

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2019 年 11 月 14 日 (14.11.2019)



(10) 国际公布号
WO 2019/214070 A1

- (51) 国际专利分类号:
H04L 9/08 (2006.01) *H04L 29/06* (2006.01)
- (21) 国际申请号: PCT/CN2018/095907
- (22) 国际申请日: 2018 年 7 月 17 日 (17.07.2018)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201810437217.7 2018年5月9日 (09.05.2018) CN
- (71) 申请人: 深圳壹账通智能科技有限公司(ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。

- (72) 发明人: 贾牧 (JIA, Mu); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。 谢丹力 (XIE, Danli); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。 陆陈一帆 (LU, Frank YiFan Chen); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。
- (74) 代理人: 深圳众鼎专利商标代理事务所 (普通合伙) (SHENZHEN ZHONGDING INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市龙岗区龙城街道中心城清林路546号城投商务中心4层/B, Guangdong 518172 (CN)。
- (81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,

(54) Title: ENCRYPTION METHOD FOR USER COMMUNICATION ON BLOCK CHAIN, APPARATUS, TERMINAL DEVICE AND STORAGE MEDIUM

(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

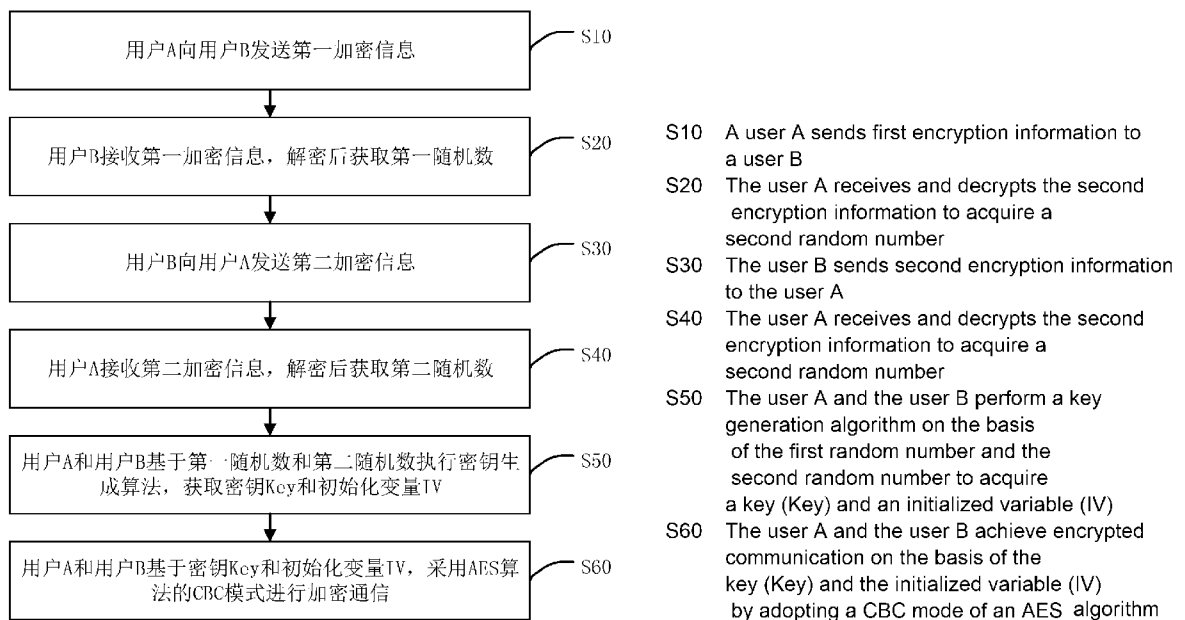


图 1

(57) Abstract: Disclosed in the present application are an encryption method for user communication on a block chain, an apparatus, a terminal device and a storage medium. The method for user communication on the block chain comprises: a user A sending first encryption information to a user B; the user B receiving and decrypting the first encryption information to acquire a first random number; the user B sending second encryption information to the user A; the user A receiving and decrypting the second encryption information to acquire a second random number; the user A and the user B performing a key generation algorithm on the basis of the first random number and the second random number to acquire a key (Key) and an initialized variable (IV); and the user A and the

CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

user B achieving encrypted communication on the basis of the key (Key) and the initialized variable (IV) by adopting a CBC mode of an AES algorithm. According to the encryption method for user communication on the block chain, the security of point-to-point communication of the users on the block chain system can be guaranteed.

