)摘要

本发明公开了一种基于区块链和DID的高校联盟用户身份管理方法,属于区块链应用技术领域。所述方法包括,多所高校组成身份联盟链,用于维护所有用户的DID身份;高校通过向用户颁发可验证证书的方式证明用户拥有某些属性;用户需要使用某些服务提供方的服务时,通过多个可验证证书组合的方式证明拥有相应的属性;其中,用户在申请不同可验证证书时使用不同的派生DID。所述方法可以有效的对基于联盟链建立的高校联盟提供全局身份管理,并基于可验证证书实现身份认证、细粒度的服务授权。



CN 118381663 A

1.一种基于区块链和DID的高校联盟用户身份管理方法,其特征在于,所述方法包括如下步骤:

步骤1、系统初始化:多所高校建立包括高校身份的联盟链,初始化高校DID服务管理员联盟链上DID身份;高校DID服务管理员定义可验证证书定义文件列表,将可验证证书定义文件列表存储在联盟链上;服务提供方生成用户可下载的属性需求列表;

步骤2、用户身份初始化:用户生成主DID,将身份验证信息和主DID提交给用户所在高校的高校DID服务管理员;高校DID服务管理员审核用户身份,将主DID存储在联盟链上,使主DID生效;

步骤3、服务所需属性需求列表及可验证证书定义文件查询:用户需要使用服务提供方的服务时,下载服务提供方公开的属性需求列表,用户依据所述属性需求列表中属性的类型在联盟链上高校的可验证证书定义文件列表中筛选具有属性需求列表部分或全部属性的所有可验证证书定义文件;

步骤4、可验证证书申请和颁发:用户生成派生DID,将其提交给任意高校DID服务管理员,所述任意高校DID服务管理员验证签名后将用户的派生DID存储在联盟链上;用户将该派生DID和身份验证信息发送给所述可验证证书定义文件所属高校的高校DID服务管理员;所述可验证证书定义文件所属高校的高校DID服务管理员对用户的身份验证通过后,向用户提交的派生DID颁发可验证证书,计算并更新存储在联盟链上的可验证证书累加器的散列值;

步骤5、证明文件生成和服务获取:用户将可验证证书处理为可验证证书声明,将所述可验证证书声明组成证明文件,并发送给服务提供方;服务提供方验证证明文件属性是否满足条件,通过联盟链上可验证证书累加器的散列值验证每个可验证证书声明的有效性,通过联盟链上公钥信息验证每个可验证证书声明对应的高校DID服务管理员的私钥签名和派生DID的私钥签名的正确性,均验证通过则提供服务;

步骤6、可验证证书撤销:可验证证书需要被撤销时,颁发所述可验证证书的高校DID服务管理员通过修改可验证证书累加器并更新联盟链上可验证证书累加器的散列值来撤销可验证证书。

2.根据权利要求1所述的一种基于区块链和DID的高校联盟用户身份管理方法,其特征在于,所述步骤1包括:

步骤1.1,n所高校提供管理节点共同构成高校身份联盟链,每所高校设置各自的高校DID服务管理员,联盟链上记录所述n所高校DID服务管理员的DID身份DID_{U_i}及公钥PK_{U_i},U_i代表第i所高校;

步骤1.2,第i所高校U_i的高校DID服务管理员生成第一可验证证书定义文件列表$\{VCDef_{i1},\ldots,VCDef_{im}\}$,$VCDef_{i1}$表示第i所高校$U_i$的第1张可验证证书定义文件,$VCDef_{im}$表示第i所高校$U_i$的第m张可验证证书定义文件,第i所高校$U_i$的第j张可验证证书定义文件$VCDef_{ij}$包含第i所高校$U_i$的第j张可验证证书定义文件$VCDef_{ij}$的公钥$PK_{VC_{ij}}$和可验证证书累加器的散列值$H(ACCUM_{ij})$,第一可验证证书属性列表$\{A_{ij_1},\ldots,A_{ij_s}\}$,该可验证证书属性列

表包括s个元素，A_{ij_1}代表第一可验证证书属性列表的第一个可验证证书属性，A_{ij_s}代表第一可验证证书属性列表的第s个可验证证书属性，将所述可验证证书定义文件列表中的所有文件分别使用第i所高校U_i的私钥SK_{U_i}签名后上联盟链存储；

步骤1.3，服务提供方SP_k生成用户可下载的属性需求列表$\{R_{k_1}:v_{k_1},...,R_{k_h}:v_{k_h}\}$，该属性需求列表中有h个键值对，$R_{k_1}$表示第1个属性，$v_{k_1}$表示满足属性$R_{k_1}$的属性值空间，$R_{k_h}$表示第h个属性，$v_{k_h}$表示满足属性$R_{k_h}$的属性值空间。

3.根据权利要求1所述的一种基于区块链和DID的高校联盟用户身份管理方法，其特征在于，所述步骤2包括：

步骤2.1，第i所高校U_i的第t个用户P_{it}生成主DID身份$DID_{P_{it}}$、用户公私钥对$(PK_{P_{it}},SK_{P_{it}})$，用户将主DID身份$DID_{P_{it}}$，用户公钥$PK_{P_{it}}$，身份验证信息发送给第i所高校$U_i$的高校DID服务管理员，请求完成主DID初始化；

步骤2.2，第i所高校U_i的高校DID服务管理员接收用户的主DID初始化请求后，验证第i所高校U_i的第t个用户P_{it}的身份验证信息，将$(DID_{P_{it}},PK_{P_{it}},DID_{U_i},sig(SK_{U_i},H(DID_{P_{it}}\|PK_{P_{it}}\|DID_{U_i})))$存储在联盟链上，使第i所高校$U_i$的第t个用户$P_{ij}$的主DID生效，$sig(SK_{U_i},H(DID_{P_{it}}\|PK_{P_{it}}\|DID_{U_i}))$代表使用第i所高校$U_i$的私钥$SK_{U_i}$对第一散列值$H(DID_{P_{it}}\|PK_{P_{it}}\|DID_{U_i})$进行签名。

