(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
2020 年 9 月 17 日 (17.09.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/181842 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) *H04L 29/08* (2006.01)

(21) 国际申请号: PCT/CN2019/123026

(22) 国际申请日: 2019 年 12 月 4 日 (04.12.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910189512.X 2019年3月13日 (13.03.2019) 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（入驻深圳市前海商务秘书有限公司）, Guangdong 518000 (CN)。

(72) 发明人: 张小利 (ZHANG, Xiaoli); 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（入驻深圳市前海商务秘书有限公司）, Guangdong 518000 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (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, 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,

(54) **Title:** METHOD AND APPARATUS FOR QUICKLY SWITCHING DEPLOYMENT KEYS, COMPUTER DEVICE AND STORAGE MEDIUM

(54) **发明名称**: 快速切换部署密钥的方法、装置、计算机设备和存储介质

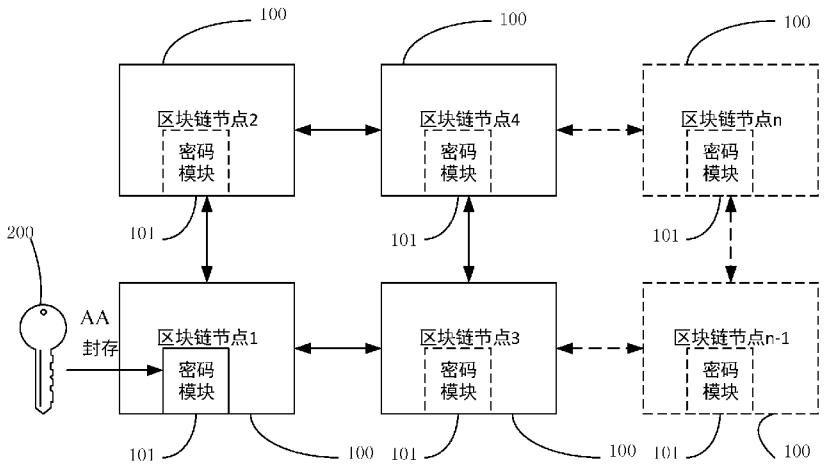

图 1

100 Blockchain node 101 Cryptographic module AA Encapsulation

(57) **Abstract:** Disclosed are a method and apparatus for quickly switching deployment keys, a computer device and a storage medium, wherein same fall within the technical field of key management, and are applied to a blockchain network composed of at least two nodes. The method for quickly switching deployment keys comprises: creating a cryptographic module in a node of the blockchain network, wherein the node where the cryptographic module is created is a first node; encapsulating a private key of the first node in the cryptographic module; and synchronously deploying the private key along with the cryptographic module to nodes other than the first node in the blockchain network, wherein the private key can only be accessed by means of entering the cryptographic module via a specific interface. In this way, private keys are quickly switched and deployed while ensuring that the private keys are secure and are not published.

WO 2020/181842 A1

[见续页]

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))。

(57) 摘要：本公开揭示了一种快速切换部署密钥的方法、装置、计算机设备和存储介质，属于密钥管理技术领域，应用于由至少两个节点组成的区块链网络中，所述快速切换部署密钥的方法包括：在所述区块链网络的一个节点中创建密码模块，所述创建有所述密码模块的节点为第一节点；将所述第一节点的私钥封存在所述密码模块中；将所述私钥随所述密码模块同步部署到所述区块链网络中除所述第一节点外的其他节点，其中，所述私钥只能通过特定接口进入密码模块进行访问。这样在保证私钥安全不公开的前提下实现了私钥的快速切换部署。

快速切换部署密钥的方法、装置、计算机设备和存储介质

本申请要求于 2019 年 03 月 13 日提交中国专利局、申请号为201910189512.X、申请名称为“快速切换部署密钥的方法、装置、计算机设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本公开涉及密钥管理技术领域，特别是涉及快速切换部署密钥的方法、装置、计算机设备和存储介质。

背景技术

现有技术中，私钥的安全影响整个加密系统的安全，传统方法私钥保存在加密卡，而传统的加密机或者加密卡是需要外购的，并且需要插入到设备或者连接到外部设备，由系统管理员来统一维护，这样，加密机中对硬件设备依赖性较强，不便于快速切换及部署。有的私钥甚至明文保存在本地，这种方式对系统安全构成很大的潜在危险。

发明内容

基于此，为解决相关技术中在保证安全的前提下，私钥的切换部署不方便的技术问题，本公开提供了一种快速切换部署密钥的方法、装置、计算机设备和存储介质。

第一方面，提供了一种快速切换部署密钥的方法，应用于由至少两个节点组成的区块链网络中，包括：

在所述区块链网络的一个节点中创建密码模块，所述创建有所述密码模块的节点为第一节点；

将所述第一节点的私钥封存在所述密码模块中；

将所述私钥随所述密码模块同步部署到所述区块链网络中除所述第一节点外的其他节点，其中，所述私钥只能通过特定接口进入密码模块进行访问。

第二方面，提供了一种快速切换部署密钥的装置，包括：

创建单元，用于在所述区块链网络的一个节点中创建密码模块，所述创建

有所述密码模块的节点为第一节点；

封存单元，用于将所述第一节点的私钥封存在所述密码模块中；

同步单元，用于将所述私钥随所述密码模块同步部署到所述区块链网络中除所述第一节点外的其他节点，其中，所述私钥只能通过特定接口进入密码模块进行访问。

第三方面，提供了一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行上述所述快速切换部署密钥的方法的步骤。

第四方面，提供了一种存储有计算机可读指令的存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行上述所述快速切换部署密钥的方法的步骤。可选的，该存储介质可以为非易失性存储介质，或者称为计算机非易失性可读存储介质。

本公开的实施例提供的技术方案保证了私钥在传输过程中不会公开，保证了私钥的安全性，实现了快速切换部署。

附图说明

图 1 是一个实施例中提供的快速切换部署密钥的方法的实施环境图。

图 2 是根据一示例性实施例示出的一种快速切换部署密钥的方法的流程图。

图 3 是根据图 2 对应实施例示出的快速切换部署密钥的方法中步骤 S200 的一种具体实现流程图。

图 4 是根据图 3 对应实施例示出的快速切换部署密钥的方法中步骤 S230 的一种具体实现流程图。

图 5 是根据图 3 对应实施例示出的快速切换部署密钥的方法中步骤 S210 的一种具体实现流程图。

图 6 是根据图 2 对应实施例示出的快速切换部署密钥的方法中步骤 S100 的一种具体实现流程图。

图 7 是根据图 2 对应实施例示出的快速切换部署密钥的方法中步骤 S100 的一种具体实现流程图。

图 8 是根据一示例性实施例示出的一种快速切换部署密钥的装置的框图。

图 9 示意性示出一种用于实现上述快速切换部署密钥的方法的电子设备示例框图。

图 10 示意性示出一种用于实现上述快速切换部署密钥的方法的计算机可读存储介质。

具体实施方式

以下结合附图及实施例，对本公开进行进一步详细说明。

图 1 为一个实施例中提供的快速切换部署密钥的方法的实施环境图，如图 1 所示，在所述实施环境中，包括组成区块链网络的多个节点 100 和私钥 200。

所述上可以建立密码模块隔绝外界联系。首先区块链网络的其中一个节点 100 在上开辟一个存储区域，建立密码模块 101，所述密码模块 101 有明确的边界，使密码模块 101 内部的环境和外部环境隔绝开，仅保留部分接口用以与外界联系。将所述私钥 200 封存入密码模块 101 中，然后将所述密钥 200 随密码模块 101 同步到区块链网络中，这样区块链网络中的每一个节点 100 都部署有私钥 200，实现了私钥 200 的快速部署。但是要获取私钥 200，必须要破解密码模块 101，这样就保证了私钥 200 的安全