(57) 摘要: 本申请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。

区块链上用户通信加密方法、装置、终端设备及存储介质

本申请以 2018 年 5 月 9 日提交的申请号为 201810437217.7，名称为“区块链上用户通信加密方法、装置、终端设备及存储介质”的中国发明专利申请为基础，并要求其优先权。

技术领域

本申请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

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

本申请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。

第一方面，本申请实施例提供一种区块链上用户通信加密方法，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。

第二方面，本申请实施例提供一种区块链上用户通信加密装置，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。

第三方面，本申请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

存储器中并可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

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。

第四方面，本申请实施例提供一个或多个存储有计算机可读指令的非易失性可读存储介质，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行如下步骤：

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。

本申请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

为了更清楚地说明本申请实施例的技术方案，下面将对本申请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申请的一些实施例，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。

图 1 是本申请实施例 1 中区块链上用户通信加密方法的一流程图。

图 2 是图 1 中步骤 S10 的一具体流程图。

图 3 是图 2 中步骤 S20 的一具体流程图。

图 4 是图 1 中步骤 S30 的一具体流程图。

图 5 是图 1 中步骤 S40 的一具体流程图。

图 6 是图 1 中步骤 S10 之前的一具体流程图。

图 7 是图 1 中步骤 S60 的一具体流程图。

图 8 是本申请实施例 2 中区块链上用户通信加密装置的一原理框图。

图 9 是本申请实施例 4 中终端设备的一示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

实施例 1

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：

S10：用户 A 向用户 B 发送第一加密信息。

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。

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。

S20：用户 B 接收第一加密信息，解密后获取第一随机数。

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。

S30：用户 B 向用户 A 发送第二加密信息。

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。

S40：用户 A 接收第二加密信息，解密后获取第二随机数。

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。

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。

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。

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。

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。

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。

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。

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：

S11：用户 A 从用户 B 的用户证书中获取第二公钥。

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。

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。

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。

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。

S13：用户 A 通过区块链系统向用户 B 发送第一加密信息。

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：

第一种通信方式，在区块链上设置用户的通信地址，以便基于该通信地址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。

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。

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：

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。

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。

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。

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 采用与第二公钥相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。

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。

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：

S31：用户 B 从用户 A 的用户证书中获取第一公钥。

与步骤 S11 相似，参考步骤 S11 的实现过程，在此不再赘述。

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。

与步骤 S12 相似，参考步骤 S11 的实现过程，在此不再赘述。

S33: 用户 B 通过区块链系统向用户 A 发送第二加密信息。

与步骤 S13 相似，参考步骤 S11 的实现过程，在此不再赘述。

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：

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。

与步骤 S21 相似，参考步骤 S21 的实现过程，在此不再赘述。

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。

与步骤 S22 相似，参考步骤 S22 的实现过程，在此不再赘述。

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：

S101: 用户 A 和用户 B 预先查询各自的本地数据库。

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。

S102: 若本地数据库中不存在密钥 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。

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。

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。

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。

在一具体实施方式中，步骤 S50 中，密钥生成算法具体为：

$$C(0) = \text{Hash}(\text{random1})$$

$$C(n) = \text{HMAC}_{C(n-1)}(\text{Hash}(\text{random2}))$$

$$\text{Key} = \text{HMAC}_{\text{Hash}(\text{random1}||\text{random2})}(C0 + C1)$$

$$\text{IV} = \text{HMAC}_{\text{Hash}(\text{random1}||\text{random2})}(C0 + C2)$$

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。

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。

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。

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：

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。

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， $KC = \text{AES_CBC}(K)$ 。

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， $VC = \text{AES_CBC}(V)$ 。

S64：用户 A 将数据 {KC：VC+IV} 写到区块链上。

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。

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， $K = \text{AES_CBC}(KC)$ 。

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， $V = \text{AES_CBC}(VC)$ 。

