(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109687965 B
(45)授权公告日 2021.09.21

(21)申请号 201910121268.3
(22)申请日 2019.02.18
(65)同一申请的已公布的文献号
申请公布号 CN 109687965 A
(43)申请公布日 2019.04.26
(73)专利权人 哈尔滨工业大学(深圳)
地址 518000 广东省深圳市南山区桃源街道深圳大学城哈尔滨工业大学校区
(72)发明人 曹斌 徐烨
(74)专利代理机构 深圳市添源知识产权代理事务所(普通合伙) 44451
代理人 黎健任
(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/30(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 108737403 A,2018.11.02
CN 108206821 A,2018.06.26
CN 106790253 A,2017.05.31
EP 3316549 A1,2018.05.02
US 2016330035 A1,2016.11.10
马丁等.《一种基于临时证书的互联网实名认证方案》.《信息安全与通信保密》.2013,
Tri Hoang Vo et al..《Privacy-preserving user identity in Identity-as-a-Service》.《2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops(ICIN)》.2018,

审查员 陈燕

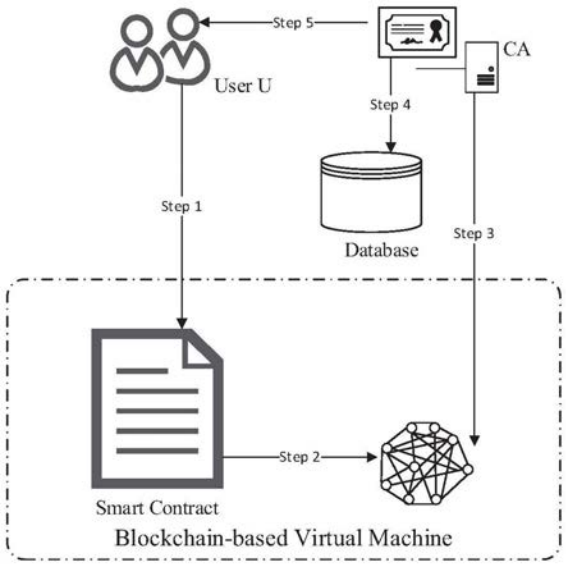
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种保护网络中用户身份信息的实名认证方法

(57)摘要

本发明专利涉及一种保护网络中用户身份信息的实名认证方法。该方法包括采用的系统框架包括实体层、策略层以及评价层,实体层包括用户U、服务提供者、认证中心CA和区块链,策略层使用的技术包括区块链和椭圆曲线密码学,评价层通过安全性分析完成对系统模型的安全评估,将用户的实名认证信息存储于区块链上,其可溯源的特性可以在需要的时候追溯到用户的真实身份,方便了互联网监管。同时,其防篡改的特性可以保证区块链上记录的信息不会被恶意改动,提高了可靠性。由于用户在不同平台使用的是不同的认证证书,因此各互联网服务提供商之间不能根据用户的实名认证证书进行信息匹配,具备不可连接性,防止互联网服务提供商对用户构建用户肖像。



CN 109687965 B

1.一种保护网络中用户身份信息的实名认证方法,其特征在于,该方法的系统框架包括实体层、策略层以及评价层,实体层包括用户U、服务提供者、认证中心CA和区块链,策略层使用的技术包括区块链和椭圆曲线密码学,评价层通过安全性分析完成对系统模型的安全评估;该方法包括:

步骤1):参数初始化;

对称加密算法E;椭圆曲线参数(p,a,b,G,n,h);

p为质数,p、a、b确定一条椭圆曲线,G为椭圆曲线的基点,n为点G的阶,协因子h为1;

CA产生私钥k_A和公钥K_A,其中$K_A=k_A*G$,$k_A\in[1,n-1]$;

U产生私钥k_U和公钥K_U,其中$K_U=k_U*G$,$k_U\in[1,n-1]$;

U加密信息前产生随机数$r\in[1,n-1]$,计算点$R=rG$;

U签名前生成的随机数$k\in[1,n-1]$;

U的个人信息记为m;

步骤2):U利用椭圆曲线加密ECIES;

计算$P=(P_x,P_y)=r*K_A$;P为椭圆曲线上的点,由K_A和r相乘计算得到的,P_x和P_y分别为P的横纵坐标;

利用KDF推导加密密钥:$k_E=KDF(P_x)$;

密文$C=E(k_E;m)$;

输出(R||C);