需要说明的是，所述区块链网络节点 100 可为智能手机、平板电脑、笔记本电脑、台式计算机等，但并不局限于此。区块链网络节点 100 两两之间可以通过蓝牙、USB(Universal Serial Bus，通用串行总线）或者其他通讯连接方式进行连接，本公开在此不做限制。

如图 2 所示，在一个实施例中，提出了一种快速切换部署密钥的方法，所述快速切换部署密钥的方法可以应用于上述的中，应用于由至少两个节点组成的区块链网络中，具体可以包括以下步骤：

步骤 S100，在所述区块链网络的一个节点中创建密码模块，所述创建有所述密码模块的节点为第一节点；

本公开的主要目的是提供一种能够快速切换部署的加密方法，其具体方法是，在区块链网络的一个节点中开辟一个存储区域用于存储私钥，由于私钥不能公开，所以本公开在存储区域中新建一个密码模块，用于将私钥封存在密码

模块中，以隔绝所述私钥与外界的联系。所述密码模块是有严格的密码边界阻隔外部与内部的联系，如果想要读取密码模块内部的私钥，只能通过特定的接口读取，保证了私钥的安全性。所述密码模块的密码边界可以是执行在可修改的运行环境中的软件部件划定界线。所述特定的接口包括数据输入接口、数据输出接口、控制输入接口以及状态输出接口。

步骤 S200，将所述第一节点的私钥封存在所述密码模块中；

在建立好所述密码模块后，就可以通过所述特定接口，将私钥输入到密码模块中，完成密码模块的封存。

步骤 S300，将所述私钥随所述密码模块同步部署到所述区块链网络中除所述第一节点外的其他节点，其中，所述私钥只能通过特定接口进入密码模块进行访问。

当私钥封存在密码模块后，就会随密码模块一起同步到区块链的所有节点中，所有的区块链都有了所述密码模块以及密码模块中封存的私钥，只要有设备加入区块链中，就可以获取所述密码模块以及密码模块中封存的私钥，这样就使得私钥随密码模块一起部署到所述区块链网络的所有节点中，以备所述第一节点损坏后，在区块链网络的其他节点中选择一个节点继续使用，也就实现了私钥的快速切换部署。而且所述私钥仍在封存在密码模块中，仍需要通过特定的接口去读取，也就同时保证了私钥的私密性和安全性。

本公开通过区块链网络和密码模块，将部署在所述区块链网络的第一节点中的私钥封存入密码模块后，随密码模块一起部署至所述区块链网络的所有节点中，在所述第一节点损坏后，在区块链网络的其他节点中选择一个节点继续使用，也就实现了私钥的快速切换部署。同时，由于私钥在区块链网络中至始至终被封存于密码模块中，所以其私密性和安全性也得到了保障。而且由于区块链有不可篡改的特性，也保证了所述私钥和所述密码模块不会被篡改为其他数据。

可选地，图 3 是根据图 2 对应实施例示出的快速切换部署密钥的方法中步骤 S200 的细节描述，所述快速切换部署密钥的方法中，所述密码模块数量有至少两个，步骤 S200 可以包括以下步骤：

步骤 S210，拆分所述私钥为与所述密码模块数量对应的数量个部分；

本公开的一个实施例中，在区块链节点中创建密码模块时，可以创建多个密码模块，然后根据所述密码模块的数量，将私钥拆分成对应数量个部分，分开存储，这样会使得存储在密码模块中的私钥更加难以破解，可以有效提高所述私钥的安全性。所述拆分方式可以是随机拆分，也可以是按照预定规则拆分，本公开在此不做限定，具体实施方式后面的实施例会详细阐述。

步骤 S220，将所述私钥的不同部分分别存储在不同的密码模块中，每个密码模块只存储一个部分的私钥；

在将私钥拆分完毕后，就可以将所述私钥的各个部分分别存储至所述密码模块中。所述存储方式可以是随机分配，也可以是按照预定规则存储，只要保证所述私钥的每一个部分都有一个独立的密码模块用以存储即可，本公开在此不做限定。这样，如果想要破解所述私钥，就需要将所有存储有所述私钥的各个部分的密码模块都破解掉，加大了破解的难度，提高了所述私钥的安全性。

步骤 S230，生生成私钥的存储顺序，并将所述存储顺序动态加密，并存储在所述第一节点。

将所述私钥的各个部分存储在密码模块中后，还需要生成所述私钥的存储顺序，所述存储顺序是将所述个部分重新拼接在一起形成一个完整的私钥的唯一凭据，一般由所述私钥的所有人掌握，但是在区块链节点中，由于所有数据都是共享的，所以为了保证所述私钥的安全性，还需要对所述存储顺序进行动态加密，保证所述私钥的安全性。

本公开的一个实施例中，在区块链节点中创建密码模块时，会创建多个密码模块，然后根据所述密码模块的数量，将私钥拆分成对应数量个部分，然后每一个密码模块存储私钥的一个部分，并生成一个存储顺序。最后把这个存储顺序动态加密后存储起来。如果要获取完整的私钥，就需要从所有的密码模块中读取数据，获得私钥的所有部分并将这些部分按顺序拼接起来，才能获得完整的私钥，这样增加了私钥存储的安全性。

可选地，图 4 是根据图 3 对应实施例示出的快速切换部署密钥的方法中步骤 S230 的细节描述，所述快速切换部署密钥的方法中，所述存储顺序为一串字符串，步骤 S230 可以包括以下步骤：

步骤 S231，获取需要加密的存储顺序字符串并进行存储；

在对所述存储顺序进行加密时，首先需要获取所述存储顺序并进行存储，以方便对所述存储顺序数据做处理，此时所述存储顺序数据可以看作为一串字符串存储在本地设备中。

步骤 S232，对所述存储顺序的指定特征信息进行指定摘要运算；

在获取所述存储顺序并进行存储后，就可以对所述存储顺序的指定特征进行摘要运算了，所述指定特征信息可以是所述存储顺序的字符串长度等，所述摘要运算的方法例如是哈希运算、随机生成一个数字除存储顺序的字符串长度取余等，本方案不做限定。以所述指定特征信息是所述存储顺序的字符串长度，所述摘要运算的方法为随机生成一个数字除存储顺序的字符串长度取余为例，假设所述存储顺序的字符串长度为 a，随机生成的数字为 b，则可以得到 a 除 b 的余数，所述余数即为指定摘要运算的结果。

