(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 108377189 A
(43)申请公布日 2018.08.07

(21)申请号 201810437217.7

(22)申请日 2018.05.09

(71)申请人 深圳壹账通智能科技有限公司
地址 518000 广东省深圳市前海深港合作区前湾一路1号A栋201室(入驻深圳市前海商务秘书有限公司)

(72)发明人 贾牧 谢丹力 陆陈一帆

(74)专利代理机构 深圳众鼎专利商标代理事务所(普通合伙) 44325
代理人 谭果林

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

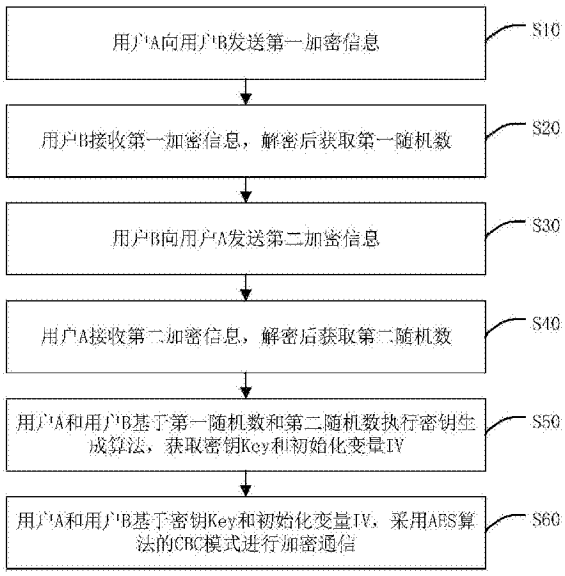
权利要求书3页 说明书12页 附图6页

(54)发明名称

区块链上用户通信加密方法、装置、终端设备及存储介质

(57)摘要

本发明公开了一种区块链上用户通信加密方法、装置、终端设备及存储介质。该区块链上用户通信方法,包括:用户A向用户B发送第一加密信息;用户B接收所述第一加密信息,解密后获取第一随机数;用户B向用户A发送第二加密信息;用户A接收所述第二加密信息,解密后获取第二随机数;用户A和用户B基于所述第一随机数和所述第二随机数执行密钥生成算法,获取密钥Key和初始化变量IV;用户A和用户B基于所述密钥Key和所述初始化变量IV,采用AES算法的CBC模式进行加密通信。采用该区块链上用户通信加密方法能够保证区块链系统上用户进行点对点通信的安全。



CN 108377189 A

1.一种区块链上用户通信加密方法,其特征在于,包括:

用户A向用户B发送第一加密信息;

用户B接收所述第一加密信息,解密后获取第一随机数;

用户B向用户A发送第二加密信息;

用户A接收所述第二加密信息,解密后获取第二随机数;

用户A和用户B基于所述第一随机数和所述第二随机数执行密钥生成算法,获取密钥Key和初始化变量IV;

用户A和用户B基于所述密钥Key和所述初始化变量IV,采用AES算法的CBC模式进行加密通信。

2.根据权利要求1所述的区块链上用户通信加密方法,其特征在于,所述用户A向用户B发送第一加密信息,包括:

用户A从用户B的用户证书中获取第二公钥;

用户A生成第一随机数,采用所述第二公钥加密所述第一随机数,获取所述第一加密信息;

用户A通过区块链系统向用户B发送所述第一加密信息;

所述用户B向用户A发送第二加密信息,包括:

用户B从用户A的用户证书中获取第一公钥;

用户B生成第二随机数,采用所述第一公钥加密所述第二随机数,获取所述第二加密信息;

用户B通过区块链系统向用户A发送所述第二加密信息。

3.根据权利要求2所述的区块链上用户通信加密方法,其特征在于,所述用户B接收所述第一加密信息,解密后获取第一随机数,包括:

用户B通过区块链系统接收用户A发送的所述第一加密信息;

用户B采用与所述第二公钥相对应的第二私钥解密所述第一加密信息,获取所述第一随机数;

所述用户A接收所述第二加密信息,解密后获取第二随机数,包括:

用户A通过区块链系统接收用户B发送的所述第二加密信息;

用户A采用与所述第一公钥相对应的第一私钥解密所述第二加密信息,获取所述第二随机数。

4.根据权利要求1所述的区块链上用户通信加密方法,其特征在于,在所述用户A向用户B发送第一加密信息的步骤之前,所述区块链上用户通信加密方法还包括:

用户A和用户B预先查询各自的本地数据库;

若所述本地数据库中存在所述密钥Key和所述初始化变量IV,则查看所述密钥Key和所述初始化变量IV的创建时间;

若所述创建时间未超过预设有效时间,则采用已存在的所述密钥Key和所述初始化变量IV,采用所述AES算法的CBC模式进行加密通信。

5.根据权利要求1所述的区块链上用户通信加密方法,其特征在于,所述密钥生成算法为:

C(0)=Hash(random1)

$C(n)=HMAC_{C(n-1)}(Hash(random2))$

$Key=HMAC_{Hash(random1||random2)}(C0+C1)$

$IV=HMAC_{Hash(random1||random2)}(C0+C2)$

其中，random1表示第一随机数，random2表示第二随机数，n为大于0的正整数，Hash表示哈希函数，算法采用SHA256算法，HMAC是指与密钥相关的哈希运算，算法采用SHA256算法，||表示连接操作。

6.根据权利要求1所述的区块链上用户通信加密方法，其特征在于，所述用户A和用户B基于所述密钥Key和所述初始化变量IV，采用AES算法的CBC模式进行通信加密，包括：

用户A以键值对的方式将数据K:V写到区块链上，其中K代表键，V代表值；

用户A基于所述密钥Key和所述初始化变量IV采用AES算法的CBC模式对K进行加密，获取KC，KC＝AES_CBC(K)；

用户A基于所述密钥Key和所述初始化变量IV采用AES算法的CBC模式对V进行加密，获取VC，VC＝AES_CBC(V)；

用户A将数据{KC:VC+IV}写到区块链上；

用户B在区块链上读取KC，根据KC获取VC和所述初始化变量IV；

用户B基于所述密钥Key和所述初始化变量IV采用AES算法的CBC模式对KC进行解密，获取K，K＝AES_CBC(KC)；

用户B基于所述密钥Key和所述初始化变量IV采用AES算法的CBC模式对VC进行解密，获取V，V＝AES_CBC(VC)；

用户B获取所述数据K:V。

7.一种区块链上用户通信加密装置，其特征在于，包括：

第一加密信息发送模块，用于用户A向用户B发送第一加密信息；

第一随机数获取模块，用于用户B接收所述第一加密信息，解密后获取第一随机数；

第二加密信息发送模块，用于用户B向用户A发送第二加密信息；

第二随机数获取模块，用于用户A接收所述第二加密信息，解密后获取第二随机数；

密钥和初始化变量获取模块，用于用户A和用户B基于所述第一随机数和所述第二随机数执行密钥生成算法，获取密钥Key和初始化变量IV；

加密通信模块，用于用户A和用户B基于所述密钥Key和所述初始化变量IV，采用AES算法的CBC模式进行加密通信。

8.根据权利要求7所述的区块链上用户通信加密装置，其特征在于，所述第一加密信息发送模块，包括：

第二公钥获取单元，用于用户A从用户B的用户证书中获取第二公钥；

第一加密信息获取单元，用于用户A生成第一随机数，采用所述第二公钥加密所述第一随机数，获取所述第一加密信息；

第一加密信息发送单元，用于用户A通过区块链向用户B发送所述第一加密信息；

所述第二加密信息发送模块，包括：

第一公钥获取单元，用于用户B从用户A的用户证书中获取第一公钥；

第二加密信息获取单元，用于用户B生成第二随机数，采用所述第一公钥加密所述第二随机数，获取所述第二加密信息；

第二加密信息发送单元，用于用户B通过区块链向用户A发送所述第二加密信息。

9.一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求1至6任一项所述区块链上用户通信加密方法的步骤。

