(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112039872 A
(43)申请公布日 2020.12.04

(21)申请号 202010882623.1

(22)申请日 2020.08.28

(71)申请人 武汉见邦融智科技有限公司
地址 430064 湖北省武汉市武昌区雄楚大街128号领秀苑2层5室6号

(72)发明人 毛赛 王婧 何德彪 姚明 何浩 王湾湾

(74)专利代理机构 武汉科皓知识产权代理事务所(特殊普通合伙) 42222
代理人 严彦

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 29/08(2006.01)

权利要求书3页 说明书9页

(54)发明名称

基于区块链的跨域匿名认证方法及系统

(57)摘要

本发明提供一种基于区块链的跨域匿名认证方法及系统,设置可信密钥生成中心为注册中心颁发公私钥对,部署区块链智能合约管理通信方的密钥信息;注册中心为普通用户提供注册服务,生成签名实现证书认证服务,并将业务系统相关的通信方标识信息与公钥信息以隐私保护的方式存入区块链智能合约中;通信双方进行相互认证时,通过匿名的方式发送认证信息,并且调用区块链智能合约查询接口查验用户的标识信息,检验认证用户公钥是否注册;智能合约管理标识信息与密钥信息,提供用户标识信息与密钥信息的实时更新,避免引入单点故障攻击和更新不同步及通信开销大等问题,并且支持用户跨域认证服务。该匿名认证技术方案具有很好的安全性、稳定性和可靠性。

CN 112039872 A

1.一种基于区块链的跨域匿名认证方法,其特征在于:设置可信密钥生成中心为注册中心颁发公私钥对,并部署区块链智能合约管理通信方的密钥信息;注册中心为普通用户提供注册服务,生成签名实现证书认证服务,并将业务系统相关的通信方标识信息与公钥信息以隐私保护的方式存入区块链智能合约中;通信双方进行相互认证时,通过匿名的方式发送认证信息,并且调用区块链智能合约查询接口查验用户的标识信息,检验认证用户公钥是否注册;同时,智能合约管理身份标识信息与密钥信息;提供用户标识信息与密钥信息的动态更新和撤销。

2.根据权利要求1所述基于区块链的跨域匿名认证方法,其特征在于:跨域匿名认证实现包括以下过程,

系统初始化过程,用于生成系统的公开参数和系统主私钥;

智能合约部署过程,用于安全管理系统内各成员的身份标识信息、公钥证书和密钥信息,为跨域认证提供注册验证服务;

注册过程,用于为系统内各成员提供对应的注册服务,并调用智能合约管理其身份标识信息、公钥证书和密钥信息;

相互认证过程中,用于为系统内需要进行相互认证的成员提供身份认证与密钥协商服务,调用智能合约查询接口验证认证成员的可靠性;

密钥更新过程,用于为系统成员身份信息提供密钥更新服务,并调用智能合约对更新的信息进行管理,防止系统成员的身份可链接攻击,支持安全高效的系统成员动态加入;

密钥撤销过程,用于为系统成员身份信息提供用户服务,调用智能合约删除撤销用户的注册信息,防止密钥泄露,支持安全高效的系统成员动态撤销。

3.根据权利要求2所述基于区块链的跨域匿名认证方法,其特征在于:在系统初始化过程中,针对匿名认证与密钥协商的参与方,生成系统公私钥和其他参数并部署区块链平台,实现方式为由可信密钥生成中心KGC完成相关操作如下,

1)KGC选择系统安全参数κ,定义初始化基点为P和阶为q的椭圆曲线加法群$\mathbb{G}$,并选定一个密码杂凑函数;

2)KGC选择一个随机种子,生成系统主私钥sk_{root}和链码$chaincode_{root}$,随后计算系统主公钥$P_{root}=sk_{root}\cdot P$;

3)KGC创建一个包含相关配置参数的创世块文件File以搭建一个健壮的联盟区块链,选定若干半诚实的联盟节点共同维护区块链运行;

4)KGC秘密保存主私钥sk_{root},File,发布公开参数$(\mathbb{G},P,q,PK_{root},h)$。

4.根据权利要求3所述基于区块链的跨域匿名认证方法,其特征在于:在智能合约部署过程中,部署一个隐私保护的智能合约以实现系统参与方的公私钥和身份的管理,实现方式包括进行以下操作,

1)KGC初始化两个智能合约,分别为管理注册中心注册信息的智能合约RCA和管理用户注册信息的智能合约UCA,每个智能合约均提供四个接口,分别为支持智能合约初始化接口init(•)、智能合约更新接口update(•)、智能合约查询接口query(•)和智能合约撤销接口revoke(•);

2)KGC为各个注册中心UR_j分配智能合约UCA的更新接口、智能合约查询接口的调用权限

以及智能合约RCA的查询接口。

5.根据权利要求4所述基于区块链的跨域匿名认证方法，其特征在于：所述注册过程在KGC和UR_j、UR_j和U_i之间交互完成，并通过智能合约对注册信息进行记录；

KGC和UR_j的注册流程如下，

1)UR_j将其身份标识ID_j发送给KGC作为注册请求；

2)KGC收到注册请求后，调用BIP32.SKD(sk_{root},$chaincode_{root}$,ID_j)生成私钥sk_j，计算公钥为$PK_j=sk_j \cdot P$，并用主私钥sk_{root}对公钥PK_j生成数字签名Sig_j；其中，BIP32.SKD(•)为私钥衍生子算法；