4.根据权利要求1所述的一种基于区块链和DID的高校联盟用户身份管理方法，其特征在于，所述步骤3包括：

步骤3.1，第i所高校U_i的第t个用户P_{it}需要使用服务提供方SP_k提供的服务时，下载公开的属性需求列表$\{R_{k_1}:v_{k_1},...,R_{k_h}:v_{k_h}\}$；

步骤3.2，第i所高校U_i的第t个用户P_{it}依据所述属性需求列表中属性的类型在高校的可验证证书定义文件列表中确定第二列表$\{VCDef_{ij},...,VCDef_{nl}\}$，使所述第二列表满足$\{R_{k_1},...,R_{k_h}\}\subseteq\{A_{ij_1},...,A_{ij_s}\}\cup.....\cup\{A_{nl_1},...,A_{nl_q}\}$，$VCDef_{nl}$表示第n个高校上联盟链存储的第1张可验证证书定义文件，含有第二可验证证书属性列表$\{A_{nl_1},...,A_{nl_q}\}$，该列表有q个元素，$A_{nl_1}$代表第二可验证证书属性列表的第一个可验证证书属性，A_{nl_q}代表第二可验证证书属性列表的第q个可验证证书属性。

5.根据权利要求1所述的一种基于区块链和DID的高校联盟用户身份管理方法，其特征在于，所述步骤4包括：

步骤4.1，第i所高校U_i的第t个用户P_{it}生成第u个派生DID DID_{D_u}、公私钥对

$\left(PK_{D_u},SK_{D_u}\right)$,将派生DID注册请求$\left(DID_{D_u},PK_{D_u},DID_{P_{it}},sig\left(SK_{P_{it}},H\left(DID_{D_u}\|PK_{D_u}\|DID_{P_{it}}\right)\right)\right)$发送给任意一所高校$U_p$的高校DID服务管理员;

步骤4.2,任意一所高校U_p的高校DID服务管理员收到派生DID注册请求,校验签名$sig\left(SK_{P_{it}},H\left(DID_{D_u}\|PK_{D_u}\|DID_{P_{it}}\right)\right)$有效后,使用第p所高校$U_p$的高校DID服务管理员的DID身份$DID_{U_p}$对应的私钥$SK_{U_p}$对第二散列值$H\left(DID_{D_u}\|PK_{D_u}\|DID_{U_p}\right)$进行签名,将$\left(DID_{D_u},PK_{D_u},DID_{U_p},sig\left(SK_{U_p},H\left(DID_{D_u}\|PK_{D_u}\|DID_{U_p}\right)\right)\right)$上联盟链存储,使第i所高校$U_i$的第t个用户$P_{it}$的第u个派生DID$DID_{D_u}$生效;

步骤4.3,第i所高校U_i的第t个用户P_{it}将第u个派生DIDDID_{D_u},第i所高校U_i的第j张可验证证书定义文件$VCDef_{ij}$,身份验证信息,发送给第i所高校U_i的高校DID服务管理员,申请第i所高校颁发的第j类可验证证书VC_{ij};

步骤4.4,第i所高校U_i的高校DID服务管理员为第i所高校U_i的第t个用户P_{it}按照第i所高校U_i的第j张可验证证书定义文件$VCDef_{ij}$中第一可验证证书属性列表$\left\{A_{ij_1},\ldots,A_{ij_s}\right\}$填写对应属性值,生成一个大素数$Q$作为序列号,添加到可验证证书累加器$ACCUM_{ij}$中,计算并更新联盟链上可验证证书累加器的散列值$H\left(ACCUM_{ij}\right)$,将属性值和序列号组合成为第i所高校颁发的第j类可验证证书VC_{ij}并发送给第i所高校U_i的第t个用户P_{it}。

6.根据权利要求1所述的一种基于区块链和DID的高校联盟用户身份管理方法,其特征在于,所述步骤5包括:

步骤5.1,第i所高校U_i的第t个用户P_{it}获得与第二列表$\left\{VCDef_{ij},\ldots,VCDef_{nl}\right\}$匹配的可验证证书$VC_{ij},\ldots,VC_{nl}$,$VC_{nl}$表示第n所高校颁发的第l类可验证证书,校验签名有效后,将可验证证书中包含于属性需求列表$\left\{R_{k_1}:v_{k_1},\ldots,R_{k_h}:v_{k_h}\right\}$的属性值以明文展示,其他以明文的散列值展示,成为可验证证书声明文件,分别使用请求可验证证书时的派生DID所对应的私钥对可验证证书声明文件签名,组合成为证明文件$Cred_Proof$发送给服务提供方SP_k;

步骤5.2,服务提供方SP_k接收到证明文件$Cred_Proof$后,检查属性和属性值是否满足属性需求列表$\left\{R_{k_1}:v_{k_1},\ldots,R_{k_h}:v_{k_h}\right\}$,对于证明文件中的每张可验证证书声明文件,分别通过可验证证书累加器信息检查可验证证书声明的有效性,通过联盟链上公钥信息验证每个可验证证书声明对应的高校DID服务管理员的私钥签名和派生DID的私钥签名的正确性,均验证通过则提供服务。

7.根据权利要求2所述的一种基于区块链和DID的高校联盟用户身份管理方法,其特征在于,所述可验证证书累加器工作的具体步骤为:

第i所高校U_i的高校DID服务管理员为第i所高校U_i的第j张可验证证书定义文件$VCDef_{ij}$在本地维护可验证证书累加器$ACCUM_{ij}$,并初始化为随机的大素数$ACCUM_{ij}=P$,之后计算可验证证书累加器的散列值$H\left(ACCUM_{ij}\right)$,并存储在联盟链上;

第i所高校U_i的高校DID服务管理员生成第j类可验证证书VC_{ij}后,随机生成一个大素数Q作为序列号,可验证证书累加器值更新$ACCUM_{ij}=ACCUM_{ij}*Q$,之后计算并更新联盟链上存储的可验证证书累加器的散列值$H\left(ACCUM_{ij}\right)$;