10.一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至6任一项所述区块链上用户通信加密方法的步骤。

区块链上用户通信加密方法、装置、终端设备及存储介质

技术领域

[0001] 本发明涉及区块链应用领域，尤其涉及一种区块链上用户通信加密方法、装置、终端设备及存储介质。

背景技术

[0002] 区块链系统上用户在进行点对点通信时，由于区块链系统上的数据都是共享的，区块链系统上任一用户都可以获取区块链系统上用户进行点对点通信的通信内容，无法保证区块链系统上用户进行点对点通信的安全。

发明内容

[0003] 本发明实施例提供一种区块链上用户通信加密方法、装置、终端设备及存储介质，以解决当前区块链系统上用户进行点对点通信不安全的问题。

[0004] 第一方面，本发明实施例提供一种区块链上用户通信加密方法，包括：

[0005] 用户A向用户B发送第一加密信息；

[0006] 用户B接收所述第一加密信息，解密后获取第一随机数；

[0007] 用户B向用户A发送第二加密信息；

[0008] 用户A接收所述第二加密信息，解密后获取第二随机数；

[0009] 用户A和用户B基于所述第一随机数和所述第二随机数执行密钥生成算法，获取密钥Key和初始化变量IV；

[0010] 用户A和用户B基于所述密钥Key和所述初始化变量IV，采用AES算法的CBC模式进行加密通信。

[0011] 第二方面，本发明实施例提供一种区块链上用户通信加密装置，包括：

[0012] 第一加密信息发送模块，用于用户A向用户B发送第一加密信息；

[0013] 第一随机数获取模块，用于用户B接收所述第一加密信息，解密后获取第一随机数；

[0014] 第二加密信息发送模块，用于用户B向用户A发送第二加密信息；

[0015] 第二随机数获取模块，用于用户A接收所述第二加密信息，解密后获取第二随机数；

[0016] 密钥和初始化变量获取模块，用于用户A和用户B基于所述第一随机数和所述第二随机数执行密钥生成算法，获取密钥Key和初始化变量IV；

[0017] 加密通信模块，用于用户A和用户B基于所述密钥Key和所述初始化变量IV，采用AES算法的CBC模式进行加密通信。

[0018] 第三方面，本发明实施例提供一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现所述区块链上用户通信加密方法的步骤。

[0019] 第四方面，本发明实施例提供一种计算机可读存储介质，所述计算机可读存储介

质存储有计算机程序，所述计算机程序被处理器执行时实现所述区块链上用户通信加密方法的步骤。

[0020] 本发明实施例所提供的区块链上用户通信加密方法、装置、终端设备及存储介质中，首先用户A向用户B发送第一加密信息，用户B接收第一加密信息，解密后获取第一随机数；用户B向用户A发送第二加密信息，用户A接收第二加密信息，解密后获取第二随机数，用户A和用户B采用加解密随机数的方式相互获取对方发送的第一随机数和第二随机数，为后续的加密通信提供了基础。然后用户A和用户B基于第一随机数和第二随机数执行密钥生成算法，获取密钥Key和初始化变量IV，生成的密钥Key和初始化变量IV是用户A和用户B共同协商获取的，该密钥Key和初始化变量IV是通过哈希算法获取，具有数据不可逆的特点，安全性高，为实现用户A和用户B之间的通信加密提供了必要的基础。最后用户A和用户B基于密钥Key和初始化变量IV，采用AES算法的CBC模式进行加密通信，使得第三方(除用户A和用户B以外的区块链上用户)在没有密钥Key和初始化变量IV的情况下不能够获取用户A和用户B的通信内容，确保了区块链上任意两个用户进行点对点通信时通信内容的安全。

附图说明

[0021] 为了更清楚地说明本发明实施例的技术方案，下面将对本发明实施例的描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0022] 图1是本发明实施例1中区块链上用户通信加密方法的一流程图。

[0023] 图2是图1中步骤S10的一具体流程图。

[0024] 图3是图2中步骤S20的一具体流程图。

[0025] 图4是图1中步骤S30的一具体流程图。

[0026] 图5是图1中步骤S40的一具体流程图。

[0027] 图6是图1中步骤S10之前的一具体流程图。

[0028] 图7是图1中步骤S60的一具体流程图。

[0029] 图8是本发明实施例2中区块链上用户通信加密装置的一原理框图。

[0030] 图9是本发明实施例4中终端设备的一示意图。

具体实施方式

[0031] 下面将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，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0032] 实施例1

[0033] 图1示出本实施例中区块链上用户通信加密方法的一流程图。该区块链上用户通信加密方法可应用在以区块链为技术基础的应用系统上，用于在区块链系统上用户进行点对点通信时对通信内容进行加密，实现区块链系统上用户通信加密的功能。如图1所示，该区块链上用户通信加密方法包括如下步骤：

[0034] S10:用户A向用户B发送第一加密信息。

[0035] 其中,用户A和用户B是指区块链系统上任意的两个用户。本实施例中区块链上的用户应理解为在区块链系统上的各个用户节点,即区块链系统上各个相关的终端。该终端可以是通过区块链网络相连的手机、平板和电脑等终端。第一加密信息是指经过加密处理后的用户A发送给用户B的信息。该第一加密信息包括用户A生成的加密后的第一随机数。其中,第一随机数是指用户A生成的,用来与用户B进行密钥协商的随机数。

[0036] 区块链是分布式数据存储、共识机制和加密算法等计算机技术的新型应用模式。区块链系统本质是一个去中心化的分布式数据库系统。本实施例中,用户A和用户B的通信过程都是在区块链上进行的,用户A在区块链系统下向用户B发送第一加密信息,以使后续用户B能够接收该第一加密信息,并解密该第一加密信息,获取第一随机数。

[0037] S20:用户B接收第一加密信息,解密后获取第一随机数。

[0038] 本实施例中,用户B在区块链系统上读取用户A发送的第一加密信息,并对该第一加密信息进行解密,获取第一随机数。用户B通过获取用户A发送的第一随机数,为后续基于该第一随机数进行用户A和用户B共同协商生成的密钥Key和初始化变量IV提供了基础。

[0039] S30:用户B向用户A发送第二加密信息。

[0040] 第二加密信息是指经过加密处理后的用户B发送给用户A的信息,该第二加密信息包括用户B生成的加密后的第二随机数。其中,第二随机数是指用户B生成的,用来与用户A进行密钥协商的随机数。用户B在区块链系统下向用户A发送第二加密信息,以使后续用户A接收该第二加密信息,并解密该第二加密信息,获取第二随机数。

[0041] S40:用户A接收第二加密信息,解密后获取第二随机数。

[0042] 本实施例中,用户A在区块链系统上读取接收用户B发送的第二加密信息,并对该第二加密信息进行解密,获取第二随机数。用户A通过获取用户B发送的第二随机数,为后续基于该第二随机数进行用户A和用户B共同协商生成的密钥Key和初始化变量IV提供了基础。

[0043] S50:用户A和用户B基于第一随机数和第二随机数执行密钥生成算法,获取密钥Key和初始化变量IV。

[0044] 本实施例中,在用户B获取用户A生成并发送的第一随机数和用户A获取用户B生成并发送的第二随机数后,用户A和用户B基于第一随机数和第二随机数同时执行密钥生成算法,并根据该密钥生成算法同时获取密钥Key和初始化变量IV(密钥Key和初始化变量IV为后续用户在区块链系统上通信加密过程所需的基础条件)。通过采用在区块链系统上只有用户A和用户B知道的第一随机数和第二随机数,结合密钥生成算法,生成安全可靠并且只有用户A和用户B拥有的密钥Key和初始化变量IV。