步骤3):U利用椭圆曲线签名ECDSA;

计算e=Hash((R||C));

计算$(x,y)=k*G$;$x'=x \bmod n$;

计算$s=k^{-1}(z+x'k_U)$, 其中z为e最左边的值;

输出(x',s)为签名;

步骤4):将(R||C,x',s)作为智能合约的输入,智能合约根据发送者的以太坊地址生成一笔交易T=(addrU,R||C,x',s)广播到区块链上;

步骤5):验证节点接收到交易后,对交易进行解析,得到请求验证者的地址以及加密的信息和签名;

步骤6):验证发送者签名;

CA先检查x'和s是否落在[1,n-1]上;

计算e=Hash((R||C)),取最左边的值为z;

计算$w=s^{-1} \bmod n$;

$u_1=zw \bmod n$, $u_2=rw \bmod n$;

$(x_1,y_1)=u_1G+u_2K_U$;

$r\equiv x_1 \bmod n$,比较r是否相等来验证签名;

步骤7):解密得到发送者信息;

$P=(P_x,P_y)=k_A*R$;令$s=P_x$;

利用KDF推导加密密钥:$k_E=KDF(s)$;

利用密钥解密得到明文$m=E^{-1}(k_E;C)$;

步骤8):验证发送者信息;

步骤8)中包括得到信息明文后,CA与数据库中用户的信息进行对比,用户信息和用户公钥都匹配后,该笔交易验证成功,CA签名后写入区块中,等待加入区块链,CA利用GUID为用户生成全局唯一标识符作为用户身份验证成功的身份标识号,签名再利用用户公钥加密后通过安全信道传输给用户,用户收到后解密得到经过CA签名的身份标识号;

步骤9):多平台身份验证;

步骤9)中包括在用户得到有CA签名的身份标识号后,用户若需要在互联网平台上进行实名认证,则只需要将该有CA签名的身份标识号与该服务提供者的唯一标识符级联,请求CA提供新的针对该服务提供者的认证证书,用户在不同的平台将利用不同的级联后的身份标识号完成实名认证。

一种保护网络中用户身份信息的实名认证方法

技术领域

[0001] 本发明属于用户身份信息的实名认证技术领域,特别涉及一种保护网络中用户身份信息的实名认证方法。

背景技术

[0002] 随着互联网技术的飞速发展,越来越多的互联网平台随之而生。经过多年的发展,互联网环境逐渐成熟,人们对互联网的依赖也逐渐加深,与此同时,层出不穷的互联网用户身份信息泄露的事件也不断增多。互联网公司通常会采取收集大量用户信息的方式使得对用户身份有更高的匹配度,以认证用户身份的真实可靠。由于对网络环境的监管,大多数互联网产品在使用前需要用户进行身份认证。为了得到真实可靠的身份信息,往往用户会被要求通过提供身份证信息或是银行卡信息的方式进行验证,这些都是用户的唯一标识符,并且是属于用户的个人隐私信息,一旦在信息的传递过程中被人窃取,或是互联网公司对数据的不当使用都会导致用户隐私的泄露,带来的严重后果将是十分恶劣的。在中心化管理的在线社交网络中,社交网络服务用户对个人信息隐私问题的意识越来越强,针对用户隐私可能泄露的问题,Aiello等人提出了LotusNet,是一个依赖端对端范式的社交网络服务发展的框架。Josang等人让用户将从不同服务供应商得到的身份和证书保存在一个防篡改的硬件设备(PAD)中,例如智能卡和其它便携式个人设备,该方法为改善用户体验和加强用户与服务提供商之间的相互认证提供了多种可能性。

[0003] 有部分互联网产品在使用过程中需要对用户进行实名认证,用户则不得不提供例如身份证号、银行卡号等可以证实个人身份的敏感信息,这些敏感信息由互联网平台各自储存。当此类敏感信息被恶意的攻击者得到时,用户将会受到一系列严重的后果,例如针对性的诈骗、身份冒用、敲诈勒索等等。现有的身份管理系统基本都是中心化的管理,用户个人身份信息的使用缺乏透明度,为了让用户的个人敏感信息被严格保护,用户在网络上所使用的身份不被除了互联网监管方以外的第三方对应到真实身份,安全的身份认证的研究十分重要。

发明内容

[0004] 为克服已有技术的不足之处,本发明提出一种保护互联网中用户身份隐私的方法,可以保护在需要实名认证的互联网环境中用户的个人身份信息隐私。具体方案如下:

[0005] 一种保护网络中用户身份信息的实名认证方法,其特征在于,该方法的系统框架包括实体层、策略层以及评价层,实体层包括用户U、服务提供者、认证中心CA和区块链,策略层使用的技术包括区块链和椭圆曲线密码学,评价层通过安全性分析完成对系统模型的安全评估;该方法包括:

[0006] 步骤1):参数初始化;

[0007] 对称加密算法E;椭圆曲线参数(p,a,b,G,n,h);

[0008] p为一个较大的质数,p、a、b确定一条椭圆曲线,G为椭圆曲线的基点,n为点G的阶,

协因子h为1；

[0009] CA产生私钥k_A和公钥K_A，其中$K_A=k_A*G$，$k_A\in[1,n-1]$；

[0010] U产生私钥k_U和公钥K_U，其中$K_U=k_U*G$，$k_U\in[1,n-1]$；

[0011] U加密信息前产生随机数$r\in[1,n-1]$，计算点$R=rG$；

[0012] U签名前生成的随机数$k\in[1,n-1]$；

[0013] U的个人信息记为m；

[0014] 步骤2)：U利用椭圆曲线加密(ECIES)；

[0015] 计算$P=(P_x,P_y)=r*K_A$；P为椭圆曲线上的点，由K_A和r相乘计算得到的，P_x和P_y分别为P的横纵坐标；

[0016] 利用KDF推导加密密钥：$k_E=KDF(P_x)$；

[0017] 密文$C=E(k_E;m)$；

[0018] 输出(R||C)；

[0019] 步骤3)：U利用椭圆曲线签名(ECDSA)；

[0020] 计算e=Hash((R||C))；

[0021] 计算$(x,y)=k*G$；$x'=x \bmod n$；

[0022] 计算$s=k^{-1}(z+x'k_U)$，其中z为e最左边的值；

[0023] 输出(x',s)为签名；

[0024] 步骤4)：将(R||C,x',s)作为智能合约的输入，智能合约根据发送者的以太坊地址生成一笔交易T=(addrU,R||C,x',s)广播到区块链上；

[0025] 步骤5)：验证节点接收到交易后，对交易进行解析，得到请求验证者的地址以及加密的信息和签名；

[0026] 步骤6)：验证发送者签名；

[0027] CA先检查x'和s是否落在[1,n-1]上；

[0028] 计算e=Hash((R||C))，取最左边的值为z；

[0029] 计算$w=s^{-1} \bmod n$；

[0030] $u_1=zw \bmod n$，$u_2=rw \bmod n$；

[0031] $(x_1,y_1)=u_1G+u_2K_U$；

[0032] $r\equiv x_1 \bmod n$，比较r是否相等来验证签名；

[0033] 步骤7)：解密得到发送者信息；

[0034] $P=(P_x,P_y)=k_A*R$；令$s=P_x$；

[0035] 利用KDF推导加密密钥：$k_E=KDF(s)$；

[0036] 利用密钥解密得到明文$m=E^{-1}(k_E;C)$；

[0037] 步骤8)：验证发送者信息；

[0038] 步骤9)：多平台身份验证。

[0039] 相比于现有的技术，本发明的优点有：

[0040] 将用户的实名认证信息存储于区块链上，其可溯源的特性可以在需要的时候追溯到用户的真实身份，方便了互联网监管。同时，其防篡改的特性可以保证区块链上记录的信息不会被恶意改动，提高了可靠性。由于用户在不同平台使用的是不同的认证证书，因此各互联网服务提供商之间不能根据用户的实名认证证书进行信息匹配，具备不可连接性，防

止互联网服务提供商对用户构建用户肖像。通过区块链进行认证和管理，较大程度地利用了区块链的优势来解决当今互联网环境存在的问题，提高互联网环境的安全，保护用户的个人身份隐私，避免由于互联网平台的漏洞和用户数据的不当使用对用户的权益造成损害。用户的个人身份隐私保护妥当，将大大减少身份冒用以及目的性诈骗等事件的发生，一定程度上保障了社会的安定。