步骤 S233，根据所述指定摘要运算的结果，确定对所述存储顺序进行加密的起始字符；

经过摘要运算后得到一个数值，可以将所述数值作为加密起始字符的位数，也可以将其前几位或者后几位作为加密起始字符的位数，这样就确定好了对所述存储顺序进行加密的起始字符。步骤 S234，从所述起始字符开始，在所述的存储顺序字符串中获取加密密钥；

确定加密起始字符的位数后，就可以对所述存储顺序字符串进行加密，加密方法可以是从起始字符开始，每隔预定位数进行摘取，摘取到预定长度，组成加密密钥，所述预定位数可以是 1 位、2 位、质数位等，所述预定长度可以是所述存储顺序字符串的长度，也可以是 20 位、304 位，所述预定位数和所述预定长度均可以按照具体情况设置，本方案不做限定。

步骤 S235，根据预定的加密算法，使用所述加密密钥对所述存储顺序字符串进行加密；

获取加密密钥后，按照预定算法，使用所述加密密钥对所述存储数据字符串进行加密，其中，所述预定算法即生成所述加密密钥的算法。

步骤 S236，发送加密后的存储顺序字符串。

加密完成后，就可以将所述加密后的存储数据字符串发送至区块链网络的其他节点。

本公开的一个实施例中，动态加密运算将存储顺序动态加密的具体方法可以是，先获取所述要加密的存储顺序，然后对所述存储顺序的指定特征信息进行摘要运算，所述指定特征信息可以是所述存储顺序的字符串长度等，所述摘要运算的方法例如是哈希运算、随机生成一个数字除存储顺序的字符串长度取余等，本方案不做限定。经过摘要运算后得到一个数值，将所述数值作为加密起始字符的位数，对所述存储顺序字符串进行加密，加密方法可以是从起始字符开始，每隔 1 位进行摘取，摘取到预定长度，组成加密密钥，所述预定长度可以按照具体情况设置，本方案不做限定，获取加密密钥后，按照预定算法，对所述存储数据字符串进行加密，加密完成后，将所述加密后的存储数据字符串发送至区块链网络的其他节点。

可选的，图 5 是根据图 3 对应实施例示出的快速切换部署密钥的方法中步骤 S210 的细节描述，所述快速切换部署密钥的方法中，步骤 S210 可以包括以下步骤：

步骤 S211，读取所述私钥的长度；

若需要拆分所述私钥，需要先测量所述私钥的长度。

步骤 S212，将所述私钥平均分成长度一致的与所述密码模块数量对应的数量个部分。

本公开的一个实施例中，拆分所述私钥为与所述密码模块数量对应的数量个部分的方法可以是根据所述密码模块的数量将所述私钥随机拆分为与所述密码模块的数量相同部分个，所述每个部分的长度平均分配，即每个部分的长度均相等。由于私钥每个部分的长度均相等，所以在存储过程中每个密码模块内存储的私钥部分的长度是相同的，就增加了密码模块拼接的难度。

可选地，对应图 3 对应实施例示出的快速切换部署密钥的方法中步骤 S210，所述快速切换部署密钥的方法中，所述区块链网络的各节点中还包含有密码模块存储长度的预定阈值，步骤 S210 还可以包括以下步骤：

拆分所述私钥为与所述密码模块数量对应的数量个部分，所述每个部分的长度均不超过密码模块存储长度的预定阈值。

本公开的另一个实施例中，拆分所述私钥为与所述密码模块数量对应的数量个部分的方法还可以是根据所述密码模块的数量将所述私钥分配为与所述

密码模块的数量相同部分个，所述每个部分的长度均不超过密码模块存储长度的预定阈值。这样可以保证部分私钥中部分重要的数据不会被分割为两部分。所述预定阈值例如是 32 位、64 位、128 位等，本公开在此不做限定。

可选地，图 6 是根据图 2 对应实施例示出的快速切换部署密钥的方法中步骤 S100 的细节描述，所述快速切换部署密钥的方法中，所述区块链网络的各节点中还包含有私钥长度与密码模块数量的对应关系，步骤 S100 还可以包括以下步骤：

步骤 S110，读取所述私钥的长度；

本公开的另一个实施例中，密码模块有多个，在区块链的一个节点中创建密码模块的具体方法可以是，根据所述私钥长度，查询保存在区块链中的私钥长度与密码模块数量的对应关系，决定密码模块创建的数量。所

步骤 S120，查询私钥长度与密码模块数量的对应关系，确定需要创建的密码模块的数量；

述私钥长度与密码模块数量的对应关系可以根据具体情况设置，例如密码长度为 32 位以下时创建 1 个密码模块、32 位至 64 位时创建 2 个密码模块、96 位至 128 位时创建 4 个密码模块等，创建本公开在此不做限定。

步骤 S130，创建与所述私钥长度对应的数量个密码模块。

这样就可以根据私钥的长度灵活设置密码模块的数量和重新拼接的难度，一般而言，私钥长度越长，越难破解，证明所述私钥也越重要，也就需要拆分为更多的部分。

可选的，图 7 是根据图 2 对应实施例示出的快速切换部署密钥的方法中步骤 S100 的细节描述，所述快速切换部署密钥的方法中，所述区块链网络的各节点中还包含有密码模块存储长度的预定阈值，步骤 S100 还可以包括以下步骤：

步骤 S101，判断所述私钥的长度是否超过密码模块存储长度的预定阈值；

本公开的另一个实施例中，密码模块有多个，在区块链的一个节点中创建密码模块的具体方法还可以是，根据区块链中存储的密码模块存储长度的预定阈值，决定私钥被拆分为几个部分，所述每个部分的长度都不超过密码模块存储长度的预定阈值，然后创建与所述私钥部分的数量对应的数量个密码模块。

所述预定阈值例如是 32 位、64 位、128 位等，本公开在此不做限定。

步骤 S102，若所述私钥的长度超过密码模块存储长度的预定阈值，拆分所述私钥为至少两个部分，所述每个部分的长度都不超过密码模块存储长度的预定阈值；

这样存储，可以据私钥的长度灵活设置密码模块的数量和重新拼接的难度，使得私钥的安全保障更有针对性。

步骤 S103，创建与所述私钥部分的数量对应的数量个密码模块。

这样也可以根据私钥的长度灵活设置密码模块的数量和重新拼接的难度，一般而言，私钥长度越长，越难破解，证明所述私钥也越重要，也就需要拆分为更多的部分，而这种方法相对于图 6 示出的方法，区块链中不再用保存一个私钥长度与密码模块数量的对应关系，而是一个预定阈值，节约了存储的空间。

如图 8 所示，在一个实施例中，提供了一种快速切换部署密钥的装置，该快速切换部署密钥的装置可以集成于上述的计算机设备 100 中，具体可以包括创建单元 110、封存单元 120、同步单元 130。