S68：用户 B 获取数据 K：V。

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。

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。

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。

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，而不对本申请实施例的实施过程构成任何限定。

实施例 2

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

优选地, 密钥生成算法为:

$$C(0) = \text{Hash}(\text{random1})$$

$$C(n) = \text{HMAC}_{C(n-1)}(\text{Hash}(\text{random2}))$$

$$\text{Key} = \text{HMAC}_{\text{Hash}(\text{random1} \parallel \text{random2})}(C0 + C1)$$

$$\text{IV} = \text{HMAC}_{\text{Hash}(\text{random1} \parallel \text{random2})}(C0 + C2)$$

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。

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。

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。

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， $KC = \text{AES_CBC}(K)$ 。

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， $VC = \text{AES_CBC}(V)$ 。

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。

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。

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， $K = \text{AES_CBC}(KC)$ 。

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， $V = \text{AES_CBC}(VC)$ 。

数据获取单元 68，用于用户 B 获取数据 K: V。

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。

实施例 3

本实施例提供一个或多个存储有计算机可读指令的非易失性可读存储介质，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个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，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个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。

实施例 4

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 上运行的计算机可读指令 83。处理器 81 执行计算机可读指令 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 执行计算机可读指令 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。

示例性的，计算机可读指令 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，以完成本申请。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可读指令 83 的指令段，该指令段用于描述计算机可读指令 83 在终端设备 80 中的执行过程。例如，计算机可读指令 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。

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。

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。

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 用于存储计算机可读指令 83 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。

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。

另外，在本申请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。

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，可以存储在一个计算机可读存储介质中。基于这样的理解，本申请实现上述实施例方法中的全部或部分流程，也可以通过计算机可读指令 83 来指令相关的硬件来完成，所

述的计算机可读指令可存储于一计算机可读存储介质中，该计算机可读指令 83 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，所述计算机可读指令 83 包括计算机可读指令的代码，所述计算机可读指令的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可读指令的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。

以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，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申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。

权 利 要 求 书

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:

$$C(0) = \text{Hash}(\text{random1})$$

$$C(n) = \text{HMAC}_{C(n-1)}(\text{Hash}(\text{random2}))$$

$$\text{Key} = \text{HMAC}_{\text{Hash}(\text{random1}||\text{random2})}(C0 + C1)$$

$$\text{IV} = \text{HMAC}_{\text{Hash}(\text{random1}||\text{random2})}(C0 + C2)$$

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, $KC = \text{AES_CBC}(K)$;

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, $VC = \text{AES_CBC}(V)$;

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, $K = \text{AES_CBC}(KC)$;

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, $V = \text{AES_CBC}(VC)$;

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可读指令, 其特征在于, 所述处理器执行所述计算机可读指令时实现如下步骤:

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。

10. 根据权利要求 9 所述的终端设备, 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。

11. 根据权利要求 10 所述的终端设备, 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。

12. 根据权利要求 9 所述的终端设备，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不存在所述密钥 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。

13. 根据权利要求 9 所述的终端设备，其特征在于，所述密钥生成算法为：

$$C(0) = \text{Hash}(\text{random1})$$

$$C(n) = \text{HMAC}_{C(n-1)}(\text{Hash}(\text{random2}))$$

$$\text{Key} = \text{HMAC}_{\text{Hash}(\text{random1}||\text{random2})}(C0 + C1)$$

$$\text{IV} = \text{HMAC}_{\text{Hash}(\text{random1}||\text{random2})}(C0 + C2)$$

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。

14. 根据权利要求 9 所述的终端设备，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， $KC = \text{AES_CBC}(K)$ ；

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， $VC = \text{AES_CBC}(V)$ ；

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， $K = \text{AES_CBC}(KC)$ ；

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， $V = \text{AES_CBC}(VC)$ ；

用户 B 获取所述数据 K: V。

15. 一个或多个存储有计算机可读指令的非易失性可读存储介质，其特征在于，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行如下步骤：

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。

16. 根据权利要求 15 所述的非易失性可读存储介质，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。

17. 根据权利要求 16 所述的非易失性可读存储介质，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。

18. 根据权利要求 15 所述的非易失性可读存储介质，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。