3)KGC调用智能合约RCA的更新接口update(•)，将UR_j的信息(ID_j,PK_j,Sig_j)添加到区块链智能合约RCA上；

4)KGC将公私钥(d_j,PK_j,$chaincode_{root}$)安全秘密地发送给RU_j，RU_j先调用RCA的查询接口query(PK_j)查询智能合约是否登记了与其身份相关的注册信息，然后验证公钥PK_j=BIP32.PKD(PK_{root},chaincode,ID_j)是否成立，如果是则完成注册过程，否则重新发起注册请求；

UR_j和U_i的注册流程如下：

1)U_i向UR_j发送一个注册请求信息，UR_j返回信息(ID_j,PK_j,Sig_j)的智能合约查询接口；

2)U_i调用接口验证签名Sig_j的正确性后，先选择一个随机种子，生成私钥d_i、链码cc_i^0和公钥$D_i=d_i \cdot P$，然后将其真实身份信息ID_i和链码cc_i^0、公钥D_i通过安全信道发送给UR_j；

3)UR_j收到(ID_i, cc_i^0, D_i)后，先选择随机数$r_i \in \mathbb{Z}_q^*$，计算密文

$C_i=(C_{i1}=r_i \cdot P, C_{i2}=ID_i \cdot h(sk_j \cdot C_{i1}) \bmod q, C_{i3}=cc_i^0+h(sk_j \cdot C_{i1}) \bmod q)$和对公钥$D_i$的数字签名$Sig_i$，然后调用智能合约UCA的update()接口将信息(D_i,C_i,Sig_i,PK_j)添加到合约UCA中；其中，C_{i1}、C_{i2}、C_{i3}均为部分密文信息；

4)UR_j返回注册成功的响应信息；

5)U_i调用智能合约UCA的查询接口query(D_i)查询智能合约UCA是否登记了与其身份相关的注册信息，并验证签名Sig_i的合法性，若合法则注册完成，否则重新发起注册请求。

6.根据权利要求5所述基于区块链的跨域匿名认证方法，其特征在于：在相互认证过程中，由两个用户交互完成认证，设有用户U_1和U_2，相应公钥为D_1和D_2，并且认证通信的发起方已知认证接收方的公钥信息，相应操作如下，

1)U_1选择一个随机数$k_1 \in \mathbb{Z}_q^*$，计算随机因子$KK_1=k_1 \cdot P$，签名信息$S=k_1-d_1h(D_1||t_1||KK_1)$和认证因子$X=k_1 \cdot D_2 \oplus (D_1||s)$，然后将消息$M_1=\{KK_1||X||t_1\}$发送给$U_2$，其中$t_1$为$U_1$当前的时间戳；

2)U_2收到信息后检查时间戳t_1是否新鲜，若不是则拒绝认证通信，否则计算$(D_1||s)=X \oplus d_2 \cdot KK_1$，并依次进行步骤：

①调用智能合约UCA的查询接口query(D_1)查询是否存在D_1的注册信息(D_i,C_i,Sig_i,PK_j)，

②调用RCA的查询接口query(PK_j)查询是否存在UR_j的注册信息并验证签名Sig_i的正确性，

③验证等式$KK_1=s\cdot P+h(D_1||t_1||KK)\cdot D_i$是否成立，

若步骤①②③中有一个不成立，则拒绝通信，否则选择一个随机数$k_2\in\mathbb{Z}_q^*$，计算随机因子$KK_2=k_2\cdot P$，进而计算会话密钥$sk_{21}=h(KK_1||KK_2||k_2\cdot KK_1||D_1||D_2)$，以及认证因子$Y=h(d_2\cdot KK_1||t_j)\oplus h(D_1||D_2||sk_{21})$，然后将消息$M_2=\{KK_2||Y||t_2\}$发送给$U_1$，其中$t_2$为$U_2$当前的时间戳；

3)U_1收到信息后检查时间戳t_2是否新鲜，若不是则拒绝认证通信，否则计算会话密钥$sk_{12}=h(KK_1||KK_2||k_1\cdot KK_2||D_1||D_2)$，和验证信息$Y'=h(k_1\cdot D_2||KK_1||t_2)\oplus(D_1||D_2||sk_{12})$，验证$Y'=Y$是否成立，若不成立，则认证失败，否则完成认证及会话密钥协商，为后续通信保证信息机密性。

7.根据权利要求6所述基于区块链的跨域匿名认证方法，其特征在于：针对密钥更新过程，有两种情况终端用户U_i需要更新密钥，

第一种：在移动自组织网络中，为了防止匿名用户的链接性，需要对注册用户的密钥信息进行定期更新以防止追踪，更新操作实现如下，

此时，UR_j首先解密获得当前链码$cc_i^k=C_{i3}-h(sk_j\cdot C_{i1})mod\ q$，然后调用公钥衍生算法$BIP32.PKD(D_i,cc_i^k,k+1)$生成新的公钥$D'_i$和链码$cc_i^{k+1}$；接着选择新的随机数$r_i^{'}\in\mathbb{Z}_q$，计算密文