创建单元 110，用于在区块链的一个节点中创建密码模块；

封存单元 120，用于将所述节点的私钥封存在所述密码模块中；

同步单元 130，用于将所述私钥随所述密码模块同步到其他区块链节点，所述私钥只能通过特定接口进入密码模块进行访问。

上述装置中各个模块的功能和作用的实现过程具体详见上述快速切换部署密钥的方法中对应步骤的实现过程，在此不再赘述。

应当注意，尽管在上文详细描述中提及了用于动作执行的设备的若干模块或者单元，但是这种划分并非强制性的。实际上，根据本公开的实施方式，上文描述的两个或更多模块或者单元的特征和功能可以在一个模块或者单元中具体化。反之，上文描述的一个模块或者单元的特征和功能可以进一步划分为由多个模块或者单元来具体化。

此外，尽管在附图中以特定顺序描述了本公开中方法的各个步骤，但是，这并非要求或者暗示必须按照该特定顺序来执行这些步骤，或是必须执行全部所示的步骤才能实现期望的结果。附加的或备选的，可以省略某些步骤，将多个步骤合并为一个步骤执行，以及/或者将一个步骤分解为多个步骤执行等。

通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本公开实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中或网络上，包括若干指令以使得一台计算设备（可以是个人计算机、服务器、移动终端、或者网络设备等）执行根据本公开实施方式的方法。

在本公开的示例性实施例中，还提供了一种能够实现上述方法的电子设备。

所属技术领域的技术人员能够理解，本公开的各个方面可以实现为系统、方法或程序产品。因此，本公开的各个方面可以具体实现为以下形式，即：完全的硬件实施方式、完全的软件实施方式（包括固件、微代码等），或硬件和软件方面结合的实施方式，这里可以统称为“电路”、“模块”或“系统”。

下面参照图 9 来描述根据本公开的这种实施方式的电子设备 500。图 9 显示的电子设备 500 仅仅是一个示例，不应对本公开实施例的功能和使用范围带来任何限制。

如图 9 所示，电子设备 500 以通用计算设备的形式表现。电子设备 500 的组件可以包括但不限于：上述至少一个处理单元 510、上述至少一个存储单元 520、连接不同系统组件（包括存储单元 520 和处理单元 510）的总线 530。

其中，所述存储单元存储有程序代码，所述程序代码可以被所述处理单元 510 执行，使得所述处理单元 510 执行本说明书上述“示例性方法”部分中描述的根据本公开各种示例性实施方式的步骤。例如，所述处理单元 510 可以执行如图 2 中所示的步骤 S100，在区块链的一个节点中创建密码模块；步骤 S200，将所述节点的私钥封存在所述密码模块中；步骤 S300，将所述私钥随所述密码模块同步到其他区块链节点，所述私钥只能通过特定接口进入密码模块进行访问。

存储单元 520 可以包括易失性存储单元形式的可读介质，例如随机存取存储单元（RAM）5201 和/或高速缓存存储单元 5202，还可以进一步包括只读存储单元（ROM）5203。

存储单元 520 还可以包括具有一组（至少一个）程序模块 5205 的程序/实用工具 5204，这样的程序模块 5205 包括但不限于：操作系统、一个或者多

个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。

总线 530 可以为表示几类总线结构中的一种或多种，包括存储单元总线或者存储单元控制器、外围总线、图形加速端口、处理单元或者使用多种总线结构中的任意总线结构的局域总线。

电子设备 500 也可以与一个或多个外部设备 700（例如键盘、指向设备、蓝牙设备等）通信，还可与一个或者多个使得用户能与该电子设备 500 交互的设备通信，和/或与使得该电子设备 500 能与一个或多个其它计算设备进行通信的任何设备（例如路由器、调制解调器等等）通信。这种通信可以通过输入/输出（I/O）接口 550 进行。并且，电子设备 500 还可以通过网络适配器 560 与一个或者多个网络（例如局域网（LAN），广域网（WAN）和/或公共网络，例如因特网）通信。如图所示，网络适配器 560 通过总线 530 与电子设备 500 的其它模块通信。应当明白，尽管图中未示出，可以结合电子设备 500 使用其它硬件和/或软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID 系统、磁带驱动器以及数据备份存储系统等。

通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本公开实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中或网络上，包括若干指令以使得一台计算设备（可以是个人计算机、服务器、终端装置、或者网络设备等）执行根据本公开实施方式的方法。

在本公开的示例性实施例中，还提供了一种计算机可读存储介质，其上存储有能够实现本说明书上述方法的程序产品。在一些可能的实施方式中，本公开的各个方面还可以实现为一种程序产品的形式，其包括程序代码，当所述程序产品在终端设备上运行时，所述程序代码用于使所述终端设备执行本说明书上述“示例性方法”部分中描述的根据本公开各种示例性实施方式的步骤。

参考图 10 所示，描述了根据本公开的实施方式的用于实现上述方法的程序产品 600，其可以采用便携式紧凑盘只读存储器(CD-ROM)并包括程序代码，并可以在终端设备，例如个人电脑上运行。然而，本公开的程序产品不限于此，

在本文件中，可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

所述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以为但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子（非穷举的列表）包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（EPROM 或闪存）、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

计算机可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了可读程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。可读信号介质还可以是可读存储介质以外的任何可读介质，该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于无线、有线、光缆、RF 等等，或者上述的任意合适的组合。

可以以一种或多种程序设计语言的任意组合来编写用于执行本公开操作的程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如 Java、C++等，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中，远程计算设备可以通过任意种类的网络，包括局域网(LAN)或广域网(WAN)，连接到用户计算设备，或者，可以连接到外部计算设备（例如利用因特网服务提供商来通过因特网连接）。

本申请通过在区块链网络的一个节点中开辟一个存储区域用于存储私钥，先在存储区域中新建一个密码模块，然后将私钥封存在密码模块中，以隔绝所述私钥与外界的联系，保证了私钥在传输过程中不会公开。所述密码模块是有严格的边界阻隔外部与内部的联系，如果想要读取密码模块内部的私钥，只能

通过特定的接口读取，保证了私钥的安全性。当私钥封存在密码模块后，就会随密码模块一起同步到区块链的所有节点中，所有的区块链都有了这个环境，只要有设备加入区块链中，就可以获取这个环境，这样就实现了快速切换部署。