当第i所高校颁发的第j类可验证证书VC_{ij}被撤销时,执行可验证证书累加器更新$ACCUM_{ij}=ACCUM_{ij}/Q$,之后计算并更新联盟链上存储的可验证证书累加器的散列值$H\left(ACCUM_{ij}\right)$;

系统中任意实体验证第i所高校颁发的第j类可验证证书VC_{ij}有效性时,从高校U_i的高校DID服务管理员处获取可验证证书累加器值$ACCUM_{ij}$,计算散列值并和存储在联盟链上的散列值进行对比,一致则验证可验证证书累加器$ACCUM_{ij}$模第i所高校颁发的第j类可验证证书VC_{ij}中的序列号Q的值是否为0,若为0,则该第i所高校U_i颁发的第j类可验证证书VC_{ij}有效。

8.根据权利要求5所述的一种基于区块链和DID的高校联盟用户身份管理方法,其特征在于,所述可验证证书生成的具体步骤为:

第i所高校U_i的高校DID服务管理员为第i所高校U_i的第t个用户P_{it}按照第一可验证证书属性列表填写明文属性值和盐值$\left\{A_{ij_1}:\left\{m_{ij_1},SALT_{ij_1}\right\},\ldots,A_{ij_s}:\left\{m_{ij_s},SALT_{ij_s}\right\}\right\}$,$m_{ij_1}$为第一可验证证书属性列表第一个可验证证书属性$A_{ij_1}$的明文属性值,$SALT_{ij_1}$是为第一可验证证书属性列表第一个可验证证书属性$A_{ij_1}$的明文属性值$m_{ij_1}$生成的随机数盐值,$m_{ij_s}$为第一可验证证书属性列表第s个可验证证书属性$A_{ij_s}$的明文属性值,$SALT_{ij_s}$是为第一可验证证书属性列表第s个可验证证书属性$A_{ij_s}$的明文属性值$m_{ij_s}$生成的随机数盐值,并为该第一可验证证书属性列表的明文属性值生成散列值列表$\left\{H_{ij_1},\ldots,H_{ij_s}\right\}$,其中,散列值列表中的第一个散列值$H_{ij_1}=H(m_{ij_1}\|SALT_{ij_1})$,散列值列表中的第s个散列值$H_{ij_s}=H(m_{ij_s}\|SALT_{ij_s})$;生成一个大素数$Q$作为序列号,添加到可验证证书累加器$ACCUM_{ij}$中,计算并更新联盟链上的可验证证书累加器的散列值$H\left(ACCUM_{ij}\right)$,将生成的可验证证书$VC_{ij}=\left(DID_{D_u},\left\{A_{ij_1}:\left\{m_{ij_1},SALT_{ij_1}\right\},\ldots,A_{ij_s}:\left\{m_{ij_s},SALT_{ij_s}\right\}\right\},Q,sig\left(SK_{VC_{ij}},H\left(DID_{D_u}\|H_{ij_1}\|\ldots\|H_{ij_s}\|Q\right)\right)\right)$发送给第i所高校$U_i$的第t个用户$P_{it}$。

9.根据权利要求6所述的一种基于区块链和DID的高校联盟用户身份管理方法,其特征

在于,所述证明文件$Cred_Proof$形成的具体步骤为:

第i所高校U_i的第t个用户P_{it}获得与第二列表$\{VCDef_{ij},...,VCDef_{nl}\}$匹配的可验证证书$VC_{ij},...,VC_{nl}$,并校验签名有效后,将可验证证书中包含于属性需求列表$\{R_{k_1}:v_{k_1},...,R_{k_h}:v_{k_h}\}$的属性值以明文展示,其他以明文的散列值展示,成为可验证证书声明列表$\{VC'_{ij},...,VC'_{nl}\}$,$VC'_{ij}$表示散列值处理后的第i所高校颁发的第j类可验证证书VC_{ij},VC'_{nl}表述散列值处理后的第n所高校颁发的第l类可验证证书VC_{nl},依次使用请求可验证证书时的第u个派生DID的私钥SK_{D_u},……,第e个派生的私钥SK_{D_e}签名组合成证明文件$Cred_Proof=\left(\left\{VC'_{ij},sig\left(SK_{D_u},H\left(VC'_{ij}\right)\right)\right\},...,\left\{VC'_{nl},sig\left(SK_{D_e},H\left(VC'_{nl}\right)\right)\right\}\right)$,将所述证明文件$Cred_Proof$发送给服务提供方$SP_k$。

一种基于区块链和DID的高校联盟用户身份管理方法

技术领域

[0001] 本发明属于区块链应用技术领域,尤其涉及一种基于区块链和DID的高校联盟用户身份管理方法。

背景技术

[0002] 随着互联网和数字化技术的发展,身份认证技术的作用变得更加重要,可以保护个人和组织的数据安全和隐私;同时,资源互通和信息互认是数字化时代发展的重要趋势,可以促进各行业之间的协同发展和合作。在高校场景下,身份认证和资源互通更为重要,可以保护学生和教师的个人信息和隐私,促进高校之间的协同发展和资源共享。因此,推动高校身份认证和资源互通具有重要的现实价值和战略价值。

[0003] 目前普及的中心化身份认证体系存在一些不足,用户对认证机构或服务提供方的依赖性很高,这意味着用户无法掌控自己的身份信息,无法自主选择认证机构或服务提供方;中心化架构依赖于单一的认证服务器或第三方服务提供方,因此一旦出现单点故障,整个系统都将受到影响;个人在不同的系统建立重复但又不完全相同的身份数据,形成了个人数据的孤岛;同时机构存在对数据不透明使用的问题。一种可行的方法是引入区块链和去中心化的身份管理方法,实现高校场景中的身份认证和信息互通。该方法可以解决中心化身份认证的机构依赖性和数据孤岛问题,高校可以实现跨机构身份管理和数据互通,提高资源服务的复杂性和机构互通的需求,但该方法存在用户隐私信息泄露的风险,即恶意攻击者通过联盟链上的公开信息对用户进行画像,侵犯用户的隐私。可以通过使用派生DID的方法保护用户的隐私信息,但现有技术中缺乏相应的解决方案。