$C_i^{'}=\{C_{i1}^{'}=C_{i1}+r_i^{'}\cdot P\quad,\quad C_{i2}^{'}=C_{i2}\cdot h(sk_j\cdot C_{i1}^{'})\cdot h(sk_j\cdot C_{i1})^{-1}\ mod\ q, C_{i3}=cc_i^{k+1}+h(sk_j\cdot C_{i1}^{'})mod\ q\}$和对公钥$D'_i$的数字签名$Sig'_i$，然后调用智能合约UCA的update( )接口将信息(D'_i,C'_i,Sig'_i,PK_j)添加到合约UCA中；用户U_i则调用私钥衍生算法$BIP32.SKD(d_i,cc_i^k,k+1)$生成新的对应私钥$d'_i$和链码$cc_i^{k+1}$；

第二种：如果U_i的私钥泄露，那么U_i就必须提前请求密钥更新，

此时，对应的UR_j需要帮助其更新密钥，并对原密钥信息进行撤销；首先，UR_j按照如上更新操作对密钥进行更新，然后调用UCA的撤销接口revoke(D_i)将对应的信息(D_i,C_i,Sig_i,PK_j)从智能合约中删除。

8.根据权利要求7所述基于区块链的跨域匿名认证方法，其特征在于：针对密钥撤销过程，有两种情况下U_i的密钥信息需要被撤销，

第一种：如果UR_j发现用户U_i存在可疑行为，UR_j调用UCA的撤销接口revoke(D_i)将对应的信息(D_i,C_i,Sig_i,PK_j)从智能合约中删除；

第二种：如果U_i想要离开系统，需要发送一个撤销请求到UR_j，然后UR_j调用UCA的撤销接口revoke(D_i)将对应的信息(D_i,C_i,Sig_i,PK_j)从智能合约中删除。

9.一种基于区块链的跨域匿名认证系统，其特征在于：用于实现如权利要求1-8任一项所述的一种基于区块链的跨域匿名认证方法。

10.根据权利要求9所述基于区块链的跨域匿名认证系统，其特征在于：包括可信密钥生成中心、注册服务器设备和终端设备，可信密钥生成中心采用可信服务器实现。

基于区块链的跨域匿名认证方法及系统

技术领域

[0001] 本发明属于信息安全技术领域,特别是基于区块链的跨域匿名认证方法及系统。

背景技术

[0002] 匿名认证协议是网络安全通信的重要组成部分。通过执行匿名认证协议,两个参与者间在公共信道上可以相互认证,并协商一个会话密钥,以便实现开放网络中的安全通信。在基于传统公钥密码认证的匿名协议中,通信双方拥有一对公私钥:公钥和私钥,其中私钥用于生成认证信息,公钥来验证信息的合法性。但是对公钥的认证需要证书中心为各用户颁发数字证书,用来实现安全的信息交换建立身份并创建信任。

[0003] 然而,依赖证书颁发机构定期颁发证书或对证书进行维护,会导致用户端高通信开销和证书更新异步问题。尽管现有基于身份的认证协议可以消除证书管理问题,但在认证过程中必须泄露真实身份给另一个认证通信以进行验证。这对于开放性网络,如自组织网络而言,存在严重的隐私泄露隐患。虽然已有许多密码协议被提出来促进网络系统的安全认证,但现有协议通常不支持条件可控匿名和灵活的密钥管理。此外,现有的技术需要用户在跨域情况下重新执行注册,难以支持高效的移动用户的跨域认证功能。

[0004] 针对这种情况,本发明设计了一种基于区块链的匿名跨域认证与密钥协商方法,并实现有效的条件可控匿名,并且在认证与密钥协商过程中无需引入额外的密码原语,通过区块链智能合约技术,实现高效的密钥管理,支持用户/设备的动态接入和撤销。

发明内容

[0005] 本发明的目的是提出一种基于区块链的跨域匿名认证技术方案,具有高效密钥管理,支持物联网设备/用户动态接入和撤销的匿名认证与密钥协商协议。

[0006] 为了实现上述目的,本发明提出一个基于区块链的跨域匿名认证方法,1.一种基于区块链的跨域匿名认证方法,其特征在于:设置可信密钥生成中心为注册中心颁发公私钥对,并部署区块链智能合约管理通信方的密钥信息;注册中心为普通用户提供注册服务,生成签名实现证书认证服务,并将业务系统相关的通信方标识信息与公钥信息以隐私保护的方式存入区块链智能合约中;通信双方进行相互认证时,通过匿名的方式发送认证信息,并且调用区块链智能合约查询接口查验用户的标识信息,检验认证用户公钥是否注册;同时,智能合约管理身份标识信息与密钥信息,可提供用户标识信息与密钥信息的动态更新和撤销。

[0007] 而且,跨域匿名认证实现包括以下过程,

[0008] 系统初始化过程,用于生成系统的公开参数和系统主私钥;

[0009] 智能合约部署过程,用于安全管理系统内各成员的身份标识信息、公钥证书和密钥信息,为跨域认证提供注册验证服务;

[0010] 注册过程,用于为系统内各成员提供对应的注册服务,并调用智能合约管理其身份标识信息、公钥证书和密钥信息;

[0011] 相互认证过程中，用于为系统内需要进行相互认证的成员提供身份认证与密钥协商服务，调用智能合约查询接口验证认证成员的可靠性；

[0012] 密钥更新过程，用于为系统成员身份信息提供密钥更新服务，并调用智能合约对更新的信息进行管理，防止系统成员的身份可链接攻击，支持安全高效的系统成员动态加入；

