(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 107181765 A
(43)申请公布日 2017.09.19

(21)申请号 201710610171.X

(22)申请日 2017.07.25

(71)申请人 光载无限(北京)科技有限公司
地址 100036 北京市海淀区西八里庄北里56号院1号写字楼五层

(72)发明人 焦继佩

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
G06F 21/62(2013.01)

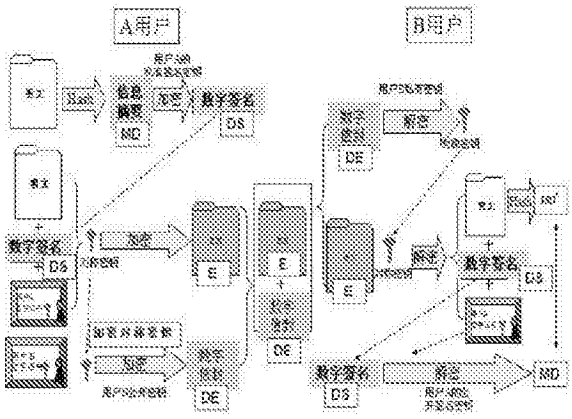
权利要求书2页 说明书5页 附图2页

(54)发明名称

基于区块链技术的网络数字身份认证方法

(57)摘要

本发明是一种基于区块链技术的网络数字身份认证方法，包括1)用户注册，采用vLink protocol议进行身份认证服务，如果合法则上传区块链，区块链将该用户信息广播至全网，每一个节点把该用户信息加入到对应的区块，区块之间彼此互为验证；2)获得用户的信息，通过vKey属性授权服务进行查询用户信息，返回用户的用户名，性别，年龄信息的同时返回一个特定的openid，来区分不同的用户；3)在使用上述块链技术的数字身份认证过程中，数据经过签名处理。本发明通过将用户个人数据存储在区块链从根源上解决了现在出现的信息泄露、网络诈骗行为，保证了数据的安全性；数据传输过程中采用数字签名处理，使敏感信息在数字签名的传输中不被篡改。



CN 107181765 A

1.一种基于区块链技术的网络数字身份认证方法,其特征在于,所述的方法包括:

1)用户注册,填写完整的个人信息,采用vLink protocol议进行身份认证服务,如果合法则上传区块链,区块链将该用户信息广播至全网,每一个节点把该用户信息加入到对应的区块,区块之间彼此互为验证;如果不合法则注册失败;

2)获得用户的信息,通过vKey属性授权服务进行查询用户信息,返回用户的用户名,性别,年龄信息的同时返回一个openid,每一个用户被标示一个特定的openid,来区分不同的用户;

3)在使用上述块链技术的数字身份认证过程中,数据经过签名处理。

2.根据权利要求1所述的网络数字身份认证方法,其特征在于,所述的数据签名处理方法如下:

1)发方A将原文信息进行哈希运算,得一哈希值即数字摘要MD;

2)发方A用自己的私钥PVA,采用非对称RSA算法,对数字摘要MD进行加密,即得数字签名DS;

3)发方A用对称算法DES的对称密钥SK对原文信息、数字签名SD及发方A证书的公钥PBA采用对称算法加密,得加密信息E;

4)发方用收方B的公钥PBB,采用RSA算法对对称密钥SK加密,形成数字信封DE,就好像将对称密钥SK装到了一个用收方公钥加密的信封里;

5)发方A将加密信息E和数字信封DE一起发送给收方B;

6)收方B接受到数字信封DE后,首先用自己的私钥PVB解密数字信封,取出对称密钥SK;

7)收方B用对称密钥SK通过DES算法解密加密信息E,还原出原文信息、数字签名SD及发方A证书的公钥PBA;

8)收方B验证数字签名,先用发方A的公钥解密数字签名得数字摘要MD;

9)收方B同时将原文信息用同样的哈希运算,求得一个新的数字摘要MD';

10)将两个数字摘要MD和MD'进行比较,验证原文是否被修改;

如果二者相等,说明数据没有被篡改,是保密传输的,签名是真实的,则同意该数据传输过去;否则拒绝该签名,数据传输失败。

3.根据权利要求2所述的网络数字身份认证方法,其特征在于,所述用户包括自然人用户,法人用户和设备用户;所提供的服务包括身份认证服务、属性授权服务、签名服务、授信第三方“他证”、用户“自证”和公众“共证”。