发明内容

[0004] 为解决上述技术问题,本发明提供了一种基于区块链和DID的高校联盟用户身份管理方法,该方法可以有效的对基于联盟链建立的高校联盟提供全局身份管理,并基于可验证证书实现身份认证、细粒度的服务授权,为高校联盟中的用户提供隐私保护、用户自我主权和用户友好的去中心化身份管理方案。

[0005] 为实现上述目的,本发明采用的技术方案如下:

步骤1、系统初始化:多所高校建立包括高校身份的联盟链,初始化高校DID服务管理员联盟链上DID身份;高校DID服务管理员定义可验证证书定义文件列表,将可验证证书定义文件列表存储在联盟链上;服务提供方生成用户可下载的属性需求列表;

步骤2、用户身份初始化:用户生成主DID,将身份验证信息和主DID提交给用户所在高校的高校DID服务管理员;高校DID服务管理员审核用户身份,将主DID存储在联盟链上,使主DID生效;

步骤3、服务所需属性需求列表及可验证证书定义文件查询:用户需要使用服务提供方的服务时,下载服务提供方公开的属性需求列表,用户依据所述属性需求列表中属性的类型在联盟链上高校的可验证证书定义文件列表中筛选具有属性需求列表部分或全部

属性的所有可验证证书定义文件;

步骤4、可验证证书申请和颁发:用户生成派生DID,将其提交给任意高校DID服务管理员,所述任意高校DID服务管理员验证签名后将用户的派生DID存储在联盟链上;用户将该派生DID和身份验证信息发送给所述可验证证书定义文件所属高校的高校DID服务管理员;所述可验证证书定义文件所属高校的高校DID服务管理员对用户的身份验证通过后,向用户提交的派生DID颁发可验证证书,计算并更新存储在联盟链上的可验证证书累加器的散列值;

步骤5、证明文件生成和服务获取:用户将可验证证书处理为可验证证书声明,将所述可验证证书声明组成证明文件,并发送给服务提供方;服务提供方验证证明文件属性是否满足条件,通过联盟链上可验证证书累加器的散列值验证每个可验证证书声明的有效性,通过联盟链上公钥信息验证每个可验证证书声明对应的高校DID服务管理员的私钥签名和派生DID的私钥签名的正确性,均验证通过则提供服务;

步骤6、可验证证书撤销:可验证证书需要被撤销时,颁发所述可验证证书的高校DID服务管理员通过修改可验证证书累加器并更新联盟链上可验证证书累加器的散列值来撤销可验证证书。

[0006] 本发明的有益效果在于:

所述方法可以有效的对基于联盟链建立的高校联盟提供全局身份管理,为联盟链上的不同用户提供隐私保护的身份使用方法,防止通过联盟链上数据对用户进行身份画像;同时使用统一格式的可验证证书实现了不同高校之间的相互认证,并通过选择性披露实现了最小范围的隐私信息使用。

附图说明

[0007] 图1为本发明一种基于区块链和DID的高校联盟用户身份管理方法流程图。

具体实施方式

[0008] 下面结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅是本发明一部分实施例,而不是全部的实施例,这并不构成对本发明的限制。基于本发明的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明的保护范围。

[0009] 如图1所示,为本发明一种基于区块链和DID的高校联盟用户身份管理方法流程图,所述方法包括如下步骤:

步骤1、系统初始化:多所高校建立包括高校身份的联盟链,初始化高校DID服务管理员联盟链上DID身份;高校DID服务管理员定义可验证证书定义文件列表,将可验证证书定义文件列表存储在联盟链上;服务提供方生成用户可下载的属性需求列表;

步骤2、用户身份初始化:用户生成主DID,将身份证明和主DID提交给用户所在高校的高校DID服务管理员;高校DID服务管理员审核用户身份,将主DID存储在联盟链上,使主DID生效;

步骤3、服务所需属性需求列表及可验证证书定义文件查询:用户需要使用服务提供方的服务时,下载服务提供方公开的属性需求列表,用户依据所述属性需求列表中属性

的类型在联盟链上高校的可验证证书定义文件列表中筛选具有属性需求列表部分或全部属性的所有可验证证书定义文件;

步骤4、可验证证书申请和颁发:用户生成派生DID,将其提交给任意高校DID服务管理员,将用户的派生DID存储在联盟链上;用户将该派生DID和身份验证信息发送给高校DID服务管理员;对用户的身份验证通过后,向用户提交的派生DID颁发可验证证书,计算并更新存储在联盟链上的可验证证书累加器的散列值;

步骤5、证明文件生成和服务获取:用户将可验证证书处理为可验证证书声明,将所述可验证证书声明组成证明文件,并发送给服务提供方;服务提供方验证证明文件属性是否满足条件,通过可验证证书累加器的散列值验证每个可验证证书声明的有效性,通过联盟链上公钥信息验证签名的正确性,均验证通过则提供服务;

步骤6、可验证证书撤销:可验证证书需要被撤销时,颁发所述可验证证书的高校DID服务管理员通过修改可验证证书累加器并更新联盟链上可验证证书累加器散列值来撤销可验证证书。

[0010] 实施例

下面根据具体的实施例对本发明作进一步说明。

[0011] 本发明提供的基于区块链和DID的高校联盟用户身份管理方法,所述方法包括如下步骤:

步骤1、系统初始化:多所高校建立包括高校身份的联盟链,初始化高校DID服务管理员联盟链上DID身份;高校DID服务管理员定义可验证证书定义文件列表,将可验证证书定义文件列表存储在联盟链上;服务提供方生成用户可下载的属性需求列表;

步骤1系统初始化具体包含以下步骤:

步骤1.1,n所高校提供管理节点共同构成高校身份联盟链,每所高校设置各自的高校DID服务管理员,联盟链上记录所述n所高校DID服务管理员的DID身份DID_{U_i}及公钥PK_{U_i},U_i代表第i所高校;

具体实现中,高校联盟链是一个许可区块链,各个联盟成员高校通过提供管理节点,定期对各自提交内容进行共识的方式维护数据,提供服务;经过所有高校按比例认证通过后,新的高校可以通过提供管理节点同步数据的方式加入该区块链系统,所述比例由具体实施方设置;