[0045] S60:用户A和用户B基于密钥Key和初始化变量IV,采用AES算法的CBC模式进行加密通信。

[0046] 其中,AES算法是一种对称分组密码体制,采用代替/置换网络,每轮由线性混合层、非线性层和密钥加密层组成。其中,线性混合层用于确保多轮之上的高度扩散,非线性层由16个S盒组成并起到混淆的作用,密钥加密层用于将子密钥异或到中间状态。AES是一个迭代分组密码,其分组长度和密钥长度都是可变的,只是为了满足AES的要求才限定处理的分组大小为128位,而密钥长度为128位、192位或256位,相应的迭代轮数N,为10轮、12轮

和14轮。AES汇聚了安全性能、效率、可实现性和灵活性等优点。最大的优点是可以给出算法的最佳查分特征的概率，并分析算法抵抗查分密码分析及线性密码分析的能力。CBC模式是一种分组加密模式，对于每个待加密的密码块在加密前会先与前一个密码块的密文异或(特别地，第一个明文块与一个叫初始化向量IV的数据块异或)，然后再用加密器加密。AES-CBC模式即采用加解密模式为CBC，算法采用AES算法的加解密方式。

[0047] 本实施例中，用户A和用户B基于双方共同协商获取的安全可靠并且只有用户A和用户B拥有的密钥Key和初始化变量IV，采用AES算法和采用CBC模式实现用户在区块链上的加密通信。

[0048] 本实施例中，结合区块链系统自身的性质和特点，通过一系列的关联加密操作，层层提高安全性，确保了在区块链系统上用户通信的安全。首先用户A向用户B发送第一加密信息，用户B接收第一加密信息，解密后获取第一随机数；用户B向用户A发送第二加密信息，用户A接收第二加密信息，解密后获取第二随机数，用户A和用户B采用加解密随机数的方式相互获取对方发送的第一随机数和第二随机数，为后续的加密通信提供了基础。然后用户A和用户B基于第一随机数和第二随机数执行密钥生成算法，获取密钥Key和初始化变量IV，生成的密钥Key和初始化变量IV是用户A和用户B共同协商获取的，该密钥Key和初始化变量IV是通过哈希算法获取，具有数据不可逆的特点，安全性高，为实现用户A和用户B之间的通信加密提供了必要的基础。最后用户A和用户B基于密钥Key和初始化变量IV，采用AES算法的CBC模式进行加密通信，使得第三方(除用户A和用户B以外的区块链上用户)在没有密钥Key和初始化变量IV的情况下不能够获取用户A和用户B的通信内容，确保了区块链上任意两个用户进行点对点通信时通信内容的安全。

[0049] 在一具体实施方式中，如图2所示，步骤S10中，用户A向用户B发送第一加密信息，具体包括如下步骤：

[0050] S11：用户A从用户B的用户证书中获取第二公钥。

[0051] 其中，用户证书是由区块链上的系统根证书对每一用户发放的用于验证用户身份的证书。区块链上的每一用户均有唯一的用户证书。该系统根证书是在区块链上自定义设置的，具体可以为区块链上系统管理员创建一个独一无二的键值对，该键值对的键为Key＝ROOT，值value＝cert，cert即系统根证书。系统根证书包括一对相对应的公钥和私钥(即一对密钥)，公钥用于用户验证，私钥用于加密原始的用户证书(即还未经过系统根证书进行数字签名的用户证书)。系统根证书在给区块链上的每一用户发放用户证书的时候为用户证书生成一对密钥对，以使区块链上的任意两个用户进行点对点通信时，可基于其对应的用户证书进行身份验证。区块链系统上进行的用户验证无需通过外部的第三方证书签发机构实现，提高了区块链系统用户之间验证的可靠性。

[0052] 本实施例中，用户A通过区块链系统与用户B进行通信，双方需要先进行用户认证后才能继续通信，如用户B要验证用户A是否为区块链系统上的合法用户，用户B会读取区块链系统上的系统根证书，采用系统根证书的公钥对用户A的用户证书进行解密验证，若解密结果包括系统根证书的数字签名，则认为用户A是区块链系统上的合法用户。在验证身份合法后，用户A将获取用户B的用户证书中的第二公钥，以便后续采用该第二公钥对用户A生成的第一随机数进行加密。其中，第二公钥是用户B的用户证书中存储的公钥。

[0053] S12：用户A生成第一随机数，采用第二公钥加密第一随机数，获取第一加密信息。

[0054] 本实施例中，用户A在区块链上生成第一随机数，采用用户B的用户证书中的第二公钥对该第一随机数进行加密，获取第一加密信息。可以理解地，在对第一随机数加密之前，可以在该第一随机数之前加上“密钥协商1”的前缀，以通过该前缀表明或区分该待加密的第一随机数的用途，从而使得用户B在解密第一加密信息后，可以根据该前缀获知该解密后的第一随机数是用户A和用户B之间进行密钥协商的随机数。

[0055] S13：用户A通过区块链系统向用户B发送第一加密信息。

[0056] 本实施例中，结合区块链自身的性质特点，区块链上用户A能通过区块链系统向用户B发送第一加密信息。具体地，可以通过以下两种方式实现：

[0057] 第一种通信方式，在区块链上设置用户的通信地址，以便基于该通信地上实现区块链上的用户通信。用户的通信地址具体可以为用户的邮箱地址。本实施例中，首先设置用户A和用户B的邮箱地址，如将用户A的邮箱地址表示为MailuserAAA。用户A和用户B的邮箱地址都是以键值对的方式创建，邮箱地址是键值对中的键。用户A的邮箱地址对应的值是Ma，用户B的邮箱地址对应的值是Mb。在发送数据的时候，用户A读取用户B的邮箱地址，根据该邮箱地址获取值Mb，在值Mb中添加键Kab(键Kab对应的值为Data1)，即完成了发送数据Data1的过程，以使后续用户B通过自身的通信地址即可获取对应的值Mb中新添加的键Kab，从而根据键Kab获取对应的值Data1，该值Data1在本实施例中即第一加密信息。

[0058] 第二种通信方式，在区块链系统上设置用户A和用户B的用户地址，如用户A的用户地址可以表示为userAAA，用户A在区块链上创建一个键值对，该键值对的键为Kab(与上述第1种方法的kab命名相同，具体内容不同)，值为Data1(该Data1在本实施例中即第一加密信息)。把该键Kab设置为特定形式Kab＝数据前缀+用户B的用户地址+用户A的用户地址，其中，数据前缀是用来区分数据的标识。通过将键kab设置为这种特定形式，在区块链系统上创建键为kab，对应的值为Data1的键值对，即完成了发送数据的过程，以使后续用户B通过查询字段为“数据前缀+用户B的用户地址”的模糊查询的方式获取所有以数据前缀+用户B的用户地址开头的键，从而获得键Kab，并通过键Kab得到值Data1。

[0059] 在一具体实施方式中，如图3所示，步骤S20中，用户B接收第一加密信息，解密后获取第一随机数，具体包括如下步骤：

[0060] S21：用户B通过区块链系统接收用户A发送的第一加密信息。

[0061] 本实施例中，用户B通过区块链系统，根据区块链系统自身的性质和特点，接收用户A发送的第一加密信息。具体地，如步骤S13列举出的两种用户在区块链上进行通信的方式，如果是采用第一种通信方式，则用户B接收用户A发送的信息具体是通过读取自身的邮箱地址，根据该邮箱地址(邮箱地址是一个键)获取对应的值Mb，然后从值Mb中获取到用户A添加到值Mb中的键Kab，再根据键Kab与值Data1是一个键值对的关系，直接根据键Kab获取值Data1。在本实施例中，值Data1即用户A想要发送给用户B的第一加密信息。如果是采用步骤S13中的第二种通信方式，根据特定形式的键Kab＝数据前缀+用户B的用户地址+用户A的用户地址，用户B将在区块链系统上以模糊查询的方式查询字段“数据前缀+用户B的用户地址”，获取所有以字段“数据前缀+用户B的用户地址”的信息，其中，获取到的信息包括键Kab，最后根据键Kab获取对应的值Data1，也即获取用户A发送的第一加密信息。基于区块链系统自身的性质和特点，使得用户B能够通过区块链系统接收获取用户A发送的第一加密信息。