4.根据权利要求2所述的网络数字身份认证方法,其特征在于,所述身份认证服务采用vLink protocol协议进行身份认证服务,确保合法的用户加入;一个用户经过验证后链接到区块链中永久存储;所记录信息字段与生成时间戳关联并对应,具有唯一性和不可篡改性;所述属性授权服务在身份认证通过之后提供,授权包括姓名和性别的属性信息;签名服务根据数字签名对该用户信息进行加密传输,确保其安全性。

5.根据权利要求4所述的网络数字身份认证方法,其特征在于,所述区块链采用Smart Data Engine,在比特币POW的基础上采用动态非线性工作量证明机制,调整每个矿工获选为验证者的困难度,避免趋向独占验证的可能性,解决了51%攻击的问题,缩短了平均区块的确认时间,大幅度提升了每秒运行的性能。

6.根据权利要求5所述的网络数字身份认证方法,其特征在于,使用Personal Data

Storage提供身份注册服务,签名/查询服务,属性管理/授权服务,身份恢复服务,属性见证服务;通过Block Chain基础能力,以区块链为核心,提供身份日志,属性日志,签名信息服务。

7.根据权利要求6所述的网络数字身份认证方法,其特征在于,所述授信第三方“他证”是在使用基于区块链技术的数字身份认证的基础上,提供第三方登录的API,基于区块链技术的数字身份认证中心将会返回一个openid以标示该用户的唯一性;所述用户“自证”是采用vLink protocol协议进行用户自证,注册之前先查询区块链中是否有该用户,如果不存在则可以注册,如果存在则注册失败,提示该用户已注册;所述公众“共证”是通过区块链的开源可共享,使分布式网络上其他用户均可参与到整个系统的运作,每个参与维护节点都能复制获得一份完整数据库的拷贝,从而对其他用户进行确认。

基于区块链技术的网络数字身份认证方法

技术领域

[0001] 本发明涉及计算机网络技术，尤其是涉及网络数字身份管理体系，完成对联网设备的注册、登录、认证和传输等过程。

背景技术

[0002] 当我们使用一些联网设备进行更加方便快捷的操作时，都需要经过各种网络身份的注册、登录、认证和传输等过程。现在我们的网络身份都已经基本实名制，其中包含了我们重要的基本信息。

[0003] 近几年出现的网络诈骗、侵权等与身份相关的违法行为，急需构建一套完整可行的数字身份管理系统，来保护公民的信息和财产安全。类似一些网络交易应用场景的背后都有一个实体，如何让其与网络身份对应是数字身份管理体系的范畴，没有好的解决办法，就会出现一系列的与网络身份有关的问题。

[0004] 身份认证：身份认证也称为“身份验证”或“身份鉴别”，是指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，进而使计算机和网络系统的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。

[0005] 区块链是指以去中心化和去信任的方式集体维护一个可靠数据库的技术方案，其交易过程如下：

第一步：所有者a利用她的私钥对前一次交易和下一位所有者b签署一个数字签名，并将这个签名附加在这枚货币的末尾，制作成交易单；

第二步：a将交易单广播至全网，比特币就发送给了b，每个节点都将收到的交易信息纳入一个区块；

第三步：每个节点通过解一道数学题，从而去获得创建新区块的权利，并争取得到比特币的奖励(新的比特币会在此过程中产生)；

第四步：当一个节点找到解时，它就向全网广播该区块记录的所有盖时间戳交易，并对全网其他节点核对；

第五步：全网其他节点核对该区块记账的正确性，没有错误后他们将该合法区域之后竞争下一个区块，这样就形成了一个合法记账的区块链。

[0006] 如何建立一种基于区块链技术的数据平台，从根源上解决了信息泄露、网络诈骗行为，保证数据的安全性是当务之急。

发明内容

[0007] 本发明的目的是提出一种基于区块链技术的数字身份认证体系，给不同应用提供数据存储认证等服务，其融合了区块链，有效保证了信息的安全性。可用于客户端等用户信息存储等业务。

[0008] 为了实现本发明的目的，采用以下技术方案：

一种基于区块链技术的网络数字身份认证方法，其特征在于，所述的方法包括：

1)用户注册，填写完整的个人信息，采用vLink protocol议进行身份认证服务，如果合法则上传区块链，区块链将该用户信息广播至全网，每一个节点把该用户信息加入到对应的区块，区块之间彼此互为验证；如果不合法则注册失败；