其中,每个高校设置各自的高校DID服务管理员,负责管理所在高校的管理节点,并将需要上链存储的数据提交给管理节点。

[0012] 步骤1.2,第i所高校U_i的高校DID服务管理员生成第一可验证证书定义文件列表$\{VCDef_{i1},\ldots,VCDef_{im}\}$,$VCDef_{i1}$表示第i所高校$U_i$的第1张可验证证书定义文件,$VCDef_{im}$表示第i所高校$U_i$的第m张可验证证书定义文件,第i所高校$U_i$的第j张可验证证书定义文件$VCDef_{ij}$包含第i所高校$U_i$的第j张可验证证书定义文件$VCDef_{ij}$的公钥$PK_{VC_{ij}}$和可验证证书累加器的散列值$H(ACCUM_{ij})$,第一可验证证书属性列表$\{A_{ij_1},\ldots,A_{ij_s}\}$,该可验证证书属性列表包括s个元素,$A_{ij_1}$代表第一可验证证书属性列表的第一个可验证证书属性,A_{ij_s}代表第一可验证证书属性列表的第s个可验证证书属性,将所述可验证证书定义文件列表中的所有

文件分别使用第i所高校U_i的私钥SK_{U_i}签名后上联盟链存储;

所述步骤1.2的证书定义文件初始化的具体过程为:

第i所高校U_i的高校DID服务管理员定义一类证书,具体实现中如学生证或成绩单等;

第i所高校U_i的高校DID服务管理员为第i所高校U_i的第j张可验证证书定义文件$VCDef_{ij}$在本地维护可验证证书累加器$ACCUM_{ij}$,并初始化为随机的大素数$ACCUM_{ij}=P$,之后计算可验证证书累加器的散列值$H\left(ACCUM_{ij}\right)$,并存储在联盟链上;

其中可验证证书定义文件之一的$VCDef_{ij}=\left(\left\{A_{ij_1},\ldots,A_{ij_x}\right\},PK_{VC_{ij}},H\left(ACCUM_{ij}\right),DID_{U_i},Sig\left(SK_{U_i},H\left(\left\{A_{ij_1},\ldots,A_{ij_x}\right\}\|PK_{VC_{ij}}\|H\left(ACCUM_{ij}\right)\|DID_{U_i}\right)\right)\right)$,将所述可验证证书定义文件分别使用$U_i$的私钥$SK_{U_i}$签名后上链存储。

[0013] 步骤1.3,服务提供方SP_k生成用户可下载的属性需求列表$\left\{R_{k_1}:v_{k_1},\ldots,R_{k_h}:v_{k_h}\right\}$,该列表中有h个键值对,$R_{k_1}$表示第1个属性,$v_{k_1}$表示满足属性$R_{k_1}$的属性值空间,$R_{k_h}$表示第h个属性,$v_{k_h}$表示满足属性$R_{k_h}$的属性值空间。

[0014] 具体实现中,服务提供方可以提供类似跨校选课,场馆预约,图书等资源共享的服务,这些服务需要对用户进行身份认证后才能进行提供;对于所需要的属性,服务提供方SP_k生成用户可下载的属性需求列表$\left\{R_{k_1}:v_{k_1},\ldots,R_{k_h}:v_{k_h}\right\}$,具体实现中,如跨校选课中,属性需求列表可以为{高校:{学校A学生证,学校B学生证},总成绩:{良好},预修课程:{课程C,课程D}},服务提供方可以将$\left\{R_{k_1}:v_{k_1},\ldots,R_{k_h}:v_{k_h}\right\}$公布在自己搭建的网页上。

[0015] 步骤2、用户身份初始化:用户生成主DID,将身份验证信息和主DID提交给用户所在高校的高校DID服务管理员;高校DID服务管理员审核用户身份,将主DID存储在联盟链上,使主DID生效;

步骤2具体包含以下步骤:

步骤2.1,第i所高校U_i的第t个用户P_{it}生成主DID身份$DID_{P_{it}}$、用户公私钥对$\left(PK_{P_{it}},SK_{P_{it}}\right)$,用户将主DID身份$DID_{P_{it}}$,用户公钥$PK_{P_{it}}$,身份验证信息发送给第i所高校$U_i$的高校DID服务管理员,请求完成主DID初始化;

步骤2.2,第i所高校U_i的高校DID服务管理员接收用户的主DID初始化请求后,验证第i所高校U_i的第t个用户P_{it}的身份验证信息,将$\left(DID_{P_{it}},PK_{P_{it}},DID_{U_i},sig\left(SK_{U_i},H\left(DID_{P_{it}}\|PK_{P_{it}}\|DID_{U_i}\right)\right)\right)$存储在联盟链上,使第i所高校$U_i$的第t个用户$P_{ij}$的主DID生效,$sig\left(SK_{U_i},H\left(DID_{P_{it}}\|PK_{P_{it}}\|DID_{U_i}\right)\right)$代表使用第i所高校$U_i$的私钥$SK_{U_i}$对第一散列值$H\left(DID_{P_{it}}\|PK_{P_{it}}\|DID_{U_i}\right)$进行签名。

[0016] 在具体实现中用户的身份验证信息由各个高校定义。

[0017] 步骤3、服务所需属性需求列表及可验证证书定义文件查询:用户需要使用服务提供方的服务时,下载服务提供方公开的属性需求列表,用户依据所述属性需求列表中属性的类型在联盟链上高校的可验证证书定义文件列表中筛选具有属性需求列表部分或全部

属性的所有可验证证书定义文件;

步骤3具体包含以下步骤:

步骤3.1,第i所高校U_i的第t个用户P_{it}需要使用服务提供方SP_k提供的服务时,下载公开的属性需求列表$\{R_{k_1}:v_{k_1},\ldots,R_{k_h}:v_{k_h}\}$;