附图说明

[0041] 图1是身份隐私保护体系框架；

[0042] 图2是本发明系统结构；

[0043] 图3是本发明实施例的实施流程图。

具体实施方式

[0044] 下面结合附图说明及具体实施方式对本发明进一步说明。

[0045] 本发明的体系框架如图1 所示，体系框架分为三大部分：实体层，策略层和评价层。其中：

[0046] (1)实体层，涉及参与系统服务的主要实体，包括用户、服务提供者、认证中心和区块链。用户向认证中心发送信息请求身份认证，认证中心认证后给用户颁发认证证书。服务提供者在本发明中特指需要实名认证的互联网服务，例如电子支付。用户向服务提供者请求服务之前需要进行实名认证，此时用户利用证书和服务提供者的统一社会信用代码等服务提供者的唯一标识符，向认证中心请求认证结果，利用该结果向服务提供者证明身份。认证中心利用区块链来实现认证过程；

[0047] (2)策略层描述了主要使用的技术以及构建的系统模型，主要有区块链和椭圆曲线密码学两大技术。区块链的主要特征是防篡改和可溯源，椭圆曲线加密依赖于椭圆曲线理论，利用椭圆曲线的离散对数问题实现更高的安全性；

[0048] (3)评价层通过安全性分析完成对系统模型的安全评估，利用假设攻击的方式评估系统模型是否能够抵抗常见攻击。

[0049] 椭圆曲线加密是基于有限域上椭圆曲线的代数结构的公钥加密方法，椭圆曲线签名算法与加密算法类似。区块链是比特币中的底层技术，得名于其整个体系是链状结构，由大量的块连接而成链条。区块链中每个区块包含了区块头和区块体两个部分，在区块头中包含了前一个区块的摘要值和当前区块的版本号、时间戳、默克尔根等重要信息。正是由于每个区块头中都包含了前一个区块的信息，链状结构才得以体现，同时也保证了区块的可溯源性。系统的结构如图2所示。主要包含用户身份认证请求、身份认证请求发布、身份验证、唯一标识符生成和数据库更新五个部分。下面将对该身份认证系统的主要技术进行说明。实体包含用户U，认证中心 CA，区块链和互联网服务提供商。

[0050] 假设条件为：1)CA运行私有区块链(私有区块链除CA节点外其他节点只拥有只读权限，无法写入)；2)CA在验证用户签名时受信任；3) CA的数据库中已经存储了用户和服务提供商的信息和公钥，用户信息为用户的个人身份信息如身份证号、姓名，服务提供商信息为统一社会信用代码等唯一标识。

[0051] 流程：

[0052] (1)参数初始化

[0053] 对称加密算法E;椭圆曲线参数(p,a,b,G,n,h);

[0054] p为一个较大的质数,p、a、b确定一条椭圆曲线,G为椭圆曲线的基点,n为点G的阶,协因子h为1;

[0055] CA产生私钥k_A和公钥K_A($K_A=k_A*G$,$k_A\in[1,n-1]$);

[0056] U产生私钥k_U和公钥K_U($K_U=k_U*G$,$k_U\in[1,n-1]$);

[0057] U加密信息前产生随机数$r\in[1,n-1]$,计算点$R=rG$;

[0058] U签名前生成的随机数$k\in[1,n-1]$;

[0059] U的个人信息记为m。

[0060] (2)U利用椭圆曲线加密(ECIES)

[0061] 计算$P=(Px,Py)=r*K_A$,$s=Px$;

[0062] 利用KDF推导加密密钥:$k_E=KDF(s)$;

[0063] 密文$C=E(k_E;m)$;

[0064] 输出(R||C);

[0065] (3)U利用椭圆曲线签名(ECDSA)

[0066] 计算e=Hash((R||C));

[0067] 计算$(x,y)=k*G$;$x'=x \bmod n$;

[0068] 计算$s=k^{-1}(z+x'k_U)$,其中z为e最左边的值;

[0069] 输出(x',s)为签名;

[0070] (4)将(R||C,x',s)作为智能合约的输入,智能合约根据发送者的以太坊地址生成一笔交易T=(addrU,R||C,x',s)广播到区块链上。

[0071] (5)验证节点接收到交易后,对交易进行解析,得到请求验证者的地址以及加密的信息和签名。

[0072] (6)验证发送者签名

[0073] CA先检查x'和s是否落在[1,n-1]上;

[0074] 计算e=Hash((R||C)),取最左边的值为z;

[0075] 计算$w=s^{-1} \bmod n$;

[0076] $u_1=zw \bmod n$,$u_2=rw \bmod n$;

[0077] $(x_1,y_1)=u_1G+u_2K_U$;