19. 根据权利要求 15 所述的非易失性可读存储介质，其特征在于，所述密钥生成算法为：

$$C(0) = \text{Hash}(\text{random1})$$

$$C(n) = \text{HMAC}_{C(n-1)}(\text{Hash}(\text{random2}))$$

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

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

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。

20. 根据权利要求 15 所述的非易失性可读存储介质, 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。

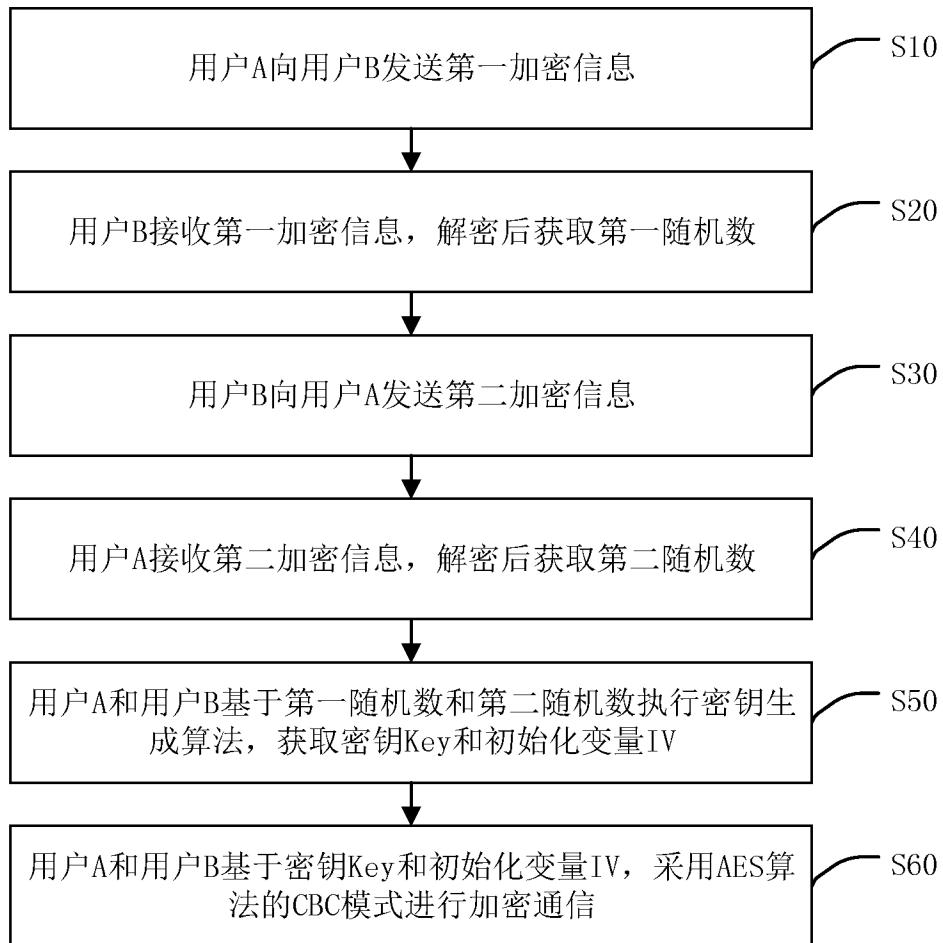


图 1

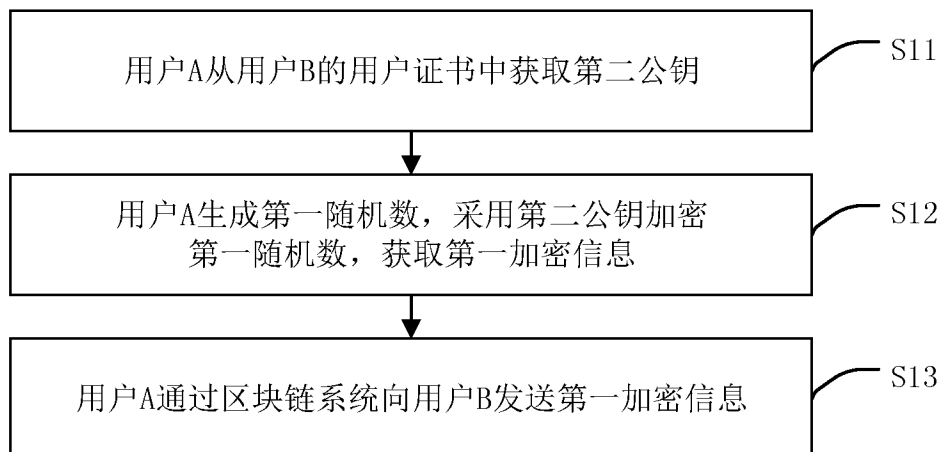


图 2

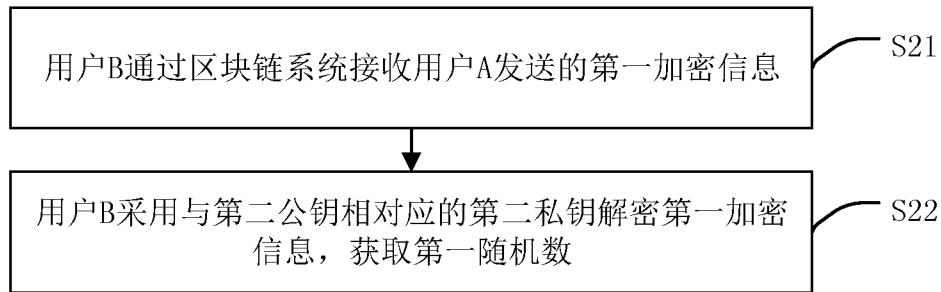


图 3

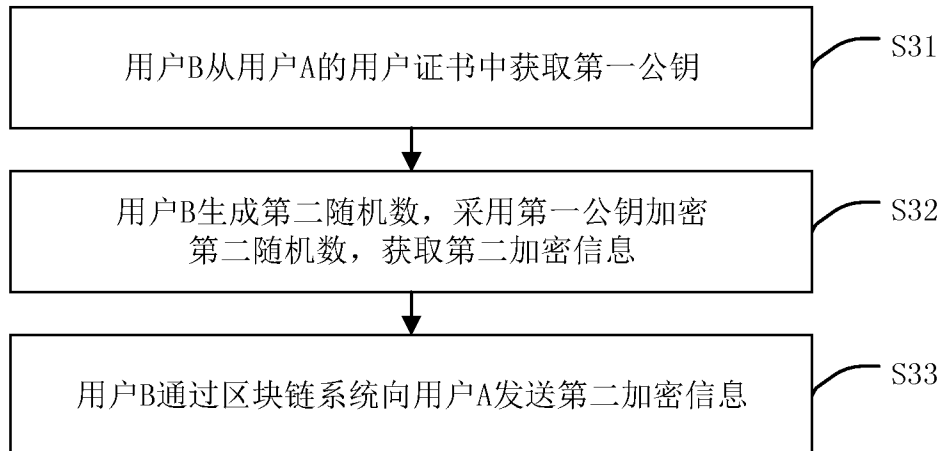


图 4