[0013] 密钥撤销过程，用于为系统成员身份信息提供用户服务，调用智能合约删除撤销用户的注册信息，防止密钥泄露，支持安全高效的系统成员动态撤销。

[0014] 而且，在系统初始化过程中，针对匿名认证与密钥协商的参与方，生成系统公私钥和其他参数并部署区块链平台，实现方式为由可信密钥生成中心KGC完成相关操作如下，

[0015] 1)KGC选择系统安全参数κ，定义初始化基点为P和阶为q的椭圆曲线加法群$\mathbb{G}$，并选定一个密码杂凑函数；

[0016] 2)KGC选择一个随机种子，生成系统主私钥sk_{root}和链码$chaincode_{root}$，随后计算系统主公钥$P_{root}=sk_{root}\cdot P$；

[0017] 3)KGC创建一个包含相关配置参数的创世块文件File以搭建一个健壮的联盟区块链，选定若干半诚实的联盟节点共同维护区块链运行；

[0018] 4)KGC秘密保存主私钥sk_{root}，File，发布公开参数$(\mathbb{G},P,q,PK_{root},h)$。

[0019] 而且，在智能合约部署过程中，部署一个隐私保护的智能合约以实现系统参与方的公私钥和身份的管理，实现方式包括进行以下操作，

[0020] 1)KGC初始化两个智能合约，分别为管理注册中心注册信息的智能合约RCA和管理用户注册信息的智能合约UCA，每个智能合约均提供四个接口，分别为支持智能合约初始化接口init(•)、智能合约更新接口update(•)、智能合约查询接口query(•)和智能合约撤销接口revoke(•)；

[0021] 2)KGC为各个注册中心UR_j分配智能合约UCA的更新接口、智能合约查询接口的调用权限以及智能合约RCA的查询接口。

[0022] 而且，所述注册过程在KGC和UR_j、UR_j和U_i之间交互完成，并通过智能合约对注册信息进行记录；

[0023] KGC和UR_j的注册流程如下，

[0024] 1)UR_j将其身份标识ID_j发送给KGC作为注册请求；

[0025] 2)KGC收到注册请求后，调用$BIP32.SKD(sk_{root},chaincode_{root},ID_j)$生成私钥$sk_j$，计算公钥为$PK_j=sk_j\cdot P$，并用主私钥$sk_{root}$对公钥$PK_j$生成数字签名$Sig_j$；其中，BIP32.SKD(•)为私钥衍生子算法；

[0026] 3)KGC调用智能合约RCA的更新接口update(•)，将UR_j的信息(ID_j,PK_j,Sig_j)添加到区块链智能合约RCA上；

[0027] 4)KGC将公私钥$(d_j,PK_j,chaincode_{root})$安全秘密地发送给$RU_j$，$RU_j$先调用RCA的查询接口query$(PK_j)$查询智能合约是否登记了与其身份相关的注册信息，然后验证公钥$PK_j=BIP32.PKD(PK_{root},chaincode,ID_j)$是否成立，如果是则完成注册过程，否则重新发起注册请求；

[0028] UR_j和U_i的注册流程如下：

[0029] 1)U_i向UR_j发送一个注册请求信息，UR_j返回信息(ID_j,PK_j,Sig_j)的智能合约查询接

口；

[0030] 2)U_i调用接口验证签名Sig_j的正确性后，先选择一个随机种子，生成私钥d_i、链码cc_i^0和公钥$D_i=d_i \cdot P$，然后将其真实身份信息ID_i和链码cc_i^0、公钥D_i通过安全信道发送给UR_j；

[0031] 3)UR_j收到(ID_i, cc_i^0, D_i)后，先选择随机数$r_i \in \mathbb{Z}_q^*$，计算密文$C_i=(C_{i1}=r_i \cdot P, C_{i2}=ID_i \cdot h(sk_j \cdot C_{i1}) \bmod q, C_{i3}=cc_i^0+h(sk_j \cdot C_{i1}) \bmod q)$和对公钥$D_i$的数字签名$Sig_i$，然后调用智能合约UCA的update()接口将信息(D_i, C_i, Sig_i, PK_j)添加到合约UCA中；其中，C_{i1}、C_{i2}、C_{i3}均为部分密文信息；

[0032] 4)UR_j返回注册成功的响应信息；

[0033] 5)U_i调用智能合约UCA的查询接口query(D_i)查询智能合约UCA是否登记了与其身份相关的注册信息，并验证签名Sig_i的合法性，若合法则注册完成，否则重新发起注册请求。

[0034] 而且，在相互认证过程中，

[0035] 由两个用户交互完成认证，设有用户U_1和U_2，相应公钥为D_1和D_2，并且认证通信的发起方已知认证接收方的公钥信息，相应操作如下，

[0036] 1)U_1选择一个随机数$k_1 \in \mathbb{Z}_q^*$，计算随机因子$KK_1=k_1 \cdot P$，签名信息$s=k_1-d_1h(D_1||t_1||KK_1)$和认证因子$X=k_1 \cdot D_2 \oplus (D_1||s)$，然后将消息$M_1=\{KK_1||X||t_1\}$发送给$U_2$，其中$t_1$为$U_1$当前的时间戳；

[0037] 2)U_2收到信息后检查时间戳t_1是否新鲜，若不是则拒绝认证通信，否则计算$(D_1||s)=X \oplus d_2 \cdot KK_1$，并依次进行步骤：