[0062] S22:用户B采用与第二公钥相对应的第二私钥解密第一加密信息,获取第一随机数。

[0063] 用户B在获取用户A发送的第一加密信息之后,由于第一加密信息是采用用户B的用户证书的公钥(即本实施例中的第二公钥)加密获取的,故解密该第一加密信息需要用户B的用户证书的私钥(即本实施例中的第二私钥)。本实施例中,用户B采用与第二公钥对应的第二私钥解密第一加密信息,解密后获取由用户A生成的第一随机数。

[0064] 本实施例中,通过在区块链自定义设置的系统根证书,采用该系统根证书生成区块链上用户的用户证书,并通过该用户证书的密钥对(公钥和私钥)实现区块链上用户生成的随机数进行加密发送、解密获取的随机数交换过程,达到区块链系统上用户交换随机数,为后续根据该随机数生成密钥Key和初始化变量IV提供了基础。

[0065] 在一具体实施方式中,如图4所示,步骤S30中,用户B向用户A发送第二加密信息,具体包括如下步骤:

[0066] S31:用户B从用户A的用户证书中获取第一公钥。

[0067] 与步骤S11相似,参考步骤S11的实现过程,在此不再赘述。

[0068] S32:用户B生成第二随机数,采用第一公钥加密第二随机数,获取第二加密信息。

[0069] 与步骤S12相似,参考步骤S11的实现过程,在此不再赘述。

[0070] S33:用户B通过区块链系统向用户A发送第二加密信息。

[0071] 与步骤S13相似,参考步骤S11的实现过程,在此不再赘述。

[0072] 在一具体实施方式中,如图5所示,步骤S40中,用户A接收第二加密信息,解密后获取第二随机数,具体包括如下步骤:

[0073] S41:用户A通过区块链系统接收用户B发送的第二加密信息。

[0074] 与步骤S21相似,参考步骤S21的实现过程,在此不再赘述。

[0075] S42:用户A采用与第一公钥相对应的第一私钥解密第二加密信息,获取第二随机数。

[0076] 与步骤S22相似,参考步骤S22的实现过程,在此不再赘述。

[0077] 在一具体实施方式中,如图6所示,在步骤S10之前,即用户A向用户B发送第一加密信息的步骤之前,该区块链上用户通信加密方法还包括如下步骤:

[0078] S101:用户A和用户B预先查询各自的本地数据库。

[0079] 区块链系统本质是一个去中心化的分布式数据库系统。本实施例中,区块链系统上任意的两个用户(即用户A和用户B)进行通信之前,会预先查询各自的本地数据库。可以理解地,该步骤的目的为在通信之前查询本地数据库以确定是否有现成的、直接可用的密钥Key和初始化变量IV。

[0080] S102:若本地数据库中存在密钥Key和初始化变量IV,则查看密钥Key和初始化变量IV的创建时间。

[0081] 本实施例中,若在本地数据库中已经存在通信过程所需的密钥Key和初始化变量IV,则需要查看该密钥Key和初始化变量IV的创建时间,以确定该密钥Key和初始化变量IV是否可以使用。

[0082] S103:若创建时间未超过预设有效时间,则采用已存在的密钥Key和初始化变量IV,采用AES算法的CBC模式进行加密通信。

[0083] 其中，预设有效时间是指预先设置、约定好的密钥Key和初始化变量IV的有效时间段。本实施例中，若密钥Key和初始化变量IV的创建时间未超过预设有效时间，则可以采用该已保存在本地数据库中的密钥Key和初始化变量IV，并采用AES算法的CBC模式进行加密通信，保证区块链系统上用户进行通信的安全。

[0084] 在一具体实施方式中，步骤S50中，密钥生成算法具体为：

[0085] $C(0)=Hash(random1)$

[0086] $C(n)=HMAC_{C(n-1)}(Hash(random2))$

[0087] $Key=HMAC_{Hash(random1||random2)}(C0+C1)$

[0088] $IV=HMAC_{Hash(random1||random2)}(C0+C2)$

[0089] 其中，random1表示第一随机数，random2表示第二随机数，n为大于0的正整数，Hash表示哈希函数，算法采用SHA256算法，HMAC是指与密钥相关的哈希运算，算法采用SHA256算法，||表示连接操作。

[0090] 本实施例中，用户A和用户B同时执行上述生成密钥Key和初始化变量IV的密钥生成算法，第一随机数和第二随机数只有用户A和用户B知道，提高了区块链系统上通信的安全性。该算法结合第一随机数和第二随机数的特点，采用哈希算法(即Hash算法)生成多个信息摘要(如C0、C1和C2)，根据第一随机数、第二随机数和生成的信息摘要(如C0、C1和C2)，通过哈希算法(又称为单向散列算法)生成获取密钥Key和初始化变量IV，为后续基于该密钥Key和初始化变量IV进行区块链系统上用户通信加密提供了坚实的基础，提高区块链系统上用户通信的安全性。

[0091] 需要说明的是，SHA256算法是哈希算法中的一种，与本实施例中AES算法是不同的算法。生成密钥Key和初始化变量IV需要用到SHA256算法，用户通信加密需要用到AES算法。

[0092] 在一具体实施方式中，如图7所示，步骤S60中，用户A和用户B基于密钥Key和初始化变量IV，采用AES算法的CBC模式进行加密通信，具体包括如下步骤：

[0093] S61：用户A以键值对的方式将数据K:V写到区块链上，其中K代表键，V代表值。

[0094] S62：用户A基于密钥Key和初始化变量IV采用AES算法的CBC模式对K进行加密，获取KC，KC＝AES_CBC(K)。

[0095] S63：用户A基于密钥Key和初始化变量IV采用AES算法的CBC模式对V进行加密，获取VC，VC＝AES_CBC(V)。

[0096] S64：用户A将数据{KC:VC+IV}写到区块链上。

[0097] S65：用户B在区块链上读取KC，根据KC获取VC和初始化变量IV。

[0098] S66：用户B基于密钥Key和初始化变量IV采用AES算法的CBC模式对KC进行解密，获取K，K＝AES_CBC(KC)。

[0099] S67：用户B基于密钥Key和初始化变量IV采用AES算法的CBC模式对VC进行解密，获取V，V＝AES_CBC(VC)。

[0100] S68：用户B获取数据K:V。

[0101] 本实施例中，步骤S61-S64是用户A基于密钥Key和初始化变量IV，采用AES算法的CBC模式对通信内容进行加密的过程。相应地，步骤S65-S68是用户B基于密钥Key和初始化变量IV，采用AES算法的CBC模式对通信内容进行解密的过程。区块链上的任一用户(如用户A)均可通过步骤S61-S64在所要进行加密通信的数据写到区块链上，使得只有拥有密钥Key

和初始化变量IV的用户(如与用户A通信的用户B)才可解密读取区块链上的这一加密的数据。通信内容即通信的数据是采用键值对的方式存储的，该AES算法的CBC模式对键值对模式存储的数据进行加密，并且很好地采用、结合了密钥Key和初始化变量IV，使得区块链上用户通信加密过程更安全可靠。

[0102] 本实施例所提供的区块链上用户通信加密方法中，首先用户A向用户B发送第一加密信息，用户B接收第一加密信息，解密后获取第一随机数；用户B向用户A发送第二加密信息，用户A接收第二加密信息，解密后获取第二随机数，用户A和用户B采用加解密随机数的方式相互获取对方发送的第一随机数和第二随机数，为后续根据该第一随机数和第二随机数生成密钥Key和初始化变量IV，并根据密钥Key和初始化变量IV的加密通信提供了基础。然后用户A和用户B基于第一随机数和第二随机数执行密钥生成算法，获取密钥Key和初始化变量IV，生成的密钥Key和初始化变量IV是用户A和用户B通过第一随机数和第二随机数共同协商获取的，该密钥Key和初始化变量IV是通过哈希算法获取，具有数据不可逆的特点，安全性高，为实现用户A和用户B之间的通信加密提供了必要的基础。最后用户A和用户B基于密钥Key和初始化变量IV，采用AES算法的CBC模式进行加密通信，使得第三方(除用户A和用户B以外的区块链上用户)在没有密钥Key和初始化变量IV的情况下不能够获取用户A和用户B的通信内容，确保了区块链上任意两个用户进行点对点通信时通信内容的安全。