[0078] $r\equiv X1 \bmod n$,比较r是否相等来验证签名。

[0079] (7)解密得到发送者信息

[0080] $P=(P_x,P_y)=k_A*R$;令$s=P_x$;

[0081] 利用KDF推导加密密钥:$k_E=KDF(s)$;

[0082] 利用密钥解密得到明文$m=E^{-1}(k_E;C)$。

[0083] (8)验证发送者信息

[0084] 得到信息明文后,CA与数据库中用户的信息进行对比,用户信息和用户公钥都匹配后,该笔交易验证成功,CA签名后写入区块中,等待加入区块链。CA利用GUID为用户生成全局唯一标识符作为用户身份验证成功的ID,签名再利用用户公钥加密后通过安全信道传输给用户,用户收到后就可以解密得到经过CA签名的身份认证ID,便可以进行后续的操作。

[0085] (9)多平台身份验证

[0086] 在用户得到有CA签名的ID后,用户若需要在互联网平台上进行实名认证,则只需要将该ID与该服务提供商的唯一标识符如统一社会信用代码级联,与上述步骤(1)-(8)相似,请求CA提供新的针对该服务提供商的认证证书ID_n,用户在不同的平台将利用不同的ID完成实名认证。

[0087] 安全性分析:

[0088] 下文将从拦截攻击、伪造攻击、修改攻击、中断攻击和重放攻击五种攻击来分析所设计系统的抗攻击能力。

[0089] 拦截攻击:假设攻击者拦截到了实体间传输的信息,由于私钥保管的严密性,以及椭圆曲线加密破解的难度巨大,攻击者基本不可能破解得到传输明文,因此,本系统可以有效抵抗拦截攻击,保证系统的保密性。

[0090] 伪造攻击:由于用户在请求身份认证时是通过以太坊区块链平台进行,智能合约由节点自动触发,合约代码无法修改,并且交易一旦发布也无法修改,攻击者无法在用户发送的请求中插入自己伪造的信息以获得授权,因此,本系统可以有效抵抗伪造攻击,保证系统的完整性。

[0091] 修改攻击:由于本系统中所有传输的信息在发送前都需要进行数字签名,因此,一旦攻击者对信息进行修改,在接收方验证签名的时候很容易发现信息被修改过,从而导致修改攻击的无效,因此,本系统可以有效抵抗修改攻击,保证系统的完整性和保密性。

[0092] 中断攻击:中断攻击最常见的就是利用DOS攻击服务器,使得服务器不能被正常使用,由于本系统的核心是利用区块链,区块链是典型的分布式结构,没有中心服务器,各节点都可以平等处理请求,因此,本系统可以有效抵抗中断攻击,保证系统的可用性。

[0093] 重放攻击:假设攻击者通过智能合约发布的交易得到交易T=(addrU, R||C,x',s),从中解析得到用户输入到智能合约的(R||C,x',s),之后通过自己的以太坊账户激活智能合约以生成交易T=(addrA,R||C,x',s)广播到区块链上。但是,CA节点通过解析得到addrA,与数据库中存储的信息进行比较,由于用户的个人信息和公钥是相互匹配的,而公钥和以太坊地址也是相互对应的(公钥->账户地址),CA很容易能发现攻击者发送的信息有误,无法通过验证。因此,本系统可以有效抵抗重放攻击。

[0094] 实施例一:

[0095] 用户在使用需要进行实名身份认证的互联网服务时,需要分为两步,首先是完成在认证中心(CA)的认证和记录保存,再是完成企业所需的认证。

[0096] 所涉及的实体:用户、服务提供商、认证中心(利用以太坊区块链工作)。

[0097] 假设前提:用户拥有CA公钥,用户的身份信息已在CA线下注册过了,CA的数据库中存有用户的身份信息和公钥。CA在验证过程中是受信任的,但是不排除CA存在包庇做出违规行为的用户的可能,因此需要引入区块链技术。

[0098] 先验知识:用户的由个人选择的PIN生成私钥,私钥计算得到公钥后存储在CA的数据库中,通过公钥可以计算得到以太坊地址。本专利使用椭圆曲线算法来完成加解密和签名过程。

[0099] 所设计系统的实施例子如图3所示。

[0100] ①+②:用户将自己的身份证号和姓名等个人信息连同公钥以JASON 格式保存,利

用CA的公钥加密后,用自己的私钥签名,通过SSL/TSL(SSL 协议位于TCP/IP协议与各种应用层协议之间,为数据通讯提供安全支持) 传输给智能合约节点,激活智能合约。