[0038] ①调用智能合约UCA的查询接口query(D_1)查询是否存在D_1的注册信息(D_i, C_i, Sig_i, PK_j)，

[0039] ②调用RCA的查询接口query(PK_j)查询是否存在UR_j的注册信息并验证签名Sig_i的正确性，③验证等式$KK_1=s \cdot P+h(D_1||t_1||KK) \cdot D_i$是否成立，

[0040] 若步骤①②③中有一个不成立，则拒绝通信，否则选择一个随机数$k_2 \in \mathbb{Z}_q^*$，计算随机因子$KK_2=k_2 \cdot P$，进而计算会话密钥$sk_{21}=h(KK_1||KK_2||k_2 \cdot KK_1||D_1||D_2)$，以及认证因子$Y=h(d_2 \cdot KK_1||t_j) \oplus h(D_1||D_2||sk_{21})$，然后将消息$M_2=\{KK_2||Y||t_2\}$发送给$U_1$，其中$t_2$为$U_2$当前的时间戳；

[0041] 3)U_1收到信息后检查时间戳t_2是否新鲜，若不是则拒绝认证通信，否则计算会话密钥$sk_{12}=h(KK_1||KK_2||k_1 \cdot KK_2||D_1||D_2)$，和验证信息

$Y'=h(k_1 \cdot D_2||KK_1||t_2) \oplus (D_1||D_2||sk_{12})$，验证$Y'=Y$是否成立，若不成立，则认证失败，否则完成认证及会话密钥协商，为后续通信保证信息机密性。

[0042] 而且，针对密钥更新过程，有两种情况终端用户U_i需要更新密钥，

[0043] 第一种：在移动自组织网络中，为了防止匿名用户的链接性，需要对注册用户的密钥信息进行定期更新以防止追踪，更新操作实现如下，

[0044] 此时，UR_j首先解密获得当前链码$cc_i^k=C_{i3}-h(sk_j \cdot C_{i1}) \bmod q$，然后调用公钥衍

生算法$\mathrm{BIP32.PKD}(D_i, cc_i^k, k+1)$生成新的公钥D′i和链码$cc_i^{k+1}$；接着选择新的随机数$r_i' \in \mathbb{Z}_q$，计算密文

$C_i' = \{C_{i1}' = C_{i1} + r_i' \cdot P, C_{i2}' = C_{i2} \cdot h(sk_j \cdot C_{i1}') \cdot h(sk_j \cdot C_{i1})^{-1} \bmod q, C_{i3} = cc_i^{k+1} + h(sk_j \cdot C_{i1}') \bmod q\}$和对公钥Di′的数字签名Sigi′，然后调用智能合约UCA的update()接口将信息(Di′,Ci′,Sigi′,PKj)添加到合约UCA中；用户Ui则调用私钥衍生算法$\mathrm{BIP32.SKD}(d_i, cc_i^k, k+1)$生成新的对应私钥di′和链码$cc_i^{k+1}$；

[0045] 第二种：如果Ui的私钥泄露，那么Ui就必须提前请求密钥更新，

[0046] 此时，对应的URj需要帮助其更新密钥，并对原密钥信息进行撤销；首先，URj按照如上更新操作对密钥进行更新，然后调用UCA的撤销接口revoke(Di(将对应的信息)Di,Ci,Sigi,PKj)从智能合约中删除。

[0047] 而且，针对密钥撤销过程，有两种情况下Ui的密钥信息需要被撤销，

[0048] 第一种：如果URj发现用户Ui存在可疑行为，URj调用UCA的撤销接口revoke(Di)将对应的信息(Di,Ci,Sigi,PKj)从智能合约中删除；

[0049] 第二种：如果Ui想要离开系统，需要发送一个撤销请求到URj，然后URj调用UCA的撤销接口revoke(Di)将对应的信息(Di,Ci,Sigi,PKj)从智能合约中删除。

[0050] 本发明还提供一种基于区块链的跨域匿名认证系统，用于实现如上所述的一种基于区块链的跨域匿名认证方法。

[0051] 而且，包括可信密钥生成中心、注册服务器设备和终端设备，可信密钥生成中心采用可信服务器实现。

[0052] 本发明与现有技术相比具有如下优点和有益效果：

[0053] 1.关于相互认证的条件匿名，现有的满足条件匿名属性的认证方案，虽然可以实现身份的条件匿名，但需要在认证过程中引入群签名等计算开销和通信开销较高的密码原语，不适应于资源受限的终端用户。本发明只需注册中心通过简单的身份解密即可恢复恶意用户的真实身份，无需在用户端增加额外开销。

[0054] 2.关于跨域认证，由于区块链的公开性和不可篡改性，用户在其他地域进行认证时，无需二次注册，只需通过查询区块链的公钥信息即可认证公钥的可靠性，从而实现跨域认证。

[0055] 3.关于密钥的高效管理，目前的密钥管理方法中，为实现密钥更新与撤销，需要引入在线证书查询协议或定期更新并发送最新的撤销列表给终端用户，从而需要消耗较大的网络资源、通信开销和存储开销等，并且撤销列表机制还面临更新同步问题，难以适用于资源受限的终端用户。

[0056] 4.终上所述，本发明通过智能合约管理对标识信息与密钥信息，可提供用户标识信息与密钥信息的实时更新，避免引入公钥证书在线实时查询协议可能遭受的单点故障攻击和撤销列表更新不同步及通信开销大等问题，并且支持用户跨域认证服务。本发明提供的该匿名认证技术方案具有很好的安全性、稳定性和可靠性。可以广泛适用于车联网自组织网络、智能电网边缘计算架构等物联网，具有重要的市场价值。