2)获得用户的信息，通过vKey属性授权服务进行查询用户信息，返回用户的用户名，性别，年龄信息的同时返回一个openid，每一个用户被标示一个特定的openid，来区分不同的用户；

3)在使用上述块链技术的数字身份认证过程中，数据经过签名处理。

[0009] 所述的数据签名绝具体处理方法如下：

1)发方A将原文信息进行哈希运算，得一哈希值即数字摘要MD；

2)发方A用自己的私钥PVA，采用非对称RSA算法，对数字摘要MD进行加密，即得数字签名DS；

3)发方A用对称算法DES的对称密钥SK对原文信息、数字签名SD及发方A证书的公钥PBA采用对称算法加密，得加密信息E；

4)发方用收方B的公钥PBB，采用RSA算法对对称密钥SK加密，形成数字信封DE，就好像将对称密钥SK装到了一个用收方公钥加密的信封里；

5)发方A将加密信息E和数字信封DE一起发送给收方B；

6)收方B接受到数字信封DE后，首先用自己的私钥PVB解密数字信封，取出对称密钥SK；

7)收方B用对称密钥SK通过DES算法解密加密信息E，还原出原文信息、数字签名SD及发方A证书的公钥PBA；

8)收方B验证数字签名，先用发方A的公钥解密数字签名得数字摘要MD；

9)收方B同时将原文信息用同样的哈希运算，求得一个新的数字摘要MD'；

10)将两个数字摘要MD和MD'进行比较，验证原文是否被修改。如果二者相等，说明数据没有被篡改，是保密传输的，签名是真实的，则同意该数据传输过去；否则拒绝该签名，数据传输失败。

[0010] 所述用户包括自然人用户，法人用户和设备用户；所提供的服务包括身份认证服务、属性授权服务、签名服务、授信第三方“他证”、用户“自证”和公众“共证”。

[0011] 所述身份认证服务采用vLink protocol协议进行身份认证服务，确保合法的用户加入；一个用户经过验证后链接到区块链中永久存储；所记录信息字段与生成时间戳关联并对应，具有唯一性和不可篡改性；所述属性授权服务在身份认证通过之后提供，授权包括姓名和性别的属性信息；签名服务根据数字签名对该用户信息进行加密传输，确保其安全性。

[0012] 所述区块链采用Smart Data Engine，在比特币POW的基础上采用动态非线性工作量证明机制，调整每个矿工获选为验证者的困难度，避免趋向独占验证的可能性，解决了51%攻击的问题，缩短了平均区块的确认时间，大幅度提升了每秒运行的性能。

[0013] 使用Personal Data Storage提供身份注册服务，签名/查询服务，属性管理/授权服务，身份恢复服务，属性见证服务；通过Block Chain基础能力，以区块链为核心，提供身份日志，属性日志，签名信息服务。

[0014] 所述授信第三方“他证”是在使用基于区块链技术的数字身份认证的基础上，提供

第三方登录的API，基于区块链技术的数字身份认证中心将会返回一个openid以标示该用户的唯一性；所述用户“自证”是采用vLink protocol协议进行用户自证，注册之前先查询区块链中是否有该用户，如果不存在则可以注册，如果存在则注册失败，提示该用户已注册；所述公众“共证”是通过区块链的开源可共享，使分布式网络上其他用户均可参与到整个系统的运作，每个参与维护节点都能复制获得一份完整数据库的拷贝，从而对其他用户进行确认。

[0015] 本发明的数字身份认证体系通过将用户个人数据存储在区块链而不是服务器，在没有个人授权的前提下，任何机构或个人不能获取本人的数据，从根源上解决了现在出现的信息泄露、网络诈骗行为，保证了数据的安全性；

数据传输过程中采用数字签名处理，使敏感信息在数字签名的传输中不被篡改，未经认证和授权的人，看不见原数据，起到了在数字签名传输中对敏感数据的保密作用。

附图说明

[0016] 图1是基于区块链技术的数字身份认证体系架构；

图2是本发明的数据加密和身份认证流程。

具体实施方式

[0017] 为使本发明的目的、技术方案和优点更加清楚明白，以下结合附图和具体实施例，对本发明进一步详细说明。

[0018] 图1是基于区块链技术的数字身份认证主要架构，如图所示。基于区块链技术的数字身份认证主要针对自然人用户，法人用户，设备用户三大类，在我们的分布式网络上记录了所有的用户资料，目前主要提供身份认证服务，属性授权服务，签名服务，授信第三方“他证”，用户“自证”，公众“共证”等。该认证中心还整合了区块链的身份日志，属性日志，签名信息等功能。