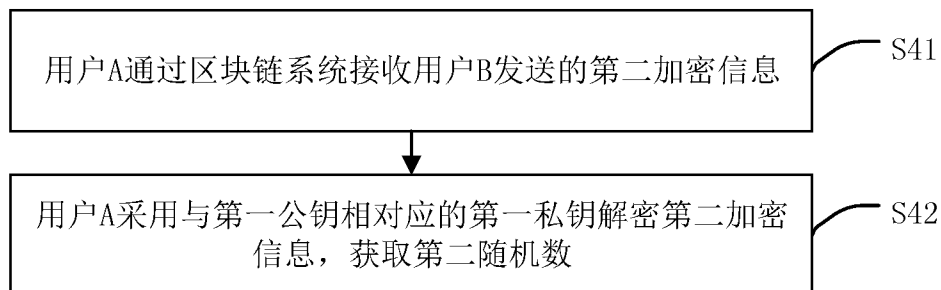


图 5

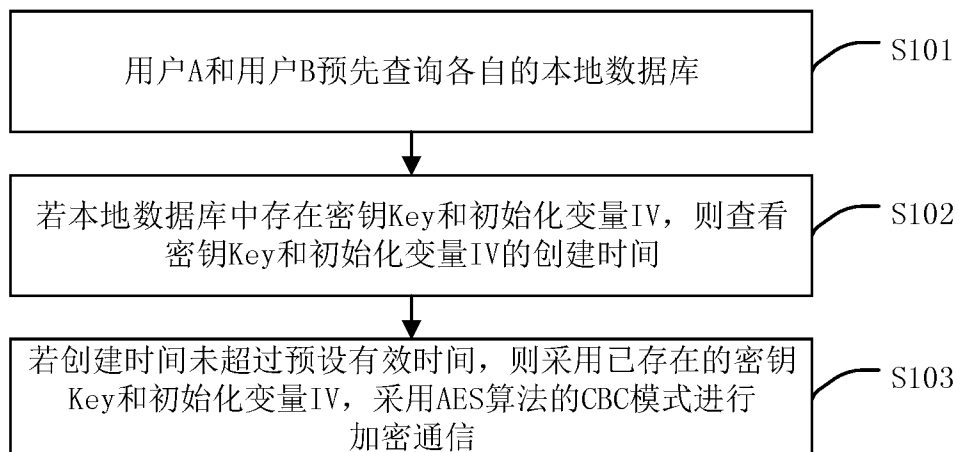


图 6

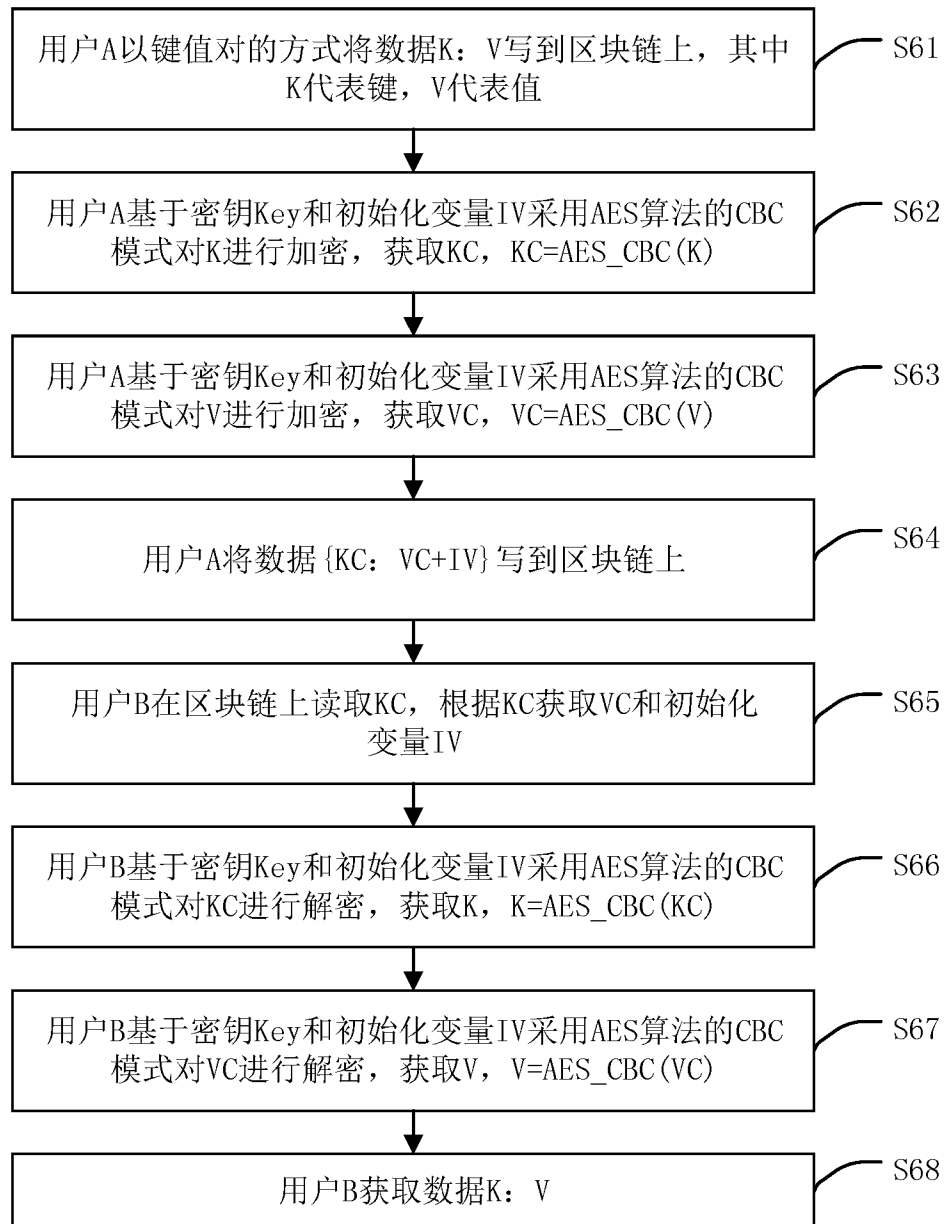


图 7

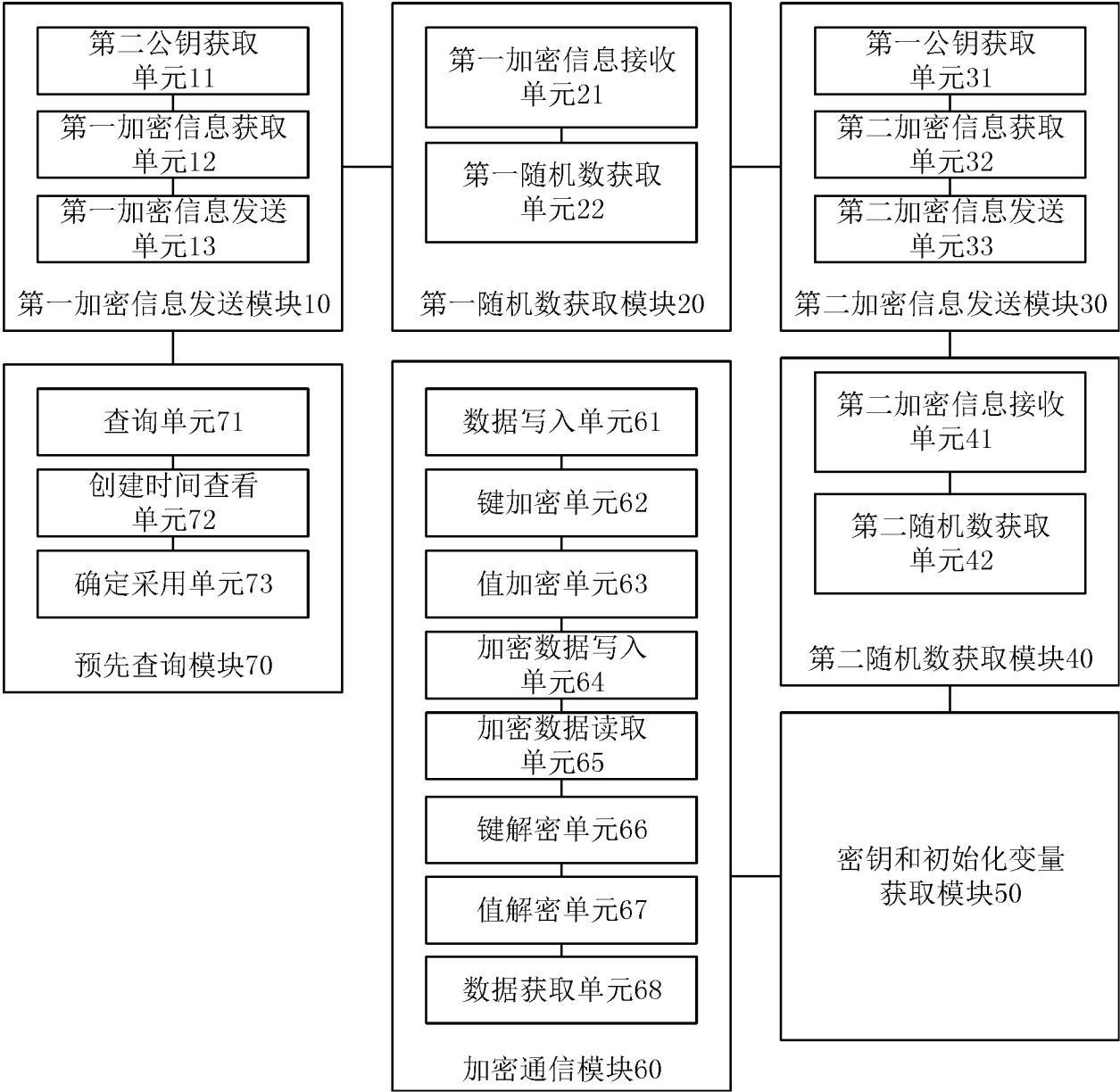


图 8

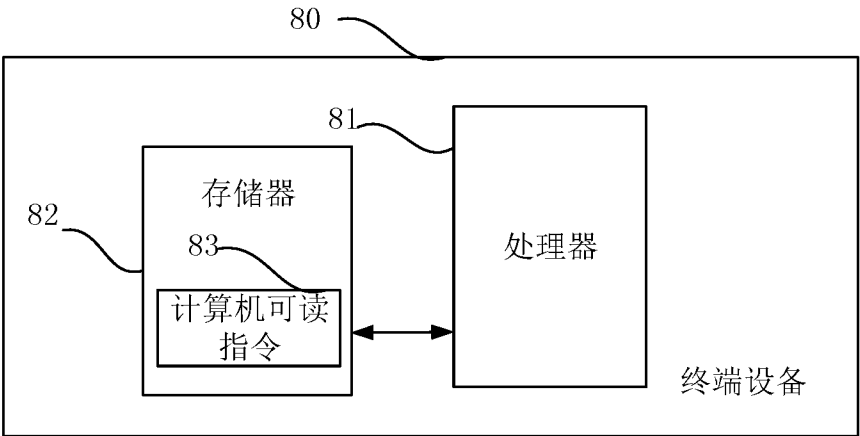


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/095907

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i; H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

VEN; CNABS; CNTXT; USTXT; EPTXT; WOTXT; CNKI: 区块链, 加密, 解密, 随机数, 交换, 生成, 密钥, 共享, 初始化, 向量, 变量, AES, CBC, block chain, encrypt+, decrypt+, random, number, exchange+, generat+, key?, IV, shar+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 