[0103] 本实施例所提供的区块链上用户通信加密方法还结合了区块链的性质和特点，在区块链系统上设置系统根证书；在区块链系统上实现并进行任意两个用户的点对点通信，即通过在区块链系统上虚拟出一条通信通道，实现区块链上任意两个用户之间的数据通信。用户只需要维护与区块链网络的通信，即可实现数据共享存储和所有用户间的数据通信，可以有效地简化应用系统的构建难度，降低系统复杂性，增强区块链系统的安全性和健壮性。通过借助于区块链系统本身的性质和特点，使得区块链系统上用户的通信过程都处在一个统一的系统下，不借助其他第三方系统、认证机构和工具，进一步确保区块链上用户通信的安全。

[0104] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0105] 实施例2

[0106] 图8示出与实施例1中区块链上用户通信加密方法一一对应的区块链上用户通信加密装置的原理框图。如图8所示，该区块链上用户通信加密装置包括第一加密信息发送模块10、第一随机数获取模块20、第二加密信息发送模块30、第二随机数获取模块40、密钥和初始化变量获取模块50和加密通信模块60。其中，第一加密信息发送模块10、第一随机数获取模块20、第二加密信息发送模块30、第二随机数获取模块40、密钥和初始化变量获取模块50和加密通信模块60的实现功能与实施例1中区块链上用户通信加密方法对应的步骤一一对应，为避免赘述，本实施例不一一详述。

[0107] 第一加密信息发送模块10，用于用户A向用户B发送第一加密信息。

[0108] 第一随机数获取模块20，用于用户B接收第一加密信息，解密后获取第一随机数。

[0109] 第二加密信息发送模块30，用于用户B向用户A发送第二加密信息。

[0110] 第二随机数获取模块40，用于用户A接收第二加密信息，解密后获取第二随机数。

[0111] 密钥和初始化变量获取模块50，用于用户A和用户B基于第一随机数和第二随机数执行密钥生成算法，获取密钥Key和初始化变量IV。

[0112] 加密通信模块60，用于用户A和用户B基于密钥Key和初始化变量IV，采用AES算法的CBC模式进行加密通信。

[0113] 优选地，第一加密信息发送模块10包括第二公钥获取单元11、第一加密信息获取单元12和第一加密信息发送单元13。

[0114] 第二公钥获取单元11，用于用户A从用户B的用户证书中获取第二公钥。

[0115] 第一加密信息获取单元12，用于用户A生成第一随机数，采用第二公钥加密第一随机数，获取第一加密信息。

[0116] 第一加密信息发送单元13，用于用户A通过区块链向用户B发送第一加密信息。

[0117] 优选地，第一随机数获取模块20包括第一加密信息接收单元21和第一随机数获取单元22。

[0118] 第一加密信息接收单元21，用于用户B通过区块链系统接收用户A发送的第一加密信息。

[0119] 第一随机数获取单元22，用于用户B采用与第二公钥相对应的第二私钥解密第一加密信息，获取第一随机数。

[0120] 优选地，第二加密信息发送模块30包括第一公钥获取单元31、第二加密信息获取单元32和第二加密信息发送单元33。

[0121] 第一公钥获取单元31，用于用户B从用户A的用户证书中获取第一公钥。

[0122] 第二加密信息获取单元32，用于用户B生成第二随机数，采用第一公钥加密第二随机数，获取第二加密信息。

[0123] 第二加密信息发送单元33，用于用户B通过区块链向用户A发送第二加密信息。

[0124] 优选地，第二随机数获取模块40包括第二加密信息接收单元41和第二随机数获取单元42。

[0125] 第二加密信息接收单元41，用于用户A通过区块链系统接收用户B发送的第二加密信息。

[0126] 第二随机数获取单元42，用于用户A采用与第一公钥相对应的第一私钥解密第二加密信息，获取第二随机数。

[0127] 优选地，该区块链上用户通信加密装置还包括预先查询模块70，该预先查询模块70包括查询单元71、创建时间查看单元72和确定采用单元73。

[0128] 查询单元71，用于用户A和用户B预先查询各自的本地数据库。

[0129] 创建时间查看单元72，用于若本地数据库中存在密钥Key和初始化变量IV，则查看密钥Key和初始化变量IV的创建时间。

[0130] 确定采用单元73，用于若创建时间未超过预设有效时间，则采用已存在的密钥Key和初始化变量IV，采用AES算法的CBC模式进行加密通信。

[0131] 优选地，密钥生成算法为：

[0132] $C(0)=Hash(random1)$

[0133] $C(n)=HMAC_{C(n-1)}(Hash(random2))$

[0134] $Key=HMAC_{Hash(random1||random2)}(C0+C1)$

[0135] $IV=HMAC_{Hash(random1||random2)}(C0+C2)$

[0136] 其中，random1表示第一随机数，random2表示第二随机数，n为大于0的正整数，Hash表示哈希函数，算法采用SHA256算法，HMAC是指与密钥相关的哈希运算，算法采用SHA256算法，||表示连接操作。

[0137] 优选地，加密通信模块60包括数据写入单元61、键加密单元62、值加密单元63、加密数据写入单元64、加密数据读取单元65、键解密单元66、值解密单元67和数据获取单元68。

[0138] 数据写入单元61，用于用户A以键值对的方式将数据K:V写到区块链上，其中K代表键，V代表值。

[0139] 键加密单元62，用于用户A基于密钥Key和初始化变量IV采用AES算法的CBC模式对K进行加密，获取KC，KC＝AES_CBC(K)。

[0140] 值加密单元63，用于用户A基于密钥Key和初始化变量IV采用AES算法的CBC模式对V进行加密，获取VC，VC＝AES_CBC(V)。

[0141] 加密数据写入单元64，用于用户A将数据{KC:VC+IV}写到区块链上。

[0142] 加密数据读取单元65，用于用户B在区块链上读取KC，根据KC获取VC和初始化变量IV。

[0143] 键解密单元66，用于用户B基于密钥Key和初始化变量IV采用AES算法的CBC模式对KC进行解密，获取K，K＝AES_CBC(KC)。

[0144] 值解密单元67，用于用户B基于密钥Key和初始化变量IV采用AES算法的CBC模式对VC进行解密，获取V，V＝AES_CBC(VC)。

[0145] 数据获取单元68，用于用户B获取数据K:V。

[0146] 本实施例所提供的区块链上用户通信加密装置中，第一加密信息发送模块10、第一随机数获取模块20、第二加密信息发送模块30和第二随机数获取模块40，用户A和用户B采用加解密随机数的方式相互获取对方发送的第一随机数和第二随机数，为后续根据该第一随机数和第二随机数生成密钥Key和初始化变量IV，并根据密钥Key和初始化变量IV的加密通信提供了基础。密钥和初始化变量获取模块50，生成的密钥Key和初始化变量IV是用户A和用户B通过第一随机数和第二随机数共同协商获取的，该密钥Key和初始化变量IV是通过哈希算法获取，具有数据不可逆的特点，安全性高，为实现用户A和用户B之间的通信加密提供了必要的基础。加密通信模块60，使得第三方(除用户A和用户B以外的区块链上用户)在没有密钥Key和初始化变量IV的情况下不能够获取用户A和用户B的通信内容，确保了区块链上任意两个用户进行点对点通信时通信内容的安全。

[0147] 实施例3

[0148] 本实施例提供一计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时实现实施例1中区块链上用户通信加密方法，为避免重复，这里不再赘述。或者，该计算机程序被处理器执行时实现实施例2中区块链上用户通信加密装置中各模块/单元的功能，为避免重复，这里不再赘述。