[0019] 身份认证服务：采用vLink protocol协议进行身份认证服务，确保只有合法的用户才能加进来；一个用户经过验证后链接到区块链中，就会永久的存储；在区块链上的数据库是不可摧毁的，所记录信息字段是与生成时间戳关联并对应，就具有唯一性，不可篡改性，确保身份的真实性，唯一性。

[0020] 属性授权服务：身份认证通过之后，可以授权一些属性信息，比如：姓名，性别信息等。有助于应用层得到更多的数据信息。

[0021] 签名服务：根据数字签名对该用户信息进行加密传输，确保其安全性。

[0022] Smart Data Engine：特指CPOW共识，该共识是在比特币POW的基础上采用动态非线性工作量证明机制，调整每个矿工获选为验证者的困难度，避免趋向独占验证的可能性，解决了51%攻击的问题。而且缩短了平均区块的确认时间，目标区块创建时间为15s，而比特币的平均区块创建时间是10分钟，大幅度提升了每秒运行的性能，相当于原本比特币每秒交易的40倍。

[0023] Personal Data Storage：提供身份注册服务，签名/查询服务，属性管理/授权服务，身份恢复服务，属性见证服务。

[0024] Block Chain基础能力：以区块链为核心，提供身份日志，属性日志，签名信息等服

务。

[0025] 授信第三方“他证”:如果使用基于区块链技术的数字身份认证,将提供第三方登录的API,如果使用该服务,基于区块链技术的数字身份认证中心,将会返回一个openid以标示该用户的唯一性。

[0026] 用户“自证”:采用vLink protocol协议进行用户自证,注册之前先查询区块链中是否有该用户,如果不存在则可以注册,如果存在则注册失败,提示该用户已注册。

[0027] 公众“共证”:区块链的开源可共享,使分布式网络上其他用户均可参与到整个系统的运作,每个参与维护节点都能复制获得一份完整数据库的拷贝,从而对其他用户进行确认。

[0028] 图2是本发明的数据加密和身份认证流程,其运行机制如下:1、首先,用户需要完成注册,把个人信息完整的填写出来,采用vLink protocol协议进行身份认证服务,如果合法则上传区块链,区块链将该用户信息,广播至全网,每一个节点将会把该用户信息加入到对应的区块。如果不合法则注册失败。由于区块之间彼此互为验证,所以不可能篡改某个信息块的数据。

[0029] 2、如果想要得到用户的信息,则可通过vKey属性授权服务进行查询用户信息,将会返回用户的用户名,性别,年龄等信息,同时返回一个openid,每一个用户被标示一个特定的openid,来区分不同的用户,有助于应用来使用。

[0030] 3、基于区块链技术的数字身份认证在使用的过程中,数据都是经过签名处理的,其详细过程如下:

1)发方A将原文信息进行哈希运算,得一哈希值即数字摘要MD;

2)发方A用自己的私钥PVA,采用非对称RSA算法,对数字摘要MD进行加密,即得数字签名DS;

3)发方A用对称算法DES的对称密钥SK对原文信息、数字签名SD及发方A证书的公钥PBA采用对称算法加密,得加密信息E;

4)发方用收方B的公钥PBB,采用RSA算法对对称密钥SK加密,形成数字信封DE,就好像将对称密钥SK装到了一个用收方公钥加密的信封里;

5)发方A将加密信息E和数字信封DE一起发送给收方B;

6)收方B接受到数字信封DE后,首先用自己的私钥PVB解密数字信封,取出对称密钥SK;

7)收方B用对称密钥SK通过DES算法解密加密信息E,还原出原文信息、数字签名SD及发方A证书的公钥PBA;

8)收方B验证数字签名,先用发方A的公钥解密数字签名得数字摘要MD;

9)收方B同时将原文信息用同样的哈希运算,求得一个新的数字摘要MD’;