具体实施方式

[0057] 以下结合实施例具体说明本发明的技术方案。

[0058] 本发明实施例提供了一种基于区块链的跨域匿名认证方法，通过以下技术方案实现：可信密钥生成中心为注册中心颁发公私钥对，并部署区块链智能合约管理通信方的密钥信息。注册中心为普通用户提供注册服务，生成签名实现证书认证服务，并将业务系统相关的通信方标识信息与公钥信息以隐私保护的方式存入区块链智能合约中；通信双方进行相互认证时，通过匿名的方式发送认证信息，并且调用区块链智能合约查询接口查验用户的标识信息，检验认证用户公钥是否注册。同时，智能合约管理身份标识信息与密钥信息，可提供用户标识信息与密钥信息的动态更新和撤销。与传统基于公钥基础设施体制的匿名认证技术相比，本发明避免了复杂的证书管理问题，以及公钥证书在线实时查询协议可能遭受的单点故障攻击和撤销列表更新不同步及通信开销大等问题；与传统基于身份密码体制的匿名认证相比，本发明避免资源受限、处理能力受限的客户端存储白名单或黑名单的开销问题。此外，由于区块链的不可篡改性、数据块可全网公开且同步等特性，本发明利用智能合约管理用户注册信息，支持用户跨域认证服务，避免用户跨域二次注册或跨域管理中心间的额外交互。该匿名认证与密钥管理方法具有很好的安全性、稳定性和可靠性。

[0059] 实施例中，所提供基于区块链的跨域匿名认证方法实现方式包括以下过程：

[0060] 系统初始化过程，用于生成系统的公开参数和系统主私钥；

[0061] 智能合约部署过程，用于安全管理系统内各成员的身份标识信息、公钥证书和密钥信息，为跨域认证提供注册验证服务；

[0062] 注册过程，用于为系统内各成员提供对应的注册服务，并调用智能合约管理其身份标识信息、公钥证书和密钥信息；

[0063] 相互认证过程中，用于为系统内需要进行相互认证的成员提供身份认证与密钥协商服务，调用智能合约查询接口验证认证成员的可靠性；

[0064] 密钥更新过程，用于为系统成员身份信息提供密钥更新服务，并调用智能合约对更新的信息进行管理，防止系统成员的身份可链接攻击，支持安全高效的系统成员动态加入；

[0065] 密钥撤销过程，用于为系统成员身份信息提供用户服务，调用智能合约删除撤销用户的注册信息，防止密钥泄露，支持安全高效的系统成员动态撤销。

[0066] 为便于实施参考起见，以下对各过程实现分别进行具体描述。

[0067] 首先，为便于理解本发明技术方案，提供本发明实施例相关符号及定义如下：

[0068] κ：系统安全参数

[0069] $\mathbb{G}$：定义于有限域$\mathbb{F}_p$椭圆曲线加法群

[0070] P：群$\mathbb{G}$的基点

[0071] q：群$\mathbb{G}$的素数阶

[0072] $\mathbb{Z}_q^*$：有限域，即{1,2,3,…,q}

[0073] k·P：椭圆曲线上点P的k倍点，即$k \cdot P = \underbrace{P + P + \cdots + P}_{k个}$，k是正整数

[0074] h(·)：密码杂凑函数(即哈希函数)，输入为任意长度字符串，输出为$\mathbb{Z}_q$上的元素

[0075] File:联盟链创世文件

[0076] KGC:可信密钥生成中心

[0077] U_i,U_1,U_2:分别为第i个用户、当前参与认证的第一用户、第二用户

[0078] UR_j:第j个分布式注册中心

[0079] sk_{root},PK_{root}:系统的主私钥和主公钥

[0080] BIP32:分层确定性钱包算法,包含私钥衍生子算法BIP32.SKD(•)和公钥衍生子算法BIP32.PKD(•)

[0081] $chaincode_{root}$:密钥生成中心KGC的用于BIP32密钥衍生的链码

[0082] cc_i^k:第i个用户的第k层链码

[0083] d_i,D_i:U_i的私钥,公钥,i∈{1,2,3,…}

[0084] C_i:密文

[0085] sk_{12}/sk_{21}:会话密钥

[0086] 对于本发明具体实施,需要可信的注册中心部署区块链平台,并且提供用户注册服务和密钥管理服务,通信双方在网络公开信道上进行相互认证,在公开信道隐藏终端用户真实身份,区块链提供公钥查询等服务。

[0087] 在系统初始化过程:

[0088] 在本发明中,针对匿名认证与密钥协商的参与方,生成系统公私钥、其他参数并部署区块链平台,该操作由可信密钥生成中心KGC完成,相关操作如下:

[0089] 1)KGC选择系统安全参数κ,定义初始化基点为P和阶为q的椭圆曲线加法群$\mathbb{G}$,并选定一个密码杂凑函数h(•)、;

[0090] 2)KGC选择一个随机种子,生成系统主私钥sk_{root}和链码$chaincode_{root}$,随后计算系统主公钥$P_{root}=sk_{root}\cdot P$;

[0091] 3)KGC创建一个包含相关配置参数的创世块文件File以搭建一个健壮的联盟区块链,选定若干半诚实的联盟节点共同维护区块链运行,如在车联网自组织网络组,半诚实路边单元RSU作为联盟链背书节点;