[0101] ③:智能合约被激活后,根据其提供的信息生成交易,广播给账户节点(外部节点),节点接收到广播后,对交易内容进行解析,首先验证用户签名是否正确,再利用自己的私钥对加密信息进行解密,得到JASON格式的消息明文,将其于数据库中存储的内容进行对比,如果信息匹配,则该笔交易验证成功,CA对验证成功的交易签名后放入区块中等待上链。

[0102] ④:CA为通过验证的用户生成一个唯一标识符IDr,作为实名认证成功的证明,在数据库中进行存储后,利用自己的私钥进行签名,再利用用户公钥加密后通过安全信道传输给用户,用户便可以利用该IDr进行后续的操作。该IDr需要用户妥善保存。

[0103] 以上为用户需要执行的实名认证过程。

[0104] ⑤:用户在首次使用需要真实身份认证的互联网服务时,服务提供商向用户请求证书。

[0105] ⑥+⑦:用户通过带有CA签名的IDr和该服务提供商的唯一标识IDs (如统一社会信用代码)进行级联得到(IDr||IDs)后加密并签名,类似步骤①发送给智能合约节点激活智能合约。

[0106] ⑧:智能合约将输入信息生成交易后进行广播,外部节点接收到交易后,对交易进行解析验证,主要验证用户所提供的(IDr||IDs)中IDr的 CA的签名是否有效,剩下操作类似步骤③。

[0107] ⑨:验证通过后则生成针对该服务提供商的唯一标识符IDc,对应更新数据库后,签名并加密发送给用户。该标识符需要在区块链上进行记录。

[0108] ⑩:用户将该IDc发送给服务提供商,服务提供商在收到IDc后验证 CA的签名是否有效。

[0109] 通过该系统,用户可以实现仅通过一次实名认证,就可以在各大需要实名认证的互联网平台上完成认证,并且在各平台提交的认证结果具有不可连接性。

[0110] 综上,本发明中通过区块链进行认证和管理,较大程度地利用了区块链的优势来解决当今互联网环境存在的问题,提高互联网环境的安全,保护用户的个人身份隐私,避免由于互联网平台的漏洞和用户数据的不当使用对用户的权益造成损害。

[0111] 以上内容是结合具体的优选实施方式对本发明所作的进一步详细说明,不能认定本发明的具体实施只局限于这些说明。对于本发明所属技术领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干简单推演或替换,都应当视为属于本发明的保护范围。