10)将两个数字摘要MD和MD’进行比较,验证原文是否被修改。如果二者相等,说明数据没有被篡改,是保密传输的,签名是真实的,则同意该数据传输过去;否则拒绝该签名,数据传输失败。

[0031] 基于区块链技术建立一套数字身份认证系统,来确保数据的安全性,这个系统提供了供第三方使用的sdk来对用户信息进行处理,用户信息存储在区块链而不是服务器,避免了数据泄漏的发生,有利于保护用户隐私。

[0032] 首先,用户的个人信息得到了保障,不会那么轻易的出现信息泄露的问题;其次,

保证了信息的真实性、不可随意更改性;数据分布在很多区块链中,可以防止腐败,而且你的身份数据几乎不可能被篡改。

[0033] 以上所述的具体实施例,对本发明的目的、技术方案和有益效果进行了进一步的详细说明,所应理解的是,以上所述仅为本发明的具体实施例而已,并不用于限制本发明,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

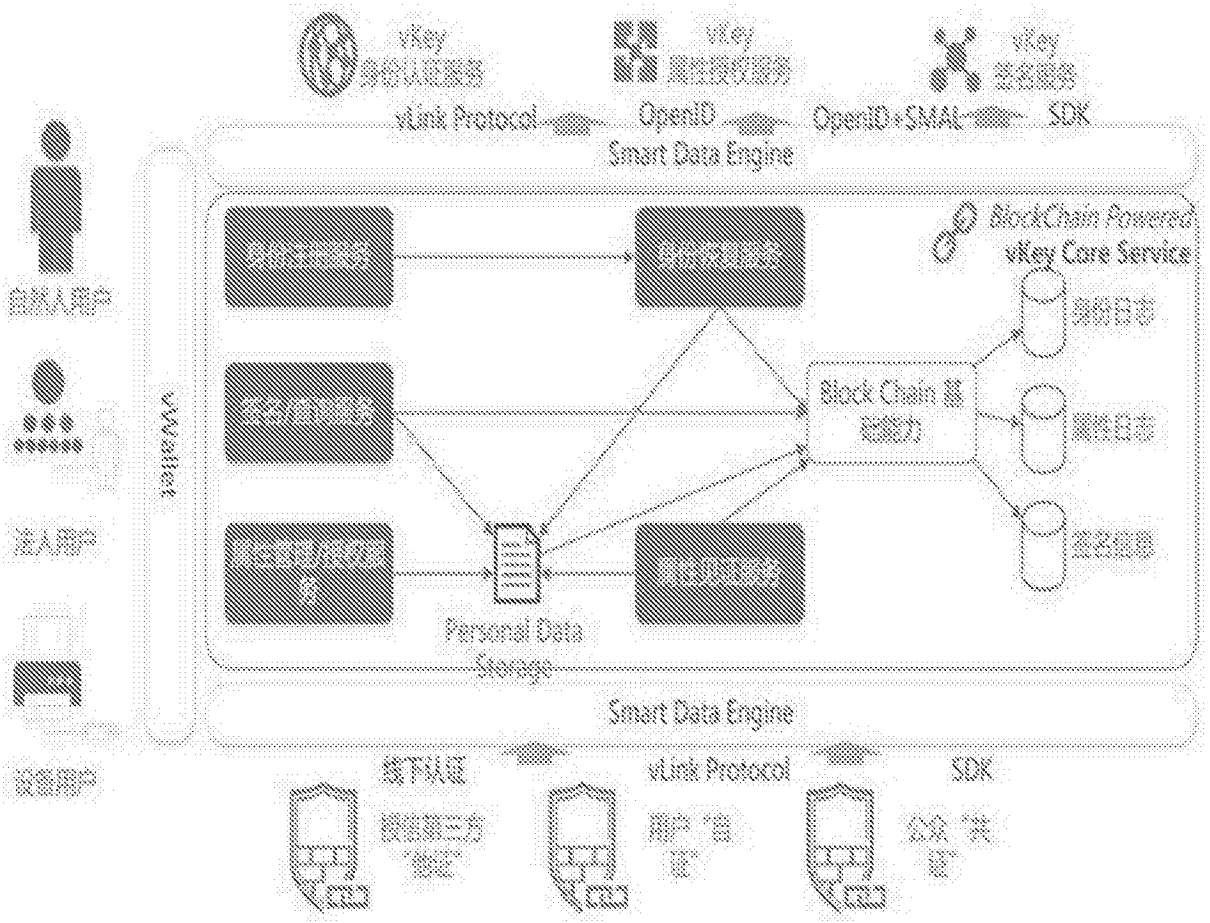

vKey
vLink Protocol
OpenID
OpenID+SMAL
SDK
Smart Data Engine
BlockChain Powered
vKey Core Service
Block Chain
Personal Data
Storage
vWallet
Smart Data Engine
vLink Protocol
SDK