上述附图所示的处理并不表明或限制这些处理的时间顺序。另外，这些处理可以是例如在多个模块中同步或异步执行的。

本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。

权利要求

1、一种快速切换部署密钥的方法，其特征在于，应用于由至少两个节点组成的区块链网络中，所述方法包括：

在所述区块链网络的一个节点中创建密码模块，所述创建有所述密码模块的节点为第一节点；

将所述第一节点的私钥封存在所述密码模块中；

将所述私钥随所述密码模块同步部署到所述区块链网络中除所述第一节点外的其他节点，其中，所述私钥只能通过特定接口进入密码模块进行访问。

2、如权利要求 1 所述的方法，其特征在于，所述密码模块数量有至少两个，所述将所述第一节点的私钥封存在所述密码模块中的步骤包括：

拆分所述私钥为与所述密码模块数量对应的数量个部分；

将所述私钥的不同部分分别存储在不同的密码模块中，每个密码模块只存储一个部分的私钥；

生成私钥的存储顺序，并将所述存储顺序动态加密，并存储在所述第一节点。

3、如权利要求 2 所述的方法，其特征在于，所述存储顺序为一串字符串，将所述存储顺序动态加密，并存储在所述第一节点，具体包括：

获取需要加密的存储顺序字符串并进行存储；

对所述存储顺序的指定特征信息进行指定摘要运算；

根据所述指定摘要运算的结果，确定对所述存储顺序进行加密的起始字符；

从所述起始字符开始，在所述的存储顺序字符串中获取加密密钥；

根据预定的加密算法，使用所述加密密钥对所述存储顺序字符串进行加密；

发送加密后的存储顺序字符串。

4、如权利要求 2 所述的方法，其特征在于，所述拆分所述私钥为与所述密码模块数量对应的数量个部分的步骤包括：

读取所述私钥的长度；

将所述私钥平均分成长度一致的与所述密码模块数量对应的数量个部分。

5、如权利要求 2 所述的方法，其特征在于，所述区块链网络的各节点中还包含有密码模块存储长度的预定阈值，所述拆分所述私钥为与所述密码模块

数量对应的数量个部分的步骤包括：

拆分所述私钥为与所述密码模块数量对应的数量个部分，所述每个部分的长度均不超过密码模块存储长度的预定阈值。

6、如权利要求 1 所述的方法，其特征在于，所述区块链网络的各节点中还包含有私钥长度与密码模块数量的对应关系，所述在所述区块链网络的一个节点中创建密码模块的步骤包括：

读取所述私钥的长度；

查询私钥长度与密码模块数量的对应关系，确定需要创建的密码模块的数量；

创建与所述私钥长度对应的数量个密码模块。

7、如权利要求 1 所述的方法，其特征在于，所述区块链网络的各节点中还包含有密码模块存储长度的预定阈值，所述在所述区块链网络的一个节点中创建密码模块的方法包括：

判断所述私钥的长度是否超过密码模块存储长度的预定阈值；

若所述私钥的长度超过密码模块存储长度的预定阈值，拆分所述私钥为至少两个部分，且所述每个部分的长度都不超过密码模块存储长度的预定阈值；

创建与所述私钥部分的数量对应的数量个密码模块。

8、一种快速切换部署密钥的装置，其特征在于，所述装置包括：

创建单元，用于在区块链网络的一个节点中创建密码模块，所述创建有所述密码模块的节点为第一节点；

封存单元，用于将所述第一节点的私钥封存在所述密码模块中；

同步单元，用于将所述私钥随所述密码模块同步部署到所述区块链网络中除所述第一节点外的其他节点，其中，所述私钥只能通过特定接口进入密码模块进行访问。

9、如权利要求 8 所述的装置，其特征在于，所述密码模块数量有至少两个，所述封存单元具体用于：

拆分所述私钥为与所述密码模块数量对应的数量个部分；

将所述私钥的不同部分分别存储在不同的密码模块中，每个密码模块只存储一个部分的私钥；

生成私钥的存储顺序，并将所述存储顺序动态加密，并存储在所述第一节点。

10、如权利要求 9 所述的装置，其特征在于，所述封存单元在存储顺序为一串字符串，将所述存储顺序动态加密，并存储在所述第一节点时，具体用于：

获取需要加密的存储顺序字符串并进行存储；

对所述存储顺序的指定特征信息进行指定摘要运算；

根据所述指定摘要运算的结果，确定对所述存储顺序进行加密的起始字符；

从所述起始字符开始，在所述的存储顺序字符串中获取加密密钥；

根据预定的加密算法，使用所述加密密钥对所述存储顺序字符串进行加密；

发送加密后的存储顺序字符串。

11、如权利要求 9 所述的装置，其特征在于，所述封存单元在拆分所述私钥为与所述密码模块数量对应的数量个部分时，具体用于：

读取所述私钥的长度；

将所述私钥平均分成长度一致的与所述密码模块数量对应的数量个部分。

12、如权利要求 9 所述的装置，其特征在于，所述区块链网络的各节点中还包含有密码模块存储长度的预定阈值，所述封存单元在拆分所述私钥为与所述密码模块数量对应的数量个部分时，具体用于：

拆分所述私钥为与所述密码模块数量对应的数量个部分，所述每个部分的长度均不超过密码模块存储长度的预定阈值。

13、如权利要求 8 所述的装置，其特征在于，所述区块链网络的各节点中还包含有私钥长度与密码模块数量的对应关系，所述创建单元具体用于：

读取所述私钥的长度；

查询私钥长度与密码模块数量的对应关系，确定需要创建的密码模块的数量；

创建与所述私钥长度对应的数量个密码模块。

14、如权利要求 8 所述的装置，其特征在于，所述区块链网络的各节点中还包含有密码模块存储长度的预定阈值，所述创建单元具体用于：

判断所述私钥的长度是否超过密码模块存储长度的预定阈值；

若所述私钥的长度超过密码模块存储长度的预定阈值，拆分所述私钥为至

少两个部分，且所述每个部分的长度都不超过密码模块存储长度的预定阈值；

创建与所述私钥部分的数量对应的数量个密码模块。

15、一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行以下步骤：

在区块链网络的一个节点中创建密码模块，所述创建有所述密码模块的节点为第一节点；

将所述第一节点的私钥封存在所述密码模块中；

将所述私钥随所述密码模块同步部署到所述区块链网络中除所述第一节点外的其他节点，其中，所述私钥只能通过特定接口进入密码模块进行访问。

16、如权利要求 15 所述的计算机设备，其特征在于，所述密码模块数量有至少两个，所述处理器在执行所述将所述第一节点的私钥封存在所述密码模块中时，具体执行以下步骤：

拆分所述私钥为与所述密码模块数量对应的数量个部分；

将所述私钥的不同部分分别存储在不同的密码模块中，每个密码模块只存储一个部分的私钥；

生成私钥的存储顺序，并将所述存储顺序动态加密，并存储在所述第一节点。

17、如权利要求 16 所述的计算机设备，其特征在于，所述存储顺序为一串字符串，所述处理器在执行将所述存储顺序动态加密，并存储在所述第一节点时，具体执行以下步骤：

获取需要加密的存储顺序字符串并进行存储；

对所述存储顺序的指定特征信息进行指定摘要运算；

根据所述指定摘要运算的结果，确定对所述存储顺序进行加密的起始字符；

从所述起始字符开始，在所述的存储顺序字符串中获取加密密钥；

根据预定的加密算法，使用所述加密密钥对所述存储顺序字符串进行加密；

发送加密后的存储顺序字符串。

18、如权利要求 16 所述的计算机设备，其特征在于，所述区块链网络的各节点中还包含有密码模块存储长度的预定阈值，所述处理器在执行所述拆分

所述私钥为与所述密码模块数量对应的数量个部分时，具体执行以下步骤：

拆分所述私钥为与所述密码模块数量对应的数量个部分，所述每个部分的长度均不超过密码模块存储长度的预定阈值。

19、如权利要求 15 所述的计算机设备，其特征在于，所述区块链网络的各节点中还包含有私钥长度与密码模块数量的对应关系，所述处理器在执行所述在所述区块链网络的一个节点中创建密码模块时，具体执行以下步骤：