[0149] 实施例4

[0150] 图9是本实施例中终端设备的示意图。如图9所示，终端设备80包括处理器81、存储器82以及存储在存储器82中并可在处理器81上运行的计算机程序83。处理器81执行计算机

程序83时实现实施例1中区块链上用户通信加密方法的各个步骤，例如图1所示的步骤S10、S20、S30、S40、S50和S60。或者，处理器81执行计算机程序83时实现实施例2中区块链上用户通信加密装置各模块/单元的功能，如图8所示第一加密信息发送模块10、第一随机数获取模块20、第二加密信息发送模块30、第二随机数获取模块40、密钥和初始化变量获取模块50和加密通信模块60的功能。

[0151] 示例性的，计算机程序83可以被分割成一个或多个模块/单元，一个或者多个模块/单元被存储在存储器82中，并由处理器81执行，以完成本发明。一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述计算机程序83在终端设备80中的执行过程。例如，计算机程序83可被分割成实施例2中的第一加密信息发送模块10、第一随机数获取模块20、第二加密信息发送模块30、第二随机数获取模块40、密钥和初始化变量获取模块50和加密通信模块60，各模块的具体功能如实施例2所示，为避免重复，此处不一一赘述。

[0152] 终端设备80可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。终端设备可包括，但不仅限于，处理器81、存储器82。本领域技术人员可以理解，图9仅仅是终端设备80的示例，并不构成对终端设备80的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如终端设备还可以包括输入输出设备、网络接入设备、总线等。

[0153] 所称处理器81可以是中央处理单元(Central Processing Unit,CPU)，还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0154] 存储器82可以是终端设备80的内部存储单元，例如终端设备80的硬盘或内存。存储器82也可以是终端设备80的外部存储设备，例如终端设备80上配备的插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)等。进一步地，存储器82还可以既包括终端设备80的内部存储单元也包括外部存储设备。存储器82用于存储计算机程序以及终端设备所需的其他程序和数据。存储器82还可以用于暂时地存储已经输出或者将要输出的数据。

[0155] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。

[0156] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0157] 所述集成的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实现上述实施例方法中的全部或部分流程，也可以通过计算机程序来指令相关的硬件来完成，所述的计

算机程序可存储于一计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机程序包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括：能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、电载波信号、电信信号以及软件分发介质等。需要说明的是，所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如在某些司法管辖区，根据立法和专利实践，计算机可读介质不包括是电载波信号和电信信号。

[0158] 以上所述实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围，均应包含在本发明的保护范围之内。

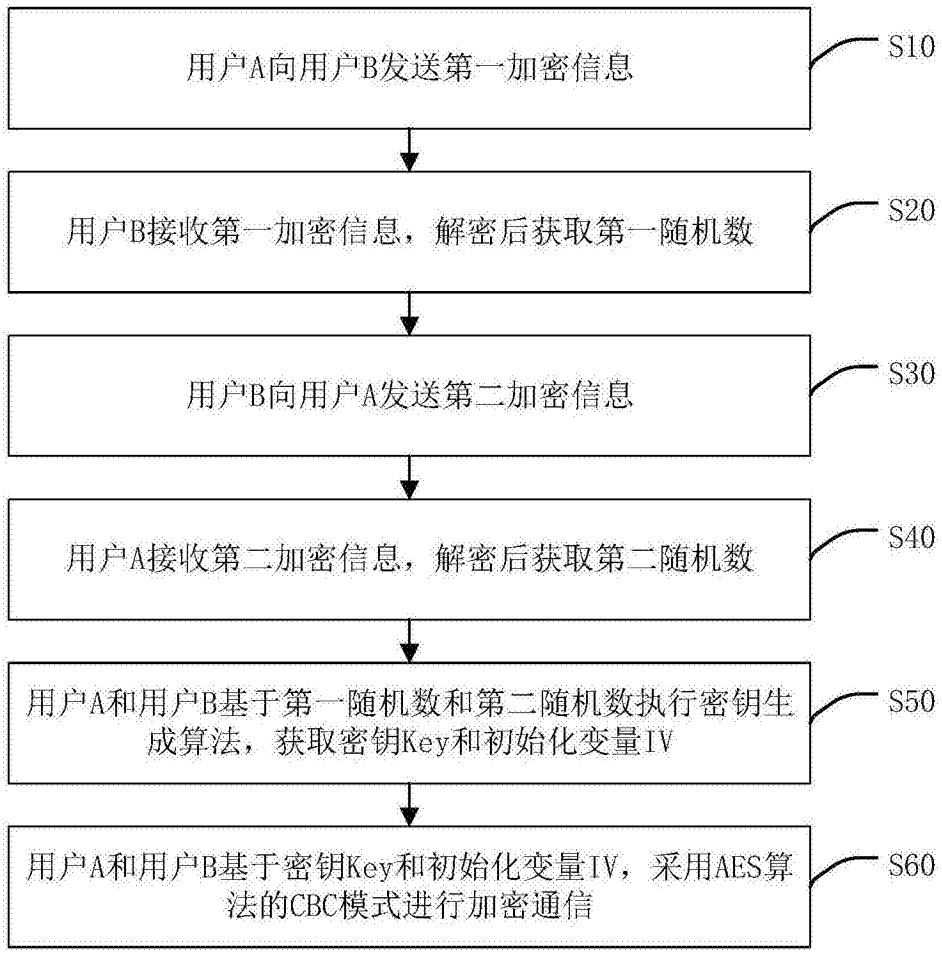

用户A向用户B发送第一加密信息
S10
用户B接收第一加密信息，解密后获取第一随机数
S20
用户B向用户A发送第二加密信息
S30
用户A接收第二加密信息，解密后获取第二随机数
S40
用户A和用户B基于第一随机数和第二随机数执行密钥生成算法，获取密钥Key和初始化变量IV
S50
用户A和用户B基于密钥Key和初始化变量IV，采用AES算法的CBC模式进行加密通信
S60

图1

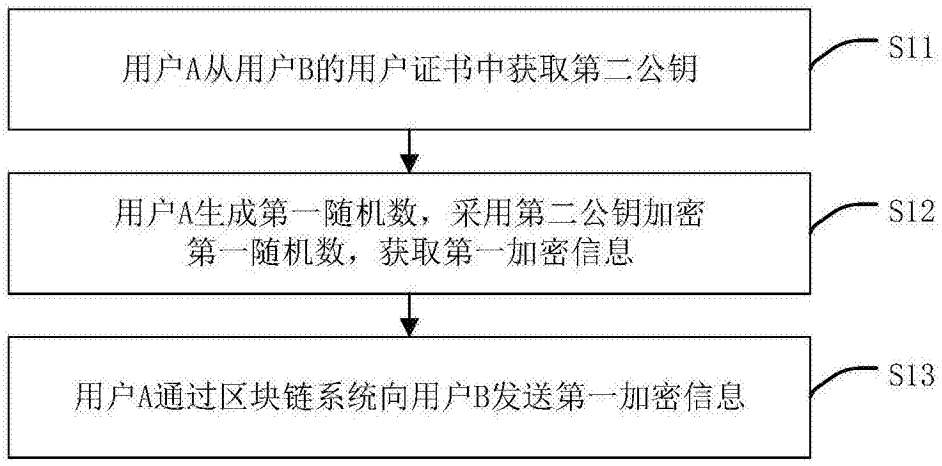

用户A从用户B的用户证书中获取第二公钥
S11
用户A生成第一随机数，采用第二公钥加密第一随机数，获取第一加密信息
S12
用户A通过区块链系统向用户B发送第一加密信息
S13