图1

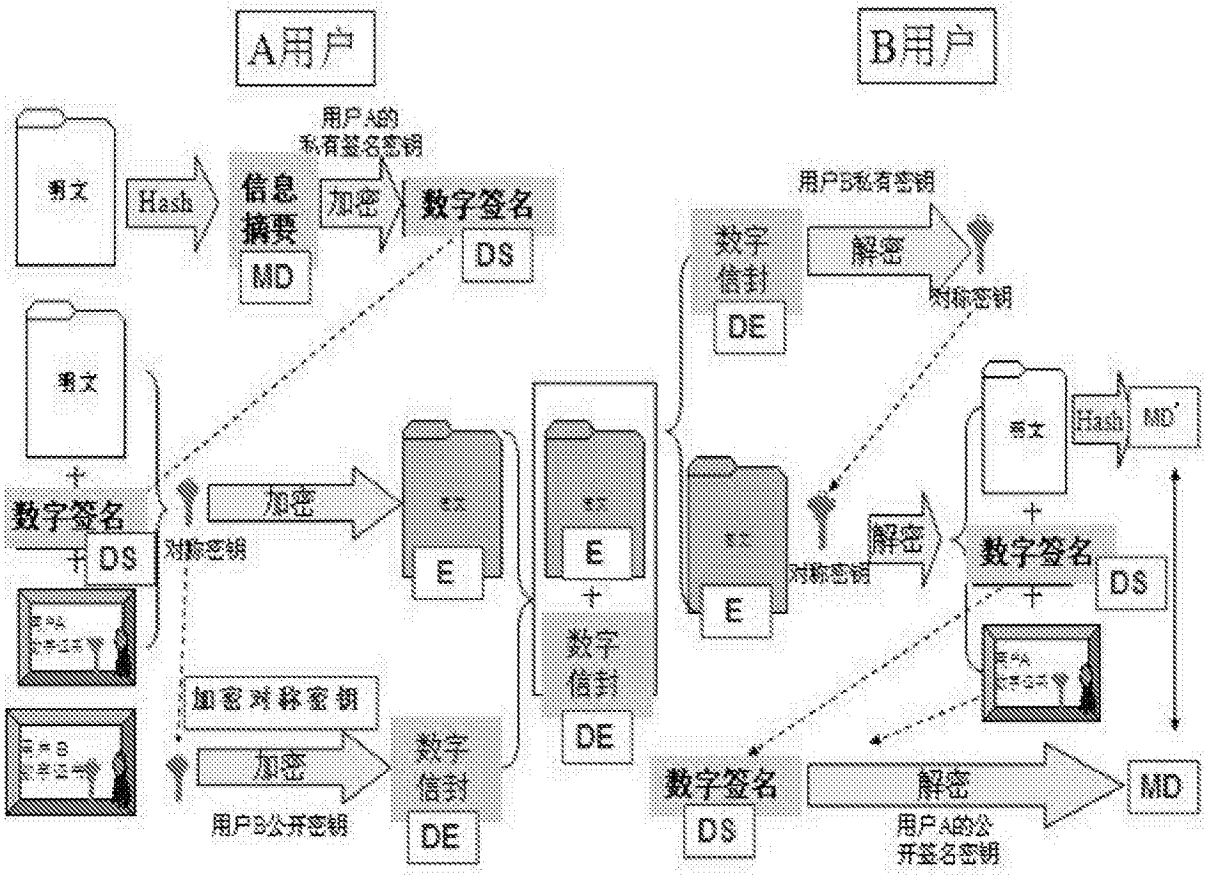

A用户
B用户
明文
Hash
信息摘要
MD
用户A的私有签名密钥
加密
数字签名
DS
数字信封
DE
加密对称密钥
用户B公开密钥
对称密钥
E
用户B私有密钥
解密
用户A的公开签名密钥
MD'

图2