[0092] 4)KGC秘密保存主私钥sk_{root},File,发布公开参数$(\mathbb{G},P,q,PK_{root},h)$。

[0093] 在智能合约部署过程:

[0094] 在本发明中,需要部署一个隐私保护的智能合约以实现系统参与方的公私钥和身份的管理,具体步骤如下:

[0095] 1)KGC初始化两个智能合约,分别为管理注册中心注册信息的智能合约RCA和管理用户注册信息的智能合约UCA,每个智能合约均提供四个接口,分别为支持智能合约初始化接口init(•)、智能合约更新接口update(•)、智能合约查询接口query(•)和智能合约撤销接口revoke(•);

[0096] 2)KGC为各个注册中心UR_j分配智能合约UCA的更新接口、智能合约查询接口的调用权限以及智能合约RCA的查询接口;

[0097] 在注册过程:

[0098] 在本发明中,注册算法由KGC和UR_j、UR_j和U_i之间交互完成,并通过智能合约对注册信息进行记录。

[0099] ①KGC和UR_j的注册流程如下：

[0100] 1)UR_j将其身份标识ID_j发送给KGC作为注册请求；

[0101] 2)KGC收到注册请求后，调用BIP32.SKD(sk_{root},$chaincode_{root}$,ID_j)生成私钥sk_j，计算公钥为$PK_j=sk_j \cdot P$，并用主私钥sk_{root}对公钥PK_j生成数字签名Sig_j；

[0102] 3)KGC调用智能合约RCA的更新接口update(•)，将UR_j的信息(ID_j,PK_j,Sig_j)添加到区块链智能合约RCA上；

[0103] 4)KGC将公私钥(d_j,PK_j,$chaincode_{root}$)安全秘密地发送给RU_j，RU_j先调用RCA的查询接口query(PK_j)查询智能合约是否登记了与其身份相关的注册信息，然后验证公钥$PK_j=$BIP32.PKD(PK_{root},chaincode,D_j)是否成立，如果是则完成注册过程，否则重新发起注册请求；

[0104] ②UR_j和U_i的注册流程如下：

[0105] 1)U_i向UR_j发送一个注册请求信息，UR_j返回信息(ID_j,PK_j,Sig_j)的智能合约查询接口；

[0106] 2)U_i调用接口验证了签名Sig_j的正确性后，先选择一个随机种子，生成私钥d_i、链码cc_i^0和公钥$D_i=d_i \cdot P$，然后将其真实身份信息ID_i和链码cc_i^0、公钥D_i通过安全信道发送给UR_j；

[0107] 3)UE_j收到(ID_i, cc_i^0, D_i)后，先选择随机数$r_i \in \mathbb{Z}_q^*$，计算密文$C_i=(C_{i1}=r_i \cdot P, C_{i2}=ID_i \cdot h(sk_j \cdot C_{i1}) \bmod q, C_{i3}=cc_i^0+h(sk_j \cdot C_{i1}) \bmod q)$和对公钥$D_i$的数字签名$Sig_i$，然后调用智能合约UCA的update()接口将信息(D_i,C_i,Sig_i,PK_j)添加到合约UCA中；其中，C_{i1}、C_{i2}、C_{i3}均为部分密文信息；

[0108] 4)UR_j返回注册成功的响应信息；

[0109] 5)U_i调用智能合约UCA的查询接口query(D_i)查询智能合约UCA是否登记了与其身份相关的注册信息，并验证签名Sig_i的合法性，若合法则注册完成，否则重新发起注册请求。

[0110] 在相互认证过程中：

[0111] 在本发明中，认证算法由两个用户交互完成，设有用户U_1和U_2，相应公钥为D_1和D_2，并且认证通信的发起方已知认证接收方的公钥信息，具体操作如下：

[0112] 1)U_1选择一个随机数$k_1 \in \mathbb{Z}_q^*$，计算随机因子$KK_1=k_1 \cdot P$，签名信息$S=k_1-d_1h(D_1||t_1||KK_1)$和认证因子$X=k_1 \cdot D_2 \oplus (D_1||s)$，然后将消息$M_1=\{KK_1||X||t_1\}$发送给$U_2$，其中$t_1$为$U_1$当前的时间戳；

[0113] 2)U_2收到信息后检查时间戳t_1是否新鲜，若不是则拒绝认证通信，否则计算$(D_1||s)=X \oplus d_2 \cdot KK_1$，并依次进行步骤：

[0114] ①调用智能合约UCA的查询接口query(D_1)查询是否存在D_1的注册信息(D_i,C_i,Sig_i,PK_j)，

[0115] ②调用RCA的查询接口query(PK_j)查询是否存在UR_j的注册信息并验证签名Sig_i的正确性，

[0116] ③验证等式$KK_1=s \cdot P+h(D_1||t_1||KK) \cdot D_i$是否成立，

[0117] 若步骤①②③中有一个不成立，则拒绝通信，否则选择一个随机数$k_2 \in \mathbb{Z}_q^*$，计算随机因子$KK_2 = k_2 \cdot P$，进而计算会话密钥$sk_{21} = h(KK_1||KK_2||k_2 \cdot KK_1||D_1||D_2)$，以及认证因子$Y = h(d_2 \cdot KK_1||t_j) \oplus h(D_1||D_2||sk_{21})$，然后将消息$M_2 = \{KK_2||Y||t_2\}$发送给$U_1$，其中$t_2$为$U_2$当前的时间戳；