106209360 A (ANHUI WANTONG POST AND TELECOMMUNICATIONS CO., LTD.) 07 December 2016 (2016-12-07) description, paragraphs [0001]-[0012]	1-5, 7-13, 15-19
A	CN 106779707 A (BANKNOTE CREDIT CARD INDUSTRY DEVELOPMENT CO., LTD.; BEIJING SMART CARD TECHNOLOGY RESEARCH INSTITUTE) 31 May 2017 (2017-05-31) entire document	1-20
A	US 2015149788 A1 (NVIDIA CORPORATION) 28 May 2015 (2015-05-28) entire document	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

16 November 2018

Date of mailing of the international search report

12 December 2018

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/095907

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	106209360	A	07 December 2016	None			
CN	106779707	A	31 May 2017	None			
US	2015149788	A1	28 May 2015	US	9274979	B2	01 March 2016

国际检索报告

国际申请号

PCT/CN2018/095907

A. 主题的分类

H04L 9/08(2006.01)i; H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

VEN;CNABS;CNTXT;USTXT;EPTXT;WOTXT;CNKI: 区块链, 加密, 解密, 随机数, 交换, 生成, 密钥, 共享, 初始化, 向量, 变量, AES, CBC, block chain, encrypt+, decrypt+, random, number, exchang+, generat+, key?, IV, shar+

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 106209360 A (安徽皖通邮电股份有限公司) 2016年 12月 7日 (2016 - 12 - 07) 说明书第[0001]-[0012]段	1-5, 7-13, 15-19
A	CN 106779707 A (中钞信用卡产业发展有限公司北京智能卡技术研究院) 2017年 5月 31日 (2017 - 05 - 31) 全文	1-20
A	US 2015149788 A1 (NVIDIA CORP) 2015年 5月 28日 (2015 - 05 - 28) 全文	1-20

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2018年 11月 16日

国际检索报告邮寄日期

2018年 12月 12日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

郝玉香

电话号码 86-512-88996092

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/095907

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	106209360	A	2016年 12月 7日	无			
CN	106779707	A	2017年 5月 31日	无			
US	2015149788	A1	2015年 5月 28日	US	9274979	B2	2016年 3月 1日