步骤3.2,第i所高校U_i的第t个用户P_{it}依据所述属性需求列表中属性的类型在高校的可验证证书定义文件列表中确定第二列表$\{VCDef_{ij},\ldots,VCDef_{nl}\}$,使所述第二列表满足$\{R_{k_1},\ldots,R_{k_h}\}\subseteq\{A_{ij_1},\ldots,A_{ij_s}\}\cup\ldots\ldots\cup\{A_{nl_1},\ldots,A_{nl_q}\}$,$VCDef_{nl}$表示第n个高校上联盟链存储的第l张可验证证书定义文件,含有第二可验证证书属性列表$\{A_{nl_1},\ldots,A_{nl_q}\}$,该列表有q个元素,$A_{nl_1}$代表第二可验证证书属性列表的第一个可验证证书属性,A_{nl_q}代表第二可验证证书属性列表的第q个可验证证书属性。

[0018] 步骤4、可验证证书申请和颁发:用户生成派生DID,将其提交给任意高校DID服务管理员,所述任意高校DID服务管理员验证签名后将用户的派生DID存储在联盟链上;用户将该派生DID和身份验证信息发送给所述可验证证书定义文件所属高校的高校DID服务管理员;所述可验证证书定义文件所属高校的高校DID服务管理员对用户的身份验证通过后,向用户提交的派生DID颁发可验证证书,计算并更新存储在联盟链上的可验证证书累加器的散列值;

步骤4具体包含以下步骤:

步骤4.1,第i所高校U_i的第t个用户P_{it}生成第u个派生DID DID_{D_u}、公私钥对(PK_{D_u},SK_{D_u}),将派生DID注册请求$\left(DID_{D_u},PK_{D_u},DID_{P_{it}},sig\left(SK_{P_{it}},H\left(DID_{D_u}\|PK_{D_u}\|DID_{P_{it}}\right)\right)\right)$发送给任意一所高校$U_p$的高校DID服务管理员;

步骤4.2,任意一所高校U_p的高校DID服务管理员收到派生DID注册请求,校验签名$sig\left(SK_{P_{it}},H\left(DID_{D_u}\|PK_{D_u}\|DID_{P_{it}}\right)\right)$有效后,使用高校$U_p$的高校DID服务管理员的DID身份$DID_{U_p}$对应的私钥$SK_{U_p}$对第二散列值$H\left(DID_{D_u}\|PK_{D_u}\|DID_{U_p}\right)$进行签名,将$\left(DID_{D_u},PK_{D_u},DID_{U_p},sig\left(SK_{U_p},H\left(DID_{D_u}\|PK_{D_u}\|DID_{U_p}\right)\right)\right)$上联盟链存储,使第i所高校$U_i$的第t个用户$P_{it}$的第u个派生DID DID_{D_u}生效;

步骤4.3,第i所高校U_i的第t个用户P_{it}将第u个派生DID DID_{D_u},第i所高校U_i的第j张可验证证书定义文件$VCDef_{ij}$,身份验证信息,发送给第i所高校U_i的高校DID服务管理员,申请第i所高校颁发的第j类可验证证书VC_{ij};

其中的身份验证信息,在系统初始时,需要附带物理世界的身份验证信息,用户拥有的可验证证书数量足够时,可以通过可验证证书证明身份。

[0019] 步骤4.4,第i所高校U_i的高校DID服务管理员为第i所高校U_i的第t个用户P_{it}按照第i所高校U_i的第j张可验证证书定义文件$VCDef_{ij}$中可验证证书属性列表$\{A_{ij_1},\ldots,A_{ij_s}\}$填写

对应属性值,生成一个大素数Q作为序列号,添加到可验证证书累加器$ACCUM_{ij}$中,计算并更新联盟链上可验证证书累加器的散列值$H\left(ACCUM_{ij}\right)$,将属性值和序列号组合成为第i所高校颁发的第j类可验证证书VC_{ij}并发送给第i所高校U_i的第t个用户P_{it}。

[0020] 第i所高校U_i的高校DID服务管理员为第i所高校U_i的第t个用户P_{it}按照第一可验证证书属性列表填写明文属性值和盐值$\left\{A_{ij_1}:\left\{m_{ij_1},SALT_{ij_1}\right\},\ldots,A_{ij_s}:\left\{m_{ij_s},SALT_{ij_s}\right\}\right\}$,$m_{ij_1}$为第一可验证证书属性列表第一个可验证证书属性$A_{ij_1}$的明文属性值,$SALT_{ij_1}$是为第一可验证证书属性列表第一个可验证证书属性$A_{ij_1}$的明文属性值$m_{ij_1}$生成的随机数盐值,$m_{ij_s}$为第一可验证证书属性列表第s个可验证证书属性$A_{ij_s}$的明文属性值,$SALT_{ij_s}$是为第一可验证证书属性列表第s个可验证证书属性$A_{ij_s}$的明文属性值$m_{ij_s}$生成的随机数盐值,并为该第一可验证证书属性列表的明文属性值生成散列值列表$\left\{H_{ij_1},\ldots,H_{ij_s}\right\}$,其中散列值列表中的第一个散列值$H_{ij_1}=H(m_{ij_1}\|SALT_{ij_1})$,散列值列表中的第s个散列值$H_{ij_s}=H(m_{ij_s}\|SALT_{ij_s})$;生成一个大素数$Q$作为序列号,添加到可验证证书累加器$ACCUM_{ij}$中,计算并更新联盟链上可验证证书累加器的散列值$H\left(ACCUM_{ij}\right)$,将生成的可验证证书$VC_{ij}=\left(DID_{D_u},\left\{A_{ij_1}:\left\{m_{ij_1},SALT_{ij_1}\right\},\ldots,A_{ij_s}:\left\{m_{ij_s},SALT_{ij_s}\right\}\right\},Q,sig\left(SK_{VC_{ij}},H\left(DID_{D_u}\|H_{ij_1}\|\ldots\|H_{ij_s}\|Q\right)\right)\right)$发送给第i所高校$U_i$的第t个用户$P_{it}$。

[0021] 更新所述可验证证书累加器值$ACCUM_{ij}=ACCUM_{ij}*Q$,计算并更新链上的可验证证书累加器的散列值$H\left(ACCUM_{ij}\right)$。