[0118] 3)U_1收到信息后检查时间戳t_2是否新鲜，若不是则拒绝认证通信，否则计算会话密钥$sk_{12} = h(KK_1||KK_2||k_1 \cdot KK_2||D_1||D_2)$，和验证信息$Y' = h(k_1 \cdot D_2||KK_1||t_2) \oplus (D_1||D_2||sk_{12})$，验证$Y' = Y$是否成立，若不成立，则认证失败，否则完成认证及会话密钥协商，为后续通信保证信息机密性。

[0119] 在密钥更新过程中：

[0120] 本发明中，针对密钥更新过程，有两种情况终端用户U_i需要更新密钥。

[0121] 第一种：在移动自组织网络中，为了防止匿名用户的链接性，需要对注册用户的密钥信息进行定期更新以防止追踪。更新操作实现如下，

[0122] 此时，UR_j首先解密获得当前链码$cc_i^k = C_{i3} - h(sk_j \cdot C_{i1}) mod\ q$，然后调用公钥衍生算法$BIP32.PKD(D_i, cc_i^k, k+1)$生成新的公钥$D'_i$和链码$cc_i^{k+1}$，接着选择新的随机数$r_i' \in \mathbb{Z}_q$，计算密文

$$C_i' = \{C_{i1}' = C_{i1} + r_i' \cdot P \quad , \quad C_{i2}' = C_{i2} \cdot h(sk_j \cdot C_{i1}') \cdot h(sk_j \cdot C_{i1})^{-1} mod\ q, C_{i3} = cc_i^{k+1} + h(sk_j \cdot C_{i1}') mod\ q\}$$

和对公钥D'_i的数字签名Sig'_i，然后调用智能合约UCA的update()接口将信息(D'_i,C'_i,Sig'_i,PK_j)添加到合约UCA中；用户U_i则调用私钥衍生算法$BIP32.SKD(d_i, cc_i^k, k+1)$生成新的对应私钥$d'_i$和链码$cc_i^{k+1}$。

[0123] 第二种：如果U_i的私钥泄露，那么U_i就必须提前请求密钥更新。此时，对应的UR_j需要帮助其更新密钥，并对原密钥信息进行撤销。首先，UR_j按照如上更新操作对密钥进行更新，然后调用UCA的撤销接口revoke(D_i)将对应的信息(D_i,C_i,Sig_i,PK_j)从智能合约中删除。

[0124] 在密钥撤销过程中：

[0125] 本发明中，针对密钥撤销过程，有两种情况下U_i的密钥信息需要被撤销。第一种：如果UR_j发现用户U_i存在可疑行为，UR_j调用UCA的撤销接口revoke(D_i)将对应的信息(D_i,C_i,Sig_i,PK_j)从智能合约中删除。第二种：如果U_i想要离开系统，需要发送一个撤销请求到UR_j，然后UR_j调用UCA的撤销接口revoke(D_i)将对应的信息(D_i,C_i,Sig_i,PK_j)从智能合约中删除。

[0126] 具体实施时，本发明技术方案提出的方法可由本领域技术人员采用计算机软件技术实现自动运行流程，实现方法的系统装置例如存储本发明技术方案相应计算机程序的计算机可读存储介质以及包括运行相应计算机程序的计算机设备，也应当在本发明的保护范围内。基于本发明的方法，很容易实施本发明方法的系统。

[0127] 实施例提基于本发明构造的匿名认证与密钥管理系统包括可信密钥生成中心、注册服务器设备，以及终端设备，系统初始化、智能合约部署和注册流程分别按照本发明的实施例方法中初始化算法、智能合约设计算法和注册算法实现，分别基于注册服务器和终端设备提供注册服务。终端设备按照本发明的匿名认证算法，生成会话密钥。

[0128] 例如，以1台可信服务器作为可信密钥生成中心，2台注册服务器设备(分别命名为

注册服务器A和注册服务器B)，2个终端设备(分别命名为用户设备A和用户设备B)。其中，注册服务器A和注册服务器B分别管理区域A和区域B中的用户，用户设备A和用户设备B则对应于区域A和区域B中的用户。

[0129] 首先，可信服务器执行系统初始化、智能合约部署流程，并且按照发明内容为两台注册服务器设备提供注册服务，颁发公私钥对和证书等注册信息，并调用智能合约RCA更新接口将该注册信息记录在区块链上，以公示两台注册服务器的可靠性；

[0130] 下一步，注册服务器A可按照发明内容为用户设备A提供注册服务，调用智能合约UCA更新接口将用户设备的注册信息记录在区块链上，如标识信息的密文、公钥和注册服务器A签发的签名，同理，注册服务器B为用户设备B提供注册服务；

[0131] 然后，用户设备A和用户设备B可按照发明内容进行匿名相互认证与密钥协商，其中，调用智能合约RCA和UCA的查询接口验证对方的注册信息可靠性，从而利用区块链的公开性避免传统跨域认证所需的额外通信开销和单点故障风险等。

[0132] 其他未说明的具体技术实施，对于相关领域技术人员而言是众所周知，不言自明的。

[0133] 本文中所描述的具体实施例仅仅是对本发明精神作举例说明。本发明所属技术领域的技术人员可以对所描述的具体实施例做各种各样的修改或补充或采用类似的方式替代，但并不会偏离本发明的精神或者超越所附权利要求书所定义的范围。