图2

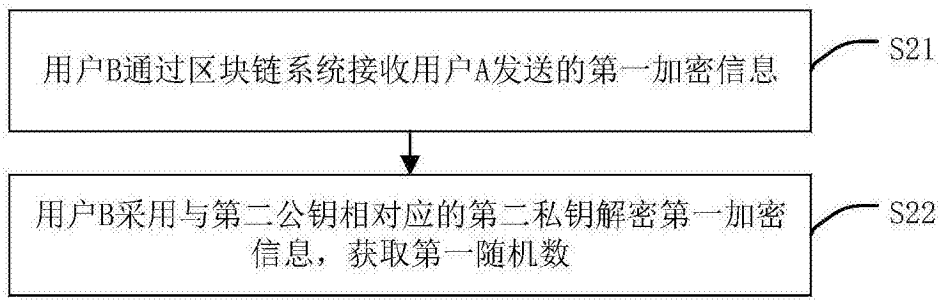

用户B通过区块链系统接收用户A发送的第一加密信息
S21
用户B采用与第二公钥相对应的第二私钥解密第一加密信息，获取第一随机数
S22

图3

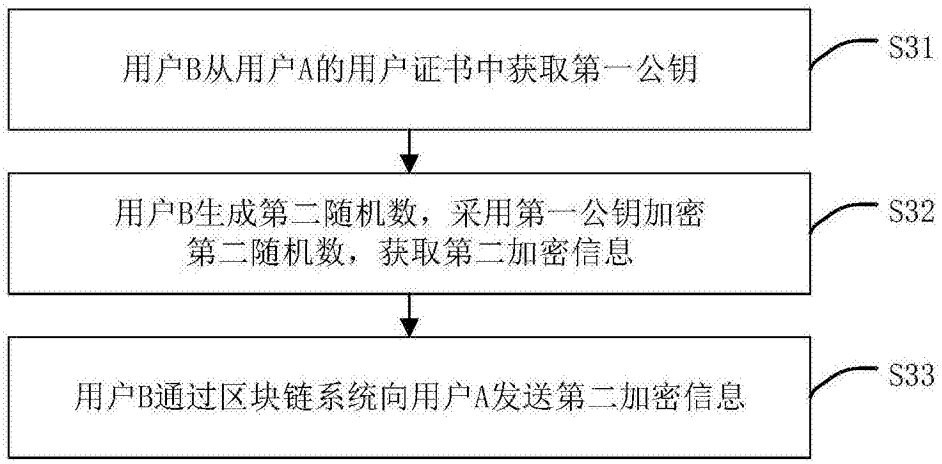

用户B从用户A的用户证书中获取第一公钥
S31
用户B生成第二随机数，采用第一公钥加密第二随机数，获取第二加密信息
S32
用户B通过区块链系统向用户A发送第二加密信息
S33

图4

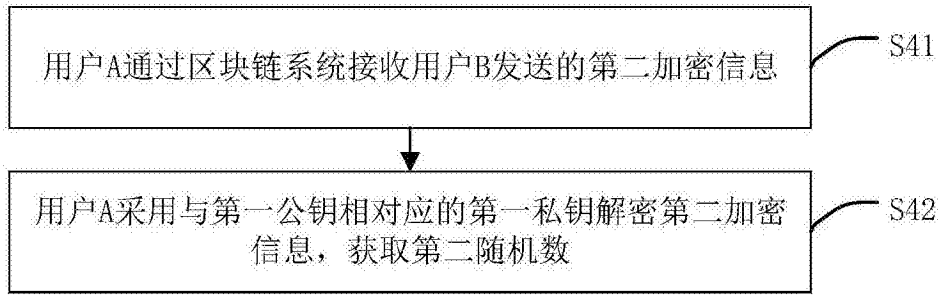

用户A通过区块链系统接收用户B发送的第二加密信息
S41
用户A采用与第一公钥相对应的第一私钥解密第二加密信息，获取第二随机数
S42

图5

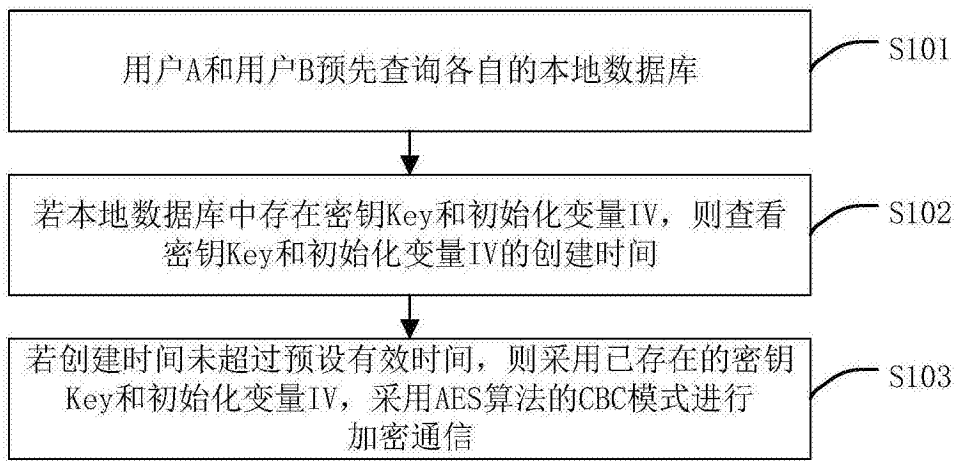

用户A和用户B预先查询各自的本地数据库
S101
若本地数据库中存在密钥Key和初始化变量IV，则查看密钥Key和初始化变量IV的创建时间
S102
若创建时间未超过预设有效时间，则采用已存在的密钥Key和初始化变量IV，采用AES算法的CBC模式进行加密通信
S103