[0022] 步骤5、证明文件生成和服务获取:用户将可验证证书处理为可验证证书声明,将所述可验证证书声明组成证明文件,并发送给服务提供方;服务提供方验证证明文件属性是否满足条件,通过联盟链上可验证证书累加器的散列值验证每个可验证证书声明的有效性,通过联盟链上公钥信息验证每个可验证证书声明对应的高校DID服务管理员的私钥签名和派生DID的私钥签名的正确性,均验证通过则提供服务;

步骤5具体包含以下步骤:

步骤5.1,第i所高校U_i的第t个用户P_{it}获得与第二列表$\left\{VCDef_{ij},\ldots,VCDef_{nl}\right\}$匹配的可验证证书$VC_{ij},\ldots,VC_{nl}$,$VC_{nl}$表示第n所高校颁发的第l类可验证证书,校验签名有效后,将可验证证书中包含于属性需求列表$\left\{R_{k_1}:v_{k_1},\ldots,R_{k_h}:v_{k_h}\right\}$的属性值以明文展示,其他以明文的散列值展示,成为可验证证书声明文件,分别使用请求可验证证书时的派生DID所对应的私钥对可验证证书声明文件签名,组合成为证明文件$Cred_Proof$发送给服务提供方SP_k;

所述步骤5.1的具体步骤为:

第i所高校U_i的第t个用户P_{it}获得与第二列表$\left\{VCDef_{ij},\ldots,VCDef_{nl}\right\}$匹配的可验证证书$VC_{ij},\ldots,VC_{nl}$,$VC_{nl}$表示第n所高校颁发的第l类可验证证书,校验签名有效后,将可验证证书中包含于属性需求列表$\left\{R_{k_1}:v_{k_1},\ldots,R_{k_h}:v_{k_h}\right\}$的属性值以明文展示,其他以散列值展示,

成为可验证证书声明列表$\{VC'_{ij},\ldots,VC'_{nl}\}$,$VC'_{ij}$表示散列值处理后的第i所高校颁发的第j类可验证证书VC_{ij},VC'_{nl}表述散列值处理后的第n所高校颁发的第l类可验证证书VC_{nl},依次使用请求可验证证书时的第u个派生DID的私钥SK_{D_u},……,第e个派生的私钥SK_{D_e}签名组合成证明文件$Cred_Proof=\left(\left\{VC'_{ij},sig\left(SK_{D_u},H\left(VC'_{ij}\right)\right)\right\},\ldots,\left\{VC'_{nl},sig\left(SK_{D_e},H\left(VC'_{nl}\right)\right)\right\}\right)$,将所述证明文件$Cred_Proof$发送给服务提供方$SP_k$。

[0023] 步骤5.2,服务提供方SP_k接收到证明文件$Cred_Proof$后,检查属性和属性值是否满足属性需求列表$\{R_{k_1}:v_{k_1},\ldots,R_{k_h}:v_{k_h}\}$,对于证明文件中的每张可验证证书声明文件,分别通过可验证证书累加器信息检查可验证证书声明的有效性,通过联盟链上公钥信息验证每个可验证证书声明对应的高校DID服务管理员的私钥签名和派生DID的私钥签名的正确性,均验证通过则提供服务。

[0024] 所述步骤5.2的具体步骤为:

服务提供方SP_k收到所述$Cred_Proof$,验证是否满足$\{R_{k_1}:v_{k_1},\ldots,R_{k_h}:v_{k_h}\}$中全部所需的属性,且其中属性的属性值属于所述属性的属性值空间;

服务提供方验证第i所高校颁发的第j类可验证证书VC_{ij}有效性时,从高校U_i的高校DID服务管理员处获取可验证证书累加器值$ACCUM_{ij}$,计算散列值并和存储在联盟链上的散列值进行对比,一致则验证证书累加器$ACCUM_{ij}$模第i所高校颁发的第j类可验证证书VC_{ij}中的序列号Q的值是否为0,若为0,则该第i所高校U_i的第j张可验证证书VC_{ij}有效;

通过联盟链上公钥信息验证每个可验证证书声明对应的高校DID服务管理员的私钥签名和派生DID的私钥签名是否正确,均验证通过则提供服务。

[0025] 步骤6、可验证证书撤销:可验证证书需要被撤销时,颁发所述可验证证书的高校DID服务管理员通过修改可验证证书累加器并更新联盟链上可验证证书累加器的散列值来撤销可验证证书。

[0026] 所述步骤6的具体步骤为:

可验证证书VC_{ij}超出有效期范围或者由于其他原因失效,需要由证书颁发高校U_i的高校DID服务管理员进行撤销,执行可验证证书累加器更新$ACCUM_{ij}=ACCUM_{ij}/Q$,之后计算并更新联盟链上存储的可验证证书累加器的散列值$H\left(ACCUM_{ij}\right)$。

[0027] 值得注意的是,本发明实施例中未作详细描述的内容属于本领域专业技术人员公知的现有技术。

[0028] 综上所述,本发明实施例所提供的方法具有如下优点:

1)身份信息可信、不可篡改存储:依托区块链技术实现高校联盟用户身份系统,可以有效地促进高校间的资源互通和信息互认,并借助区块链不可篡改的特性,保证了高校间信息共享的可信度和安全性;

2)跨机构全局身份管理:采用DID和可验证证书技术,实现跨越不同机构的身份管理,实现了身份验证和信息共享的去中心化和高效性;用户只需要拥有一个DID标识和一些可验证证书,就可以在不同的机构和应用场景中实现身份验证和信息共享;

3)联盟链上信息关联性保护:采用派生DID技术,抵抗恶意用户通过联盟链上身份对用户进行画像,使得用户的联盟链上身份与其他联盟链上身份之间没有关联;

4)证书使用中的隐私保护:使用基于散列函数的属性处理方法,确保在生成证明文件时,使用最小范围的证书内容。

[0029] 另外,本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件完成,相应的程序可以存储于一种计算机可读存储介质中,上述提到的存储介质可以是只读存储器,磁盘或光盘等。