读取所述私钥的长度；

查询私钥长度与密码模块数量的对应关系，确定需要创建的密码模块的数量；

创建与所述私钥长度对应的数量个密码模块。

20、一种存储有计算机可读指令的存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行如权利要求 1 至 7 中任一项所述的方法。

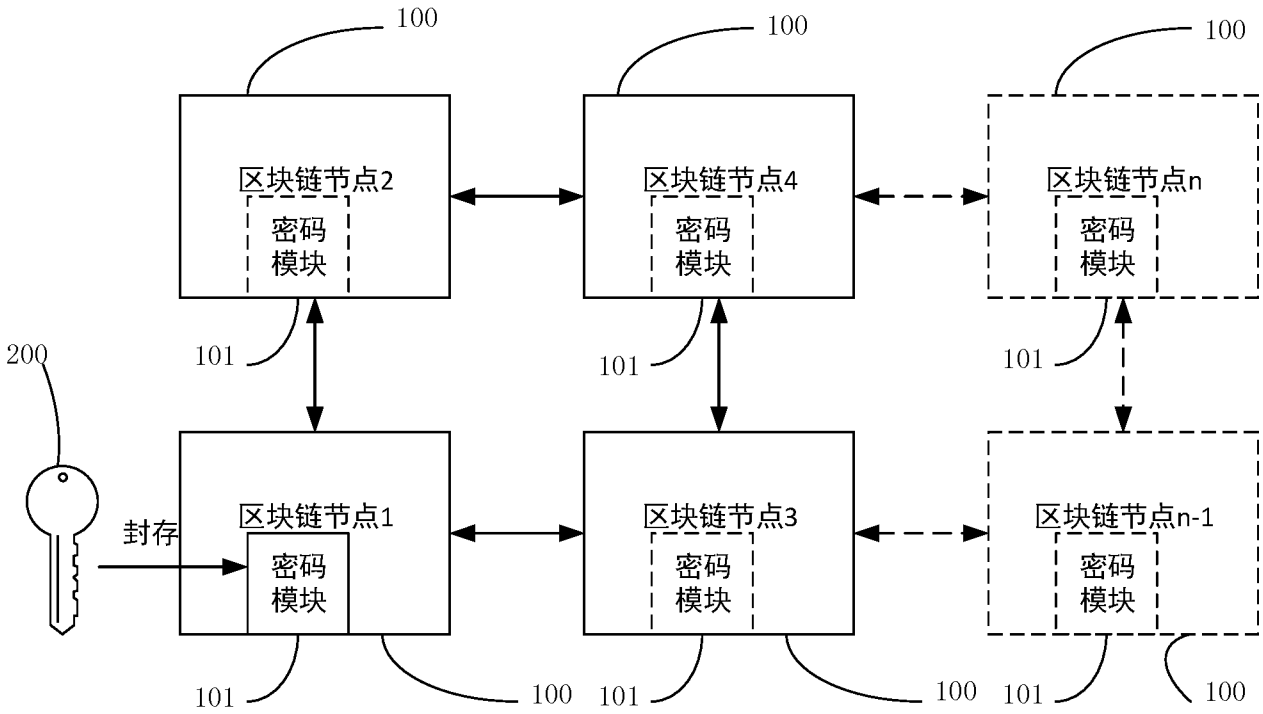
100
区块链节点2
密码模块
100
区块链节点4
密码模块
100
区块链节点n
密码模块
101
101
101
200
封存
区块链节点1
密码模块
区块链节点3
密码模块
区块链节点n-1
密码模块
101
100
101
100
101
100

图 1

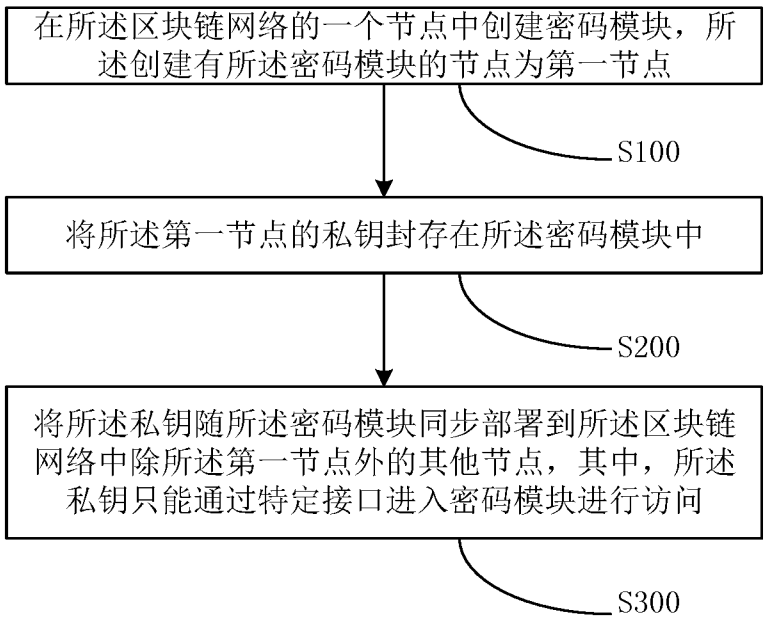
在所述区块链网络的一个节点中创建密码模块，所述创建有所述密码模块的节点为第一节点
S100
将所述第一节点的私钥封存在所述密码模块中
S200
将所述私钥随所述密码模块同步部署到所述区块链网络中除所述第一节点外的其他节点，其中，所述私钥只能通过特定接口进入密码模块进行访问
S300

图 2

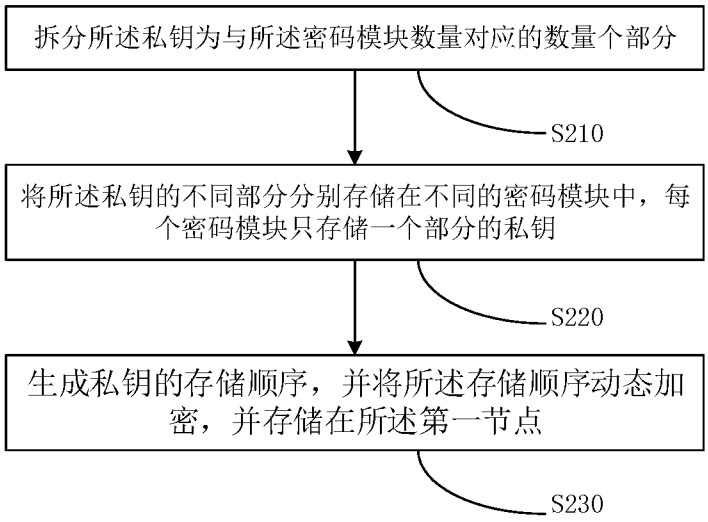
拆分所述私钥为与所述密码模块数量对应的数量个部分
S210
将所述私钥的不同部分分别存储在不同的密码模块中，每个密码模块只存储一个部分的私钥
S220
生成私钥的存储顺序，并将所述存储顺序动态加密，并存储在所述第一节点
S230