图6

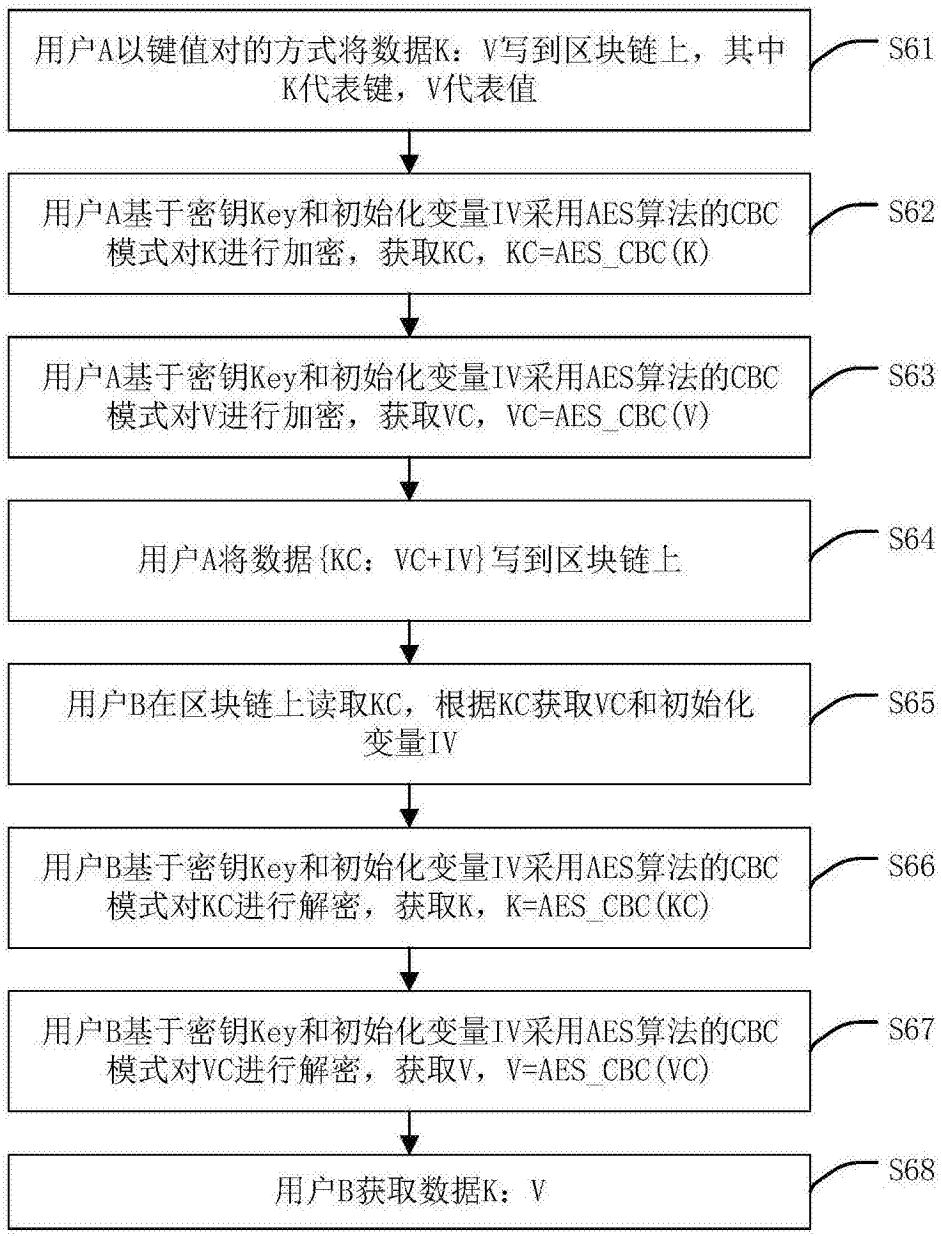

用户A以键值对的方式将数据K：V写到区块链上，其中K代表键，V代表值
S61
用户A基于密钥Key和初始化变量IV采用AES算法的CBC模式对K进行加密，获取KC，KC=AES_CBC(K)
S62
用户A基于密钥Key和初始化变量IV采用AES算法的CBC模式对V进行加密，获取VC，VC=AES_CBC(V)
S63
用户A将数据{KC：VC+IV}写到区块链上
S64
用户B在区块链上读取KC，根据KC获取VC和初始化变量IV
S65
用户B基于密钥Key和初始化变量IV采用AES算法的CBC模式对KC进行解密，获取K，K=AES_CBC(KC)
S66
用户B基于密钥Key和初始化变量IV采用AES算法的CBC模式对VC进行解密，获取V，V=AES_CBC(VC)
S67
用户B获取数据K：V
S68

图7

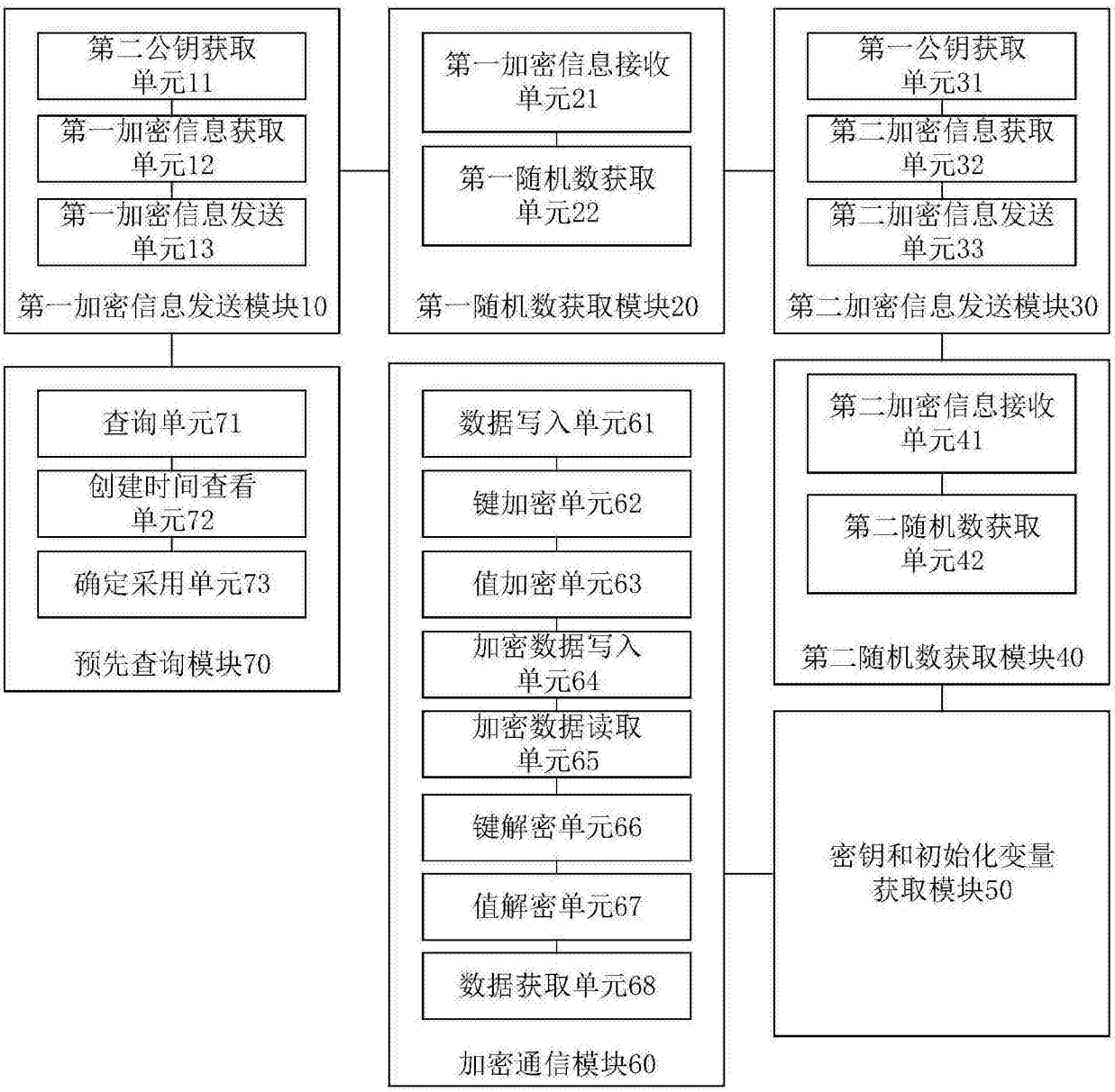

第二公钥获取单元11
第一加密信息获取单元12
第一加密信息发送单元13
第一加密信息发送模块10
第一加密信息接收单元21
第一随机数获取单元22
第一随机数获取模块20
第一公钥获取单元31
第二加密信息获取单元32
第二加密信息发送单元33
第二加密信息发送模块30
查询单元71
创建时间查看单元72
确定采用单元73
预先查询模块70
数据写入单元61
键加密单元62
值加密单元63
加密数据写入单元64
加密数据读取单元65
键解密单元66
值解密单元67
数据获取单元68
加密通信模块60
第二加密信息接收单元41
第二随机数获取单元42
第二随机数获取模块40
密钥和初始化变量获取模块50

图8

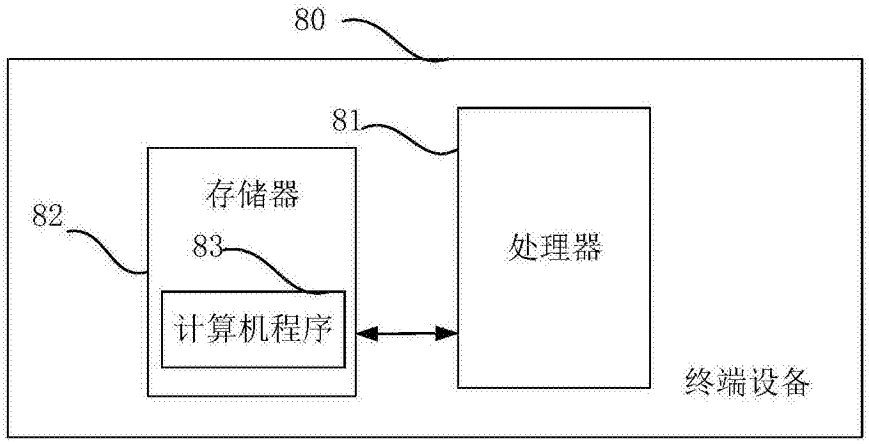


图9