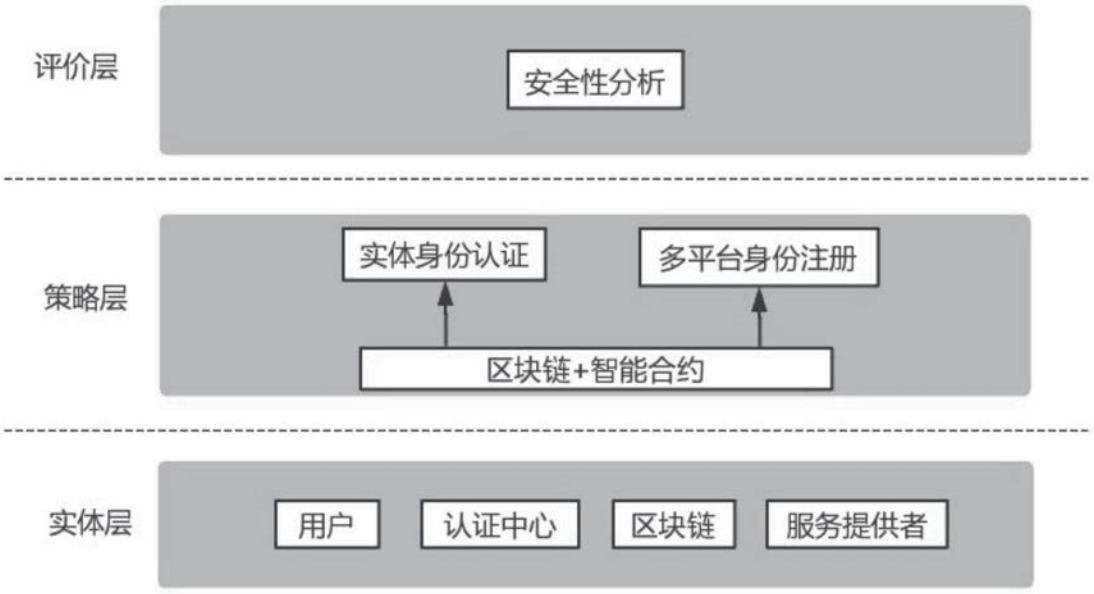

评价层
安全性分析
策略层
实体身份认证
多平台身份注册
区块链+智能合约
实体层
用户
认证中心
区块链
服务提供者

图1

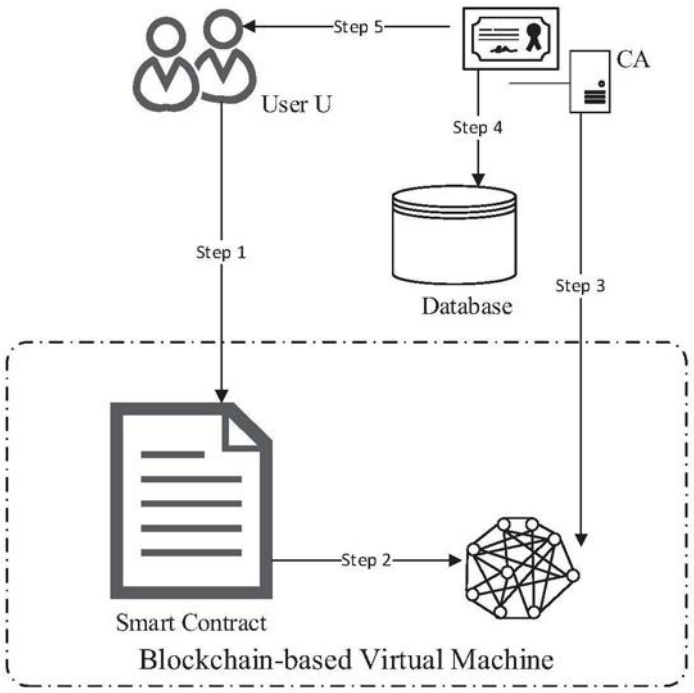

Step 5
CA
User U
Step 4
Step 1
Database
Step 3
Step 2
Smart Contract
Blockchain-based Virtual Machine

图2

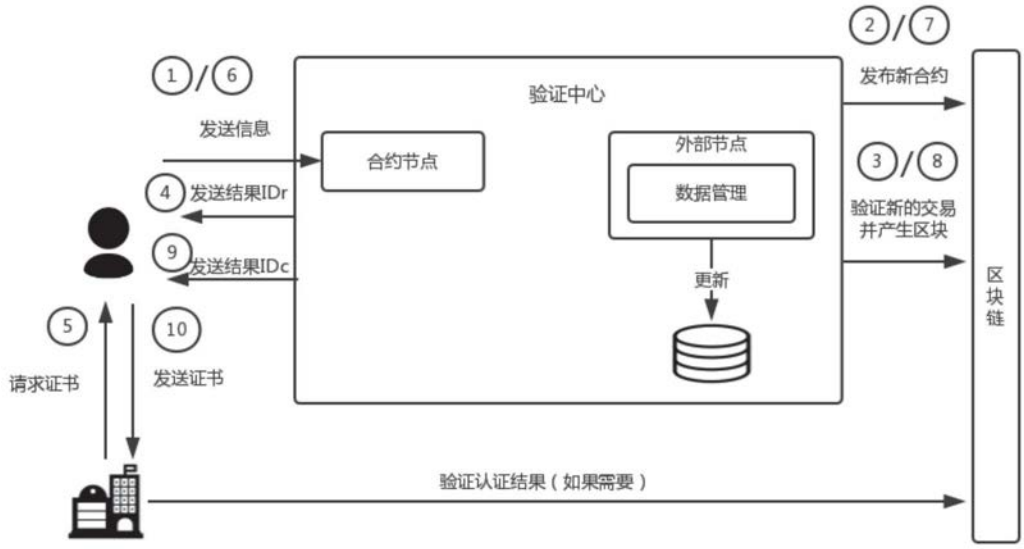

1/6
发送信息
4 发送结果IDr
9 发送结果IDc
5
请求证书
10
发送证书
验证中心
合约节点
外部节点
数据管理
更新
2/7
发布新合约
3/8
验证新的交易
并产生区块
区块链
验证认证结果（如果需要）

图3