图 3

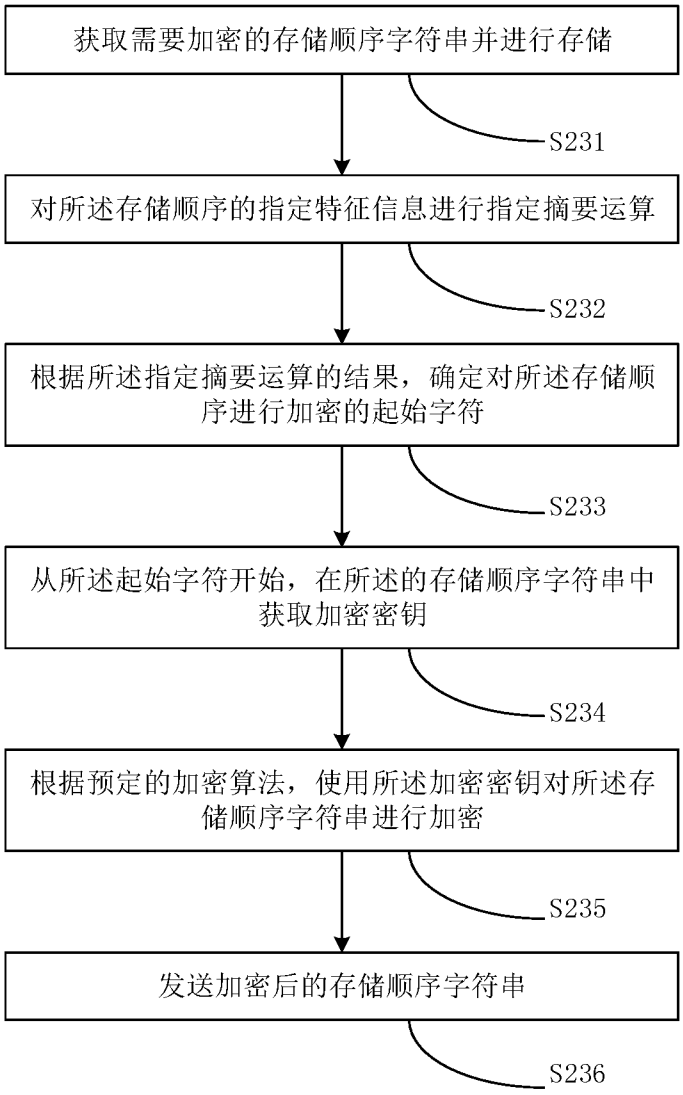
获取需要加密的存储顺序字符串并进行存储
S231
对所述存储顺序的指定特征信息进行指定摘要运算
S232
根据所述指定摘要运算的结果，确定对所述存储顺序进行加密的起始字符
S233
从所述起始字符开始，在所述的存储顺序字符串中获取加密密钥
S234
根据预定的加密算法，使用所述加密密钥对所述存储顺序字符串进行加密
S235
发送加密后的存储顺序字符串
S236

图 4

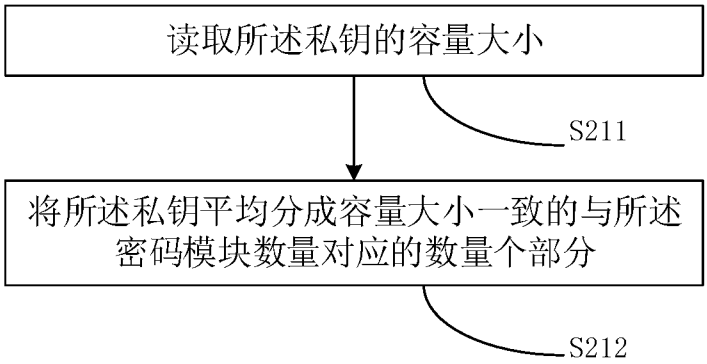
读取所述私钥的容量大小
S211
将所述私钥平均分成容量大小一致的与所述密码模块数量对应的数量个部分
S212

图 5

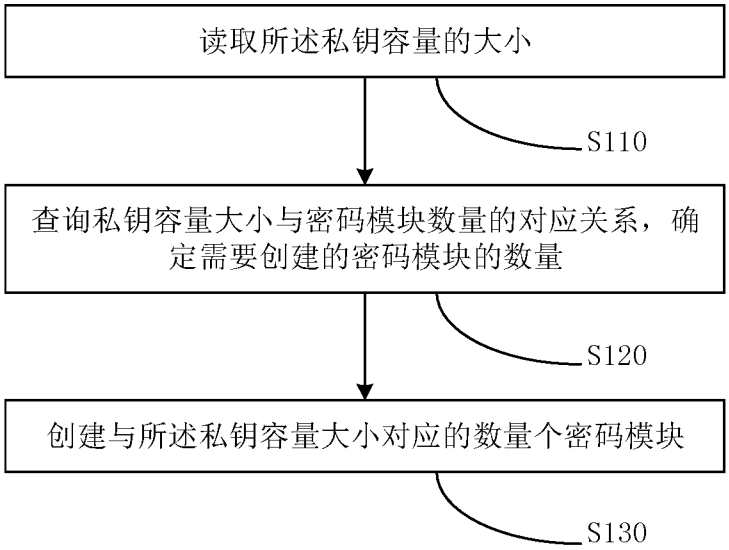
读取所述私钥容量的大小
S110
查询私钥容量大小与密码模块数量的对应关系，确定需要创建的密码模块的数量
S120
创建与所述私钥容量大小对应的数量个密码模块
S130

图 6

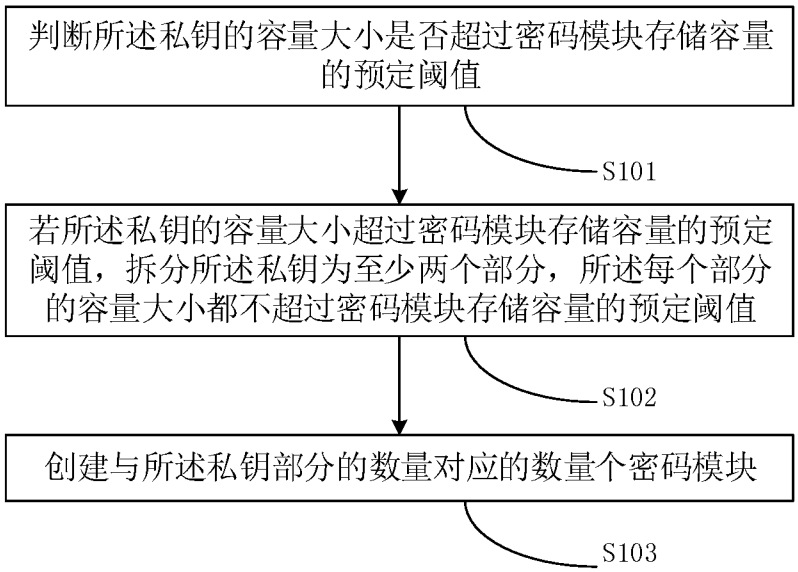
判断所述私钥的容量大小是否超过密码模块存储容量的预定阈值
S101
若所述私钥的容量大小超过密码模块存储容量的预定阈值，拆分所述私钥为至少两个部分，所述每个部分的容量大小都不超过密码模块存储容量的预定阈值
S102
创建与所述私钥部分的数量对应的数量个密码模块
S103