[0030] 以上所述,仅为本发明较佳的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明披露的技术范围内,可轻易想到的变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应该以权利要求书的保护范围为准。本文背景技术部分公开的信息仅仅旨在加深对本发明的总体背景技术的理解,而不应当被视为承认或以任何形式暗示该信息构成已为本领域技术人员所公知的现有技术。

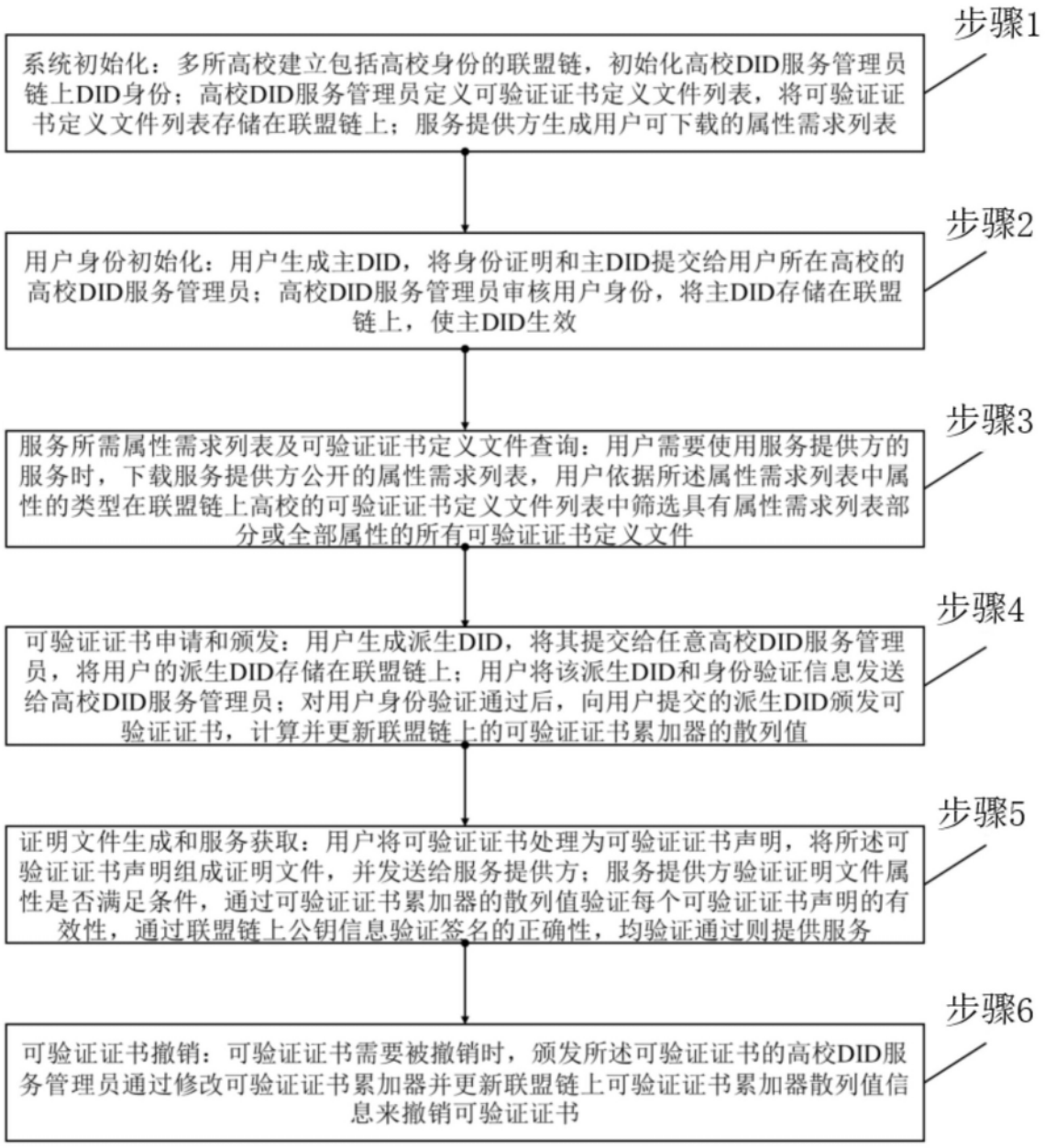

步骤1
系统初始化：多所高校建立包括高校身份的联盟链，初始化高校DID服务管理员链上DID身份；高校DID服务管理员定义可验证证书定义文件列表，将可验证证书定义文件列表存储在联盟链上；服务提供方生成用户可下载的属性需求列表
步骤2
用户身份初始化：用户生成主DID，将身份证明和主DID提交给用户所在高校的高校DID服务管理员；高校DID服务管理员审核用户身份，将主DID存储在联盟链上，使主DID生效
步骤3
服务所需属性需求列表及可验证证书定义文件查询：用户需要使用服务提供方的服务时，下载服务提供方公开的属性需求列表，用户依据所述属性需求列表中属性的类型在联盟链上高校的可验证证书定义文件列表中筛选具有属性需求列表部分或全部属性的所有可验证证书定义文件
步骤4
可验证证书申请和颁发：用户生成派生DID，将其提交给任意高校DID服务管理员，将用户的派生DID存储在联盟链上；用户将该派生DID和身份验证信息发送给高校DID服务管理员；对用户身份验证通过后，向用户提交的派生DID颁发可验证证书，计算并更新联盟链上的可验证证书累加器的散列值
步骤5
证明文件生成和服务获取：用户将可验证证书处理为可验证证书声明，将所述可验证证书声明组成证明文件，并发送给服务提供方；服务提供方验证证明文件属性是否满足条件，通过可验证证书累加器的散列值验证每个可验证证书声明的有效性，通过联盟链上公钥信息验证签名的正确性，均验证通过则提供服务
步骤6
可验证证书撤销：可验证证书需要被撤销时，颁发所述可验证证书的高校DID服务管理员通过修改可验证证书累加器并更新联盟链上可验证证书累加器散列值信息来撤销可验证证书

图1