图 7

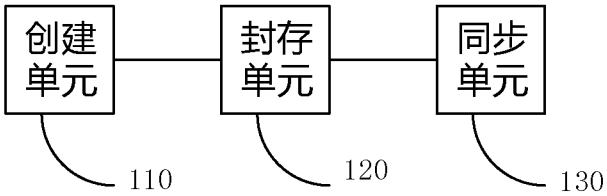
创建单元
封存单元
同步单元
110
120
130

图 8

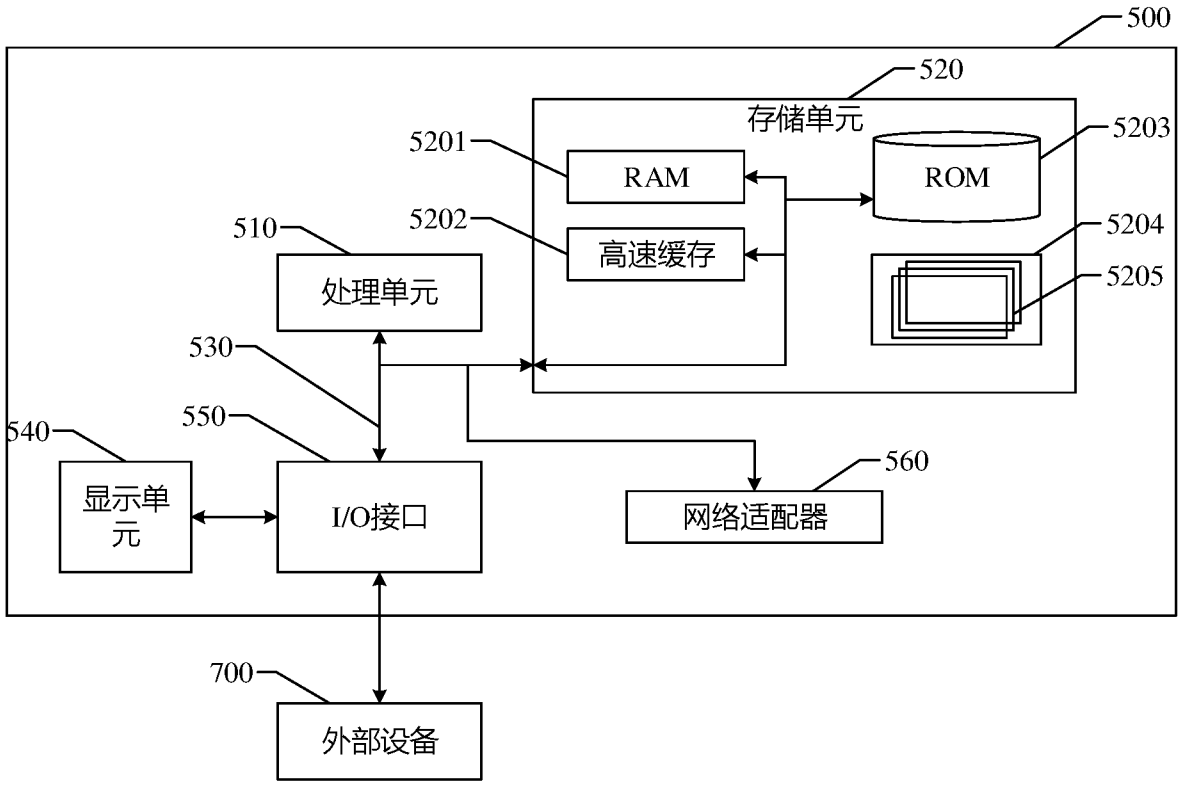
500
520
存储单元
5201
RAM
ROM
5203
5202
高速缓存
5204
510
处理单元
5205
530
550
540
显示单元
I/O接口
网络适配器
560
700
外部设备

图 9

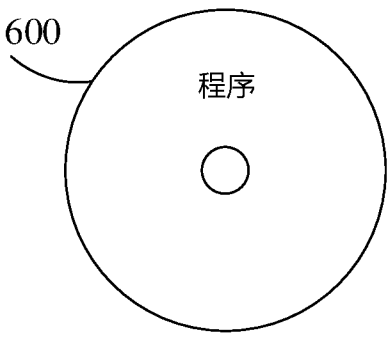
600
程序

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/123026

A. CLASSIFICATION OF SUBJECT MATTER

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

CNPAT, CNKI, WPI, EPODOC, GOOGLE: 密钥, 私钥, 私有密钥, 区块, 同步, 复制, 备份, 其他, 其它, 第二, 另一, KEY, block chain, synchroni+, replicat+, backup, second, other

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110086607 A (ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) 02 August 2019 (2019-08-02) claims 1-10	1-20
X	CN 107483446 A (SHANGHAI DIANRONG INFORMATION TECHNOLOGY CO., LTD.) 15 December 2017 (2017-12-15) description, paragraphs [0038], [0039], and [0047]-[0053], and figure 5	1-20
A	CN 109345386 A (ALIBABA GROUP HOLDING LIMITED) 15 February 2019 (2019-02-15) entire document	1-20
A	US 2018083932 A1 (BANK OF AMERICA CORPORATION) 22 March 2018 (2018-03-22) 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	Date of mailing of the international search report
14 January 2020	**27 February 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/123026

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110086607 A	02 August 2019	None	
CN 107483446 A	15 December 2017	HK 1248039 A0	05 October 2018
CN 109345386 A	15 February 2019	None	
US 2018083932 A1	22 March 2018	None	

国际检索报告

国际申请号
PCT/CN2019/123026

A. 主题的分类

H04L 9/08(2006.01)i; H04L 29/08(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）)

CNPAT, CNKI, WPI, EPODOC, GOOGLE：密钥，私钥，私有密钥，区块，同步，复制，备份，其他，其它，第二，另一，KEY, block chain, synchroni+, replicat+, backup, second, other

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
PX	CN 110086607 A (深圳壹账通智能科技有限公司) 2019年 8月 2日 (2019-08-02) 权利要求1-10	1-20
X	CN 107483446 A (上海点融信息科技有限责任公司) 2017年 12月 15日 (2017-12-15) 说明书第[0038]-[0039]、[0047]-[0053]段，图5	1-20
A	CN 109345386 A (阿里巴巴集团控股有限公司) 2019年 2月 15日 (2019-02-15) 全文	1-20
A	US 2018083932 A1 (BANK OF AMERICA CORPORATION) 2018年 3月 22日 (2018-03-22) 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	国际检索报告邮寄日期
2020年 1月 14日	2020年 2月 27日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	王怡轩
传真号 (86-10)62019451	电话号码 86-10-53961621

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/123026

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 110086607 A	2019年 8月 2日	无	
CN 107483446 A	2017年 12月 15日	HK 1248039 A0	2018年 10月 5日
CN 109345386 A	2019年 2月 15日	无	
US 2018083932 A1	2018年 3月 22日	无	